# **NIST SPECIAL PUBLICATION 1800-10B**

# Protecting Information and System Integrity in Industrial Control System Environments:

Cybersecurity for the Manufacturing Sector

#### Volume B:

Approach, Architecture, and Security Characteristics

#### **Michael Powell**

National Cybersecurity Center of Excellence National Institute of Standards and Technology

Michael Pease Keith Stouffer CheeYee Tang Timothy Zimmerman Engineering Laboratory National Institute of Standards and Technology Joseph Brule Chelsea Deane John Hoyt Mary Raguso Aslam Sherule Kangmin Zheng The MITRE Corporation McLean, Virginia

#### **Matthew Zopf**

Strativia Largo, Maryland

FINAL

March 2022

This publication is available free of charge from <a href="https://doi.org/10.6028/NIST.SP.1800-10">https://doi.org/10.6028/NIST.SP.1800-10</a>

The first draft of this publication is available free of charge from <u>https://www.nccoe.nist.gov/publications/practice-guide/protecting-information-and-system-integrity-industrial-control-system-draft</u>





#### **DISCLAIMER**

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCOE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Domain name and IP addresses shown in this guide represent an example domain and network environment to demonstrate the NCCoE project use case scenarios and the security capabilities.

National Institute of Standards and Technology Special Publication 1800-10B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-10B, 149 pages, March 2022, CODEN: NSPUE2

#### **FEEDBACK**

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at <u>manufacturing nccoe@nist.gov</u>.

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence National Institute of Standards and Technology 100 Bureau Drive Mailstop 2002 Gaithersburg, MD 20899 Email: <u>nccoe@nist.gov</u>

#### NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST *Cybersecurity Framework* (CSF) and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit <u>https://www.nist.gov</u>.

#### NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

#### ABSTRACT

Today's manufacturing organizations rely on industrial control systems (ICS) to conduct their operations. Increasingly, ICS are facing more frequent, sophisticated cyber attacks—making manufacturing the second-most-targeted industry [1]. Cyber attacks against ICS threaten operations and worker safety, resulting in financial loss and harm to the organization's reputation.

The architecture and solutions presented in this guide are built upon standards-based, commercially available products, and represent some of the possible solutions. The solutions implement standard cybersecurity capabilities such as behavioral anomaly detection (BAD), application allowlisting (AAL), file

integrity-checking, change control management, and user authentication and authorization. The solution was tested in two distinct lab settings: a discrete manufacturing workcell, which represents an assembly line production, and a continuous process control system (PCS), which represents chemical manufacturing industries.

An organization that is interested in protecting the integrity of a manufacturing system and information from destructive malware, insider threats, and unauthorized software should first conduct a risk assessment and determine the appropriate security capabilities required to mitigate those risks. Once the security capabilities are identified, the sample architecture and solution presented in this document may be used.

The security capabilities of the example solution are mapped to the <u>NIST Cybersecurity Framework</u>, the <u>National Initiative for Cybersecurity Education Framework</u>, and <u>NIST Special Publication 800-53</u>.

#### **KEYWORDS**

Application allowlisting; behavioral anomaly detection; file integrity checking; firmware modification; industrial control systems; manufacturing; remote access; software modification; user authentication; user authorization.

#### **ACKNOWLEDGEMENTS**

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Dan Frechette	Microsoft
lan Schmertzler	Dispel
Ben Burke	Dispel
Chris Jensen	Tenable
Bethany Brower	VMWare
Dennis Hui	OSIsoft (now part of AVEVA)
John Matranga	OSIsoft (now part of AVEVA)
Michael A. Piccalo	Forescout
Tim Jones	Forescout
Yejin Jang	Forescout
Samantha Pelletier	TDI Technologies
Rusty Hale	TDI Technologies
Steve Petruzzo	GreenTec

Name	Organization
Josh Carlson	Dragos
Alex Baretta	Dragos

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Product
Carbon Black (VMware)	Carbon Black App Control
<u>Microsoft</u>	Azure Defender for the internet of things (IoT) (incorporating technology from the acquisition of CyberX)
<u>Dispel</u>	Dispel Wicket ESI
	Dispel Enclave
	Dispel VDI (Virtual Desktop Interface)
<u>Dragos</u>	Dragos Platform
Forescout	eyeInspect (Formerly SilentDefense)
	ICS Patrol
	EyeSight
GreenTec	WORMdisk and ForceField
OSIsoft (now part of AVEVA)	PI System (which comprises products such as PI Server, PI Vision and others)
TDi Technologies	ConsoleWorks
Tenable	Tenable.ot

#### **DOCUMENT CONVENTIONS**

The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

iv

#### **PATENT DISCLOSURE NOTICE**

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

# Contents

1	Sun	nmary1			
	1.1	Challenge2			
	1.2	Solution			3
		1.2.1	Relevant S	tandards and Guidance	4
	1.3	Benefits			4
2	Hov	v to Use	e This Gu	ide	5
	2.1	Typogra	phic Conve	ntions	6
3	Арр	roach.	•••••		8
	3.1	Audienc	e		8
	3.2	Scope			8
	3.3	Assumpt	tions		9
	3.4	Risk Asse	essment	1	.0
		3.4.1	Threats		.0
		3.4.2	Vulnerabili	ties 1	.1
		3.4.3	Risk		.2
		3.4.4	Security Co	ontrol Map 1	.2
	3.5	Technologies15			
4	Arcl	hitecture			
	4.1	Manufad	cturing Pro	cess and Control System Description1	9
	4.2	Cyberse	curity for S	mart Manufacturing Systems Architecture1	9
	4.3	Process	Control Sys		0
	4.4	Collabor	ative Robo	tics System (CRS)2	3
	4.5	Logical Network and Security Architectures25			
		4.5.1	Build 1		6
		4.5.2	Build 2		9
		4.5.3	Build 3		2
		4.5.4	Build 4		4

5	Sec	urity Cł	naracteristic Analysis	36
	5.1	Assump	tions and Limitations	36
	5.2	Example	e Solution Testing	36
		5.2.1	Scenario 1: Protect Host from Malware Infection via USB	. 37
		5.2.2	Scenario 2: Protect Host from Malware Infection via Network Vector	. 37
		5.2.3	Scenario 3: Protect Host from Malware via Remote Access Connections	. 39
		5.2.4	Scenario 4: Protect Host from Unauthorized Application Installation	. 40
		5.2.5	Scenario 5: Protect from Unauthorized Addition of a Device	. 42
		5.2.6	Scenario 6: Detect Unauthorized Device-to-Device Communications	. 43
		5.2.7	Scenario 7: Protect from Unauthorized Deletion of Files	. 43
		5.2.8	Scenario 8: Detect Unauthorized Modification of PLC Logic	. 45
		5.2.9	Scenario 9: Protect from Modification of Historian Data	. 46
	5.3	Scenario	os and Findings	49
		5.3.1	PR.AC-1: Identities and Credentials are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes	d . 50
		5.3.2	PR.AC-3: Remote Access is Managed	. 50
		5.3.3	PR.AC-4: Access Permissions and Authorizations are Managed, Incorporating th Principles of Least Privilege and Separation of Duties	e . 50
		5.3.4	PR.AC-7: Users, Devices, and Other Assets are Authenticated (e.g., single-factor multi-factor) Commensurate with the Risk of the Transaction (e.g., Individual Security and Privacy Risks and Other Organizational Risks)	, 50
		5.3.5	PR.DS-1: Data-at-Rest is Protected	. 51
		5.3.6	PR.DS-6: Integrity Checking Mechanisms are Used to Verify Software, Firmware and Information Integrity	51.
		5.3.7	PR.IP-4: Backups of Information are Conducted, Maintained, and Tested	. 51
		5.3.8	PR.MA-1: Maintenance and Repair of Organizational Assets are Performed and Logged, with Approved and Controlled Tools	. 51
		5.3.9	PR.MA-2: Remote Maintenance of Organizational Assets is Approved, Logged, a Performed in a Manner that Prevents Unauthorized Access	and . 51
		5.3.10	DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users a Systems is Established and Managed	and . 52
		5.3.11	DE.AE-2: Detected Events are Analyzed to Understand Attack Targets And Meth	10ds . 52

	5.3.12	DE.AE-3: Event Data are Collected and Correlated from Multiple Sources and Sensors	52
	5.3.13	DE.CM-1: The Network is Monitored to Detect Potential Cybersecurity Events !	52
	5.3.14	DE.CM-3: Personnel Activity is Monitored to Detect Potential Cybersecurity Even	ts 52
	5.3.15	DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software is Performed	53
6 Futu	ure Buil	d Considerations5	4
Append	lix A Li	st of Acronyms	1
Append	lix B G	lossary	3
Append	lix C Re	eferences	6
Append	lix D So	enario Execution Results	8
D.1	Executing	g Scenario 1: Protect Host from Malware via USB	.8
	D.1.1	Build 1	.8
	D.1.1.1	Configuration	.8
	D.1.1.2	Test Results	.8
	D.1.2	Build 2	10
	D.1.2.1	Configuration	10
	D.1.2.2	Test Results	10
	D.1.3	Build 3	11
	D.1.3.1	Configuration	11
	D.1.3.2	Test Results	11
	D.1.4	Build 4	12
	D.1.4.1	Configuration	12
	D.1.4.2	Test Results	12
D.2	Executin	g Scenario 2: Protect Host from Malware via Network Vector	13
	D.2.1	Build 1	14
	D.2.1.1	Configuration	14
	D.2.1.2	Test Results	14
	D.2.2	Build 2	18

	D.2.2.1	Configuration 1	.8
	D.2.2.2	Test Results 1	.8
	D.2.3	Build 3 2	24
	D.2.3.1	Configuration 2	24
	D.2.3.2	Test Results 2	24
	D.2.4	Build 4 2	28
	D.2.4.1	Configuration 2	28
	D.2.4.2	Test Results 2	28
D.3	Executin	g Scenario 3: Protect Host from Malware via Remote Access Connections .3	2
	D.3.1	Build 1	3
	D.3.1.1	Configuration	3
	D.3.1.2	Test Results	3
	D.3.2	Build 2	\$5
	D.3.2.1	Configuration	\$5
	D.3.2.2	Test Results	\$5
	D.3.3	Build 3	57
	D.3.3.1	Configuration	57
	D.3.3.2	Test Results 3	57
	D.3.4	Build 4	9
	D.3.4.1	Configuration	9
	D.3.4.2	Test Results	9
D.4	Executin	g Scenario 4: Protect Host from Unauthorized Application Installation4	1
	D.4.1	Build 1	1
	D.4.1.1	Configuration 4	1
	D.4.1.2	Test Results 4	2
	D.4.2	Build 2	3
	D.4.2.1	Configuration 4	3
	D.4.2.2	Test Results 4	4
	D.4.3	Build 3	6
	D.4.3.1	Configuration 4	6
	D.4.3.2	Test Results 4	6

	D.4.4	Build 4	. 50
	D.4.4.1	Configuration	. 50
	D.4.4.2	Test Results	. 50
D.5	Executir	ng Scenario 5: Protect from Unauthorized Addition of a Device	54
	D.5.1	Build 1	. 54
	D.5.1.1	Configuration	. 54
	D.5.1.2	Test Results	. 54
	D.5.2	Build 2	. 56
	D.5.2.1	Configuration	. 56
	D.5.2.2	Test Results	. 56
	D.5.3	Build 3	. 57
	D.5.3.1	Configuration	. 57
	D.5.3.2	Test Results	. 57
	D.5.4	Build 4	. 59
	D.5.4.1	Configuration	. 59
	D.5.4.2	Test Results	. 59
D.6	Executir	ng Scenario 6: Detect Unauthorized Device-to-Device Communications	62
	D.6.1	Build 1	. 63
	D.6.1.1	Configuration	. 63
	D.6.1.2	Test Results	. 63
	D.6.2	Build 2	. 63
	D.6.2.1	Configuration	. 63
	D.6.2.2	Test Results	. 63
	D.6.3	Build 3	. 64
	D.6.3.1	Configuration	. 64
	D.6.3.2	Test Results	. 64
	D.6.4	Build 4	. 65
	D.6.4.1	Configuration	. 65
	D.6.4.2	Test Results	. 65
D.7	Executin	ng Scenario 7: Protect from Unauthorized Deletion of Files	66
	_//0000000	5	

	D.7.1.1	Configuration	66
	D.7.1.2	Test Results	66
	D.7.2	Build 2	67
	D.7.2.1	Configuration	67
	D.7.2.2	Test Results	67
	D.7.3	Build 3	68
	D.7.3.1	Configuration	68
	D.7.3.2	Test Results	68
	D.7.4	Build 4	68
	D.7.4.1	Configuration	68
	D.7.4.2	Test Results	69
D.8	Executin	g Scenario 8: Detect Unauthorized Modification of PLC Logic	.69
	D.8.1	Build 1	69
	D.8.1.1	Configuration	69
	D.8.1.2	Test Results	70
	D.8.2	Build 2	73
	D.8.2.1	Configuration	73
	D.8.2.2	Test Results	73
	D.8.3	Build 3	76
	D.8.3.1	Configuration	76
	D.8.3.2	Test Results	76
	D.8.4	Build 4	79
	D.8.4.1	Configuration	79
	D.8.4.2	Test Results	79
D.9	Executin	g Scenario 9: Protect from Modification of Historian Data	.82
	D.9.1	Build 1	82
	D.9.1.1	Configuration	82
	D.9.1.2	Test Results	83
	D.9.2	Build 2	84
	D.9.2.1	Configuration	. 84
	D.9.2.2	Test Results	85

	D.9.3	Build 3		86
	D.9.3.1	Configurati	on	86
	D.9.3.2	Test Result	s	87
	D.9.4	Build 4		88
	D.9.4.1	Configurati	on	88
	D.9.4.2	Test Result	s	89
D.10	Executin	g Scenario	10: Detect Sensor Data Manipulation	.90
	D.10.1	All Builds		90
	D.10.1.1	Configurati	on	90
	D.10.1.2	Test Result	S	91
D.11	Executin	g Scenario	11: Detect Unauthorized Firmware Modification	.91
	D.11.1	Build 1		91
	D.11.1.1	Configurati	on	91
	D.11.1.2	Test Result	s	92
	D.11.2	Build 2		93
	D.11.2.1	Configurati	on	93
	D.11.2.2	Test Result	S	93
	D.11.3	Build 3		95
	D.11.3.1	Configurati	on	95
	D.11.3.2	Test Result	S	95
	D.11.4	Build 4		96
	D.11.4.1	Configurati	on	96
	D.11.4.2	Test Result	S	96
Append	lix E B	enefits o	f IoT Cybersecurity Capabilities	98
E.1	Device C	apabilities	Mapping	.98
E.2	Device C	apabilities	Supporting Functional Test Scenarios	L17

# List of Figures

Figure 4-2 Simplified Tennessee Eastman Process Model
Figure 4-3 HMI Screenshot for the PCS Showing the Main Components in the Process
Figure 4-4 PCS Network
Figure 4-5 The CRS Workcell
Figure 4-6 CRS Network25
Figure 4-7 Build 1, PCS Complete Architecture with Security Components
Figure 4-8 Build 2, PCS Complete Architecture with Security Components
Figure 4-9 Build 3, CRS Complete Architecture with Security Components
Figure 4-10 Build 4, CRS Complete Architecture with Security Components
Figure D-1 An Alert from Carbon Black Showing that Malware (1.exe) was Blocked from Executing 9
Figure D-2: Carbon Black's Server Provides Additional Details and Logs of the Event
Figure D-3 Carbon Black's Server Log of the Event
Figure D-4 Windows 7 Alert as a Result of Windows SRP Blocking the Execution of 1.exe
Figure D-5 Windows 10 Alert as a Result of Windows SRP Blocking the Execution of 1.exe11
Figure D-6 Carbon Black Blocks the Execution of 1.exe for Build 4
Figure D-7 Tenable.ot Dashboard Showing the Events that were Detected
Figure D-8 Detected RDP Session Activity from External System to DMZ System
Figure D-9 Event Detection Detail for the RDP Connection from the External System to the Historian in the DMZ
Figure D-10 Tenable.ot Detected VNC Connection Between the DMZ and the Testbed LAN
Figure D-11 Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in the Testbed LAN
Figure D- 12 Detected RDP from a DMZ system to a Testbed LAN system
Figure D-13 Tenable.ot Event Detail Showing the RDP Connection Between the Historian in the DMZ to a Workstation in the Testbed LAN
Figure D-14 Attempt to Execute 1.exe Failed
Figure D-15 Alert Dashboard Showing Detection of an RDP Session
Figure D-16 Details of the Detected RDP Session Activity from an External System to DMZ System 20

Figure D-17 Detection of Scanning Traffic and RDP Connection into Manufacturing Environment 21
Figure D-18 Details of One of the Port Scan Alerts
Figure D-19 Details of Alert for RDP Connection into Manufacturing Environment
Figure D-20 Dialog Message Showing 1.exe was Blocked from Executing
Figure D-21 Windows SRP blocked 1.exe From Executing
Figure D-22 Log of Alerts Detected by Dragos
Figure D-23 Detail of RDP Session Activity Between an External System and a DMZ System
Figure D-24 Detail for Network Scanning Alert
Figure D-25 Detail of RDP Session Activity Between a DMZ System and a Testbed LAN System
Figure D-26 Azure Defender for IoT "info" Event Identified Remote Access Connection to the DMZ 28
Figure D-27 Alert for Scanning Activity
Figure D-28 Details for the Scanning Alert
Figure D-29 Detection of RDP Connection into the Manufacturing Environment
Figure D-30 Carbon Black Shows an Alert for Blocking File 1.exe
Figure D-31 Secured VPN Connection to Environment with Cisco AnyConnect
Figure D-32 Remote Access is Being Established Through ConsoleWorks
Figure D-33 Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket ESI 36
Figure D-34 Nested RDP Session Showing Dispel Connection into the PCS Workstation
Figure D-35 VPN Connection to Manufacturing Environment
Figure D-36 Remote Access is Being Established Through ConsoleWorks
Figure D-37 Dispel VDI Showing Interface for Connecting Through Dispel Enclave to Dispel Wicket 40
Figure D-38 Nested RDP Session Showing Dispel Connection into the CRS Workstation
Figure D-39 Carbon Black Blocks the Execution of putty.exe and Other Files
Figure D-40 Tenable.ot Alert With the SMB Connection Between the HMI and the GreenTec Server 43
Figure D-41 Tenable.ot Alert Details of the SMB Connection Between the HMI and the network file system (NFS) Server in the DMZ
Figure D-42 Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration
Figure D-43 putty-64bit-0.74-installer.msi is blocked by Windows SRP

Figure D-44 Forescout Alert on the File Transfer Activity
Figure D-45 Forescout Alert Details for the File Transfer Activity
Figure D-46 Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration
Figure D-47 putty-64bit-0.74-installer.msi is Blocked by Windows SRP
Figure D-48 Dragos Alert on the File Transfer Activity
Figure D-49 Dragos Alert Details of the File Transfer Alert
Figure D-50 Carbon Black Alert Showing that putty.exe is Blocked from Executing
Figure D-51 Carbon Black Alert Showing Execution of putty-64bit-0.74-installer.msi Being Blocked 52
Figure D-52 Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity
Figure D-53 Azure Defender for IoT Alert Details Showing RPC Connection Between the DMZ and the Testbed LAN
Figure D-54 Azure Defender for IoT Event Alert Timeline Showing the File Transfer
Figure D-55 Tenable.ot Event Showing a New Asset has Been Discovered
Figure D-56 Tenable.ot Event Showing Unauthorized SSH Activities
Figure D-57 Forescout Alert on the DNS Request from the New Device
Figure D-58 Forescout alert showing the SSH connection
Figure D-59 Detailed Forescout alert of the Unauthorized SSH Connection
Figure D-60 Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network Scanning
Figure D-61 Details of Network Scanning Activity
Figure D-62 Additional Details of Network Scanning Activity
Figure D-63 Alert for New Asset on the Network
Figure D-64 Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset 60
Figure D-65 Azure Defender for IoT Detects New Asset in the Environment
Figure D-66 Azure Defender for IoT Alert Management Options
Figure D-67 Details for Network Scanning Alert
Figure D-68 Tenable.ot Event Log Showing the Unapproved SSH Traffic
Figure D-69 Forescout Alert Showing the Unapproved SSH Traffic
Figure D-70 Dragos Alert Showing the Unapproved SSH Connection Between Devices

Figure D-71 Azure Defender for IoT Event Identified the Unauthorized SSH Connection
Figure D-72 Event Messages from Carbon Black Showing File Deletion Attempts
Figure D-73 Security Onion Wazuh Alert Showing a File Has Been Deleted
Figure D-74 Alert from Security Onion for a File Deletion
Figure D-75 Carbon Black Alerts Showing That a File Has Been Deleted
Figure D-76 Remote Access to Systems in PCS Network is Established Through ConsoleWorks71
Figure D-77 Remote Session into Studio 5000 to Perform PLC File Operations
Figure D-78 Tenable.ot Detected the Transfer of PLC Logic File to the Rockwell PLC
Figure D-79 Tenable.ot PLC Stop alert details
Figure D-80 Tenable.ot PLC Program Download Alert Details
Figure D-81 Remote Access to Systems in PCS Network is Being Established Through Dispel
Figure D-82 Modifying the Parameters for the Allen-Bradley PLC Controller Using Studio 500074
Figure D-83 Forescout Alerts Showing It Detected the Traffic Between the Engineering Workstation and the PLC
Figure D-84 Forescout Alert Details for the Stop Command Issued to the PLC75
Figure D-85 Forescout Alert Details for the Configuration Download Command
Figure D-86 VPN Connection to the Manufacturing Environment
Figure D-87 Remote Access is Being Established through ConsoleWorks
Figure D-88 Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the Beckhoff PLC
Figure D-89 Dragos Alert Details for the PLC Logic File Download
Figure D-90 Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket
Figure D-91 Nested RDP Connections Showing Dispel Connection into the CRS Workstation
Figure D-92 Azure Defender for IoT Alert for Unauthorized PLC Programming
Figure D-93 Tenable.ot alert Shows SMB Connection from External Workstation to the Historian 83
Figure D-93 Tenable.ot alert Shows SMB Connection from External Workstation to the Historian 83 Figure D-94 GreenTec Denies Modification and Deletion File Operations in the Protected Drive 84
Figure D-93 Tenable.ot alert Shows SMB Connection from External Workstation to the Historian 83 Figure D-94 GreenTec Denies Modification and Deletion File Operations in the Protected Drive 84 Figure D-95 Forescout Alert Shows Network Connection from Corporate Network to the Historian 85
Figure D-93 Tenable.ot alert Shows SMB Connection from External Workstation to the Historian 83 Figure D-94 GreenTec Denies Modification and Deletion File Operations in the Protected Drive 84 Figure D-95 Forescout Alert Shows Network Connection from Corporate Network to the Historian 85 Figure D-96 GreenTec Denies Modification and Deletion File Operations in the Protected Drive 86

Figure D-98 GreenTec Denies Modification and Deletion File Operations in the Protected Drive 88
Figure D-99 Azure Defender for IoT Event Timeline Showing the Remote Access Connection to the Historian
Figure D-100 GreenTec Denies Modification and Deletion File Operations in the Protected Drive 90
Figure D-101 PI Server's Event Frames Showing Out-of-Range Sensor Readings for the Reactor Pressure
Figure D-102 Tenable.ot Detects a Collection of Events Generated by a Firmware Change
Figure D-103 Details for One of the Alerts Showing the Firmware Change
Figure D-104 Forescout Detects a Collection of Alerts Associated with the Firmware Change
Figure D-105 Alert Details Detected by Forescout for the Firmware Change
Figure D-106 ICS Patrol Scan Results Showing a Change Configuration was Made
Figure D-107 Dragos Dashboard Showing an Alert for Firmware Change
Figure D-108 Details for Firmware Change Alert96
Figure D-109 Azure Defender for IoT Alert Showing a Version Mismatch in the Firmware Build

# **List of Tables**

Table 3-1 Security Control Map	13
Table 3-2 Products and Technologies	15
Table 4-1 Summary of What Products Were Used in Each Build	18
Table 4-2 Build 1 Technology Stack to Capabilities Map	26
Table 4-3 Build 2 Technology Stack to Capabilities Map	29
Table 4-4 Build 3 Technology Stack to Capabilities Map	32
Table 4-5 Build 4 Technology Stack to Capabilities Map	34

Table E-1 Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities to	C
NIST Cybersecurity Framework Subcategories of the ICS Project	99
Table E-2 Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities that Map to E	ach
of the Functional Test Scenarios	119

## **1** Summary

While availability is always a critical aspect of manufacturing system environments, manufacturers also need to consider maintaining the integrity of their systems and information to ensure continued operations. The integrity of information can be degraded or lost as a result of behaviors by authorized users (e.g., failure to perform backups or record their actions) or malicious actors seeking to disrupt manufacturing operations for illicit profits, political statements, or other reasons.

Manufacturers are unique because of their reliance on industrial control systems (ICS) to monitor and control their manufacturing operations. ICS typically prioritize information availability and integrity over confidentiality. As a result, cybersecurity solutions used in traditional information technology (IT) settings are not optimized to protect ICS from cyber threats.

This guide, prepared by the National Cybersecurity Center of Excellence (NCCoE) and the NIST Engineering Laboratory (EL), contains four examples of practical solutions that organizations can implement in their environments to protect ICS from information and system integrity attacks.

The goal of this NIST Cybersecurity Practice Guide is to help organizations protect the integrity of systems and information by:

- securing historical system data
- preventing execution or installation of unapproved software
- detecting anomalous behavior on the network
- identifying hardware, software, or firmware modifications
- enabling secure remote access
- authenticating and authorizing users

This document provides a detailed description of how each solution was implemented and what technologies were used to achieve each of the above listed goals across four example builds. Scenarios are used to demonstrate the efficacy of the solutions. The results and challenges of each scenario in the four example builds are also presented and discussed.

Ultimately, manufacturing organizations that rely on ICS can use the example solutions described in this guide to safeguard their information and system integrity from:

- destructive malware
- insider threats
- unauthorized software
- unauthorized remote access

- loss of historical data
- anomalous network traffic
- unauthorized modification of systems

This document contains the following sections:

<u>Section 1, Summary</u>, presents the challenges addressed by the NCCoE project, with a look at the solutions demonstrated to address the challenge, as well as benefits of the solutions.

<u>Section 2, How to Use This Guide</u>, explains how readers—business decision makers, program managers, control system engineers, cybersecurity practitioners, and IT professionals (e.g., systems administrators)— might use each volume of this guide.

<u>Section 3, Approach</u>, offers a description of the intended audience and the scope of the project. This section also describes the assumptions on which the security architecture and solution development was based, the risk assessment that informed architecture development, the NIST *Cybersecurity Framework* functions supported by each component of the architecture and reference design, and which industry collaborators contributed support in building, demonstrating, and documenting the solutions. This section also includes a mapping of the NIST *Cybersecurity Framework* Subcategories to other industry guidance, and identifies the products used to address each subcategory.

<u>Section 4, Architecture</u>, summarizes the Cybersecurity for Smart Manufacturing Systems (CSMS) demonstration environment, which emulates real-world manufacturing processes and their ICS by using software simulators and commercial off-the-shelf hardware in a laboratory environment. The implementation of the information and system integrity solutions is also described.

<u>Section 5, Security Characteristic Analysis</u>, summarizes the scenarios and findings that were employed to demonstrate the example implementations' functionality. Each of the scenarios is mapped to the relevant NIST *Cybersecurity Framework* functions and Subcategories and the security capabilities of the products that were implemented. Additionally, it briefly describes how the security capabilities that were used in the solution implementation help detect cyber attacks and protect the integrity of the manufacturing systems and information.

<u>Section 6, Future Build Considerations</u>, identifies additional areas that should be reviewed in future practice guides.

Section <u>Appendix D, Scenario Execution Results</u>, describes, in detail, the test results of the scenarios, including screenshots from the security products captured during the tests.

#### 1.1 Challenge

Manufacturing organizations that rely on ICS to monitor and control physical processes face risks from malicious and non-malicious insiders along with external threats in the form of increasingly

sophisticated cyber attacks. A compromise to system or information integrity may very well pose a significant threat to human safety and can adversely impact an organization's operations, resulting in financial loss and harm production for years to come.

Manufacturing organizations may be the targets of malicious cyber actors or may be incidentally impacted by a broader malware event such as ransomware attacks. ICS components remain vulnerable to cyber attacks for numerous reasons, including adoption and integration of enhanced connectivity, remote access, the use of legacy technologies, flat network topologies, lack of network segmentation, and the lack of cybersecurity technologies (e.g., anti-virus, host-based firewalls, encryption) typically found on IT systems.

Organizations are increasingly adopting and integrating IT into the ICS environment to enhance connectivity to business systems and to enable remote access. As a result, ICS are no longer isolated from the outside world, making them more vulnerable to cyber attacks. Security controls designed for the IT environment may impact the performance of ICS when implemented within the operational technology (OT) environment, so special precautions are required when introducing these controls. In some cases, new security techniques tailored to the specific ICS environment are needed.

Another challenge facing manufacturing organizations comes from authorized users who accidentally or intentionally compromise information and system integrity. For example, a user may install an unapproved software utility to perform maintenance activities or update the logic of a programmable logic controller (PLC) to fix a bug. Even if the software or logic changes are not malicious, they may inadvertently disrupt information flows, starve critical software of processing resources, or degrade the operation of the system. In a worst-case scenario, malware may be inadvertently installed on the manufacturing system, causing disruptions to system operations, or opening a backdoor to remote attackers.

#### **1.2 Solution**

This NCCoE Cybersecurity Practice Guide demonstrates how manufacturing organizations can use commercially available technologies that are consistent with cybersecurity standards to detect and prevent cyber incidents on their ICS.

Manufacturers use a wide range of ICS equipment and manufacturing processes. This guide contains four different example solutions that are applicable to a range of manufacturing environments, focusing on discrete and continuous manufacturing processes.

This project provides example solutions, composed of the following capabilities, for manufacturing environments:

- application allowlisting (AAL)
- behavior anomaly detection (BAD)

- file integrity
- user authentication and authorization
- remote access

#### 1.2.1 Relevant Standards and Guidance

The solutions presented in this guide are consistent with the practices and guidance provided by the following references:

- NIST Special Publication (SP) 800-167: Guide to Application Whitelisting [2]
- Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance [3]
- Executive Order no. 13636: *Improving Critical Infrastructure Cybersecurity* [4]
- NIST, Framework for Improving Critical Infrastructure Cybersecurity [5]
- NIST Interagency Report (NISTIR) 8219: Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection [6]
- NIST Internal Report (NISTIR) 8183: Cybersecurity Framework Manufacturing Profile [7]
- NISTIR 8089: An Industrial Control System Cybersecurity Performance Testbed [8]
- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Federal Information Systems and Organizations [9]
- NIST SP 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [10]
- NIST Special Publication 1800-25: *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* [11]
- NIST Interagency or Internal Report 7298 Rev 3: Glossary of Key Information Security Terms [12]
- U.S.-Canada Power System Outage Task Force [13]
- NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security [14]

#### **1.3 Benefits**

This NCCoE practice guide can help organizations:

- mitigate cybersecurity risk
- reduce downtime for operations
- provide a reliable environment that can detect cyber anomalies
- respond to security alerts through automated cybersecurity-event products

- develop and execute an OT cybersecurity strategy for which continuous OT cybersecurity monitoring is a foundational building block
- implement current cybersecurity standards and best practices

## 2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a modular design and provides users with the information they need to replicate the described manufacturing ICS security solutions, specifically focusing on information and system integrity. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-10A: *Executive Summary*
- NIST SP 1800-10B: Approach, Architecture, and Security Characteristics what we built and why (this document)
- NIST SP 1800-10C: How-To Guide instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Senior information technology (IT) executives, including chief information security and technology officers, will be interested in the *Executive Summary*, NIST SP 1800-10A, which describes the following topics:

- challenges that enterprises face in ICS environments in the manufacturing sector
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** might share the *Executive Summary*, NIST SP 1800-10A, with your leadership to help them understand the importance of adopting a standards-based solution. Doing so can strengthen their information and system integrity practices by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-10B (this document), which describes what we did and why. The following section will be of particular interest:

 Section <u>3.4.4</u>, which maps the security characteristics of the example solutions to cybersecurity standards and best practices

**IT and OT professionals** who want to implement an approach like this will find the whole practice guide useful, particularly the how-to portion, NIST SP 1800-10C, which provides step-by-step details to replicate all, or parts of the example solutions created in our lab. Volume C does not re-create the

product manufacturers' documentation, which is generally widely available. Rather, Volume C shows how we integrated the products together to create an example solution.

This guide assumes that IT and OT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the manufacturing ICS solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution. Every organization is unique in its priorities, risk tolerance, and the cyber ecosystem they operate in. This document presents a possible solution that may be tailored or augmented to meet an organization's own needs.

This document provides initial guidance. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>manufacturing\_nccoe@nist.gov</u>.

#### 2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names;	For language use and style guidance,
	references to documents that	see the NCCoE Style Guide.
	are not hyperlinks; new	
	terms; and placeholders	
Bold	names of menus, options,	Choose File > Edit.
	command buttons, and fields	
Monospace	command-line input,	mkdir
	onscreen computer output,	
	sample code examples, and	
	status codes	
Monospace Bold	command-line user input	service sshd start
	contrasted with computer	
	output	
<u>blue text</u>	link to other parts of the	All publications from NIST's NCCoE
	document, a web URL, or an	are available at_
	email address	https://www.nccoe.nist.gov.

# **3** Approach

This practice guide documents the approach the NCCoE used to develop example solutions, called builds, to support information and system integrity objectives. The approach includes a logical design, example build development, testing, security control mapping, and analysis.

Based on our discussions with cybersecurity practitioners in the manufacturing sector, the NCCoE pursued the Information and System Integrity in ICS Environments project to illustrate the broad set of capabilities available to manage and protect OT assets.

The NCCoE collaborated with the NIST Engineering Lab (EL), Community of Interest (COI) members, and the participating vendors to produce an example architecture and its corresponding implementations. Vendors provided technologies that met project requirements and assisted in installation and configuration of those technologies. This practice guide highlights the implementation of example architectures, including supporting elements such as functional tests, security characteristic analysis, and future build considerations.

### 3.1 Audience

This guide is intended for individuals or entities responsible for cybersecurity of ICS and for those interested in understanding information and system integrity capabilities for OT and how one approaches the implementation of an architecture. It may also be of interest to anyone in industry, academia, or government who seeks general knowledge of an OT information and system integrity solution for manufacturing-sector organizations.

## 3.2 Scope

This document focuses on information and system integrity in ICS environments typical of manufacturing organizations. It provides real-world guidance on implementing a solution for manufacturing ICS environments.

The scope of this project is to assist organizations in maintaining the integrity of information and systems by:

- Preventing execution or installation of unapproved software
- preventing unauthorized access to systems and information
- detecting anomalous behavior on the network that affects system or information integrity
- detecting hardware, software, or firmware modification

Organizational cybersecurity policies and procedures, as well as response and recovery functions, are out of scope for this document. The scenarios and security capabilities covered in this practice guide

should be part of a comprehensive OT/ICS security plan that addresses the NIST *Cybersecurity Framework* Protect and Detect functions.

The security capabilities used in this demonstration for protecting information and system integrity in ICS environments are briefly described below. These capabilities are implemented using commercially available third-party and open source solutions that provide the following capabilities:

- Application Allowlisting (AAL): A list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. [2]
- Behavioral Anomaly Detection (BAD): A mechanism providing a multifaceted approach to detecting cybersecurity attacks. [6]
- Hardware/Software/Firmware Modification Detection: A mechanism providing the ability to detect changes to hardware, software, and firmware on systems or network connected devices.
- **File Integrity Checking**: A mechanism providing the ability to detect changes to files on systems or network-connected devices.
- User Authentication and Authorization: A mechanism for verifying the identity and the access privileges granted to a user, process, or device. [12]
- Remote Access: A mechanism supporting access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet). [12]

#### 3.3 Assumptions

This project makes the following assumptions:

- Each solution is comprised of several readily available products. The modularity of the solutions might allow organizations to consider swapping one or more products, depending on their specific requirements.
- A cybersecurity stakeholder might implement all or part of a solution in a manner that is compatible with their existing environment.
- Organizations will test and evaluate the compatibility of the solutions with their ICS devices prior to production implementation and deployment. Response and recovery functions are beyond the scope of this guide.
- Events detected by the security tools are passed on to the security operation team for further action.

#### 3.4 Risk Assessment

<u>NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments</u>, states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of <u>NIST SP 800-37 Revision 2</u>, *Risk Management Framework for* <u>Information Systems and Organizations</u>, material that is available to the public. The <u>Risk Management</u> <u>Framework (RMF)</u> guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

#### 3.4.1 Threats

A threat is "any circumstance or event with the potential to adversely impact organizational operations" [11]. Within an IT environment, threats are typically thought of in terms of threats to confidentiality, integrity, or availability.

The realization of a threat to confidentiality, integrity, and availability may have different impacts to the OT versus the IT environments. OT environments are sensitive to loss of safety, availability, and integrity, while traditional IT environments tend to direct more resources toward confidentiality. Organizations that combine IT and OT operations are advised to evaluate the threats from both perspectives.

In a cyber-physical system, cybersecurity stakeholders are advised to consider events that occur in the OT environment may have impact to physical assets and events that occur in the physical world may impact the OT environment. For example, in 2021 a ransomware attack against an American oil pipeline system led to a disruption of operations and ultimately resulted in fuel shortages at airports and filling stations on the United States east coast. At the time of this writing, a full assessment has not been completed, but the economic impact to the pipeline was substantial.

An integrity loss need not be malicious to cause a significant impact. For example, a race condition in a supervisory control and data acquisition (SCADA) program caused a loss of information integrity. This led to alarm and notification failures and ultimately caused the Northeast Blackout of 2003. In excess of 55 million people were affected by this blackout and more than 100 people died. [13] Similarly, a sensor or metrology malfunction can lead to corrupted values in databases, logs, or other repositories.

Examples of integrity loss that may have an impact on the physical system include:

- Data corruption of alarm thresholds or control setpoints may lead to poor production quality in products or, in the extreme case, damage and destruction to physical manufacturing equipment.
- A loss of integrity of telemetry data may cause control algorithms to produce erroneous or even detrimental commands to manufacturing or control equipment.
- Corrupted routing tables or a denial-of-service attack on the communications infrastructure may cause the manufacturing processes to enter into a fail-safe state, thus inhibiting production. If the process is not designed to be fail-safe, an attack could result in equipment damage and lead to a greater disaster.
- Unauthorized remote access to the plant network could enable an attacker to stop production
  or operate the plant and equipment beyond its intended operating range. An attacker
  succeeding in disabling the safety instrument systems or changing its threshold parameters—
  operating the plant beyond its intended range—could lead to severe equipment damage.

#### 3.4.2 Vulnerabilities

A vulnerability as defined in <u>NISTIR 7298, Glossary of Key Information Security Terms</u> [12] is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

As indicated in <u>Section 1</u> of this document, when IT and OT environments are integrated, each domain inherits the vulnerabilities of the other. Increasing complexity of the interfaces typically results in the vulnerability of the overall system being much greater than the sum of the vulnerabilities of the subsystems.

NIST SP 800-82 categorizes ICS vulnerabilities into the following categories with examples [14]:

- Policy and Procedure: incomplete, inappropriate, or nonexistent security policy, including its documentation, implementation guides (e.g., procedures), and enforcement
- Architecture and Design: design flaws, development flaws, poor administration, and connections with other systems and networks
- Configuration and Maintenance: misconfiguration and poor maintenance
- Physical: lack of or improper access control, malfunctioning equipment
- Software Development: improper data validation, security capabilities not enabled, inadequate authentication privileges
- Communication and Network: nonexistent authentication, insecure protocols, improper firewall configuration

The first step in understanding the vulnerabilities and securing an organization's ICS infrastructure is knowledge of deployed assets and their interfaces. The knowledge of an asset's location and baselining

its behavior enable detection of anomalous behavior, via network monitoring, that may be the result of a successfully exploited vulnerability. The ability to reliably detect changes in asset behavior and knowing an asset's attributes are key in responding to potential cybersecurity incidents.

#### 3.4.3 Risk

The risk to an organization is the intersection of:

- the vulnerabilities and threats to the organization
- the likelihood that the vulnerability and threat event will be realized
- the impact to the organization should the event be realized

A meaningful risk assessment must be performed in the context of the cyber-ecosystem and the impact to an organization should a loss or degradation occur. The usefulness of the risk assessment is limited by how well the organization identifies and prioritizes the criticality of its assets, identifies the threats, and estimates the likelihood of the threats being realized.

Though risk analysis is a mature discipline, careful deliberations and analyses are necessary to determine the effect integrating IT and OT assets has on the threats, vulnerabilities, and impact to the organization. Once a baseline risk assessment has been completed, information assurance controls, such as the integrity protection measures investigated in this project, can be evaluated on how well they reduce the likelihood of the threat and subsequent reduction of risk. Cybersecurity stakeholders are strongly encouraged to leverage the NIST *Cybersecurity Framework* and manufacturing overlays to identify the components, elements, or items for which a risk assessment must be conducted. In addition, <u>NIST SP</u> <u>800-82</u> [14] mentions special considerations for performing an ICS risk assessment.

#### 3.4.4 Security Control Map

Implementation of cybersecurity architectures is most effective when executed in the context of an overall cybersecurity framework. Frameworks include a holistic set of activities or functions (i.e., what needs to be done) and a selection of controls (i.e., how these are done) that are appropriate for a given cyber-ecosystem. For this project, the NIST *Cybersecurity Framework* provided the overarching framework.

The subset of NIST *Cybersecurity Framework* Functions, Categories, and Subcategories that are supported by this example solution are listed below in Table 3-1, along with the subset of mappings to <u>NIST SP 800-53 Rev. 5</u> and to the <u>National Initiative for Cybersecurity Education (NICE) Workforce</u> <u>Framework. NIST SP 800-53 Rev 5: Security and Privacy Controls for Information Systems and</u> <u>Organizations</u> provides a list of controls for protecting operations, assets, and individuals. The controls detail requirements necessary to meet organizational needs. The <u>NICE Cybersecurity Workforce</u> <u>Framework</u> identifies knowledge, skills, and abilities needed to perform cybersecurity tasks. It is a reference guide on how to recruit and retain talent for various cybersecurity roles. For more information on the security controls, the *NIST SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations* is available at <u>https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final</u>.

For more information about NICE and resources that are available to employers, education and training providers, students, and job seekers, the *NIST SP-181 Rev. 1, NICE Cybersecurity Workforce Framework*, and other NICE resources are available at <a href="https://nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center">https://nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center</a>.

#### Table 3-1 Security Control Map

Func- tion	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
PRO- TECT (PR)	Identity Management, Authentication, and Ac- cess Control (PR.AC): Ac- cess to physical and logi- cal assets and associated facilities is limited to au- thorized users, processes, and devices, and is man- aged consistent with the assessed risk of unau- thorized access to author- ized activities and trans- actions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, us- ers, and processes	IA-2, IA-4, IA-5, IA-7, IA-9, IA-10, IA-12	SP-DEV-001, OM-ADM-001, OV-PMA-003
		PR.AC-3: Remote access is managed	AC-17, AC-19	SP-SYS-001, OM-ADM-001, PR-INF-001
		PR.AC-4: Access permissions and authorizations are man- aged, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-14, AC-24	OM-STS-001, OM-ADM-001
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and pri- vacy risks and other organizational risks)	AC-14, IA-2, IA-4, IA-5	OM-STS-001, OM-ADM-001
	Data Security (PR.DS): In- formation and records	PR.DS-1: Data-at-rest is protected	MP-7, SC-28	SP-DEV-002, SP-SYS-002, OM-DTA-001

Func- tion	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
	(data) are managed con- sistent with the organiza- tion's risk strategy to pro- tect the confidentiality, integrity, and availability of information.	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	OM-DTA-001
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibili- ties, management com- mitment, and coordina- tion among organiza- tional entities), pro- cesses, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-4: Backups of information are conducted, main- tained, and tested	CP-9	SP-SYS-001, SP-SYS-002, OM-DTA-001
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system com- ponents is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	MA-3	SP-SYS-001, OM-ANA-001
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	MA-4	SP-SYS-001, OM-ANA-001
DE- TECT (DE)	Anomalies and Events (DE.AE): Anomalous activ- ity is detected in a timely manner and the potential impact of events is under- stood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	CM-2, SI-4	SP-ARC-001, PR-CDA-001
		DE.AE-2: Detected events are analyzed to understand at- tack targets and methods	CA-7, SI-4 RA-5	OM-DTA-002, PR-CDA-001, CO-OPS-001
		DE.AE-3: Event data are collected and correlated from mul- tiple sources and sensors	CA-7, SI-4	OM-DTA-002, PR-CDA-001,

Func- tion	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
				PR-CIR-001, CO-OPS-001
	Security Continuous Mon- itoring (DE.CM): The in- formation system and as- sets are monitored at dis- crete intervals to identify cybersecurity events and verify the effectiveness of	DE.CM-1: The network is monitored to detect potential cy- bersecurity events	AU-12, CA-7, CM-3, SC-7, SI-4	OM-NET-001, PR-CDA-001, PR-CIR-001
		DE.CM-3: Personnel activity is monitored to detect poten- tial cybersecurity events	AU-12, CA-7, CM-11	PR-CDA-001, AN-TWA-001
	protective measures.	DE.CM-7: Monitoring for unauthorized personnel, connec- tions, devices, and software is performed	AU-12, CA-7, CM-3, SI-4	PR-CDA-001, PR-CIR-001, AN-TWA-001, CO-OPS-001

## 3.5 Technologies

Table 3-2 lists the capabilities demonstrated in this project, the products, and their functions, along with a mapping of the capabilities to the NIST *Cybersecurity Framework*. Refer to Table 3-1 for an explanation of the NIST *Cybersecurity Framework* subcategory codes.

Table 3-2 Products and Technologies

Capability	Product	Function	NIST Cybersecurity Framework Subcatego- ries Mapping
AAL	VMWare Carbon Black		

Capability	Product	Function	NIST Cybersecurity Framework Subcatego- ries Mapping	
	Windows Software Re- striction Policies (SRP) (Note: This component was not provided by collabora- tor. It is a feature of the Windows operating system product.)	Allow approved ICS applications to execute.	DE.AE-2, DE.AE-3, DE.CM-3, DE.CM-7	
	GreenTec WORMdisk and ForceField	Provides immutable storage for data, sys- tem, and configuration files.	PR.DS-1, PR.IP-4, PR.MA-1	
File Integrity	VMWare Carbon Black		PR.DS-6, PR.MA-1, DE.AE-2, DE.CM-3	
Checking	Wazuh Security Onion (Note: This component was not provided by collabora- tor. It is an open source product.)	Provides integrity checks for files and soft- ware.		
	Microsoft Azure Defender for IoT	Passively scans the OT	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7	
	Dragos Platform	network to create a baseline of devices and		
BAD Hardware/	Forescout eyeInspect (for- merly SilentDefense)	Alerts when activity de-		
Software/ Firm- ware Modifica-	Tenable Tenable.ot	line.		
tion Detection	PI System	Collects, analyzes, and visualizes time-series data from multiple sources. Alerts when activity de- viates from the base- line.	PR.IP-4, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3	

Capability	Product	Function	NIST Cybersecurity Framework Subcatego- ries Mapping
User Authentica- tion and User Authoriza- tion	TDi ConsoleWorks	Provides a central loca- tion for managing pass- word changes. Provides a security pe- rimeter for all devices within the OT environ- ment.	PR.AC-1, PR.AC-3, PR.AC-4, PR.MA-1, PR.MA-2, DE.AE-2, DE.AE-3, DE.CM-3, DE.CM-7
	Dispel		
Remote Access	Dispel		PR.AC-3, PR.MA-2, DE.AE-2, DE.CM-7
	Cisco AnyConnect (Note: This component was not provided by collabora- tor. It was a component of the existing lab infrastruc- ture.)	Records and logs user activity for each ses- sion.	

## **4** Architecture

These mechanisms and technologies were integrated into the existing NIST CSMS lab environment [8]. This cybersecurity performance testbed for ICS is comprised of the Process Control System (PCS) and the Collaborative Robotic System (CRS) ICS environments along with additional networking capabilities to emulate common manufacturing environments.

Typically, manufacturing organizations have unique cyber-ecosystems and specific needs for their operation. To demonstrate the modularity and interoperability of the provided solutions, this project used available CRADA partner technologies to assemble four "builds" deployed across both the PCS and CRS. Additionally, to increase the diversity of technologies between builds, two of the builds also utilized open source solutions (Security Onion Wazuh), native operating system features (Windows SRP), and a Cisco Adaptive Security Appliance (ASA) device configured with the AnyConnect virtual private network (VPN) client.

This modular approach, focusing on specific products and outcomes, demonstrates how solutions might be tailored to the operating environment. Table 4-1 provides a summary of the four builds and how the products were distributed across them. Detailed descriptions of the installation, configuration, and integration of these builds are included in Volume C of this guide.

Capability	Build 1	Build 2	Build 3	Build 4
	PCS		CRS	
AAL	Carbon Black	Windows SRP	Windows SRP	Carbon Black
BAD,	PI Server	PI Server	PI Server	PI Server
Hardware/Software/Firmware Modification Detection	Tenable.ot	eyelnspect	Dragos	Azure De- fender for IoT
File Integrity Checking	Carbon Black	Wazuh	Wazuh	Carbon Black
	ForceField, WORMdisk	ForceField, WORMdisk	ForceField, WORMdisk	ForceField, WORMdisk
User Authentication and Au- thorization	ConsoleWorks	Dispel	ConsoleWorks	Dispel
Remote Access	AnyConnect	Dispel	AnyConnect	Dispel

Table 4-1 Summary of What Products Were Used in Each Build

Sections 4.1, 4.2, <u>4.3</u>, and <u>4.4</u>, present descriptions of the manufacturing processes and control systems of the testbed that are used for demonstrating the security capabilities required for protecting information and system integrity in ICS environments. Section 4.5 describes the network and security architectures that are used to implement the above security capabilities.
#### 4.1 Manufacturing Process and Control System Description

The CSMS demonstration environment emulates real-world manufacturing processes and their ICS by using software simulators and commercial off-the-shelf (COTS) hardware in a laboratory environment [8]. The CSMS environment was designed to measure the performance impact on ICS that is induced by cybersecurity technologies. For this effort, the CSMS and the integrated PCS and CRS are used to demonstrate the information and system integrity capabilities and are described in Sections <u>4.3</u> and <u>4.4</u>.

#### 4.2 Cybersecurity for Smart Manufacturing Systems Architecture

Figure 4-1 depicts a high-level architecture for the demonstration environment consisting of a testbed local area network (LAN), a demilitarized zone (DMZ), the PCS, and the CRS. The environment utilizes a combination of physical and virtual systems and maintains a local network time protocol server for time synchronization. Additionally, the environment utilizes virtualized Active Directory servers for domain services. The tools used to support information and system integrity are deployed and integrated in the DMZ, Testbed LAN, PCS, and CRS according to vendor recommendations and standard practices as described in the detailed sections for each build.

#### Figure 4-1: CSMS Network Architecture



#### 4.3 Process Control System

A continuous manufacturing process is a type of manufacturing process that produces or processes materials continuously and in which the materials are continuously moving, going through chemical reactions, or undergoing mechanical or thermal treatment. Continuous manufacturing usually implies a 24-hours a day, seven days a week (24/7) operation with infrequent maintenance shutdowns. Examples of continuous manufacturing systems are chemical production, oil refining, natural gas processing, and wastewater treatment.

The PCS emulates the Tennessee-Eastman (TE) chemical reaction process. The TE problem, presented by Downs and Vogel [15], is a well-known process-control problem in continuous chemical manufacturing. A control loop is required in the PCS to maintain a steady and stable chemical production. The PCS

presents a real-world scenario in which a cybersecurity attack could represent a real risk to human safety, environmental safety, and economic viability. This allows the PCS to be used to assess the impact of cybersecurity attacks on the continuous process manufacturing environment.

The PCS includes a software simulator to emulate the TE chemical reaction process. The simulator is written in C code and is executed on a workstation-class computer. In addition, the system includes a series of COTS hardware, including an Allen-Bradley ControlLogix 5571 PLC, a software controller implemented in MATLAB for process control, a Rockwell FactoryTalk Human Machine Interface (HMI), an object linking and embedding for process control (OPC) data access (DA) server, a data historian, an engineering workstation, and several virtual LAN (VLAN) switches and network routers. Figure 4-2 and Figure 4-3 outline the process flow of the TE manufacturing process. The simulated TE process includes five major units with multiple input feeds, products, and byproducts that has 41 measured variables (sensors) and 12 manipulated variables (actuators). The PCS consists of a software simulated chemical manufacturing process (TE process), integrated with a series of COTS hardware, including PLCs, industrial network switches, protocol converters, and hardware modules to connect the simulated process and the control loop.

#### Figure 4-2 Simplified Tennessee Eastman Process Model





#### Figure 4-3 HMI Screenshot for the PCS Showing the Main Components in the Process

The PCS network architecture is shown in Figure 4-4. The PCS network is connected to the Testbed LAN via a boundary router. The boundary router is an Allen-Bradley Stratix 8300. All network traffic is going through the boundary router to access the Testbed LAN and the DMZ. The PCS environment is segmented into three local networks, namely the engineering LAN, Operations LAN (VLAN1), and the Supervisory LAN (VLAN2). Each of these local networks is connected using an industrial network switch, an Allen-Bradley Stratix 5700. The engineering workstation is hosted in the engineering LAN. The HMI and the Plant Controller are hosted in the operations LAN. The Plant Simulator is hosted in the supervisory LAN along with the Local Historian, OPC Server, and the Supervisory PLC.

The Operations LAN (VLAN1) simulates a central control room environment. The supervisory LAN (VLAN2) simulates the process operation/ manufacturing environment, which typically consists of the operating plant, PLCs, OPC server, and data historian.

An OPC DA server is the main data gateway for the PLC and the simulated controller. The PLC reads in the manufacturing process sensor data from the Plant Simulator using the DeviceNet connection and communicates the data to the OPC DA server. The PLC also retrieves actuator information from the controller through the OPC DA and transmits to the Plant Simulator. The controller uses a MATLAB Simulink interface to communicate with the OPC DA server directly.

#### **Figure 4-4 PCS Network**



### 4.4 Collaborative Robotics System (CRS)

The CRS workcell, shown in Figure 4-5, contains two robotic arms that perform a material handling process called machine tending [8]. Robotic machine tending utilizes robots to interact with machinery, performing physical operations a human operator would normally perform (e.g., loading and unloading of parts in a machine, opening and closing machine doors, activating operator control panel buttons, etc.).

Parts are transported by two Universal Robots UR3e robotic arms through four simulated machining stations. Each station communicates with the Supervisory PLC (a Beckhoff CX9020) over the workcell network, which monitors and controls all aspects of the manufacturing process. An HMI (Red Lion G310) allows the workcell operator to monitor and control process parameters.

#### Figure 4-5 The CRS Workcell



The CRS network, shown in Figure 4-6, is hierarchically architected, separating the supervisory devices from the low-level OT that control the manufacturing process. The top-level router is a Siemens RUGGEDCOM RX1510, which provides firewall capabilities, logical access to the Testbed LAN network, network address translation (NAT), and other cybersecurity capabilities. The router is connected to the Testbed LAN (identified in Figure 4-1 as the Testbed LAN) using NAT. Layer 2 network traffic for the Supervisory LAN is handled by a Netgear GS724T-managed Ethernet switch, and network traffic for the Control LAN is handled by a Siemens i800-managed Ethernet switch.

#### **Figure 4-6 CRS Network**



#### 4.5 Logical Network and Security Architectures

The following sections provide a high-level overview of the technology integration into the ICS environments for each solution, also referred to as a build. Additional details related to the installation and configuration of these tools are provided in Volume C of this guide.

#### 4.5.1 Build 1

For Build 1, the technologies in Table 4-2 were integrated into the PCS environment, Testbed LAN, and DMZ segments of the testbed environment to enhance system and information integrity capabilities.

Table 4-2 Build 1 Technology Stack to Capabilities Map

Capability	Products	Description
AAL	Carbon Black	Carbon Black Server is deployed within the Testbed LAN with the Carbon Black Agents installed on key workstations and servers in the Testbed LAN, PCS en- vironment, and DMZ to control applica- tion execution.
BAD, Hardware/Software/Firmware Modification Detection	PI Server	Deployed in the DMZ and PCS environ- ments, the PI Server provides the histo- rian repository for process data through its Data Archive and generates Event Frames upon detection of abnormal manufacturing system behavior.
	Tenable.ot	Passively monitors the PCS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports, and is also configured to capture detailed asset information for supporting inventory, change via both passive and active scan- ning.
File Integrity Checking	Carbon Black	Deployed within the Testbed LAN envi- ronment with the Carbon Black Agents installed on key workstations and serv- ers to monitor the integrity of local files.
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ environment and configured with both a ForceField and WORM drive to provide a protected archive for the his- torian data and the approved versions of configuration, source (PLC Programs), and executable files for the ICS environ- ment.

Capability	Products	Description
User Authentication and Author- ization	ConsoleWorks	Deployed to centralize the access and management of the systems and cre- dentials. ConsoleWorks is deployed to the Testbed LAN to allow connections to the PCS environment.
Remote Access	AnyConnect	Supports authenticated VPN connec- tions to the environment with limited access to only the TDI ConsoleWorks web interface.

The technology was integrated into the lab environment as shown in Figure 4-7.



#### Figure 4-7 Build 1, PCS Complete Architecture with Security Components

#### 4.5.2 Build 2

For Build 2, the technologies in Table 4-3 were integrated into the PCS, Testbed LAN, and DMZ segments of the testbed environment to enhance system and information integrity capabilities.

Table 4-3 Build 2 Technology Stack to Capabilities Map

Capability	Product	Description
AAL	Windows SRP	AD Group Policy Objects (GPOs) are used to con- figure and administer the Windows Software Re- striction Policy (SRP) capabilities within the Testbed LAN environment and PCS environ- ments. For non-domain systems (e.g., Dispel VDI and DMZ systems), the GPO was applied as local settings on the systems.
BAD, Hardware/Software/Firm- ware Modification Detection	PI Server	Deployed in the DMZ and PCS environments, the PI Server provides the historian repository for process data through its Data Archive and gener- ates Event Frames upon detection of abnormal manufacturing system behavior.
	eyeInspect ICSPatrol	Passively monitors the PCS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports, and is also configured to capture detailed asset information for supporting inven- tory and change management capabilities using the ICSPatrol server, which can perform scans on ICS components.
File Integrity Checking	Wazuh	The Security Onion server is used to manage and monitor the integrity of local files using the Wazuh agents deployed on the Dispel VDI, DMZ, Testbed LAN, and PCS.
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ envi- ronment and configured with both a ForceField and WORM drive to provide a protected archive for the historian data and the approved versions of configuration, source, and executable files for the ICS environment.

Capability	Product	Description
User Authentication and Au- thorization	Dispel	The Dispel Wicket is deployed to the DMZ envi- ronment and integrated with the Dispel cloud-
Remote Access		based environment to provide a virtual desktop interface (VDI) with a secure remote connection to the testbed environment. Through this con- nection, authorized users are permitted to ac- cess resources in both the Testbed LAN and PCS environment.

The technology was integrated into the lab environment as shown in Figure 4-8.



#### Figure 4-8 Build 2, PCS Complete Architecture with Security Components

#### 4.5.3 Build 3

The technologies in Table 4-4 were integrated into the CRS for Build 3 to enhance system and data integrity capabilities.

Table 4-4 Build 3 Technology Stack to Capabilities Map

Capability	Products	Description
AAL	Windows SRP	AD Group Policy Objects (GPOs) are used to con- figure and administer the Windows Software Re- striction Policy (SRP) capabilities within the Testbed LAN environment and CRS environ- ments.
BAD, Hardware/Software/Firm- ware Modification Detection	PI Server	Deployed in the DMZ and CRS environments, the PI Server provides the historian repository for process data through its Data Archive and gener- ates Event Frames upon detection of abnormal manufacturing system behavior
	Dragos	Passively monitors the CRS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports and receives Event Frames from the DMZ PI system through the PI Web API inter- face.
File Integrity Checking	Wazuh	The Security Onion server is used to manage and monitor the integrity of local files using the Wazuh agents deployed on the DMZ, Testbed LAN, and CRS.
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ envi- ronment and configured with both a ForceField and WORM drive to provide a protected archive for the historian data and the approved versions of configuration and coding files for the ICS envi- ronment.
User Authentication and Author- ization	ConsoleWorks	Deployed to centralize the access and manage- ment of the systems and credentials. Console- Works is deployed to allow connections within the CRS environment.
Remote Access	AnyConnect	Supports authenticated VPN connections to the environment with limited access to only the TDI ConsoleWorks web interface.

The technology was integrated into the lab environment as shown in Figure 4-9.

Figure 4-9 Build 3, CRS Complete Architecture with Security Components



#### 4.5.4 Build 4

For Build 4, the technologies in Table 4-5 were integrated into the CRS, Testbed LAN, and DMZ segments of the testbed environment to enhance system and data integrity capabilities.

Table 4-5 Build 4 Technology Stack to Capabilities Map

Capability	Products	Description	
AAL	Carbon Black	Deployed within the Testbed LAN environment with the Carbon Black agents installed on key workstations and servers to control application ex- ecution.	
BAD, Hardware/Software/Firm- ware Modification Detection	Pl Server	Deployed in the DMZ and CRS environments, the PI Server provides the historian repository for pro- cess data through its Data Archive and generates Event Frames upon detection of abnormal manu- facturing system behavior.	
	Azure De- fender for IoT	Passively monitors the CRS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports and is also configured to capture detailed as- set information for supporting inventory and change management capabilities.	
File Integrity Checking	Carbon Black	Deployed within the Testbed LAN environment with the Carbon Black agents installed on key workstations and servers to monitor the integrity of local files.	
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ envi- ronment and configured with both a ForceField and WORM drive to provide a protected archive for the historian data and the approved versions of configuration and coding files for the ICS envi- ronment.	
User Authentication and Author- ization	Dispel	The Dispel Wicket is deployed to the DMZ environ- ment and integrated with the Dispel cloud-based	
Remote Access		environment to provide a VDI with a secure mote connection to the testbed environmer Through this connection, authorized users a mitted to access resources in both the Testb LAN and CRS environment.	environment to provide a VDI with a secure re- mote connection to the testbed environment. Through this connection, authorized users are per- mitted to access resources in both the Testbed LAN and CRS environment.

The technology was integrated into the lab environment as shown in Figure 4-10.

Figure 4-10 Build 4, CRS Complete Architecture with Security Components



### **5** Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective to demonstrate protecting information and system integrity in ICS environments. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

#### 5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure.

#### 5.2 Example Solution Testing

This section presents a summary of the solution testing and results. A total of eleven tests were developed for the builds. The following information is provided for each scenario:

- Objective: Purpose of the scenario and what it will demonstrate
- Description: Brief description of the scenario and the actions performed
- Relevant NIST Cybersecurity Framework Subcategories: Mapping of NIST Cybersecurity Framework subcategories relevant to the scenario
- Assumptions: Assumptions about the cyber-environment
- Security Capabilities and Products: Capabilities and products demonstrated during the scenario
- Test Procedures: Steps performed to execute the scenario
- Expected Results: Expected results from each capability and product demonstrated during the scenario, and for each build
- Actual Test Results: Confirm the expected results
- Overall Result: Were the security capabilities and products able to meet the objective when the scenario was executed (PASS/FAIL rating).

Additional information for each scenario such as screenshots captured during the execution of the test procedures and detailed results from the security capabilities are presented in <u>Appendix D</u>.

#### 5.2.1 Scenario 1: Protect Host from Malware Infection via USB

Objective	This test demonstrates blocking the introduction of malware through physical access to a workstation within the manufacturing environment.
Description	An authorized user transports executable files into the manufacturing system via a USB flash drive that contains malware.
Relevant NIST Cybersecurity Framework Subcategories	PR.DS-6, PR.MA-2, DE.AE-2
Assumptions	<ul> <li>User does not have administrative privileges on the target machine.</li> </ul>
	<ul> <li>User has physical access to the target machine.</li> </ul>
Security Capabilities and Products	Build 1: Carbon Black: AAL Build 2: Windows SRP: AAL Build 3: Windows SRP: AAL Build 4: Carbon Black: AAL
Test Procedures	1. Attempt to execute malware on the target machine.
Expected Results	<ul> <li>The AAL tool will detect and stop the malware upon execution.</li> </ul>
Actual Test Results	<ul> <li>The AAL technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> </ul>
Overall Result	PASS

#### 5.2.2 Scenario 2: Protect Host from Malware Infection via Network Vector

Objective	This test demonstrates the detection of malware introduced from
	the network.

Description	An attacker pivoting from the corporate network into the manufac- turing environment attempts to insert malware to establish persis- tence in the manufacturing environment.	
Relevant NIST Cybersecurity Framework Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7	
Assumptions	<ul> <li>The attacker has completed reconnaissance and initial access, gaining the ability to pivot into the manufacturing environment.</li> </ul>	
Security Capabilities and	Build 1:	
Products	<ul> <li>Carbon Black: AAL</li> </ul>	
	<ul> <li>Tenable.ot: BAD</li> </ul>	
	Build 2:	
	<ul> <li>Windows SRP: AAL</li> </ul>	
	<ul> <li>Forescout eyeInspect: BAD</li> </ul>	
	Build 3:	
	<ul> <li>Windows SRP: AAL</li> </ul>	
	Dragos: BAD	
	Build 4:	
	Carbon Black: AAL	
	<ul> <li>Azure Defender for IoT: BAD</li> </ul>	
Test Procedures	1. Attacker pivots into the manufacturing environment.	
	2. Attacker copies malware to the server in Testbed LAN.	
	<ol> <li>Attacker attempts to execute malware on server in Testbed LAN.</li> </ol>	
Expected Results	<ul> <li>The AAL capabilities installed on target systems will block execution of the malicious code.</li> </ul>	
	<ul> <li>The BAD tool will capture the suspicious traffic and generate an alert.</li> </ul>	

Actual Test Results	<ul> <li>The AAL technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> <li>The BAD tool is able to detect and alert on activity pivoting into manufacturing systems.</li> </ul>
Overall Result	PASS

#### 5.2.3 Scenario 3: Protect Host from Malware via Remote Access Connections

Objective	This test demonstrates blocking malware that is attempting to in- fect the manufacturing system through authorized remote access connections.
Description	A remote workstation authorized to use a remote access connec- tion has been infected with malware. When the workstation is con- nected to the manufacturing environment through the remote ac- cess connection, the malware attempts to pivot and spread to vul- nerable host(s).
Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-7, PR.MA-1, PR.MA-2, DE.CM-3, DE.CM-7
Assumptions	<ul> <li>Infection of the remote workstation occurs prior to remote access session.</li> </ul>

Security Canabilities and	
Products	
	<ul> <li>Cisco VPN: Remote Access</li> </ul>
	<ul> <li>ConsoleWorks: User Authentication and User Authorization</li> </ul>
	Build 2:
	<ul> <li>Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>
	Build 3:
	<ul> <li>Cisco VPN: Remote Access</li> </ul>
	<ul> <li>ConsoleWorks: User Authentication and User Authorization</li> </ul>
	Build 4:
	<ul> <li>Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>
Test Procedures	<ol> <li>Authorized remote user connects to the manufacturing environment.</li> </ol>
	<ol><li>Malware on remote host attempts to pivot into the manufacturing environment.</li></ol>
Expected Results	<ul> <li>Malware will be blocked from propagation by the remote access capabilities.</li> </ul>
Actual Test Results	<ul> <li>Remote access connection blocks malware attempts to pivot into the manufacturing environment.</li> </ul>
Overall Result	PASS

### 5.2.4 Scenario 4: Protect Host from Unauthorized Application Installation

Objective	This test demonstrates blocking installation and execution of unau- thorized applications on a workstation in the manufacturing sys- tem.
Description	An authorized user copies downloaded software installation files from a shared network drive accessible from the workstation in the manufacturing system. The user then attempts to install the unau- thorized software on the workstation.

Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	<ul> <li>User does not have administrative privileges on the target machine.</li> </ul>
	<ul> <li>Applications to be installed are unapproved applications.</li> </ul>
Security Capabilities and	Build 1:
Products	Carbon Black: AAL
	<ul> <li>Tenable.ot: BAD</li> </ul>
	Build 2:
	<ul> <li>Windows SRP: AAL</li> </ul>
	<ul> <li>eyeInspect: BAD</li> </ul>
	Build 3:
	<ul> <li>Windows SRP: AAL</li> </ul>
	<ul> <li>Dragos: BAD</li> </ul>
	Build 4:
	Carbon Black: AAL
	<ul> <li>Azure Defender for IoT: BAD</li> </ul>
Test Procedures	<ol> <li>The user copies software to a host in the manufacturing environment.</li> </ol>
	2. The user attempts to install the software on the host.
	<ol><li>The user attempts to execute software that does not require installation.</li></ol>
Expected Results	<ul> <li>The AAL tool will detect and stop the execution of the software installation or executable file.</li> </ul>
	<ul> <li>The BAD tool will capture the suspicious traffic and generate an alert.</li> </ul>
Actual Test Results	<ul> <li>The AAL technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> </ul>
	The BAD tool is able to detect and alert on activity in the manufacturing system.

### 5.2.5 Scenario 5: Protect from Unauthorized Addition of a Device

Objective	This test demonstrates detection of an unauthorized device con-
Description	An individual authorized to access the physical premises connects and uses an unauthorized device on the manufacturing network.
Relevant NIST <i>Cybersecurity</i> Framework Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	<ul> <li>Ports on switch are active and available.</li> </ul>
Security Capabilities and Products	Build 1: Tenable.ot: BAD Build 2: eyeInspect: BAD Build 3: Dragos: BAD Build 4: Azure Defender for IoT: BAD
Test Procedures	<ol> <li>The individual connects the unauthorized device to the manufacturing network.</li> <li>The individual uses an unauthorized device to access other devices on the manufacturing network.</li> </ol>
Expected Results	<ul> <li>The BAD detection tool will capture the suspicious traffic and generate an alert.</li> </ul>
Actual Test Results	<ul> <li>The BAD detection tool is able to detect and alert on activity in the manufacturing system.</li> </ul>
Overall Result	PASS

Objective	This test demonstrates detection of unauthorized communications between devices.
Description	A device authorized to be on the network attempts to establish an unapproved connection.
Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	<ul> <li>The environment has a predictable communications pattern.</li> </ul>
Security Capabilities and	Build 1:
Products	<ul> <li>Tenable.ot: BAD.</li> </ul>
	Build 2:
	<ul> <li>eyeInspect: BAD.</li> </ul>
	Build 3:
	<ul> <li>Dragos: BAD</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: BAD</li> </ul>
Test Procedures	<ol> <li>The device attempts to establish an unapproved connection.</li> </ol>
Expected Results	<ul> <li>The BAD tool will capture the suspicious traffic and generate an alert.</li> </ul>
Actual Test Results	<ul> <li>The BAD tool is able to detect and alert on activity in manufacturing systems.</li> </ul>
Overall Result	PASS

#### 5.2.6 Scenario 6: Detect Unauthorized Device-to-Device Communications

### 5.2.7 Scenario 7: Protect from Unauthorized Deletion of Files

Objective	This test demonstrates protection of files from unauthorized dele-
	tion both locally and on network file share.

Description	An authorized user attempts to delete files on an engineering work- station and a shared network drive within the manufacturing sys- tem.
Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.DS-1, PR.DS-6, PR.IP-4, PR.MA-1, DE.AE-2
Assumptions	<ul> <li>User does not have administrative privileges on the target machine.</li> </ul>
Security Capabilities and	Build 1:
Products	<ul> <li>Carbon Black: File Integrity Checking.</li> </ul>
	<ul> <li>WORMdisk: File Integrity Protection.</li> </ul>
	Build 2:
	<ul> <li>Security Onion: File Integrity Checking.</li> </ul>
	<ul> <li>WORMdisk: File Integrity Protection.</li> </ul>
	Build 3:
	<ul> <li>Security Onion: File Integrity Checking.</li> </ul>
	<ul> <li>WORMdisk: File Integrity Protection.</li> </ul>
	Build 4:
	<ul> <li>Carbon Black: File Integrity Checking.</li> </ul>
	<ul> <li>WORMdisk: File Integrity Protection.</li> </ul>
Test Procedures	1. User attempts to delete files located on a workstation in the manufacturing system.
	2. User attempts to delete files from the network file share containing the golden images for the manufacturing system.
Expected Results	<ul> <li>Deletion of files on the workstation will be detected and alerted on by the file integrity checking tool.</li> </ul>
	<ul> <li>Deletion of files on the network file share will be prevented by the file integrity checking tool.</li> </ul>
Actual Test Results	<ul> <li>Host-based file integrity checking is able to detect and alert on deletion of files.</li> </ul>

	<ul> <li>Protected network file share is able to prevent deletion of files on the network file share.</li> </ul>
Overall Result	PASS

### 5.2.8 Scenario 8: Detect Unauthorized Modification of PLC Logic

Objective	This test demonstrates detection of PLC logic modification.
Description	An authorized user performs an unapproved or unauthorized modi- fication of the PLC logic from an engineering workstation.
Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.AC-3,PR.AC-7, PR.DS-6, PR.MA-1, PR.MA-2, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	None
Security Capabilities and	Build 1:
Products	<ul> <li>Tenable.ot: BAD and Software Modification</li> </ul>
	Cisco VPN: Remote Access
	<ul> <li>ConsoleWorks: User Authentication, User Authorization, and Remote Access</li> </ul>
	Build 2:
	<ul> <li>eyeInspect: BAD and Software Modification</li> </ul>
	<ul> <li>Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>
	Build 3:
	<ul> <li>Dragos: BADand Software Modification</li> </ul>
	Cisco VPN: Remote Access
	<ul> <li>ConsoleWorks: User Authentication, User Authorization, and Remote Access</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: BAD and Software Modification</li> </ul>
	<ul> <li>Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>

Test Procedures	<ol> <li>The authorized user remotely connects to a manufacturing environment.</li> <li>The user modifies and downloads a logic file to the PLC.</li> </ol>
Expected Results	<ul> <li>The BAD tool will capture the suspicious traffic and generate an alert.</li> </ul>
	<ul> <li>The user authentication/authorization/remote access is able to remotely access the engineering systems as intended.</li> </ul>
Actual Test Results	<ul> <li>The BAD is able to detect and alert on activity accessing the PLC.</li> </ul>
Overall Result	PASS

### 5.2.9 Scenario 9: Protect from Modification of Historian Data

Objective	This test demonstrates blocking of modification of historian archive data.
Description	An attacker coming from the corporate network pivots into the manufacturing environment and attempts to modify historian ar- chive data.
Relevant NIST <i>Cybersecu-</i> <i>rity Framework</i> Subcatego- ries	PR.DS-6, PR.MA-1, DE.AE-2
Assumptions	<ul> <li>The attacker has completed reconnaissance and initial access, gaining the ability to pivot into the manufacturing environment.</li> </ul>
Security Capabilities and	Build 1:
Products	<ul> <li>Tenable.ot: BAD</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>
	Build 2:
	<ul> <li>eyeInspect: BAD</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>

	Build 3:
	<ul> <li>Dragos: BAD</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: BAD</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>
Test Procedures	<ol> <li>Attacker pivots into the manufacturing environment from the corporate network.</li> </ol>
	2. Attacker attempts to delete historian archive data file.
	3. Attacker attempts to replace historian archive data file.
Expected Results	<ul> <li>The file operations will be blocked by the file integrity checking tool.</li> </ul>
Actual Test Results	<ul> <li>File integrity checking tool is able to prevent file operations on the protected files.</li> </ul>
Overall Result	PASS

### 5.2.9.1 Scenario 10: Detect Sensor Data Manipulation

Objective	This test demonstrates detection of atypical data reported to the historian.
Description	A sensor in the manufacturing system begins sending atypical data values to the historian.
Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.IP-4, PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	<ul> <li>Devices in the manufacturing system (HMI and PLCs) are not validating sensor data.</li> </ul>
Security Capabilities and Products	<ul> <li>PI Server: BAD</li> </ul>
Test Procedures	1. A sensor sends invalid data to the historian.

Expected Results	<ul> <li>The BAD capability will detect atypical sensor data and generate alerts.</li> </ul>
Actual Test Results	<ul> <li>The BAD tool is able to detect atypical data and create an event frame.</li> </ul>
Overall Result	PASS

#### 5.2.9.2 Scenario 11: Detect Unauthorized Firmware Modification

Objective	This test demonstrates detection of device firmware modification.
Description	An authorized user performs a change of the firmware on a PLC.
Relevant NIST <i>Cybersecu- rity Framework</i> Subcatego- ries	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	None

Security Capabilities and Products	Build 1:
	<ul> <li>Cisco VPN: Remote Access.</li> </ul>
	<ul> <li>ConsoleWorks: Remote Access, User Authentication, and User Authorization.</li> </ul>
	<ul> <li>Tenable.ot: BAD and Firmware Modification.</li> </ul>
	Build 2:
	<ul> <li>Dispel: Remote Access, User Authentication, and User Authorization.</li> </ul>
	<ul> <li>eyeInspect and ICSPatrol: BAD and Firmware Modification.</li> </ul>
	Build 3:
	<ul> <li>Cisco VPN: Remote Access.</li> </ul>
	<ul> <li>ConsoleWorks: Remote Access, User Authentication, and User Authorization.</li> </ul>
	<ul> <li>Dragos: BAD and Firmware Modification.</li> </ul>
	Build 4:
	<ul> <li>Dispel: Remote Access, User Authentication, and User Authorization.</li> </ul>
	<ul> <li>Azure Defender for IoT: BAD and Firmware Modification.</li> </ul>
Test Procedures	<ol> <li>Authorized remote user connects to manufacturing environment.</li> </ol>
	2. The user changes firmware on the PLC component.
Expected Results	<ul> <li>The behavioral anomaly detection tool will identify the change to the PLC and generate an alert for review.</li> </ul>
Actual Test Results	<ul> <li>The BAD is able to detect and generate alerts for updates to PLC component firmware.</li> </ul>
Overall Result	PASS

#### 5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The NIST *Cybersecurity Framework* Subcategories were used to provide structure to the security assessment by consulting the specific

sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the NIST *Cybersecurity Framework* Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the necessary security characteristics.

### 5.3.1 PR.AC-1: Identities and Credentials are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes

This NIST *Cybersecurity Framework* Subcategory is supported through user authentication and user authorization capabilities in addition to the native credential management capabilities associated with the tools. In each of the systems, user accounts were issued, managed, verified, revoked, and audited.

#### 5.3.2 PR.AC-3: Remote Access is Managed

This NIST *Cybersecurity Framework* Subcategory is supported by remote access tools integrated with the user authentication and authorization systems. Together, these tools provide a secure channel for an authorized user to access the manufacturing environment from a remote location. These tools are configurable to allow organizations to control who can remotely access the system, what the user can access, and when access is allowed by a user.

## 5.3.3 PR.AC-4: Access Permissions and Authorizations are Managed, Incorporating the Principles of Least Privilege and Separation of Duties

This NIST *Cybersecurity Framework* Subcategory is supported by the user authentication and user authorization capabilities. These tools are used to grant access rights to each user and notify if suspicious activity is detected. This includes granting access to maintenance personnel responsible for certain sub-systems or components of ICS environments while preventing them from accessing other sub-systems or components. Suspicious activities include operations attempted by an unauthorized user, restricted operations performed by an authenticated user who is not authorized to perform those operations, and operations that are performed outside of the designated time frame.

# 5.3.4 PR.AC-7: Users, Devices, and Other Assets are Authenticated (e.g., single-factor, multi-factor) Commensurate with the Risk of the Transaction (e.g., Individual Security and Privacy Risks and Other Organizational Risks)

This NIST *Cybersecurity Framework* Subcategory is supported through user authentication and user authorization capabilities in addition to the native credential management capabilities associated with the tools. Based on the lab's risk assessment, the authentication and authorization systems used user passwords as one factor to verify identity and grant access to the environment. To bolster security in the environment, IP addresses were used as a secondary factor for remote access.

#### 5.3.5 PR.DS-1: Data-at-Rest is Protected

This NIST *Cybersecurity Framework* Subcategory is supported using file integrity checking. For end points, the file integrity tools alert when changes to local files are detected. For historian backups and system program and configuration backups, data was stored on read only or write-once drives to prevent data manipulation.

## 5.3.6 PR.DS-6: Integrity Checking Mechanisms are Used to Verify Software, Firmware, and Information Integrity

This NIST *Cybersecurity Framework* Subcategory is supported through file integrity checking tools and the BAD tools. The file integrity checking tools monitor the information on the manufacturing end points for changes. The BAD tools monitor the environments for changes made to software, firmware, and validate sensor and actuator information.

#### 5.3.7 PR.IP-4: Backups of Information are Conducted, Maintained, and Tested

This NIST *Cybersecurity Framework* Subcategory is supported by file integrity checking using secure storage to protect backup data. System configuration settings, PLC logic files, and historian databases all have backups stored on secure storage disks. The secure storage is constructed in a way that prohibits modifying or deleting data that is on the disk.

## 5.3.8 PR.MA-1: Maintenance and Repair of Organizational Assets are Performed and Logged, with Approved and Controlled Tools

This NIST *Cybersecurity Framework* Subcategory is supported by a combination of tools including AAL, the user authentication and user authorization tools, and the behavior anomaly detection tools. User authentication and user authorization tools provide a controlled environment for authorized users to interact with the manufacturing environment. Behavior anomaly detection tools provide a means to detect maintenance activities in the environment such as PLC logic modification or PLC firmware updates via the network. This information can be combined with data from a computerized maintenance management system to ensure that all maintenance activities are appropriately approved and logged. Also, AAL prevents unapproved software from running on systems to ensure that only approved tools are used for maintenance activities.

## 5.3.9 PR.MA-2: Remote Maintenance of Organizational Assets is Approved, Logged, and Performed in a Manner that Prevents Unauthorized Access

This NIST *Cybersecurity Framework* Subcategory is supported by the remote access capability integrated with the user authentication and user authorization system. The tools in the solution were used to grant access for performing remote maintenance on specific assets. The tools prevent unauthorized users from gaining access to the manufacturing environment.

## 5.3.10 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and Systems is Established and Managed

This NIST *Cybersecurity Framework* Subcategory is supported by behavior anomaly detection tools. Network baselines were established and approved based on an understanding of normal operations and data flows identified by the behavior anomaly detection tools.

## 5.3.11 DE.AE-2: Detected Events are Analyzed to Understand Attack Targets And Methods

This NIST *Cybersecurity Framework* Subcategory is supported by all the capabilities included in the solutions. Logs of suspicious activities from the tools can be used by security managers and engineers to understand what unusual activity has occurred in the manufacturing system. Analyzing these logs provides a mechanism to determine what systems were accessed and what actions may have been performed on them. Although not demonstrated in these solutions, an analytic engine would enhance the detection capability of the solution.

## 5.3.12 DE.AE-3: Event Data are Collected and Correlated from Multiple Sources and Sensors

This NIST *Cybersecurity Framework* Subcategory is supported by all the capabilities included in the solutions. Each tool detects different aspects of the scenarios from diverse perspectives. Although not demonstrated in these solutions, a data aggregation and correlation tool such as a security information and event management tool would enhance the detection capability of the solution.

## 5.3.13 DE.CM-1: The Network is Monitored to Detect Potential Cybersecurity Events

This NIST *Cybersecurity Framework* Subcategory is supported by the BAD and remote access capabilities used in the example solutions to monitor the manufacturing network to detect potential cybersecurity events. The BAD tools monitor network communications at the external boundary of the system and at key internal points within the network, along with user activities and traffic patterns, and compare it to the established baseline. The remote access capabilities monitor the network communications at the external boundary of the system. This helps detect unauthorized local, network, and remote connections and identify unauthorized use of the manufacturing system.

## 5.3.14 DE.CM-3: Personnel Activity is Monitored to Detect Potential Cybersecurity Events

This NIST *Cybersecurity Framework* Subcategory is supported by the authentication and authorization tools that allow for monitoring personnel activity while connected through these tools. Further, AAL and

file integrity checking tools provide the ability to monitor user actions on hosts. Additionally, BAD tools monitor and record events associated with personnel actions traversing network traffic. Each tool provides a different perspective in monitoring personnel activity within the environment. The resulting alerts and logs from these tools can be monitored individually or collectively to support investigations for potential malicious or unauthorized activity within the environment.

## 5.3.15 DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software is Performed

This NIST *Cybersecurity Framework* Subcategory is supported by BAD, AAL, user authentication and user authorization, and remote access capabilities of the solutions. The BAD tools established an information baseline for approved assets and connections. Then the manufacturing network is monitored using the BAD capability for any deviation by the assets and connections from the established baseline. If any deviation is detected, an alert is generated. Additionally, the AAL tool blocks any unauthorized application installation or execution and generates an alert on these events. User authentication and user authorization tools monitor for unauthorized personnel connecting to the environment. Remote access capabilities monitor for unauthorized connections to the environment.

### 6 Future Build Considerations

This guide has presented technical solutions for maintaining and monitoring system and information integrity, which will help detect and prevent incidents in a manufacturing environment. Future builds should demonstrate methods and techniques for fusing event and log data from multiple platforms into a security operations center to improve monitoring and detection capabilities for an organization. Future builds should also demonstrate how to recover from a loss of system or information integrity such as a ransomware attack for ICS environments.

Additionally, trends in manufacturing such as Industry 4.0 and the industrial IoT are increasing connectivity, increasing the attack surface, and increasing the potential for vulnerabilities. Future builds should consider how these advances can be securely integrated into manufacturing environments.
# Appendix A List of Acronyms

AAL	Application Allowlisting
BAD	Behavioral Anomaly Detection
CRS	Collaborative Robotic System
CRADA	Cooperative Research and Development Agreement
CSF	NIST Cybersecurity Framework
CSMS	Cybersecurity for Smart Manufacturing Systems
DMZ	Demilitarized Zone
EL	Engineering Laboratory
FOIA	Freedom of Information Act
ICS	Industrial Control System
ΙοΤ	Internet of Things
ІТ	Information Technology
LAN	Local Area Network
NCCoE	National Cybersecurity Center of Excellence
NFS	Network File Share
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
ОТ	Operational Technology
PCS	Process Control System
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block
SP	Special Publication
SPAN	Switched Port Analyzer

SRP	Software Restriction Policies
SSH	Secure Shell
TE	Tennessee-Eastman
VDI	Virtual Desktop Interface
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

# Appendix B Glossary

Access Control	The process of granting or denying specific requests to: 1) obtain and use in- formation and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border cross- ing entrances). SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009
Architecture	A highly structured specification of an acceptable approach within a frame- work for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability). SOURCE: FIPS 201-2
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: FIPS 200
Authorization	The right or a permission that is granted to a system entity to access a system resource. SOURCE: NIST SP 800-82 Rev. 2
Backup	A copy of files and programs made to facilitate recovery if necessary. SOURCE: NIST SP 800-34 Rev. 1
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. SOURCE: NIST SP 800-137
CRADA	Collaborative Research and Development Agreement SOURCE: NIST SP 1800-5b, NIST SP 1800-5c
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, elec- tronic communications systems, electronic communications services, wire communication, and electronic communication, including information con- tained therein, to ensure its availability, integrity, authentication, confidential- ity, and nonrepudiation. SOURCE: CNSSI 4009-2015 (NSPD-54/HSPD-23)
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a com- puting environment/infrastructure; or destroying the integrity of the data or stealing controlled information. SOURCE: NIST SP 800-30 Rev. 1

Data	A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unau- thorized or accidental manner. SOURCE: CNSSI-4009
File Integrity Checking	Software that generates, stores, and compares message digests for files to de- tect changes made to the files. SOURCE: NIST SP 800-115
Firmware	Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execu- tion of the programs. SOURCE: CNSSI 4009-2015
Industrial Control Systems	An information system used to control industrial processes such as manufac- turing, product handling, production, and distribution. SOURCE: NIST SP 800-30 Rev. 1
Information Security	The protection of information and information systems from unauthorized ac- cess, use, disclosure, disruption, modification, or destruction in order to pro- vide confidentiality, integrity, and availability. SOURCE: FIPS 199 (44 U.S.C., Sec. 3542)
Information System	A discrete set of information resources organized for the collection, pro- cessing, maintenance, use, sharing, dissemination, or disposition of infor- mation. SOURCE: FIPS 200 (44 U.S.C., Sec. 3502)
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, move- ment, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. SOURCE: FIPS 200
Log	A record of the events occurring within an organization's systems and net- works. SOURCE: NIST SP 800-92
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. SOURCE: NIST SP 800-111

Network Traffic	Computer network communications that are carried over wired or wireless networks between hosts. SOURCE: NIST SP 800-86
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). SOURCE: NIST SP 800-37 Rev. 2
Privacy	Assurance that the confidentiality of, and access to, certain information about an entity is protected. SOURCE: NIST SP 800-130
Remote Access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).
	SOURCE: NIST SP 800-128 under Remote Access from NIST SP 800-53
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: FIPS 200
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis. SOURCE: NIST SP 800-63-2
Risk Management Framework	The Risk Management Framework (RMF), presented in NIST SP 800-37, pro- vides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. SOURCE: NIST SP 800-82 Rev. 2 (NIST SP 800-37)
Security Control	A protection measure for a system SOURCE: NIST SP 800-123
Virtual Machine	Software that allows a single host to run one or more guest operating sys- tems SOURCE: NIST SP 800-115

## Appendix C References

- [1] C. Singleton et al., X-Force Threat Intelligence Index 2021, IBM, February 2021, https://www.ibm.com/security/data-breach/threat-intelligence
- [2] A Sedgewick et al., *Guide to Application Whitelisting*, NIST SP 800-167, NIST, Oct. 2015. Available: http://dx.doi.org/10.6028/NIST.SP.800-167.
- [3] Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance, 2015. Available: <u>https://www.cisa.gov/uscert/sites/de-</u> <u>fault/files/c3vp/framework\_guidance/critical-manufacturing-framework-implementation-guide-</u> <u>2015-508.pdf</u>.
- [4] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD201300091, Feb. 12, 2013. Available: <u>https://obamawhitehouse.archives.gov/the-press-of-fice/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity</u>.
- [5] NIST, Framework for Improving Critical Infrastructure Cybersecurity, V1.1 April 16, 2018. Available: <u>https://doi.org/10.6028/NIST.CSWP.04162018</u>.
- [6] J. McCarthy et al., Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection, NIST Interagency Report (NISTIR) 8219, NIST, Nov. 2018. Available: <u>https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf</u>.
- [7] K. Stouffer et al., Cybersecurity Framework Manufacturing Profile, NIST Internal Report 8183, NIST, May 2017. Available: <u>https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf</u>.
- [8] R. Candell et al., An Industrial Control System Cybersecurity Performance Testbed, NISTIR 8089, NIST, Nov. 2015. Available: <u>http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf</u>.
- [9] Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53 Revision 5, NIST, Apr. 2013. Available: <u>https://doi.org/10.6028/NIST.SP.800-53r5</u>.
- [10] W. Newhouse et al., National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST SP 800-181, Aug. 2017. Available: <u>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf</u>.
- [11] J. Cawthra et al., Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, NIST Special Publication 1800-25 Dec. 2020, <u>https://doi.org/10.6028/NIST.SP.1800-25</u>.
- [12] Celia Paulsen, Robert Byers, Glossary of Key Information Security Terms NISTIR 7298, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf.

- [13] U.S.-Canada Power Systems Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Available: <u>https://www.en-ergy.gov/sites/default/files/oeprod/DocumentsandMedia/Outage\_Task\_Force\_DRAFT\_Report\_on\_Implementation.pdf</u>
- [14] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Revision 2, NIST, June 2015, Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf</u>
- [15] J. J. Downs and E. F. Vogel, "A Plant-wide Industrial Problem Process," Comput. Chem. Eng., vol. 17, no. 3, 1993, pp. 245–255

## Appendix D Scenario Execution Results

The following section provides details regarding the execution and results from each scenario. Details such as usernames, filenames, IP addresses, etc. are specific to the NCCoE lab environment and are provided for reference only.

## D.1 Executing Scenario 1: Protect Host from Malware via USB

An authorized user inserts a USB storage device containing a malware file (1.exe) into a system in the manufacturing environment (e.g., an engineering workstation). After insertion, the malware file (1.exe) attempts to execute. The expected outcome is that the application allowlisting technology blocks the execution of the file.

## D.1.1 Build 1

## D.1.1.1 Configuration

- Application Allowlisting: Carbon Black
  - Agent installed on an HMI Workstation and configured to communicate to the Carbon Black Server.

#### D.1.1.2 Test Results

Carbon Black successfully detects and blocks the malware (1.exe) from running as shown in Figure D-1. Figure D-2 shows Carbon Black's server log. The log provides more detail on the activity detected by Carbon Black.

Figure D-1 An Alert from Carbon Black Showing that Malware (1.exe) was Blocked from Executing

ecurity Notification - Unapproved File
Cberry Target: 1.exe Path: e:\ Process: explorer.exe
Cb Protection blocked an attempt by explorer.exe to run 1.exe because the file is not approved. If you require access to this file, please contact your system administrator or submit an approval request. Note that approval requests are processed based on priority and arrival time. Please be patient while your request is reviewed and processed. Scroll down for diagnostic data.
▼ Submit Approval Request>>
Process Target Path
1 explorer.exe 1.exe e:\
<u>۱</u>
Approval Request
Enter your reason for access (512 characters A Your Email:
Priority: Medium
Submit
Protection by Carbon Black, Inc.

#### Figure D-2: Carbon Black's Server Provides Additional Details and Logs of the Event

	CB-Server	lan.lab Home <del>-</del>	Reports - Assets - Rul	es 🕶 Tools 🕶				-
Home - Events						Version 8.1.10.3		
(The Current View Has Unsav	ed Changes - I	Discard)	Group By:	Subgro	up By:	Max Age:		
	~	Cache	Add (none)	Ascending  v (none)	<ul> <li>Descending by count </li> </ul>	None		
Show Columns * Export	to CSV Acce	ss Event Archives   Refresh Ti	able					
×								
ed before V 04/0	8/2021 15:	23:08						
Cancel Reset								
earch:			tomatically apply Showing	5 out of ?? item(s)				
Timestama =	Countity	Type	Subtra	Source	Description		ID Address	lleer
Threstamp -	Seventy	type	Subtype	Jource	Computer LAN/EGS-61338HH discovery	nd now file 'e') 1 ave' [2D2CB_41224]. Discovered BullKernel-Execute]	IF Audiess	Coel
Apr 7 2021 02:51:09 PM	Notice	Discovery	New unapproved file to computer	LAN\FGS-61338HH	FileCreated[8/24/2020 2:23:10 PM] Disc YaraClassifyVersionId[2] Rules[IsExe,IsE	overed[4/7/2021 6:51:09 PM (Hash: 4/7/2021 6:51:09 PM)] bepincompatibleExe]	172.16.1.4	LAN\nccoeUser
Apr 7 2021 02:51:09 PM	Notice	Policy Enforcement	Execution block (unapproved file)	LAN\FGS-61338HH	File 'e:\1.exe' [2D2CBA1224] was bloc	ked because it was unapproved.	172.16.1.4	LAN\nccoeUser
Apr 7 2021 02:47:35 PM	Notice	Discovery	New unapproved file to computer	LAN\FGS-61338HH	Computer LAN\FGS-61338HH discovere FileCreated[8/24/2020 2:23:10 PM] Disc YaraClassifyVersionId[2] Rules[IsExe.IsE	ed new file 'e:\1.exe' [2D2CBA1224]. DiscoveredBy[Kernel:Execute] :overed[4/7/2021 6:47:35 PM (Hash: 4/7/2021 6:47:35 PM)] bepIncompatibleExe]	172.16.1.4	LAN\nccoeUser
Apr 7 2021 01:43:52 PM	Notice	Policy Enforcement	Execution block (unapproved file)	LAN\POLARIS	File 'e:\1.exe' [2D2CBA1224] was bloc	ked because it was unapproved.	10.100.0.20	LAN\nccoeUser
Apr 7 2021 01:43:52 PM	Notice	Discovery	New unapproved file to computer	LAN\POLARIS	Computer LAN\POLARIS discovered ner FileCreated[8/24/2020 2:23:10 PM] Disc YaraClassifyVersionId[2] Rules[IsExe,IsE	w file 'e:\1.exe' [2D2CBA1224]. DiscoveredBy[Kernel:Execute] :overed[4/7/2021 5:43:52 PM (Hash: 4/7/2021 5:43:52 PM)] !epIncompatibleExe]	10.100.0.20	LAN\nccoeUser
of 22 item(s)					Showing all data			

#### Figure D-3 Carbon Black's Server Log of the Event

File 'e:\1.exe' [2D2CB...A1224] was blocked because it was unapproved.

Computer LAN\POLARIS discovered new file 'e:\1.exe' [2D2CB...A1224]. DiscoveredBy[Kernel:Execute] FileCreated[8/24/2020 2:23:10 PM] Discovered[4/7/2021 5:43:52 PM (Hash: 4/7/2021 5:43:52 PM)] YaraClassifyVersionId[2] Rules[IsExe,IsDepIncompatibleExe]

## D.1.2 Build 2

#### D.1.2.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to HMI Workstation.

#### D.1.2.2 Test Results

The execution of *1.exe* is blocked successfully when Windows SRP is enforced as shown in Figure D-4.

Figure D-4 Windows 7 Alert as a Result of Windows SRP Blocking the Execution of 1.exe

Compu	iter 🕨 Local Disk (C:) 🕨 Temp 🕨			• 49 Search Te	imp
Organize 🔹 🛛 👼 Ope	en New folder				
Favorites	Name	Date modified	Туре	Size	
E Desktop	SysinternalsSuite	11/13/2018 4:35 PM	File folder		
🗼 Downloads	1	8/24/2020 10:23 AM	Application	73 KB	
Libraries	UpdatePending.csv	2/15/2018 9:56 AM	CSV Hie	76 KB	
Music ·	C:\Temp\1.exe				_
	This program is blocked b administrator.	y group policy. For more information	on, contact your sy	stem	

## D.1.3 Build 3

## D.1.3.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to Engineering Workstation.

## D.1.3.2 Test Results

For Build 3, Windows SRP application allowlisting is enabled in the Collaborative Robotics environment. Figure D-5 shows that the executable is blocked on the CRS workstation.

Figure D-5 Windows 10 Alert as a Result of Windows SRP Blocking the Execution of 1.exe



## D.1.4 Build 4

#### D.1.4.1 Configuration

- Application Allowlisting : Carbon Black
  - Agent installed on Engineering Workstation and configured to communicate to the Carbon Black Server.

#### D.1.4.2 Test Results

Carbon Black successfully detects and blocks the malicious file as shown by the Carbon Black notification in Figure D-6.

#### Figure D-6 Carbon Black Blocks the Execution of 1.exe for Build 4

Security Notification - Unapproved File

Cb Protection blocked not approved. If you administrator or subm Note that approval rec Please be patient whil diagnostic data.	.exe :\ xplorer.exe an attempt by explorer.ex require access to this file, it an approval request. quests are processed base e your request is reviewed	e to run 1.exe becaus please contact your s d on priority and arriv and processed. Scro	se the file is ystem val time. oll down for
			~
Submit Approval Requ	est>>		ОК
Process	Target	Path	
1 explorer.exe	1.exe	e:\	
<			>
- Approval Request			
Enter your reason for a max).	access (512 characters	Your Email:	n 💌
Protection by Carbon Bla	ck, Inc.		

## D.2 Executing Scenario 2: Protect Host from Malware via Network Vector

An attacker who has already gained access to the corporate network attempts to pivot into the ICS environment through the DMZ. From a system in the DMZ, the attacker scans for vulnerable systems in the Testbed LAN environment to continue pivoting toward the ICS environments. In an attempt to establish a persistent connection into the ICS environment, the malicious file (1.exe) is copied to a system in the Testbed LAN environment and executed. The expected outcome is that the malicious file is

blocked by the application allowlisting tool, and the RDP and scanning network activity is observed by the behavioral anomaly detection tool.

## D.2.1 Build 1

## D.2.1.1 Configuration

- Application Allowlisting: Carbon Black
  - Agent installed on systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2 and configured to communicate to the Carbon Black Server.
- Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## D.2.1.2 Test Results

Abnormal network traffic is detected by Tenable.ot as shown in <u>Figure D-7</u>. <u>Figure D-8</u> shows the initial RDP connection between an external system and the DMZ system, and <u>Figure D-9</u> provides more detail of the session activity. <u>Figure D-10</u> shows that Tenable.ot detected the VNC connection between the DMZ and the Testbed LAN. <u>Figure D-11</u> shows a detected ports scan performed by the DMZ system target at a system in the Testbed LAN. Tenable.ot detected the RDP scan from the DMZ to the NESSUS VM in the Testbed LAN, as shown in <u>Figure D-12</u>, and <u>Figure D-13</u> provides more details on that detected event. The execution of the malware (1.exe) is blocked by Carbon Black agent as shown in <u>Figure D-14</u>.

#### Figure D-7 Tenable.ot Dashboard Showing the Events that were Detected

E C tenable.ot							01:54 PM	<ul> <li>Tuesday, Apr 13, 203</li> </ul>	21 NCCOE User
• Events			_						
All Events	All Events	Search	٩				1	Resolve All	Export O
Configuration Events	LOG ID	TIME 🕹	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD
SCADA Events	19279	02:53:58 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		CRS NAT Interface	
Network Threats	19282	02:53:53 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		LAN-AD	
Network Events	19285	02:53:50 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		Rigel	
<b>9</b> Policies	19277	02:53:46 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		George.local	
🍰 Inventory	19283	02:53:43 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		SysLog	
Controllers	19267	02:53:39 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		LAN-ADO2	
Network Assets	19269	02:53:35 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		WSUSVM	3
≜ Risk	19266	02:53:35 PM · Apr 12, 2021	Intrusion Detection	Medium	Scans - VNC	HistorianDMZ		Orion	
🛔 Network	19270	02:53:32 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		Orion	
Groups	19265	02:53:31 PM · Apr 12, 2021	Intrusion Detection	Medium	Scans - VNC	HistorianDMZ		VEEAM	
Reports	19271	02:53:28 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		VEEAM	
o <sup>o</sup> Local Settings	19268	02:53:23 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		SymantecMgrVM.I	
	19263	02:49:47 PM · Apr 12, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19		HistorianDMZ	
	<								
	Items: 1-100 out	of 17135						K 🤇 Page	e1of172 > >
	Event 19308	12:25:03 PM · Apr 13, 2021 Por	t Scan High Not resolved						
	Details	<b>A</b>							
	Source	A Port scan is a pro	be to reveal what ports are open a	nd listening on a	given asset				
	Affected Assets	SOURCE NAME	OPC Server		Why is this im	portant?	Suggest	ed Mitigation	
	Policy	SOURCE ADDRESS			Wily is uns in	portanti	DOPPERS	cu mingation	
	Scanned Ports	DESTINATION NAME	Server #22		Port scans are communicatio Some port sca	part of mapping n channels to an asset. ns are legitimate and do	Make s source ne scan w	ure that you are familiar w of the port scan and that to as expected. In case you ar	ith the his port re not

#### Figure D-8 Detected RDP Session Activity from External System to DMZ System

LOG ID	тіме 🗸	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD	
19251	02:18:57 PM · Apr 12, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19		HistorianDMZ		
19250	02:18:45 PM · Apr 12, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19		HistorianDMZ		

15

Figure D-9 Event Detection Detail for the RDP Connection from the External System to the Historian in the DMZ

Event 19251	51 02:18:57 PM · Apr 12, 2021 Unauthorized Conversation Medium Not resolved	
Details	A conversation in an unauthorized protocol has been detected	
Source		
Destination	SOURCE NAME Work Station #19	
Policy	SOURCE ADDRESS	
Status	DESTINATION NAME <u>HistorianDMZ</u>	
	DESTINATION ADDRESS	
	PROTOCOL RDP (tcp/3389)	
	PORT 3389	
	PROTOCOL GROUP In Any Protocol	

#### Figure D-10 Tenable.ot Detected VNC Connection Between the DMZ and the Testbed LAN

Details	Intrusion Detection e	events may indicate malicious communications based of	on known traffic patterns	
ule Details ource	SOURCE NAME	HistorianDMZ	Why is this important?	Suggested Mitigation
estination	bation SOURCE ADDRESS 10.100.1.4 DESTINATION NAME <u>Stratix8300 FA2</u>	10.100.1.4	Interview detection quests may indicate	Make sure that the source and destination
blicy		Stratix8300 FA2	that the network has been compromised and is exposed to malicious entities. It is	assets are familiar to you. In addition, depending on the suspicious traffic, you
atus	DESTINATION ADDRESS	10.100.0.40   172.16.2.1	important to be aware of any such traffic that may indicate reconnaissance activity,	may consider updating anti-virus definitions, firewall rules or other security
	PROTOCOL	rfb (tcp/5900)	threat to/from other subnets of the network.	particular rule.
	PORT	5900		
	RULE MESSAGE	ET SCAN Potential VNC Scan 5900-5920		
	SID	2002911		

Figure D-11 Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in the Testbed LAN

Details	A Port scan is a probe to reveal what ports are open and listening on a given asse		
Source	the state is a prose to receive must be to see a periodic and state in Sec. a Sec.		
Affected Assets	SOURCE NAME HistorianDMZ	Why is this important?	Suggested Mitigation
Policy	SOURCE ADDRESS 10.100.1.4	Port scans are part of mapping	Make sure that you are familiar with the
Scanned Ports	DESTINATION NAME Laptop	communication channels to an asset. Some port scans are legitimate and done by	source of the port scan and that this port scan was expected. In case you are not
Status	DESTINATION ADDRESS 10.100.0.101   192.168.0.205	monitoring devices in the network. However, such mapping may also be done in the article store of matterk in order to	familiar with the source check with the source asset owner to see whether this wa
	PROTOCOL tcp	detect vulnerable and accessible ports for malicious communication.	check which other assets have been scanned by the source asset and consider
	PORT		isolating the source asset to decrease network exposure while you investigate

#### Figure D-12 Detected RDP from a DMZ system to a Testbed LAN system

19299	03:01:39 PM · Apr 12, 2021	RDP Connection (Authenticated)	Medium	External RDP Communication	HistorianDMZ	10.100.1.4	NESSUSVM	10.100.0.25

Figure D-13 Tenable.ot Event Detail Showing the RDP Connection Between the Historian in the DMZ to a Workstation in the Testbed LAN

Details	An authenticated init	tiation of an RDP connection		
ource	SOURCE NAME	<u>HistorianDMZ</u>		Provide a state of the
olicy	SOURCE ADDRESS	10.100.1.4	why is this important?	Suggested Mitigation
atus	DESTINATION NAME	NESSUSVM	common way for cyber threats to propagate towards their target. Often	<ol> <li>Check if this communication was approved.</li> <li>Investigate if it was done by an</li> </ol>
	DESTINATION ADDRESS	10.100.0.25	system administrators prefer to limit use of such protocols to unique support cases so that they can identify the use of such	authorized employee. 3. Check for potential initiation of such a communication by malware.
	PROTOCOL	Rdstls	protocols as anomalies.	,
	COOKIE	Cookie: mstshash=nccoeuser		

#### Figure D-14 Attempt to Execute 1.exe Failed

		Security Notific	ation - Ur	napproved	File	
(	Cb Target: Path: Process:	1.exe c:\users\nccoeuse explorer.exe	r\desktop\			
Cb F not i adm Note Plea diag	Protection block approved. If yo inistrator or sul a that approval use be patient w pnostic data.	ed an attempt by ei ou require access to bmit an approval re requests are proces hile your request is	xplorer.exe this file, p quest. sed based reviewed a	to run 1.ex lease conta on priority and process	e because the ct your system and arrival tim ed. Scroll dow	n n ne. wn for
Subr	nit Approval Re	ouest>>				ОК
1	Process	Target		Path		
1	Process explorer.exe	Target 1.exe		Path c:\user	s\nccoeuser\d	esktop\
1	Process explorer.exe	Target 1.exe		Path c:\user	s\nccoeuser\d	esktop\
1	Process explorer.exe	Target 1.exe		Path c:\user	s\nocoeuser\id	esktop\

## D.2.2 Build 2

#### D.2.2.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

#### D.2.2.2 Test Results

<u>Figure D-15</u> shows the RDP alert for connection into the DMZ, while <u>Figure D-16</u> shows the details of the alert. <u>Figure D-17</u> shows a collection of suspicious activity detected by Forescout eyeInspect when scanning and an RDP connection is executed. <u>Figure D-18</u> and <u>Figure D-19</u> show details of a port scanning alert and the second RDP connection into the manufacturing environment, respectively. The attempt to execute malware (1.exe) is blocked by Windows SRP as shown in <u>Figure D-20</u>.



#### Figure D-15 Alert Dashboard Showing Detection of an RDP Session

Figure D-16 Details of the Detected RDP Session Activity from an External System to DMZ System

Ale al a serie de la conserie de	t datalle								
anima     Searches	t details	Back Edit Delete	trim St	10W   0 ASS	ign to case Download   -				
minu     instantion     instantion     Marrien     Marrien       result     101     100     1000000000000000000000000000000000000									
nd 0121 01210 01210 0120	ummary			^	Source host info		^	Alert Details	
smmend end manual end manual end	ert ID	203138			IP address	(Public IP)		ID and name	lan_cp_cnw_c - Communication pattern not whitelisted
standard	mestamp	Oct 16, 2020 10:05:47			Host MAC addresses	Unknown			Communication pattern not whitelisted: the source and destin
Mending Mender Mende	nsor name	sensor-bundle-nccoe			Other observed MAC	(Rockwell)		Description	ore write issue in some communication rule, but not with this combination
du     #10 memory     memory <td>etection engine</td> <td>Communication patterns (LAN CP)</td> <td></td> <td></td> <td>Role</td> <td>Terminal dieor</td> <td></td> <td>Triggering rule/default</td> <td>alert</td>	etection engine	Communication patterns (LAN CP)			Role	Terminal dieor		Triggering rule/default	alert
	ofile	8 - TCP communications			Vendor and model	Rockwell		action	
unide         Unide         Servere         Se	verity	Medium			Client protocols	RDP (TCP 3389)			
main     ensite     ensite     ensite       main     image     image     image       main     image     image <td>urce MAC</td> <td>(Cisco)</td> <td></td> <td></td> <td>Server protocols</td> <td>NozAKnownOne (TCP 4444)</td> <td></td> <td></td> <td></td>	urce MAC	(Cisco)			Server protocols	NozAKnownOne (TCP 4444)			
	stination MAL	Corporate Workstation			Purdue level	4 - Site business network			
	urce in	0 (al-sime)			Security Risk	BILLID 3.3			
image	urce port	49932			Operational Risk	0.0			
mm     mm     mm       mm     P       mm     To	stination port	3389			Criticality	81000 L			
pm     p     pm     pm <t< td=""><td>proto</td><td>Ethernet</td><td></td><td></td><td>Known vulnerabilities</td><td>0</td><td></td><td></td><td></td></t<>	proto	Ethernet			Known vulnerabilities	0			
prome me me me me me me me me me me me me m	proto	IP.			Related alerts	6 (Show)			
prote     60       remained     600       remained     600       remained     600       state     1000       remained     600       remained     600 <td>proto</td> <td>TCP</td> <td></td> <td></td> <td>First seen</td> <td>Oct 14, 2020 11:56:54</td> <td></td> <td></td> <td></td>	proto	TCP			First seen	Oct 14, 2020 11:56:54			
Presentation       Interview       Interview <td>proto</td> <td>RDP</td> <td></td> <td></td> <td>Last seen</td> <td>Oct 16, 2020 10:16:45</td> <td></td> <td></td> <td></td>	proto	RDP			Last seen	Oct 16, 2020 10:16:45			
Name Annotation Series Seri	P stream opened in hot	folse							
interview       Partners       Partners       Partners         interview       Normal       Partners       Partners         interview       Normal       Normal       Normal         intenon       No	art mode	Not analyzed			Destination host info		^		
international	bels	stor selelyzeu			IR address	(Dei, and 10)			
neme in the second seco	er notes				IP address	(Private IP)			
Joint dictories     Joint die Service     Joint die Service     Joint die Service     Joint die Service     Joint die Service       Service     National     National     Service     Service       ALUM     10001.020     no     Service     Service       Service     National     Service     Service       Service     Service     Service     Service       Service     Service     Service     Service					Other bost names	produce.			
oniced networks         Address         Value Second descended           rec         Address         VAL 05 o         Gene Address         Gene						(Microsof)			
me       Advast       VAN Do       Operationance Marco       Operationance Marco         KLAN       10.00.1204       ay       Anome       Income         Service       Service       Monte Marco       Monte Marco       Monte Marco         Service       Service       Monte Marco       Monte Marco       Monte Marco         Service       Service       Monte Marco       Monte Marco       Monte Marco         Service       Service       Service       Monte Marco       Monte Marco         Service       Service       Service       Service       Service         Service       Service       Service       Service       Service       Service         Service       Service       Service       Service       Service       Service       Service         Service       <	onitored networks			^	Host MAC addresses	Last seen: Oct 16, 2020 10:44:57			
RLNN     Io 1000.1024     ary     Reference     Constrained       Normaliane     Ober roles     Ober roles     Ober roles       Ober roles     Ober roles     Ober roles     Ober roles       VIII STATUS     VIII STATUS     VIII STATUS     VIII STATUS       VIII STATUS     VIII STATUS     VIII STATUS <t< td=""><td>me</td><td>Address VL</td><td>LAN IDs</td><td></td><td>Other observed MAC</td><td>(Rockwell) (Buggedco)</td><td></td><td></td><td></td></t<>	me	Address VL	LAN IDs		Other observed MAC	(Rockwell) (Buggedco)			
Action       Bok       Tennol arree         Apple and arree       Other rate       Other rate         Other rate       Other rate       Other rate         APPL (CF 44)       Windows User versions (Tennol diret)         Other rate       APPL (CF 44)         APPL (CF 44)       APPL (CF 44)         APPL (CF 24)       APPL (CF 24)	47 LAN	10 100 1 0/24			addresses	(Cisco)			
Abelies     Abbelies       Abbelies     Value, start       Value, start     3- Sine sporaziones and control       Security Filolik     1111 do 100       Operationes/Filolik     1112 do 100       Criticality     1113 do 100       Known vulnerabilities     0       Belies alarets     92 (Spow)					Client protocols	DCOM.(TCP 13) DCOM.(TCP 13) PaleConversion (TC 21, 7), 93, 110, 389, 8834, 49179, 49 Salaction (TC 21, 7), 93, 110, 389, 8834, 49179, 49 Salaction (TC 21, 7), 93, 110, 389, 8834, 49179, 49 Salaction (TC 21, 45), 50 Salaction (TC 21, 45), 50 NotAlexandrow (TC 24, 45), 50 NotAlexandrow (TC 24, 45), 50 NotAlexandrow (TC 24, 45), 51 NotAlexandrow (TC 24, 45), 51 Stop (TC 24, 35), 55 Stop	93, 43724, 49690,		
Firstseen 54p 3, 2020 1647/58					Labels Purdue level Security Risk Operational Risk Criticality Known vulnerabilities Related alers First seen	CMG (TCP 445) SSL (TCP 547), 5572) Van,dia+1 3 - Site operations and control METE 5.0 MEDE 2.0 MEDE 1.0 0 222 (Show) Sap 3, 2020 16/47.58			

<) FORESCOUT	🚯 Dash	board 🚓 Network	Events 🔊 Sensors 🛛	Settings									🖵 🧶 🌻	admir
llerts	Reload	Export   ~ Aggregate	details Create new case	Settings										? Hel
Filters: Edit Time-based Filters	Reset	Alerts per event type (top	9 10)										1m <del>-</del>	<b>^</b> 15 •
Today     Last 7 days     Last 7 days     Last 30 days     last 30 days     last 30 days     last X days     From days     Last X days     From days X tay X days after     From date X to 30 days after     Alert Filters	~	38 aterts 30 aterts 20 sterts 10 aterts 10.40	10.45 10.59 10.45 10.59	10:55	1	00	11.05	11:10	11:15	Communic 11:20	11.25	11:30	Application protocol	11:40
Excluding event type ID     By monitored network     Excluding profile     Excluding arc MAC		O items selected  Timestamp +	Event name(s)	Sensor (Not set	Engine (Not 🖕	Profile (Not set)	Status (Not set)	Severity (Not set	Source address		Destination address	Dest. Port	L7 Proto (Not set)	Case ID
Excluding dat MAC Excluding src IP Excluding src IP Excluding str IP		Oct 16, 2020 10:11:37           Oct 16, 2020 10:11:35	Communication pattern not	sensor-bu	Comm	9 - UDP com 9 - UDP com	Not analyzed Not analyzed	M Bank	10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz)		10.100.0.25 (nessus 10.100.0.25 (nessus	3389 (UDP) 3389 (UDP)	NotAKnownOne NotAKnownOne	
Excluding dst part By L2 protocol By L3 protocol		Oct 16, 2020 10:11:13     Oct 16, 2020 10:11:10     Oct 16, 2020 10:09:41	Communication pattern not Communication pattern not TCP SYN portscan	sensor-bu sensor-bu	Comm Comm Portscan	8 - TCP com 8 - TCP com	Not analyzed Not analyzed Not analyzed	III CEO L	10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz)		10.100.0.25 (nessus 10.100.0.25 (nessus	3389 (TCP) 3389 (TCP)	RDP RDP	
By L4 protocol By upstream data By downstream data		Oct 16, 2020 10:09:11 Oct 16, 2020 10:09:10	Communication pattern not	sensor-bu	Comm	8 - TCP com 8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz)		10.100.0.181 10.100.0.177 (opena	22 (TCP) 22 (TCP)	SSH SSH	
By FEA type By field path By lebels		Οct 16, 2020 10:07:59           Οct 16, 2020 10:07:52	Communication pattern not	sensor-bu	Comm	8 - TCP com 8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz)		10.100.0.65 (rugged 10.100.0.50 (ir800.ir	22 (TCP) 22 (TCP)	SSH SSH	
Excluding labels By vlan Excluding vlan		<ul> <li>Oct 16, 2020 10:07:44</li> <li>Oct 16, 2020 10:07:42</li> <li>Oct 16, 2020 10:07:39</li> </ul>	Communication pattern not Communication pattern not	sensor-bu	Comm	8 - TCP com 8 - TCP com	Not analyzed	нца м 1110 м	10.100.1.4 (pi-dmz)		10.100.0.26 (securit 10.100.0.20 (polaris)	22 (TCP) 22 (TCP) 22 (TCP)	SSH SSH	
By detailed description     Excluding detailed description     By alert case		<ul> <li>Oct 16, 2020 10:07:38</li> <li>Oct 16, 2020 10:07:38</li> </ul>	Communication pattern not	sensor-bu	Comm	8 - TCP com 8 - TCP com	Not analyzed Not analyzed	M	10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz)		10.100.0.16 (rigel.lo 10.100.0.15 (george	22 (TCP) 22 (TCP)	SSH SSH	
Miscellaneous Filters	~	Oct 16, 2020 10:07:38	Communication pattern not	sensor-bu	Comm	8 - TCP com 8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz) 10.100.1.4 (pi-dmz)		10.100.0.14 (rugged 10.100.0.11 (orion.lo	22 (TCP) 22 (TCP)	SSH SSH	
		1 to 16 items of 16												

#### Figure D-17 Detection of Scanning Traffic and RDP Connection into Manufacturing Environment

Ab

#### Figure D-18 Details of One of the Port Scan Alerts



#### Figure D-19 Details of Alert for RDP Connection into Manufacturing Environment

	Beck Edit	Delete Trim	Show   - Assi	ign to case Download I			
ummary			^	Source host info	^	Alert Details	
lert ID	203188			IP address	10.100.1.4 (Private (P)	ID and name	lan_cp_cnw_c - Communication pattern not whitelisted
imestamp	Oct 16, 2020 10:11:10			Host name	pi-dmz		Communication pattern not whitelisted: the source and destinati
ensor name	sensor-bundle-nccoe			Other host names	ruggedcom.mgmt.lab	Description	ore whitelisted in some communication rule, but not with this
etection engine	Communication patterns (LAN C	(P)			00:15:5D:02:0D:03 (Microsof)		compression
rofile	8 - TCP communications			Host MAC addresses	Last seen: Oct 16, 2020 11:47:52	Triggering rule/default action	alert
everity	Medium			Other observed MAC	E4:90:69:3B:C2:C2 (Rockwell)		
ource MAC	00:15:5D:02:0D:03 (Microsoft			addresses	94.88.CS.0E.E1.9F (Ruggedco) 7C.0E.CE.67:86.83 (Cisco)		
estigation MAC	20-0E-0E-67-05-88 (Circo)			Role	Terminal server		
ource IP	9 10 100 1 4 (ni-dett)			Other roles	Windows workstation. Terminal client		
incente in	• 10.100.0.25 (company)			OSvertion	Vindous 10 or Windows Server 2016		
vere port	3733				AFP (TCP 445)		
ante por	3733				DCOM (TCP 135)		
estimation port	5.4				DNS (UDP 53, 5353, 5355) FailedConnection (TCP 21, 21, 98, 110, 389, 8834, 49129, 49195		
r proto	Ethernes				54128, 62531, 62532, 62841, 62899)		
proto	lb.				HTTP (TCP 80, 445, 8530) Kerberos (TCP 445)		
proto	TCP				LDAP (TCP 445)		
/ proto	кuP				MSSQL (TCP 445) NTP (UDP 123)		
IP stream opened in hot art mode	false				NetBIOS (UDP 137)		
atus	Not analyzed			Client protocols	NoData (TCP 139) NotAKnownOne (TCP 445)		
ibels	1000 C. 104 C. 104				NotAKnownOne (UDP 443, 1434, 1514, 3389, 32904, 43463, 43724,		
ier potes					43734, 43789, 44102, 44690) OssoftPI (TCP: 5450)		
ALC - HULES					RDP (TCP 3389)		
					SMB (TCP 445) SMB (UDP 138)		
onitored networks			^		SSDP (UDP 1900)		
					SSH (TCP 22) SSI (TCP 443, 445)		
arne	Address	VLAN IDs			SunRPC (TCP 445)		
MZ LAN	10.100.1.0/24	ariy			WS_Discovery (UDP 3702)		
b LAN	10.100.0.0/24	any			FailedConnection (TCP 1542, 1574, 1577, 1585, 2311, 28860, 49690, 49693)		
				Server protocols	NetBIOS (TCP 139)		
				Server protocola	RDP (TCP 3389) SMB (TCP 445)		
					SSL (TCP 5671, 5672)		
				Labels	vlan_ids=1		
				Purdue level	3 - Site operations and control		
				Security Risk	11 6.0		
				Operational Risk	1000 2.0		
				Criticality	1000 L		
				Koman subserabilities	0		
				Related electr	012 (Shara)		
				Related alerts	543 (300W)		
				First seen	58p 3, 2020 10:47:58		
				Last seen	Oct 16, 2020 11:48:50		
				Destination host info	^		
				10.11	10 100 0 17 10 1		
				er adoress	munommula (Private IP)		
				rlost name	nessuaym		
				Other host names	ruggedcom.mgmt.lab		
				Host MAC addresses	00:15:5D:02:0A:06 (Microsof)		
				Other observed MAC	04.00/5.00.01.02.00.01.00.0000		
				addresses	7C/DE/CE/67:86:88 (Cisco)		
				Role	Terminal server		
				Other roles	Windows workstation, Terminal client		
				OS version	Windows 8.1 or Windows Server 2012 R2		
					DNS (UDP 5353, 5355)		
					HTTP (TCP 80)		
					LLDP (LLDP) NetBIOS (UDP 137)		
					NatAKnownOne (TCP 4444)		
				Client protocols	NotAKnownOne (UDP 443) RDP (TCP 3389)		
					SMB (TCP 445)		
					SMB (UDP 138) SSDP (UDP 1900)		
					55H (TCP 22)		
					SSL (TCP 443)		
					DCOM (TCP 135) Extendiorecentrics (TCP 21, 22, 53, 71, 60, 68, 110, 111, 260, 110, 7777		
					5801, 5901, 6667, 7777, 7878, 8080, 8834, 49179, 49195)		
				Server protocols	NetBIOS (UDP 137) NoDate (TCP 139)		
					NotAknownOne (UDP 1434, 3389, 6838, 31037, 36734, 47455)		
					RDP (TCP 3389)		
					RDP (TCP 3389) SMB (TCP 445)		
				Purdue level	RDP (TCP 3389) SMB (TCP 445) 3 - Site operations and control		
				Purdue level Security Risk	RD# (TCP 3389) SM8 (TCP 445) 3 - Site operations and control		
				Purdue level Security Risk Operational Risk	ICIDP (TCP 2000) SMB (TCP 445) 3 - Site operations and control 1011 6.0		
				Purdue level Security Risk Operational Risk Criticality	IRPP(TC13)000           3 - State operations and control           Imp           Imp      <		
				Purdue level Security Risk Operational Risk Criticality Known vulnerabilities	In CP (CC 3 386) 3 - State operations and control In CC 40 KXXX 0.0 KXXX 0.0 KXXXX 0.0 KXXXX 0.0 KXXX 0.0 KXXX 0.0 KXXX 0.0 KX		
				Purdue level Security Risk Operational Risk Criticality Known vulnerabilities Related alerts	Rich (CC 2006)           3 - Stat speakations and constrol           800           8000 <td></td> <td></td>		
				Purdue level Security Risk Operational Risk Criticelity Known vulnerabilities Related aleres First seen	Rich (CC 3 386)           3 - Stie operations and control           Rich (2)		
				Purdue level Security Risk Operational Risk Criticality Known vulnerabilities Related alerts First seen Last seen	RCP (CTC 3106) 31-Stee operations and control 4000 0 0 4000 0 0 4000 0 500		

Figure D-20 Dialog Message Showing 1.exe was Blocked from Executing



## D.2.3 Build 3

## D.2.3.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and Supervisory LAN
- Behavior Anomaly Detection: Dragos
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

## D.2.3.2 Test Results

Windows SRP blocks the attempted execution of 1.exe (Figure D-21). Figure D-22 shows the alerts generated by Dragos when it detected the remote connection to the target. Figure D-23 depicts the detected RDP session from an external system to the DMZ system. Figure D-24 depicts network scanning alert details. Figure D-25 depicts the RDP session from a DMZ system to the Testbed LAN system.



#### Figure D-21 Windows SRP blocked 1.exe From Executing

#### Figure D-22 Log of Alerts Detected by Dragos

DETECTION INFORMATION		ASSOCIATED ASSETS	
WHAT HAPPENED: FILTER: RDP Negeliation Required		View         0         Type         0         0         Name           VIEW         mm         Windows Serv         85         Asset 85	≎ Dir. ≎ dist
CCCURRENT:	LAT FEER Brite Course FATE Brite Course Brite Course Brite Course Brite Course Brite Course Course Brite	VICE     The Asset 54       COMMUNICATIONS SUMMARY       Image: Second Sec	UC
ID Cocurred At		Summary	¢
		No Related Notifications.	

#### Figure D-23 Detail of RDP Session Activity Between an External System and a DMZ System

DETECTION INFORMATION		ASSOCIATED ASSETS
T FILTER		View         1         D         Name         D           View         amon         Windows Sarv, 85         Asset 85         Asset 25
OCCINETS AT:     OCCINETS AT:     OCCINETS AT:     OCCINETS     O	LATTER: STORTO BASING STATE: UNINECONS DORE: NAMART TIME DORE: NAMART TIME DORE: D	VICE     Maset     644     Asset 644       COMMUNICATIONS SUMMARY       Image: State of the state of
RELATED NOTIFICATIONS		Summary . No Reizer Nofications

#### Figure D-24 Detail for Network Scanning Alert

DETECTION INFORMATION		ASSOCIATED ASSETS		
WHAT HAPPENED: Sequential ICMP Sweep Detected		View         Type         ID           VIEW         ID         ID           VIEW         ID         ID	Name	Dir. 10.100.1.4 other
COURRED AT: 02/17/21, 02:50 PM EST COUNT: 1	LAST SEEN: 12/23/04,020 PM EST STATE: UNRESOLVED	COMMUNICATIONS SUMMARY		
DETECTED BY: Scan Sequential DETECTION QUAD: Threat Behavior	SOURCE: Network Traffic ZONES: DMZ	No Communicat	ions Summary.	
ACTIVITY GROUP: ELECTRUM	ICS CYBER KILLCHAIN STEP: Stage 1 - Reconstissance			
MITRE ATT&CK FOR ICS TACTIC Discovery @	MITRE ATT&CK FOR ICS TECHNIQUE T0846: Remote System Discovery 12			
QUERY-FOCUSED DATASETS: Scanning	NOTIFICATION RECORD: No Associated Record			
Network Advects Scanning Activity Detected CASES: No Cases Linked	No Associated Components			
RELATED NOTIFICATIONS				
ID CCcurred At C		Summary		
8		No Related Notifications		

## Figure D-25 Detail of RDP Session Activity Between a DMZ System and a Testbed LAN System

DETECTION INFORMATION		ASSOC	ATED ASSETS						
WHAT HAPPENED: RDP Negotiation Request		Vies	С Туре	≎ ID ≎		Name		•	Dir.
OCCURRED AT:	LACT CEEN-	Vie	Window	s Serv 85 Asset 85				10.100.1.4	erc
02/17/21, 19:51 UTC	01/01/70, 00:00 UTC	Vie	ViEW Vulherability S 37 Asset 37						
	STATE: UNRESOLVED	COMM	JNICATIONS SU	MMARY					_
BDP Port Mismalch	SOURCE: Network Traffic	())							
DETECTION QUAD:	ZONES: DMZ: Orbiersecurity LAN	ð			ICM	P			
	IMC, Optimisatify LAN ISC OFFICE RELATION STREP: ISLight 1- Action Optimise MITTER ATTREEK FOR ICS TECHNIQUE T0885: Commany Land Part ©			1	SS UD	<ssl►< td=""><td></td></ssl►<>			
XENOTIME			Microsoft Corporation pi-dma				e Desktop orporation svm		
MITRE ATTACK FOR ICS TACTIC				10.100	1.1.4	nessu 192.16	svm 5.0.11 10.25		
	LUBAS, CATHRONY USED PORT @	Protocol	Client	C Ephemeral Ports	© Server	Server Ports	C TX Bytes	C RX Bytes	
QUERY-FOCUSED DATASETS: No Applicable Gurry-Focusted Balaxets	NOTIFICATION RECORD: No Associated Record	ICMP	10.100.1.4		10.100.0.25		222.0 bytes	148.0 bytes	
PLAYBOOKS: No Associated Playbooks	NOTIFICATION COMPONENTS: View in Kibana	ICMP	10.100.0.25	52265 52267	10.100.1.4	-	148.0 Dytes	222.0 bytes	
CASES:		UDP	10.100.1.4	56180,56181	10.100.0.25	3389	14.9.68	0 bytes	
RELATED NOTIFICATIONS									
ID Cocurred At C			Summary						_
		No Related Notifications.							
1 .									

## D.2.4 Build 4

#### D.2.4.1 Configuration

- Application Allowlisting: Carbon Black
  - Agent installed on systems in the DMZ, Testbed LAN, and Supervisory LAN and configured to communicate to the Carbon Black Server.
- Behavior Anomaly Detection: Azure Defender for IoT
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

## D.2.4.2 Test Results

Azure Defender for IoT is able to detect the remote access connection to the DMZ as seen in <u>Figure D-26</u>. <u>Figure D-27</u> shows detection of scanning activity, while <u>Figure D-28</u> shows details of the scan. The RDP connection into the manufacturing environment is seen in Figure D-29. Carbon Black blocks 1.exe from executing as shown in <u>Figure D-30</u>.

Figure D-26 Azure Defender for IoT "info" Event Identified Remote Access Connection to the DMZ



#### Figure D-27 Alert for Scanning Activity

💿 Azure Defender for	r loT 🔹 🗡	i 📩 🛨 ul	NESSUS 10.100.2.10 gml.	lab	×	_ 0 ×
← → C ▲	Not secure   1	0.100.0.61/#/events				Q ☆ 😝 :
bushbourd	· · ·	vent i imeline				Ø
Asset Map (95)	윪	Free Search	Q Advanced Filters	All Events 👻 🎗	User Operations	
Asset Inventory	=				(Defus)	Orante Durant D. Durant
Alerts (68)		Device Connection Detect	ed 🗾		CREITESIT	
Reports		Jan 5, 2021 1:54:03 PM		· · · · · · · · · · · · · · · · · · ·		Info 15
		Grouped Events	13:	54:03		
Event Timeline	Ê	Jan 5, 2021 1:54:03 PM Connected devices 10.100.0.62 and 10.100.1	.4			
Data Mining	2	Jan 5, 2021 1:54:03 PM				
Investigation	4	Connected devices 10.100.0.50 and 10.100.1	.4			
Risk Assessment	A	×	Info		Alert Detected Jan 5, 2021 1:53:45 PM	
Attack Vectors	Ø		13:	53:45	Address scan detected. Scanning address: 10.100.1.4 Scanned subnet: 10.100.0/16	
	_				Scanned addresses: 10.100.0.10, 10.100.0.11 10.100.0.12, 10.100.0.13, 10.100.0.14, 10.100	l, 0.0.15.
Custom Alerts	.*				10.100.0.16, 10.100.0 more	
Users	*				PCAP file	
Forwarding	Ö	Remote Access Connectio	on Established		_	
System Settings	•	Jan 5, 2021 1:53:05 PM				Alert
Anun Defender for	*	Grouped Events	13:	53:05		
Version 3.1.1		Jan 5, 2021 1:53:05 PM				
🕂 占 🛛		<b>O</b>				2:08 PM

#### Figure D-28 Details for the Scanning Alert



🔕 Azure Defender fo	r IoT	×		all Nassu		miniate		1
$\leftrightarrow$ $\rightarrow$ C (	Not secure	e	/#/events		U U		Q \$	9
Asset Map (95)	윦	Event Ti	meline					0
Asset Inventory	=	Free Sear	rch	Q	Advanced Filt	ers All E	Events + 2, User Operations 🖸 Select Date	
Alerts (68)	۵						েRefresh 🛛 Create Event 🚯 Exp	ort
Reports						Jan 5, 2021		Î
ANALYSIS				File Transfer Detected Jan 5, 2021 2:04:19 PM				
Event Timeline	Ê		<u>v</u>	HTTP File transfer from client IP: Content type application/octe	Server: t-stream	14-04-19		
Data Mining	2			*		14.04.15	Remote Access Connection Established	
Investigation	\$				Notice		Jan 5, 2021 1:59:30 PM Connection detected from ' to	
Risk Assessment	▲					13:59:30	using Remote Desktop	
Attack Vectors	Ø		0	File Transfer Detected Jan 5, 2021 1:58:08 PM	0			
ADMINISTRATION				Content type application/vne	i.ms-cab-	13:58:08		
Custom Alerts	.*			compressed			Device Connection Detected	
Users	**			Ŷ	Notice		Jan 5, 2021 1:56:03 PM	
Forwarding	Ø					13:56:03	Grouped Events	
System Settings	\$						Jan 5, 2021 1:56:03 PM	
Azure Defender for	ют	-					Connected devices and Jan 5, 2021 1:56:03 PM	
Version 3.1.1							Connected devices and	

#### Figure D-29 Detection of RDP Connection into the Manufacturing Environment

Figure D-30 Carbon Black Shows an Alert for Blocking File 1.exe

Security Notification - Unapproved File
Cb Target: 1.exe Path: c:\users\nccoeuser\desktop\ Process: explorer.exe
Cb Protection blocked an attempt by explorer.exe to run 1.exe because the file is not approved. If you require access to this file, please contact your system administrator or submit an approval request. Note that approval requests are processed based on priority and arrival time. Please be patient while your request is reviewed and processed. Scroll down for diagnostic data.
Submit Approval Request>>
Process Target Path
1 explorer exe 1 exe c:\users\nccoeuser\desktop\
<
- Approval Request
Enter your reason for access (512 characters A Your Email: Priority: Medium
▼ Submit
Protection by Carbon Black, Inc.

# **D.3 Executing Scenario 3: Protect Host from Malware via Remote Access Connections**

An authorized user with an authorized remote workstation, infected with a worm-type malware, connects via remote access capabilities to the manufacturing environments. The malware on the remote host attempts to scan the manufacturing environment to identify vulnerable hosts. The expected result

32

is that the remote access tools effectively stop the worm-type malicious code from propagating to the manufacturing environment from the infected remote workstation.

## D.3.1 Build 1

## D.3.1.1 Configuration

- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for access PCS environment.

## D.3.1.2 Test Results

Figure D-31 shows the remote connection being established through the Cisco AnyConnect VPN application through which a browser is used to access the ConsoleWorks web interface (Figure D-32). Once a connection to ConsoleWorks was established, the simulated worm attack was executed on the remote PC to scan the target network. The scan was successfully blocked by the VPN configuration.



#### Figure D-31 Secured VPN Connection to Environment with Cisco AnyConnect

#### Figure D-32 Remote Access is Being Established Through ConsoleWorks

← → C ▲ Not secure   10.100.0.53;	5176/index.html	÷ \varTheta :
Console <mark>Works</mark> ® vssta	Devices	NCCOE USER NCCOE PCS
	Devices C In Filter Devices	
	PELLEORETARIA Manual analysis	
TDI Technologies, Inc.	2921636410.33 UTC-66.60	Invocation: NCCC

## D.3.2 Build 2

## D.3.2.1 Configuration

- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured to allow authorized users to access PCS environment through the Dispel Enclave to the Dispel Wicket.

## D.3.2.2 Test Results

The user connects to the Dispel VDI as shown in <u>Figure D-33</u> and then connects to the PCS workstation as shown in <u>Figure D-34</u>. Once a connection to the NCCOE environment was established, the simulated worm attack was executed on the remote PC to scan the target network. The scan was successfully blocked by the Dispel VDI configuration.



Figure D-33 Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket ESI


Figure D-34 Nested RDP Session Showing Dispel Connection into the PCS Workstation

## D.3.3 Build 3

## D.3.3.1 Configuration

- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for access CRS environment.

## D.3.3.2 Test Results

<u>Figure D-35</u> shows the remote connection being established through the Cisco AnyConnect VPN application, where a browser is used to access the ConsoleWorks web interface (<u>Figure D-36</u>). Once a connection to ConsoleWorks was established, the simulated worm attack was executed on the remote PC to scan the target network. The scan was successfully blocked by the VPN configuration.



#### Figure D-35 VPN Connection to Manufacturing Environment

## 

#### Figure D-36 Remote Access is Being Established Through ConsoleWorks

## D.3.4 Build 4

#### D.3.4.1 Configuration

- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured to allow authorized users to access the PCS environment through the Dispel Enclave to the Dispel Wicket.

## D.3.4.2 Test Results

<u>Figure D-37</u> shows the Dispel VDI desktop, which allows a connection to the CRS workstation in <u>Figure D-38</u>. Once a connection to the NCCOE environment was established, the simulated worm attack was executed on the remote PC to scan the target network. The scan was successfully blocked by the use of the Dispel VDI.



Figure D-37 Dispel VDI Showing Interface for Connecting Through Dispel Enclave to Dispel Wicket



#### Figure D-38 Nested RDP Session Showing Dispel Connection into the CRS Workstation

## **D.4** Executing Scenario 4: Protect Host from Unauthorized Application Installation

An authorized user copies downloaded software installation files and executable files from a shared network drive to a workstation. The user attempts to execute or install the unauthorized software on the workstation. The expected result is that the application allowlisting tool prevents execution or installation of the software. Also, the behavioral anomaly detection identifies file transfer activity in the manufacturing environment.

## D.4.1 Build 1

## D.4.1.1 Configuration

- Application Allowlisting: Carbon Black
  - Agent installed on systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2 and configured to communicate to the Carbon Black Server.
- Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## D.4.1.2 Test Results

As shown in <u>Figure D-39</u>, Carbon Black is able to block and alert on the execution of putty.exe. Tenable.ot is able to detect the server message block (SMB) connection between an HMI in the Testbed LAN and the GreenTec server (<u>Figure D-40</u>). Details of that alert are shown in <u>Figure D-41</u>.

Figure D-39 Carbon Black Blocks the Execution of putty.exe and Other Files

	(	Target: p Path: c Process: e	outty.exe ::\users\nccoeuser\desktop\ explorer.exe	
1	beca to st	use the file is no op it from runnin	t approved. Choose Allow to let th g at this time. Scroll down for diac	is file run, or choose Block mostic data  Allow Block
S	ubm	hit Justification>>		le.u
????	6 7 8 9	explorer.exe explorer.exe explorer.exe explorer.exe	nmap-7.80-setup.exe putty.exe putty.exe nutty.64bit-0.74-installer.msi	ram c:\users\nccoeuser\desktop c:\users\nccoeuser\desktop c:\users\nccoeuser\desktop
~	-	capioreneae		
?				

Figure D-40 Tenable.ot Alert With the SMB Connection Between the HMI and the GreenTec Server

Powered by Indegy							02.1	o Fix - Weunesuay, Ap	01 14, 2021 NCC	OC.
Events All Events	All Events 10.10	00.1.7	۹					Actions 🗸 🛛 Re	esolve All Export	1
Configuration Events SCADA Events	LOG ID	TIME 4	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD	
Network Threats Network Events Policies Inventory Controllers Network Assets Risk	Items: 1-1 out of 1								< < Page 1 of 1	>
	Event 19555 02.10	1.04 PM Apr 14, 2021 Onat	unonzed conversation Lov	v Notresor	veu					
ontrollers Vetwork Assets Lisk	Details Source Destination	A conversation in an	unauthorized protocol has b	een detected	Why is	this important?		Suggested Mitigation		
Controllers Vetwork Assets Lisk Vetwork Groups Reports	Details Source Destination Policy Status	A conversation in an source name source address destination name	unauthorized protocol has be HMI 172.16.1.4 GreenTec	een detected	Why is Conver- may in are no stands	this important? rsations in unauthori dicate suspicious tra dexpected to commu of portocols and any	zed protocols ffic. Some assets inicate in non- deviation from	Suggested Mitigation Check if this communi it is expected traffic, th conditions so that Ever for similar communics	cation is expected. If hen adjust the Policy nts aren't generated tions in the future. If	f
Controllers Network Assets Risk Network Network Network Reports Controllers Network Ne	Details Source Destination Policy Status	A conversation in an SOURCE NAME SOURCE ADDRESS DESTINATION NAME DESTINATION ADDRESS	unauthorized protocol has be HMI 172.16.1.4 GreenTec 10.100.1.7	een detected	Why is Conve may in are no stand	this important? rsations in unauthori dicate suspicious tra t expected to commu rd protocols and any educt expected to commu	zed protocols ffic. Some assets inicate in non- deviation from	Suggested Mitigation Check if this communi it is expected traffic, th conditions so that Eve for similar communication if	ication is nen adjus nts aren't ations in t	expected. If t the Policy generated he future. I

Figure D-41 Tenable.ot Alert Details of the SMB Connection Between the HMI and the network file system (NFS) Server in the DMZ

= tenable.ot				02:10 PM • Wednesday, Apr 14, 2021 NCCOE User 🛩
Events     All Events     Configuration Events     SCADA Events     Network Threats	Category Network Events	ommunication from En ed Conversation	g Station Detected	STATUS C
Network Events	Details	Policy Definition		
<b>9</b> Policies	Triggered Events	NAME	SMB communication from Eng Station Detected	
∽ 🖧 Inventory	Exclusions	SOURCE	(In ENG. Stations) or (In HMIs)	
Controllers		DESTINATION / AFFECTED ASSET	In Any Asset	
Network Assets		PROTOCOL GROUP	In SMB	
> 🚊 Risk		SCHEDULE	In Any Time	
> 🚆 Network		Policy Actions		
> 🕲 Groups		SEVERITY	Low	
Reports		SYSLOG		
> o <sup>o</sup> Local Settings		EMAIL		
		DISABLE AFTER HIT		
		General		
		CATEGORY	Network Events	
		DISABLED	Enabled	

## D.4.2 Build 2

## D.4.2.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2.

- Behavior Anomaly Detection: eyelnspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

#### D.4.2.2 Test Results

With Windows SRP enabled, putty.exe is not allowed to execute because it is not a permitted application under group policy, as shown in <u>Figure D-42</u>. Windows SRP also blocks the user's attempt to run putty-64bit-0.74-installer.msi. (<u>Figure D-43</u>). Forescout detected the file transfer activity (<u>Figure D-44</u>). <u>Figure D-45</u> shows a detailed description of the alert that was generate for the file transfer activity.

Figure D-42 Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration



#### Figure D-43 putty-64bit-0.74-installer.msi is blocked by Windows SRP



#### Figure D-44 Forescout Alert on the File Transfer Activity

<) FORESCOUT	•		rd 👍 Ne	twork 🔳 Events	Sensors (	OC Settings							🖵 🤌 🇳	🔳 edm
lerts	ke:	load E	eport   ~	Aggregate details	create new case	Settings								
From date X to 30 days after From date X to Y days before														
Alert Filters	^													
Excluding event type ID		0 iter	ns selected											
By mankared neswork			Timestamp +	Event name(s)	Senso	r Ergne	Profile	Status	Severey	Source address	Destination address	Dest. Port	L7 Prata	Case ID
Excluding profile														
Excluding see MAC					O (Net s	- (Ne -	(Not sel) .	(Not set)	(Not st .	1238.04 0	10.100.17	0	(Not set) .	COLASS & *
Excluding dat MAC			Oct 7, 2020	Communication pa	attern senso	r-b Com	8 - TCP co	Not analyzed	M	172.16.1.4 (fgs-61	10.100.1.7 (greent	445 (TCP)	SMB	
Excluding set IP			07.12.20											
Excluding dat IP		1 to 1 its	maoft											
Excluding dist port														
Dy L2 protocol														
By L3 protocol														

Figure D-45 Forescout Alert Details for the File Transfer Activity

Back Edit Delete Trim Show   Y					
		ioad   ×			9 Hel
	Source host info		^	Alert Details	•
130391	IP address	172.10.1.4 (Privata IP)		D and name	lan.cp. cnw.s - Communication pattern not whitelisted
Ort 7, 2020 09:12:38	Host name	fep-613387-h			Communication pattern not ultrailated: the source and destination
sensor-bundle-reces	Other host names	fes-61338Hh.Jan.Jab		Description	hosts are whitelisted in some communication rule, but not with this
Communication petterns (LAN CP)		0C:C4:7A:31:44:47 (SuperMic)			combination
8-TCP communications	Plost MPC addresses	Lost soury Oct 7, 2020 09:22/18		action	alert
Medium		E4:90:69:38:C2:C3 (Rockwell)			
0CiC47A31i44i47 (SuperMic)	Other observed MAC	54:50:69:38:C2:C0 (Rockwell)			
E4:90:69:38:C2:C1 (Reclevell)	ADDresses	7C.6E.CE.67.86:88 (Cisco)			
0 172.16.1.4 (fgs-61338hb)	Refer	Terete al secon			
9 10.100.1.7 (greentec-server)	Other solar	Windows workstation			
49783	Vandor and model	Rectand.			
445	Pl una line	Windows 7 or Windows Securi 2008 87			
Ethernet		DCOM (702 135 20155 20150)			
9		DNS (TCP 53)			
TOP		DNS (UDP 53, 5355) FailedConnection (TCP 80, 139)			
SMB		HTTP (TCP 8530)			
false		LDAP (TCP 389) LDAP (UDP 389)			
Not analyzed	Client protocols	NTP (UDP 123) NetBIOS (UDP 137)			
		NoDaca (TCP 50005)			
		NasAKnawnOne (TCP 1332, 2500, 2501, 10003) NasIAKnawnOne (UDP 1314) SMB (TCP 443)			
^		SADE (UCP 138) SSDP (UCP 1900) SSH (UCP 22) SSL (UCP 443, 10005)			
	Total           Total </td <td>Comparison of the Comparison of the Compari</td> <td>A         A Mod Marka and Marka           Statistics         212.81.24 Process Pt           Statistics         Process Statistics           Statistics         Process Statistics           Demonstrations         Process Statistics           Statistics         Pro</td> <td>A         Mail Mater Manuel         A           Statist Mater Manuel         Participa         10111         1011</td> <td>No         Note Nation         Note Nation         Note Nation         Note Nation           1001        </td>	Comparison of the Compari	A         A Mod Marka and Marka           Statistics         212.81.24 Process Pt           Statistics         Process Statistics           Statistics         Process Statistics           Demonstrations         Process Statistics           Statistics         Pro	A         Mail Mater Manuel         A           Statist Mater Manuel         Participa         10111         1011	No         Note Nation         Note Nation         Note Nation         Note Nation           1001

## D.4.3 Build 3

#### D.4.3.1 Configuration

- Application Allowlisting : Windows SRP
  - Settings are applied to systems in the DMZ, Testbed LAN, and Supervisory LAN
- Behavior Anomaly Detection: Dragos
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

## D.4.3.2 Test Results

With Windows SRP enabled, putty.exe is not allowed to execute because it is not a permitted application under group policy, as shown in <u>Figure D-46</u>. Windows SRP also blocks the user's attempt to run putty-64bit-0.74-installer.msi (<u>Figure D-47</u>). Dragos detected the file transfer activity (<u>Figure D-48</u>). <u>Figure D-49</u> shows a detailed description of the alert that was generated for the file transfer activity.



Figure D-46 Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration



#### Figure D-47 putty-64bit-0.74-installer.msi is Blocked by Windows SRP

Figure D-48	Dragos	Alert	on	the File	Transfer	Activity
-------------	--------	-------	----	----------	----------	----------

				ASSET NOTIFICATI	ONS		SYSTEM ALERTS			RULES		
FILTH	ENG 3		om 2/17/21, 19:00	0 UTC 🛗 10	17/21, 21:00 UTC C REFEREN	394					Q Sweeth 10.100.1.7	×
	View	Sever :	ID :	Occurred At	туре	: Summary	Message	Detected By	: Asset IDs	Source IPv4	: Dest. IPvi :	Other
	VIEW		148575	02/17/21, 19:48 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	80,96	10.100.1.7	192.168.0.2	
1	VIEW		148574	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148573	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148572	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 35 downloaded a file with sha256 hash of cbc	File Transfer of Suspicious PE	151,35	10.100.1.7	192.169.0.20	
	VIEW		148571	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 35 downloaded a file with sha256 hash of obc.	File Transfer of Suspicious PE	151, 35	10.100.1.7	192.168.0.20	
	VIEW		148570	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 48d.	File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148569	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_rew_size	Asset 96 downloaded a file with sha256 hash of 3b4	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2	
	VIEW		140560	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_rew_size	Asset 96 downloaded a file with sha256 hash of 43d.	. File Transfer of Suspicious PE	151,96	10.100.1.7	192.160.0.2	
	VIEW		148557	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 3b4.	File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148555	02/17/21, 19:48 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 35 downloaded a file with sha256 hash of aa6	File Transfer of Suspicious PE	151, 35	10.100.1.7	192.168.0.20	
	VIEW		148565	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 95 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2	
	VIEW.		140564	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious.pe, section	Asset 35 downloaded a file with sha256 hash of cbc.,	File Transfer of Suspicious PE	151,35	10.100.1.7	192.168.0.20	
	VIEW		148563	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 58a.	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.169.0.2	
	VIEW		148502	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 3b4.	File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148561	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_section	Asset 96 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2	
	VIEW		148560	02/17/21, 19:40 UTC	Communication	A Downloaded file hit on: suspicious, raw, size	Asset 96 downloaded a file with sha256 hash of 58a	. File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148559	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on suspicious_pe_section	Asset 35 downloaded a file with sha256 hash of aa6	File Transfer of Suspicious PE	151,35	10.100.1.7	192.168.0.20	
	AIEM		148558	02/17/21, 19:48 UTC	Communication	A Downloaded file hit on: suspicious_pe_section	Asset 96 downloaded a file with sha256 hash of 48d.	File Transfer of Suspicious PE	157,96	10.100.1.7	192.168.0.2	
	VIEW		148557	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_section	Asset 35 downloaded a file with sha256 hash of cbc	File Transfer of Suspicious PE	151,35	10.100.1.7	192.168.0.20	
	VIEW		148556	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious, pe_section	Asset 96 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	80,96	10.100.1.7	192,168.0.2	

#### Figure D-49 Dragos Alert Details of the File Transfer Alert

DETECTION INFORMATION		ASSOCI	TED ASSETS					
WHAT HAPPENED: Asset 95 downloaded a file with sha?56 bash of 41054/6/bas7	490-196/198/450/H794864-71714446-190ha34136-511640-14a from 80 which matched the exerciseus raw size file	View	с туре	≎ ID ≎		Name		C Dir.
FILTER signature rule		VIEV	General L	ise D 80 Asset 80				10.100.1.7 sec
OCCURRED AT:	LAST SEEN:	VIEV	E Router	96 Asset 96				192.168.0.2 dst
COUNT:	STATE:	COMML	NICATIONS SUM	MMARY				
	UNRESOLVED	(2)						
File Transfer of Suspicious PC	SUDIRCE: 0102a555-aac0-4abc-9026-dx69e231916a							
DETECTION QUAD: Threat Behavior	ZONES: DMZ, Cybersecurty LAN	•						
ACTIVITY GROUP:	ICS CYBER KILLCHAIN STEP:	Θ			General Use D Super Micro Computer, 10,100,1	ino : SuperMio		
Nena Nena	Stage 1 - Dalvery				preside-este	ver ver riscel		
MITRE ATT&CK FOR ICS TACTIC	MITRE ATTACK FOR ICS TECHNIQUE	Protocol	Client	Ephemeral Ports	: Server	Server Ports	TX Bytes	: RX Bytes
		SMB	10.100.0.20		10.100.1.7		42.9 KB	43.0 KB
OUERY-FOCUSED DATASETS: No Applicabile Query-Focused Datasets	NOTIFICATION RECORD: View in Kliene	NTLM	10.100.0.20		10.100.1.7		120.1 KB	121.7 KB
PLAYBOOKS: No Associated Playbooks	NOTIFICATION COMPONENTS: View In Kibens	DCE_RPC	10.100.0.20		10.100.1.7		2.1 MD	65.5 MB
CASES:								
RELATED NOTIFICATIONS								
ID C Occurred At C			Summary					
	No Relate	ed Notifications.						

## D.4.4 Build 4

#### D.4.4.1 Configuration

- Application Allowlisting: Carbon Black
- Agent installed on systems in the DMZ, Testbed LAN, and Supervisory LAN and configured to communicate to the Carbon Black Server.
  - Behavior Anomaly Detection: Azure Defender for IoT

Configured to receive packet streams from DMZ, Testbed LAN and Supervisory LAN, and Control LAN.

#### D.4.4.2 Test Results

Carbon Black was able to block execution of putty.exe (Figure D-50) and the installation of putty-64bit-0.74-installer.msi (Figure D-51). Figure D-52 is the alert dashboard for Azure Defender for IoT that shows new activity has been detected. The detailed alert in Figure D-53 provides details of an RPC connection between the GreenTec server and the Testbed LAN. A timeline of events showing a file transfer has occurred is shown in Figure D-54. Figure D-50 Carbon Black Alert Showing that putty.exe is Blocked from Executing

curity N	otification - Unapp	roved Network Location						
C	D Target: p Path: \ Process: e	utty.exe .10.100.1.7\working\appl xplorer.exe	icatio	ns\				
Cb Protection blocked an attempt by explorer.exe to run putty.exe because the network location \\10.100.1.7\working is not approved. If you require access to this file, please contact your system administrator or submit an approval request. Note that approval requests are processed based on priority and arrival time. Please be patient while your request is reviewed and processed. Scroll down for diagnostic data.								
Subm	it Approval Reque	<u>:st&gt;&gt;</u>				ОК		
	Process	Target		Path			^	
Х З	msiexec.exe	putty-64bit-0.74-install	er	c:\users\	nccoeuser	\desktop\		
<b>X</b> 4	explorer.exe	7z1900-x64.exe		c:\users\	nccoeuser	\desktop\		
<b>X</b> 5	explorer.exe	nmap-7.80-setup.exe		c:\users\	nccoeuser	\desktop\	_	
<u>A</u> 6	explorer.exe	putty.exe		\\10.100	.1.7\worki	ng\applicat	on:	
<							>	
	1.0							
Enter max).	your reason for a	access (512 characters	A Ye	our Email:	nefarious	.user@nist	.gov	
					Imeaium .	Submit		
Protectio	on by Carbon Bla	ck, Inc.						

Figure D-51 Carbon Black Alert Showing Execution of putty-64bit-0.74-installer.msi Being Blocked

Security N	otification - Unapp	roved Script			
C	D Target: p Path: c Process: n	utty-64bit-0.74-instal :\users\nccoeuser\de isiexec.exe	ller.msi asktop\		
Cb P 0.74- file, j Note Pleas diagr	rotection blocked installer.msi beca blease contact yo that approval re- te be patient whil hostic data.	an attempt by msiex ause the file is not ap ur system administra quests are processed e your request is rev	kec.exe to proved. Itor or sul based or iewed and	o run the script putty-64bit- If you require access to this Ibmit an approval request. n priority and arrival time. d processed. Scroll down for	~
Subm	it Approval Requ	est>>		ОК	
	Process	Target		Path	_
X 1	ccsvchst.exe	idsxpx86.dll		c:\programdata\symantec\sym	nante
X 2	explorer.exe	1.exe		c:\users\nccoeuser\desktop\	
A 3	msiexec.exe	putty-64bit-0.74-in	staller	c:\users\nccoeuser\desktop\	
<					>
Approv	val Request				
Enter max).	your reason for a	access (512 characte	rs o Yi	Your Email: nefarious.user@nist. Priority: Medium	•
Protecti	on by Carbon Bla	ck, Inc.			

Figure D-52 Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity

Hicrosoft	÷	Alerts			θ
		10.100.1.7	Q   Advanced Filters Security Operational		Main View 👻 🖺 Export All Alerts
Dashboard	(I)				
Devices Map (75)	윪	Important A	lerts (26) 🖪 🛩 🛍	Pinned Ale	rts (0)
Device Inventory	=	POLICY VIOLATION	New Activity Detected - Unauthorized RPC Message Type   6 minutes ago RPC host sent a RPC Message Type previously not seen. Source: 10.100.1.7, Destination: 192.168.0.2		No Alerts
Alerts (113)	۰	POLICY VIOLATION	New Activity Detected - Unauthorized RPC Procedure Invocation   6 minutes ago RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Interface: 6BFF		
Reports		POLICY	New Activity Detected - Unauthorized RPC Message Type   6 minutes ago RPC host sent a RPC Message Type previously not seen. Source: 192.168.0.20, Destination: 10.100.1		
ANALYSIS	Â	POLICY VIOLATION	New Activity Detected - Unauthorized RPC Message Type   6 minutes ago RPC host sent a RPC Message Type previously not seen. Source: 10.100.1.7, Destination: 192.168.0.2.		
Data Mining		POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation   6 minutes ago RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Interface: 4832		
Investigation	¢	POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation   6 minutes ago RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Interface: 4832		
Risk Assessment	<b>A</b>	POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation   6 minutes ago RPC client sent procedure invocation request. Client: 10.100.20, Server: 10.100.1.7, Interface: 48324	Recent Ale	rts (26) 🖺 🛷 🛍
Attack Vectors	ø	POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation   6 minutes ago RPC client sent procedure Invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Interface: 4832	POLICY	New Activity Detected - Unauthorized RPC Message Type Apr 14 14:17 RPC host sent a RPC Message Type previously not seen. Source: 10.100.1.7, Destination
Custom Alerts	.*	POLICY	New Activity Detected - Unauthorized RPC Message Type   6 minutes ago RPC host sent a RPC Message Type previously not seen. Source: 10.100.0.20. Destination: 10.100.1.7.	POLICY VIOLATION	New Activity Detected - Unauthorized RPC Procedure Invocation RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Apr 14 14:17
Users	*	POLICY	New Activity Detected - Unauthorized RPC Message Type   6 minutes ago BPC host sent a RPC Message Type provide not seen. Source: 10:100.1.7 Destination: 10:100.0.20	POLICY VIOLATION	New Activity Detected - Unauthorized RPC Message Type Apr 14 14:17 RPC host sent a RPC Message Type previously not seen. Source: 192.168.0.20, Destination
Forwarding	0	POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation of minutes ago PPC-client and reproduce Invocation request. Client: 10.100.0.20. Server: 10.100.1.7. Interform GPE	POLICY	New Activity Detected - Unauthorized RPC Message Type Apr 14 14:17 RPC host sent a RPC Message Type previously not seen. Source: 10.100.1.7, Destination
System Settings	<b>₽</b> ◆	POLICY	New Activity Detected - Unauthorized RPC Message Type 16 flooring memory of 100 17	POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, P
SUPPORT	-	POLICY	New Activity Detected - Unatherized RPC Message Type   6 minutes ago	POLICY	New Activity Detected - Unauthorized RPC Procedure Invocation RPC client sent procedure invocation reguest. Client: 192.168.0.20, Server: 10.100.1.7, Apr 14 14:17
Horizon	<u>-``</u>	FIGLATION	nru nosi seni a nru message i ype previously not seeñ. Source: 10.100.1.7, Destination: 10.100.0.20,		
Azure Defender for Version 10.0.3	юT	Ŧ			

Figure D-53 Azure Defender for IoT Alert Details Showing RPC Connection Between the DMZ and the Testbed LAN

Microsoft	÷	Alerts		e
		10.100.1.7		自由主臣王× Main View - 各Export All Alerta
			New Activity Detected - Unauthorized RPC Proce	edure Invocation
		Important Alerts (	RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100 01D3-1278-5A478F6EE188, Function: 21.	0.1.7, Interface: 48324FC8-1670-
		POLICY New		No Alerts
		VIOLATION BPC :	$\Box  \longleftrightarrow  \Box$	
		VIOLATION RPC #	POLARIS GREEN	TEC-
		POLICY New VIOLATION IRPC	SERV	En
		POLICY New	Remediation Steps	
		VIOLATION REC.	<ul> <li>This alert represents a deviation from a learned network policy.</li> </ul>	
		VIOLATION RPC 4	If this activity is valid, learn it.	
		POLICY New VIOLATION RPC.	<ul> <li>If this is an invalid communication, consult a relevant Control Systems Er alert.</li> </ul>	ngineer to validate the origin of this
		POLICY New VIOLATION RPC		thorized RPC Message Type Apr 34 14:17
		POLICY New		thorized RPC Procedure Invocation
		VIOLATION RPC client and	it procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Intertaine: 40.82	VIOLATION BPC class and procedure insocation request. Client; 192,168.8.20, Server: 10.100.1.1
		VIOLATION HPC heat sent :	y Detected - Unauthorized RPC Message Type   6 minutes ago a RPC Message Type pervised not seen. Source: 10.100.0.30, Desferation: 10.100.1.7	POLICY New Activity Detected - Unauthorized RPC Message Type Apr 14 14:17 VIOLATION BPC loss sent a RPC Message Type previously not seen. Source: 192.168.0.20, Desministry
		POLICY New Activity VIOLATION RPC Institution	y Detected - Unauthorized RPC Message Type   6 minutes ago a BPC Message Type pervised rint axes. Secret: 10 100.1.7, Destination: 16.100.0.20	POLICY New Activity Detected - Unauthorized RPC Message Type Apr 14 14:17
		POLICY New Activity	y Detected - Unauthorized RPC Procedure Invocation   6 minutes ago	POLICY New Activity Detected - Unauthorized RPC Procedure Invocation
		POLATION RPC ment ser	r procedure investigation request. Cleart: 10.100.0.20, Server: 10.100.1.7, Interface: MIFF	VIOLATION RPC class and procedure invocation report. Clinit: 192.168.6.29, Berver: 10.100.1.7
		VIOLATION RPC hast sent o	a RPC Meanage Type previously not neek. Source: 10.100.0.20, Destruction: 10.100.1.7,	VIOLATION BPC class sent procedure invocation reguest. Client: 192:168.0.20, Server: 10.100.1.7 Apr 14.14:17

#### 📑 Microsoft Event Timeline Θ anced Filters... All Events - 2. User Operation ns 🔄 Select Date O Create Event E Expor Apr 14, 2021 ces Map (75) 옮 File Transfer Detected Q = 14:17:19 ۵ Apr 14, 2021 2:17:19 PM File transfer from client IP: 192.168.0.20, Se Protocol: SMB, File Name: Applications\putt s\putty-64bit-0.74-in: Ê Apr 14, 2021 2:17:19 PM File transfer from client IP: 10.100.0.20, Server IP: 10.100.1.7 Protocol: SMB, File Name: Applications\putty-64bit-0.74-insta Alert Detected 4 Apr 14, 2021 2:17:14 Hm RPC client sent procedure invocation reques 192.168.0.20, Server: 10.100.1.7, Interface: 1670-01D3-1278-5A47BF6EE188, Function: ▲ 14:17:14 Ø lert Detected API 19, 2021 217,19 PM RPC client sent procedure invocation request. Client: 10.100.0.20, Server: 10.100.1.7, Interface: 4B324FC8 1670-01D3-1278-5A47BF6EE188, Function: 16. 14:17:14 \$ PCAP file Alert Detected RPC client sent proced RPC client sent procedure invocation request. Client: 192.168.0.20, Server: 10.100.1.7, Interface: 4B324FC8-1670-01D3-1278-5A47BF6EE188, Function: 15. 14:17:14 0 PCAP file

#### Figure D-54 Azure Defender for IoT Event Alert Timeline Showing the File Transfer

## **D.5** Executing Scenario 5: Protect from Unauthorized Addition of a Device

An authorized individual with physical access connects an unauthorized device on the manufacturing network and then uses it to connect to devices and scan the network. The expected result is behavioral anomaly detection identifies the unauthorized device.

## D.5.1 Build 1

#### D.5.1.1 Configuration

- Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## D.5.1.2 Test Results

Tenable.ot detects and alerts on addition of a device to the environment. <u>Figure D-55</u> shows an event reported by Tenable.ot when a device was connected to the wireless access point in the manufacturing environment. Tenable.ot also detects other activity from the device, as shown in <u>Figure D-56</u>, where the new device tries to establish a secure shell (SSH) connection to the network switch.

#### Figure D-55 Tenable.ot Event Showing a New Asset has Been Discovered

Powered by Indegy					03:	07 PM • Friday, Jan 29, 2	2021 NCCOE U
Events     All Events	All Events 172.1	6.1.30	2			Actions ~ Resolve A	ll Export
Configuration Events	LOGID	TIME 🕹	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS
SCADA Events	9069	02:42:23 PM · Jan 29, 2021	New asset discov	Low	New Asset Discovered	Endpoint #61	172.16.1.30
Network Events							
Policies							
Inventory							
Controllers	4						
Network Assets	Items: 1-1 out of 1					K <	Page 1 of 1 >
Risk	Event 9069 02:42:2	3 PM · Jan 29, 2021 New as	set discovered Low	Not resolve	d		
Network	Details	A new accet has been	detected in the poten	ork by Topoblo	ot		
Network Summary	Affected Assets	A new asset has been	detected in the netwo	ork by renable	.01		
Packet Captures	Policy	SOURCE NAME Endpoi	<u>nt #61</u>		Why is this	Suggested	
Conversations	Status	SOURCE ADDRESS 172.16.	1.30		important?	Mitigation	
Assets Map		DESTINATION			It is important to know what	Make sure that t	he asset is
Groups		NAME			assets exist in your network New assets can indicate	. expected to be a is familiar to you	t this IP and or to other
Reports		DESTINATION			unexpected network	asset owners. If y familiar with the	you are not
					connections, third party		

#### Figure D-56 Tenable.ot Event Showing Unauthorized SSH Activities

<b>tenable.ot</b>					03	:07 PM • Friday, Jan 29	9, 2021 NCCOE Use
Events						_	
All Events	All Events 172.1	6.1.30	2			Actions ~ Resolve	All Export O
Configuration Events	LOGID		EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS
SCADA Events	0060	02:42:22 DM Jap 20, 2021	New accet discou	Low	New Accet Discovered	Endpoint #61	172 16 1 20
Network Threats	9009	02.42.23 PM Jan 29, 2021	New asset discov	LOW	New Asset Discovered	Endpoint #01	172.10.1.50
Network Events							
Policies							
Inventory							
Controllers	4						*
Network Assets	Items: 1-1 out of 1					K	<pre> Page 1 of 1 &gt; &gt;</pre>
Risk	Event 9069 02:42:2	3 PM · Jan 29, 2021 New as	set discovered Low	Not resolved	ł		
Network	Details	A new asset has been	detected in the netwo	ork by Tenable	to		
Network Summary	Affected Assets	A new assertias been	detected in the netwo	ork by renable			
Packet Captures	Policy	SOURCE NAME Endpoi	<u>nt #61</u>		Why is this	Suggested	
Conversations	Status	SOURCE ADDRESS 172.16	1.30		important?	Mitigation	
Assets Map		DESTINATION			It is important to know what	at Make sure tha	t the asset is
Groups		NAME			assets exist in your networ New assets can indicate	k. expected to be is familiar to y	e at this IP and ou or to other
Reports		DESTINATION			unexpected network connections, third party	asset owners. familiar with t	If you are not he asset,
• • • • • • • • • • • • • • • • • • •		ADDRESS			connectivity or potential	contact the re	levant n to check if
Investors 2.0.17   Evolution Day 0. 2021					threats to the network.	network aum	IT LO CHECK II

## D.5.2 Build 2

#### D.5.2.1 Configuration

- Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

#### D.5.2.2 Test Results

Forescout detects when an unauthorized device connects to a wireless access point in the manufacturing environment. Figure D-57 shows that Forescout raises an alert on the DNS request from the wireless access point to the gateway. The device establishes an SSH connection, which is detected by Forescout as shown in Figure D-58. A more detailed view of the alert is shown in Figure D-59.

Figure D-57 Forescout Alert on the DNS Request from the New Device

<) FORES	COUT. 🚳 Dashboard	🔥 Network 🔳 Even	ts 🔊 Sensors 📽 Settings		🖵 📌 🜻 admir
lert details	Back Edit	Delete Trim Show	× Assign to case Download   ×		<li>Help</li>
Summary		Source host	info ^	Alert Details	^
Alert ID	169436	IP address	172.16.2.30 (Private IP)	ID and name	lan_cp_cnw_c - Communication pattern not whitelisted
Timestamp Sensor name	Oct 13, 2020 13:33:55 sensor-bundle-nccoe	Host name Host MAC	stochastic 00:09:58:AA:E9:29 (Netgear) Jant searc Orr 13, 2020 13-22-38	Description	Communication pattern not whitelisted: the source and destination hasts are whitelisted in
Detection engine Profile	Communication patterns (LAN CP) 9 - UDP communications	Other observe MAC addresse	d E4:90:69:38:C2:C3 (Rockwell) s E4:90:69:38:C2:C0 (Rockwell)	Trinsmins	some communication rule, but not with this combination
Severity	Medium	Role	SNMP manager	rule/default	alert
Source MAC Destination MAC	00:09:58:A4:E9:29 (Netgear) E4:90:69:38:C2:C2 (Rockwell)	Other roles	Windows workstation, Web server, Terminal client	accom	
Source IP	0 172.16.2.30 (stochastic)		DNS (UDP 53)		
Destination IP	• 172.16.2.1 (stratix8300.mgmt.lab)		7004, 7005, 7006, 7007, 7008, 7009, 52311)		
Destination port	53 53	Client protocol	NotAKnowmOne (UDP 443, 19000) 8 RDP (TCP 3389) SMB (TCP 445)		
rey / Blart datalis					Conversion (C) 2009-2020 Encanceut lo 4.3

Figure D-58 Forescout alert showing the SSH connection



Figure D-59 Detailed Forescout alert of the Unauthorized SSH Connection

Alert details	Back Edit	Delete Tr	im Show   ~	Assign to case Download   🛩		9 Help
Summary		^	Source host info	^	Alert Details	^
Alert ID 1	69373		IP address	172.16.2.30 (Private IP)	ID and name	lan_cp_cnw_c - Communication pattern not
Timestamp 0	Det 13, 2020 13:24:58		Host name	stochastic		whitelisted
Sensor name se	sensor-bundle-nccoe		Host MAC	00:09:58:AA:E9:29 (Netgear)		Communication pattern not whitelisted: the
Detection engine C	Communication patterns (LAN CP)		addresses	Last seen: Oct 13, 2020 13:24:58	Description	some communication rule, but not with this
Profile 8	- TCP communications		Other observed	E4:90:69:3B:C2:C3 (Rockwell)		combination
Severity	Medium		MAC addresses	E4:90:69:38:C2:C0 (Rockwell)	Triggering	
Saura MAC D	0.00.5P.44.50.20 (Nerrows)		Role	SNMP manager	rule/default action	alert
Source MAL 0	NONSERVICES (Neigear)		Other roles	Windows workstation, Web server, Terminal		
Destination MAC F	F4:54:33:2F:E1:C1 (Rockwell)			dient		
Source IP	172.16.2.30 (stochastic)			DNS (UDP 53) ExiledConnection (TCP 80, 7000, 7001, 7002		
Destination IP	172.16.2.2 (operations.lan.lab)			7004, 7005, 7006, 7007, 7008, 7009, 52311)		
Source port 5	55262			LDAP (UDP 389)		
Destination port 2	22		Client protocols	NotAKnownOne (UDP 443, 19000) RDP (TCP 3389)		
12 proto F	Ethernet			3MD (17% 443)		Conversions (2) 1000-1010 Encourant In (3 1 1)

## D.5.3 Build 3

#### D.5.3.1 Configuration

- Behavior Anomaly Detection: Dragos
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

#### D.5.3.2 Test Results

Dragos detected the traffic generated by the new asset and generated several alerts as seen in the list of alerts in <u>Figure D-60</u>. Details of different aspects of the network scanning can be seen in <u>Figure D-61</u> and <u>Figure D-62</u>. Details on the new device can also be seen in <u>Figure D-63</u>.

Figure D-60 Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network Scanning

			ASSET NOTIFICATIO	DNS			SYSTEM ALERTS			RULES		
₹ FILTERING	• 💼 Pro	m 17/21, 19:00	UTC 🗖 10	7/21, 21:00 UTC	C REFRESH						Q treath 0.205	
View	Sever :	ID ÷	Occurred At 3		Туре	a Summary	Message	Detected By	2 Asset IDs	Source IPv4	C Dest. IPv4	÷ Other
VIEW		148691	02/17/21, 20:59 UTC	Asset		NewSourceEth Detected	Asset 2789 seen as the ethemet source for the first L.	New Source Ethernet Address Detection	2709			192.168.0
VIEW		148675	02/17/21, 20:56 UTC	Communication		NewDestEth Detected	Asset 2789 seen as the Ethernet destination for the	New Destination Ethernet Address Detection	2789			192.168.0
VIEW		148674	02/17/21, 20:59 UTC	Communication		Detected 6 NewCommunication between 2021-02-1.	Sample NewCommunication values include: ip.src	New Communication Pairing	2791, 102,	. 10.100.0.101	10.100.0.101	
VIEW	10	148583	02/17/21, 19:48 UTC	Communication		NewCommunication Detected	Asset 102 (10.100.0.101) communicated with Asset	New Communication Pairing	102, 85	192.168.0.205	10.100.1.4	
VIEW		148582	02/17/21, 19:50 UTC	Asset		ICMP Scan Detected	ICMP scan observed from asset 85. 10.100.1.4 swe	ICMP Sweep	85			10.100.1.4

#### Figure D-61 Details of Network Scanning Activity

DETECTION INFORMATION		ASSOCIATED ASSETS				
International and the second form same distribution of the second form same distribution of the second form same distribution of the second form (second for the second form (second for the second for the seco	Lation from (b) the dot int trapport) is too top it inputs in 2016, Addresses were incrementing 1570 trees and Sing the bias were in (1570). The impact and of ordinaus addresses was 240 too 24. Addresses that addresses and the bias and the bias an	View 2 Type 2 0 2 VOW White All the Windows See 85 Asset 85 COMMUNICATIONS SUMMARY No Com	Name	2 Di- 10.100.1.4 oth		
1         10.01.21,21.21.21.21.21.21.21.21.21.21.21.21.21.2						
62/17/21, 1959 UTC COUNT: I DETECTED BY:	eren Trace Book ource STATE: UNEFECUATO SOURCE:					
DETECTION QUAD: Threat Behavior	ZONES: DM2					
ACTIVITY GROUP: Common	ICS CYBER KILLCHAIN STEP; Stage 1 - Reconstissance					
MITRE ATT&CK FOR ICS TACTIC	MITRE ATTACK FOR ICS TECHNIQUE TUBH4: Remote Bystern Discovery 2					
QUERY-FOCUSED DATASETS: Scanning	NOTIFICATION RECORD: View in Kibana					
PLAYBOOKS: Network Address Stanning Activity Detected	NOTIFICATION COMPONENTS: View in Kibara					
CASES:						

Figure D-62 Additional Details of Network Scanning Activity

DETECTION INFORMATION		ASSOCIATED ASSETS	
F FILTER Asset 2789 seen as the ethernet source for the first time		View         ⊂         Type         ⊂         ID         ⊂         Name           VIEW         mme         2789         Asset2729         Asset2729 <th>= Di</th>	= Di
OCCUBRED AT: 02/17/21, 20.59 UTC COUNT:	LAST SEEN: 01017/0.00.00 UTC STATE:	COMMUNICATIONS SUMMARY	
I     DETECTED BY:     Nem Source Date: Detection     DetEction Quad:     Configuration	UNREFECT/FD SOURCE Obstazial STice: 4509 w200 wffc16119587# ZONES: CRS - Lower T	No Communications Summary.	
ACTIVITY GROUP: None MITER AT SEK TACTIC: None	ICS CYBER KILLCHAIN STEP: None Minte ATTACK TECHNIQUE: None		
QUERY-FOCUSED DATASETS: Zone Communications PLAYBOOKS: New Source Ethernet on IP Address Detected	NOTIFICATION RECORD: View in Koans NOTIFICATION COMPONENTS: View in Koans		
CASES: No Classes Lablest			
ID COCUTED AT COCUTED		Summary	
		No Rotes Natificators	

#### Figure D-63 Alert for New Asset on the Network

2 192,168.0.203

## D.5.4 Build 4

## D.5.4.1 Configuration

- Behavior Anomaly Detection: Azure Defender for IoT
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

## D.5.4.2 Test Results

A "New Asset Detected" alert is shown on Azure Defender for IoT dashboard (Figure D-64) and on the Alert screen (Figure D-65). Figure D-66 shows the alert management options in Azure Defender for IoT. The details of the network scanning alert are shown in Figure D-67.



Figure D-64 Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset

Figure D-65 Azure Defender for IoT Detects New Asset in the Environment

Hicrosoft	÷	Alerts	0
		192.168.0.205 Q  Advanced Filters Security Operational	Main View -   B Export All Alerts
Dashboard	(°)		
Asset Map (96)	쁆	Important Alerts (2)	Pinned Alerts (0)
Asset Inventory		POLICY Unauthorized Internet Connectivity Detected   just now VIOLATION An asset defined in your internal network is communicating with addresses on the Internet. These addresses have not been	arne No Alerts
Alerts (63)		POLICY New Asset Detected   just now VIOLATION A new asset was detected on the network. Asset 192,168.0.205 was added to your network. Verify that this is a valid network	aset
Reports			
Event Timeline	Ê		
Data Mining	۶.		
Investigation	¢		
Risk Assessment	▲		Recent Alerts (2)
Attack Vectors			POLICY Unauthorized Internet Connectivity Detected Jan 6 14 36
			VIOLATION An asset defined in your internal network is communicating with addresses on the Internet. These addresses have an approximately the set of the
Custom Alerts			Jan 6 14:36 VIOLATION A new asset was detected on the network. Asset 192.168.0.205 was added to your network. Verify that this is a value
Users			
Forwarding			
System Settings	٠		
Import Settings	£		
Horizon	<u>:0</u> :		
Support	۲		
Azure Defender for I Version 3.1.1	loT		

Figure D-66 Azure Defender for IoT Alert Management Options

ID: 232	Ê	6	<b>⊥</b>	×	Ŧ	×
New Asset Detected Policy Violation   Jan 6, 2021 2:36:03 PM ( 2 minutes ago ) A new asset was detected on the network. Asset 192.168.0.205 was added to your network	ς.					
Verify that this is a valid network asset.						
192.168.0.205						
Manage this Event						
<ul> <li>Approve this asset as a valid network device.</li> </ul>						
• Select Acknowledge to save the alert. Another alert will trigger if the event is dete	cted agai	n.				
<ul> <li>Disconnect the asset from the network. Select Delete Asset. This asset will not be unless it is detected again.</li> </ul>	e analyzed	l by th	e ser	nsor		
Delete Asset	Аррге	ove	A	cknow	/ledg	9

#### Figure D-67 Details for Network Scanning Alert

	Device Connection Detected Jan 6, 2021 2:36:03 PM	6
Grouped	d Events	<b>A</b>
Jan 6, 2021 Connecte	1 2:36:03 PM ed devices 192.168.1.103 and 192.168.0.205	
Jan 6, 2021 Connecte	1 2:36:03 PM ed devices 192.168.0.205 and 192.168.1.101	
Jan 6, 2021 Connecte	1 2:36:03 PM ad devices 192 168 0 205 and 10 100 0 17	•
	^	
Assets		<b></b>
Туре	Name	
	Station 2	
	LAN-AD	
	Station 4	
	Station 3	
	Station 1	
	CRS Supervisory LAN Gateway	
	192.168.0.205	•
		Info

# D.6 Executing Scenario 6: Detect Unauthorized Device-to-Device Communications

An authorized device that is installed on the network attempts to establish an unapproved connection that is not recorded in the baseline. The expected result is the behavioral anomaly detection products alert on the non-baseline network traffic.

## D.6.1 Build 1

#### D.6.1.1 Configuration

- Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

#### D.6.1.2 Test Results

The unapproved SSH traffic is detected by Tenable.ot as shown in Figure D-68.

Figure D-68 Tenable.ot Event Log Showing the Unapproved SSH Traffic

tenable.ot					03	:30 PM • Friday, Jan 29, 2	021 NCCOE US	
Events								
All Events	All Events ssh	0	2			Actions 🗸 Resolve A	Export	
Configuration Events	LOG ID T	іме 🗸	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	
SCADA Events	9097 0	2:22:51 DM - Jan 29:2021	Linauthorized Co	Madium	SSH Communications	PCS Eng Station	172 16 3 10	
Network Threats	9093 0	12:20:44 PM - Jan 29, 2021	Unauthorized Co		SSH Communications	PCS Eng. Station	172 16 2 10	
Network Events	9093 0	5.20.44 PM - Jan 29, 2021	chaddionzed co	Medium	SSH commonications	EC3 ED8: 344000	172.10.5.10	
Policies	Items: 1-10 out of 10					к <	Page 1 of 1 >	
Inventory	Event 9093 03:20:44 Pt	M - Jan 29 2021 Unauth	orized Conversation	Medium N	lot resolved			
Controllers					unter d			
Network Assets	Details	A conversation in an u	nauthorized protocol	has been det	ected			
Risk	Source	SOURCE NAME PCS EDS	. Station		Why is this	Suggested		
Network	Destination	SOURCE ADDRESS 172.16.	3.10		important?	Mitigation		
Network Summary	Policy				Conversations in	Check if this some unication		
Packet Captures	Status	NAME	TION Stratix5700 VLAN1	unauthorized protocols ma	y is expected. If it is expected			
Conversations					Some assets are not	Policy conditions	so that	
Assets Map		ADDRESS	1.3		non-standard protocols an	n Events aren't ger d similar communi	cations in	
Groups		CC11 (Arr	- (22)		any deviation from the standard protocols may	the future. If this communication i	s not	
Reports		PROTOCOL SSH (tc)	1/22)		suggest a potential threat. In addition, some protocol	expected, check asset to determi	the source he whether	
.0 1 1 C-++		PORT 22			are unsecure and should not be used at all, in order	the source asset	itself has ed. If this	

## D.6.2 Build 2

#### D.6.2.1 Configuration

- Behavior Anomaly Detection: eyelnspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## D.6.2.2 Test Results

SSH communication from HMI computer to the network switch is not defined in the baseline; Forescout flags this communication as shown in Figure D-69.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-10

Figure D-69 Forescout Alert Showing the Unapproved SSH Traffic

FURESCU		events en sensors Ve se	itings			
rt details	Back Edit Delete Tron S	how   - Assign to case - E	lowriodd   -			<b>9</b> Hel
Summary		Source host info		^	Alert Details	^
Vert ID	139850	IP address	172.16.1.4 (Private IP)		ID and name	lan, cp.,cmx,c - Communication pattern not whitelisted
limestamp	Oct 7, 2020 12:06:19	Host name	fgs-61238hh			Communication pattern not whitelisted: the source and
Sensor name	sensor bundle nccoe	Other host names	fgs-61338hh.lan.lab		Description	destination hosts are whitefated in some communication rule, but not out this combination
Detection engine	Communication patterns (LAN CP)	March 1997, addresses	0C:C4:7A:31:44:47 (SuperMic)		Total and the solution of the solution of the	
Profile	8 - TCP communications	COURSE BOOK BOARTESSES	Laur seeve Get 7, 2020 12/18/07		action	alert
Sevenity	Medium		E4-90-69-30-C2-C3 (Reckwell)			
Source MAC	0C-C4-7A-31-44-47 (SuperMit)	Other observed MAC	E4:90:69:38:C2:C0 (Rockwell)			
Destination MAC	F454:33:2F59:C1 (Rockwell)		7C-0E-CE-67-85-88 (Cisco) 2C-0E-CE-67-85-88 (Cisco)			
Source IP	0 172.16.1.4 (fgs-61330th)	Refer	Territorial second			
Destination IP	9 172.16.1.3 (plant)	Other sales	Windows undersation			
Source port	58540	Vander and model	Entral			
Destination port	22	OS version	Windows 7 or Windows Server 2008 82			
L2 proto	Ethernet		DCOM/TCR 135, J0155, J0156			
.3 proto	2		DAS (TCP 53)			
4 proto	TCP		DNS (UDP 53, 5355) FaledConnection (TCP 23, 80, 139)			
7 proto	55H		HTTP (TCP 0530)			
TCP stream opened in hot start mode	false		Kerberos (TCP BE) LDAP (TCP 389) LDAP (UDP 389)			
itatus.	hist analyzed	Ciary protocols	NTP (UDP 123) North(05 (UDP 137)			
Labels			NoData (TCP 50005)			
User notes Monitored networks			Nex4AnsemDex (DP 1332, 2303, 2301, 10020) Nex4AnsemDex (DB 1514) SMB (DP 130) SDP (DD 1400) SDP (DD 1400) SDP (DP 440, 1000) SDF (TO 22) SM (TO 440, 1000) SM (DP 440, 1000)			

## D.6.3 Build 3

## D.6.3.1 Configuration

- Behavior Anomaly Detection: Dragos
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

## D.6.3.2 Test Results

Dragos detected the non-baseline SSH traffic as shown in Figure D-70.

#### Figure D-70 Dragos Alert Showing the Unapproved SSH Connection Between Devices

	DETECTION INFORMATION		10000	ATED ACCETS						
_	WHAT HAPPENED:		View	: Type	: ID :		Nam	e .	: 1	Dir. :
	New Communication from host 192.168.1.104 to host 192.168.1.1	01 over SSH on port [22] for the first time.	VIE	Controller	3177 Asse	3177			192.168.1.104	arc
Af Status	OCCURRED AT:	LAST SEEN:	VIE	Controller	3186 Asse	3186			192.168.1.101	dst
	COUNT:	STATE:	COMM	INICATIONS SUM	IMARY					
	DETECTED BY:	SOURCE:								
	New Communication Planing	4/b5e530 5568 4c32 a2et ctt1 59ta5865	( <u>)</u>							
	DETECTION QUAD: No Applicable Detection Quad	ZONES: CRS - Level 0	0		đ	SSH				
	ACTIVITY GROUP:	ICS CYBER KILLCHAIN STEP:	ě		Texas	Instriments	Тежаз	Instriments		
	No Applicable Activity Group	MITRE ATT&CK TACTIC:			80.D51 192	CCF4/26:EC 168 1.104 to local	B0:D5 192 machitin	CC:FA:70:C9 168.1.101 p-station-1.local		
	MITRE ATT&CK TECHNIQUE:				machining	-station-4.local		icp.local		
	No Applicable MITRE ATT&CK Technique		Protocol	Client	<ul> <li>Ephemeral Po 26735</li> </ul>	102 168 1 101	C Server Por	2.6 KR	C RX Bytes	-
	QUERY-FOCUSED DATASETS: No Applicable Overy-Focused Datasets	NOTIFICATION RECORD: View in Kibana	SSH	80.05.CC.F4.26.EC	46736	80.05.00.FA 70.09	22	2.6 KB	1.8 KB	
	PLAYBOOKS:	NOTIFICATION COMPONENTS:	AKP	82.05-CC #4.26 HC		HD:05.CC.94.70:09		oo.o bytes	0 bytes	
	CASES:	arest in robatio	ARP	BRDS/CC/FA/70/C9		80/05/CC/F4/26/EC		0 bytes	60.0 bytes	
	No Cases Linked									
	ID CONTRACTIONS			Summary						-
			No Related Notifications							
										ľ

## D.6.4 Build 4

## D.6.4.1 Configuration

- Behavior Anomaly Detection: Azure Defender for IoT
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

## D.6.4.2 Test Results

A device attempts to establish a remote access connection via SSH. Azure Defender for IoT was able to detect this activity as shown in Figure D-71.



#### FigureD-71 Azure Defender for IoT Event Identified the Unauthorized SSH Connection

## D.7 Executing Scenario 7: Protect from Unauthorized Deletion of Files

An authorized user attempts to delete files on an engineering workstation and a shared network drive within the manufacturing system. The expected result is the file integrity checking tools in the environment alert on the deletion or prevent deletion entirely.

## D.7.1 Build 1

#### D.7.1.1 Configuration

- File Integrity Checking: Carbon Black
  - Agent installed on workstations and configured to communicate to the Carbon Black Server.
- File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

#### D.7.1.2 Test Results

Carbon Black reports file deleting activities as shown in Figure D-72. GreenTec protects the files on its drive from being deleted.

Figure D-72 Event Messages from Carbon Black Showing File Deletion Attempts

Timestamp 👻	Se	Туре	Subtype	Source	Description	IP Address	User	Process Nar
Feb 3 2021 01:35:55 PM	Info	Policy Enforcement	Report write (Custom Rule)	LAN\FGS-47631EHH	'c:\users\administrator\downloads\ra\nccoe_test_file.txt' was deleted by 'FGS- 47631EHH\Administrator'.	172.16.3.10	FGS-47631EHH\Admini	explorer.exe
Feb 3 2021 01:35:50 PM	Info	Policy Enforcement	Report write (Custom Rule)	LAN\FGS-47631EHH	'c:\users\administrator\downloads\ra\testscenarios\nccoe_test_file.txt' was deleted by 'FGS-47631EHH\Administrator'.	172.16.3.10	FGS-47631EHH\Admini	explorer.exe
Feb 3 2021 01:35:35 PM	Info	Policy Enforcement	Report write (Custom Rule)	LAN\FGS-47631EHH	'c:\users\administrator\documents\tesim\nccoe_test_file.txt' was deleted by 'FGS-47631EHH\Administrator'.	172.16.3.10	FGS-47631EHH\Admini	explorer.exe

## D.7.2 Build 2

#### D.7.2.1 Configuration

- File Integrity Checking: Security Onion
  - The agent is installed on workstations and configured to communicate to the Security Onion Server.
- File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

#### D.7.2.2 Test Results

Security Onion Wazuh alerts on file deletion as shown in Figure D-73. Files stored on a storage drive protected by GreenTec are protected from deletion.

Figure D-73 Security Onion Wazuh Alert Showing a File Has Been Deleted

0	@timestamp	Q Q 🗉 🛊	October 15th 2020, 13:05:33.753
	@version	Q Q II *	
	_id	Q Q 🗆 🛊	JXY5LXUB1YHtrLLyVhik
	_index	Q Q 🗆 🛊	seconion:logstash-ossec-2020.10.15
	_score	Q Q 🖽 🛊	
	_type	a a 🗆 🛊	doc
	agent.id	a a 🗆 🛊	005
	agent.ip	Q Q 🛛 🛊	A 172.16.3.10
	agent.name	Q Q 🗆 🛊	PCS-EWS
	alert_level	Q Q 🗆 🛊	
	classification	a a 🗆 🛊	"Bad word" matching
	decoder.name	Q Q 🗆 🛊	syscheck_integrity_changed
	description	Q Q 🗆 🛊	File deleted.
	event_type	e e 🗆 🛊	ossec
	full_log	Q Q II *	File 'c:\users\administrator\downloads\ra\testscenarios\test_file.txt' was deleted. (Audit) User: 'Administrator (5-1-5-21-239850103-4004920075-3296975006-500)' (Audit) Process id: '6056' (Audit) Process name: 'C:\Windows\explorer.exe'
	host	Q Q 🗆 🛊	gateway
	id	Q Q 🛙 🛊	1602781532.2062049
	location	Q Q 🛙 🛊	syscheck
	logstash_time	Q Q 🗆 🛊	0.002

## D.7.3 Build 3

#### D.7.3.1 Configuration

- File Integrity Checking: Security Onion
  - Agent installed on workstations and configured to communicate to the Security Onion Server.
- File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

#### D.7.3.2 Test Results

Security Onion Wazuh detected the file deletions as shown in the Security Onion Server log in Figure D-74. Files stored on a storage drive protected by GreenTec are protected from deletion.

Figure D-74 Alert from Security Onion for a File Deletion

8	Dashboard   OSSEC		0	
	JSON			T
	Øtimestamp	Feb 12, 2821 # 18:41:46.583		
	f Oversion			
	1_index	seconion:logstash-ossec-2871.42.12		
	/ _score			
	t_type	_dec		
	<pre>r agent.id</pre>	983		
	<pre>@ agent.ip</pre>	△ 192.168. <b>8</b> .28		
	1 agent.name	CPS-ENS		
	/ alert_level			
	classification	"Bad word" matching		.,
	decoder.name	syscheck_integrity_changed		
	t description	File deleted.		
	event_type			
	full_log	File 's:\users\nccoexuer\documents\twincat projects\crs workell\_boot\twincat co? (arm/?)\plc\port_831.oce' was deleted.		
	1 host	gateway		
		1613144504.13013045		
	t location	ayscheck		
	<pre>// logstash_time</pre>	9.607		
	t manager.name	seconion		
	t message	) ('timestamp':'2021-82-12715:d1:44.709+0000', "nule':('level':y, 'description':'File doleted.', 'id':'0553', 'firediame':d0,'mull':true, 'groups':['dessec', 'syscheck'], 'pci_des':['11.5'], 'gg13':['4.11'], 'gg47':['11.5'], 'gg13':['4.11'], 'gg47':['11.5'], 'gg13':['4.11'], 'gg47':['11.5'], 'gg13':['11.5'], 'g	_5.1. \\twi ode	
	∉ port	36634		
	/ syscheck.event	deleted		
	<pre>syscheck.path</pre>	c:\users\ncceuser\documents\twincat projects\crs workcell\_boot\twincat ce7 (arm/7)\plc\port_851.oce		

## D.7.4 Build 4

## D.7.4.1 Configuration

File Integrity Checking: Carbon Black

- Agent installed on workstations and configured to communicate to the Carbon Black Server.
- File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

#### D.7.4.2 Test Results

The attempts to delete a file are detected by Carbon Black as shown in Figure D-75. Files stored on a storage drive protected by GreenTec are protected from deletion.

Figure D-75 Carbon Black Alerts Showing That a File Has Been Deleted

Timestamp 👻	Severit	Туре	Subtype	Source	Description	IP Address	User	Process Name
Jan 6 2021 02:25:56 PM	Notice	Computer Manage	Agent deleted events	WORKGROUP\eee	Computer 'WORKGROUP\eee93e4e44od-vm' deleted 508 events.	10.100.1.61		
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2_old_v1myp3ji\twinsafegroup1\twinsafegroup1.sal' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2_old_v1myp3ji\untitled2.splcproj' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2_old_v1myp3ji' was deleted by 'eee93e4e44od-vm\guest- user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2\twinsafegroup1\alias devices\term 4 (el2904) - module 1 (fsoes).sds' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2\twinsafegroup1\alias devices' was deleted by	10.100.1.61	eee93e4e44od-vm\auest-user	explorer.exe

## D.8 Executing Scenario 8: Detect Unauthorized Modification of PLC Logic

An authorized user performs an unapproved or unauthorized modification of the PLC logic through the secure remote access tools. The expected result is the behavioral anomaly detection tools will detect and capture the activity, flagging it for review.

The behavior anomaly detection tools can detect program downloads to the PLC. Program download detection needs to be correlated with the maintenance management system to determine if the download was authorized and approved. This was not demonstrated as part of this scenario.

## D.8.1 Build 1

#### D.8.1.1 Configuration

- Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for accessing the PCS environment

## D.8.1.2 Test Results

In this build, a remote session Studio 5000 Logix Designer is established to perform PLC file operations as shown in Figure D-76 and Figure D-77. Tenable.ot is able to detect the PLC file modifications as shown in Figure D-78 with details shown in Figure D-79 and Figure D-80.

lallankak		
onsole <mark>, vorks</mark> " +53148	Devices	NCCOE_USER E
	Devices C In Filter Devices C > 3 Devices	
	PCLMA Market 1	

Figure D-76 Remote Access to Systems in PCS Network is Established Through ConsoleWorks

Figure D-77 Remote Session into Studio 5000 to Perform PLC File Operations



All Events	Search	Q		Actions V Resolve All Export
LOG ID	TIME 🗸	EVENT TYPE	SEVERITY	POLICY NAME
12416	01:47:47 PM · Feb 4, 2021	Change in Key Sw	High	Change in controller key state
12414	01:46:52 PM · Feb 4, 2021	Rockwell PLC Start	Low	Rockwell PLC Start
12413	01:46:30 PM · Feb 4, 2021	Rockwell Code Do	Medium	Rockwell Code Download
12412	01:46:27 PM · Feb 4, 2021	Rockwell PLC Stop	High	Rockwell PLC Stop
12410	01:45:05 PM · Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session
12409	01:44:38 PM · Feb 4, 2021	RDP Connection (	Medium	RDP Communication to an Engineerin

Figure D-78 Tenable.ot Detected the Transfer of PLC Logic File to the Rockwell PLC

Figure D-79 Tenable.ot PLC Stop alert details

Rockwell F	PLC Stop			STATUS Actions ~
Category Configuration Events				
Details	Items: 1-1 out of 1		K	< Page 1 of 1 > >
Triggered Events	Event 12412 01:46:27 P	M · Feb 4, 2021 Rockwell Pl	LC Stop <mark>High</mark> N	lot resolved
Exclusions	Details	The controller state was cl	hanged to Stop	-
	Source Destination	SOURCE <u>PCS Eng. Station</u> NAME	Why is this	Suggested Mitigation
	Policy Status	SOURCE 172.16.3.10 ADDRESS	important? The system	1) Check whether the
		DESTINATION <u>Plc_tesim</u> NAME	detected a change in the controller	state change was made as part of scheduled
		DESTINATION172.16.2.102	state that was made	maintenance work and
#### Figure D-80 Tenable.ot PLC Program Download Alert Details

K Rockwell C	Code Download			STATUS Actions ~
Category				
Configuration Events				
Details	Items: 1-1 out of 1		K	< Page 1 of 1 > >
Triggered Events	Event 12413 01:46:30 l resolved	PM · Feb 4, 2021 Rockwell Co	ode Download M	<mark>edium</mark> Not
Exclusions	Details	Code was downloaded fro	m an engineering s	station to the controlle
	Code	SOURCEPCS Eng. Station	Why is	Suggested
	Source	NAME	this	Mitigation
	Destination	SOURCE 172.16.3.10	important?	
	Policy	ADDRESS	The system	1) Check whether the
	Status	DESTINATION <u>PIC tesim</u> NAME	detected a change in the controller	change was made as part of scheduled work and
		DESTINATION172.16.2.102	code that was made	whether the source of the 👻

## D.8.2 Build 2

## D.8.2.1 Configuration

- Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured to allow authorized users to access PCS environment through the Dispel Enclave to the Dispel Wicket.

## D.8.2.2 Test Results

As shown in Figure D-81 the authorized user establishes a session into the manufacturing environment using the Dispel VDI. The user connects to the engineering workstation and launches the Studio 5000 Logix Designer as shown in Figure D-82 to modify the PLC logic. Figure D-83, Figure D-84 and Figure D-85 show that Forescout is able to detect the traffic between the engineering workstation and the PLC, including details of the Stop command and Download command.

Figure D-81 Remote Access to Systems in PCS Network is Being Established Through Dispel

•	Remote Desktop Connection				- 🗆 X
Recycle Bin TC3	AddRo Reply from 10 Reply from 10 Reply from 10	ompt .100.1.7: bytes=32 time=184ms TTL=62 .100.1.7: bytes=32 time=182ms TTL=62 100.1.7: bytes=32 time=182ms TTL=62		- • ×	
	Reply from 10 Reply from 10 Ping statisti Packets:	<pre>.100.1.7: bytes=32 time=184ms TTL=62 cs for 10.100.1.7: Sent = 8. Received = 8. Lost = 0 (0% loss).</pre>			
he re fi Google Chrome	Dispel Client Settings Help	Dispel is running Disconnect		x	
n OpenVPN GUI	Available Projects NCCOE-Manufacturing	Available Entry Points Chicago, IL ()	Available Exit Points		
putty TC31-FULL					
GreenTec					
GreenTec_D					
TC3_Remo					

Figure D-82 Modifying the Parameters for the Allen-Bradley PLC Controller Using Studio 5000

Logix Designer - plc_tesim (1756-L7     Ella Edit View Saarch Logis	1 21.11]	Window Halo						
Image: Second	AB_ETHIP-1\172.16.2.102\	lackplane\2"	् ् Setert language	- 1	ð			
Controller Organizer	Program Mode Bun Mode Test Mode Lock Controller	BE & Timer/Counter & F troller Tags - plc_tesim(cor	put/Output 🔏 Compo stroller)	re 🔏 ConputeMisth 🔏 Movel	Logical 🖌 FileMiss	K Fleishit	t 🔏 Sequencer 🔏 Program Cot	terol 🔏 FontBreak 🔏 Special 🔏 Trig Fu
Controller Tags     Controller Fault Handler     Controller Fault Handler	Clear <u>F</u> aults Go To Faults	c ∰ pic_tosim → 1 me	Show: All Tags	Value •	Force Mask	Style	Y. Enter Name Filter.     Data Type	Descrip * Properties
Twis     Twis     Construction     Construction		mmaxiii           mmaxiii		()     (	()	Float Float Float Float Float Float Float Float Float Float Float Float Float Float Float Float	польций) ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL ПКАL	Constant     Constant
	Sec	xmeas[14] xmeas[15] xmeas[16]		25.300936 49.936478 3330.0437		Float Float Float	REAL REAL REAL	TO

Figure D-83 Forescout Alerts Showing It Detected the Traffic Between the Engineering Workstation and the PLC

<) FORESCOUT	-	Dashboard	Network 🔲 Eve	nts 🎝	Sensors	OS Setti	ngs				-	**	admin
													<li>Help</li>
Excluding event type ID		Timestamp *	Event name(s)	Sensor	Engine	Profile	Status	Severity	Source address	Destination	Dest. Port	L7 Proto	Case ID
By monitored network											-		
Excluding profile			0	(Nut	0.4	(Not br .	(Not set) .	ine	172.16.3.10	172.16.2.112	0	(Not set) .	(Unasi
Excluding src MAC		Oct 13, 2020	(FEA Exit) Message t	senso	Co	8-TCP c	Not analy		172.16.3.10 (fg	172.16.2.102 [	44818	ETHIP	
Excluding dst MAC		134752						м			(TCP)		
Excluding src IP		Oct 13, 2020 13:47:52	(FEA Exit) Message t	senso	Co	8 - TCP c	Not analy	M	172.16.3.10 (fg-	172.16.2.102 (	44818 (TCP)	ETHIP	
Excluding dist IP						0.000							
Excluding dst port	ц.	Det 13, 2020 13:47:52	(PEA Exit) Message L	senso	Co	8+1CP c	Not analy	м	172.16.3.10 (tg	172.16.2.102 (	(TCP)	FIHIN	
By L2 protocol		Oct 13, 2020	(FEA Exit) Message L.	senso	Co	8 - TCP c	Not analy		172, 16, 3, 10 (fg.,	172.16.2.102 (	44818	ETHIP	
By L3 protocol		13:47:52						м			(TCP)		
By L4 protocol		Oct 13, 2020	(FEA Exit) Message t	senso	Co	8 - TCP c	Not analy		172.16.3.10 (fg	172.16.2.102 (	44818	ETHIP	
By upstream data		13:47:52						м			(TCP)		
<ul> <li>By downstream data</li> </ul>		Oct 13, 2020	ETHIP controller star	senso	Indu_		Not analyz	1000 L	172.16.3.10 (fg	172.16.2.102 (	44818	ETHIP	
By FEA type		13:46:49									(109)		
<ul> <li>By field path</li> </ul>		Oct 13, 2020 13:46:49	Message type not w	senso	Co	8 - TCP c	Not analy	M	172.16.3.10 (fg	172.16.2.102 (	44818 (TCP)	ETHIP	
By labels		0			~				171 10 1 10 10	-			
-		544 13, 2020	meanage type not will	20100-0		e-icre-	read allong		the target of the	**************************************	11010		

Figure D-84 Forescout Alert Details for the Stop Command Issued to the PLC

FORESC	COUT. 🙆 Dashboard 🚠 Network	Events 🔊 Se	nsors 😋 Settings	🖵 🏓 🏓	admin
rt details	Back Edit Delete Show	r   ~ Assign to case	: Download   ~		Help
ammary		Source bast info		Alast dataile	
urning		Jource noac mo		Alter Concession	
Jert ID	169537	IP address	172.16.3.10 (Private IP)	Command: Stop controller	
imestamp	Oct 13, 2020 13:46:10	Host name	fgs-47631ehh	User name: FGS-47631EHH\Administrator	
ensor name	sensor-bundle-nccoe	Other host names	fgs-47631ehh.lan.lab		
letection engine	Industrial threat library (ITL)	Host MAC	40:A0:F0:3D:40:AE (HewlettP)		
D and name	It_ops_pdop_ethip_controller_stop - ETHIP controller stop command	autresses	E4:90:69:38:C2:C3 (Rockwell)		
lescription	Potentially dangerous ETHIP operation: the ETHIP master or an operator has requested a PLC to stop. This operation may be part of resular maintenance.	Other observed MAC addresses	84.90:69:38:C2:C2 (Rockwell) 84.90:69:38:C2:C1 (Rockwell) 7C:0E:CE:67:86:83 (Cisco)		
	but can also be used in a Denial of Service attack.	Role	EWS		
everity	High	Other coles	Windows workstation, Terminal server, Terminal		4
ource MAC	40.48 F0.3D.48.48 (HewlettP)	ounce roles	client, Master		
estination MAC	E4:90:69:38:C2:C0 (Rockwell)	Vendor and model	Rockwell		
iource IP	172.16.3.10 (fgs-47631ehh)		DCOM (TCP 135, 49155, 49159)		
lestination IP	172.16.2.102 (plc_tesim)		DNS (UDP 53, 5355)		
ource port	58324		ETHIP (TCP 44818)		
	44818		EIPPP (UDP 44016) FailedConnection (TCP 23 80 139 1332 8000 8443)		

Figure D-85 Forescout Alert Details for the Configuration Download Command

t details	Back Edit Delete Show	~ Assign to case	Download   ~		😧 He
ummary	^	Source host info	^	Alert details	^
lert ID	169543	IP address	172.16.3.10 (Private IP)	Command: Configuration download	-
imestamp	Oct 13, 2020 13:46:20	Host name	fgs-47631ehh	Destination route: Module 2 Uner name: ECC 476215480 Administrator	
ensor name	sensor-bundle-nccoe	Other host names	fgs-47631ehh.lan.lab	Carrier Party Control Control and	
etection engine	Industrial threat library (ITL)	Host MAC	40:A8:F0:30:48:AE (HewlettP)	Downloaded items:	
and name	it_ops_pdop_ethip_download - ETHIP configuration	addresses	Last seen: Oct 13, 2020 12:52:01	Program/MainProgram	
escription	download command Potencially dangerous ETHIP operation: the ETHIP master or an operator has requested a FLC to initiate a configuration download. This operation may be part of regular maintenance but can also be control to the second	Other observed MAC addresses Role	E4305933C2C2(Rockwell) E4305933C2C2(Rockwell) E4305933C2C2(Rockwell) 7C0ECE673683(Cisco) EWS	User Tasis: Task:MainTask IVO Map: Mappin: Mapcontrol_host_elp Mapcontrol_host_elp	
everity	Hill High	Other roles	Windows workstation, Terminal server, Terminal client, Master		
ource MAC	40:A8 F0:3D:43:AE (Hew/ettP)	Vendor and model	Rockwell		
estination MAC	E4:90:69:38:C2:C0 (Rockwell)		DCOM (TCP 135, 49155, 49159)		
ource IP	172.16.3.10 (fgs-47631ehh)		DNS (TCP 53) DNS (UDP 53, 5355)		
estination IP	172.16.2.102 (plc_tesim)		ETHIP (TCP 44815)		
ource port	58324		ETHIP (UDP 44818)		

## D.8.3 Build 3

#### D.8.3.1 Configuration

- Behavior Anomaly Detection: Dragos
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for accessing the CRS environment.

### D.8.3.2 Test Results

In this build, a remote session to the CRS workstation is established to perform PLC file operations as shown in <u>Figure D-86</u> and <u>Figure D-87</u>. Dragos is able to detect the PLC file modifications as shown in Figure D-88 with details shown in <u>Figure D-89</u>.

Figure D-86 VPN Connection to the Manufacturing Environment



Console Works & v 5.3-1u6	Devices	
	Devices	

#### Figure D-87 Remote Access is Being Established through ConsoleWorks

Figure D-88 Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the Beckhoff PLC

				ASSET NOTIFIC	ATIONS		SYSTEM ALTERTS			RUCES		
∓ PUT	ERING T	· 🖬 :	rom 2/11/21,02:4	5 PM UTC To 02/12/	21, 04:45 PM UTC C RELO	Ω.					Q, Search	
	View	Sever :	ID	Cocurred At	Detection Quadrants	: Summary	Message	Detected By	2 Asset IDs	Source IPv4	: Dest. IPvd	: Other
	VILW	8	109858	02/12/21, 03:25:43	Indicator	TR-2020-27 related indicator detected in the environment	6 logs matching on the 18-2020-27 Indicator 72-21-91-29 were seen in	Dragos IOCa: 18-2020-27	144, 102			72.21.91.21
	VIEW		138857	02/12/21, 03:23:16	Change Detection	New Logic Applied To PLC via Beckhott ADS	New Logic Applied To PLC via Beckhoff ADS	Beckhoff ADS Logic Charge	35, 15	192 168 0 20	192.168.0.30	
	VIEW	2	138842	02/12/21, 02:49:51	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 8	Authentication to Multiple Hosts				
	VIEW	2	138841	02/12/21, 02:49:52	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by edmin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138840	02/12/21, 02:49:56	Threat Behavior	Multiple Logons Detected	Multiple Logens Detected by admin, who quickly logged into at least 8	Authentication to Multiple Hosts				
	VIEW	2	139809	02/12/21, 02:49:54	Threat Dehavior	Multiple Logons Detected	Multiple Logons Delected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138838	02/12/21,02:41:53	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	139837	02/12/21, 02:49:55	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138836	02/12/21,02:49:57	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138835	02/12/21, 02:49:58	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138834	02/12/21, 02:50:02	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138833	02/12/21, 02:50:01	Threat Behavior	Multiple Logons Detected	Multiple Lagens Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138832	02/12/21, 02.50:00	Threat Dehavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
	VIEW	2	138831	02/12/21, 02:50:03	Threat Behavior	Multiple Logors Detected	Multiple Logens Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				

#### Figure D-89 Dragos Alert Details for the PLC Logic File Download

	ASSOCIATED ASSETS		
	View 2 Type 2 ID 2	Name	¢ Dir
	VICW Engineering W 35 POLARIS		192.168.0.20 s
DETECTED RY: Bestant AGO Lage Change DETECTION QUAD: Change Delicities	VEW A Process Days 15 BagenNewyPLC		192,168,0,30
	RELATED NOTIFICATIONS (0)		
ICS ATTACK TACTIC:	ID C Occurred At C	Summary	
ICS ATTACK TECHNIQUE: Change Program State		No Related Notifications.	
NOTIFICATION RECORD: No Associated Record			
View m Koons			
	BETECTED BY: Beard of Add Lage Charge Charge Indexton Charge Indexton College Indexton Coll	DEFECTED PF:         Second AGU Logit Charge         DETECTION QUB:         Charge Descharge         Charge Descharge	EXECUTED ASSETS       Name         NOTIFICATION EXECUTES       Name         NOTIFICATION EXECUTES       Notifications         Notification       Notification         Notification       Notification         Notification       Notification

## D.8.4 Build 4

## D.8.4.1 Configuration

- Behavior Anomaly Detection: Azure Defender for IoT
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured to allow authorized users to access the PCS environment through the Dispel Enclave to the Dispel Wicket.

## D.8.4.2 Test Results

<u>Figure D-90</u> and <u>Figure D-91</u> show the connection to the CRS environment through the Dispel VDI. The changes to the PLC programs are detected by Azure Defender for IoT, as shown in <u>Figure D-92</u>, because the Dispel VDI is not an authorized programming device.

Figure D-90 Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket

•	Remote Desktop Connection				- 🗆 X
	E Command Pro	ompt	- 0	I X	^
y.	Addko Reply from 10 Reply from 10 Reply from 10	.100.1.7: bytes=32 time=184ms TTL=62 .100.1.7: bytes=32 time=182ms TTL=62			
	Reply from 10 Reply from 10	.100.1.7: bytes=32 time=101ms TTL=62 .100.1.7: bytes=32 time=184ms TTL=62			
0. N Dispel	Ping statisti Packets:	cs for 10.100.1.7: Sent = 8, Received = 8, Lost = 0 (0% loss),			
he	🧿 Dispel Client		- 0 ×		
i 🤦 👘					
fi Google Chrome	Ø DISPEL	Dispel is running Disconnect			
	Available Projects	Available Entry Points	Available Exit Points		
GUI	NCCOE-Manufacturing	Chicago, IL (	Exit NCCOE (cutter)		
-					
putty					
1					
TC31-FULL-					
Test Tote					
GreenTec					
- Constanting					
GreenTec. D					
weenree_p.a					
TC3_Remo					
					·



#### Figure D-91 Nested RDP Connections Showing Dispel Connection into the CRS Workstation



		11:36:08
<u>ب</u>	Alert Detected Mar 17, 2021 11:36:01 AM An asset that is not defined as a programming device carried out a programming change on a PLC.	11:36:01
	Source asset 10.100.1.61 performed programming on destination PLC asset 192.168.0.30.	
	Programming chan more	
	^	
Devices		
Туре	Name	
	CX-17DB08	
	10.100.1.61	
	Filter events by related devices	
		11:36:01

## D.9 Executing Scenario 9: Protect from Modification of Historian Data

An attacker who has already gained access to the corporate network attempts to modify historian archive data located in the DMZ. The expected result is the behavioral anomaly detection products detect the connection to the historian archive. File modification is prevented by the file integrity checking capability.

## D.9.1 Build 1

#### D.9.1.1 Configuration

Behavior Anomaly Detection: Tenable.ot

- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- File Integrity Checking: ForceField
  - PI Server is configured to use ForceField drive.

#### D.9.1.2 Test Results

Figure D-93 shows Tenable.ot detecting the remote access connections. Figure D-94 shows that GreenTec successfully blocks the attacker from deleting archive data.

Figure D-93 Tenable.ot alert Shows SMB Connection from External Workstation to the Historian



Figure D-94 GreenTec Denies Modification and Deletion File Operations in the Protected Drive

Kali Linux on LAN	VH - Virtual Machine Connection
File Action Media Clipboard View Help	
🌂 📔 🐂 🐂 🗽 👗 👗 FreeRDP: 10 🗈 administrato 🗈	🗉 administrato 🗈 administrato 😑 Arc Files - Fi 03:40 PM 🗖 🐠 🚱 🔒 🕒
administrator@ka	li: -/Documents/Arc Files _ □ ×
File Actions	Volume 100%
	PreeRDP:10.100.1.4
[15:33:38:433]	- 0 ×
[15:33:38:433] File Home Share View	~ <b>0</b>
[15:33:38:433] ← → ~ ↑ 🚽 > Network > 10.100.1.7 > ForceField	✓ ひ Search ForceField ク
[15:33:38:433] Name	)e Size ^
[15:33:38:433] A Quick access	ler Access Denied — X
[15:33:38:433] Desktop	sion to perform this action
[15:33:38:434] University Downloads	C File 03,530 KB
[15:33:38:434]	ceField C File 57 344 VR
[15:33:38:434] E Pictures # 2020-10-08 11	C File 8 192 KB
[15:33:38:434]	C File 1.256 KB
[15:33:38:434] This PC [15:33:38:434] 2020-10-08 11	Try Again Cancel 50,176 KB
[15:33:38:434 Desktop 2020-10-08_11	C File 15,360 KB
[15:33:38:434] Documents 2020-10-09_09 O More details	C File 1,256 KB
[15:33:38:434] United States 2020-10-09_09	-21_17-22-12-134C File 29,696 KB
[15:33:38:434] = home on kali 2020-10-09_091008_PI-DMZ_2020-08	8-27_17-22-15#2.arc 10/9/2020 9:09 AM ARC File 35,840 KB
[15:33:38:434] Music 2020-10-09_091018_PI-DMZ_2020-08	8-26_17-22-15#1.arc 10/9/2020 9:12 AM ARC File 1,256 KB
[15:33:38:434] Pictures 2020-10-09_091018_PI-DMZ_2020-08	3-27_17-22-15#1.arc 10/9/2020 9:12 AM ARC File 30,720 KB
[15:33:38:434] [15:33:38:434] [15:33:38:434] [15:33:38:434]	8-27_17-22-15#2.arc 10/9/2020 9:12 AM ARC File 34,816 KB
[15:33:38:434] and and and a second s	3-26_17-22-15#1.arc 10/9/2020 9:15 AM ARC File 1,256 KB
[15:33:38:434] DI Server (E)	3-27_17-22-15#1.arc 10/9/2020 9:15 AM ARC File 19,456 KB
[15:33:38:434] Product (C) 2020-10-09_091040_PI-DMZ_2020-08	-27_17-22-15#2.arc 10/9/2020 9:15 AM ARC File 46,080 KB
[15:33:38:434]	-26_17-22-15#1.arc 10/16/2020 1:15 PM ARC File 1,256 KB
[15:33:38:434] Queues (G:) 2020-10-16_131001_PI-DMZ_2020-08	-27_17_22-15#1.arc 10/16/20201:15 PM ARC Hite 20,480 KB
[15:33:38:535] Backups (H:) 2020-10-16_131001_PI-DINZ_2020-08	10/10/2020 101 PM ARC File 43,030 KB
[15:33:38:535] A Network	10/10/2020 1.39 PM ARC File 1,230 KB
[15:33:38:618] [15:33:38:660 2020-10-16 131017 PI-DMZ 2020-08	I-27 17-22-15#2.arc 10/16/2020 1:59 PM ARC File 45.056 KB
[15:33:38:661] 2020-10-16 131026 PI-DMZ 2020-08	1-26 17-22-15#1.arc 10/16/2020 1:54 PM ARC File 1.256 KB
[15:33:38:932] 2020-10-16 131027 PI-DMZ 2020-08	-27 17-22-15#1.arc 10/16/2020 1:54 PM ARC File 20.480 KB
[15:33:39:490] [15:33:39:490] [2020-10-16_131027_PI-DMZ_2020-08	1-27 17-22-15#2.arc 10/16/2020 1:54 PM ARC File 45,056 KB
[15:33:39:490] 2020-10-16_131033_PI-DMZ_2020-08	I-26_17-22-15#1.arc 10/16/2020 1:49 PM ARC File 1,256 KB
[15:33:39:490] [15:33:39:490] [2020-10-16_131034_PI-DMZ_2020-08	3-27_17-22-15#1.arc 10/16/2020 1:49 PM ARC File 20,480 KB
[15:33:39:490] 74 items	
[15:33:39:749] []	~ 및 4 340 PM 11/12/2020
Status: Running	

## D.9.2 Build 2

## D.9.2.1 Configuration

- Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- File Integrity Checking: ForceField
  - PI Server is configured to use ForceField drive.

## D.9.2.2 Test Results

Forescout detects the remote session as shown in Figure D-95. When the user attempts to alter a file on the protected drive, GreenTec denies the operation as shown in Figure D-96.

Figure D-95 Forescout Alert Shows Network Connection from Corporate Network to the Historian

<) FORESC	OUT. 🚳 Dashboard 🚠 N	etwork 🗮 Events	s 🔊 Sensors 🗱 Settings		🖵 🔊 📌 😑 admin
Alert details					📀 Help
Summary		∧ Source	e host info	▲ Alert Details	^
Alert ID Timestamp Sensor name Detection engine Profile Severity Source MAC	330437 Nov 12, 2020 15:33:31 sensor-bundle-nccoe Communication patterns (LAN CP) 8 - TCP communications 10.3 Medium (Cisco)	IP addres Host MJ address Other o MAC ad Role Vendor Client n	ess 129.6.1.3 (Public IP) AC Unknown beserved E4.90.69.38.C2.C0 (Rockwell) Idresses 7C:0E:CE:67.96.88 (Clsco) Terminal client and model Rockwell werproces Rockwell	ID and name Description Triggering rule/default act	Ian, cp_cnw, c- Communication pattern not whitelisted Communication pattern not whitelisted: the source and destination hosts are whitelisted in some communication rule, but not with this combination alert
Destination MAC Source IP Destination IP Source port Destination port L2 proto L3 proto L4 proto L7 proto TCP stream opened in hot start mode	00:15:5D:02:0D:03 (Microsof)	Chert p Server p Purdue Security Operati Criticali Known vulnera Related First sec Last see	NoteKinownOne (TCP 4444)           level         4 - Site business network           y Risk         IDDD 3.2           lonal Risk         IDDD 1.0           billities         0           alaerts         8 (Show)           en         Oct 14, 2020 11:56:54           en         Nov 12, 2020 15:45:56		
Alerts / Alert details					Copyright (C) 2009-2020 Forescout (v. 4.1.2)

Figure D-96 GreenTec Denies Modification and Deletion File Operations in the Protected Drive

2	Kali Linux on LANVH - Virtual Machine Connection		Ŀ	- 0 X
File Action Media Clipboard View Help				
& O O O O I D 5 5 1 K				
😫   📰 🖿 🖷 📲   👗 👘 👗 F	eeRDP: 10 🗵 administrato 🗈 administrato 🗈 administrato 💻 Arc File	s - Fi 03:4	орм 🗖 🜒 🎝 🕴	<b>0   ≙</b> G
	administrator@kali: ~/Documents/Arc Files			_ = ×
File Actions	E		Volume 100%	1990 <b>- 1</b> 9
	FreekDP:10:100.1.4		_	
[15:33:38:433] [15:33:38:433] [15:33:38:433]			-	
[15:33:38:433] File Home Share	View			~ 0
[15:33:38:433] ← → ~ ↑ 및 > Netwo	k > 10.100.1.7 > ForceField	~ Õ	Search ForceField	Q
[15:33:38:433]	Name	le	Size	^
[15:33:38:433 📌 Quick access	Destination Folder Access Denied - X		15555	
[15:33:38:433]	2020-10-08_11	C File	1,256 KB	
[15:33:38:434] - Downloads *		C File	00,030 KB	
[15:33:38:434]	2020-10-08_11	C File	1,230 KB	
[15:33:38:434] Pictures		C File	8 197 KB	
[15:33:38:434]		C File	1,256 KB	
[15:33:38:434] This PC	2020-10-08_11 Try Again Cancel	C File	50.176 KB	
[15:33:38:434] Desktop	2020-10-08 11	C File	15.360 KB	
[15:33:38:434]  Documents	2020-10-09_09 More details	C File	1,256 KB	
[15:33:38:434]	2020-10-09_09-000000	File	29,696 KB	
[15:33:38:434] 🛖 home on kali	2020-10-09_091008_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:09 AM	ARC File	35,840 KB	
[15:33:38:434 [15:33:38:434] Music	2020-10-09_091018_PI-DMZ_2020-08-26_17-22-15#1.arc 10/9/2020 9:12 AM	ARC File	1,256 KB	
[15:33:38:434] Pictures	2020-10-09_091018_PI-DMZ_2020-08-27_17-22-15#1.arc 10/9/2020 9:12 AM	ARC File	30,720 KB	
[15:33:38:434]	2020-10-09_091018_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:12 AM	ARC File	34,816 KB	
[15:33:38:434]	2020-10-09_091039_PI-DMZ_2020-08-26_17-22-15#1.arc 10/9/2020 9:15 AM	ARC File	1,256 KB	
[15:33:38:434] Di Corano (6)	2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#1.arc 10/9/2020 9:15 AM	ARC File	19,456 KB	
[15:33:38:434] = Pisever(E)	2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:15 AM	ARC File	46,080 KB	
[15:33:38:434]	2020-10-16_131000_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:15 PM	ARC File	1,256 KB	
[15:33:38:434] Queues (G:)	2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc 10/16/2020 1:15 PM	ARC File	20,480 KB	
[15:33:38:434 Backups (H:)	2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#2.arc 10/16/2020 1:15 PM	ARC File	45,056 KB	
[15:33:38:535] Network	2020-10-16_131016_PI-DMZ_2020-06-26_17-22-15#1.arc 10/16/2020 1:59 PM 1	ARC File	1,230 KB	
[15:33:38:618]	2020-10-10_151017_PEDM2_0020-00-21_17-22-15#1.arc     10/10/20201.59 PM	ARC File	45.056 KB	
[15:33:38:661]	2020-10-16_131076_PL-DM7_2020-08-26_17-22-15#2.arc 10/16/2020_1-54 PM	ARC File	1,256 KB	
[15:33:38:932]	2020-10-16 131027 PI-DMZ 2020-08-27 17-22-15#1.arc 10/16/2020 1-54 PM	ARC File	20.480 KB	
[15:33:39:490]	2020-10-16 131027 PI-DMZ 2020-08-27 17-22-15#2.arc 10/16/2020 1:54 PM	ARC File	45.056 KB	
[15:33:39:490]	2020-10-16_131033_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:49 PM	ARC File	1,256 KB	
[15:33:39:490]	2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc 10/16/2020 1:49 PM	ARC File	20,480 KB	
[15:33:39:490] [15:33:39:490] 74 items	E.			
[15:33:39:749]			∧ 탓 ₫ ₫ 3:40	PM
			11/12	/2020
Status: Running				8

## D.9.3 Build 3

## D.9.3.1 Configuration

- Behavior Anomaly Detection: Dragos
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- File Integrity Checking: ForceField
  - PI Server is configured to use ForceField drive.

## D.9.3.2 Test Results

Dragos detects the remote session as shown in Figure D-97. When the user attempts to alter a file on the protected drive, GreenTec denies the operation as shown in Figure D-98.

Figure D-97 Dragos Detection of RDP Session from an External Network to the Historian

DETECTION INFORMATION		ASSOCIATED ASSETS	
WHAT HAPPENED: RDP Negotiation Request		View C Type C ID C Name	C Dir. C
OCCURRED AT: 02/17/23, 19:46 UTC	LAST SEEN: 01/01/70, 00:00 UTC		10.100.1.4 dst src
DETECTOR (V). DETECTOR (V). DETECT	SOURCE: SOURCE: Falance: Table: CALL, NET DALL, NET		
XENOTIME MITRE ATTACK FOR ICS TACTIC Command And Control D	Stage 1. Act on Digitatives	Model Copyregation Financial Parts 2 Server Parts 2 TX 6 pp	Nes : RX Bytes :
Coder 14 00-020 UNI Index 15 Internet To Agencies Coder Providents Pol AreaDooks: To Account Physicolas CASES: No Cases Linked	NO IFFORTINE RELAKE. In Additional Relation	ιας - Υκτάκτι ΥΥ - Ε. 1999	1.03.9 //952
RELATED NOTIFICATIONS			
ID © Occurred At ©		Sunmary	3
		No Ridded Norfcattore.	

Figure D-98 GreenTec Denies Modification and Deletion File Operations in the Protected Drive

File       Action       Merce       Sector	2	Kali Linux on LANVH - Virtual Machine Connection		-	D X
Image: Sector District       I	File Action Media Clipboard View Help				
Image: State       Image: State <th< th=""><th>&amp; O O O II I I I I I I</th><th></th><th></th><th></th><th>-</th></th<>	& O O O II I I I I I I				-
State     State     Control     Control       File     Actions     FreedBP1010014	S   =	FreeRDP: 10 🗈 administrato 🗈 administrato 🗈 administrato 🔳 Arc File	es - Fi 03:4	юрм 🗆 🜒 🗟 🕤	🔒 G
File       Actions       FreedDP1:01:00:14       Volume 100%         155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:13:08:13; 155:33:38:14:14; 155		administrator@kali:~/Documents/Arc Files			_ = ×
Nature 20000000       Nature 1       Nature 1       Nature 1       Nature 1         13333384033       Image: 1       Nature 1       Nature 1       Nature 1       Nature 1         1333384033       Image: 1       Nature 1       Nature 1       Nature 1       Nature 1         1333384033       Image: 1       Nature 1       Nature 1       Nature 1       Nature 1         1333384033       Image: 1       Nature 1       Nature 1       Nature 1       Nature 1       Nature 1         1333384033       Image: 1       Nature	File Actions	E200-10.100.1.4		Volume 100%	
1333288484       Image: Subset Vew         13332884844       Image: Subset Vew         1333288444       Image: Subset Vew         13333288444       Image: Subset Vew <th></th> <th>PreekDP: 10.100.1.4</th> <th></th> <th></th> <th></th>		PreekDP: 10.100.1.4			
13333383843       Image: State Wrw       Image: State Wrw         133338433       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw         Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw       Image: State Wrw	[15:33:38:433] 2 V ForceField			- 1	· ·
1333384643 <ul> <li></li></ul>	[15:33:38:433] File Home Share	View			~ 0
1533338.443       Munit       200-10-00,11       You need permission to perform this action       File       1,256.88         1533338.443       Downloads       2000-10-00,11       You need permission to perform this action       File       1,256.88         1533338.4443       Downloads       2000-10-00,11       You need permission to perform this action       File       1,256.88         1533338.4443       Downloads       2000-10-00,11       You need permission to perform this action       File       1,256.88         1533338.4444       Downloads       2000-10-00,11       You need permission to perform this action       File       1,256.88         1533338.4444       Downloads       2000-10-00,11       You need permission to perform this action       File       1,256.88         1533338.4444       Downloads       2000-10-00,11       More details       File       1,256.88         1533338.4444       Downloads       2000-10-00,9000, PL bMZ, 2000-04-21,77-22.15F2.arc       109/2020 903 AL       ALC File       2,564.88         1533338.4444       Downloads       2000-10-00,9000, PL bMZ, 2000-04-21,77-22.15F2.arc       109/2020 903 AL       ALC File       1,256.88         153338.4444       Downloads       2000-10-00,9000, PL bMZ, 2000-04-21,77-22.15F2.arc       109/2020 903 AL       ALC File       1,256.88	[15:33:38:433] ← → ~ ↑ 및 > Ne	work > 10.100.1.7 > ForceField	~ Ö	Search ForceField	,c
15:333:84:43 <ul> <li>Quick acces:</li> <li>Quick acces:</li></ul>	[15:33:38:433]	Name	le	Size	^
1 333 38 84.43 1 333 38 84.43 1 333 38 84.43 1 333 38 84.43 1 333 38 84.44 1 353 38 84.44 1 35	[15:33:38:433] # Quick access	Destination Folder Access Denied - X			
11:333:8:4:43 <ul> <li>Downloads</li> <li>2020:10:00,11</li> <li>Fire</li> <li>13:33:8:4:43</li> <li>Pictures</li> <li>2020:10:00,11</li> <li>Fire</li> <li>13:33:8:4:44</li> <li>Pictures</li> <li>2020:10:00,11</li> <li>Cancel</li> <li>File</li> <li>12:33:33:4:44</li> <li>Documents</li> <li>2020:10:00,01</li> <li>Ontologit</li> <li>Ocuments</li> <li>2020:10:00,01</li> <li>Ontologit</li> <li>Cancel</li> <li>File</li> <li>12:56:48</li> <li>12:33:38:44</li> <li>Documents</li> <li>2020:10:00,01</li> <li>Ontologit</li> <li>Cancel</li> <li>File</li> <li>12:56:48</li> <li>12:26:48</li> <li12:27:27:27:27:27:27:27:27:27:27:27:27:27< th=""><th>[15:33:38:433 [15:33:38:433 Desktop )</th><th>2020-10-08_11 2020-10-08_11 You need permission to perform this action</th><th>C File</th><th>1,250 KB</th><th></th></li12:27:27:27:27:27:27:27:27:27:27:27:27:27<></ul>	[15:33:38:433 [15:33:38:433 Desktop )	2020-10-08_11 2020-10-08_11 You need permission to perform this action	C File	1,250 KB	
1333383843	[15:33:38:434] - Downloads		C File	00,030 KB	
<ul> <li>Pictures             <ul> <li>Quote 10-00, 1</li> <li>Quote 10-00, 0</li> <li>Market 2000-10-00, 0</li> <li>Market 2000-10-00, 0</li> <li>Market 2000-10-00, 0</li> <li>Quote 10-00, 0</li></ul></li></ul>	[15:33:38:434]	2020-10-08_11 ForceField	C File	57 244 VP	
11333383434       Image: Conceler of the second seco	[15:33:38:434] Pictures		File	8 107 KB	
15:33:33:84.34       Thi PC       220:10-00_11       Try Again       Cancel       File       51,75 KB         15:33:33:84.34       Dexitop       200:10-00_00       More details       File       12,25 KB         15:33:33:84.34       Downloads       2000:10-00_00       More details       File       12,25 KB         15:33:33:84.34       Downloads       2000:10-00_00       More details       File       12,25 KB         15:33:33:84.34       Music       2000:10-00_000100_Ph/DMZ_2000-06-27,17-22:15F2.arc       10/9/2000 Ph2 AM       ARC File       35,64 KB         15:33:33:84.34       Music       2000:10-00_000100_Ph/DMZ_2000-06-27,17-22:15F2.arc       10/9/2000 Ph2 AM       ARC File       34,64 KB         15:33:33:84.34       Music       2000:10-00_000100_Ph/DMZ_2000-06-27,17-22:15F2.arc       10/9/2000 Ph2 AM       ARC File       34,64 KB         15:33:33:84.34       Local Disk (C)       2000:10-00_000100_Ph/DMZ_2000-06-27,17-22:15F2.arc       10/9/2000 Ph3 AM       ARC File       14,600 KB         15:33:33:84:34       Local Disk (C)       2000:10-16_131000_Ph/DMZ_2000-06-27,17-22:15F1.arc       10/9/2000 Ph3 AM       ARC File       14,600 KB         15:33:33:84:34       Local Disk (C)       2000:10-16_131000_Ph/DMZ_2000-06-27,17-22:15F1.arc       10/9/2000 Ph3 AM       ARC File       12,56 KB </th <th>[15:33:38:434]</th> <th>2020-10-08 11</th> <th>C File</th> <th>1,256 KB</th> <th></th>	[15:33:38:434]	2020-10-08 11	C File	1,256 KB	
15:33:38:4426       ■ Desktop       2020-10-09,11       File       15:30:86426         15:33:38:4426       ■ Documents       2020-10-09,00 m/m cmtcs       Explore       Explore       Explore         15:33:38:4426       ■ Documents       2020-10-09,00 m/m cmtcs       10:772-21:5F1.arc       10:972-2020-90.90 m/m cmtc       Explore         15:33:38:4426       ■ Documents       2020-10-09,00 m/m cmtcs       2020-10-09,00 m/m cmtcs       10:772-21:5F1.arc       10:972-2020-912 AM       ARC File       35.840 KB         15:33:38:4426       ■ Music       2020-10-09,00 m/m kp-DMZ,2020-08-27,17-22:15F1.arc       10:972-2020-912 AM       ARC File       32.820 KB         15:33:38:4364       ■ Videos       2020-10-09,00 m/m kp-DMZ,2020-08-27,17-22:15F1.arc       10:972-2020-912 AM       ARC File       32.840 KB         15:33:38:4364       ■ Load Dix (C)       = 2020-10-09,00 m/m kp-DMZ,2020-08-27,17-22:15F1.arc       10:972020-915 AM       ARC File       34.86 KB         15:33:38:4364       ■ Load Dix (C)       = 2020-10-09,00 m/m kp-DMZ,2020-08-27,17-22:15F1.arc       10:972020-915 AM       ARC File       12.56 KB         15:33:38:4364       ■ Load Dix (C)       = 2020-10-16,131000,P-DMZ,2020-08-27,17-22:15F1.arc       10:972020-915 AM       ARC File       12.56 KB         15:33:38:4364       ■ Load Dix (C)       = 2020-10-16,131000,P-DM	[15:33:38:434 This PC	2020-10-08 11 Try Again Cancel	C File	50,176 KB	
15:33:38:434	[15:33:38:434] Desktop	2020-10-08 11	C File	15,360 KB	
15:33:38:434 <ul> <li>Downloads</li> <li>2020:10:09_09100g,PI:DMZ_2020:08:27,17-22:1582.arc</li> <li>109/2020 90:12 AM</li> <li>ARC File</li> <li>25,400 KB</li> </ul> 15:33:38:444 <ul> <li>Music</li> <li>2020:10:09_091018,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>109/2020 91:12 AM</li> <li>ARC File</li> <li>35,400 KB</li> </ul> 15:33:38:443 <ul> <li>Pictures</li> <li>2020:10:09_091018,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>109/2020 91:12 AM</li> <li>ARC File</li> <li>34,716 KB</li> </ul> 15:33:38:443 <ul> <li>Videos</li> <li>2020:10:09_091040,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>109/2020 91:15 AM</li> <li>ARC File</li> <li>34,765 KB</li> <li>15:33:38:443</li> <li> <ul> <li>Local Disk (C:)</li> <li>2020:10:09_091040,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>109/2020 11:5 PM</li> <li>ARC File</li> <li>1,556 KB</li> <li>15:33:38:434</li> <li> <ul> <li>Archive (F)</li> <li>2020:10:10:10,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>109/2020 11:5 PM</li> <li>ARC File</li> <li>1,556 KB</li> <li>2020:10:10:16,13100,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>1016/2020 11:5 PM</li> <li>ARC File</li> <li>1,556 KB</li> <li>2020:10:16,13100,PI:DMZ_2020:08:27,17-22:1581.arc</li> <li>1016/2020 11:5 PM</li> <li>ARC File</li></ul></li></ul></li></ul>	[15:33:38:434]  Documents	2020-10-09_09 O More details	C File	1,256 KB	
15:33:38:434 <ul> <li>home on kali</li> <li>2020-10-09_091008_PI-DMZ_2020-08-27_17-22-15#2.arc</li> <li>109/2020 9:12 AM</li> <li>ARC File</li> <li>1.256 KB</li> <li>2020-10-09_091018_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>109/2020 9:12 AM</li> <li>ARC File</li> <li>3.256 KB</li> <li>Videos</li> <li>2020-10-09_091018_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>109/2020 9:12 AM</li> <li>ARC File</li> <li>3.4616 KB</li> <li>3.333:8:434</li> <li>Videos</li> <li>2020-10-09_0910108_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>109/2020 9:12 AM</li> <li>ARC File</li> <li>3.4616 KB</li> <li>3.333:8:434</li> <li>Videos</li> <li>2020-10-09_0910104_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>109/2020 9:15 AM</li> <li>ARC File</li> <li>1.464080 KB</li> <li>2.333:8:434</li> <li>PI Server (E)</li> <li>2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>109/2020 9:15 AM</li> <li>ARC File</li> <li>1.464080 KB</li> <li>3.333:8:434</li> <li>Archives (F)</li> <li>2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>101/6/2020 1:15 PM</li> <li>ARC File</li> <li>2.266 KB</li> <li>3.333:8:434</li> <li>Backupp (H)</li> <li>2020-10-16_1310101_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>101/6/2020 1:15 PM</li> <li>ARC File</li> <li>2.266 KB</li> <li>2.200-10-16_131010_PI-DMZ_2020-08-27_17-22-15#1.arc</li> <li>101/6/2020 1:59 PM</li> <li>ARC File</li> <li>2.266 KB</li> <li>2.333:38:436</li></ul>	[15:33:38:434] Uownloads	2020-10-09_09 1000_F1*DMIL_2020*00*21_17*22*13*1.arc 10/5/2020 5:05 MINI	And File	29,696 KB	
15:33:38:43/4 <ul> <li>Music</li> <li>2020-10-09_091018_Pi-DMZ_2020-08-26_17-22-15#1.arc</li> <li>10/9/2020_912 AM</li> <li>ARC File</li> <li>1,256 KB</li> <li>2020-10-09_091018_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/9/2020_912 AM</li> <li>ARC File</li> <li>30,720 KB</li> <li>2020-10-09_091018_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/9/2020_912 AM</li> <li>ARC File</li> <li>30,720 KB</li> <li>2020-10-09_091018_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/9/2020_915 AM</li> <li>ARC File</li> <li>1,256 KB</li> <li>2020-10-09_091040_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/9/2020_915 AM</li> <li>ARC File</li> <li>1,256 KB</li> <li>2020-10-09_091040_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/9/2020_915 AM</li> <li>ARC File</li> <li>1,256 KB</li> <li>2020-10-16_131000_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/9/2020_915 AM</li> <li>ARC File</li> <li>1,256 KB</li> <li>2020-10-16_131000_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/16/2020_115 PM</li> <li>ARC File</li> <li>2020-10-16_131001_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/16/2020_115 PM</li> <li>ARC File</li> <li>2020-10-16_131001_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/16/2020_115 PM</li> <li>ARC File</li> <li>2020-10-16_131007_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/16/2020_115 PM</li> <li>ARC File</li> <li>2020-10-16_131007_Pi-DMZ_2020-08-27_17-22-15#1.arc</li> <li>10/16/2020_159 PM</li> <li>ARC File</li> <li>2020-10-16_131007_Pi-DMZ_2020-0</li></ul>	[15:33:38:434] 🛖 home on kali	2020-10-09_091008_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:09 AM	ARC File	35,840 KB	
15:33:38:434 (15:33:38):434 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15:33:39):490 (15	[15:33:38:434 [15:33:38:434] Music	2020-10-09_091018_PI-DMZ_2020-08-26_17-22-15#1.arc 10/9/2020 9:12 AM	ARC File	1,256 KB	
15:33:38:434       □ 2020-10-09_091018_PI-OMZ_2020-08-27_17-22-15#2.arc       10/9/2020_912_AM       ARC File       34,816 KB         15:33:38:434       □ Local Disk (C:)       □ 2020-10-09_091040_PI-OMZ_2020-08-26_17-22-15#1.arc       10/9/2020_915 AM       ARC File       1,256 KB         15:33:38:434       □ Disk (C:)       □ 2020-10-09_091040_PI-OMZ_2020-08-26_17-22-15#1.arc       10/9/2020_915 AM       ARC File       1,256 KB         15:33:38:434       □ Archives (F:)       □ 2020-10-09_091040_PI-OMZ_2020-08-26_17-22-15#1.arc       10/9/2020_915 AM       ARC File       1,256 KB         15:33:38:434       □ Archives (F:)       □ 2020-10-16_131001_PI-OMZ_2020-08-26_17-22-15#1.arc       10/16/2020 1:15 PM       ARC File       2,480 KB         15:33:38:434       □ Queues (G:)       □ 2020-10-16_13101PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       45,056 KB         15:33:38:435       □ Network       □ 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       12,266 KB         15:33:38:660       □ 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       12,266 KB         15:33:38:660       □ 2020-10-16_131026_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       12,266 KB         15:33:39:490       □ 2020-10-16_131026_PI-DMZ_2020-08-27_17-2	[15:33:38:434] Pictures	2020-10-09_091018_PI-DMZ_2020-08-27_17-22-15#1.arc 10/9/2020 9:12 AM	ARC File	30,720 KB	
15:33:33:434       □       <	[15:33:38:434]	2020-10-09_091018_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:12 AM	ARC File	34,816 KB	
15:33:38:434       ■ Desrver (E)       2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#1.arc       10/9/2020 9:15 AM       ARC File       19.456 KB         15:33:38:434       ■ PI Server (E)       2020-10-16_131000_PI-DMZ_2020-08-27_17-22-15#1.arc       10/9/2020 9:15 AM       ARC File       46.060 KB         15:33:38:434       ■ Archives (F)       2020-10-16_131000_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:15 PM       ARC File       12.256 KB         15:33:38:434       ■ Queues (G:)       2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:15 PM       ARC File       45.056 KB         15:33:38:434       ■ Backups (H:)       2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:15 PM       ARC File       45.056 KB         15:33:38:458       ■ Octions (E)       = 2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       45.056 KB         15:33:38:668       = 2020-10-16_131007_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       45.056 KB         15:33:38:6168       = 2020-10-16_131007_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       12.56 KB         15:33:39:490       = 2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       12.56 KB         15:33:39:490       = 2020-10-16_131027_PI-DMZ_2020-08-27_1	[15:33:38:434]	2020-10-09_091039_PI-DMZ_2020-08-26_17-22-15#1.arc 10/9/2020 9:15 AM	ARC File	1,256 KB	
15:33:33:8:434       = Archives (F)       2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#2_arc       10//6/2020 9:15 AM       ARC File       46,080 KB         15:33:38:434       = Archives (F)       2020-10-16_131000_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:15 PM       ARC File       1,256 KB         15:33:38:434       = Queues (G:)       2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:15 PM       ARC File       24,800 KB         15:33:38:434       = Backups (H:)       2020-10-16_131010_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:59 PM       ARC File       44,080 KB         15:33:38:434       = Backups (H:)       2020-10-16_131016_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:59 PM       ARC File       12,56 KB         15:33:38:618       = 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:59 PM       ARC File       12,56 KB         15:33:38:618       = 2020-10-16_131012_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:59 PM       ARC File       12,56 KB         15:33:38:618       = 2020-10-16_131012_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:54 PM       ARC File       12,56 KB         15:33:39:490       = 2020-10-16_131032_PI-DMZ_2020-08-27_17-22-15#1_arc       10//16/2020 1:54 PM       ARC File       12,56 KB         15:33:39:490       = 2020-10-16_131032_PI-DMZ_2020-08-27_17-22-15#1_arc	[15:33:38:434] DI Secure (E)	2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#1.arc 10/9/2020 9:15 AM	ARC File	19,456 KB	
15:33:33:434       ■ Archive (r:)       2020-10-16_131000_PI-DMZ_2020-08-2_0_7-22-15#1.arc       10/16/2020 1:15 PM       ARC File       1,256 KB         15:33:33:434       ■ Queues (G:)       2020-10-16_131001_PI-DMZ_2020-08-2_7_17-22-15#1.arc       10/16/2020 1:15 PM       ARC File       20,480 KB         15:33:33:434       ■ Backups (H:)       2020-10-16_131001_PI-DMZ_2020-08-2_7_17-22-15#1.arc       10/16/2020 1:15 PM       ARC File       1,256 KB         15:33:33:454       ■ Dackups (H:)       2020-10-16_131001_PI-DMZ_2020-08-2_7_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:81-618       □ 2020-10-16_131007_PI-DMZ_2020-08-2_7_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:81-618       □ 2020-10-16_131007_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:81-618       □ 2020-10-16_131007_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:81-628       □ 2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         15:33:33:91:490       □ 2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         15:33:33:91:490       □ 2020-10-16_1310327_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020	[15:33:38:434 - Fisever(c)	2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:15 AM	ARC File	46,080 KB	
[15:33:38:434       → Queues (cc)       2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:51 PM       ARC File       20,480 KB         [15:33:38:434       → Backups (H:)       2020-10-16_131001_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       45,056 KB         [15:33:38:618       → Network       2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       20,480 KB         [15:33:38:668       → Network       2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       20,480 KB         [15:33:38:668       □ 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         [15:33:38:661       □ 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490       □ 2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490       □ 2020-10-16_131032_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490       □ 2020-10-16_131032_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490       □ 2020-10-16_131032_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM	[15:33:38:434]	2020-10-16_131000_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:15 PM	ARC File	1,256 KB	
15:33:33:35:43       → Backups (H)       □ 2020-10-16_13101[-PI-DMZ_2020-08-25_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:38:555       □ Network       □ 2020-10-16_131017_PI-DMZ_2020-08-25_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:38:660       □ 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:8660       □ 2020-10-16_131017_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:59 PM       ARC File       1,256 KB         15:33:33:81:661       □ 2020-10-16_131007_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         15:33:39:490       □ 2020-10-16_131007_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       2,480 KB         15:33:39:490       □ 2020-10-16_131032_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       2,480 KB         15:33:39:490       □ 2020-10-16_131033_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         15:33:39:490       □ 2020-10-16_131033_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         15:33:39:490       □ 2020-10-16_131033_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       1,256 KB <th>[15:33:38:434] Queues (G:)</th> <th>2020-10-16_131001_PI-DM2_2020-08-27_17-22-15#1.arc 10/16/20201115 PM</th> <th>ARC File</th> <th>20,480 KB</th> <th></th>	[15:33:38:434] Queues (G:)	2020-10-16_131001_PI-DM2_2020-08-27_17-22-15#1.arc 10/16/20201115 PM	ARC File	20,480 KB	
[15:33:38:553 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:38:668 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490 [15:33:39:490         [15:33:39:490 [15:33:39:490         [15:33:39:490	[15:33:38:434 Backups (H:)	2020-10-10_131001_PI-DM2_0020-06-27_17-22-13#2.arc 10/16/20201015 PM	ARC FILE	40,000 KB	
151333381648       □ 000 100 110 10 100 100 100 100 100 100	[15:33:38:535] 🚽 Network	2020-10-10_131010_PFDMZ_0020-08-20_17-22-13#1.arc 10/10/20201.39 PM	ARC File	20.480 KB	
15133338:661       2020-10-16_131025_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         15133339:490       2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       2,480 KB         15133339:490       2020-10-16_131037_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       2,56 KB         15133339:490       2020-10-16_131037_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         151333:39:490       2020-10-16_131033_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         151333:39:490       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         151333:39:490       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       2,480 KB         151333:39:490       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       2,480 KB         151333:39:490       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       2,480 KB         151333:39:490       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       2,480 KB         15133:39:490       11/12/200       11/12/	[15:33:38:618]	2020-10-16 131017 PL-DMZ 2020-08-27 17-22-15#2 arc 10/16/2020 1-59 PM	ARC File	45.056 KB	
[15:33:38:922]       2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       20,480 KB         [15:33:39:490]       2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#2.arc       10/16/2020 1:54 PM       ARC File       45,056 KB         [15:33:39:490]       2020-10-16_131037_PI-DMZ_2020-08-26_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       45,056 KB         [15:33:39:490]       2020-10-16_131033_PI-DMZ_2020-08-26_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490]       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       20,480 KB         [15:33:39:490]       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       20,480 KB         [15:33:39:490]       74 items       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       20,480 KB         [15:33:39:490]       74 items       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       20,480 KB         [15:33:39:490]       74 items       2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       20,480 KB         [15:33:39:490]       74 items       2020-10-16_131034_PI-DMZ_2020_PI-201-24-15#1.arc       10/16/2020 1:49 PM       ARC File<	[15:33:38:661]	2020-10-16 131026 PI-DMZ 2020-08-26 17-22-15#1.arc 10/16/2020 1:54 PM	ARC File	1.256 KB	
15:33:39:490       □ 2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#2.arc       10/16/2020 1:54 PM       ARC File       45,056 KB         [15:33:39:490       □ 2020-10-16_131033_PI-DMZ_2020-08-26_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       1,256 KB         [15:33:39:490       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       20,480 KB         [15:33:39:490       □ 4 Emms       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       20,480 KB         [15:33:39:490       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       20,480 KB         [15:33:39:490       □ 4 Emms       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       20,480 KB         [15:33:39:490       □ 4 Emms       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:54 PM       ARC File       20,480 KB         [15:33:39:490       □ 4 Emms         [15:33:39:490       □ 4 Emms         [15:33:39:490 <th>[15:33:38:932]</th> <th>2020-10-16 131027 PI-DMZ 2020-08-27 17-22-15#1.arc 10/16/2020 1:54 PM</th> <th>ARC File</th> <th>20,480 KB</th> <th></th>	[15:33:38:932]	2020-10-16 131027 PI-DMZ 2020-08-27 17-22-15#1.arc 10/16/2020 1:54 PM	ARC File	20,480 KB	
[15:33:39:490 [15:	[15:33:39:490	2020-10-16_131027_PI-DMZ_2020-08-27_17-22-15#2.arc 10/16/2020 1:54 PM	ARC File	45,056 KB	
1151:33:39:4990       □ 2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc       10/16/2020 1:49 PM       ARC File       20,480 KB         [151:33:39:4940       74 items       □       □       11/12/2020       □       □       □       3:40 PM       □       □       □       3:40 PM       □ </th <th>[15:33:39:490</th> <th>2020-10-16_131033_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:49 PM</th> <th>ARC File</th> <th>1,256 KB</th> <th></th>	[15:33:39:490	2020-10-16_131033_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:49 PM	ARC File	1,256 KB	
15:33:39:440       74 items         15:33:39:749	[15:33:39:490 [15:33:39:490	2020-10-16_131034_PI-DMZ_2020-08-27_17-22-15#1.arc 10/16/2020 1:49 PM	ARC File	20,480 KB	~
15:33:39:749	[15:33:39:490] 74 items				
Status: Running	[15:33:39:749] □	ê 🚍 🗷		^ 〒 🔩 3:40 Pl	M 🖓
	Status: Running				88

## D.9.4 Build 4

## D.9.4.1 Configuration

- Behavior Anomaly Detection: Azure Defender for IoT
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- File Integrity Checking: ForceField
  - PI Server is configured to use ForceField drive.

## D.9.4.2 Test Results

The connection to the Historian data storage was detected by Azure Defender for IoT as shown in Figure D-99. Figure D-100 shows a Windows error message after attempting to overwrite protected Historian files.

Figure D-99 Azure Defender for IoT Event Timeline Showing the Remote Access Connection to the Historian

Azure Defender for IoT	×	+										-	0 X
← → C ▲ Not	secure   1	0.100.0.61/#/eve	ents									☆	<b>e</b> :
Microsoft	÷	Event Time	eline										0
NAVIGATION		Free Search			Q 🗆 🖬	Advanced Fil	ters All	Events 👻	2, User Operations	🖬 Select Date			
Dashboard	(Ø)									CRefresh	Create Event	B Exp	port
Devices Map (76)	윪					A	or 14, 2021						
Device Inventory	=		File	Transfer Detected									
Alerts (114)	۰		ИТТ	P File transfer from client IP: 10 Content type applicat	0.100.1.4, Serv tion/vnd.ms-ca	er: ab-	14-42-12						
Reports			com	pressed			14.43.13						
ANALYSIS				~		Notice		0	Remote Access C Apr 14, 2021 2:41:47 Pl	onnection Es	tablished		
Event Timeline	Ê						14:41:47	*	Remote Desktop	1 from	to 10.100.1.4 using		
Data Mining										^			
Investigation	4							Devices Type	Nan	ne			
Risk Assessment	A								PI-D	MZ			
Attack Vectors	Ø								Inte	met			
ADMINISTRATION			Aler	t Detected					Filter events b	y related devic	ces		
Custom Alerts	*	. 1	Apr 1-	4, 2021 2:36:43 PM w asset was detected on the ne	etwork. Asset						Info		
Azure Defender for lo Version 10.0.3	л		Verif	fy that this is a valid network as	set.		14:36:43						
		0	8								4	3 12	2:47 PM 4/14/2021

- 🗆 🗙 Kali Linux on LANVH - Virtual Machine Connection File Action Media Clipboard View Help 4 0 0 0 0 1 1 5 5 3 🗈 administrator@kali: ~/P... 🗈 administrator@kali: ~/P. 02:59 PM 🖸 FreeRDP: 10.100.1.4 1) • FreeRDP: 10.100.1.4 × Minimize all open windows and show the desktop 0 Properties (Alt+Enter) Show the properties for the selected item. .1.7 > ForceField ✓ ♂ Search ForceField Name Size **Destination Folder Access Denied** × Quick access 2021-01-05 03 65.536 KB File Desktop You need permission to perform this action 2021-01-05\_03 File 65.536 KB Downloads 2021-01-05\_03 File 1,256 KB Documents 2021-01-04\_03 ForceField File 65,536 KB Pictures 2021-01-04\_03 File 65,536 KB 2021-01-04\_03 File 1,256 KB Arc Files Try Again Cancel ForceField 2021-01-03\_03 File 65 536 KB 2021-01-03\_03 File 65.536 KB This PC More details 2021-01-03\_03 File 1,256 KB Desktop C File 65,536 KB Documents 2021-01-02 033006 PI-DMZ 2020-08-27 17-22-15#1.arc 1/2/2021 3:30 AM ARC File 65,536 KB 2021-01-02\_033005\_PI-DMZ\_2020-08-26\_17-22-15#1.arc 1/2/2021 3-30 AM ARC File 1.256 KB Downloads 2021-01-01\_033024\_PI-DMZ\_2020-12-09\_17-55-41#1.arc 1/1/2021 3:30 AM ARC File 65,536 KB 🛖 home on kali 2021-01-01\_033006\_PI-DMZ\_2020-08-27\_17-22-15#1.arc 1/1/2021 3:30 AM ARC File 65,536 KB Music 2021-01-01\_033005\_PI-DMZ\_2020-08-26\_17-22-15#1.arc 1/1/2021 3:30 AM 1,256 KB ARC File Pictures 2020-12-31 033024 PI-DMZ 2020-12-09 17-55-41#1.arc 12/31/2020 3:30 AM ARC File 65.536 KB Videos 2020-12-31\_033006\_PI-DMZ\_2020-08-27\_17-22-15#1.arc 12/31/2020 3:30 AM ARC File 65.536 KB Local Disk (C:) 2020-12-31\_033005\_PI-DMZ\_2020-08-26\_17-22-15#1.arc 12/31/2020 3:30 AM ARC File 1,256 KB 2020-12-30\_033024\_PI-DMZ\_2020-12-09\_17-55-41#1.arc 65,536 KB PI Server (E:) 12/30/2020 3:30 AM ARC File 2020-12-30\_033006\_PI-DMZ\_2020-08-27\_17-22-15#1.arc 12/30/2020 3:30 AM ARC File 65,536 KB Archives (F:) 2020-12-30 033005 PI-DMZ 2020-08-26 17-22-15#1.arc 12/30/2020 3:30 AM ARC File 1.256 KB Queues (G:) 2020-12-29\_033024\_PI-DMZ\_2020-12-09\_17-55-41#1.arc 12/29/2020 3:30 AM ARC File 65 536 KB Backups (H:) 2020-12-29\_033006\_PI-DMZ\_2020-08-27\_17-22-15#1.arc 12/29/2020 3:30 AM ARC File 65.536 KB Network 2020-12-29\_033005\_PI-DMZ\_2020-08-26\_17-22-15#1.arc 12/29/2020 3:30 AM ARC File 1,256 KB 2020-12-28\_033024\_PI-DMZ\_2020-12-09\_17-55-41#1.arc 12/28/2020 3:30 AM ARC File 65,536 KB 2020-12-28 033006 PI-DMZ 2020-08-27 17-22-15#1.arc 12/28/2020 3:30 AM ARC File 65,536 KB 2020-12-28\_033005\_PI-DMZ\_2020-08-26\_17-22-15#1.arc 12/28/2020 3:30 AM ARC File 1.256 KB 2020-12-27\_033024\_PI-DMZ\_2020-12-09\_17-55-41#1.arc 12/27/2020 3:30 AM 65,536 KB ARC File 209 ite へ 行口 🕼 1/5/2021 Ŧ Ω e 2 8 Status: Running

Figure D-100 GreenTec Denies Modification and Deletion File Operations in the Protected Drive

## **D.10 Executing Scenario 10: Detect Sensor Data Manipulation**

A sensor in the manufacturing system sends out-of-range data values to the Historian. The expected result is the behavioral anomaly detection (data historian) capability alerts on out-of-range data.

## D.10.1 All Builds

## D.10.1.1 Configuration

- Behavior Anomaly Detection: PI Server
  - Configured to receive process data from across the manufacturing system.

Configured to perform analysis on incoming data points.

## D.10.1.2 Test Results

The Historian process monitoring capabilities provided by the PI System are able to monitor out-ofrange sensor readings and generate alerts. Figure D-101 shows the PI Server's event frame alerts on the out-of-range reactor pressure readings in the PCS.

Figure D-101 PI Server's Event Frames Showing Out-of-Range Sensor Readings for the Reactor Pressure



## D.11 Executing Scenario 11: Detect Unauthorized Firmware Modification

An authorized user accesses the system remotely and performs an unauthorized firmware change on a PLC. The expected result is the behavioral anomaly detection tools will alert on the new firmware.

The behavior anomaly detection tools can detect changes to the firmware. Firmware change detection needs to be correlated with the maintenance management system to determine if the firmware change was authorized and approved. This was not demonstrated as part of this scenario.

## D.11.1 Build 1

## D.11.1.1 Configuration

Behavior Anomaly Detection: Tenable.ot

- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for accessing the PCS environment.

#### D.11.1.2 Test Results

Figure D-102 depicts the list of the events detected by Tenable.ot resulting from the firmware change. The details of one of the alerts are shown in Figure D-103.

Figure D-102 Tenable.ot Detects a Collection of Events Generated by a Firmware Change

= Ctenable.ot											02:30 PM + Thursday, Feb 4, 2021 NCCOE	User 🗸
✓ ♣ Events All Events	Configuration E	Events search	Q								Actions ~ Resolve All Expert	0
Configuration Events	LOS ID 🕹	TIME	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD	PROTOCOL		«
SCADA Events	12436	02:28:03 PM - Feb 4, 2021	Change in Firmwa	High	Change in controller firmwar	Comm. Adapter #1				Unknown		* Internet
Network Threats	12434	02:25:41 PM - Feb 4, 2021	Rockwell Module	Low	Rockwell Module Restart	PCS Eng. Station	172.16.3.10	Comm. Adapter #1	172.16.2.102	CIP (top)		13
Network Events	12433	02:25:49 PM - Feb 4, 2021	Rockwell Firmwar	High	Rockwell Firmware Download	PCS Eng. Station	172.16.3.10	Comm. Adapter #1	172.16.2.102	CIP (top)		
Policies	12427	02:11:24 PM - Feb 4, 2021	Rockwell Module	Low	Rockwell Module Restart	PCS Eng. Station	172.16.3.10	Time Module	172.16.2.102	CIP (top)		
✓ ♣ Inventory	12425	02:05:50 PM - Feb 4, 2021	Rockwell Module	Low	Bockwell Module Restart	PCS Eng. Station	172.16.3.10	Time Module	172.16.2.102	CIP (top)		
controllers	12423	02:03:55 PM - Feb 4, 2021	Rockwell Tag Dele	Low	Bockwell Delete Tax	PCS Eng. Station	172.16.3.10	nic tesim	172.16.2.102	CIP (ttp)		
Network Assets	12422	02:03:55 PM - Feb 4, 2021	Rockwell Tag Cre	Low	Rockwell Create Tag	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CIP (tcp)		
> 章 RISK	12421	02:02:47 PM - Feb 4, 2021	Change in State	Medium	Change in controller state	pic tesim				Unknown		
> A Network	12416	01:47:47 PM - Feb 4, 2021	Change in Key Sw	High	Change in controller key state	plc_tesim				CIP (top)		
> G Groups	12414	01:46:52 PM - Feb 4, 2021	Rockwell PLC Start	Low	Rockwell PLC Start	PCS Eng. Station	172.16.3.10	plc_tesim	172.16.2.102	CIP (top)		
Reports	12413	01:46:30 PM - Feb 4, 2021	Rockwell Code Do	Medium	Rockwell Code Download	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CIP (top)		
> o <sup>o</sup> Local Settings	12412	01:46:27 PM - Feb 4, 2021	Rockwell PLC Stop	High	Nockwell PLC Scop	PCS Eng. Station	172.16.3.10	plc.tesim	172.16.2.102	CIP (tcp)		
	12410	01:45:05 PM - Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	nic tesim	172.16.2.102	CIP (tcp)		
	12408	01:42:21 PM · Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CIP (top)		
	12406	01:41:28 PM - Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CIP (top)		
	9133	04:33:00 PM - Jan 29, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	plo_tesim	172.16.2.102	CIP (top)		
	9121	04:02:47 PM - Jan 29, 2021	Change in Key Sw.,	High	Change in controller key state	plc.tesim				CIP (top)		
	9120	04:02:47 PM - Jan 29, 2021	Change in State	Medium	Change in controller state	plc tesim				Unknown		
	9115	03:47:47 PM - Jan 29, 2021	Change in Key Sw	High	Change in controller key state	plc tesim				CIP (ttp)		
	9114	03:47:47 PM - Jan 29, 2021	Change in State	Medium	Change in controller state	plc.tesim				Unknown		
	9110	03:38:51 PM - Jan 29, 2021	Rockwell Code Up	Low	Bockwell Code Upload	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CIP (ttcp)		
	Items: 1-25 out of 25										K S Page 1 of 1 ->	×
	Event 12436 02:28:0	03 PM · Feb 4, 2021 Change	e in Firmware Version	High Not	resolved							
	Details	A shares in the former										1
	Affected Assets	A change in the inniv	are version was detec	teu								
	Policy	SOURCE NAME	Cornen, Adapt	er,#1				Why is this it	noortant?		Suggested Mitigation	
	Status	SOURCE ADDRESS	172.16.2.102	172.16.4.102								
		BACKPLANE NAME	Backplane #1					A change in occur over t	he firmware version te network or through	was detected. Such a change can h physical access to the device.	<ol> <li>Check if the change was made as part of scheduled work.</li> <li>If this was not part of a planned operation, check if the network.</li> </ol>	
		OLD FIRMWARE VERSION	10.007					An attacker i the asset. In:	nay use firmware cha iert backdoors or disr	anges to alter the functionality of rupt normal operations.	behavior of the asset has changed.	
		NEW FIEWWARE VERSION	10.010									
March 2 Average Providence Providence Providence												

#### Figure D-103 Details for One of the Alerts Showing the Firmware Change

Event 12436 02:28:03 P	vent 12436 02:28:03 PM · Feb 4, 2021 Change in Firmware Version High Not resolved												
Details Affected Assets	A change in the firmware ver	sion was detected											
Policy	SOURCE NAME	Comm. Adapter #1	Why is this important?	Suggested Mitigation									
Status	SOURCE ADDRESS	172.16.2.102   172.16.4.102	A change in the firmware version was detected. Such a change can	1) Check if the change was made as part of scheduled work.									
	BACKPLANE NAME	Backplane #1	occur over the network or through physical access to the device.	2) If this was not part of a planned operation, check if the network									
	OLD FIRMWARE VERSION	10.007	An attacker may use firmware changes to after the functionality of the asset, insert backdoors or disrupt normal operations.	behavior of the asset has changed.									
	NEW FIRMWARE VERSION	10.010											

## D.11.2 Build 2

#### D.11.2.1 Configuration

- Behavior Anomaly Detection: eyelnspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2
- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured to allow authorized users to access the PCS environment through the Dispel Enclave to the Dispel Wicket.

### D.11.2.2 Test Results

Figure D-104 shows the activities detected by Forescout as a result of firmware change. Figure D-104, Figure D-105 and Figure D-106 show more details on the alerts associated with the firmware update.

<) FORESCOUT	🚯 Dashboar	d 🚠 Network 📕	Events 🔊 Sensors 🕻	Settings								🖵 🧶 🏓	admin
Alerts	Reload Ex	port   v Aggregate	e details Create new case	Settings									? Help
In a given interval  On e given dey  Last X days  From date X to 30 days after  From date X to Y days before		5 alerts 10:30	10.35 10.40 10.35 10.40	10:45		10.50	10.55	11:00	11.05 11.1	0 11.15	11:20	11.25	11:30 11:30
Alert Filters	•	items selected											
Excluding event type ID     By monitored network		Timestamp 👻	Event name(s)	Sensor	Engine	Profile	Status	Severity	Source address	Destination address	Dest. Port	L7 Proto	Case ID
Excluding profile			0	(Not set 🖕	(Not 🖕	(Not set) 🖕	(Not set)	High, Ci 🖕	172.16.0.0/22	172.16.2.102	0	(Not set)	(Unessigns 🖕
Excluding dst MAC		Oct 15, 2020 11:14:42	Communication pattern no	sensor-b	Comm	8 - TCP com	Not analyzed	M Game	172.16.2.62	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
Excluding src IP		Oct 15, 2020 11:14:32	Communication pattern no	sensor-b	Comm	8 - TCP com	Not analyzed	M COM	172.16.2.62	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
Excluding dst IP		Oct 15, 2020 11:14:31	Communication pattern no	sensor-b	Comm	8 - TCP com	Not analyzed	M COM	172.16.2.62	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
Excluding dst port		Oct 15, 2020 11:11:55	Message type not whitelisted	sensor-b	Comm	8 - TCP com	Not analyzed	M COM	172.16.3.10 (fgs-476	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
By L3 protocol		Oct 15, 2020 11:11:52	(FEA Exit) Message type not	sensor-b	Comm	8 - TCP com	Not analyzed	M	172,16.3.10 (fgs-476	172.16.2.102 (plc te	44818 (TCP)	ETHIP	
By L4 protocol		Oct 15, 2020 11-10-52	(FEA Exit) Message type not	sensor-b	Comm	8. TCP com	Not analyzed		172 16 3 10 (fgs.476	172 16 2 102 (plc te	44818 (TCP)	ETHIP	
By upstream data		0 = 15, 2020 11, 10,00	THID controller cores come	seeses bui	la di sere	o ter conta	Networked		172 16 2 10 //m 176	172.16.2.102.(ale te	44919 (TCD)	ETHID	
By downstream data		00013,202011110.09	ETHIP CONDILIER RESEL COMMIL	sensorroo	industria.		Not analyzed		172.10.3.10 (189-476	172.10.2.102 (pic_be	44010 (TCP)	ETHIP	
By FEA type		Oct 15, 2020 11:10:07	Message type not whitelisted	sensor-b	Comm	8 - TCP com	Not analyzed	M	172.16.3.10 (fgs-476	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
By labels		Oct 15, 2020 11:09:37	(FEA Enter) Message type n	sensor-b	Comm	8 - TCP com	Not analyzed	M GER	172.16.3.10 (fgs-476	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
Excluding labels		Oct 15, 2020 11:09:36	ETHIP firmware update com	sensor-bu	Industr		Not analyzed	88880 H	172.16.3.10 (fgs-476	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
By vlan		Oct 15, 2020 11:09:36	Message type not whitelisted	sensor-b	Comm	8 - TCP com	Not analyzed	M (Table	172.16.3.10 (fgs-476	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
Excluding vlan		Oct 15, 2020 11:09:22	(FEA Enter) Message type n	sensor-b	Comm	8 - TCP com	Not analyzed	M CIT	172.16.3.10 (fgs-476	172.16.2.102 (plc_te	44818 (TCP)	ETHIP	
Li by detailed description	-											Copyright (C) 2005-2020	Porescout (v. 4.1.2)

Figure D-104 Forescout Detects a Collection of Alerts Associated with the Firmware Change

Figure D-105 Alert Details Detected by Forescout for the Firmware Change

Alert details Summary Alert ID 11 Timestamp D Sensor name is Detection engine in ID and name is Detection is Severity III	Back Edit Delete Show V Assign to a	ase Download ; ~ Source host info IP address Host name Other host names Host MAC addresses	172.163.10 (Private IP) (gg.47031ash) (gg.47031ash)	^	Alert details Command: Firmware update	Help
Summary Aker ID 11 Timestamp 0 Sensor name se Detection engère in Dand name in Description in Severity III	186671     166571     100 15,0200 11.0936     sansar-bundle-ncose     ndastrad finese litway (0TL)     It, papt public chip firmware update - ETHP firmware update     command	Source host info IP address Host name Other host names Host MAC addresses	172.163.10 (Private IP) fgg-470314ah fgg-470314ah	^	Alert details Command: Firmware update	^
Alert ID t Timestamp O Sensor name si Detection engine Ir ID and name detection Description O Severity	186671 Det 15, 2020 11:0936 Industrial Uhreat Blancy (TL) (Jugu Jobge, philip, formware, update - CTHP Formware update command	IP address Host name Other host names Host MAC addresses	172.16.3.10 (Private IP) fgr-47631ehh fgr-47631ehh.lan.lab		Command: Firmware update	
Timestamp 0 Sensor name se Detection engine in ID and name de Description of Severity	Dex 15, 2020 11:09:36 sensor-bundle-necose industrai fibrest library (TL) juga, pulsky _sthip_firmware_update - ETHIP firmware update command	Host name Other host names Host MAC addresses	fgs-47631ehh fgs-47631ehh.lan.lab		Development of the data of the	
Sensor name 9 Detection engine In ID and name di Description 0 Severity	sensor-bundle-nccoe industrial threat library (ITL) Itl_ops_pdop_ethip_firmware_update - ETHIP firmware update command	Other host names Host MAC addresses	fgs-47631ehhlan.lab		Destination route: module 4	
Detection engine ir ID and name id Description or Severity	industrial threat library (ITL) Itl_ops_pdop_ethip_firmware_update - ETHIP firmware update command	Host MAC addresses			Updated firmware revision: 3.4	
ID and name it cr Description or jun Severity	tt_ops_pdop_ethip_firmware_update - ETHIP firmware update command	These mine sourcestes	40:A8:F0:3D:48:AE (HewlettP)			
P Description 0; in Severity			Last seen: Oct 19, 2020 10:35:40 E4:90:69:3B:C2:C3 (Rockwell)			
Severity	Potentially dangerous ETHIP operation: the ETHIP master or an operator has requested a PLC to initiate a firmware update. This operation may be part of regular maintenance but can also be used in a other attack.	Other observed MAC addresses	E4:90:69:38-C2:C2 (Rockwell) E4:90:69:38:C2:C1 (Rockwell) 7C10E:CE:67:86:88 (Cisco) 7C10E:CE:67:86:83 (Cisco)			
	High	Role	EWS			
Source MAC 44	40:A8:F0:3D:48:AE (HewlettP)	Other roles	Windows workstation, Terminal server, Terminal client, Master			
Destination MAC E-	E4:90:69:38:C2:C0 (Rockwell)	Vendor and model	Rockwell			
Source IP 1	172.16.3.10 (fgs-47631ehh)		DCOM (TCP 135, 49155, 49159) DNS (TCP 53)			
Destination IP 1	172.16.2.102 (plc_tesim)		DNS (UDP 53, 5355)			
Source port 50	50753		ETHIP (TCP 44818) ETHIP (UDP 44818)			
Destination port 4	44818		FailedConnection (TCP 23, 80, 139, 1332, 8000, 8443)			
L2 proto Et	Ethernet		HTTP (TCP 8080, 8530) Kerberos (TCP 88)			
L3 proto IP	P		LDAP (TCP 389)			
L4 proto Tr	TCP	Client protocols	NTP (UDP 123)			
L7 proto E*	ETHIP		NetBIOS (UDP 137) NotAKnownOne (TCP 2500, 2501, 4444, 10005)			
Status N	Not analyzed		NatAKnownOne (UDP 1514)			
Labels			RDP (TCP 3389) SMB (TCP 445)			
User notes			SMB (UDP 138) SSDP (UDP 1390) SSH (TCP 22) SSL (TCP 443, 3389, 10003, 10005) Svalar (UDP 14)			
Name	^		DCOM (TCP 135, 6160) FailedConnection (TCP 139, 445, 11731)			

#### Figure D-106 ICS Patrol Scan Results Showing a Change Configuration was Made

Scan	details					3
Scar	ID	15	Started on	Oct 15, 2020 11:14:28		
Scar	n type	EtherNet/IP	Duration	01m37s		
Scar	n targets	172.16.2.102	Scan status	📀 Completed		
Scar	nning sensors	PCS_Sensor	Scanned IPs	1		
Scar	n policy		Responding hosts	1		
Initia	ated by	Admin User	Updated hosts	1		
0	) items selected				×	c
	Target IP 🔺	Scanning sensor	Scan status	Host status		
		OPCS_Sensor	(Not set)	(Not set)		•

#### Result

Result is not available.

## D.11.3 Build 3

### D.11.3.1 Configuration

- Remote Access: Cisco VPN
  - configured to allow authorized VPN users to access only the ConsoleWorks web interface
- User Authentication/User Authorization: ConsoleWorks
  - configured to allow remote access to hosts in manufacturing environment
- Behavior Anomaly Detection: Dragos
  - configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN

## D.11.3.2 Test Results

Dragos detects the change to the firmware as shown on the dashboard in Figure D-107with details shown in Figure D-108.

Figure D-107 Dragos Dashboard Showing an Alert for Firmware Change



#### Figure D-108 Details for Firmware Change Alert

DETECTION	N INFORMATION		ASSOCIATED ASSETS		C
WHAT HAPPED	DNED: 1. Targethic by Station 2 on Award 3175		View T Type T 10 T Name	: Dz. : 197.168.1.107 offer	0
OCCUPRED AT 04/25/21, 12:14 00/00/17:	π: lore	LAST GEDI: e429421.1514.000 STATE	COMMUNICATIONS SUDMARY		
1 DETECTED BY OSBIT BUTTON O Modeling	f: ane Notification DFD DEARDs	UNRESCONS BCURCE: In Tox Lond ZORES: OR Lond	No Demonstrations Summary.		
ACTIVITY GRO MITRE ATT&C	OUP: CK TACTIC:	ICS CYBER KILLCHAIN STEP: MITHE ATTACK TECHNIQUE:			
, famote Cade En	NEODOTAGETS:	NOTIFICATION RECORD: View in display			
No Associated P CASES: No Cases Lavier	Aptools d	No. Accounter Company Its			0
RELATED N	NOTIFICATIONS				
n :	Coourred At 2		Sammary	:	
			No Retack Notifications.		TECTED
		prior or plots		PAT DECORAGE MENT LAST	

## D.11.4 Build 4

## D.11.4.1 Configuration

- Behavior Anomaly Detection: Azure Defender for IoT
  - configured to receive packet streams from the DMZ, Testbed LAN, Supervisory LAN, and Control LAN
- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured as the engineering workstation to connect through the Dispel Enclave to the Dispel Wicket to manage the Beckhoff PLC.

## D.11.4.2 Test Results

Azure Defender for IoT alerts on the firmware update as shown below in Figure D-109.

Figure D-109 Azure Defender for IoT Alert Showing a Version Mismatch in the Firmware Build

Hicrosoft	÷	Alerts			e
		Free Search Q G Adv		☐ □ ∓ × Main View + ● Except All 4	forts
			Version Build Mismatch		
		Important Alerts (72)	Policy Violation   Jan 6, 2021 2:00:37 PM ( just now ) The PLC Version Build was not the expected result		
		POLICY Unauthorized Internet Co	The PEC version band was not the expected result	No Alerts	
		VIOLATION An asset defined in your intent			
Alerts (72)	۰	POLICY Unauthorized Internet Co VIOLATION An asset defined in your intern			
		POLICY Unauthorized Internet Co VIOLATION An asset defined in your internet	Supervisory En PLC We	yineering vikstation	
ANALYSIS		POLICY Unauthorized Internet Co	M		
Event Timeline	Ê	VIOLATION An auset defined in your intern	Manage this Event	a provision meteori aluaia. If	
Data Mining		VIOLATION An asset defined in your intern	<ul> <li>mas is a Horizon custom aren that provides information resolved by required, contact your security administrator for more details.</li> </ul>	a proprietary protocol plugin. In	
		POLICY Unauthorized Internet Co VIOLATION An accest defined in your intern			
Risk Assessment		POLICY Unauthorized Internet Co		Acknowledge	10
Attack Vectors		VIOLATION An easet defined in your intern		POLICY Version Build Mismatch	-
ADMINISTRATION		VIOLATION An asset defined in your internal a	nectivity Detected [1] month ago retwork is communicating with addresses on the Internet. These addresses have not been les	VIOLATION The PLC Version Build was not the expected result.	
		POLICY Unauthorized Internet Con VIOLATION An accest defined in your internet	nectivity Detected   1 month ago where is communicating with addresses on the Internet. These addresses have not been lea	OPERATIONAL Device is Suspected to be Disconnected (Unresponsive) Jan 6 13:50 Device 197, THE 0.30 is suspected to be disconnected (corresponsive).	В
Users		POLICY Unauthorized Internet Con VIOLATION An exercit defined in your internet	nectivity Detected   1 month ago	OPERATIONAL Suspicion of Unresponsive MODBUS Device Jan 6 13:50 Distribution device 192:168.8.30 (Protocol Address 255) seems to be unresponsive to MODBUS requests.	¥.
Forwarding		POLICY Unauthorized Internet Con	nectivity Detected   1 month ago	OPERATIONAL HTTP Client Error Jan 6 13:2	
System Settings		VIOLATION An esset defined in your internal of	setwork is communicating with addresses on the internet. These addresses have not been lea	An HTTP chert sent an invalid request to a server. Chert Tu 100.0.25 sent an invalid request to server 30.700.0.0.	
		POLICY Unauthorized Internet Con VIOLATION An assist defined in your internal of	nectivity Detected ( 1 month ago retwork is communicating with addresses on the Internet. These addresses have not feen its	VIOLATION An esset defined in your internet externet is communicating with addresses on the Internet. These addresses how	
SUPPORT		POLICY Unauthorized Internet Con VIOLATION An sesset defined in your internal in	nectivity Detected 11 month ego servers is communicating with addresses on the Internet. Three addresses have not been lea.	OPERATIONAL Device 19 Suspected to be Disconnected (Unresponsive) Device 192.168.0.98 in suspected to be disconnected (unresponsive).	5
Horizon					
Support					
Azure Defender for Version 3.1.1	loT				

# Appendix E Benefits of IoT Cybersecurity Capabilities

The National Institute of Standards and Technology's (NIST's) Cybersecurity for the Internet of Things (IoT) program supports development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

Cyber-physical components, including sensors and actuators, are being designed, developed, deployed, and integrated into networks at an ever-increasing pace. Many of these components are connected to the internet. IoT devices combine network connectivity with the ability to sense or affect the physical world. Stakeholders face additional challenges with applying cybersecurity controls as cyber-physical devices are further integrated.

NIST's Cybersecurity for IoT program has defined a set of device cybersecurity capabilities that device manufacturers should consider integrating into their IoT devices and that consumers should consider enabling/configuring in those devices. Device cybersecurity capabilities are cybersecurity features or functions that IoT devices or other system components (e.g., a gateway, proxy, IoT platform) provide through technical means (e.g., device hardware and software). Many IoT devices have limited processing and data storage capabilities and may not be able to provide these device cybersecurity capabilities on their own; instead, they may rely on other system components to provide these technical capabilities on their behalf. Nontechnical supporting capabilities are actions that a manufacturer or third-party organization performs in support of the cybersecurity of an IoT device. Examples of nontechnical support include providing information about software updates, instructions for configuration settings, and supply chain information.

Used together, device cybersecurity capabilities and nontechnical supporting capabilities can help mitigate cybersecurity risks related to the use of IoT devices while assisting customers in achieving their goals. If IoT devices are integrated into industrial control system (ICS) environments, device cybersecurity capabilities and nontechnical supporting capabilities can assist in securing the ICS environment.

## E.1 Device Capabilities Mapping

<u>Table E-1</u> lists device cybersecurity capabilities and nontechnical supporting capabilities as they map to the NIST *Cybersecurity Framework* Subcategories of particular importance to this project. It is acknowledged that IoT devices vary in their capabilities, and there may not be a clear delineation between the device cybersecurity capabilities that are provided by the IoT devices and those provided by another system component. It is also understood that the capabilities of cyber-physical components are evolving, so many of the mappings are not necessarily exact.

In this project, the focus was on the engineering workstations and not on the manufacturing components. The mapping presented in <u>Table E-1</u> is a summary of both technical and nontechnical capabilities that would enhance the security of a manufacturing environment. It is acknowledged that many of the device cybersecurity capabilities may not be available in modern sensors and actuators and that other system elements (e.g., proxies, gateways) or other risk mitigation strategies (e.g., network segmentation) may be necessary.

 Table E-1 Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities to

 NIST Cybersecurity Framework Subcategories of the ICS Project

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
Subcategory PR.AC-1: Identi- ties and creden- tials are issued, managed, veri- fied, revoked, and audited for authorized de- vices, users, and processes.	<ul> <li>Ability to uniquely identify the loT device logically.</li> <li>Ability to uniquely identify a remote loT device.</li> <li>Ability for the device to support a unique device ID.</li> <li>Ability to configure loT device access control policies using loT device identity.</li> <li>Ability to verify the identity of an loT device.</li> <li>Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.</li> <li>Ability to set and change authentication configurations, policies, and limitations settings for the loT device.</li> <li>Ability to create unique loT device user accounts.</li> <li>Ability to identify unique loT device user accounts.</li> </ul>	<ul> <li>Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.</li> <li>Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.</li> <li>Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.</li> <li>Providing the details necessary to require unique identifiers for each IoT device associated with the system components within which it is used.</li> </ul>	Rev. 5 AC-2 IA-2 IA-5 IA-8 IA-12
	organizationally defined	and critical system	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>accounts that support privileged roles with automated expiration conditions.</li> <li>Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface.</li> <li>Ability to enable automation and reporting of account management activities.</li> <li>Ability to establish conditions for shared/group accounts on the IoT device.</li> <li>Ability to administer conditions for shared/group accounts on the IoT device.</li> <li>Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.</li> </ul>	<ul> <li>components within which it is used.</li> <li>Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources.</li> <li>Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.</li> <li>Providing education explaining how to enforce authorized access at the system level.</li> </ul>	
PR.AC-3: Re- mote access is managed.	<ul> <li>Ability to configure IoT device access control policies using IoT device identity.</li> <li>Ability for the IoT device to differentiate between authorized and unauthorized remote users.</li> <li>Ability to authenticate external users and systems.</li> <li>Ability to securely interact with authorized external, third-party systems.</li> </ul>	N/A	AC-17 AC-19 AC-20

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>Ability to identify when an external system meets the required security requirements for a connection.</li> </ul>		
	<ul> <li>Ability to establish secure communications with internal systems when the device is operating on external networks.</li> </ul>		
	<ul> <li>Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including:</li> </ul>		
	<ul> <li>usage restrictions</li> </ul>		
	<ul> <li>configuration requirements</li> </ul>		
	connection requirements		
	<ul> <li>manufacturer established requirement</li> </ul>		
	<ul> <li>Ability to enforce the established local and remote access requirements.</li> </ul>		
	<ul> <li>Ability to prevent external access to the IoT device management interface.</li> </ul>		
	<ul> <li>Ability to control the IoT device's logical interface (e.g., locally or remotely).</li> </ul>		
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>		
	<ul> <li>Ability to detect remote activation of sensors.</li> </ul>		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	<ul> <li>Ability to assign roles to IoT device user accounts.</li> <li>Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary).</li> <li>Ability to establish user accounts to support role-based logical access privileges.</li> </ul>	<ul> <li>Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.</li> <li>Providing details about the specific types of manufacturer's needs to access the IoT device interfaces, such as for specific support undated consists</li> </ul>	AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24
	<ul> <li>Ability to administer user accounts to support role- based logical access privileges.</li> <li>Ability to use organizationally defined roles to define each user account's access and permitted device actions.</li> <li>Ability to support multiple levels of user/process account functionality and roles for the IoT device.</li> </ul>	<ul> <li>support, updates, ongoing maintenance, and other purposes.</li> <li>Providing documentation with instructions for the IoT device customer to follow for how to restrict interface connections that enable specific activities.</li> <li>Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis.</li> </ul>	
	<ul> <li>Ability to apply least privilege to user accounts.</li> <li>Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege.</li> <li>Ability to apply least privilege settings within</li> </ul>	<ul> <li>Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis.</li> <li>Providing documentation and/or other communications describing how to implement management and operational</li> </ul>	

<i>Cybersecurity</i> <i>tramework</i> v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions).</li> <li>Ability to limit access to privileged device settings that are used to establish and administer authorization requirements.</li> </ul>	<ul> <li>controls to protect data         obtained from IoT devices and         associated systems from         unauthorized access,         modification, and deletion.</li> <li>Providing a detailed         description of the other types         of devices and systems that         will access the IoT device         during customer use of the         device, and how they will         access it.</li> </ul>	
	<ul> <li>Ability for authorized users to access privileged settings.</li> <li>Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions.</li> <li>Ability to enable automation and reporting of account management activities.</li> <li>Ability to establish conditions for shared/group accounts on</li> </ul>	<ul> <li>Providing communications and detailed instructions for implementing a hierarchy of privilege levels to use with the IoT device and/or necessary associated information systems.</li> <li>Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.</li> </ul>	
	<ul> <li>the IoT device.</li> <li>Ability to administer conditions for shared/group accounts on the IoT device.</li> <li>Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.</li> </ul>	<ul> <li>Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources.</li> <li>Providing education explaining how to control access to IoT devices</li> </ul>	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on:         <ul> <li>run-time access control decisions facilitated by dynamic privilege management.</li> <li>organizationally defined actions to access/use device.</li> </ul> </li> <li>Ability to allow information sharing capabilities based upon the type and/or role of the user attempting to share the information.</li> <li>Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization.</li> <li>Ability to restrict updating actions to authorized entities.</li> <li>Ability to restrict access to the cybersecurity state indicator to authorized entities.</li> </ul>	<ul> <li>implemented within IoT device customer information systems.</li> <li>Providing education explaining how to enforce authorized access at the system level.</li> <li>Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that communicate or interface with the device.</li> <li>Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device.</li> <li>Providing education and supporting materials for how to establish roles to support IoT device policies, procedures, and associated documentation.</li> </ul>	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-fac- tor, multi-fac- tor) commensu- rate with the risk of the trans- action (e.g., in- dividuals' secu- rity and privacy risks and other organizational risks).	<ul> <li>Ability for the IoT device to require authentication prior to connecting to the device.</li> <li>Ability for the IoT device to support a second, or more, authentication method(s) such as:         <ul> <li>temporary passwords or other one-use log-on credentials</li> <li>third-party credential checks</li> <li>biometrics</li> <li>hard tokens</li> </ul> </li> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul> <li>Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.</li> <li>Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.</li> <li>Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.</li> </ul>	AC-7 AC-8 AC-9 AC-12 AC-14 IA-2 IA-3 IA-4 IA-5 IA-8 IA-11
PR.DS-1: Data- at-rest is pro- tected.	<ul> <li>Ability to execute cryptographic mechanisms of appropriate strength and performance.</li> <li>Ability to obtain and validate certificates.</li> <li>Ability to perform authenticated encryption algorithms.</li> <li>Ability to change keys securely.</li> <li>Ability to generate key pairs.</li> </ul>	<ul> <li>Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device.</li> <li>Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet</li> </ul>	SC-28 MP-2 MP-4 MP-5

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>Ability to store encryption keys securely.</li> </ul>	requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies	
	<ul> <li>Ability to cryptographically store passwords at rest, as wel as device identity and other authentication data.</li> </ul>		
	<ul> <li>Ability to support data encryption and signing to prevent data from being altered in device storage.</li> </ul>	regulations, standards, and other legal requirements.	
	<ul> <li>Ability to secure data stored locally on the device.</li> </ul>		
	<ul> <li>Ability to secure data stored in remote storage areas (e.g., cloud, server).</li> </ul>		
	<ul> <li>Ability to utilize separate storage partitions for system and user data.</li> </ul>		
	<ul> <li>Ability to protect the audit information through mechanisms such as:</li> </ul>		
	<ul> <li>encryption</li> </ul>		
	<ul> <li>digitally signing audit files</li> </ul>		
	<ul> <li>securely sending audit files to another device</li> </ul>		
	<ul> <li>other protections created by the device manufacturer</li> </ul>		
PR.DS-6: Integ- rity checking mechanisms are	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity</li> </ul>	<ul> <li>Providing documentation</li> </ul>	SC-16
		and/or other communications	SI-7
used to verify software, firm-	on for device identity.	management and operational controls to protect data	MP-4

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
ware, and infor- mation integ- rity.	<ul> <li>Ability to verify digital signatures.</li> <li>Ability to run hashing algorithms.</li> <li>Ability to perform authenticated encryption algorithms.</li> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>Ability to verify and authenticate any update before installing it.</li> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul> <li>obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>	MP-5

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manuf	acturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
PR.IP-4: Backups of information are conducted, maintained, and tested.	; N/A	-	Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary.	CP-4 CP-9
			Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.	
			Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.	
PR.MA-1: Maintenance and repair of or- ganizational as- sets are per- formed and logged, with ap- proved and con- trolled tools.	N/A	•	Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home.	MA-2 MA-3 MA-5 MA-6
		-	Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.	
Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support-	NIST SP 800-53 Rev. 5	
--	-----------------------------------	--	-----------------------------	
		<ul> <li>Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used.</li> </ul>		
		<ul> <li>Providing the details necessary for IoT device customers to implement only organizationally approved IoT device diagnostic tools within their system.</li> </ul>		
		<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>		
		<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>		
		<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> </ul>		
		<ul> <li>Providing communications and comprehensive documentation describing</li> </ul>		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
		maintenance operations that the IoT device customer is required to perform. If such comprehensive IoT device maintenance operations documentation does not exist, the manufacturer should clearly communicate to IoT device customers that the user must perform these operations themselves.	
		<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>	
		<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>	
		<ul> <li>Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> </ul>	
		<ul> <li>Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel.</li> </ul>	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
		<ul> <li>Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.</li> </ul>	
		<ul> <li>Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow.</li> </ul>	
		<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>	
		<ul> <li>Providing the details necessary for customers to document attempts to obtain IoT device components or IoT device information system service documentation when such documentation is either unavailable or nonexistent, and documenting the appropriate response for manufacturer employees, or</li> </ul>	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
		supporting entities, to follow.	
		<ul> <li>Providing a process for IoT device customers to contact the manufacturer to ask questions or obtain help related to the IoT device configuration settings.</li> </ul>	
		<ul> <li>Providing information to allow for in-house support from within the IoT device customer organization.</li> </ul>	
		<ul> <li>Providing education explaining how to inspect IoT device and/or use maintenance tools to ensure the latest software updates and patches are installed.</li> </ul>	
		<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>	
		<ul> <li>Providing education that explains the legal requirements governing IoT device maintenance responsibilities or how to meet specific types of legal requirements when using the IoT device.</li> </ul>	

<i>Cybersecurity Framework</i> v1.1 Subcategory	Device Cybersecurity Capabilities	Manufactu i	rer Nontechnical Support- ng Capabilities	NIST SP 800-53 Rev. 5
PR.MA-2: Re- mote mainte- nance of organi- zational assets is approved, logged, and per- formed in a manner that prevents unau- thorized access	N/A	<ul> <li>Provide type</li> <li>trigg</li> <li>mai</li> <li>requide the</li> <li>ecosi</li> <li>indi</li> </ul>	viding details about the es of, and situations that ger, local and/or remote ntenance activities uired once the device is chased and deployed in organization's digital system or within an vidual consumer's home.	MA-4
		<ul> <li>Providect</li> <li>physicapt</li> <li>capt</li> <li>loT</li> <li>type</li> </ul>	viding instructions and umentation describing the sical and logical access abilities necessary to the device to perform each e of maintenance activity.	
		<ul> <li>Provand</li> <li>physics</li> <li>secult</li> <li>base</li> <li>use,</li> <li>control</li> <li>the</li> <li>with</li> <li>inte</li> </ul>	viding other information actions as necessary for sically securing, and urely using, the IoT device ed upon the IoT device purpose, and other textual factors related to digital ecosystem(s) nin which they are nded to be used.	
		<ul> <li>Provinst</li> <li>necome mai</li> </ul>	viding the details and ructions to perform essary IoT device ntenance activities and airs.	
		<ul> <li>Provand</li> <li>doc</li> <li>loT</li> <li>ope</li> <li>mar</li> </ul>	viding communications comprehensive umentation describing the device maintenance rations performed by the nufacturer and the	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Sup ing Capabilities	port- NIST SP 800-53 Rev. 5
		manufacturer's supportinentities.	ng
		<ul> <li>Providing communication and documentation deta how to perform recommended local and/ remote maintenance activities.</li> </ul>	ns iling ′or
		<ul> <li>Providing the details necessary to enable IoT device customers to mor onsite and offsite IoT dev maintenance activities.</li> </ul>	iitor /ice
		<ul> <li>Providing the details necessary for maintaining records for nonlocal IoT device maintenance and diagnostic activities.</li> </ul>	g
		<ul> <li>Providing the details necessary to implement management and operat controls for IoT device maintenance personnel a associated authorization and record-keeping of maintenance organizatio and personnel.</li> </ul>	ional and s, ins
		<ul> <li>Providing communication describing the type and nature of the local and/or remote maintenance activities that will involve require manufacturer personnel, or their contractors, once the devisi is purchased and deployed</li> </ul>	ns or e and vice ed in

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
		the IoT device customer's organization.	
		<ul> <li>Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow.</li> </ul>	
		<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>	
DE.AE-1: A base- line of network operations and expected data flows for users and systems is established and managed.	N/A	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> </ul>	AC-4 CA-3 CM-2 SI-4
DE.AE-2: De- tected events are analyzed to understand at- tack targets and methods.	N/A	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>	AU-6 CA-7 IR-4 SI-4
DE.AE-3: Event data are col- lected and cor- related from multiple sources and sensors.	<ul> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing</li> </ul>	<ul> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> </ul>	AU-6 AU-12 CA-7 IR-4 IR-5 SI-4

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	NIST SP 800-53 Rev. 5
	information can be checked to allow for review, analysis, and reporting).		
	<ul> <li>Ability to keep an accurate internal system time.</li> </ul>		
DE.CM-1: The information sys- tem and assets are monitored to identify cy- bersecurity events and ver- ify the effective- ness of protec- tive measures.	<ul> <li>Ability to monitor specific actions based on the IoT device identity.</li> <li>Ability to access information about the IoT device's cybersecurity state and other necessary data.</li> <li>Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.</li> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check).</li> <li>Ability to monitor communications traffic.</li> </ul>	<ul> <li>Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information.</li> <li>Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools.</li> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> <li>Providing documentation describing how to perform monitoring activities.</li> </ul>	AU-12 CA-7 CM-3 SC-7 SI-4
DE.CM-3: Per- sonnel activity is monitored to detect potential cybersecurity events.	N/A	N/A	AC-2 AU-12 CA-7 CM-3 SC-5 SC-7

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Support- ing Capabilities	T SP 0-53 v. 5
DE.CM-7: Moni-	<ul> <li>Ability to support a monitoring</li> </ul>	<ul> <li>Providing appropriate tools,</li> </ul>	2
toring for unau- thorized person- nel, connec- tions, devices, and software is performed.	process to check for disclosure of organizational information to unauthorized entities. (The	assistance, instructions, or AU- other details describing the AU- capabilities for monitoring the CA-7	12 13 7
	this check itself or provide the information necessary for an external process to check).	device customer to report actions to the monitoring service of the manufacturer's	·10 ·11
	<ul> <li>Ability to monitor changes to the configuration settings.</li> </ul>	<ul><li>supporting entity.</li><li>Providing the details</li></ul>	
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>	necessary to monitor IoT devices and associated systems.	
	<ul> <li>Ability to detect remote activation of sensors.</li> </ul>	<ul> <li>Providing documentation describing details necessary</li> </ul>	
	<ul> <li>Ability to take organizationally defined actions when unauthorized hardware and</li> </ul>	to identify unauthorized use of IoT devices and their associated systems.	
	software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>	

## E.2 Device Capabilities Supporting Functional Test Scenarios

In this project, the focus was on the engineering workstations and not on the manufacturing components. It is acknowledged that many of the **device cybersecurity capabilities** may not be available in modern sensors and actuators and that other system elements (e.g., proxies, gateways) or other risk mitigation strategies (e.g., network segmentation) may be necessary.

<u>Table E-2</u> builds on the functional test scenarios included in <u>Section 5</u> of this document. The table lists both **device cybersecurity capabilities** and **nontechnical supporting capabilities** that map to relevant *Cybersecurity Framework* Subcategories for each of the functional test scenarios. If IoT devices are integrated into future efforts or a production ICS environment, selecting devices and/or third parties that provide these capabilities can help achieve the respective functional requirements.

It is acknowledged that IoT devices vary in their capabilities, and there may not be a clear delineation between **the device cybersecurity capabilities** that are provided by the IoT devices and those provided by another system component. It is also understood that the capabilities of cyber-physical components are evolving, so many of the mappings are not necessarily exact.

In this project, the focus was on the engineering workstations and not on the manufacturing components. It is acknowledged that many of the **device cybersecurity capabilities** may not be available in modern sensors and actuators and that other system elements (e.g., proxies, gateways) or other risk mitigation strategies (e.g., network segmentation) may be necessary.

Table E-2 Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities that Map to Each of the Functional Test Scenarios

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
Scenario 1: Protect Host from Mal- ware via USB: This test will demon- strate blocking the introduction of malware through physical access to a workstation within the manufacturing system. PR.DS-6 PR.MA-2 DE.AE-2	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital signatures.</li> <li>Ability to run hashing algorithms.</li> <li>Ability to perform authenticated encryption algorithms.</li> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT</li> </ul>
	<ul> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures.</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>checksums, certificate validation).</li> <li>Ability to verify and authenticate any update before installing it.</li> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> <li>Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
Scenario 2: Protect Host from Mal- ware via Network Vector This test will demonstrate the	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital signatures.</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
detection of mal- ware introduction from the network. <b>PR.DS-6</b>	<ul> <li>Ability to run hashing algorithms.</li> <li>Ability to perform authenticated encryption algorithms.</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary</li> </ul>
DE.AE-1 DE.AE-2	<ul> <li>Ability to compute and compare hashes.</li> </ul>	to support secure implementation of the IoT device and associated systems data integrity controls.
DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7	<ul> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> </ul>	<ul> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> </ul>
	<ul> <li>Ability to validate the integrity of data transmitted.</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data</li> </ul>
	<ul> <li>Ability to verify software undates come from valid</li> </ul>	integrity.
	sources by using an effective method (e.g., digital signatures, checksums, certificate	<ul> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> </ul>
	validation).	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
	<ul> <li>Ability to store the operating environment (e.g., firmware image, software, applications)</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance</li> </ul>

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	in read-only media (e.g., Read Only Memory).	operations performed by the manufacturer and the manufacturer's supporting entities.
	<ul> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to send requested audit</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>
<ul> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> </ul>	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>	
	information can be checked to allow for review, analysis, and reporting).	<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>
	<ul> <li>Ability to keep an accurate internal system time.</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>
	<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information</li> </ul>	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
	<ul> <li>Ability to monitor changes to the configuration settings</li> </ul>	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> </ul>
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
	<ul> <li>Ability to detect remote activation of sensors.</li> </ul>	<ul> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the</li> </ul>
	<ul> <li>Ability to take organizationally defined actions when</li> </ul>	IoT device.

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	<ul> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> </ul>
		<ul> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> </ul>
		<ul> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> </ul>
		<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
Scenario 3: Protect Host from Mal- ware via Remote Access Connec- tions: This test will demonstrate block- ing malware at- tempting to infect manufacturing sys- tem through au- thorized remote access connec-	<ul> <li>Ability to uniquely identify the loT device logically.</li> <li>Ability to uniquely identify a remote loT device.</li> <li>Ability for the device to support a unique device ID.</li> <li>Ability to configure loT device access control policies using loT device identity.</li> <li>Ability to verify the identity of an loT device.</li> </ul>	<ul> <li>Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.</li> <li>Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.</li> <li>Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.</li> </ul>

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
PR.AC-1 PR.AC-3 PR.AC-4 PR.AC-7 PR.MA-1 PR.MA-2 DE.CM-3 DE.CM-7	<ul> <li>Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.</li> <li>Ability to set and change authentication configurations, policies, and limitations settings for the IoT device.</li> <li>Ability to revoke access to the device.</li> </ul>	<ul> <li>Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.</li> <li>Providing details about the specific types of manufacturer's needs to access the IoT device interfaces, such as for specific support, updates, ongoing maintenance, and other purposes.</li> <li>Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.</li> </ul>
	<ul> <li>Ability to create unique IoT device user accounts.</li> <li>Ability to identify unique IoT device user accounts.</li> <li>Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions.</li> <li>Ability to configure IoT device access control policies using IoT device identity.</li> <li>Ability to authenticate external users and systems.</li> </ul>	<ul> <li>Providing education explaining how to enforce authorized access at the system level.</li> <li>Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.</li> <li>Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.</li> <li>Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.</li> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to securely interact with authorized external, third-party systems.</li> <li>Ability to identify when an external system meets the required security requirements for a connection.</li> <li>Ability to establish secure communications with internal</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>
	<ul> <li>systems when the device is operating on external networks.</li> <li>Ability to establish requirements for remote access to the IoT device and/or IoT device interface.</li> </ul>	<ul> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> </ul>
	<ul> <li>Ability to enforce the established local and remote access requirements.</li> <li>Ability to prevent external access to the IoT device management interface.</li> </ul>	<ul> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
	<ul> <li>Ability to assign roles to IoT device user accounts.</li> </ul>	

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to support a hierarchy of logical access privileges for the IoT device based on roles.</li> </ul>	
	<ul> <li>Ability to apply least privilege to user accounts.</li> </ul>	
	<ul> <li>Ability to enable automation and reporting of account management activities.</li> </ul>	
	<ul> <li>Ability for the IoT device to require authentication prior to connecting to the device.</li> </ul>	
	<ul> <li>Ability for the IoT device to support a second, or more, authentication method(s).</li> </ul>	
	<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> </ul>	
	<ul> <li>Ability to monitor changes to the configuration settings.</li> </ul>	
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>	
	<ul> <li>Ability to detect remote activation of sensors.</li> </ul>	

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	
Scenario 4: Protect Host from Unau- thorized Applica- tion Installation: This test will	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion</li> </ul>
This test will demonstrate block- ing the installation and execution of unauthorized appli- cations on work- station in the man- ufacturing system Ability to verify digital signatures.and deletion Ability to run hashing algorithms Ability to run hashing algorithms Providing communications to describing how to implement controls to protect IoT device systems data integrity Ability to perform algorithms Ability to perform authenticated encryption algorithms Providing IoT device custome to support secure implement	<ul> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and</li> </ul>	
PR.DS-6 PR.MA-1 DE.AE-1 DE.AE-2 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7	<ul> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> </ul>	<ul> <li>associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>Ability to verify and authenticate any update before installing it.</li> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>Providing documented descriptions of the specific</li> </ul>
		maintenance procedures for defined maintenance tasks.

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to keep an accurate internal system time.</li> </ul>	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
	<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>Ability to monitor changes to the configuration settings.</li> </ul>	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
	<ul> <li>Ability to detect remote activation attempts.</li> <li>Ability to detect remote</li> </ul>	<ul> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> </ul>
	<ul> <li>Ability to detect remote activation of sensors.</li> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are</li> </ul>	<ul> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> </ul>
	detected (e.g., disallow a flash drive to be connected even if a	<ul> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> </ul>
	Universal Serial Bus [USB] port is present).	<ul> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> </ul>
		<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
Scenario 5: Protect from Unauthorized Addition of a De- vice: This test will demonstrate the detection of an un- authorized device connecting to the manufacturing sys- tem. PR.DS-6 PR.MA-1 DE.AE-1 DE.AE-1 DE.AE-2 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital signatures.</li> <li>Ability to run hashing algorithms.</li> <li>Ability to perform authenticated encryption algorithms.</li> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device data integrity.</li> </ul>
	<ul> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to verify and authenticate any update</li> </ul>	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul><li>before installing it.</li><li>Ability to store the operating</li></ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
	environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> </ul>
	<ul> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to send requested audit</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform</li> </ul>
Pro	logs to an external audit process or information system (e.g., where its auditing information can be checked to	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>
	<ul> <li>Information can be checked to allow for review, analysis, and reporting).</li> <li>Ability to keep an accurate internal system time.</li> <li>Ability to support a monitoring process to check for disclosure of organizational information</li> </ul>	<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities</li> </ul>
		<ul> <li>Providing documented descriptions of the specific</li> <li>maintenance accordures for defined maintenance tasks</li> </ul>
		<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
	<ul><li>to unauthorized entities.</li><li>Ability to monitor changes to the configuration settings.</li></ul>	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to detect remote activation attempts.</li> <li>Ability to detect remote activation of sensors.</li> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
Scenario 6: Detect Unauthorized De- vice-to-Device Communications: This test will demonstrate the detection of unau-	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital signatures.</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
thorized communi- cations between	<ul> <li>Ability to run hashing algorithms.</li> </ul>	controls to protect IoT device data integrity and associated systems data integrity.
devices. PR.DS-6 PR.MA-1	<ul> <li>Ability to perform authenticated encryption algorithms.</li> </ul>	<ul> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> </ul>
PR.MA-1 DE.AE-1 DE.AE-2 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7	<ul> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation)</li> </ul>	<ul> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul> <li>Ability to verify and authenticate any update before installing it.</li> <li>Ability to store the operating anvironment (e.g. firmware)</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary loT device maintenance activities and repairs.</li> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> </ul>
	image, software, applications)	

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	in read-only media (e.g., Read Only Memory).	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>
	<ul> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to conduct requested audit</li> </ul>	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system</li> </ul>
	<ul> <li>Ability to send requested audit logs to an external audit</li> </ul>	reviews and/or maintenance by the manufacturer.
	process or information system (e.g., where its auditing information can be checked to	<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>
	allow for review, analysis, and reporting).	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>
	<ul> <li>Ability to keep an accurate internal system time.</li> </ul>	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>Ability to monitor changes to the configuration settings.</li> <li>Providing documentation de indicators that could occur launched.</li> </ul>	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> </ul>	
	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>	
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>	<ul> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the</li> </ul>
	<ul> <li>Ability to detect remote activation of sensors.</li> </ul>	IoT device.
	<ul> <li>Ability to take organizationally defined actions when</li> </ul>	<ul> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	<ul> <li>actions to the monitoring service of the manufacturer's supporting entity.</li> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>Providing documentation that describes indicators of</li> </ul>
Scenario 7: Protect from Unauthorized Modification and Deletion of Files:	<ul> <li>Ability to execute cryptographic mechanisms of appropriate strength and performance.</li> </ul>	<ul> <li>Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device.</li> </ul>
This test will demonstrate pro- tection of files from unauthorized deletion both lo- cally and on net- work file share. PR.DS-1 PR.DS-6	<ul> <li>Ability to obtain and validate certificates.</li> <li>Ability to change keys securely.</li> <li>Ability to generate key pairs.</li> <li>Ability to store encryption keys securely.</li> <li>Ability to cryptographically.</li> </ul>	<ul> <li>Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.</li> <li>Providing documentation and/or other communications describing how to implement management and operational</li> </ul>
PR.IP-4 PR.MA-1 DE.AE-2	<ul> <li>Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.</li> </ul>	controls to protect data obtained from IoT devices and associated systems from unauthorized access, modificatio and deletion.

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to support data encryption and signing to prevent data from being altered in device storage.</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> </ul>
	<ul> <li>Ability to secure data stored locally on the device.</li> <li>Ability to secure data stored in</li> </ul>	<ul> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> </ul>
	remote storage areas (e.g., cloud, server).	<ul> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> </ul>
	<ul> <li>Ability to utilize separate storage partitions for system and user data.</li> </ul>	
	<ul> <li>Ability to protect the audit information through mechanisms such as:</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>
	<ul><li>encryption</li><li>digitally signing audit files</li></ul>	<ul> <li>Providing education to IoT device customers covering the instructions and details necessary for them to create</li> </ul>
	<ul> <li>securely sending audit files to another device</li> <li>accurate backups and to recover the backups wh necessary.</li> </ul>	accurate backups and to recover the backups when necessary.
	<ul> <li>other protections created by the device manufacturer</li> </ul>	<ul> <li>Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.</li> </ul>
	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> </ul>	<ul> <li>Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to verify digital signatures.</li> </ul>	webinar) for various aspects involved with backing up the IoT device data.
	<ul> <li>Ability to run hashing algorithms.</li> </ul>	<ul> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT dovise to perform each type of maintenance activity.</li> </ul>
	<ul> <li>Ability to perform authenticated encryption algorithms.</li> </ul>	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul> <li>Ability to compute and compare hashes.</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
	<ul> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> </ul>
	<ul><li>modification.</li><li>Ability to validate the integrity of data transmitted.</li></ul>	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>
	<ul> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> </ul>	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>
		<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>
	<ul> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
Scenario 8: Detect Unauthorized Modification of PLC Logic:	<ul> <li>Ability to configure IoT device access control policies using IoT device identity.</li> </ul>	<ul> <li>Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.</li> </ul>
PLC Logic: This test will demonstrate the detection of PLC logic modification. PR.AC-3 PR.AC-7 PR.DS-6 PR.MA-1 PR.MA-2 DE.AE-1 DE.AE-1 DE.AE-2 DE.AE-3	<ul> <li>Ability to authenticate external users and systems.</li> <li>Ability to securely interact with</li> </ul>	<ul> <li>Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.</li> </ul>
	<ul> <li>Ability to securely interact with authorized external, third-party systems.</li> <li>Ability to identify when an external system meets the</li> </ul>	<ul> <li>Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.</li> </ul>
	<ul> <li>external system meets the required security requirements for a connection.</li> <li>Ability to establish secure communications with internal systems when the device is</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> </ul>
DE.CM-1 DE.CM-3 DE.CM-7	<ul> <li>operating on external networks.</li> <li>Ability to establish requirements for remote</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> </ul>

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul><li>access to the IoT device and/or</li><li>IoT device interface.</li><li>Ability to enforce the</li></ul>	<ul> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> </ul>
	established local and remote access requirements.	<ul> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT</li> </ul>
	<ul> <li>Ability to prevent external access to the IoT device management interface.</li> </ul>	device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.
	<ul> <li>Ability for the IoT device to require authentication prior to connecting to the device.</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>
	<ul> <li>Ability for the IoT device to support a second, or more, authentication method(s).</li> </ul>	<ul> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> </ul>
	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> </ul>	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul> <li>Ability to verify digital signatures.</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
	<ul> <li>Ability to run hashing algorithms.</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the</li> </ul>
	<ul> <li>Ability to perform authenticated encryption algorithms.</li> </ul>	manufacturer's supporting entities.

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to compute and compare hashes.</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>
	<ul> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and</li> </ul>	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>
	<ul><li>modification.</li><li>Ability to validate the integrity of data transmitted.</li></ul>	<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>
<ul> <li>Ability to verify software updates come from valid</li> <li>Providing documented des maintenance procedures from</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>	
	sources by using an effective method (e.g., digital signatures, checksums, certificate	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
	<ul><li>validation).</li><li>Ability to verify and</li></ul>	<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities</li> </ul>
	authenticate any update before installing it.	<ul> <li>Providing the details necessary to enable IoT device</li> <li>sustamors to monitor onsite and offsite IoT device</li> </ul>
	<ul> <li>Ability to store the operating environment (e.g., firmware</li> </ul>	maintenance activities.
	image, software, applications) in read-only media (e.g., Read Only Memory).	<ul> <li>Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their</li> </ul>
	<ul> <li>Ability to provide a physical indicator of sensor use.</li> </ul>	contractors, once the device is purchased and deployed in the IoT device customer's organization.

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>Ability to keep an accurate internal system time.</li> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>Ability to monitor changes to the configuration settings.</li> <li>Ability to detect remote activation attempts.</li> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash</li> </ul>	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
	drive to be connected even if a	

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	Universal Serial Bus [USB] port is present).	
Scenario 9: Protect from Modification of Historian Data: This test will demonstrate the	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital signatures.</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> </ul>
blocking of modifi- cation of historian archive data. PR.DS-6 PR.MA-1 DE.AE-2	<ul> <li>Ability to run hashing algorithms.</li> <li>Ability to perform authenticated encryption algorithms.</li> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> </ul>
	<ul> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures,</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul><li>checksums, certificate</li><li>validation).</li><li>Ability to verify and</li></ul>	<ul> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> </ul>
	before installing it.	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
		<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> </ul>
		<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>
	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>	
		<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>
		<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>
		<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
Scenario 10: De- tect Sensor Data Manipulation:	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital</li> </ul>	<ul> <li>Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary.</li> </ul>
demonstrate de- tection of atypical data reported to	<ul> <li>Ability to verify digital signatures.</li> <li>Ability to run hashing algorithms</li> </ul>	<ul> <li>Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.</li> </ul>
PR.IP-4 PR.DS-6 PR.MA-1 DE.AE-1 DE.AE-2 DE.AE-3 DE.CM-1 DE.CM-3 DE.CM-7	<ul> <li>Ability to perform authenticated encryption algorithms.</li> </ul>	<ul> <li>Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.</li> </ul>
	<ul> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> </ul>
Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
--	---	--
	method (e.g., digital signatures, checksums, certificate validation).	<ul> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> </ul>
	<ul> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity</li> </ul>
<ul> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>Ability to keep an accurate internal system time.</li> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>Controls built into the IoT device custo device data integrity.</li> <li>Providing details for how to re device and associated system integrity.</li> <li>Providing instructions and dor physical and logical access cap device to perform each type of the details and instructions and documentation describing the details and instruction system time.</li> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> </ul>	<ul> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>Ability to provide a physical indicator of sensor use.</li> <li>Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> </ul>	controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve Ic device data integrity.
		<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>
		<ul> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> </ul>
		<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
		<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the</li> </ul>	
	<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> </ul>	manufacturer's supporting entities.

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to monitor changes to the configuration settings.</li> <li>Ability to detect remote activation attempts.</li> <li>Ability to detect remote activation of sensors.</li> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the</li> </ul>
	other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report	

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		actions to the monitoring service of the manufacturer's supporting entity.
		<ul> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> </ul>
		<ul> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> </ul>
		<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
Scenario 11: De- tect Unauthorized Firmware Modifi- cation:	<ul> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and</li> </ul>
This test will demonstrate the detection of device	<ul> <li>Ability to verify digital signatures.</li> </ul>	associated systems from unauthorized access, modification, and deletion.
	<ul> <li>Ability to run hashing algorithms.</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated</li> </ul>
tion	<ul> <li>Ability to perform authenticated encryption</li> </ul>	systems data integrity.
PR.DS-6	algorithms.	<ul> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity</li> </ul>
PR.MA-1 DE.AE-1	<ul> <li>Ability to compute and compare hashes</li> </ul>	
DE.AE-2 DE.AE-3 DE.CM-1	<ul> <li>Ability to utilize one or more capabilities to protect transmitted data from</li> </ul>	
DE.CM-3		controls built into the IoT device, include documentation

Scenario ID and Description with <i>Cybersecurity</i> <i>Framework</i> Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
DE.CM-7	unauthorized access and modification.	explaining to IoT device customers the ways to achieve IoT device data integrity.
	<ul> <li>Ability to validate the integrity of data transmitted.</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity</li> </ul>
	<ul> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> </ul>	<ul> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> </ul>
		<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>
	<ul> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>
	<ul> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> </ul>
	<ul> <li>Only Memory).</li> <li>Ability to provide a physical indicator of sensor use</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>
	<ul> <li>Ability to send requested audit logs to an external audit process or information system</li> </ul>	<ul> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>
	(e.g., where its auditing information can be checked to	<ul> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>

Scenario ID and Description with Cybersecurity Framework Sub- categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	allow for review, analysis, and reporting).	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>
	<ul> <li>Ability to keep an accurate internal system time.</li> </ul>	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>Ability to monitor changes to the configuration settings.</li> <li>Ability to detect remote activation attempts.</li> <li>Ability to detect remote activation of sensors.</li> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> <li>Providing documentation of sensors.</li> <li>Providing the details necess associated systems.</li> <li>Providing documentation of identify unauthorized use of associated systems.</li> </ul>	<ul> <li>Ability to support a monitoring process to check for disclosure of organizational information</li> </ul>	<ul> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> </ul>
	<ul> <li>to unauthorized entities.</li> <li>Ability to monitor changes to the configuration settings.</li> </ul>	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>	<ul> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> </ul>
	<ul> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> </ul>	
	detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	<ul> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> </ul>
		<ul> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> </ul>
		<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>