# **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

#### **Joseph Brule\***

Cyber Security Directorate National Security Agency

#### Michael Pease Keith Stouffer CheeYee Tang Timothy Zimmerman

Engineering Laboratory National Institute of Standards and Technology Chelsea Deane John Hoyt Mary Raguso Aslam Sherule Kangmin Zheng The MITRE Corporation McLean, Virginia

#### **Matthew Zopf**

Strativia Largo, Maryland

\*Former employee; all work for this publication done while at employer.

September 2021

DRAFT

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics">https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics</a>

National Institute of Standards and Technology U.S. Department of Commerce



#### 1 **DISCLAIMER**

- 2 Certain commercial entities, equipment, products, or materials may be identified by name or company
- 3 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
- 4 experimental procedure or concept adequately. Such identification is not intended to imply special
- 5 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
- 6 intended to imply that the entities, equipment, products, or materials are necessarily the best available
- 7 for the purpose.
- 8 While NIST and NCCoE address goals of improving the management of cybersecurity and privacy risk
- 9 through outreach and application of standards and best practices, it is the stakeholder's responsibility to
- 10 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise
- and the impact should the threat be realized before adopting cyber security measures such as this
- 12 recommendation.
- 13 Domain name and IP addresses shown in this guide represent an example domain and network
- 14 environment to demonstrate the NCCoE project use case scenarios and the security capabilities.
- 15 National Institute of Standards and Technology Special Publication 1800-10B, Natl. Inst. Stand. Technol.
- 16 Spec. Publ. 1800-10B, 170 pages, (September 2021), CODEN: NSPUE2

#### 17 **FEEDBACK**

- 18 You can improve this guide by contributing feedback. As you review and adopt this solution for your
- 19 own organization, we ask you and your colleagues to share your experience and advice with us.
- 20 Comments on this publication may be submitted to: <u>manufacturing nccoe@nist.gov</u>.
- 21 Public comment period: September 23, 2021 through November 07, 2021
- 22 All comments are subject to release under the Freedom of Information Act (FOIA).

23	National Cybersecurity Center of Excellence
24	National Institute of Standards and Technology
25	100 Bureau Drive
26	Mailstop 2002
27	Gaithersburg, MD 20899
28	Email: <u>nccoe@nist.gov</u>

# 29 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

44 <u>https://www.nist.gov</u>.

# 45 NIST CYBERSECURITY PRACTICE GUIDES

- 46 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
- 47 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
- 48 adoption of standards-based approaches to cybersecurity. They show members of the information
- 49 security community how to implement example solutions that help them align more easily with relevant
- 50 standards and best practices, and provide users with the materials lists, configuration files, and other
- 51 information they need to implement a similar approach.
- 52 The documents in this series describe example implementations of cybersecurity practices that
- 53 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- 54 or mandatory practices, nor do they carry statutory authority.

## 55 ABSTRACT

- 56 Today's manufacturing organizations rely on industrial control systems (ICS) to conduct their operations.
- 57 Increasingly, ICS are facing more frequent, sophisticated cyber attacks—making manufacturing the
- 58 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.
- 60 The architecture and solutions presented in this guide are built upon standards-based, commercially
- 61 available products, and represent some of the possible solutions. The solutions implement standard
- 62 cybersecurity capabilities such as behavioral anomaly detection (BAD), application allowlisting, file
- 63 integrity-checking, change control management, and user authentication and authorization. The
- 64 solution was tested in two distinct lab settings: a discrete manufacturing workcell, which represents an
- assembly line production, and a continuous process control system, which represents chemical
- 66 manufacturing industries.

- 67 An organization that is interested in protecting the integrity of a manufacturing system and information
- 68 from destructive malware, insider threats, and unauthorized software should first conduct a risk
- 69 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
- 71 may be used.
- 72 The security capabilities of the example solution are mapped to the *NIST Cybersecurity Framework*, the
- 73 National Initiative for Cybersecurity Education Framework, and NIST Special Publication 800-53.

#### 74 **KEYWORDS**

- 75 Manufacturing; industrial control systems; application allowlisting; file integrity checking; user
- 76 authentication; user authorization; behavioral anomaly detection; remote access; software modification;
- 77 *firmware modification.*

#### 78 ACKNOWLEDGEMENTS

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
Josh Carlson	Dragos
Alex Baretta	Dragos

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

- 80 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
- 81 response to a notice in the Federal Register. Respondents with relevant capabilities or product
- 82 components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
- 83 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)
Dispel	Dispel Wicket ESI
	Dispel Enclave
	Dispel VDI (Virtual Desktop Interface)
Dragos	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
<u>Tenable</u>	Tenable.ot

# 84 **DOCUMENT CONVENTIONS**

85 The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the

86 publication and from which no deviation is permitted. The terms "should" and "should not" indicate that

87 among several possibilities, one is recommended as particularly suitable without mentioning or

88 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in

89 the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms

90 "may" and "need not" indicate a course of action permissible within the limits of the publication. The

91 terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

# 92 CALL FOR PATENT CLAIMS

93 This public review includes a call for information on essential patent claims (claims whose use would be

94 required for compliance with the guidance or requirements in this Information Technology Laboratory

95 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication

96 or by reference to another publication. This call also includes disclosure, where known, of the existence

97 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant

- 98 unexpired U.S. or foreign patents.
- 99 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in
- 100 written or electronic form, either:
- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
- 102 currently intend holding any essential patent claim(s); or

- b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
- to utilize the license for the purpose of complying with the guidance or requirements in this ITL draftpublication either:
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
   or
- without compensation and under reasonable terms and conditions that are demonstrably free
   of any unfair discrimination
- 110 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
- behalf) will include in any documents transferring ownership of patents subject to the assurance,
- 112 provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,
- and that the transferee will similarly include appropriate provisions in the event of future transfers with
- 114 the goal of binding each successor-in-interest.
- 115 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
- 116 whether such provisions are included in the relevant transfer documents.
- 117 Such statements should be addressed to: <u>manufacturing nccoe@nist.gov</u>

# 118 Contents

119	1	Sum	mary.		.1
120		1.1	Challen	ge	. 2
121		1.2	Solution	1	.3
122			1.2.1 F	Relevant Standards and Guidance	3
123		1.3	Benefits	3	.4
124	2	Hov	v to Us	e This Guide	.4
125		2.1	Typogra	phic Conventions	.6
126	3	Арр	roach		.6
127		3.1	Audienc	e	.6
128		3.2	Scope		.7
129		3.3	Assump	tions	.7
130		3.4	Risk Ass	essment	.8
131			3.4.1	۲hreats	8
132			3.4.2	/ulnerabilities	9
133			3.4.3 F	Risk	10
134			3.4.4	Security Control Map	10
135		3.5	Technol	ogies	13
136	4	Arc	nitectu	re1	L <b>4</b>
137		4.1	Manufa	cturing Process and Control System Description	15
138		4.2	Cyberse	curity for Smart Manufacturing Systems Architecture	15
139		4.3	Process	Control System	16
140		4.4	Collabo	rative Robotics System (CRS)	19
141		4.5	Logical I	Network and Security Architectures	21
142			4.5.1 E	Build 1	21
143			4.5.2 E	Build 2	25
144			4.5.3 E	3uild 3	28
145			4.5.4 E	3uild 4	30
146	5	Secu	urity Ch	naracteristic Analysis	32
147		5.1	Assump	tions and Limitations	32
148		5.2	Example	e Solution Testing	32
149			5.2.1 9	Scenario 1: Protect Host from Malware Infection via USB	33

#### DRAFT

150		5.2.2	Scenario 2: Protect Host from Malware Infection via Network Vector
151		5.2.3	Scenario 3: Protect Host from Malware via Remote Access Connections35
152		5.2.4	Scenario 4: Protect Host from Unauthorized Application Installation
153		5.2.5	Scenario 5: Protect from Unauthorized Addition of a Device
154		5.2.6	Scenario 6: Detect Unauthorized Device-to-Device Communications
155		5.2.7	Scenario 7: Protect from Unauthorized Deletion of Files40
156		5.2.8	Scenario 8: Detect Unauthorized Modification of PLC Logic41
157		5.2.9	Scenario 9: Protect from Modification of Historian Data42
158		5.2.10	Scenario 10: Detect Sensor Data Manipulation44
159		5.2.11	Scenario 11: Detect Unauthorized Firmware Modification44
160	5.3	Scenar	ios and Findings46
161 162		5.3.1	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes46
163		5.3.2	PR.AC-3: Remote access is managed46
164 165		5.3.3	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties46
166 167 168		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., individuals' security and privacy risks and other organizational risks)47
169		5.3.5	PR.DS-1: Data-at-rest is protected47
170 171		5.3.6	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity47
172		5.3.7	PR.IP-4: Backups of information are conducted, maintained, and tested47
173 174		5.3.8	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
175 176		5.3.9	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
177 178		5.3.10	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
179		5.3.11	DE.AE-2: Detected events are analyzed to understand attack targets and methods 48
180 181		5.3.12	DE.AE-3: Event data are collected and correlated from multiple sources and sensors . 
182		5.3.13	DE.CM-1: The network is monitored to detect potential cybersecurity events49
183		5.3.14	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events 49
184 185		5.3.15	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

186	6 Fut	ure B	uild Considerations	50
187	Append	A xib	List of Acronyms	51
188	Append	dix B	Glossary	53
189	Append	dix C	References	57
190	Append	dix D	Scenario Execution Results	59
191	D.1	Execu	ting Scenario 1: Protect Host from Malware via USB	59
192		D.1.1	Build 1	59
193		D.1.2	Build 2	61
194		D.1.3	Build 3	61
195		D.1.4	Build 4	62
196	D.2	Execu	ting Scenario 2: Protect Host from Malware via Network Vector	63
197		D.2.1	Build 1	64
198		D.2.2	Build 2	67
199		D.2.3	Build 3	73
200		D.2.4	Build 4	77
201	D.3	Execu	ting Scenario 3: Protect Host from Malware via Remote Access	
202		Conn	ections	81
203		D.3.1	Build 1	81
204		D.3.2	Build 2	83
205		D.3.3	Build 3	85
206		D.3.4	Build 4	87
207	D.4	Execu	ting Scenario 4: Protect Host from Unauthorized Application Installation	89
208		D.4.1	Build 1	89
209		D.4.2	Build 2	91
210		D.4.3	Build 3	93
211		D.4.4	Build 4	96
212	D.5	Execu	ting Scenario 5: Protect from Unauthorized Addition of a Device	99
213		D.5.1	Build 1	100
214		D.5.2	Build 2	101
215		D.5.3	Build 3	102
216		D.5.4	Build 4	106
217	D.6	Execu	ting Scenario 6: Detect Unauthorized Device-to-Device Communications	108

219		D.6.2	Build 2	109
220		D.6.3	Build 3	110
221		D.6.4	Build 4	111
222	D.7	Execut	ing Scenario 7: Protect from Unauthorized Deletion of Files	
223		D.7.1	Build 1	112
224		D.7.2	Build 2	113
225		D.7.3	Build 3	114
226		D.7.4	Build 4	115
227	D.8	Execut	ing Scenario 8: Detect Unauthorized Modification of PLC Logic	
228		D.8.1	Build 1	116
229		D.8.2	Build 2	119
230		D.8.3	Build 3	123
231		D.8.4	Build 4	126
232	D.9	Execut	ing Scenario 9: Protect from Modification of Historian Data	
233		D.9.1	Build 1	128
234		D.9.2	Build 2	130
235		D.9.3	Build 3	132
236		D.9.4	Build 4	134
237	D.10	Execut	ing Scenario 10: Detect Sensor Data Manipulation	136
238		D.10.1	All Builds	136
239	D.11	Execut	ing Scenario 11: Detect Unauthorized Firmware Modification	
240		D.11.1	Build 1	137
241		D.11.2	Build 2	138
242		D.11.3	Build 3	141
243		D.11.4	Build 4	142
244	Append	lix E	Benefits of IoT Cybersecurity Capabilities	144
245	E.1	Device	Capabilities Mapping	
246	E.2	Device	Capabilities Supporting Functional Test Scenarios	

# 247 List of Figures

248	Figure 4-1: CSMS Network Architecture
249	Figure 4-2: Simplified Tennessee Eastman Process Model
250	Figure 4-3: HMI Screenshot for the PCS Showing the Main Components in the Process
251	Figure 4-4: PCS Network
252	Figure 4-5: The CRS Workcell
253	Figure 4-6: CRS Network
254	Figure 4-7: Build 1, PCS Complete Architecture with Security Components24
255	Figure 4-8: Build 2, PCS Complete Architecture with Security Components27
256	Figure 4-9: Build 3, CRS Complete Architecture with Security Components29
257	Figure 4-10: Build 4, CRS Complete Architecture with Security Components31
258	Figure D-1: An Alert from Carbon Black Showing that Malware (1.exe) was Blocked from Executing60
259	Figure D-2: Carbon Black's Server Provides Additional Details and Logs of the Event60
260	Figure D-3: Carbon Black's Server Log of the Event61
261	Figure D-4: Windows 7 Alert as a Result of Windows SRP Blocking the Execution of 1.exe61
262	Figure D-5: Windows 10 Alert as a Result of Windows SRP Blocking the Execution of 1.exe62
263	Figure D-6: Carbon Black Blocks the Execution of 1.exe for Build 463
264	Figure D-7: Tenable.ot Dashboard Showing the Events that were Detected64
265	Figure D-8: Detected RDP Session Activity from External System to DMZ System65
266 267	Figure D-9: Event Detection Detail for the RDP Connection from the External System to the Historian in the DMZ
268	Figure D-10: Tenable.ot Detected VNC Connection Between the DMZ and the Testbed LAN65
269 270	Figure D-11: Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in the Testbed LAN
271	Figure D-12: Detected RDP from a DMZ system to a Testbed LAN system
272 273	Figure D-13: Tenable.ot Event Detail Showing the RDP Connection Between the Historian in the DMZ to a Workstation in the Testbed LAN
274	Figure D-14: Attempt to Execute 1.exe Failed67
275	Figure D-15: Alert Dashboard Showing Detection of an RDP Session
276	Figure D-16: Details of the Detected RDP Session Activity from an External System to DMZ System69

DRAFT	•

277	Figure D-17: Detection of Scanning Traffic and RDP Connection into Manufacturing Environment70
278	Figure D-18: Details of One of the Port Scan Alerts
279	Figure D-19: Details of Alert for RDP Connection into Manufacturing Environment72
280	Figure D-20: Dialog Message Showing 1.exe was Blocked from Executing73
281	Figure D-21: Windows SRP blocked 1.exe From Executing74
282	Figure D-22: Log of Alerts Detected by Dragos
283	Figure D-23: Detail of RDP Session Activity Between an External System and a DMZ System75
284	Figure D-24: Detail for Network Scanning Alert
285	Figure D-25: Detail of RDP Session Activity Between a DMZ System and a Testbed LAN System76
286 287	Figure D-26: Azure Defender for IoT "info" Event Identified the Remote Access Connection to the DMZ
288	Figure D-27: Alert for Scanning Activity
289	Figure D-28: Details for the Scanning Alert
290	Figure D-29: Detection of RDP Connection into the Manufacturing Environment80
291	Figure D-30: Carbon Black Shows an Alert for Blocking File 1.exe
292	Figure D-31: Secured VPN Connection to Environment with Cisco AnyConnect82
293	Figure D-32: Remote Access is Being Established Through ConsoleWorks
294	Figure D-33: Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket ESI84
295	Figure D-34: Nested RDP Session Showing Dispel Connection into the PCS Workstation85
296	Figure D-35: VPN Connection to Manufacturing Environment86
297	Figure D-36: Remote Access is Being Established Through ConsoleWorks
298	Figure D-37: Dispel VDI Showing Interface for Connecting Through Dispel Enclave to Dispel Wicket88
299	Figure D-38: Nested RDP Session Showing Dispel Connection into the CRS Workstation
300	Figure D-39: Carbon Black Blocks the Execution of putty.exe and Other Files90
301 302	Figure D-40: Tenable.ot alert Showing the SMB Connection Between the HMI and the GreenTec Server
303 304	Figure D-41: Tenable.ot Alert Details of the SMB Connection Between the HMI and the network file system (NFS) Server in the DMZ
305	Figure D-42: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration92
306	Figure D-43: putty-64bit-0.74-installer.msi is blocked by Windows SRP92
307	Figure D-44: Forescout Alert on the File Transfer Activity93
308	Figure D-45: Forescout Alert Details for the File Transfer Activity93

#### DRAFT

309	Figure D-46: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration94
310	Figure D-47: putty-64bit-0.74-installer.msi is Blocked by Windows SRP94
311	Figure D-48: Dragos Alert on the File Transfer Activity95
312	Figure D-49: Dragos Alert Details of the File Transfer Alert96
313	Figure D-50: Carbon Black Alert Showing that putty.exe is Blocked from Executing97
314 315	Figure D-51: Carbon Black Alert Showing the Execution of putty-64bit-0.74-installer.msi Being Blocked
316	Figure D-52: Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity98
317 318	Figure D-53: Azure Defender for IoT Alert Details Showing RPC Connection Between the DMZ and the Testbed LAN
319	Figure D-54: Azure Defender for IoT Event Alert Timeline Showing the File Transfer
320	Figure D-55: Tenable.ot Event Showing a New Asset has Been Discovered101
321	Figure D-56: Tenable.ot Event Showing Unauthorized SSH Activities101
322	Figure D-57: Forescout Alert on the DNS Request from the New Device
323	Figure D-58: Forescout alert showing the SSH connection102
324	Figure D-59: Detailed Forescout alert of the Unauthorized SSH Connection102
	Figure D. 60: Drages Dashboard Showing Alerts Concreted upon Detecting New Device and Network
325 326	Scanning
325 326 327	Scanning
325 326 327 328	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network      Scanning      104      Figure D-61: Details of Network Scanning Activity      104      Figure D-62: Additional Details of Network Scanning Activity
325 326 327 328 329	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning         104         Figure D-61: Details of Network Scanning Activity         104         Figure D-62: Additional Details of Network Scanning Activity         105         Figure D-63: Alert for New Asset on the Network
325 326 327 328 329 330	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning         104         Figure D-61: Details of Network Scanning Activity         104         Figure D-62: Additional Details of Network Scanning Activity         105         Figure D-63: Alert for New Asset on the Network         105         Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset
325 326 327 328 329 330 331	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning       104         Figure D-61: Details of Network Scanning Activity       104         Figure D-62: Additional Details of Network Scanning Activity       105         Figure D-63: Alert for New Asset on the Network       105         Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset       106         Figure D-65: Azure Defender for IoT Detects New Asset in the Environment       107
325 326 327 328 329 330 331 332	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning       104         Figure D-61: Details of Network Scanning Activity       104         Figure D-62: Additional Details of Network Scanning Activity       105         Figure D-63: Alert for New Asset on the Network       105         Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset       106         Figure D-65: Azure Defender for IoT Detects New Asset in the Environment       107         Figure D-66: Azure Defender for IoT Alert Management Options       107
325 326 327 328 329 330 331 332 333	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning
325 326 327 328 329 330 331 332 333 334	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning       .104         Figure D-61: Details of Network Scanning Activity       .104         Figure D-62: Additional Details of Network Scanning Activity       .105         Figure D-63: Alert for New Asset on the Network       .105         Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset       .106         Figure D-65: Azure Defender for IoT Detects New Asset in the Environment       .107         Figure D-66: Azure Defender for IoT Alert Management Options       .107         Figure D-67: Details for Network Scanning Alert       .108         Figure D-68: Tenable.ot Event Log Showing the Unapproved SSH Traffic       .109
325 326 327 328 329 330 331 332 333 334 335	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning
325 326 327 328 329 330 331 332 333 334 335 336	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network         Scanning       104         Figure D-61: Details of Network Scanning Activity       104         Figure D-62: Additional Details of Network Scanning Activity       105         Figure D-63: Alert for New Asset on the Network       105         Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset       106         Figure D-65: Azure Defender for IoT Detects New Asset in the Environment       107         Figure D-66: Azure Defender for IoT Alert Management Options       107         Figure D-67: Details for Network Scanning Alert       108         Figure D-68: Tenable.ot Event Log Showing the Unapproved SSH Traffic       109         Figure D-69: Forescout Alert Showing the Unapproved SSH Traffic       110         Figure D-70: Dragos Alert Showing the Unapproved SSH Connection Between Devices       111
325 326 327 328 329 330 331 332 333 334 335 336 337	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and NetworkScanning104Figure D-61: Details of Network Scanning Activity104Figure D-62: Additional Details of Network Scanning Activity105Figure D-63: Alert for New Asset on the Network105Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset106Figure D-65: Azure Defender for IoT Detects New Asset in the Environment107Figure D-66: Azure Defender for IoT Alert Management Options107Figure D-67: Details for Network Scanning Alert108Figure D-68: Tenable.ot Event Log Showing the Unapproved SSH Traffic110Figure D-70: Dragos Alert Showing the Unapproved SSH Connection Between Devices111Figure D-71: Azure Defender for IoT Event Identified the Unauthorized SSH Connection112
325 326 327 328 329 330 331 332 333 334 335 336 337 338	Figure D-60: Dragos Dashboard Showing Aferts Generated upon Detecting New Device and NetworkScanning
325 326 327 328 329 330 331 332 333 334 335 336 337 338 339	Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and NetworkScanning

341	Figure D-75: Carbon Black Alerts Showing That a File Has Been Deleted116
342 343	Figure D-76: Remote Access to Systems in PCS Network is Being Established Through ConsoleWorks
344	Figure D-77: Remote Session into Studio 5000 to Perform PLC File Operations
345	Figure D-78: Tenable.ot Detected the Transfer of PLC Logic File to the Rockwell PLC118
346	Figure D-79: Tenable.ot PLC Stop alert details
347	Figure D-80: Tenable.ot PLC Program Download Alert Details119
348	Figure D-81: Remote Access to Systems in PCS Network is Being Established Through Dispel
349	Figure D-82: Modifying the Parameters for the Allen-Bradley PLC Controller Using Studio 5000121
350 351	Figure D-83: Forescout Alerts Showing It Detected the Traffic Between the Engineering Workstation and the PLC
352	Figure D-84: Forescout Alert Details for the Stop Command Issued to the PLC
353	Figure D-85: Forescout Alert Details for the Configuration Download Command
354	Figure D-86: VPN Connection to the Manufacturing Environment124
355	Figure D-87: Remote Access is Being Established through ConsoleWorks
356 357	Figure D-88: Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the Beckhoff PLC
358	Figure D-89: Dragos Alert Details for the PLC Logic File Download
359	Figure D-90: Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket127
360	Figure D-91: Nested RDP Connections Showing Dispel Connection into the CRS Workstation
361	Figure D-92: Azure Defender for IoT Alert for the Unauthorized PLC Programming128
362 363	Figure D-93: Tenable.ot alert Showing SMB Connection from an External Workstation to the Historian
364	Figure D-94: GreenTec Denies Modification and Deletion File Operations in the Protected Drive130
365 366	Figure D-95: Forescout Alert Showing Network Connection from the Corporate Network to the Historian
367	Figure D-96: GreenTec Denies Modification and Deletion File Operations in the Protected Drive132
368	Figure D-97: Dragos Detection of RDP Session from an External Network to the Historian133
369	Figure D-98: GreenTec Denies Modification and Deletion File Operations in the Protected Drive134
370 371	Figure D-99: Azure Defender for IoT Event Timeline Showing the Remote Access Connection to the Historian
372	Figure D-100: GreenTec Denies Modification and Deletion File Operations in the Protected Drive136
373 374	Figure D-101: PI Server's Event Frames Showing Out-of-Range Sensor Readings for the Reactor Pressure

#### DRAFT

375	Figure D-102: Tenable.ot Detects a Collection of Events Generated by a Firmware Change
376	Figure D-103: Details for One of the Alerts Showing the Firmware Change138
377	Figure D-104: Forescout Detects a Collection of Alerts Associated with the Firmware Change
378	Figure D-105: Alert Details Detected by Forescout for the Firmware Change140
379	Figure D-106: ICS Patrol Scan Results Showing a Change Configuration was Made141
380	Figure D-107: Dragos Dashboard Showing an Alert for Firmware Change142
381	Figure D-108: Details for Firmware Change Alert142
382	Figure D-109: Azure Defender for IoT Alert Showing a Version Mismatch in the Firmware Build143

# 383 List of Tables

384	Table 3-1: Security Control Map    11
385	Table 3-2: Products and Technologies   13
386	Table 4-1: Summary of What Products Were Used in Each Build
387	Table 4-2: Build 1 Technology Stack to Capabilities Map
388	Table 4-3: Build 2 Technology Stack to Capabilities Map
389	Table 4-4: Build 3 Technology Stack to Capabilities Map
390	Table 4-5: Build 4 Technology Stack to Capabilities Map
391 392	Table E-1: Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities toNIST Cybersecurity Framework Subcategories of the ICS Project
393 394	Table E-2 Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities that Map toEach of the Functional Test Scenarios155

# 395 **1 Summary**

- 396 While availability is always a critical aspect of manufacturing system environments, manufacturers also
- 397 need to consider maintaining the integrity of their systems and information to ensure continued
- 398 operations. The integrity of information can be degraded or lost as a result of behaviors by authorized
- 399 users (e.g., failure to perform backups or record their actions) or malicious actors seeking to disrupt
- 400 manufacturing operations for illicit profits, political statements, or other reasons.
- 401 Manufacturers are unique because of their reliance on industrial control systems (ICS) to monitor and
- 402 control their manufacturing operations. ICS typically prioritize information availability and integrity over
- 403 confidentiality. As a result, cybersecurity solutions used in traditional information technology (IT)
- 404 settings are not optimized to protect ICS from cyber threats.
- 405 This guide, prepared by the National Cybersecurity Center of Excellence (NCCoE) and the NIST
- 406 Engineering Laboratory (EL), contains four examples of practical solutions that organizations can
- 407 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 ofsystems and information by:
- 410 securing historical system data
- 411 preventing execution or installation of unapproved software
- 412 detecting anomalous behavior on the network
- 413 identifying hardware, software, or firmware modifications
- 414 enabling secure remote access
- 415 authenticating and authorizing users
- 416 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 thefour example builds are also presented and discussed.
- Ultimately, manufacturing organizations that rely on ICS can use the example solutions described in thisguide to safeguard their information and system integrity from:
- 422 destructive malware
- 423 insider threats
- 424 unauthorized software
- 425 unauthorized remote access
- 426 Ioss of historical data
- 427 anomalies network traffic
- 428 unauthorized modification of systems

- 429 This document contains the following sections:
- 430 Section 1, Summary, presents the challenges addressed by the NCCoE project, with a look at the
- 431 solutions demonstrated to address the challenge, as well as benefits of the solutions.
- 432 <u>Section 2, How to Use This Guide</u>, explains how readers—business decision makers, program managers,
- 433 control system engineers, cybersecurity practitioners, and IT professionals (e.g., systems
- 434 administrators) might use each volume of this guide.
- 435 <u>Section 3, Approach</u>, offers a description of the intended audience and the scope of the project. This
- 436 section also describes the assumptions on which the security architecture and solution development
- 437 was based, the risk assessment that informed architecture development, the NIST Cybersecurity
- 438 *Framework* functions supported by each component of the architecture and reference design, and
- 439 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
- 441 other industry guidance, and identifies the products used to address each subcategory.
- 442 <u>Section 4, Architecture</u>, summarizes the Cybersecurity for Smart Manufacturing Systems (CSMS)
- 443 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.
- 446 Section 5, Security Characteristic Analysis, summarizes the scenarios and findings that were employed to
- demonstrate the example implementations' functionality. Each of the scenarios is mapped to the
- 448 relevant NIST Cybersecurity Framework functions and subcategories and the security capabilities of the
- 449 products that were implemented. Additionally, it briefly describes how the security capabilities that
- 450 were used in the solution implementation help detect cyber attacks and protect the integrity of the
- 451 manufacturing systems and information.
- 452 <u>Section 6, Future Build Considerations</u>, identifies additional areas that should be reviewed in future 453 practice guides.
- 454 Section Appendix D, Scenario Execution Results, describes, in detail, the test results of the scenarios,
- 455 including screenshots from the security products captured during the tests.

# 456 **1.1 Challenge**

- 457 Manufacturing organizations that rely on ICS to monitor and control physical processes face risks from
- 458 malicious and non-malicious insiders along with external threats in the form of increasingly
- 459 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
- 461 financial loss and harming production for years to come.
- 462 Manufacturing organizations may be the targets of malicious cyber actors or may be incidentally
- 463 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
- 467 found on IT systems.
- 468 Organizations are increasingly adopting and integrating IT into the ICS environment to enhance
- 469 connectivity to business systems and to enable remote access. As a result, ICS are no longer isolated
- 470 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 OT environment,
- so special precautions are required when introducing these controls. In some cases, new security
- 473 techniques tailored to the specific ICS environment are needed.
- 474 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
- 476 unapproved software utility to perform maintenance activities or update the logic of a programmable
- 477 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
- 480 manufacturing system, causing disruptions to system operations, or opening a backdoor to remote
- 481 attackers.

# 482 **1.2 Solution**

- 483 This NCCoE Cybersecurity Practice Guide demonstrates how manufacturing organizations can use
- 484 commercially available technologies that are consistent with cybersecurity standards to detect and
   485 prevent cyber incidents on their ICS.
- 486 Manufacturers use a wide range of ICS equipment and manufacturing processes. This guide contains
   487 four different example solutions that are applicable to a range of manufacturing environments, focusing
   488 on discrete and continuous manufacturing processes.
- This project provides example solutions, composed of the following capabilities, for manufacturingenvironments:
- 491 application allowlisting
- 492 behavior anomaly detection (BAD)
- 493 file integrity
- 494 user authentication and authorization
- 495 remote access
- 496 1.2.1 Relevant Standards and Guidance
- The solutions presented in this guide are consistent with the practices and guidance provided by thefollowing references.
- 499 NIST Special Publication (SP) 800-167: *Guide to Application Whitelisting* [2]
- 500• Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework501Implementation Guidance [3]

502	1.1	Executive Order no. 13636: Improving Critical Infrastructure Cybersecurity [4]
503		NIST, Framework for Improving Critical Infrastructure Cybersecurity [5]
504 505	1	NIST Interagency Report (NISTIR) 8219: Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection [6]
506		NIST Internal Report (NISTIR) 8183: Cybersecurity Framework Manufacturing Profile [7]
507		NISTIR 8089: An Industrial Control System Cybersecurity Performance Testbed [8]
508 509	1	NIST SP 800-53 Rev. 5: Security and Privacy Controls for Federal Information Systems and Organizations [9]
510 511	1	NIST SP 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [10]
512 513	1	NIST Special Publication 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events [11]
514		NIST Interagency or Internal Report 7298 Rev 3: Glossary of Key Information Security Terms [12]
515	1.1	U.SCanada Power System Outage Task Force [13]
516		NIST SP 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security [14]
517	1.3	Benefits
518	This NO	CCoE practice guide can help organizations:
519		mitigate cybersecurity risk
520		reduce downtime to operations
521	1.1	provide a reliable environment that can detect cyber anomalies
522	1.1	respond to security alerts through automated cybersecurity-event products
523 524	1	develop and execute an OT cybersecurity strategy for which continuous OT cybersecurity monitoring is a foundational building block
525	1.1	implement current cybersecurity standards and best practices
526	2 H	low to Use This Guide
527 528	This NI inform	ST Cybersecurity Practice Guide demonstrates a modular design and provides users with the ation they need to replicate the described manufacturing ICS security solutions, specifically

- 529 focusing on information and system integrity. This reference design is modular and can be deployed in
- 530 whole or in part.
- 531 This guide contains three volumes:
- 532 NIST SP 1800-10A: Executive Summary
- NIST SP 1800-10B: Approach, Architecture, and Security Characteristics what we built and why
   (this document)
- 535 NIST SP 1800-10C: *How-To Guide* instructions for building the example solution

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

#### 537 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:

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

543 **Technology or security program managers** might share the *Executive Summary*, NIST SP 1800-10A, with 544 your leadership to help them understand the importance of adopting a standards-based solution. Doing 545 so can strengthen their information and system integrity practices by leveraging capabilities that may 546 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. Section 3.4.4, which maps the security characteristics of the example solutions to
 cybersecurity standards and best practices, will be of particular interest:

- 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.
- 557 This guide assumes that IT and OT professionals have experience implementing security products within 558 the enterprise. While we have used a suite of commercial products to address this challenge, this guide
- 558 the enterprise. While we have used a suite of commercial products to address this challenge, this guide 559 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
- 561 implementing parts of the manufacturing ICS solution. Your organization's security experts should
- 562 identify the products that will best integrate with your existing tools and IT system infrastructure. We
- 563 hope that you will seek products that are congruent with applicable standards and best practices.
- 564 <u>Section 3.5</u>, Technologies, lists the products we used and maps them to the cybersecurity controls
- 565 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.
- 569 This document provides initial guidance. We seek feedback on its contents and welcome your input.
- 570 Comments, suggestions, and success stories will improve subsequent versions of this guide. Please
- 571 contribute your thoughts to <u>manufacturing\_nccoe@nist.gov</u>.

# 572 **2.1 Typographic Conventions**

573 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.

# 574 **3** Approach

575 This practice guide documents the approach the NCCoE used to develop example solutions, called

576 builds, supporting information and system integrity objectives. The approach includes a logical design,

577 example build development, testing, security control mapping, and analysis.

- 578 Based on our discussions with cybersecurity practitioners in the manufacturing sector, the NCCoE
- 579 pursued the Information and System Integrity in ICS Environments project to illustrate the broad set of 580 capabilities available to manage and protect OT assets.
- 581 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.
- 583 Vendors provided technologies that met project requirements and assisted in installation and
- 584 configuration of those technologies. This practice guide highlights the implementation of example
- architectures, including supporting elements such as functional tests, security characteristic analysis,
- 586 and future build considerations

#### 587 **3.1 Audience**

- 588 This guide is intended for individuals or entities responsible for cybersecurity of ICS and for those
- 589 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,
- 591 academia, or government who seeks general knowledge of an OT information and system integrity
- 592 solution for manufacturing-sector organizations.

#### 593 **3.2 Scope**

- 594 This document focuses on information and system integrity in ICS environments typical of
- 595 manufacturing organizations. It provides real-world guidance on implementing a solution for 596 manufacturing ICS environments.
- 597 The scope of this project is to protect the integrity of information and systems, which includes:
- 598 securing the data historians
- 599 preventing the execution or installation of unapproved software
- 600 detecting anomalous behavior on the network that affects system or information integrity
- 601 detecting hardware, software, or firmware modification
- 602 enabling secure remote access
- 603 authenticating and authorizing users
- 604 Organizational cybersecurity policies and procedures, as well as response and recovery functions, are 605 out of scope for this document.
- 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: 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]

## 623 **3.3 Assumptions**

- 624 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.

# 633 3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, 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
- 640 an information system. Part of risk management incorporates threat and vulnerability analyses, and
- 641 considers mitigations provided by security controls planned or in place."
- 642 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*
- 644 Information Systems and Organizations, material that is available to the public. The Risk Management
- 645 <u>Framework (RMF)</u> guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks,
- 646 from which we developed the project, the security characteristics of the build, and this guide.

## 647 3.4.1 Threats

- 648 A threat is "any circumstance or event with the potential to adversely impact organizational operations"
- 649 [11]. Within an IT environment, threats are typically thought of in terms of threats to confidentiality,
- 650 integrity, or availability.
- 651 The realization of a threat to confidentiality, integrity, and availability may have different impacts to the
- 652 OT versus the IT environments. OT environments are sensitive to loss of safety, availability, and
- 653 integrity, while traditional IT environments tend to direct more resources toward confidentiality.
- 654 Organizations that combine IT and OT operations are advised to evaluate the threats from both
- 655 perspectives.
- In a cyber-physical system, cybersecurity stakeholders are advised to consider events that occur in the
- 657 OT environment may have impact to physical assets and events that occur in the physical world may
- 658 impact the OT environment. For example, in 2021 a ransomware attack against an American oil pipeline
- 659 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
- 661 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
- 663 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
- 665 million people were affected by this blackout and more than 100 people died. [13] Similarly, a sensor or
- 666 metrology malfunction can lead to corrupted values in databases, logs, or other repositories.

668

669

- A loss of integrity of telemetry data may cause control algorithms to produce erroneous or even 670 detrimental commands to manufacturing or control equipment. 671 672 Corrupted routing tables or a denial-of-service attack on the communications infrastructure may 673 cause the manufacturing processes to enter into a fail-safe state, thus inhibiting production. If 674 the process is not designed to be fail-safe, an attack could result in equipment damage and lead 675 to a greater disaster. 676 Unauthorized remote access to the plant network could enable an attacker to stop production 677 or operate the plant and equipment beyond its intended operating range. An attacker 678 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. 679 3.4.2 Vulnerabilities 680 A vulnerability as defined in NISTIR 7298, Glossary of Key Information Security Terms [12] is a "weakness 681 682 in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." 683 684 As indicated in Section 1 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 685 686 vulnerability of the overall system being much greater than the sum of the vulnerabilities of the 687 subsystems. 688 *NIST SP 800-82* categorizes ICS vulnerabilities into the following categories with examples [14]: 689 Policy and Procedure: incomplete, inappropriate, or nonexistent security policy, including its 690 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 695 **Software Development:** improper data validation, security capabilities not enabled, inadequate 696 authentication privileges 697 Communication and Network: nonexistent authentication, insecure protocols, improper firewall 698 configuration 699 The first step in understanding the vulnerabilities and securing an organization's ICS infrastructure is 700 knowledge of deployed assets and their interfaces. The knowledge of an asset's location and baselining 701 of its behavior enable detection of anomalous behavior, via network monitoring, that may be the result 702 of a successfully exploited vulnerability. The ability to reliably detect changes in asset behavior and 703 knowing an asset's attributes are key in responding to potential cybersecurity incidents.
- - 691 692
  - 693
  - 694

NIST SP 1800-10B: Protecting Information and System Integrity in Industrial Control System Environments

667 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.

#### 704 **3.4.3** Risk

- 705 The risk to an organization is the intersection of:
- 706 the vulnerabilities and threats to the organization
- 707 the likelihood that the vulnerability and threat event will be realized
- 708 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
- 712 estimates the likelihood of the threats being realized.
- 713 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.
- 715 Once a baseline risk assessment has been completed, information assurance controls, such as the
- 716 integrity protection measures investigated in this project, can be evaluated on how well they reduce the
- 717 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
- 719 components, elements, or items for which a risk assessment must be conducted. In addition, <u>NIST SP</u>
- 720 <u>800-82 [14]</u> mentions special considerations for performing an ICS risk assessment.

# 721 3.4.4 Security Control Map

- 722 Implementation of cybersecurity architectures is most effective when executed in the context of an
- 723 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
- 726 framework.
- 727 The subset of NIST Cybersecurity Framework Functions, Categories, and Subcategories that are
- supported by this example solution are listed below in <u>Table 3-1</u>, along with the subset of mappings to
- 729 NIST SP 800-53 Rev. 5 and to the National Initiative for Cybersecurity Education (NICE) Workforce
- 730 Framework. NIST SP 800-53 Rev 5: Security and Privacy Controls for Information Systems and
- 731 *Organizations* provides a list of controls for protecting operations, assets, and individuals. The controls
- 732 detail requirements necessary to meet organizational needs. The <u>NICE Cybersecurity Workforce</u>
- 733 *Framework* identifies knowledge, skills, and abilities (KSAs) 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*
- 736 for Information Systems and Organizations is available at
- 737 <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.</u>
- 738 For more information about NICE and resources that are available to employers, education and training
- 739 providers, students, and job seekers, the NIST SP-181 Rev. 1, NICE Cybersecurity Workforce Framework,
- 740 and other NICE resources are available at <u>https://nist.gov/itl/applied-cybersecurity/nice/nice-</u>
- 741 <u>framework-resource-center.</u>

# 742 Table 3-1: Security Control Map

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
	Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, 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
			AC-19	OM-ADM-001, PR-INF-001
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-14, AC-24	OM-STS-001, OM-ADM-001
PROTECT (PR)		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 privacy risks and other organizational risks)	AC-14, IA-2, IA-4, IA-5	OM-STS-001, OM-ADM-001
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	MP-7, SC-28	SP-DEV-002, SP-SYS-002, OM-DTA-001
		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, responsibilities, management commitment, and coordination among organizational	PR.IP-4: Backups of information are conducted, maintained, and tested	CP-9	SP-SYS-001, SP-SYS-002, OM-DTA-001

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
	and procedures are maintained and used to manage protection of information systems and assets.			
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is	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
	performed consistent with policies and procedures.	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
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	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 attack 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 multiple sources and sensors	CA-7, SI-4	OM-DTA-002, PR-CDA-001, PR-CIR-001, CO-OPS-001
DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity 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 potential cybersecurity events	AU-12, CA-7, CM-11	PR-CDA-001, AN-TWA-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, 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

# 743 **3.5 Technologies**

744 <u>Table 3-2</u> 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 <u>Table 3-1</u> for an explanation

- 746 of the NIST *Cybersecurity Framework* subcategory codes.
- 747 Table 3-2: Products and Technologies

Capability	Product	Function	NIST Cybersecurity Framework Subcategories Mapping	
	VMWare Carbon Black			
Application Allowlisting (AAL)	Windows Software Restriction Policies (SRP) (Note: This component was not provided by collaborator. 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, system, 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 collaborator. It is an open source product.)	Provides integrity checks for files and software.		
	Microsoft Azure Defender for IoT	Passively scans the OT		
BAD, Hardware/ Software/	Dragos Platform	network to create a baseline of devices and network traffic	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2,	
Modification Detection	Forescout eyeInspect (formerly SilentDefense)	Alerts when activity deviates from the	DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7	
	Tenable Tenable.ot	baseline.		

Capability	Product	Function	NIST Cybersecurity Framework Subcategories Mapping	
	PI System	Collects, analyzes, and visualizes time-series data from multiple sources. Alerts when activity deviates from the baseline.	PR.IP-4, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3	
User Authentication and	TDi ConsoleWorks	Provides a central location for managing password changes. Provides a security perimeter for all devices within the OT environment.	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	
User Authorization	Dispel			
	Dispel		PR.AC-3, PR.MA-2, DE.AE-2, DE.CM-7	
Remote Access	Cisco AnyConnect (Note: This component was not provided by collaborator. It was a component of the existing lab infrastructure.)	Provides secure remote access. Records and logs user activity for each session.		

# 748 **4** Architecture

- 749 These mechanisms and technologies were integrated into the existing NIST Cybersecurity for Smart
- 750 Manufacturing Systems (CSMS) lab environment [8]. This cybersecurity performance testbed for ICS is
- 751 comprised of the Process Control System (PCS) and the Collaborative Robotic System (CRS) ICS
- 752 environments along with additional networking capabilities to emulate common manufacturing
- 753 environments.
- 754 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
- vised available CRADA partner technologies to assemble four "builds" deployed across both the PCS and
- 757 CRS. Additionally, to increase the diversity of technologies between builds, two of the builds also utilized
- 758 open source solutions (Security Onion Wazuh), native operating system features (Windows Software
- 759 Restriction Policies [SRP]), and a Cisco Adaptive Security Appliance (ASA) device configured with the
- 760 AnyConnect VPN client.
- This modular approach, focusing on specific products and outcomes, demonstrates how solutions might be tailored to the operating environment. <u>Table 4-1</u> provides a summary of the four builds and how the

763 products were distributed across them. Detailed descriptions of the installation, configuration, and

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

Capability	Build 1	Build 2	Build 3	Build 4
	PCS		CRS	
Application Allowlisting	Carbon Black	Windows SRP	Windows SRP	Carbon Black
Behavior Anomaly Detection ,	PI Server	PI Server	PI Server	PI Server
Hardware/Software/Firmware Modification Detection	Tenable.ot	eyeInspect	Dragos	Azure Defender for IoT
File Integrity Checking	Carbon Black	Wazuh	Wazuh	Carbon Black
	ForceField, WORMdisk	ForceField, WORMdisk	ForceField, WORMdisk	ForceField, WORMdisk
User Authentication and Authorization	ConsoleWorks	Dispel	ConsoleWorks	Dispel
Remote Access	AnyConnect	Dispel	AnyConnect	Dispel

766 <u>Sections 4.1, 4.2, 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. <u>Section 4.5</u> describes the network and security

architectures that are used to implement the above security capabilities.

# 770 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 <u>Sections 4.3</u> and <u>4.4</u>.

# 776 **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 (NTP) server
 for time synchronization. Additionally, the environment utilizes virtualized Active Directory (AD) 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.



784 Figure 4-1: CSMS Network Architecture

# 785 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
- 793 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
- 797 of cybersecurity attacks on the continuous process manufacturing environment.
- 798 The PCS includes a software simulator to emulate the TE chemical reaction process. The simulator is
- 799 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
- 801 implemented in MATLAB for process control, a Rockwell FactoryTalk Human Machine Interface(HMI), an
- 802 object linking and embedding for process control (OPC) data access (DA) server, a data historian, an
- 803 engineering workstation, and several virtual LAN (VLAN) switches and network routers. Figure 4-2 and
- 804 <u>Figure 4-3</u> 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
- 806 (sensors) and 12 manipulated variables (actuators). The PCS consists of a software simulated chemical
- 807 manufacturing process (TE process), integrated with a series of COTS hardware, including PLCs,
- 808 industrial network switches, protocol converters, and hardware modules to connect the simulated
- 809 process and the control loop.







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

- 812 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
- 814 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
- 816 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
- 819 supervisory LAN along with the Local Historian, OPC Server, and the Supervisory PLC.
- 820 The Operations LAN (VLAN1) simulates a central control room environment. The supervisory LAN
- 821 (VLAN2) simulates the process operation/ manufacturing environment, which typically consists of the 822 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
- 827 Simulink interface to communicate with the OPC DA server directly.

#### 828 Figure 4-4: PCS Network



# 829 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 of machine doors, activating operator control panel buttons, etc.).

- 835 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
- 837 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.

#### 839 Figure 4-5: The CRS Workcell



- 840 The CRS network, shown in Figure 4-6, is hierarchically architected, separating the supervisory devices
- 841 from the low-level OT that control the manufacturing process. The top-level router is a Siemens
- 842 RUGGEDCOM RX1510, which provides firewall capabilities, logical access to the Testbed LAN network,
- 843 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
- 845 Supervisory LAN is handled by a Netgear GS724T-managed Ethernet switch, and network traffic for the
- 846 Control LAN is handled by a Siemens i800-managed Ethernet switch.

847 Figure 4-6: CRS Network



# 848 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.
- 852 4.5.1 Build 1

For Build 1, the technologies in <u>Table 4-2</u> were integrated into the PCS environment, Testbed LAN, and DMZ segments of the testbed environment to enhance system and information integrity capabilities.
#### 855 Table 4-2: Build 1 Technology Stack to Capabilities Map

Capability	Products	Description
Application Allowlisting	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 environment, and DMZ to control application execution.
Behavior Anomaly Detection, Hardware/Software/Firmware 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 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 scanning.
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 environment 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 (PLC Programs), and executable files for the ICS environment.
User Authentication and Authorization	ConsoleWorks	Deployed to centralize the access and management of the systems and credentials. ConsoleWorks is deployed to the Testbed LAN to allow connections to the PCS environment.

Capability	Products	Description
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 4-7.



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

### 857 4.5.2 Build 2

- 858 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.
- 860 Table 4-3: Build 2 Technology Stack to Capabilities Map

Capability	Product	Description
Application Allowlisting	Windows SRP	AD Group Policy Objects (GPOs) are used to configure and administer the Windows Software Restriction Policy (SRP) capabilities within the Testbed LAN environment and PCS environments. For non-domain systems (e.g., Dispel VDI and DMZ systems), the GPO was applied as local settings on the systems.
Behavior Anomaly Detection, Hardware/Software/Firmware Modification Detection	Pl Server	Deployed in the DMZ and PCS environments, the PI Server provides the historian repository for process data through its Data Archive and generates 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 inventory 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 environment 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 Authorization	Dispel	The Dispel Wicket is deployed to the DMZ environment and integrated with the Dispel
Remote Access		cloud-based environment to provide a virtual desktop interface (VDI) with a secure remote connection to the testbed environment. Through this connection, authorized users are permitted to access resources in both the Testbed LAN and PCS environment.

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



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

### 863 4.5.3 Build 3

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

- 865 integrity capabilities.
- 866 Table 4-4: Build 3 Technology Stack to Capabilities Map

Capability	Products	Description
Application Allowlisting	Windows SRP	AD Group Policy Objects (GPOs) are used to configure and administer the Windows Software Restriction Policy (SRP) capabilities within the Testbed LAN environment and CRS environments.
Behavior Anomaly Detection, Hardware/Software/Firmware 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 generates 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 interface.
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 environment 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 environment.
User Authentication and Authorization	ConsoleWorks	Deployed to centralize the access and management of the systems and credentials. ConsoleWorks 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.

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

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



#### 869 4.5.4 Build 4

- 870 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.
- 872 Table 4-5: Build 4 Technology Stack to Capabilities Map

Capability	Products	Description
Application Allowlisting	Carbon Black	Deployed within the Testbed LAN environment with the Carbon Black agents installed on key workstations and servers to control application execution.
Behavior Anomaly Detection, Hardware/Software/Firmware Modification Detection	Pl Server	Deployed in the DMZ and CRS environments, the PI Server provides the historian repository for process data through its Data Archive and generates Event Frames upon detection of abnormal manufacturing system behavior.
	Azure Defender for loT	Passively monitors the CRS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports and is also configured to capture detailed asset 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 environment 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 environment.
User Authentication and Authorization	Dispel	The Dispel Wicket is deployed to the DMZ environment 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 connection, authorized users are permitted to access resources in both the Testbed LAN and CRS environment.

873 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



### 874 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.

#### 878 **5.1 Assumptions and Limitations**

- 879 The security characteristic analysis has the following limitations:
- 880 It is neither a comprehensive test of all security components nor a red-team exercise.
- 881 It cannot identify all weaknesses.
- 882
   883
   883
   884
   884
   885
   884
   886
   884
   885
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886
   886

#### 885 **5.2 Example Solution Testing**

- 886 This section presents a summary of the solution testing and results. A total of eleven tests were 887 developed for the builds. The following information is provided for each scenario:
- 888 **Objective:** Purpose of the scenario and what it will demonstrate
- 889 **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
- 892 Assumptions: Assumptions about the cyber-environment
- 893 Security Capabilities and Products: Capabilities and products demonstrated during the scenario
- 894 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
- 897 Actual Test Results: Confirm the expected results
- 898 Overall Result: Were the security capabilities and products able to meet the objective when the scenario was executed (PASS/FAIL rating).
- 900 Additional information for each scenario such as screenshots captured during the execution of the test
- 901 procedures and detailed results from the security capabilities are presented in <u>Appendix D</u>.

### 902 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 <i>Cybersecurity Framework</i> 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	Build 1:
Products	<ul> <li>Carbon Black: Application Allowlisting</li> </ul>
	Build 2:
	<ul> <li>Windows SRP: Application Allowlisting</li> </ul>
	Build 3:
	<ul> <li>Windows SRP: Application Allowlisting</li> </ul>
	Build 4:
	<ul> <li>Carbon Black: Application Allowlisting</li> </ul>
Test Procedures	1. Attempt to execute malware on the target machine.
Expected Results	<ul> <li>The application allowlisting tool will detect and stop the malware upon execution.</li> </ul>
Actual Test Results	<ul> <li>The application allowlisting technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> </ul>
Overall Result	PASS

Objective	This test demonstrates the detection of malware introduced from the network.	
Description	An attacker pivoting from the corporate network into the manufacturing environment attempts to insert malware to establish persistence 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: Application Allowlisting</li> </ul>	
	<ul> <li>Tenable.ot: Behavioral Anomaly Detection</li> </ul>	
	Build 2:	
	<ul> <li>Windows SRP: Application Allowlisting</li> </ul>	
	<ul> <li>Forescout eyeInspect: Behavioral Anomaly Detection</li> </ul>	
	Build 3:	
	<ul> <li>Windows SRP: Application Allowlisting</li> </ul>	
	<ul> <li>Dragos: Behavioral Anomaly Detection</li> </ul>	
	Build 4:	
	<ul> <li>Carbon Black: Application Allowlisting</li> </ul>	
	<ul> <li>Azure Defender for IoT: Behavioral Anomaly Detection</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>	

### 903 5.2.2 Scenario 2: Protect Host from Malware Infection via Network Vector

Expected Results	<ul> <li>The application allowlisting capabilities installed on target systems will block execution of the malicious code.</li> </ul>
	<ul> <li>The behavioral anomaly detection tool will capture the suspicious traffic and generate an alert.</li> </ul>
Actual Test Results	<ul> <li>The application allowlisting technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> </ul>
	<ul> <li>The BAD tool is able to detect and alert on activity pivoting into manufacturing systems.</li> </ul>
Overall Result	PASS

### 904 5.2.3 Scenario 3: Protect Host from Malware via Remote Access Connections

Objective	This test demonstrates blocking malware that is attempting to infect the manufacturing system through authorized remote access connections.
Description	A remote workstation authorized to use a remote access connection has been infected with malware. When the workstation is connected to the manufacturing environment through the remote access connection, the malware attempts to pivot and spread to vulnerable host(s).
Relevant NIST <i>Cybersecurity Framework</i> Subcategories	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 Capabilities and	Build 1:
Products	Cisco VPN: Remote Access
	<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:
	Cisco VPN: Remote Access
	<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

### 905 5.2.4 Scenario 4: Protect Host from Unauthorized Application Installation

Objective	This test demonstrates blocking installation and execution of unauthorized applications on a workstation in the manufacturing system.
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 unauthorized software on the workstation.

Relevant NIST <i>Cybersecurity Framework</i> 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>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	<ul> <li>Carbon Black: Application Allowlisting</li> </ul>
	<ul> <li>Tenable.ot: Behavioral Anomaly Detection</li> </ul>
	Build 2:
	<ul> <li>Windows SRP: Application Allowlisting</li> </ul>
	<ul> <li>eyeInspect: Behavioral Anomaly Detection</li> </ul>
	Build 3:
	<ul> <li>Windows SRP: Application Allowlisting</li> </ul>
	<ul> <li>Dragos: Behavioral Anomaly Detection</li> </ul>
	Build 4:
	<ul> <li>Carbon Black: Application Allowlisting</li> </ul>
	<ul> <li>Azure Defender for IoT: Behavioral Anomaly Detection</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.
	3. The user attempts to execute software that does not require installation.
Expected Results	<ul> <li>The application allowlisting 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 application allowlisting technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> </ul>
	<ul> <li>The BAD tool is able to detect and alert on activity in the manufacturing system.</li> </ul>
Overall Result	PASS

### 906 5.2.5 Scenario 5: Protect from Unauthorized Addition of a Device

Objective	This test demonstrates detection of an unauthorized device connecting to the manufacturing system.
Description	An individual authorized to access the physical premises connects and uses an unauthorized device on the manufacturing network.
Relevant NIST <i>Cybersecurity Framework</i> 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	Build 1:
Products	<ul> <li>Tenable.ot: Behavioral Anomaly Detection</li> </ul>
	Build 2:
	<ul> <li>eyeInspect: Behavioral Anomaly Detection</li> </ul>
	Build 3:
	<ul> <li>Dragos: Behavioral Anomaly Detection</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: Behavioral Anomaly Detection</li> </ul>
Test Procedures	<ol> <li>The individual connects the unauthorized device to the manufacturing network.</li> </ol>
	<ol><li>The individual uses an unauthorized device to access other devices on the manufacturing network.</li></ol>
Expected Results	<ul> <li>The behavioral anomaly detection tool will capture the suspicious traffic and generate an alert.</li> </ul>

Actual Test Results	<ul> <li>The behavioral anomaly detection tool is able to detect and alert on activity in the manufacturing system.</li> </ul>
Overall Result	PASS

### 907 5.2.6 Scenario 6: Detect Unauthorized Device-to-Device Communications

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>Cybersecurity Framework</i> 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 environment has a predictable communications pattern.</li> </ul>
Security Capabilities and	Build 1:
Products	<ul> <li>Tenable.ot: Behavioral Anomaly Detection.</li> </ul>
	Build 2:
	<ul> <li>eyeInspect: Behavioral Anomaly Detection.</li> </ul>
	Build 3:
	<ul> <li>Dragos: Behavioral Anomaly Detection.</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: Behavioral Anomaly Detection.</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

### 908 5.2.7 Scenario 7: Protect from Unauthorized Deletion of Files

Objective	This test demonstrates protection of files from unauthorized deletion both locally and on network file share.
Description	An authorized user attempts to delete files on an engineering workstation and a shared network drive within the manufacturing system.
Relevant NIST <i>Cybersecurity Framework</i> Subcategories	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	<ol> <li>User attempts to delete files located on a workstation in the manufacturing system.</li> </ol>
	<ol><li>User attempts to delete files from the network file share containing the golden images for the manufacturing system.</li></ol>

Expected Results	<ul> <li>Deletion of files on the workstation will be detected and alerted on by the file integrity checking tool.</li> <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

### 909 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 modification of the PLC logic from an engineering workstation.
Relevant NIST <i>Cybersecurity Framework</i> Subcategories	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 Products	<ul> <li>Build 1:</li> <li>Tenable.ot: Behavioral Anomaly Detection and Software Modification</li> <li>Cisco VPN: Remote Access</li> <li>ConsoleWorks: User Authentication, User Authorization, and Remote Access</li> <li>Build 2:</li> <li>eyeInspect: Behavioral Anomaly Detection and Software Modification</li> <li>Dispel: User Authentication and User Authorization, and</li> </ul>

	Build 3:
	<ul> <li>Dragos: Behavioral Anomaly Detection and Software Modification</li> </ul>
	<ul> <li>Cisco VPN: Remote Access</li> </ul>
	<ul> <li>ConsoleWorks: User Authentication, User Authorization, and Remote Access</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: Behavioral Anomaly Detection 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> </ol>
	2. The user modifies and downloads a logic file to the PLC.
Expected Results	<ul> <li>The behavioral anomaly detection 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 behavioral anomaly detection tool is able to detect and alert on activity accessing the PLC.</li> </ul>
Overall Result	PASS

### 910 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 archive data.
Relevant NIST <i>Cybersecurity Framework</i> Subcategories	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: Behavioral Anomaly Detection.</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>
	Build 2:
	<ul> <li>eyeInspect: Behavioral Anomaly Detection.</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>
	Build 3:
	<ul> <li>Dragos: Behavioral Anomaly Detection.</li> </ul>
	<ul> <li>ForceField WFS: File Integrity Protection.</li> </ul>
	Build 4:
	<ul> <li>Azure Defender for IoT: Behavioral Anomaly Detection.</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

### 911 5.2.10 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>Cybersecurity Framework</i> Subcategories	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: Behavioral Anomaly Detection</li> </ul>
Test Procedures	1. A sensor sends invalid data to the historian.
Expected Results	<ul> <li>The behavioral anomaly detection capability will detect atypical sensor data and generate alerts.</li> </ul>
Actual Test Results	<ul> <li>The behavioral anomaly detection tool is able to detect atypical data and create an event frame.</li> </ul>
Overall Result	PASS

### 912 5.2.11 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>Cybersecurity Framework</i> 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>None</li> </ul>

Security Capabilities and	Build 1:
Products	<ul> <li>Cisco VPN: Remote Access.</li> </ul>
	<ul> <li>ConsoleWorks: Remote Access, User Authentication, and User Authorization.</li> </ul>
	<ul> <li>Tenable.ot: Behavioral Anomaly Detection and Firmware Modification.</li> </ul>
	Build 2:
	<ul> <li>Dispel: Remote Access, User Authentication, and User Authorization.</li> </ul>
	<ul> <li>eyeInspect and ICSPatrol: Behavioral Anomaly Detection 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: Behavioral Anomaly Detection 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: Behavioral Anomaly Detection 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 behavioral anomaly tool is able to detect and generate alerts for updates to PLC component firmware.</li> </ul>
Overall Result	PASS

### 913 **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

917 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* 

919 *Framework* Subcategories as a basis for organizing our analysis allowed us to systematically consider 920 how well the reference design supports the intended security characteristics.

# 921 5.3.1 PR.AC-1: Identities and credentials are issued, managed, verified, revoked, 922 and audited for authorized devices, users, and processes

This NIST *Cybersecurity Framework* Subcategory is supported through the 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.

#### 926 5.3.2 PR.AC-3: Remote access is managed

927 This NIST *Cybersecurity Framework* Subcategory is supported by remote access tools integrated with the 928 user authentication and authorization systems. Together, these tools provide a secure channel for an 929 authorized user to access the manufacturing environment from a remote location. These tools are 930 configurable to allow organizations to control who can remotely access the system, what the user can 931 access, and when access is allowed by a user.

# 932 5.3.3 PR.AC-4: Access permissions and authorizations are managed, 933 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 the 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

940 perform the operations, and operations that are performed outside of the designated time frame.

# 941 5.3.4 PR.AC-7: Users, devices, and other assets are authenticated (e.g., single942 factor, multi-factor) commensurate with the risk of the transaction (e.g., 943 individuals' security and privacy risks and other organizational risks)

This NIST *Cybersecurity Framework* Subcategory is supported through the user authentication and user authorization capabilities in addition to the native credential management capabilities associated with the tools. Based on the risk assessment of the lab, 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 to for remote access.

949 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.

## 954 5.3.6 PR.DS-6: Integrity checking mechanisms are used to verify software,955 firmware, and information integrity

956 This NIST *Cybersecurity Framework* Subcategory is supported through file integrity checking tools and

957 the behavioral anomaly detection tools. The file integrity checking tools monitor the information on the

958 manufacturing end points for changes. The behavioral anomaly detection tools monitor the

959 environments for changes made to software, firmware, and validate sensor and actuator information.

#### 960 5.3.7 PR.IP-4: Backups of information are conducted, maintained, and tested

961 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

964 modifying or deleting data that is on the disk.

# 965 5.3.8 PR.MA-1: Maintenance and repair of organizational assets are performed966 and logged, with approved and controlled tools

This NIST *Cybersecurity Framework* Subcategory is supported by a combination of tools including
 application allowlisting, the user authentication and user authorization tools, and the behavior anomaly

969 detection tools. User authentication and user authorization tools provide a controlled environment for

970 authorized users to interact with the manufacturing environment. Behavior anomaly detection tools

971 provide a means to detect maintenance activities in the environment such as PLC logic modification or

#### 972 PLC firmware updates via the network. This information can be combined with data from a

- 973 computerized maintenance management system to ensure that all maintenance activities are
- appropriately approved and logged. Also, application allowlisting prevents unapproved software from
- 975 running on systems to ensure that only approved tools are used for maintenance activities.

# 976 5.3.9 PR.MA-2: Remote maintenance of organizational assets is approved, 977 logged, and performed in a manner that prevents unauthorized access

978 This NIST *Cybersecurity Framework* Subcategory is supported by the remote access capability integrated 979 with the user authentication and user authorization system. The tools in the solution were used to grant 980 access for performing remote maintenance on specific assets. The tools prevent unauthorized users 981 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

984 This NIST *Cybersecurity Framework* Subcategory is supported by behavior anomaly detection tools.

985 Network baselines were established and approved based on an understanding of normal operations and986 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

989 This NIST *Cybersecurity Framework* Subcategory is supported by all the capabilities included in the

990 solutions. Logs of suspicious activities from the tools can be used by security managers and engineers to

991 understand what unusual activity has occurred in the manufacturing system. Analyzing these logs

992 provides a mechanism to determine what systems were accessed and what actions may have been

- 993 performed on them. Although not demonstrated in these solutions, an analytic engine would enhance994 the detection capability of the solution.
- 5.3.12 DE.AE-3: Event data are collected and correlated from multiple sources andsensors
- 997 This NIST *Cybersecurity Framework* Subcategory is supported by all the capabilities included in the
- 998 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
- 1000 and event management (SIEM) tool would enhance the detection capability of the solution.

# 1001 5.3.13 DE.CM-1: The network is monitored to detect potential cybersecurity1002 events

1003 This NIST Cybersecurity Framework Subcategory is supported by the behavioral anomaly detection and 1004 remote access capabilities used in the example solutions to monitor the manufacturing network to 1005 detect potential cybersecurity events. The behavioral anomaly detection tools monitor network 1006 communications at the external boundary of the system and at key internal points within the network, 1007 along with user activities and traffic patterns, and compare it to the established baseline. The remote 1008 access capabilities monitor the network communications at the external boundary of the system. This 1009 helps detect unauthorized local, network, and remote connections and identify unauthorized use of the 1010 manufacturing system.

# 1011 5.3.14 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity1012 events

1013 This NIST Cybersecurity Framework Subcategory is supported by the authentication and authorization 1014 tools that allow for monitoring personnel activity while connected through these tools. Further, 1015 application allowlisting and file integrity checking tools provide the ability to monitor user actions on 1016 hosts. Additionally, behavioral anomaly detection tools monitor and record events associated with 1017 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 1018 1019 monitored individually or collectively to support investigations for potential malicious or unauthorized 1020 activity within the environment.

# 1021 5.3.15 DE.CM-7: Monitoring for unauthorized personnel, connections, devices,1022 and software is performed

1023 This NIST Cybersecurity Framework Subcategory is supported by behavioral anomaly detection, 1024 application allowlisting, user authentication and user authorization, and remote access capabilities of 1025 the solutions. The behavioral anomaly detection tools established a baseline of information for 1026 approved assets and connections. Then the manufacturing network is monitored using the behavioral 1027 anomaly detection capability for any deviation by the assets and connections from the established 1028 baseline. If any deviation is detected, an alert is generated. Additionally, the application allowlisting tool 1029 blocks any unauthorized application installation or execution and generates an alert on these events. 1030 User authentication and user authorization tools monitor for unauthorized personnel connecting to the 1031 environment. Remote access capabilities monitor for unauthorized connections to the environment.

### 1032 6 Future Build Considerations

1033 This guide has presented technical solutions for maintaining and monitoring system and information 1034 integrity, which will help detect and prevent incidents in a manufacturing environment. Future builds 1035 should demonstrate methods and techniques for fusing event and log data from multiple platforms into 1036 a security operations center (SOC) to improve monitoring and detection capabilities for an organization. 1037 Future builds should also demonstrate how to recover from a loss of system or information integrity

- such as a ransomware attack for ICS environments.
- 1039 Additionally, trends in manufacturing such as Industry 4.0 and the industrial IoT are increasing
- 1040 connectivity, increasing the attack surface, and increasing the potential for vulnerabilities. Future builds
- 1041 should consider how these advances can be securely integrated into manufacturing environments.

#### DRAFT

1042	Appendix A	List of Acronyms
1043	AAL	Application Allowlisting
1044	AD	Active Directory
1045	BAD	Behavioral Anomaly Detection
1046	CRS	Collaborative Robotic System
1047	CRADA	Cooperative Research and Development Agreement
1048	CSF	NIST Cybersecurity Framework
1049	CSMS	Cybersecurity for Smart Manufacturing Systems
1050	DMZ	Demilitarized Zone
1051	EL	Engineering Laboratory
1052	FOIA	Freedom of Information Act
1053	ICS	Industrial Control System
1054	ют	Internet of Things
1055	ІТ	Information Technology
1056	KSA	Knowledge, Skills and Abilities
1057	LAN	Local Area Network
1058	NCCoE	National Cybersecurity Center of Excellence
1059	NFS	Network File Share
1060	NIST	National Institute of Standards and Technology
1061	NISTIR	NIST Interagency or Internal Report
1062	NTP	Network Time Protocol
1063	ОТ	Operational Technology
1064	PCS	Process Control System
1065	PLC	Programmable Logic Controller
1066	SCADA	Supervisory Control and Data Acquisition

1067	SIEM	Security Information and Event Management
1068	SMB	Server Message Block
1069	SOC	Security Operations Center
1070	SP	Special Publication
1071	SRP	Software Restriction Policies
1072	SSH	secure shell
1073	VDI	Virtual Desktop Interface
1074	VLAN	Virtual Local Area Network
1075	VPN	Virtual Private Network

### 1076 Appendix B Glossary

Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).
	SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009
Architecture	A highly structured specification of an acceptable approach within a framework 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, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, 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 computing 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 unauthorized or accidental manner.
	SOURCE: CNSSI-4009
File Integrity Checking	Software that generates, stores, and compares message digests for files to detect 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 execution of the programs.
	SOURCE: CNSSI 4009-2015
Industrial Control Systems	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution.
	SOURCE: NIST SP 800-30 Rev. 1

Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide 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, processing, maintenance, use, sharing, dissemination, or disposition of information.
	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, movement, 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 networks.
	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, provides 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 systems
	SOURCE: NIST SP 800-115

### 1077 Appendix C References

1078 1079	[1]	C. Singleton et al., X-Force Threat Intelligence Index 2021, IBM, February 2021, <a href="https://www.ibm.com/security/data-breach/threat-intelligence">https://www.ibm.com/security/data-breach/threat-intelligence</a>
1080 1081	[2]	A Sedgewick et al., <i>Guide to Application Whitelisting</i> , NIST SP 800-167, NIST, Oct. 2015. Available: <u>http://dx.doi.org/10.6028/NIST.SP.800-167</u> .
1082 1083 1084 1085	[3]	Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance, 2015. Available: <u>https://www.cisa.gov/sites/default/files/publications/critical-manufacturingcybersecurity-framework-implementation-guide-2015-508.pdf</u> .
1086 1087 1088	[4]	Executive Order no. 13636, <i>Improving Critical Infrastructure Cybersecurity, DCPD201300091</i> , Feb. 12, 2013. Available: <u>https://obamawhitehouse.archives.gov/the-press-</u> office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
1089 1090	[5]	NIST, Framework for Improving Critical Infrastructure Cybersecurity, V1.1 April 16, 2018. Available: <u>https://doi.org/10.6028/NIST.CSWP.04162018</u> .
1091 1092 1093	[6]	J. McCarthy et al., Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection, NIST Interagency Report (NISTIR) 8219, NIST, Nov. 2018. Available: <a href="https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf">https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf</a> .
1094 1095	[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> .
1096 1097	[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> .
1098 1099	[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> .
1100 1101 1102	[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> .
1103 1104 1105	[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> .
1106 1107	[12]	Celia Paulsen, Robert Byers, Glossary of Key Information Security Terms NISTIR 7298, <a href="https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf">https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf</a> .
1108[13]U.S.-Canada Power Systems Outage Task Force, Final Report on the August 14, 2003 Blackout in1109the United States and Canada: Causes and Recommendations. Available:1110https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/Outage Task Force1111- DRAFT\_Report\_on\_Implementation.pdf

- 1112[14]K. Stouffer et al., Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Revision 2,1113NIST, June 2015, Available: <a href="https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82">https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-</a>111482r2.pdf
- 1115 [15] J. J. Downs and E. F. Vogel, "A Plant-wide Industrial Problem Process," Comput. Chem. Eng., vol.
  1116 17, no. 3, 1993, pp. 245–255.

## 1117 Appendix D Scenario Execution Results

- 1118 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 areprovided for reference only.

## 1121 D.1 Executing Scenario 1: Protect Host from Malware via USB

1122 An authorized user inserts a USB storage device containing a malware file (*1.exe*) into a system in the 1123 manufacturing environment (e.g., an engineering workstation). After insertion, the malware file (1.exe)

- 1124 attempts to execute. The expected outcome is that the application allowlisting technology blocks the
- 1125 execution of the file.
- 1126 D.1.1 Build 1
- 1127 D.1.1.1 Configuration
- 1128 Application Allowlisting: Carbon Black
- Agent installed on an HMI Workstation and configured to communicate to the Carbon
   Black Server.
- 1131 *D.1.1.2 Test Results*
- 1132 Carbon Black successfully detects and blocks the malware (1.exe) from running as shown in Figure D-1.
- 1133 Figure D-2 shows Carbon Black's server log. The log provides more detail on the activity detected by
- 1134 Carbon Black.

1135 Figure D-1: An Alert from Carbon Black Showing that Malware (1.exe) was Blocked from Executing

Security Notification - Unapproved File									
Cb B 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:\									
۲									
Approval Request									
Enter your reason for access (512 characters Your Email:									
Priority: Medium									
Submit									
Protection by Carbon Black, Inc.									

1136 Figure D-2: Carbon Black's Server Provides Additional Details and Logs of the Event

	CB-Server	:lan.lab Home ▼	Reports ▼ Assets ▼ Rule	is ▼ Tools ▼		0	0	•
Home > Events						Version 8.1.10.3		
(The Current View Has Unsave	ed Changes - E	Discard) Cache	Group By: Add (none) v	Subgroup Ascending V (none)	By:	Max Age: None v		
ed before v 04/02 on contains v t.exe Cancel Reset	3/2021 15:2	23.08	•					
earch:		Au	tomatically apply Showing Show	5 out of ?? item(s)				
Timestamp 🝷	Severity	Туре	Subtype	Source	Description		IP Address	User
Apr 7 2021 02:51:09 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,IsD	d new file 'e:\1.exe' [2D2CBA1224]. DiscoveredBy[Kernel:Execute] overed[4/7/2021 6:51:09 PM (Hash: 4/7/2021 6:51:09 PM)] epIncompatibleExe]	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 block	ed 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,IsD	d 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)] epIncompatibleExe]	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 block	ed 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 new FileCreated[8/24/2020 2:23:10 PM] Disc YaraClassifyVersionId[2] Rules[IsExe,IsD	/ 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 ?? item(s)					Showing all data			

1137 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]

- 1138 D.1.2 Build 2
- 1139 D.1.2.1 Configuration
- 1140 Application Allowlisting: windows SRP
- Allowlisting policies are applied to HMI Workstation.
- 1142 *D.1.2.2 Test Results*
- 1143 The execution of *1.exe* is blocked successfully when Windows SRP is enforced as shown in Figure D-4.
- 1144 Figure D-4: Windows 7 Alert as a Result of Windows SRP Blocking the Execution of 1.exe



## 1145 D.1.3 Build 3

- 1146 D.1.3.1 Configuration
- 1147 Application Allowlisting: Windows SRP
- Allowlisting policies are applied to Engineering Workstation.
- 1149 *D.1.3.2 Test Results*
- 1150 For Build 3, Windows SRP application allowlisting is enabled in the Collaborative Robotics environment.
- 1151 Figure D-5 shows that the executable is blocked on the CRS workstation.

1152 Figure D-5: Windows 10 Alert as a Result of Windows SRP Blocking the Execution of 1.exe



- 1153 D.1.4 Build 4
- 1154 D.1.4.1 Configuration
- 1155 Application Allowlisting : Carbon Black
- Agent installed on Engineering Workstation and configured to communicate to the Carbon
   Black Server.
- 1158 D.1.4.2 Test Results
- 1159 Carbon Black successfully detects and blocks the malicious file as shown by the Carbon Black notification 1160 in Figure D-6.

#### 1161 Figure D-6: Carbon Black Blocks the Execution of 1.exe for Build 4

Security Notification - Unapproved File

Cb Port Target: 1 Path: e Process: e	.exe :\ xplorer.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.								
,				or				
Submit Approval Requ	est>>			OK				
Process	Target		Path		_			
1 explorer.exe	1.exe		e:\		-			
<					>			
Approval Request					_			
Enter your reason for max).	access (512 characters 🔺	Yc Pr	our Email: riority: Medium	▼ Submit				
Protection by Carbon Bla	ick Inc							

## 1162 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.

## 1170 D.2.1 Build 1

1173

1174

1176

- 1171 D.2.1.1 Configuration
- 1172 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.
- 1175 Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## 1177 *D.2.1.2 Test Results*

- 1178 Abnormal network traffic is detected by Tenable.ot as shown in Figure D-7. Figure D-8 shows the initial
- 1179 RDP connection between an external system and the DMZ system, and <u>Figure D-9</u> provides more detail
- 1180 of the session activity. Figure D-10 show that Tenable.ot detected VNC connection between the DMZ
- 1181 and the Testbed LAN. Figure D-11 shows a detected ports scan performed by the DMZ system target at a
- 1182 system in the Testbed LAN. Tenable.ot detected the RDP scan from the DMZ to the NESSUS VM in the
- 1183 Testbed LAN, as shown in Figure D-12, and Figure D-13 provides more details on that detected event.
- 1184 The execution of the malware (1.exe) is blocked by Carbon Black agent as shown in Figure D-14.
- 1185 Figure D-7: Tenable.ot Dashboard Showing the Events that were Detected

tenable.ot Powered by Indegy							01:54 PM	Tuesday, Apr 13, 202	
Events			-						
All Events	All Events	Search	٩				Ad	tions 🗸 Resolve All	Export G
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	
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		SvsLog	
Controllers	19267	02:53:39 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		LAN-AD02	
Network Assets	19269	02:53:35 PM · Apr 12, 2021	Port Scan	High	SYN Scan Detected	HistorianDMZ		WSUSVM	
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	
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	
	4								•
	Items: 1-100 out o	f 17135						K < Page	e1of172 > >
	Event 19308 1	2:25:03 PM · Apr 13, 2021 Port	Scan High Not resolved						
	Details	A Dest even is a nuch	a to usual what make and again	nd listening on a					
	Source	A Port scan is a prob	e to reveal what ports are open a	nd listening on a	i given asser				
	Affected Assets	SOURCE NAME	SOURCE NAME OPC Server Why is this important?						
	Policy	SOURCE ADDRESS				and the second se			
	Scanned Ports	DEPTHATION	Server #22		Port scans are p communication	art of mapping channels to an asset.	Make sur source of	e that you are familiar w f the port scan and that ti	ith the his port
	Status	DESTINATION NAME	201401-922		Some port scan	s are legitimate and don	e scan was	expected. In case you ar	e not

1186 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	

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

Details	A conversation in a	an unauthorized protocol has been detected
Source		
Destination	SOURCE NAME	Work Station #19
Policy	SOURCE ADDRESS	
Status	DESTINATION NAME	HistorianDMZ
	DESTINATION ADDRES	55
	PROTOCOL	RDP (tcp/3389)
	PORT	3389
	PROTOCOL GROUP	In Any Protocol

1189 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	on known traffic patterns			
ule Details						
ource	SOURCE NAME	HistorianDMZ	Why is this important?	Suggested Mitigation		
estination	SOURCE ADDRESS	10.100.1.4	Intrusion detection events may indicate	Make sure that the source and destination		
olicy	DESTINATION NAME	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		
itus	DESTINATION ADDRESS	10.100.0.40   172.16.2.1	important to be aware of any such traffic that may indicate reconnaissance activity, attacks on the network or propagation of a	may consider updating anti-virus definitions, firewall rules or other security patches. You can open the Rule Details panel to view additional details about this particular rule.		
	PROTOCOL	rfb (tcp/5900)	threat to/from other subnets of the network.			
	PORT	5900				
	RULE MESSAGE	ET SCAN Potential VNC Scan 5900-5920				
	SID	2002911				

1190 Figure D-11: Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in

## 1191 the Testbed LAN

Details	A Port scan is a probe to reveal what ports are open and listening on a given a	asset			
Source Affected Assets	SOURCE NAME HistorianDMZ	Why is this important?	Suggested Mitigation		
olicy canned Ports	SOURCE ADDRESS 10.100.1.4	Port scans are part of mapping	Make sure that you are familiar with the		
	DESTINATION NAME LARLOR	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 familiar with the source check with the source asset owner to see whether this w		
tatus	DESTINATION ADDRESS 10.100.0.101   192.168.0.205	monitoring devices in the network. However, such mapping may also be done in the early stages of an attack, in order to			
	PROTOCOL CCP	detect vulnerable and accessible ports for malicious communication.	check which other assets have been scanned by the source asset and consider isolating the source asset to decrease network exposure while you investigate		
	PORT				

1192 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 DMZto a Workstation in the Testbed LAN

Event 19299 03:01:39	PM · Apr 12, 2021 RDP	Connection (Authenticated) Medium Not re	solved			
Details	An authenticated init	tiation of an RDP connection				
Source						
Destination	SOURCE NAME	HistorianDMZ	Why is this important?	Suggested Mitigation		
Policy Status	SOURCE ADDRESS	10.100.1.4	Remote access to a workstation is a	1. Check if this communication was		
	DESTINATION NAME	NESSUSVM	common way for cyber threats to propagate towards their target. Often	approved. 2. Investigate if it was done by an		
	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				

1195 Figure D-14: Attempt to Execute 1.exe Failed

S	ecurity Notification - U	Inapproved File						
Cb Target: 1. Path: c: Process: ex	exe \users\nccoeuser\desktop kplorer.exe	Ν						
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 Reque	<u>est&gt;&gt;</u>	ОК						
Process	Target	Path						
1 explorer.exe	1.exe	c:\users\nccoeuser\desktop\						
<	ш	>						
- Approval Request								
	(E1D shareshare	Your Ferril						
max).	ccess (512 characters A	Tour Email:						
		Priority: Medium						
	~	Submit						
Protection by Carbon Bla	ck, Inc.							

## 1196 D.2.2 Build 2

- 1197 D.2.2.1 Configuration
- 1198 Application Allowlisting: Windows SRP
- Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and
   2.
- 1201 Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## 1203 *D.2.2.2 Test Results*

1202

1204 Figure D-15 shows the RDP alert for connection into the DMZ while Figure D-16 shows the details of the

- alert. Figure D-17 shows a collection of suspicious activity detected by Forescout eyeInspect when
- scanning and an RDP connection is executed. Figure D-18 and Figure D-19 show details of a port
- scanning alert and the second RDP connection into the manufacturing environment, respectively. The
- 1208 attempt to execute malware (1.exe) is blocked by Windows SRP as shown in Figure D-20.

#### 1209 Figure D-15: Alert Dashboard Showing Detection of an RDP Session



1210 Figure D-16: Details of the Detected RDP Session Activity from an External System to DMZ System

<complex-block>Auto dot dot dot dot dot dot dot dot dot d</complex-block>	<) FORESCOU	T. 🙆 Dashboard	A Network	Events	Sen:	sors 😋 Settings				<b>Q</b>	s¶ 🌻	admin
	Alert details	Back Edit	Delete Trin	n Show ~	Assign	to case Download	1921 - Carlos Ca					Help
Kender werden version of the second versi						Weisseld Schercher						
image												
<ul> <li>mary Normal Standard Standard</li></ul>	Summary			^		Source host info		^	Alert Details			^
Net with Net with Net with Net with Net With Net	Alert ID	203138				IP address	(Public IP)		ID and name	lan_cp_cnw_c - Communication patte	rn not whitelist	ed
Net of the second se	Timestamp	Oct 16, 2020 10:05:47				Host MAC addresses	Unknown			Communication pattern not whitelisted: ti	he source and de:	tination hosts
bit     bit <td>Sensor name</td> <td>sensor-bundle-nocoe</td> <td></td> <td></td> <td></td> <td>Other observed MAC</td> <td>(Rackwell)</td> <td></td> <td>Description</td> <td>are whitelisted in some communication ru combination</td> <td>ile, but not with t</td> <td>his</td>	Sensor name	sensor-bundle-nocoe				Other observed MAC	(Rackwell)		Description	are whitelisted in some communication ru combination	ile, but not with t	his
	Detection engine	Communication patterns (LAN	CP)			addresses	(Cisco)		Triggering rule/default	alart		
bit Bit	Profile	8 - TCP communications				Vendor and model	Rochwell		action	alert		
	Severity	Medium				Client protocols	RDP (TCP 3389)					
NormOpportBorneyB	Source MAC	(Cisco)				Server protocols	NotAKnownOne (TCP 4444)					
	Source IP	Corporate Workstation	n			Purdue level	4 - Site business network					
Marcal Marc     Marcal Marc       Decomposition     Marcal Marc       Decomposition     Marcal Marc       Decomposition     Marcal Marcal Marc       Decomposition     Marcal Marca Marca Marcal Marcal Marcal Marca Marcal Marcal Marcal Marcal Mar	Destination IP	0 (pi-dmz)				Security Risk	11000 3.3					
Board       Bia       Colume       Bia         Lyne       Norwe       Bia       Bia         Lyne       Source       Source       Bia         Lyne       Source       Source       Source         Lyne       Source       Source       Source         Lyne       Source       Source       Source         Lyne       Source       Source       Source         Source       Source       Source<	Source port	49932				Operational Risk	B000 0.0					
Lipen     Biten       Space	Destination port	3389				Criticality	RECEL L					
Unit       #         Manual       10         Unit       10         Manual	L2 proto	Ethernet				Known vulnerabilities	0					
Mare       NO       <	L3 proto	IP				Related alerts	6 (Show)					
I per me       0.0       0.0       0.0         Sume       0.0       0.0       0.0       0.0         Sume       0.0       0.0       0.0       0.0       0.0         Sume       0.0       0.0       0.0       0.0       0.0       0.0       0.0         Sume       0.0	L4 proto	TCP				First seen	Oct 14, 2020 11:56:54					
Binding       Marcing         Summer       Summer	L7 proto	RDP				Last seen	Oct 16, 2020 10:16:45					
max       Nonsymple         Max       Max         Max	TCP stream opened in hot	false										
unit       main       main         bit main       intermine       intermine         intermine       intermine       intermi	Statur	Not analyzed				Destination host info		^				
berner     Series       Mainer detector     Series <tr< td=""><td>Labels</td><td>Hot analyzed</td><td></td><td></td><td></td><td>IR address</td><td>(Dei-14) (D)</td><td></td><td></td><td></td><td></td><td></td></tr<>	Labels	Hot analyzed				IR address	(Dei-14) (D)					
Image:	User notes					IP address	(Private IP)					
Matical distance       Mature       Mature         inter distance       Mature       Mature </td <td></td> <td></td> <td></td> <td></td> <td></td> <td>Other bost names</td> <td>promz</td> <td></td> <td></td> <td></td> <td></td> <td></td>						Other bost names	promz					
Meterical networks     Materical Subscription       Name     Advant     UNARDA       Name     Advant     UNARDA       Statu     10000.0004     and         Statu     10000.0004         Statu     100000004 <tr< td=""><td></td><td></td><td></td><td></td><td></td><td>outer nost numes</td><td>Microsoft</td><td></td><td></td><td></td><td></td><td></td></tr<>						outer nost numes	Microsoft					
Autom       Autom       Autom       Bindering         DRUM       1000.020       av         Breiner       Seiner       Bindering         Breiner       Bindering       Bindering         Breiner	Monitored networks			^		Host MAC addresses	Last seen: Oct 16, 2020 10:44:57					
DKLM       10.102.1024       ay       Dec       Color         No       Color       Sec       Sec       Sec         Sec       Sec       Sec       Sec	Name	Address	VLAN IDs			Other observed MAC	(Rackwell)					
NorExematationOber andSecond Second Secon	DMZ LAN	10.100.1.0/24	anv		- 1	addresses	(Cisco)					
Other roles       Microsour soluticates, Terma lands:         Disk microsour 2016       Microsour 2016         Disk microsour 2017       Microsour 2018         Disk microsour 2018       Microsour 2018         Microsour 2019       Microsour 2018         Microsour 2018       Microsour 2018         Microour 2018       Microur 2018						Role	Terminal server					
Of wration       Writesine flow Wratesine Signed         Writesine Flow Wratesine Signed       References flow 301         Stream Protocol       Refere						Other roles	Windows workstation, Terminal client					
CHear pressors       Ref (7 48) (10 + 10 + 10 + 10 + 10 + 10 + 10 + 10 +						OS version	Windows 10 or Windows Server 2016					
Dist (Dis 5), 353, 313, 314, 4017, 4013, 4017,							AFP (TCP 445) DCOM (TCP 135)					
Giver protection       Rester control							DNS (UDP 53, 5353, 5355)	10105				
River protection       River protection         River protection							54128, 62531, 62532, 62841, 62899)	, 49195,				
Clever protocols       Clever protocols         NextNown-Over (10) 701         Server protocols       NextNown-Over (10) 701         Server							HTTP (TCP 80, 445, 8530) Kerberos (TCP 445)					
Market of 1931         Name of 1971							LDAP (TCP 445)					
Gleet protocol       NoCas (T0 19)         NoCas (T0 19)       NoCas (T0 19)         State (T0 14)       NoCas (T0 19)         NoCas (T0 14)       NoCas (T0 14)         NoCas (T0 14)       NoCas (T0 19)         NoCas (T0 14)       NoCas (T0 14)         NoCas (T0 14							MSSQL (TCP 445) NTP (UDP 123)					
Client protocols       Notation for Notation for Display 100 441 104, 1314, 2309, 2300, 43403, 4724, 2014, 4709, 44102, 4400, 398 (100 193) 309 398 (100							NetBIOS (UDP 137)					
Next Mexicol Constants Next Mexicol Constant Next Mexicol Constant Ne						Client protocols	NotAKnownOne (TCP 445)					
Server protection         Server protection <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td>NotAKnownOne (UDP 443, 1434, 1514, 3389, 32904, 434 43734 43789 44102 44690)</td><td>163, 43724,</td><td></td><td></td><td></td><td></td></t<>							NotAKnownOne (UDP 443, 1434, 1514, 3389, 32904, 434 43734 43789 44102 44690)	163, 43724,				
Before State         State State							OsisoftPI (TCP 5450)					
MSEDD F130 SSP (UD F130) SSP (UD F130) SSP (UD F22) SSP (UD F22)							KDP (1CP 3389) SMB (TCP 445)					
Server protocols Server proto							SMB (UDP 138) SSDP (UDP 1900)					
Survey (107 443, 445) Survey (107 445, 445)							SSH (TCP 22)					
M0,Decomy (UD 9730)           Felectometric (UT 5942, 1574, 1577, 1585, 2311, 2886), 48690, 48694           M0,Bell           Felectometric (UT 592, 357)           Server protocols           M0,Decomy (UD 9730)           SM (TC 448)           SM (TC 448) <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>SSE (TCP 443, 445) SunRPC (TCP 445)</td> <td></td> <td></td> <td></td> <td></td> <td></td>							SSE (TCP 443, 445) SunRPC (TCP 445)					
Server protocols       Reformation (C2 152, 157, 157, 152, 211, 2880, 4680, 4690, 4090), 4090         Server protocols       Ref (C3 139), 300, 300, 300, 300, 300, 300, 300, 30							WS_Discovery (UDP 3702)					
Server protocols     NRD(TCP 399) NRD(TCP 399) SS (TCP 451) SS (TCP 577, SP27)       Lakels     Varu/Sert       Pundle (TCP 451) SS (TCP 577, SP27)       Lakels     Varu/Sert       Socratly Rink     SS (TCP 577, SP27)       Christing     SS (TCP 577, SP27)       Christing     SS (TCP 577, SP27)       Related allersts     SS (TCP 577, SP27)       Related allersts     SS (TCP 577, SP27)       Lake Serter     SS (TCP 577, SP27)							FailedConnection (TCP 1542, 1574, 1577, 1585, 2311, 28 49694)	860, 49690,				
Labels       Mar (der)         Labels       Mar (der)         Punde Ivel       3-Site spearations and control         Security Risk       Mar (der)         Operational Risk       Mar (der)         Chicality       Mar (der)         Risteral allors       22 (Drow)         First seen       0x 16, 2020 11.45542						Server protocols	NetBIOS (TCP 139)					
Labels       valu_uleri         Pardise level       3-Site sperations and control         Security Rink       W100         Operations Rights       W100         Criticality       W100         Rise et al.       22 (Brow)         Rester al.       59,3 2020 1647.56         Last seen       01 16,7 2021 11.4548							SMB (TCP 445)					
Labes ut/(s)=" Pardue level 3 - Ste spectrations and control Security Ripk ■10 : 6.0 Operations Ripk ■10 : 2.0 Criticality ■10 : 2.0 Criticality ■10 : 2.0 Criticality ■10 : 2.0 Criticality ■2.0 Criticality ■2.0 Critica						Labola -	SSL (1CP 5671, 5672)					
Factor Rev     S       Scruty Risk     S       Operational Risk     S       Nonon vulnerabilities     O       Related allers     S       S     S <td></td> <td></td> <td></td> <td></td> <td></td> <td>Purdue Issuel</td> <td>march12=1</td> <td></td> <td></td> <td></td> <td></td> <td></td>						Purdue Issuel	march12=1					
Crickally     €00       Known volkneskilssi     0       Raisted alors     92 (5%w)       First seen     6g 3, 2020 11/45/42						Security Risk	5 - Jose operations and control					
Criticality     ILIT       Krown volmerabilities     0       Related allerus     922 (19ww)       First seen     5-0 3, 2020 16:47:58       Lass seen     Ort 16, 2020 11:45:43						Operational Risk	1000 2.0					
Known vulnerabilities         0           Relates alerts         922 (19xm)           First seen         5xp 3, 2020 11:45758           Last seen         Ort 16, 2020 11:4548						Criticality	11000 L					
Related alerts         922 (39xx)           First seen         Sup 3, 2020 16:47:58           Last seen         Ort 16, 2020 11:45:43						Known vulnerabilities	0					
First seen         Sep 3, 2020 1647,58           Lass seen         Oct 16, 2020 11x5x83						Related alerts	922 (Show)					
Last seen 0α 16,2020 11.4543						First seen	Sep 3, 2020 16:47:58					
						Last seen	Oct 16, 2020 11:45:43					
here i here and a second se												
	Alassa / Alass dassite										AV 103 2008-2009	Connection for the second

etterini in te		-											
Filters: Edit	Reset	Alerts per event type (to	p 10)										
Time-based Filters	^											1m •	
✓ Today		38 alerts							Comm	unication patter    RPC/C	COM IID/opnum n	Application protoc	.01
Last 7 days		30 alerts											
Last 30 days													
In a given interval		20 alerts											1
On a given day		10 alerts	$\wedge$							~			-
Last X days			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					~				$\Delta $	
From date X to 30 days after		10:40	10:45 10:50	10:55		11:00	11:05	11:10	11:15 11:20	11:25	11:30	11:35	11
From date X to Y days before			~									$\wedge$	~
		10:40	10.45 10.50	10:55		11.00	11:05	11:10	11:15 11:20	11.25	11.30	11:35	11
Alert Filters	^												
Evolution event tune ID		0 items selected											
Rumanitered extuark		Timestamp *	Event name(s)	Sensor	Engine	Profile	Status	Severity	Source address	Destination address	Dest. Port	L7 Proto	Cas
Euclusian escala			Construction of the			1. 1999 P.	460000				0.000	Barran Solot	
Excluding profile			0	(Not set -	(Not 🖕	(Not set)	(Not set)	(Not set	10.100.1.4	0	0	(Not set)	(Una
Excluding det MAC		Oct 16, 2020 10:11:37	Communication pattern not	sensor-bu	Comm	9 - UDP com	Not analyzed	M	10.100.1.4 (pi-dmz)	10.100.0.25 (nessus	3389 (UDP)	NotAKnownOne	
Excluding out links		0-16 2020 10-11-26	Commission			0.100	Net contact		10 100 1 101 1000	10 100 0 35 (	2200 (1100)	NextKeen	
Excluding det 10		0ct 16, 2020 10:11:35	Communication pattern not	sensor-bu	Comm	9 - UDP com	Not analyzed		10.100.1.4 (pi-dmz)	10.100.0.25 (nessus	3389 (009)	NotAknownUne	
Excluding dat n		Oct 16, 2020 10:11:13	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M E	10.100.1.4 (pi-dmz)	10.100.0.25 (nessus	3389 (TCP)	RDP	
Bul 2 protocol		Oct 16, 2020 10:11:10	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M CT	10.100.1.4 (pi-dmz)	10.100.0.25 (nessus	3389 (TCP)	RDP	
By L2 protocol			700.000										
By L4 protocol		U OCT 10, 2020 10:09/41	TCF STN portscan	sensoriou	Portscan		Not analyzed	MILLO L	To, Tou, the (photnic)				
By unstream data		Oct 16, 2020 10:09:11	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M D	10.100.1.4 (pi-dmz)	10.100.0.181	22 (TCP)	SSH	
By downstream data		Oct 16, 2020 10:09:10	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz)	10.100.0.177 (opena	22 (TCP)	SSH	
By EFA nine			·		C	0.700	Margaretaria		10 100 1 111 1 111	10 100 0 45 1	22.07.000		
By field path		L 044 10, 2020 10:07:59	communication pattern not.	sensor-pu	comm	0 - 107 com	NUL analyzed		rocrow rat (pi-dmz)	to. too.o.oo (rugged	22(107)	3311	
Bylabels		Oct 16, 2020 10:07:52	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz)	10.100.0.50 (ir800.ir	22 (TCP)	SSH	
Excludion labels		Oct 16, 2020 10:07:44	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M E	10.100.1.4 (pi-dmz)	10.100.0.33 (betelgu	22 (TCP)	SSH	
By vlan		Det 16, 2020 10-07-13	Communication patters not	sensoriby	Comm	8 - TCP core	Not analyzed		10 100 1 4 (niders)	10 100 0 26 (second	22 (TCP)	5514	
Excluding vien		04 10, 2020 10:07:42	communication pattern not	sensor bu	comm	o - rer com	Hor analyzed	141	rocross ris (promz)	ro. roo.u.zo (securit	Le (ICP)	3311	
By detailed description		Oct 16, 2020 10:07:39	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M. 0.11	10.100.1.4 (pi-dmz)	10.100.0.20 (polaris)	22 (TCP)	SSH	
Excluding detailed description		Oct 16, 2020 10:07:38	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz)	10.100.0.16 (rigel.lo	22 (TCP)	SSH	
By alert case		0 0 16 2020 10:07:28	Communication pattern pot	concor bu	Comm	9 . TCP. com	Not an alvored		10 100 1 4 (ni.dmz)	10 100 0 15 (moores	22 (TCP)	55LJ	
		001 10, 2020 10:07:38	communication pattern not	sensor-od	Somman	er ter com	Not analyzed	and the set	is now the (promit)	10.100.0.13 (SeoTSe	ad (10P)	200	
Miscellaneous Filters	~	Oct 16, 2020 10:07:38	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M	10.100.1.4 (pi-dmz)	10.100.0.14 (rugged	22 (TCP)	SSH	
		Oct 16, 2020 10:07:37	Communication pattern not	sensor-bu	Comm	8 - TCP com	Not analyzed	M Care	10.100.1.4 (pi-dmz)	10.100.0.11 (orion.la	22 (TCP)	SSH	

## 1211 Figure D-17: Detection of Scanning Traffic and RDP Connection into Manufacturing Environment

1212 Figure D-18: Details of One of the Port Scan Alerts

	Back Edit	Delete Show   + Assig	n to case — Download   +			<b>9</b> +
mmary		~	Source host info	-	Aler: details	^
et ID	203180		IP address	(Priorite IP)	Faled connections	
estamp	Dec 16, 2020 10,09,41		Host name Other host carnes	las epars	- (scanner) * 22 ( 1 Galed consecutive(3) (5%) (3)	
ection engine	Portscen		Host MAC addresses	Microsof)	221 1 failed convector(s) (5% 11)	
ind name	ps_top_syn + TCP SVN pointso	ND		Last seen Oct 16, 2020 10:44:57 (Rodovell)	* 22 ( 1 failed connector(s) ( 5/% 1 ) )	
cription	victim's hosts and determine	ends multiple SYN packets to scan the a the open ports. This might be	addresses	(Baggeiden) (Cisco)	* 22 [ 1 fieled convector(b][59% 1])	
	exploit]	rtrst phase of) an attack (e.g., UeS,	Role	Terminal server	• 3389 ( 1 failed connection(s) [ 59% 1 ] ]	
erity	CE Low		Other roles OS version	Windows workstation, Terminal dians Windows 10 or Windows Server 2016	* 3389 ( 1 failed connection(s)[SYN:1])	
01050	Ethernet			AFP (TCP 445)	* 3389 ( 1 failed connection(s) [ 59% 1 ] )	
0000	P			DOM (TCP 135) DNS (UDP 53, 5353, 5355)	<ul> <li>Z2 [ 1 failed connector(s)[SYN:1]]</li> </ul>	
rolo	TCP N/A			54128,62531,62532,62541,62890) HTTp://7CB.80.445.6530	* 3389 ( 1 failed convection(s)[SVN: 1])	
un-	Not analyzed			Kerbergs (TCP 445) LDAP (TCP 445)	<ul> <li>221 [field connector(s)[5Wi1])</li> </ul>	
els.				MSSQL (TCP 445) NTP (UDP 123)	<ul> <li>3330 ( 1 failed convector(a) [ SYN: 1 ] ]</li> </ul>	
			Client protocols	NetBIOS (UDP 157) NoDece (TCP 139)	<ul> <li>JJ89 (11%)ed connection(a) [5YN:1])</li> <li>2000 (11%)ed connection(a) [5YN:1])</li> </ul>	
nitored networks				Nos4KnownOns (TCP 443) Nos4KnownOne (UDP 443, 1434, 1514, 3389, 32904, 43463, 43724,	3009(10)     10000000000000000000000000000000	
				43730, 43709, 44102, 44690) Oesef01(TCF 5450)	* 2289 ( 1 failed convector(s) SYN 11)	
z LAN	Address	NAN DA		SNB (TCP 445)	* 3389 ( 1 failed connection(s) [ 5% [ 1 ] )	
				55D7 (LDP 1900) 55L7 (LDP 1900)	* 22 [ 1 failed correscoure(s)[ 59% 1 ]]	
				SSL (TCP 448, 445) SumPC (TCP 445)	Successful connections:	
				WS_Discovery (UDP 3702)	(revenue)	
				reveauumtection (iiur 1542, 1574, 1577, 1585, 2311, 28880, 49690, 49694) Nextors CCP 1381	<ul> <li>80(1 successful connection(s))</li> <li>80(1 successful connection(s))</li> </ul>	
			Server protocols	RDP (TCP 3389) SMB (TCP 445)	OU[ Successive connection(S)]     So[ Successive connection(s)]	
				SSL (TCP 5671, 5672)	4431 52 successful contectionis1	
			Labels Purdue level	vier_jos#1 3 - Site operations and control	<ul> <li>3389 ( 1 wareworkal convection(n))</li> </ul>	
			Security Risk	1002 6.0	* 3389 ( 1 successful connection(s) )	
			Operational Risk		<ul> <li>22 ( 1 successful connection(s))</li> <li>3389 ( 1 successful connection(s))</li> </ul>	
			Known vulnerabilities	0	* 3389 ( 1 successful contection(s) )	
			Related alorts	923 (Show)	- source autocommution(s)	
			First seen	54p 3, 2020 10:47:58 Oct 16, 2020 11:47:47	<ul> <li>22[ 1 successful connection(d)]</li> </ul>	
					221 1 successful connection(s)	
			Destination host info	~	<ul> <li>22 ( 1 successful connection(s))</li> </ul>	
					* 3389 ( 1 successful connection(s))	
					<ul> <li>ZZ [ 1 successful connection(s)]</li> </ul>	
					* 3289 ( 1 successful connection(s) )	
					* 22( 1 successful connection(s))	
					221 1 successful convector(s)	
					* 22 ( 1 successful connection(s) )	
					<ul> <li>22 ( 1 successful convector(s))</li> </ul>	
					<ul> <li>Z2 ( 1 successful connection(s))</li> </ul>	
					* 22 ( 1 successful connection(s))	
					* 80 ( 5 successful connection(s))	
					<ul> <li>80 [ 1 successful convector(s))</li> </ul>	
					20 [ 1 successful connector(s) ]	
					<ul> <li>so( successi consector(s))</li> <li>so( i successi consector(s))</li> </ul>	
					BUT 1 successful convector(s)	
					* 443 ( 1 successful connection(s))	
					<ul> <li>445(-) successful connection(s))</li> </ul>	
					* 443 ( 1 successful connection(s) )	
					* 443 ( 26 successful connection(s))	
					<ul> <li>445 (1 successful consisting(s))</li> </ul>	
					448 ( 1 successful connection(s) )	
					* 443 ( 2 successful connection(st )	
					<ul> <li>80[ 1 successful convector(s))</li> </ul>	
					* 443 ( 40 successful connection(s) )	
					* 80 ( 3 successful connection(s))	
					<ul> <li>80 ( 1 successful convector(s))</li> </ul>	
					* 446 ( 1 successful connection(s))	
					* 80 ( 4 successful convector(s) )	
					<ul> <li>443 (1 successful connection(s))</li> </ul>	
					* 443 ( 3 successful connection(s))	
					* 443 ( 1 successful connection(s))	
					* 80[ 1 successful connector(s))	
					<ul> <li>au1, z successes convector(a))</li> </ul>	
					Constant of the second s	
					LEGEND : The failed connection are listed first, the successful connections are listed removed.	ach of the lists we
					presented in the following structure: - ( < Scarrent's   < comment's   comment's   commentPs   commen	and the second dist
					- <scannerip>  <scannedip> * <scannedpart> (   <b> &lt;*successful &gt;   &lt;*failed"&gt; connection(s)   <l>  )</l></b></scannedpart></scannedip></scannerip>	
					<a+ :="" connections="" number="" of="" port<="" successful="" td="" to=""><td></td></a+>	
					<b>: Mumber of failed connections to port xCP : In rows of failed connections, a break-down of 48p by fail reasons (1997). The rows of failed connections, a failed connection of the failed connection.</b>	
					NULL #: Failed due to Out Of State packet (NULL packet)	
					ACK # Failed due to Out Of State packet (ACK packet)	
					ACK #: Failed due to Out Of State packet (ACK packet) RN #: Failed due to Out Of State packet (RN packet) Masmon III Failed due to Out Of State packet (Marmon packet) Xerball due to Out Of State packet (Marmon packet)	
					ACK # Failed dut to Que Of Sate packet (ACK packet) RN 4F Failed dut to Que Of Sate packet (RN archer) Mainton H Failed dut to Que Of Sate packet (Mainton packet) Xinut = Failed dut to Que Of Sate packet (Xinut are packet) Use 0005F Failed dut to Que Of Sate packet (Kinut are packet) Use 0005F Failed dut to Que Of Sate packet (Kinut are packet) ON 4 Back (Article dut to Que Of Sate packet) (Kinut are packet) ON 4 Back (Article dut to Que Of Sate packet (Kinut are packet) ON 4 Back (Article dut to Que Of Sate packet) (Kinut are Que Of Sate Of Sate (Kinut are packet))	

1213 Figure D-19: Details of Alert for RDP Connection into Manufacturing Environment

<) FORESCOU	T. 🚳 Dashboard	A Network	Events	Sen	sors 😋 Settings				Ģ	P 🔊 🧶	admin
Alert details	Back Edit	Delete Trim	Show   ~	Assig	to case Download   •	ž.					Help
Summary			^		Source host info	^	Alert Details				^
Alert ID	203188				IP address	10.100.1.4 (Private IP)	ID and name		lan_cp_cnw_c - Communication p	attern not whiteliste	d
Timestamp Sensor name	Oct 16, 2020 10:11:10				Other host names	pi-dmz	Description		Communication pattern not whitelist are whitelisted in some communicati	ed: the source and dest on rule, but not with th	ination hosts s
Detection engine	Communication patterns (LAN C	CP)			User MAC addresses	00:15:5D:02:0D:03 (Microsof)	Telesseles est	defende	combination		
Profile	8 - TCP communications				Host MAC addresses	Last seen: Oct 16, 2020 11:47:52	action	croerault	alert		
Severity	Medium				Other observed MAC addresses	94:B8:C5:0E:E1:9F (Ruggedco)					
Source MAC	00:15:5D:02:0D:03 (Microsof)				Bole	/C:UE:CE:67:86:83 (Cisco)					
Source IP	10.100.1.4 (pi-dmz)				Other roles	Windows workstation, Terminal client					
Destination IP	• 10.100.0.25 (nessusym)				OS version	Windows 10 or Windows Server 2016					
Source port	3733					AFP (TCP 445)					
Destination port	3389					DNS (UDP 53,5353,5355) Exiled Concerning (CR 21, 21, 98, 110, 200, 9934, 49170, 49195					
L2 proto	Ethernet					54128, 6253 6, 62532, 62841, 62899)					
L4 proto	TCP					Kerberos (TCP 445)					
L7 proto	RDP					LDAP (TCP 445) MSSQL (TCP 445)					
TCP stream opened in hot	false					NTP (UDP 123) NetBIOS (UDP 137)					
Status	Not analyzed				Client protocols	NoData (TCP 139) NotAKnownOne (TCP 445)					
Labels						NotAKnownOne (UDP 443, 1434, 1514, 3389, 32904, 43463, 43724, 43789, 44102, 44690)					
User notes						OstooftPI (TCP 5450) RDP (TCP 3389)					
						5MB (TCP 445) 5MB (TCP 445)					
Monitored networks			^			SSDP (UDP 1900)					
Manage	Address	MAN ID.				SSH (TCP 22) SSL (TCP 443, 445)					
DMZ LAN	10 100 1 0/24	am.		-		SunRPC (TCP 445) WS_Discovery (UDP 3702)					
Lab LAN	10.100.0.0/24	any				FailedConnection (TCP 1542, 1574, 1577, 1585, 2311, 28860, 49690,					
					Server protocols	NetBIOS (TCP 139)					
						SMB (TCP 445)					
					Labels	SSE (TCP 56/1, 56/2) vian ids=1					
					Purdue level	3 - Site operations and control					
					Security Risk	6.0					
					Operational Risk	LED 2.0					
					Criticality						
					Related alerts	923 (Show)					
					First seen	Sep 3, 2020 16:47:58					
					Last seen	Oct 16, 2020 11:48:50					
					Destination host info	^					
					IP address	10.100.0.25 (Private IP)					
					Host name	nessusvm					
					Other host names	ruggedcom.mgmt.leb					
					Host MAC addresses	00:15:50:02:0A:06 (Microsof) Last seen: Oct 16, 2020 11:45:39					
					Other observed MAC	94:B8:C5:0E:E1:9F (Ruggedco)					
					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)					
						NotAKnownOne (TCP 4444) NotAKnownOne (IDP 4443)					
					Client protocols	RDP (TCP 3389)					
						SMB (UDP 138)					
						SSH (COP 1900) SSH (TCP 22)					
						55L (TCP 443) DCOM (TCP 135)					
						FailedConnection (TCP 21, 22, 53, 71, 80, 98, 110, 111, 389, 443, 5555, 5801, 5901, 6667, 7777, 7878, 8080, 9894, 46176, 46165)					
					Server protocols	NetBIOS (UDP 137) No Date (TCP 130)					
						NotAKnownOne (UDP 1434, 3389, 6838, 31037, 36734, 47455) RDD (ZC 3389)					
						SMB (TCP 445)					
					Purdue level	3 - Site operations and control					
					Security Risk	<b>1111111111111</b>					
					Operational Risk Criticality						
					Known vulnerabilities	0					
					Related alerts	1063 (Show)					
					First seen	Sep 3, 2020 16:57:16					
					Last seen	UCC 10, 2020 11:48:19					
Alexand 1 Alexandra alexandra											retrout in \$1.71

1214 Figure D-20: Dialog Message Showing 1.exe was Blocked from Executing



- 1215 D.2.3 Build 3
- 1216 D.2.3.1 Configuration
- 1217 Application Allowlisting: Windows SRP
- 1218 Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and Supervisory LAN
- 1219 Behavior Anomaly Detection: Dragos
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.

## 1222 *D.2.3.2 Test Results*

- 1223 Windows SRP blocks the attempted execution of 1.exe (Figure D-21). Figure D-22 shows the alerts
- 1224 generated by Dragos when it detected the remote connection to the target. Figure D-23 depicts the
- 1225 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.

1227 Figure D-21: Windows SRP blocked 1.exe From Executing



## 1228 Figure D-22: Log of Alerts Detected by Dragos

∓ FIL	TERING	• 🖻 🕅	om /17/21,07:	35 PM UTC 🛅 To 02/17	7/21, 07:50 PM UTC C RELOA	D					Q. Search		
	View	Sever ÷	ID	Occurred At	Detection Quadrants	Summary	Message	Detected By =	Asset IDs	Source IPv4	Contract Dest. IPv	\$ Other IPv4	•
	VIEW		148546	02/17/21, 07:39:49	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 85 (IP: ) connected to Asset:	Network Device Access	85,96				
	VIEW	1	148545	02/17/21, 07:37:59	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 85 (IP: ) connected to Asset:	Network Device Access	85,96				
	VIEW	۰	148544	02/17/21, 07:38:14	Threat Behavior	Administrative Access to a Network Device D	Asset: 1807 (IP: i) connected to _	Network Device Access	1807, 94				
	VIEW	1	148543	02/17/21, 07:42:57	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 85 (IP: ) connected to Asset:	Network Device Access	85,96				
	VIEW		148542	02/17/21, 07:42:40	Threat Behavior	Administrative Access to a Network Device D	Asset: 1807 (IP: ) connected to _	Network Device Access	1807, 94				
	VIEW	1	148541	02/17/21, 07:43:46	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 1807 (IP: connected to	Network Device Access	1807, 94				
	VIEW		148540	02/17/21, 07:44:53	Threat Behavior	Administrative Access to a Network Device D	Asset: 1807 (IP: i) connected to _	Network Device Access	1807, 94				
	VIEW	1	148539	02/17/21, 07:40:27	Threat Behavior	Administrative Access to a Network Device D	Asset: 1807 (IP: ) connected to	Network Device Access	1807, 94				
	VIEW		148538	02/17/21, 07:46:11	Indicator	Default Community Signature Fired	Activity that meets the criteria of a default co	Snort Community Rules	85, 844				
	VIEW	0	148537	02/17/21, 07:46:11	Indicator	Default Community Signature Fired	Activity that meets the criteria of a default co	Snort Community Rules	85, 844				
	VIEW		148536	02/17/21, 07:46:11	Threat Behavior	RDP Negotiation Request	RDP Negotiation Request	RDP Port Mismatch	85, 844				
	VIEW	1	148531	02/17/21, 07:36:02	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 1807 (IP: ) connected to _	Network Device Access	1807, 94				
	VIEW		148530	02/17/21,07:38:15	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 1807 (IP: connected to	Network Device Access	1807, 94				
	VIEW	1	148529	02/17/21, 07:37:08	Threat Behavior	Administrative Access to a Network Device D.,	Asset: 1807 (IP: ) connected to _	Network Device Access	1807, 94				

1229 Figure D-23: Detail of RDP Session Activity Between an External System and a DMZ System

	DETECTION INFORMATION		ASSOCIATED ASSETS	
₹ FILTER	WHAT HAPPENED: RDP Negotiation Request		View         C         Type         ID         Name         C           Vew         Import Sime         5         Asset IS         C <td< th=""><th>Dir. 0</th></td<>	Dir. 0
	OCCURRED AT: 2017/12/13 Mar UTC COUNT: 1 Mar Development Mar Development Mar Development ACTIVITY GROUP: ACTIVITY ACTIVITY GROUP: ACTIVITY ACTIVITY GROUP: ACTIVITY ACTIVITY	LAST SEEN: UNITERIOR UNITE HARTERIORUS HA	Verw     Image: Asset     B46       COMMUNICATIONS SUMMARY       Vindous Sever Uncount of the sever protein       Vindous Sever Uncount of the sever protein       Potocol :     Client :     Epheneral Ports :       Sig.     -     2.1 MB     15 5 MB	9rc ) 2
	RELATED NOTIFICATIONS		Summay Ho Related Notifications	¢

1230 Figure D-24: Detail for Network Scanning Alert

WAT LARSPERDID: despectational CARP Service Market Support State Componential Contract Componential Co	Group by: DETECTION INFORMATION		ASSOCIATED ASSETS		
CCURREP AT: LAT SEP:   DUTIAL UCAS IMMENT TADATURE STATUS   COURT TADATURE STATUS   COURT TATUE   DETECTION 00/AD: SOURCE:   Test Beauser Detection 00/AD:   Test Test Beauser Detection 00/AD:   Test Test Test For ICS Test Test Detection 00/AD:   Test Test Test Test Test Test Test Test	WHAT HAPPENED: Sequential ICMP Sweep Detected		View C Type ID C VIEW Serv 85 Asset 85	Name	Dir. 10.100.1.4 oth
Construction   Construction <th>( OCCURRED AT: 02/17/21, 02:50 PM EST R0 COUNT: 1</th> <th>LAST SEEN: 12/31/49, 07:00 PM EST: STATE: UMEREDUATD</th> <th>COMMUNICATIONS SUMMARY</th> <th></th> <th></th>	( OCCURRED AT: 02/17/21, 02:50 PM EST R0 COUNT: 1	LAST SEEN: 12/31/49, 07:00 PM EST: STATE: UMEREDUATD	COMMUNICATIONS SUMMARY		
A CTIVITY GROUP:       LCS CYEER KILLCHAIN STEP:         LLCTRAM       Suge 1 - Seconsultances         MITEE ATTACK FOR ICS TACTIC       MITEE ATTACK FOR ICS TCHONOLE         Diccovery 61       TOB64-Instances         PLATBOCKS:       NOTFICATION ESCORD:         CASES:       NOTFICATION COMPONENTS:         YC Course Linear       NOTFICATION COMPONENTS:         YC Course Linear       NOTFICATION COMPONENTS:         YC Course Linear       NOTFICATION SCORD COMPONENTS:         YC Course Linear       NOTFICATION SCORD COMPONENTS:         YC Course Linear       NOTFICATION SCORD COMPONENTS:         YC Course Linear       Summary	DETECTED BY: Scan Sequential DETECTION QUAD: Threat Behavior	SOURCE: Network Traffic ZONES: UNL2	No Comm	inications Summary.	
Image: Strattick For IcS TACTIC     Imite ATTACK For IcS TACHIC       Discovery S     TOBAS Remote System Discovery S       QUERY-FOCUSED DATASETS:     NOTFIGUATION BECORD: No Associated Remote       Scientific     No Associated Remote       CASES:     No Associated Remote       Concent Linket     No Associated DemoteNetTS: No Canadidated Components       RELATED NOTFIGATIONS     Summary       D ° Cocorred At °     Summary	ACTIVITY GROUP: ELECTRUM	ICS CYBER KILLCHAIN STEP: Stage 1 - Reconnaissance			
WIEW     OUERY-FOCUSED DATASETS:     NOTIFICATION RECORD: Not Associated Record       Not Associated Components:     Not Associated Components:       Not Costs:     Not Associated Components:       Not Costs:     Not Associated Components:       Not Costs:     Not Costs:       Not Costs:     Not Associated Components:       Not Costs:     Not Costs:       Not Costs:     Not Associated Components:       Not Costs:     Not Costs:       Not Costs:     Not Associated Components:       Not Costs:     Not Costs:       Not Costs:     Not Associated Components:	MITRE ATT&CK FOR ICS TACTIC Discovery	MITRE ATT&CK FOR ICS TECHNIQUE T0846: Remote System Discovery @			
PLAYBOKE     NOTIFICATION COMPONENTS: No Associated Components       PLAYBOKE     Notification components       PLAYBOKE     Notification components       PLAYBOKE     RELATED NOTIFICATIONS       ID ° Cocarred At °     Summiry	QUERY-FOCUSED DATASETS: Scanning	NOTIFICATION RECORD: No Associated Record			
By View RELATED NOTIFICATIONS ID © Occurred At © Summary	PLAYBOOKS: Network Address Scanning Activity Detected CASES:	NOTIFICATION COMPONENTS: No Associated Components			
By risk?         RELATED NOTIFICATIONS           10 °         Occurred At         °           Summary         Summary	No Cases Linked				
ID Courred At Courred	RELATED NOTIFICATIONS				
	ID 🌣 Occurred At 🗢		Summary		

1231 Figure D-25: Detail of RDP Session Activity Between a DMZ System and a Testbed LAN System

DETECTION INFORMATION		ASSOCI	ATED ASSETS					
WHAT HAPPENED:		View	С Туре	÷ ID ÷		Name	P	÷ 1
FILTER NOP REQUIRING REQUESS		VIE	Windows	s Serv 85 Asset 85				10.100.1.4
OCCURRED AT: 02/17/21, 19:51 UTC	LAST SEEN: 01/01/70,00:00 UTC	VIE	Vulnerab	olity S 37 Asset 37				10.100.0.25
	STATE: UNRESOLVED	COMMU	NICATIONS SUP	MMARY				
DETECTED BY:	SOURCE:							
BOP Port Mismatch	ZONES:							
Threat Behavior	DMZ, Cybersecurity LAN			8	ICMI	p	8	
ACTIVITY GROUP:	ICS CYBER KILLCHAIN STEP:	Θ		Windows	UDF Server	General U	se Desktop	
1 6				pi-d 10.10	mz 0.1.4	ness ness	usvm usvm	
MITRE ATT&CK FOR ICS TACTIC Command And Control @	MITRE ATT&CK FOR ICS TECHNIQUE T0885: Commonly Used Port @	Protocol	Client	* Enhameral Porte	- Carver	192.10 10.10	55.0.11 n.n.25	* DY Duter
QUERY-FOCUSED DATASETS:	NOTIFICATION RECORD:	ICMP	10.100.1.4		10.100.0.25		222.0 bytes	148.0 bytes
No Applicable Query-Focused Datasets	No Associated Record	ICMP	10.100.0.25		10.100.1.4		148.0 bytes	222.0 bytes
No Associated Playbooks	View in Kibana	SSL	10.100.1.4	53365, 53367	10.100.0.25	3389	1.2 MB	2.0 MB
CASES: No Cases Linked		UDP	10.100.1.4	56180, 56181	10.100.0.25	3389	14.9 KB	0 bytes
RELATED NOTIFICATIONS								
ID C Occurred At C			Summary					
		No Related Notifications						

1232	D.2.4	<b>Build 4</b>
------	-------	----------------

1235

1236

- 1233 D.2.4.1 Configuration
- 1234 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.
- 1237 Behavior Anomaly Detection: Azure Defender for IoT
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.

## 1240 *D.2.4.2 Test Results*

- 1241 Azure Defender for IoT is able to detect the remote access connection to the DMZ as seen in Figure D-
- 1242 <u>26. Figure D-27</u> shows detection of scanning activity, while <u>Figure D-28</u> shows details of the scan. The
- 1243 RDP connection into the manufacturing environment is seen in <u>Figure D-29</u>. Carbon Black blocks 1.exe
- 1244 from executing as shown in Figure D-30.
- 1245 Figure D-26: Azure Defender for IoT "info" Event Identified the Remote Access Connection to the DMZ





#### 1246 Figure D-27: Alert for Scanning Activity

1247 Figure D-28: Details for the Scanning Alert

ID: 183	Ê	0	<u>+</u>	×	Ŧ	∢
Address Scan Detected Anomaly   Jan 5, 2021 1:53:44 PM ( 12 minutes ago ) Address scan detected. Scanning address: 10.100.1.4 Scanned subnet: 10.100.0.0/16 Scanned addresses: 10.100.0.10, 10.100.0.11, 10.100.0.12, 10.100.0.13, 10.100.0.14, 10.100.0 10.100.0.17, 10.100.0.18, 10.100.0.19 It is recommended to notify the security officer of the incident.	.15, 10	0.100.	0.16,			
₽I-DMZ						
Manage this Event						
<ul> <li>Multiple scans in the network can be an indication for a new device in the network, a resisting device, improper configuration of an application (for example: due to a firmwork), or malicious activity in the network, such as reconnaissance.</li> </ul>	iew fu are up	inctio date,	nality or a i	of ar new	n	
<ul> <li>During the reconnaissance phase, a tool usually collects system configuration data, ir installed antivirus applications and steals data on the computer systems themselves, back to the attackers.</li> </ul>	cludii whicł	ng dat n is th	a abo en se	out ar ent	ıy	
	Lea	arn	A	cknow	vledg	e

1248 Figure D-29: Detection of RDP Connection into the Manufacturing Environment



1249 Figure D-30: Carbon Black Shows an Alert for Blocking File 1.exe

S	ecurity Notification - U	Unapproved File								
Cb Target: 1. Path: c: Process: ex	.exe \\users\nccoeuser\desktop xplorer.exe	p\								
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 Reque	<u>est&gt;&gt;</u>	ОК								
Process	Target	Path	_							
🛕 1 explorer.exe	1.exe	c:\users\nccoeuser\desktop\								
		· · · · · · · · · · · · · · · · · · ·	<u>'</u>							
Approval Request										
Enter your reason for a max).	access (512 characters A	Your Email: Priority: Medium           Submit								
Protection by Carbon Bla	ck, Inc.									

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

- 1252 An authorized user with an authorized remote workstation, infected with a worm-type malware,
- 1253 connects via remote access capabilities to the manufacturing environments. The malware on the remote
- 1254 host attempts to scan the manufacturing environment to identify vulnerable hosts. The expected result
- is that the remote access tools effectively stop the worm-type malicious code from propagating to the
- 1256 manufacturing environment from the infected remote workstation.
- 1257 D.3.1 Build 1

1260

- 1258 D.3.1.1 Configuration
- 1259 Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- 1261 User Authentication/User Authorization: ConsoleWorks

1262

## Configured for access PCS environment.

## 1263 *D.3.1.2 Test Results*

- 1264 Figure D-31 shows the remote connection being established through the Cisco AnyConnect VPN
- 1265 application through which a browser is used to access the ConsoleWorks web interface (Figure D-32).
- 1266 Once a connection to ConsoleWorks was established, the simulated worm attack was executed on the
- 1267 remote PC to scan the target network. The scan was successfully blocked by the VPN configuration.
- 1268 Figure D-31: Secured VPN Connection to Environment with Cisco AnyConnect



← → C A Not secure   10,100,0,53:	51/6/index.html	H O
Console <mark>Works</mark> ® v53-1u3	Devices	NCCOE_USER NCCOE_POS
	Devices C In Filter Devices C S	
	PCS HISTORIAN Nutrie of convectors. 1	
	PCS 146	
	0 2021/02/04 10:33 LITC 08:00	Invocation: NCC

1269 Figure D-32: Remote Access is Being Established Through ConsoleWorks

- 1270 D.3.2 Build 2
- 1271 D.3.2.1 Configuration
- 1272 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.

## 1275 *D.3.2.2 Test Results*

- 1276 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 Figure D-34. Once a connection to the NCCOE environment was established, the simulated
- 1278 worm attack was executed on the remote PC to scan the target network. The scan was successfully
- 1279 blocked by the Dispel VDI configuration.

1280 Figure D-33: Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket ESI

10	lemote Desktop Connection							- 0 ×
Recycle Bin NC	AddRa. Reply from 15 Reply from 15 Reply from 15 Reply from 15	0.500.1.7: bytes=32 time=184ms 0.500.1.7: bytes=32 time=181ms 0.500.1.7: bytes=32 time=181ms 0.500.1.7: bytes=32 time=184ms	TTL-62 TTL-62 TTL-62 TTL-62		- 0	×		
Dapel	Ping statist Packets:	lcs for 10.100.1.7: Sent + 0, Received + 0, Lost	+ 0 (0% loss),		- D X			
Geogle Cheme	Semingu Helo	Dispel is running	Disconnect					
CipertyFin	Available Projects	Available Entry Points		Available Exit Points			-	
	NCCUE Manufacturing	Chicago, E. (		Exit NCCOE (outline)				
SCIE-RAL-								
GreenTec								
GreenTec, D.,								
TCI, famo.								
4								· · · · ·

- 40 Remote Desktop Connection ote Desktop Conr -55 Ð 3 đ Google Chrome OpenVPN GUI putty 31-FULL-T Ł Æ 1 20/ reenTec. 恳 1
- 1281 Figure D-34: Nested RDP Session Showing Dispel Connection into the PCS Workstation

## 1282 D.3.3 Build 3

- 1283 D.3.3.1 Configuration
- 1284 Remote Access: Cisco VPN
- Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- 1286 User Authentication/User Authorization: ConsoleWorks
- Configured for access CRS environment.

## 1288 *D.3.3.2 Test Results*

- 1289 Figure D-35 shows the remote connection being established through the Cisco AnyConnect VPN
- 1290 application, where a browser is used to access the ConsoleWorks web interface (Figure D-36). Once a
- 1291 connection to ConsoleWorks was established, the simulated worm attack was executed on the remote
- 1292 PC to scan the target network. The scan was successfully blocked by the VPN configuration.

1293 Figure D-35: VPN Connection to Manufacturing Environment



Console Works® v 5.3-1u6	Devices	NCCOE_USER NCCOE_CRS
	Devices O 🏠 Filter Devices	
	6 Devices Extrement Matteries Educate 64 trement of universetters ?	
	CRS_WORKSTATION Description: CIP Expressing Witakaliton Number of intercentions 1	
	<b>▼</b>	
TDi Technologiae, Inc.	0 2021/05/06 05:22 LITC 07:00	Investion: NC/

1294 Figure D-36: Remote Access is Being Established Through ConsoleWorks

- 1295 D.3.4 Build 4
- 1296 D.3.4.1 Configuration
- 1297 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.

## 1300 *D.3.4.2 Test Results*

- 1301 Figure D-37 shows the Dispel VDI desktop, which allows a connection to the CRS workstation in
- 1302 <u>Figure D-38</u>. Once a connection to the NCCOE environment was established, the simulated worm attack
- 1303 was executed on the remote PC to scan the target network. The scan was successfully blocked by the
- use of the Dispel VDI.

1305 Figure D-37: Dispel VDI Showing Interface for Connecting Through Dispel Enclave to Dispel Wicket



1306 Figure D-38: Nested RDP Session Showing Dispel Connection into the CRS Workstation



# 1307 D.4 Executing Scenario 4: Protect Host from Unauthorized Application 1308 Installation

- 1309 An authorized user copies downloaded software installation files and executable files from a shared
- 1310 network drive to a workstation. The user attempts to execute or install the unauthorized software on
- 1311 the workstation. The expected result is that the application allowlisting tool prevents execution or
- 1312 installation of the software. Also, the behavioral anomaly detection identifies file transfer activity in the
- 1313 manufacturing environment.
- 1314 D.4.1 Build 1
- 1315 D.4.1.1 Configuration
- 1316 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.
- 1319 Behavior Anomaly Detection: Tenable.ot
- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## 1321 *D.4.1.2 Test Results*

- 1322 As shown in Figure D-39, Carbon black is able to block and alert on the execution of putty.exe.
- 1323 Tenable.ot is able to detect the server message block (SMB) connection between an HMI in the Testbed
- 1324 LAN and the GreenTec server (Figure D-40). Details of that alert are shown in Figure D-41.

1325 Figure D-39: Carbon Black Blocks the Execution of putty.exe and Other Files

Secur	ity No	otification - Unappr	oved File	
	С	Def Target: pu Path: c: Process: ex	tty.exe \users\nccoeuser\desktop\ :plorer.exe	
	Cb Pr becai to sto	rotection identified use the file is not op it from running	d and paused an attempt by explor approved. Choose Allow to let this at this time. Scroll down for diagn	er.exe to run putty.exe file run, or choose Block ostic data.
5	ubmi	it Justification>>		Allow Block
		Process	Target	Path 🔺
?	6	explorer.exe	nmap-7.80-setup.exe	c:\users\nccoeuser\desktop
?	7	explorer.exe	putty.exe	c:\users\nccoeuser\desktop
?	8	explorer.exe	putty.exe	c:\users\nccoeuser\desktop
?	9	explorer.exe	putty-64bit-0.74-installer.msi	c:\users\nccoeuser\desktop 👻
•				•
- 10	stific	ation		
	inter nax).	your reason for a	ccess (512 characters 🔺 Your Er Priority	mail: * Medium Submit
Pro	tectio	on by Carbon Blac	k, Inc.	

1326 Figure D-40: Tenable.ot alert Showing the SMB Connection Between the HMI and the GreenTec Server

_								02	10 PM - Wadaasday Ar	×14 2021 NCCO	Elleor
=	Powered by indegy							02:	TO PM • Wednesday, Ap	97 14, 2021 - NCCO	ie user 🗸
× •	Events All Events	All Events 10.100.1.7	0	٩					Actions 🗸 Re	solve All Export	0
	Configuration Events	LOG ID TIME	4	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE A	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD	p≪
	Network Threats	19333 02:1	0:04 PM · Apr 14, 2021	Unauthorized Conversation	Low	SMB communication from Eng S	tation HMI	172.16.1.4	GreenTec	10.100.1.7	ettings
ò	Network Events Policies	Items: 1-1 out of 1								< < Page1of1 >	► N
~ <u>a</u>	Inventory	Event 19333 02:10:04 PI	M · Apr 14, 2021 Unau	thorized Conversation Low	Not resolve	ed					
	Controllers Network Assets	Details	A conversation in an	unauthorized protocol has be	en detected						
> <u>≜</u>	Risk	Destination	SOURCE NAME	HMI			Why is this import	ant?	Suggested Mitigation		
> @	Groups	Policy	SOURCE ADDRESS	172.16.1.4			Conversations in u	nauthorized protocols	Check if this communi	cation is expected. If	
	Reports	Status	DESTINATION NAME	GreenTec			are not expected to	cious traffic. Some assets o communicate in non-	conditions so that Eve	nts aren't generated	
> 0°	Local Settings		DESTINATION ADDRESS	10.100.1.7			the standard protocols potential threat. In	and any deviation from cols may suggest a addition, some	this communication is the source asset to de	tions in the future. If not expected, check termine whether the	
			PROTOCOL	SMB (tcp/445)			protocols are unse used at all, in order and assets secure	cure and should not be r to keep the network	source asset itself has If this communication	been compromised. Is not expected, traffic to various	
			PORT	445			and assets secure.		assets across the netw	ork.	
			PROTOCOL GROUP	In SMB							

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

=	Devered by Indegy				02:10 PM • Wednesday, Apr 14, 2021 NCCOE User 🗸
~ .	Events All Events Configuration Events SCADA Events Network Threats	SMB com Unauthorized C Category Network Events	Imunication from Enj Conversation	g Station Detected	STATUS Actions V
	Network Events	Details	Policy Definition		
۽ چ ~	Policies	Exclusions	NAME	SMB communication from Eng Station Detected	
	Controllers		SOURCE DESTINATION / AFFECTED ASSET	(In ENG. Stations) or (In HMIs) In Any Asset	
> 🛓	Network Assets Risk		PROTOCOL GROUP	In SMB	
> #	Network		Policy Actions		
	Reports		SEVERITY	Low	
> o°	Local Settings		EMAIL		
			DISABLE AFTER HIT		
			CATEGORY	Network Events	
			DISABLED	Enabled	

## 1329 D.4.2 Build 2

1335

## 1330 D.4.2.1 Configuration

1331	 Application Allowlisting: Windows SRP
1332 1333	<ul> <li>Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2.</li> </ul>
1334	 Behavior Anomaly Detection: eyeInspect

- benavior anomaly beteenon eyemspeer
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

## 1336 *D.4.2.2 Test Results*

- 1337 With Windows SRP enabled, putty.exe is not allowed to execute because it is not a permitted
- application under group policy, as shown in Figure D-42. Windows SRP also blocks the user's attempt to
- 1339 run putty-64bit-0.74-installer.msi. (Figure D-43). Forescout detected the file transfer activity (Figure D-
- 1340 <u>44</u>). Figure D-45 shows a detailed description of the alert that was generate for the file transfer activity.
- 1341 Figure D-42: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration

17	
putty-64bit	C:\Users\nccoeUser\Desktop\putty.exe
	This program is blocked by group policy. For more information, contact your system administrator.
nmap-7.80	ОК
putty	

1342 Figure D-43: putty-64bit-0.74-installer.msi is blocked by Windows SRP



1343 Figure D-44: Forescout Alert on the File Transfer Activity

<) FORESCOUT	🙆 Dasi	nboard 👍 Netwo	ork 🔳 Events 🔊 Sen	sors <b>OS</b> Settin							🖵 🏓 🏓	= edmin
Alerts	Reload	Export   ~ A	ggregate details Create n									
From date X to 30 days after From date X to Y days before												
Alert Filters		0 items selected										
By monitored network		Timestamp +	Event name(s)	Sensor En	gine Profile	Status	Severity	Source address	Destination address	Dest. Port	L7 Proto	Case ID
Excluding profile     Excluding src MAC			0	(Nation	Not set)	(Not set)	Old IC.	172.16.1.4 O	10.100.1.7	0	(Not set)	(Unessigna
Excluding dat MAC		Oct 7, 2020 09:12:38	Communication pattern	sensorib Co	m 8 - TCP co	Not analyzed	M State	172.16.1.4 (fgs-61	10.100.1.7 (greent	445 (TCP)	SMB	
Excluding sec IP     Excluding dat IP	1 10	1 items of 1										
Excluding dst port     By L2 protocol												
By L3 protocol												

1344 Figure D-45: Forescout Alert Details for the File Transfer Activity

FORESCOL	JT. 🚳 Dashboard 🚣 Network 🔳 Eventi	a 🔊 Sensora 😋 Settin	5 <sup>4</sup>			· · · · · · · · · · · · · · · · · · ·
rt details	Back Edit Delete Trim Show J	<ul> <li>Assign to case</li> <li>Down</li> </ul>	ioad   ×			0
Summary	^	Source host info		^	Alert Details	
Vert ID	139391	IP address	172.10.1.4 (Private IP)		ID and name	lan_cp_cnw_c - Communication pattern not whitelisted
Imestemp	Oct 7, 2020 09:12:38	Host name	fgs-61330Hh			Communication pattern not withelisted: the source and destinate
ensor name	sensor-bundle-riccie	Other host names	fgs-61338Hh.Jan.Jab		Description	hosts are whitelated in some communication rule, but not with the
letection engine	Communication patterns (LAN CP)	Host MAC addresses	0C:C4:7A:31:44:47 (SuperMic)		Triggering rule/default	
rufile	E - TCP communications		Laut were Oct 7, 2020 09:22:14		action	alert
Severity	Medium	120000000000000000000000000000000000000	EA:90:69:38:C2:C3 (Rockwell) EA:90:69:38:C2:C2 (Rockwell)			
Source MAC	0CiC4/7A(31)44(47 (SuperMic)	Other observed MAL addresses	54:90:69:38:C2:C0 (Rockwell)			
Destination MAC	E4:90:69:38:C2:C1 (Reclevel)		7C-0E-CE-67-86-88 (Cires) 7C-0E-CE-67-86-83 (Cires)			
Source IP	• 172.16.1.4 (fgs-61338hb)	Role	Terminal server			
Destination IP	9 10.100.1.7 (greentet-server)	Other roles	Windows workstation			
Source part	49783	Vendor and model	Rockwell			
Destination port	445	O5 version	Windows 7 or Windows Server 2008 R2			
L2 proto	Ethernet		DCOM (TCP 135, 49155, 49159)			
L3 prote	9		DNS (TCP 53) DNS (LCP 53, 5355)			
L4 proto	TCP		FailedConnection (TCP 80, 139)			
L7 proto	SMB		HTTP (TCP 8530) Kerberos (TCP 88)			
TCP stream opened in hot start mode	faise		LDAP (TCP 389) LDAP (UDP 389)			
Status	Not analyzed	Clerit sectorsh	NTP (UDP 123) NetBIOS (LOP 137)			
Labels		course protocolory	NoDaca (TCP 50005)			
User notes			NotKnownOne (TCP 1332, 2500, 2301, 10005) NotKnownOne (UDP 1514) SMB (TCP 445) SMB 4100 1320			
Monitored networks	*		SSDP (UOP 1900) SSH (TCP 22) SSL (TCP 443, 10005) Svalar (UCP 558)			
THE THE REAL PROPERTY OF	ASSESS YON US					

## 1345 D.4.3 Build 3

- 1346 D.4.3.1 Configuration
- 1347 Application Allowlisting : Windows SRP
- Settings are applied to systems in the DMZ, Testbed LAN, and Supervisory LAN
- 1349 Behavior Anomaly Detection: Dragos
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.

## 1352 *D.4.3.2 Test Results*

- 1353 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 (Figure D-47). Dragos detected the file transfer activity (Figure D-48).
- 1356 Figure D-49 shows a detailed description of the alert that was generated for the file transfer activity.
1357 Figure D-46: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration



1358 Figure D-47: putty-64bit-0.74-installer.msi is Blocked by Windows SRP



# 1359 Figure D-48: Dragos Alert on the File Transfer Activity

				ASSET NOTIFICATIO	ONS			SYSTEM ALERTS			RULES		
T P	LTERING	• 🖬 🕅	sm /17/21, 19:00	р UTC 🗖 🗖 10 02/1	7/21, 21:00 UTC	С иннини	_					Q Sweek 10.100.1.7	×
	View	Sever :	ID :	Occurred At	,	()the	: Summary	Message	Detected By	Asset IDs	Source IPv4	Dest. IPv4 :	Other IPv
	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	
	VIEW	0	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 she256 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 she256 hash of cbc	File Transfer of Suspicious PE	151, 35	10.100.1.7	192.160.0.20	
	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 cbc	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 43d.	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_raw_size	Asset 96 downloaded a file with she256 hash of 3b4	File Transfer of Suspicious PE	80,96	10.100.1.7	192.168.0.2	
	VIEW		148568	02/17/21, 19:49 UTC	Communication		A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with she256 hash of 43d	File Transfer of Suspicious PE	151,96	10.100.1.7	192.160.0.2	
	VIEW		148567	02/17/21, 19:43 UTC	Communication		A Downloaded file hit on: suspicious_raw_size	Asset 16 downloaded a file with sha256 hash of 3b4	File Transfer of Suspicious PE	151,96	10.100.1.7	192.168.0.2	
	VIEW		148500	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 96 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_sections	Asset 35 downloaded a file with she256 heah 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	192.168.0.2	
	VIEW	1	148502	02/17/21, 19:48 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_sections	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, 19:43 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	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_sections	Asset 35 downloaded a file with she256 hash of aa6	File Transfer of Suspicious PE	151,35	10.100.1.7	192.168.0.20	
	AIPM		148558	02/17/21, 19:48 UTC	Communication		A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d.	File Transfer of Suspicious PE	157, 96	10.100.1.7	192.168.0.2	
	VIEW		148557	02/17/21, 19:43 UTC	Commutication		A Downloaded file hit on: suspicious_pe_sections	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, sections	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	

1360 Figure D-49: Dragos Alert Details of the File Transfer Alert

DETE	CTION INFORMATION		ASSOCIA	FED ASSETS					
WHAT	HAPPENED:	Debr74056-51714482500hols180511n00r41na from 50 union matched the currentsure musicing the	View	с Туре	≎ ID ≎		Name		C Die
W FILTER	e colori e conserva e nel man e cezara nella con su conservativa e conservativa e nella. Il color	NAME PROVIDE A FEMALE PROVIDENCE PROVIDE P	VIEW	General I	lise D 80 Asset 8	0			10.100.1.7 st
OCCUR	RED AT:	LAST SEEN:	VIEW	Router	96 Asset 9	6			192.168.0.2 di
COUNT	1	STATE:	COMMUN	ICATIONS SU	MMARY				
	TED DV-	UNRESOLVED	(2)						
E Fie Tran	offer of Suspicious PE	0102u555 oue0-4ubc-0826 de69e231916e							
DETEC' Threat B	TION QUAD:	ZONES: DMZ, Cybernecurity LAN	•						
ACTIV	TY GROUP:	ICS CYBER KILLCHAIN STEP:				General Un Super Micro Comp 10.10	<ul> <li>Desktop</li> <li>der, Ino : SuperMio</li> <li>0, 1, 7</li> </ul>		
None None		Stage 1 - Delivery				preste preste-s	Haarver Haarver erverlocel Innal		
MITRE	ATT&CK FOR ICS TACTIC	MITRE ATTACK FOR ICS TECHNIQUE T0867: Remote File Copy @	Protocol :	Client	Ephemeral Ports	C Server	Server Ports	TX Bytes	: RX Bytes
	EDCISED DATASETS-	NOTIFICATION RECORD-	SMB	10.100.0.20		10.100.1.7		42.9 KB	43.0 KB
No Aupt	cuble Query Focused Datasets	View in Kibana	NTLM	10.100.0.20		10.100.1.7		120.1 KB	121.7 KB
PLAYB	DOKS: Iolated Playbooks	NOTIFICATION COMPONENTS: View In Kübasa	DCE_RPC	10.100.0.20		10.100.1.7		2.1 MD	65.5 MB
	s Lokert								
	TED NOTIFICATIONS								
	ID 0 Occurred At 0			Summary					
2 0		No Relate	d Notifications						

# 1361 D.4.4 Build 4

- 1362 D.4.4.1 Configuration
- 1363 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.
- 1366 Behavior Anomaly Detection: Azure Defender for IoT
- Configured to receive packet streams from DMZ, Testbed LAN and Supervisory LAN, and
   Control LAN.

#### 1369 *D.4.4.2 Test Results*

- 1370 Carbon Black was able to block the execution of putty.exe (Figure D-50) and the installation of putty-
- 1371 64bit-0.74-installer.msi (Figure D-51). Figure D-52 is the alert dashboard for Azure Defender for IoT that
- 1372 shows new activity has been detected. The detailed alert in <u>Figure D-53</u> provides details of an RPC
- 1373 connection between the GreenTec server and the Testbed LAN. A timeline of events showing a file
- 1374 transfer has occurred is shown in Figure D-54.

1375 Figure D-50: Carbon Black Alert Showing that putty.exe is Blocked from Executing

Security Notification - Unapproved Network Location	
Cb Target: putty.exe	
Path: \\10.100.1.7\working\applications\	
Process: explorer.exe	
	_
Cb Protection blocked an attempt by explorer.exe to run putty.exe because the network location \\10.100.1 Z\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.	
diagnostic data.	
	~
	_
ОК	
Submit Approval Request>>	_
Dente Dente	
Process Target Path	_^
X 3 msiexec.exe putty-64bit-0.74-installer c:\users\nccoeuser\desktop\	
A 4 explorer.exe /Z1900-x64.exe c:\users\nccoeuser\desktop\	
S explorer.exe mmap-7.80-setup.exe C: (users (incodedser (desktop))	-
exploremente putty exe ((10.100.1.7 (working appricate))	~
< c	>
Approval Request	
Enter your reason for access (512 characters A Your Email: Defarious user@nist	001
max).	
Priority: Medium	-
	_
Submit	
· · · · · · · · · · · · · · · · · · ·	
Protection by Carbon Black, Inc.	

1376 Figure D-51: Carbon Black Alert Showing the Execution of putty-64bit-0.74-installer.msi Being Blocked

Security Notification - Unappr	oved Script	
Cb Target: pu Path: c: Process: m	nty-64bit-0.74-installer.m \users\nccoeuser\deskto siexec.exe	nsi Jp\
Cb Protection blocked 0.74-installer.msi beca file, please contact you Note that approval req Please be patient while diagnostic data.	an attempt by msiexec.e use the file is not approv ir system administrator o uests are processed base your request is reviewe	exe to run the script putty-64bit- red. If you require access to this or submit an approval request. ed on priority and arrival time. ed and processed. Scroll down for
		~
Submit Approval Reque	<u>st&gt;&gt;</u>	ок
Process	Target	Path
× 1 ccsvchst.exe	idsxpx86.dll	c:\programdata\symantec\symante
X 2 explorer.exe	1.exe	c:\users\nccoeuser\desktop\
A 3 msiexec.exe	putty-64bit-0.74-installe	er c:\users\nccoeuser\desktop\
<		>
Approval Request		
Enter your reason for a	ccess (512 characters 📈	Your Email: nefarious.user@nist.gov
max).		
		Priority: Medium
		Submit
Protection by Carbon Blac	k, Inc.	

1377 Figure D-52: Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity



- 1378 Figure D-53: Azure Defender for IoT Alert Details Showing RPC Connection Between the DMZ and the
- 1379 Testbed LAN



1380 Figure D-54: Azure Defender for IoT Event Alert Timeline Showing the File Transfer

Hicrosoft	÷	Event Timeline									Θ
		Free Search			Q Advanced Filters	All Events 👻	式, User Op	erations 🗇 Select Date	CRefresh	O Create Event	B Export
Dashboard	(Ø)					Apr 14 2021					
Devices Map (75)	윪			File Transfer Detected	2	Apr 14, 2021					
Device Inventory	=		9	Apr 14, 2021 2:17:19 PM	_						
Alerts (113)	۰		Apr 14, 2021 2:1	17:19 PM	*	14:17:19					
Reports			File transfer f Protocol: SMI	rom client IP: 192.168.0.20, Ser B, File Name: Applications\putty	ver IP: 10.100.1.7 -64bit-0.74-installer.msi						
Event Timeline	Ê		Apr 14, 2021 2:1 File transfer f	17:19 PM from client IP: 10.100.0.20, Serve	er IP: 10.100.1.7						
Data Mining	۶.		Protocol: SMI	B, File Name: Applications\putty	-64bit-0.74-installer.msi 👻			Alast Datastad			
Investigation	\$			~	Notice			Apr 14, 2021 2:17:14 PM RPC client sent procedure inv	ocation request. Client:		
Risk Assessment	▲					14:17:14	Ŧ	192.168.0.20, Server: 10.100 1670-01D3-1278-5A47BF6EE	1.7, Interface: 4B324FC8- 188, Function: 16.		
Attack Vectors											
								PCAP file			
Custom Alerts				Alert Detected Apr 14, 2021 2:17:14 PM				~	Alert		
Users			÷	RPC client sent procedure inv 10.100.0.20, Server: 10.100.1	ocation request. Client: .7, Interface: 4B324FC8-	14:17:14					
Forwarding				1670-01D3-1278-5A47BF6EE	188, Function: 16.						
System Settings	\$			PCAP file							
Import Settings				*				Alert Detected			
					Alert	·	Ļ.	RPC client sent procedure inv 192.168.0.20. Server: 10.100.	ocation request. Client: 1.7. Interface: 4B324FC8-		
Horizon	<u>. 0</u> .					14:17:14		1670-01D3-1278-5A478F6EE	188, Function: 15.		
Azure Defender for Version 10.0.3	loT							PCAP file			

# 1381 D.5 Executing Scenario 5: Protect from Unauthorized Addition of a Device

- 1382 An authorized individual with physical access connects an unauthorized device on the manufacturing
- 1383 network and then uses it to connect to devices and scan the network. The expected result is behavioral
- anomaly detection identifies the unauthorized device.

# 1385 D.5.1 Build 1

1388

- 1386 D.5.1.1 Configuration
- 1387 Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

# 1389 *D.5.1.2 Test Results*

- 1390 Tenable.ot detects and alerts on the addition of a device to the environment. Figure D-55 shows an
- 1391 event reported by Tenable.ot when a device was connected to the wireless access point in the
- 1392 manufacturing environment. Tenable.ot also detects other activity from the device, as shown in Figure
- 1393 <u>D-56</u>, in which the new device tries to establish a secure shell (SSH) connection to the network switch.

1394 Figure D-55: Tenable.ot Event Showing a New Asset has Been Discovered

Powered by Indegy					03	8:07 PM • Friday, Jan 29, 2	2021 NCCOE Use
🗸 🌲 Events	Î						
All Events	All Events 172.1	16.1.30	٩			Actions ~ Resolve A	ll Export €
Configuration Events	LOG ID	TIME 🗸	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS
SCADA Events Network Threats	9069	02:42:23 PM · Jan 29, 2021	New asset discov	Low	New Asset Discovered	Endpoint #61	172.16.1.30
Network Events							
Policies							
v 🚔 Inventory							
Controllers	4						,
Controllers Network Assets	Items: 1-1 out of 1					K K	Page 1 of 1 > >
Controllers Network Assets	<ul> <li>Items: 1-1 out of 1</li> <li>Event 9069 02:42:2</li> </ul>	23 PM · Jan 29, 2021 New as	set discovered Low	Not resolved		к <	Page 1 of 1 > >
Controllers Network Assets	<ul> <li>Items: 1-1 out of 1</li> <li>Event 9069 02:42:2</li> <li>Details</li> </ul>	23 PM · Jan 29, 2021 New as	set discovered Low	Not resolved		К <	Page 1 of 1 > >
Controllers Network Assets a Risk Metwork Network Summary	Event 9069 02:42:2 Details	23 PM · Jan 29, 2021 New as A new asset has been	set discovered Low	Not resolved	ot	K K	Page 1 of 1 > →
Controllers Network Assets  a Risk  A Network Network Network Summary Packet Captures	Event 9069 02:42:2 Details Affected Assets Policy	23 PM · Jan 29, 2021 New as A new asset has been SOURCE NAME Endpoi	set discovered Low detected in the netwo	Not resolved	ot Why is this	K < Suggested	Page 1 of 1 > →
Controllers Network Assets Risk Network Network Summary Packet Captures Conversations	terms: 1-1 out of 1 Rems: 1-1 out of 1 Event 9069 02:42:2 Details Affected Assets Policy Status	23 PM · Jan 29, 2021 New as A new asset has been source NAME Endpoi source Address 172.16.	set discovered Low detected in the netwo nt #61 1.30	Not resolved	ot Why is this important?	K K Suggested Mitigation	Page 1 of 1 > >
Controllers Network Assets Risk Network Network Network Network Network Conversations Assets Map	t Berns: 1-1 out of 1 Event 9069 02:42:2 Details Affected Assets Policy Status	23 PM - Jan 29, 2021 New as A new asset has been Source NAME Endpoi Source Address 172.16 DESTINATION	set discovered Low detected in the netwo nt #61 1.30	Not resolved	ot Why is this important? It is important to know wh	K < Suggested Mitigation at Make sure that 1	Page 1 of 1 > >
Controllers Network Assets      Kisk      Kisk Network Network Network Summary Packet Captures Conversations Assets Map      Goups	<ul> <li>Rems: 1-1 out of 1</li> <li>Event 9069 02:42:3</li> <li>Details</li> <li>Affected Assets</li> <li>Policy</li> <li>Status</li> </ul>	23 PM - Jan 29, 2021 New as A new asset has been SOURCE NAME Endboi SOURCE ADDRESS 172.16. DESTINATION NAME	set discovered Low detected in the netwo nt #61 1.30	Not resolved	ot Why is this important? It is important to know wh assets exist in your netwo New assets can indicate	K < Suggested Mitigation at Make sure that rk. Make sure that	Page 1 of 1 > >
Controllers Network Assets > & Risk Network Summary Packet Captures Conversations Assets Map > @ Groups @ Reports	Henrs: 1-1 out of 1 Event 9069 02:42:2 Details Affected Assets Policy Status	23 PM · Jan 29, 2021 New as A new asset has been source name Endpoil source name Endpoil source anoness 172.16 DESTINATION NAME DESTINATION	set discovered Low detected in the netwo nt #61 .1.30	Not resolved	ot Why is this important? It is important to know wh assets exist in your research unexpected network connections, third party	K < Suggested Mitgation at Make sure that is familiar to you asset owners. If familiar with the	Page 1 of 1 ≥ ≥ he asset is it this IP and ior to other you are not asset.

1395 Figure D-56: Tenable.ot Event Showing Unauthorized SSH Activities

					03:12	PM • Friday, Jan 29,	, 2021 NCCOE U
Events	All Events	0				ctions v Resolve	All Export
All Events	All Evenes	-					
Configuration Events	LOG ID	тіме 🕹	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS
SCADA Events	9086	03:10:50 PM · Jan 29, 2021	Unauthorized Co	Medium	SSH Communications to Engineeging S	Endpoint #61	172.16.1.30
Network Threats	9085	03:06:01 PM - Jan 29: 2021	Unauthorized Co	Medium	SSH Communications to Engineeging S	ConsoleWorks	10,100.0.53
Network Events		05/00/011111 (01/25, 2021			2211221111011011011212200011230005200	SALASSISTER	
Policies							
Inventory							
Controllers							
Network Assets	Items: 1-2 out of 2					K K	Page 1 of 1 >
Network Assets Risk	Items: 1-2 out of 2 Event 9086 03:10:5	0 PM · Jan 29, 2021 Unauth	orized Conversation	Medium M	Not resolved	ĸĸ	Page 1 of 1 >
Network Assets Risk Network	Items: 1-2 out of 2 Event 9086 03:10:5 Details	0 PM · Jan 29, 2021 Unauth	orized Conversation	Medium M	Not resolved	K <	Page 1 of 1 >
Controllers Network Assets Risk Network Network Summary	Items: 1-2 out of 2 Event 9086 03:10:5 Details Source	0 PM · Jan 29, 2021 Unauth A conversation in an u	orized Conversation inauthorized protocol	Medium M	Not resolved	ĸĸ	Page 1 of 1 >
Controllers Network Assets Risk Network Network Summary Packet Captures	Items: 1-2 out of 2 Event 9086 03:10:5 Details Source Destinatior.	0 PM · Jan 29, 2021 Unauth A conversation in an u	orized Conversation inauthorized protocol nt #61	Medium M	Not resolved tected	K K	Page 1 of 1 > >
Controllers Network Assets Risk Network Network Summary Packet Captures Conversations	Item: 1-2 out of 2 Event 9086 03:10:5 Details Source Destination Policy	0 PM - Jan 29, 2021 Unauth A conversation in an u	orized Conversation inauthorized protocol nt #61 1.30	Medium M	Not resolved	K < Suggested Mitigation	∑ Page 1 of 1 > →
Controllers Network Assets Risk Network Network Summary Packet Captures Conversations Assets Map	Items: 1-2 out of 2 Event 9086 03:10:5 Details Source Destination Policy Status	0 PM - Jan 29, 2021 Unauth A conversation in an u	orized Conversation inauthorized protocol nt#61 1.30	Medium M	Not resolved tected Why is this important?	K < Suggested Mitigation	Page 1 of 1 > :
Controlers Network Assets Risk Network Network Summary Packet Captures Conversations Assets Map Groups	Items 1-2 out of 2 Event 9086 03:10:5 Details Source Destinatior. Policy Status	0 PM - Jan 29, 2021 Unauth A conversation in an u source answer Endpoi source anowers 172.16 DESTINATION Stratist NAME	orized Conversation inauthorized protocol nt #61 1.30 5700 VLAN1	Medium M	Not resolved tected Why is this important? Conversations in unauthorized protocols may indicate suppion artific.	K < Suggested Mitigation Check if this co is expected. If i traffic, then adj	Page 1 of 1 > 2
Controllers Network Assets Risk Network Network Summary Packet Captures Conversations Assets Map Groups Reports	Items: 1-2 out of 2 Event 9086 03:10:5 Details Source Destination Policy Status	0 PM - Jan 29, 2021 Unauth A conversation in an u source wave Endpoi source adverss 172.16 postivation Strated name DISTINATION 172.16	orized Conversation inauthorized protocol nt.#61 1.30 5700 VLAN1 1.3	Medium N	Not resolved tected Why is this important? Conversations in unauthored protocols may indicate suppious traffic. Some assets are not expected to communicate in	K K Suggested Mitigation Check if this co is expected. If traffic, then ad Policy condition Events arent gr	Page 1 of 1 > 2 mmunication this expected just the ns so that enerated for

- D.5.2 Build 2 1396
- D.5.2.1 Configuration 1397
- 1398 Behavior Anomaly Detection: eyeInspect
- 1399
- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2. •

#### D.5.2.2 Test Results 1400

- 1401 Forescout detects when an unauthorized device connects to a wireless access point in the
- 1402 manufacturing environment. Figure D-57 shows that Forescout raises an alert on the DNS request from
- 1403 the wireless access point to the gateway. The device establishes an SSH connection, which is detected by
- 1404 Forescout as shown in Figure D-58. A more detailed view of the alert is shown in Figure D-59.

1405 Figure D-57: Forescout Alert on the DNS Request from the New Device

						<li>Help</li>
Summary		^	Source host info	• •	Alert Details	^
Alert ID	169436 Oct 13, 2020 13:33:55		IP address	172.16.2.30 (Private IP)	ID and name	lan_cp_cnw_c - Communication pattern not whitelisted
Sensor name	sensor-bundle-nccoe		Host MAC addresses	00:09:58:AA:E9:29 (Netgear) Last seen: Oct 13: 2020 13:32:38	Description	Communication pattern not whitelisted: the source and destination hosts are whitelisted in
Detection engine Profile	9 - UDP communications		Other observed MAC addresses	E4:90:69:38:C2:C3 (Rockwell) E4:90:69:38:C2:C0 (Rockwell)	Trinorday	some communication rule, but not with this combination
Severity	Medium		Role	SNMP manager	rule/default	alert
Source MAC Destination MAC	00:09:5B:AA:E9:29 (Netgear) E4:90:69:3B:C2:C2 (Rockwell)		Other roles	Windows workstation, Web server, Terminal client	action	
Source IP	0 172.16.2.30 (stochastic)			DNS (UDP 53)		
Destination IP	172.16.2.1 (stratix8300.mgmt.lab)			FailedConnection (TCP 80, 7000, 7001, 7002, 7004, 7005, 7006, 7007, 7008, 7009, 52311)		
Source port	65444			LDAP (UDP 389) NotAKnownOne (UDP 443, 19000)		
Destination port	53		Client protocols	RDP (TCP 3389)		
12 nmtn	Ethernet			2010 (107 440)		

1406 Figure D-58: Forescout alert showing the SSH connection

Oct 13, 2020 13:24:58	Communication	sens	Co	8 - TC	Not ana	M	172.16.2.30	172.16.2.2 (	22 (TCP)	SSH
--------------------------	---------------	------	----	--------	---------	---	-------------	--------------	-------------	-----

1407 Figure D-59: Detailed Forescout alert of the Unauthorized SSH Connection

<) FORES	COUT. 🙆 Dashboard	A Ne	twork 📕 Events	Sensors 📽 Settings		🖵 💐 🙎 🗮 admin
Alert details	Back Edit	Delete	Trim Show   ~	Assign to case 🛛 Download   🛩		Help
Summary		^	Source host info	^	Alert Details	^
Alert ID	169373		IP address	172.16.2.30 (Private IP)	ID and name	lan_cp_cnw_c - Communication pattern not
Timestamp	Oct 13, 2020 13:24:58		Host name	stochastic		Communication pottern opt whitelisted the
Sensor name	sensor-bundle-nccoe		Host MAC	00:09:58:AA:E9:29 (Netgear)	Description	source and destination hosts are whitelisted in
Detection engine	Communication patterns (LAN CP)		addresses	Loss seen: GCE 13, 2020 13:24:36	Description	some communication rule, but not with this
Profile	8 - TCP communications		MAC addresses	E4:90:69:38:C2:C3 (Rockwell) E4:90:69:38:C2:C0 (Rockwell)		combination
Severity	Medium		Role	SNMP manager	rule/default	alert
Source MAC	00:09:5B:AA:E9:29 (Netgear)			Windows workstation. Web server. Terminal	action	
Destination MAC	F4:54:33:2F:E1:C1 (Rockwell)		Other roles	client		
Source IP	0 172.16.2.30 (stochastic)			DNS (UDP 53)		
Destination IP	0 172.16.2.2 (operations.lan.lab)			FailedConnection (TCP 80, 7000, 7001, 7002, 7004, 7005, 7006, 7007, 7008, 7009, 52311)		
Source port	55262			LDAP (UDP 389)		
Destination port	22		Client protocols	NotAKnownOne (UDP 443, 19000) RDP (TCP 3389) SMB (TCP 445)		
Alerts / Alert details	FTRAMAT					Copyright (C) 2009-2020 Forescout (v. 4.1.2)

- 1408 D.5.3 Build 3
- 1409 D.5.3.1 Configuration
- 1410 Behavior Anomaly Detection: Dragos
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.

# 1413 *D.5.3.2 Test Results*

- 1414 Dragos detected the traffic generated by the new asset and generated several alerts as seen in the list of
- 1415 alerts in Figure D-60. Details of different aspects of the network scanning can be seen in Figure D-61 and
- 1416 <u>Figure D-62</u>. Details on the new device can also be seen in <u>Figure D-63</u>.

1417 Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network

# 1418 Scanning

				ASSET NOTIFICAT	IONS			SYSTEM ALERTS			RULES		
( <del>-</del> = F)	TERING	- Fre 02	xm /17/21, 19:00	о итс 🛅 📆	17/21, 21:00 UTC	C REFRESH						Q Seath 0.205	×
	View	Sever :	ID :	Occurred At	•	Туре	÷ Summary	Message	Detected By	2 Asset IDs	Source IPv4	C Dest. IPv4	C Other IPv4
	VIEW		148691	02/17/21, 20.59 UTC	Asset		NewSourceEth Detected	Asset 2709 seen as the ethernet source for the first t.	New Source Ethernet Address Detection	2709			192.168.0.205
	VIEW		148675	02/17/21, 20:56 UTC	Communication		NewDestEth Detected	Asset 2789 seen as the Ethemet destination for the	New Destination Ethernet Address Detection	2789			192.168.0.205
	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	65			10.100.1.4

1419 Figure D-61: Details of Network Scanning Activity

DETECTION INFO	RMATION		ASSOCIATE	D ASSETS				
FILTER     WHAT HAPPENED:     ICMP scan observed floor)     of 1070 (100.00%). A step     to     for 00.00, 18, 10, 100.00, 19, 10     100.00, 18, 10, 100.00, 19, 10     100.00, 18, 10, 100.00, 19, 10     100.00, 18, 10, 100.00, 10, 10     100.00, 18, 10, 100.00, 10, 10     100.00, 18, 10, 100.00, 14, 10	sset: 85, 10.100.1,4 swept at least 214 unique hosts faxe of 1 occurred 1670 times (100.00%). Top ships at 0.6, 10.1000.7, 10.1000.6, 10.1000.2, 10.1000.1, 10.000.20, 10.1000.02, 10.100.02, 21, 10.1000.22, 10. 1000.034, 10.1000.035, 10.100.036, 10.1000.037, 11 1000.48, 10.1000.04%, 10.100.036, 10.1000.037, 11	(this do instreagond) via iona topo 8 neguesta in 2005. Addresses were incrementary 1070 (in res out es were. 1012700; The longest care of configurues addresses was 240 long. All destination addresses 1,6 1050-11,0 1000; T. E. 1000; T. E. 1000; A. F. 1000; A. F. 10,000; A. F. 10,000; A. F. 10,000; A. F. 1000; B. J. 10,1000; T. E. 1000; A. F. 1000; C. 7,000; B. Z. 1000; B. Z. F. 1000; Z. F. 1000; B. Z. 1000; B. Z. F. 1000; B. J. 1000; B. Z. 1000; A. F. 1000; C. Z. 1000; B. Z. 200;	View	C Type	÷ iD ≑ sServ 85 Asset	No 85	me	÷ Dir 10.100.1.4 oti
J         10 1000 74 [10 100.0.1]           G         10 000 74 [10 100.0.1]           G         10 000 74 [10 100.0.1]           G         10 000 702,10 0008 [10 100.0.01]           G         10 000 702,10 000,112 000,112           G         10 000 702,10 000,113           G         10 000 702,10 000,110           G         10 000 702,10 000,110           G         10 000 702,10 000,110           G         10 000 729,10 000,110           G         10 0000 729,10 000,100           <	$\label{eq:2} \begin{array}{l} 3.000\ J, W_1 = 101 Im J, V_1 = 101$	$\begin{array}{c} \label{eq: 1} (0,0) = 0.00 \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $				No. Communications Commany.		
OCCURRED AT: 02/17/21, 19:50 UTC		LAST SEEN: 01/01/70,00:00 UTC						
COUNT:		STATE: UNRESOLVED						
DETECTED BY: ICMP Sworp		SOURCE: 64370443 c117.4053 a163 Matter/961486						
DETECTION QUAD: Threat Behavior		ZONES: DMZ						
ACTIVITY GROUP: Common		ICS CYBER KILLCHAIN STEP: Stage 1 - Recentratesance						
MITRE ATT&CK FOR IC	STACTIC	MITRE ATTACK FOR ICS TECHNIQUE T0844: Remote System Discovery 2						
QUERY-FOCUSED DATA Scienting	SETS:	NOTIFICATION RECORD: View In fibina						
PLAYBOOKS: Network Address Scanning	Activity Detected	NOTIFICATION COMPONENTS: View in Vibana						

1420 Figure D-62: Additional Details of Network Scanning Activity

DETECTION INFORMATION	De LECTION INFORMATION WHAT MAPPEND information and the second se				
WHAT HAPPENED:           Sample Navid Commonization values includer (p. sm_staskL)(r. 10 102 2:05, 192 148.0.2, 224.0.0251, 10 100 2:05, 192 148.0.2, 224.0.0251, 10 100 2:05, 192 148.0.2, 424.0.0251, 10 100 2:05, 425.0.0251, 426.0.02				Name	+ 0 1 fe80:0:0:0:5971:100e:8570:3121
OCCURRED AT: 02/17/23, 20:99 UTC	LAST SEEN: DIJOT/70, ORCO UTC		96 Asset 96		192.168.0.2
DETECTED BY:	STATE UNREDOLVED SOURCE:				
	UFFILIDZER-SODIE-WIDER-SUDIERDER TERMIN, RUDORS-HIDTER-WIDER-SUDIERDER DER BT II FERSTeilt 2022 MERFF 2015 DER KOMSTERBIN, GUSSTerbit That Lander 2017 ARTISTER 1773/16/24 S STURY 4667 all/SE 10/24/02/27/34, 15560011 (624 AstiS 1086 02/44bc1 Babod TANKER-		No Cor	nmunications Summary	
No Applicable Detection Quad	ZUNRES: RTC1910, Cyberseouthy LAN				
Ac Applicable Activity Group	MITRE ATTACK TACTIC: No Applicable MITRE ATTACK Tactic				
MITRE ATT&CK TECHNIQUE: No Applicable MITRE ATT&CK Technique					
QUERY-FOCUSED DATASETS: No Applicable Query-Focused Datasets	NOTIFICATION RECORD: View in Klasna				
PLAYBOOKS: No Associated Playbooks CASES:	NOTIFICATION COMPONENTS: View in Kösene				
No Canes Linked					
RELATED NOTIFICATIONS					
ID C Occurred At C		Summary			
ID - UCCUITING AT -		summary			

1421 Figure D-63: Alert for New Asset on the Network

DETECTION INFORMATION		ASSOCIATED ASSETS	
HILTER Addet.2789 does as the othernet source for the first time.		View         Type         ID         Name           VIEW         mm         Berver         2789         Asset 2789	<ul> <li>Dir.</li> <li>192.768.0.200 oth</li> </ul>
COURT AT: COURT 25 UTC COURT 25	LAT STOR UNIVERSITY OF AN AND AND AND AND AND AND AND AND AND	COMMUNICATIONS SUMMARY	
RELATED NOTIFICATIONS	2015 55 242	Submay No Reader Notification	

1422 D.5.4 Build 4

1425

1426

- 1423 D.5.4.1 Configuration
- 1424 Behavior Anomaly Detection: Azure Defender for IoT
  - Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- 1427 *D.5.4.2 Test Results*
- 1428 A "New Asset Detected" alert is shown on Azure Defender for IoT dashboard (Figure D-64) and on the
- 1429 Alert screen (Figure D-65). Figure D-66 shows the alert management options in Azure Defender for IoT.
- 1430 The details of the network scanning alert are shown in Figure D-67.
- 1431 Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset



1432 Figure D-65: Azure Defender for IoT Detects New Asset in the Environment

🚦 Microsoft	÷	Alerts		Θ
		192.168.0.205 Q. Advanced Filters Security Operational	Main View ~ B	Export All Alerts
Dashboard				
Asset Map (96)		Important Alerts (2) 🔯 🛷 🛍	Pinned Alerts (0)	
	=	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 learne	No Alerts	
Alerts (63)		POLICY New Asset Detected   just now VIOLATION A new asset was detected on the orthoryk. Asset 192,168.0.203 was added to your meteoryk. Verify that this is a wald network asset		
Reports				
Event Timeline	Ê			
Data Mining				
Investigation				
	▲		Recent Alerts (2)	B =/ 10
Attack Vectors			POLICY Unauthorized Internet Connectivity Detected	Jan 6 14:36
			VIOLATION As asset defined in your internal network is communicating with addresses on the Internet. These addresses hav POLICY New Asset Detected	e 10
			VIOLATION A new asset was detected on the network. Asset 192.168.0.205 was added to your network. Verify that this is a	Jan 6 14:36
Forwarding				
System Settings	٠			
Import Settings				
Support	۲			
Azure Defender for i				

1433 Figure D-66: Azure Defender for IoT Alert Management Options

	Ê	G	<b>⊥</b>	<u>بر</u>	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.										
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 detected	d agaiı	ı.								
<ul> <li>Disconnect the asset from the network. Select Delete Asset. This asset will not be an unless it is detected again.</li> </ul>	<ul> <li>Disconnect the asset from the network. Select Delete Asset. This asset will not be analyzed by the sensor unless it is detected again.</li> </ul>									
Delete Asset	Аррго	ove	Ac	:know	ledge					

1434 Figure D-67: Details for Network Scanning Alert

	Device Connection Detected Jan 6, 2021 2:36:03 PM	6
Grouped	1 Events	
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 od devices 192 168 0 205 and 10 100 0 17	•
	~	
Assets		
Туре	Name	
	Station 2	
	LAN-AD	
	Station 4	
	Station 3	
	Station 1	
	CRS Supervisory LAN Gateway	
	192.168.0.205	-
		Info

# 1435 D.6 Executing Scenario 6: Detect Unauthorized Device-to-Device 1436 Communications

- 1437 An authorized device that is installed on the network attempts to establish an unapproved connection
- 1438 not recorded in the baseline. The expected result is the behavioral anomaly detection products alert on 1439 the non-baseline network traffic.
- 1440 D.6.1 Build 1

1443

- 1441 D.6.1.1 Configuration
- 1442 Behavior Anomaly Detection: Tenable.ot
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

- 1444 *D.6.1.2 Test Results*
- 1445 The unapproved SSH traffic is detected by Tenable.ot as shown in Figure D-68.
- 1446 Figure D-68: Tenable.ot Event Log Showing the Unapproved SSH Traffic

tenable.ot					03:5	30 PM • Friday, Jan 29, 2	2021 NCCOE U	
Events			_					
All Events	All Events ssh	٥	٩			Actions ~ Resolve A	ll Export	
Configuration Events	LOG ID	TIME 🕹	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	
SCADA Events	0007	02:22:51 DM- Ion 20, 2021	Linauthorized Co.	Modium	SSH Communications	DCS Eng Station	172 16 2 10	
Network Threats	3037	03.22.51 PM - Jan 29, 2021	Unauthorized Co		COLI Communications	PCS Eng. Station	172.10.3.10	
Network Events	9093	03:20:44 PM - Jan 29, 2021	Unautionzed Co	Mealum	SSH communications	PCS Engl. Station	172.10.3.10	
Policies	Items: 1-10 out of 10					K K	Page 1 of 1 >	
Inventory	Event 0002 02:20:44	PM Jap 20 2021 Lipsuth	orized Conversation	Medium	Not recolved			
Controllers	Event 9093 03:20:44	PM - Jan 29, 2021 - Onautr	ionzed conversation	Medium r	NOLTESOIVED			
Network Assets	Details	A conversation in an	unauthorized protocol	has been del	tected			
Risk	Source	SOURCE NAME PCS Er	g. Station		Why is this	Suggested		
Network	Destination	SOURCE ADDRESS 172 16	3.10		important?	Mitigation		
Network Summary	Policy	SOURCE RODINESS IT LITE						
Packet Captures	Status	DESTINATION Stratix NAME	5700 VLAN1		Conversations in unauthorized protocols may indicate suspicious traffic.	is expected. If it i traffic, then adju	in expected is the	
Conversations		DESTINATION 172.16	.1.3		Some assets are not expected to communicate in	Policy conditions Events aren't ger	s so that nerated for	
Assets Map		ADDRESS			non-standard protocols and	similar communi	ications in	
Groups		PROTOCOL SSH (to	:p/22)		standard protocols may suggest a potential threat.	communication i expected, check	, is not the source	
Reports		PORT 22			In addition, some protocols are unsecure and should	asset to determine the source asset	ne whether itself has	
on 3.8.17   Evolves: Dec 9, 2021					not be used at all, in order	been compromis	sed. If this	

1447 D.6.2 Build 2

1450

- 1448 D.6.2.1 Configuration
- 1449 Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

# 1451 *D.6.2.2 Test Results*

- 1452 SSH communication from HMI computer to the network switch is not defined in the baseline; Forescout
- 1453 flags this communication as shown in Figure D-69.

1454 Figure D-69: Forescout Alert Showing the Unapproved SSH Traffic

<) FORESCO	UT. 🖪 Dashboard 🚣 Network 🔳 Event	s 🎝 Sensors 📽 Se			🖵 🧈 🙎 🗮 admin
rt details	Back Edit Delete Trim Show (	- Assign to case I	Downlaid   -		🕑 Help
Summary	^	Source host info	^	Alert Details	^
Nert ID	139850	IP address	172.16.1.4 (Private IP)	ID and name	$lan,cp,cnw,\varepsilon\cdot Communication pattern not whitelisted$
limestamp	Oct 7, 2020 12:06:19	Host name	fgp-61338hh		Communication pattern not whitelized the source and
ienoor name	sensor-bundle-nccoe	Other host names	fgs-61338hh.lan.lab	Description	destination hosts are whitelisted in some communication rule, but not with this combination
Detection engine Profile	Communication patterns (LAN CP)	Host MAC addresses	0C:C4/74/31:64/47 (SuperMic) Sant sever: Oct 7, 2020 12/18/07	Triggering rule/default action	plan
levenity	Medium	Phase shares at little	E4:00:69:38:C2:C3 (Rockwell) E4:90:69:38:C2:C2 (Rockwell)		
iource MAC	0C.C4/7A:31:44:47 (SuperMic)	addresses	E450.69/38/C2/C0 (Rockwell) 7C/0E/CE:67:85:88 (Cisco)		
in the second second	0 17116 1 ( (m. 1713))		7C.0E:CE:67:86:83 (Cisco)		
territe a	O TTALE A December of	Role	Terminal server		
PENDENDORN IF	<ul> <li>sectors (beaut)</li> </ul>	Other roles	Windows workstation		
ource port	51540	Vendor and model	Rockwell		
festination port		O5 version	Windows 7 or Windows Server 2008 R2		
1 proto	Ethernet		DCOM (TCP 135, 49155, 49159)		
3 proto			DNS (UDP 53, 5355)		
4 proto	10		FailedConnection (TCP 23, 80, 139) HTTP (TCP Ibild)		
7 proto	25H		Kerberos (TCP 88)		
CP stream opened in sot start mode	feise		LDAP (TCP 389) LDAP (UDP 389)		
atus	Not analyzed	Client protocols	NetBLOS (UDP 137)		
obels			NoData (TCP 50005)		
lser notes Aonitored networks	^		Nob/Knewn/knike(UDF 1314) SNB (CP 445) SNB (UDP 138) SDP (UDP 1900) SSH (TCP 22)		
Name	Address VLAN IDs		Syslog (UDP 514)		
			DCOM (TCP 135, 6160)		

- 1455 D.6.3 Build 3
- 1456 D.6.3.1 Configuration
- 1457 Behavior Anomaly Detection: Dragos
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.
- 1460 *D.6.3.2 Test Results*
- 1461 Dragos detected the non-baseline SSH traffic as shown in Figure D-70.

1462 Figure D-70: Dragos Alert Showing the Unapproved SSH Connection Between Devices

DETECTION INFORMATION		ASSOC	IATED ASSETS						
WHAT HAPPENED: New Communication from here 1162 106 1 100 to here 1	192 168 3 103 new SSU on next 1921 for the first firms	Vie	/ : Туре	5 ID 5		Name			Dir. 1
T PILTER	and the structure oper one part paging the most since.	VI.	Controller	3177 Asset 31	77			192.160.1.104	810
AJ Status OCCURRED AT: 04/29/21, 15:00 UTC	LAST SEEN: 04/79/21, 19:00 UTC	- VI	W Controller	3186 Asset 31	86			192.168.1.101	dst
COUNT:	STATE:	COMM	UNICATIONS SUM	MARY					
	UNRESOLVED		8						
New Communication Planing	4/b5e530 5568 4c32 a2et ct1159ta2085	<>							
DETECTION QUAD: No Applicable Detection Quad	ZONES: CRS - Level 0	Ð			-		-		
				Sam	ARP		nin		
No Appleable Activity Broup	ICS CYBER KILLCHAIN STEP:			Texas Ins 80.D5:CC: 192.168	riments 54:26:EC 1.104	B0.D5.Cl	tstriments C:FA:70:C9 58.1.101		
	No Applicable MITRE ATTACK Tacts:			_tcp i machining-sta	ical dion-4.local	maching-	station-1 local		
MITRE ATTACK TECHNIQUE: No Applicable MITRE ATTACK Technique		Protocol	¢ Olient	Ephemeral Ports	t Server	Server Ports	TX Bytes	÷ RX Bytes	\$
	NOTIFICATION RECORD:	SSH	192.168.1.104	48736	192.168.1.101	22	2.6 KB	1.8 KB	
No Applicable Query-Focused Defasets	Wew in Kibana	SSH	80.05.CC.F4.26.EC	48736	80.05.00.FA.70.09	22	2.6 KB	1.8 KB	
PLAYBOOKS: No Associated Playbooks	NOTIFICATION COMPONENTS: View in Kbana	ARP	82.05-00.F4/26/ED		ND 05.00 FA 70:09		60.0 bytes	© bytes	
CASES:		ARP	BRDS-CCFA-70-C9		80/05/0C/F4/26/EC		0 bytes	60.0 bytes	
No Cases Linked									
RELATED NOTIFICATIONS			Summary						-
			,						
		No Related Notifications							

# 1463 D.6.4 Build 4

- 1464 D.6.4.1 Configuration
- 1465 Behavior Anomaly Detection: Azure Defender for IoT
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.
- 1468 *D.6.4.2 Test Results*
- 1469 A device attempts to establish a remote access connection via SSH. Azure Defender for IoT was able to
- 1470 detect this activity as shown in Figure D-71.

Microsoft	÷	Event Timeline				
		Free Search	Q.         C Advanced Filters         All Events -         2. User Openations         C Select Date	ORefresh C	Create Event	B Exp
ashboard						
sset Map (96)			Jan 6, 2021 Remote Access Connection Established			
			Connection detected from 192.168.1.104 to			
	۰		192.168.1.102 using \$5H			
		_	Hit Transfer Detected			
			14:42:16 Grouped Events			
ent Timeline	Ê		Jan 6, 2221 2:42:18 PM			
ata Mining			H11P Hit transfer Irem Grent IP: 10.100.0.37, Server: Content type application/vnd.m more			
rvestigation			Jan 6, 2221 2:42:30 PM File transfor from client IP: 10.100.0.62, Server IP: 10.100.0.18			
	▲		Protocol: SMB, File Name: Ian Jabh more			
			Alert Detected			
			An asset defined in your internal network is communicating with addresses on the Internet. These 14:41:42			
			addresses have not been learned by Cyberx as valid addresses.			
			Asset 192.168.0.110 communicated with ad			
rstern Settings	٠		PLAME			
nport Settings		_	Alert Detected Alert			
			14:38:01 communicating with addresses on the Internet. These addresses have not been learned by Others as valid			
			addresses.			
upport	ø		Asset 10.100.1.7 communicated with addre			
			SNMP Trap detected			
Azure Defender for			An SNMP agent on 10.100.0.242 sent a trap to 10.100.0.14 14.07.46			

1471 Figure D-71: Azure Defender for IoT Event Identified the Unauthorized SSH Connection

# 1472 D.7 Executing Scenario 7: Protect from Unauthorized Deletion of Files

1473 An authorized user attempts to delete files on an engineering workstation and a shared network drive 1474 within the manufacturing system. The expected result is the file integrity checking tools in the

1475 environment alert on the deletion or prevent deletion entirely.

- 1476 D.7.1 Build 1
- 1477 D.7.1.1 Configuration
- 1478 File Integrity Checking: Carbon Black
- Agent installed on workstations and configured to communicate to the Carbon Black
   Server.
- 1481 File Integrity Checking: WORMdisk
- Network file share on server is configured to use WORMdisk.

# 1483 *D.7.1.2 Test Results*

1484 Carbon Black reports file deleting activities as shown in <u>Figure D-72</u>. GreenTec protects the files on its 1485 drive from being deleted.

1486 Figure D-72 Event Messages from Carbon Black Showing File Deletion Attempts

Timestamp 🔻	Se	Туре	Subtype	Source	Description	IP Address	User	Process Nat
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

- 1487 D.7.2 Build 2
- 1488 D.7.2.1 Configuration
- 1489 File Integrity Checking: Security Onion
- The agent is installed on workstations and configured to communicate to the Security
   Onion Server.
- 1492 File Integrity Checking: WORMdisk
- Network file share on server is configured to use WORMdisk.

#### 1494 *D.7.2.2 Test Results*

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

1497 Figure D-73: Security Onion Wazuh Alert Showing a File Has Been Deleted

	12 12 12 14	
@timestamp	Q, Q, []] *	October 15th 2020, 13:05:33.753
@version	Q Q 🗆 🛊	
_id	Q Q 🗉 🛊	JXY5LXUB1YHtrLLyVhik
_index	Q Q 🖽 🛊	seconion:logstash-ossec-2020.10.15
_score	Q Q 🗉 🛊	
_type	a a 🗆 🛊	doc
agent.id	Q Q 🗉 🛊	005
agent.ip	Q Q 🗉 🛊	A 172.16.3.10
agent.name	Q Q 🛙 🛊	PCS-EWS
alert_level	Q Q 🛙 🛊	
classification	Q Q 🛙 🛊	"Bad word" matching
decoder.name	Q Q 🗉 🛊	syscheck_integrity_changed
description	Q Q 🗉 🛊	File deleted.
event_type	Q Q 🗉 🛊	ossec
full_log	Q Q [] *	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 II *	1602781532.2062049
location	Q Q 🗉 🛊	syscheck
logstash_time	Q Q II *	0.002

# 1498 D.7.3 Build 3

- 1499 D.7.3.1 Configuration
- File Integrity Checking: Security Onion
  Agent installed on workstations and configured to communicate to the Security Onion Server.
- 1503 File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

# 1505 *D.7.3.2 Test Results*

1504

- 1506 Security Onion Wazuh detected the deletion of the files as shown in the Security Onion Server log in
- 1507 <u>Figure D-74</u>. Files stored on a storage drive protected by GreenTec are protected from deletion.

1508 Figure D-74: Alert from Security Onion for a File Deletion

🛛 🚱 🛛 Dashboard /	OSSEC		0
Table JSON			
- Ptin	mestamp	Feb 12, 2021 # 18:41:46.583	
T @ver	rsion		
t_inc	dex	seconion:logstash-ossec-2821.42.12	
-scc	ore		
t_typ	pe	_dec	
r ager	nt.id	983	
ා ager	nt.ip	△ 192.168.0.20	
t ager	nt.name	CR5-ENS	
/ aler	rt_level		
t clas	ssification	*Bad word* matching	
l decc	oder.name	syncheck_integrity_changed	
t desc	cription	File deleted.	
t ever	nt_type		
f full	1_log	File "c:\users\nccoexuer\documents\twincat projects\crs workcell\_boot\twincat co? (arm/?)\plc\port_851.oce' was deleted.	
1 host		gateway	
		1613144584.13813845	
t loca	ation	syscheck	
# logs	stash_time	9.697	
t mana	ager.name	seconion	
† mest	sage	<pre>&gt; {'tamestamp':'2021-02-12715:41:44.769+00000', "nule':("level':/, "description':'File doleted.", "id':'DS3", "fordiame':dd, "mail':true, "groups':["dessec", "syscheck"], "pci, des":["11.5"], "gog13":["4.11"], "god1":["11.5"], "gog13":["4.11"], "god1":["11.5"], "gog13":["4.11"], "god1":["11.5"], "gog13":["11.5"], "gog13":["11.5"]</pre>	5.1. Atwi de
/ port		26684	
i syst	check.event	deleted	
i syst	check.path	e:\usarsinccomuser\documents\trincat projects\crs workcall\_boot\trincat ce7 (arm/7)upl<\port_851.oce	

- 1509 D.7.4 Build 4
- 1510 D.7.4.1 Configuration
- 1511 File Integrity Checking: Carbon Black
- Agent installed on workstations and configured to communicate to the Carbon Black
   Server.
- 1514 File Integrity Checking: WORMdisk
- 1515 Network file share on server is configured to use WORMdisk.

# 1516 *D.7.4.2 Test Results*

- 1517 The attempts to delete a file are detected by Carbon Black as shown in <u>Figure D-75</u>. Files stored on a
- 1518 storage drive protected by GreenTec are protected from deletion.

#### 1519 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\toxaeshell\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\toxaeshell\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\toxaeshell\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

# 1520 D.8 Executing Scenario 8: Detect Unauthorized Modification of PLC Logic

- 1521 An authorized user performs an unapproved or unauthorized modification of the PLC logic through the
- 1522 secure remote access tools. The expected result is the behavioral anomaly detection tools will detect
- and capture the activity, flagging it for review.
- 1524 The behavior anomaly detection tools can detect program downloads to the PLC. Program download
- 1525 detection needs to be correlated with the maintenance management system to determine if the
- 1526 download was authorized and approved. This was not demonstrated as part of this scenario.
- 1527 D.8.1 Build 1
- 1528 D.8.1.1 Configuration
- 1529 Behavior Anomaly Detection: Tenable.ot
- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1531 Remote Access: Cisco VPN
- Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- 1533 User Authentication/User Authorization: ConsoleWorks
- Configured for accessing the PCS environment

# 1535 *D.8.1.2 Test Results*

- 1536 In this build, a remote session Studio 5000 Logix Designer is established to perform PLC file operations as
- 1537 shown in Figure D-76 and Figure D-77. Tenable.ot is able to detect the PLC file modifications as shown in
- 1538 Figure D-78 with details shown in Figure D-79 and Figure D-80.

1539 Figure D-76: Remote Access to Systems in PCS Network is Being Established Through ConsoleWorks

P NCCOE on 10.100.0.53 - Console × +		– ö ×
← → C ▲ Not secure   10.100.0.53:51	76/index.html	☆ \varTheta :
Console Works v 53-1u3	Devices Devices  Devices  Control of the devices  Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices Devices	
	Nursië of connections. 1  PCS_HAB Auchie of connections. 1  PCS_WORKSTATION  PCS_WORKSTATION PCS_WORKTATION PCS_WORKSTATION PCS_WORKSTATION PCS_	
TD) Technologies, Inc.	<ul> <li>2021/02/04 10:33 UTC-06:00</li> <li>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □</li></ul>	Invocation: NCCOE 요구 ~ 도고 네

1540 Figure D-77: Remote Session into Studio 5000 to Perform PLC File Operations



1541 Figure D-78: Tenable.ot Detected the Transfer of PLC Logic File to the Rockwell PLC	
--	--

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

# 1542 Figure D-79: Tenable.ot PLC Stop alert details

< Rockwell R Rockwell PLC stor Category	PLC Stop		[	STATUS Action	15 🗸
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	C Stop High N	lot resolved	
Exclusions	Details	The controller state was ch	nanged to Stop		•
	Source Destination	SOURCE <u>PCS Eng. Station</u> NAME	Why is	Suggested	П
	Policy	SOURCE 172.16.3.10	important?		11
	Status	ADDRESS	The system	1) Check whether the	
		destination <u>plc tesim</u> NAME	change in the controller	was made as part of scheduled	н
		DESTINATION172.16.2.102	state that was made	maintenance work and	• •

ategory				
Details	Items: 1-1 out of 1		K	< Page 1 of 1 > >
Triggered Events	Event 12413 01:46:3 resolved	0 PM · Feb 4, 2021 Rockwell C	ode Download 🛛 🛚	<mark>ledium</mark> Not
Exclusions	Details	Code was downloaded fro	om an engineering	station to the contro
	Code Source	SOURCE <mark>PCS Eng. Station</mark> NAME	Why is this important2	Suggested Mitigation
	Policy	SOURCE 172.16.3.10 ADDRESS	The system	1) Check whether the
	Status	DESTINATION <u>PIC tesim</u> NAME	detected a change in the	change was made as part of scheduled
		DESTINATION172.16.2.102	controller code that	whether the

#### 1543 Figure D-80: Tenable.ot PLC Program Download Alert Details

- 1544 D.8.2 Build 2
- 1545 D.8.2.1 Configuration
- 1546 Behavior Anomaly Detection: eyeInspect
- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1548 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.

# 1551 *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. 1557 Figure D-81: Remote Access to Systems in PCS Network is Being Established Through Dispel

5	Remote Desktop Connection				- 🗆 X
Recycle Bin	TC3_AddRo Reply from 16 Reply from 16 Reply from 16 Reply from 16 Reply from 16	ompt 9.100.1.7: bytes=32 time=184ms TTL=62 9.100.1.7: bytes=32 time=182ms TTL=62 9.100.1.7: bytes=32 time=184ms TTL=62 9.100.1.7: bytes=32 time=184ms TTL=62		- • ×	
Di N Dispel	Ping statisti Packets:	lcs for 10.100.1.7: Sent = 8, Received = 8, Lost = 0 (0% loss),			
fi Google Chrome	O Disped Client Settlings Help	Dispel is running Disconnect	-		
	Available Projects	Available Entry Points	Available Exit Points		
GUI	NCCOE-Manufacturing	Chicago, IL (	Exit NCCOE (cutter)		
putty					
TC31-FULL					
GreenTec					
GreenTec_D.					
TC3_Remo					
<					ب ایر ۲

1558 Figure D-82: Modifying the Parameters for the Allen-Bradley PLC Controller Using Studio 5000

File Edit View Search Logic	formunications Tools	Window Help							
🗎 📽 🖬 🍯 🕺 🛍 🛍	Who Active	- 🚜 🕰 🥱		Q. Q. Select language	- (	2			
Offline 0. ERUN	Select necent Path	AB_ETHIP-1\172.16.2.102\B	lackplane\2*	▼ 👪					
No Forces  No Edits Redundancy	<u>G</u> o Online Upload Download								
	<u>P</u> rogram Mode <u>B</u> un Mode <u>T</u> est Mode	Bit & Timer/Counter & In	put/Output 🔏 Comp	are 🔏 Compute/Math 🔏 Move/	Logical 🔏 File/Miss	e 🔏 File/Shirt	t 🔏 Sequencer 🔏 Program Co	ntrol 🔏 For/Breek 🔏 Spe	acial 🔏 Trig
Controller Organizer	Lock Controller	troller Tags - plc_tesim(con	stroller)						
- 2 Controller Tags	- Clear Faults	👔 pic_tesim 🔹 S	Show: All Tags				👻 💘 Erster Name Filter .		
- Controller Fault Handler	Go To Faults	me	22 2	Value +	Force Mask	Style	Data Type	Descrip *	Properties
Power-Up Handler		xmeas		()	()	Float	REAL[42]		21
		- xmeat[0]		0.0		Float	REAL		E Genera
MainProgram		xmeas[1]		0.2596462		Float	REAL		Name
Unscheduled Programs		xmeas[2]		3643.7734		Float	REAL		Descrip
A G Motion Groups		xmeas[3]		4400.6484		Float	REAL		Usage
Ungrouped Axes		xmeas[4]		9.152077		Float	REAL		Туре
Add-On Instructions		xmeas[5]		32.442017		Float	REAL		Alias Fo
🖃 🛅 Data Types		-xmeac[6]		47.07831		Float	REAL		Base I Date T
User-Defined		xmeas[7]		2798.7004		Float	REAL	E	Scope
🗄 📻 Strings		xmeas[8]		64.58219		Float	REAL		Externa
Add-On-Defined		xmeas[9]		122.92178		Float	REAL		Style
Predefined		xmeas[10]		0.23947726		Float	REAL		Consta
In Module-Defined		- xmeas[11]		92.13777		Float	REAL		Require
I - M Module-Delines		xmeas[12]		49.024353		Float	REAL		Visible
- Trends				2703 4492		Float	REAL		🗄 Data
- Trends I/O Configuration		- xmeas[13]		2703.4402					
Trends 1/0 Configuration 1756 Backplane, 1756-A7		xmeas[13] xmeas[14]		25.300936		Float	REAL		Value
→ Trends → 1/O Configuration → 1/56 Backplane, 1756-A7 ↓ → 1 [0] 1756-EN2TSC Enet[F	Sec	xmeas[13] xmeas[14] xmeas[15]		25.300936 49.936478		Float Float	REAL REAL		Value

- 1559 Figure D-83: Forescout Alerts Showing It Detected the Traffic Between the Engineering Workstation
- 1560 and the PLC

<) FORESCOUT	Dashboard	🔒 Network 🔲 Ever	nts 🔊 S	ensors	06 Settin	185					** 🙎	admii
Alerts	Reload Export	- Aggregate detail	s Create	new cas	e Settin	85						<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	(Not	0.4	(Nut sr .	(Not set) .	(No .	172.16.3.10	172.16.2.112 0	0	(Not set) .	(Unait .
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	13:47:52						M			(109)		
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 dst IP				142	(2) (2) (2) (1)	152510 0107					100000	
Excluding dst port	0ct 13, 2020 13:47:52	(PEA Exit) Message L	senso	C0+	8 - TCP c	Not analy	м	172.16.3.10 (tg	172.16.2.102 (	44818 (TCP)	ETHIP	
By L2 protocol	Ort 13 2020	(FFA Fixit) Message T	58050	Cn	8.TCP c	Not analy		172 16 3 10 //	172.16.2.102 (	44818	FTHEP	
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)		
By downstream data	Oct 13, 2020	ETHIP controller star	senso	Indu	2	Not analyz	88000 L	172.16.3.10 (fg	172.16.2.102 (	44818	ETHIP	
By FEA type	13:46:49									(10.9)		
<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 (	44815 (TCP)	ETHIP	
By labels	Oct 13 2020	Message type not w	68950	60	B. TCP.C	Not analy		177 16 3 10 ///#	172 16 2 102 1	44818	FTHIP	
-	L Str 13, 2020	meanage type not with	and an	C.C.I.I.	a lates	rece analy		the restriction	17 a. 19( a. 19/a ( ))			

1561 Figure D-84: Forescout Alert Details for the Stop Command Issued to the PLC

<) FORES	COUT. 🙆 Dashboard 🚠 Network	Events 🎝 Se	nsors 😋 Settings	🖵 🏓 🖉	admin 🗮
Alert details	Back Edit Delete Show	I - Assign to case	: Download   🛩		Help
Summary	^	Source host info	^	Alert details	^
Alert ID	169537	IP address	172.16.3.10 (Private IP)	Command: Stop controller	
Timestamp	Oct 13, 2020 13:46:10	Host name	fgs-47631ehh	Destination route: Module 2	
Sensor name	sensor-bundle-nocoe	Other host names	fgs-47631ehh.Jan.Jab	Court manne, rearrand terr condition accesse	
Detection engine	Industrial threat library (ITL)	Host MAC	40:A8:F0:3D:48:AE (HewlettP)		
ID and name	iti_ops_pdop_ethip_controller_stop - ETHIP controller	addresses	Last seen: Oct 13, 2020 12:52:01		
Description	stop commend Potentially dangerous ETHIP operation: the ETHIP master or an operator has requested a PLC to stop. This operation may be part of regular maintenance	Other observed MAC addresses	E490(6938)C2C3 (Rockwell) E490(6938)C2C2 (Rockwell) E490(6938)C2C1 (Rockwell) 7C0E/CE6738(33)C(sco)		
	but can also be used in a Denial of Service attack.	Role	EWS		
Severity	High High	Other roles	Windows workstation, Terminal server, Terminal		
Source MAC	40:A8:F0:3D:48:AE (HewlettP)		client, Master		
Destination MAC	E4:90:69:38:C2:C0 (Rockwell)	Vendor and model	Rocioveli		
Source IP	172.16.3.10 (fgs-47631ehh)		DCOM (TCP 135, 49155, 49159) DNS (TCP 53)		
Destination IP	172.16.2.102 (plc_tesim)		DNS (UDP 53, 5355)		
Source port	58324		ETHIP (TCP 44818)		
Destination port	44818		FailedConnection (TCP 23, 80, 139, 1332, 8000, 8443)		
Alerts / Alert details				Copyright (C) 2009-20	20 Forescout by 41.2)

1562 Figure D-85: Forescout Alert Details for the Configuration Download Command

TORESC	Network	evenes on set	isona Ca seconda		= adm
t details	Back Edit Delete Show	- Assign to case	Download   🛩		He
ummary	^	Source host info	^	Alert details	^
Vert ID	169543	IP address	172.16.3.10 (Private IP)	Command: Configuration download	-
limestamp	Oct 13, 2020 13:46:20	Host name	fgs-47631ehh	Destination rouse: Module 2 User name: EGS_47631EHE0.4dministrator	
iensor name	sensor-bundle-nccoe	Other host names	fgs-47631ehh.lan.lab	and the second second second second second	
Detection engine	Industrial threat library (ITL)	Host MAC	40:A8:F0:3D:48:AE (HewlettP)	Downloaded Items:	
D and name	itl_ops_pdop_ethip_download - ETHIP configuration	addresses	Last seen: Oct 13, 2020 12:52:01	Program:MainProgram	
Description	download command Potentially dangerous ETHIP operation: the ETHIP master or an operator has requested a PIC to initiate a configuration download. This operation	Other observed MAC addresses	E490:69.38.(2):C3 (Rockwell) E490:69.38.(2):C2 (Rockwell) E490:69.38.(2):C1 (Rockwell) 7C:0E:CE:67:86:83 (Cisco)	User Tasks: Task:MainTask I/O Maps: Mappic_time	
	may be part of regular maintenance but can also be	Role	EWS	Map:control_host_eip Map:enet	
Severity	used in a cyber attack.	Other roles	Windows workstation, Terminal server, Terminal client, Master	, emigrantes	
Source MAC	40:A8:F0:3D:48:AE (HewlettP)	Vendor and model	Rockwell		
Destination MAC	E4:90:69:38:C2:C0 (Rockwell)		DCOM (TCP 135, 49155, 49159)		
Source IP	172.16.3.10 (fgs-47631ehh)		DNS (TCP 53) DNS (LIDP 53, 5355)		
Destination IP	172.16.2.102 (pic_tesim)		ETHIP (TCP 44818)		
iource port	58324		ETHIP (UDP 44818) FailedConnection (TCP 23, 80, 139, 1332, 8000, 8443)		
Alart datally				Conversions (C) 2020-2021	Engarment In A 1

# 1563 D.8.3 Build 3

## 1564 D.8.3.1 Configuration

- **Behavior Anomaly Detection: Dragos** 1565 Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and 1566 • Control LAN. 1567 Remote Access: Cisco VPN 1568 1569 Configured to allow authorized VPN users to access to ConsoleWorks web interface. • User Authentication/User Authorization: ConsoleWorks 1570 Configured for accessing the CRS environment. 1571 • D.8.3.2 Test Results 1572
- 1573 In this build, a remote session to the CRS workstation is established to perform PLC file operations as
- shown in Figure D-86 and Figure D-87. Dragos is able to detect the PLC file modifications as shown in
   Figure D-88 with details shown in Figure D-89.

1576 Figure D-86: VPN Connection to the Manufacturing Environment



1577 Figure D-87: Remote Access is Being Established through ConsoleWorks



1578 Figure D-88: Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the

#### 1579 Beckhoff PLC

			ASSET NOTIFI	CATIONS		SYSTEM ALERTS			80,25		
	-	From 02/11/21,02:4	5 PM UTC 💼 To 02/12/	21,04:45 PM UTC @ RELO	GMG					Q, Search	
U Viev	Sever	: ID	Occurred At 1	Delection Quadrants	: Summary	Message	Detected By	C Asset IDs	Source IPv4	: Dest. IPvd	: Other IPv
VILY	0	108858	02/12/21, 03:25:43	Indicator	TR-2020-27 related indicator detected in the environment	6 logs matching on the TR 2020-27 Indicator 72 21 91.29 were seen in	Dragos IOCs. TR-2020-27	144, 102			72.21.91.29 .
VIEW		138857	02/12/21, 03:23:16	Change Detection	New Logic Applied To PLC via Beckhoff ADS	New Logic Applied To PLC via Beckhoff ADS	Beckhoff ADS Logic Charge	35, 15	192 168.0 20	192.168.0.30	
VIEW		138842	02/12/21, 02:49:51	Threat Behavior	Multiple Logons Detected	Multiple Logens Detected by admin, who quickly logged into at least 8	Authentication to Multiple Hosts				
VIC		138841	02/12/21, 02:49:52	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 3	Authentication to Multiple Hosts				
VIEW	1 2	138840	02/12/21, 02:49:59	Threat Behavior	Multiple Logons Detected	Multiple Lagens Detected by admin, who quickly logged into at least 8	Authentication to Multiple Hosts				
VIC	2	138839	02/12/21, 02.49.54	Threat Dehavior	Multiple Logons Detected	Multiple Logons Detected by admin, who quickly logged into at least 0	Authentication to Multiple Hosts				
VIEW	2	138838	62/12/21, 02:49:53	Threat Behavior	Multiple Logons Detected	Multiple Logens Detected by scienic, who quickly logged into at least 3	Authentication to Multiple Hosts				
VIEW		138837	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				
	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 8	Authentication to Multiple Hosts				
	2	138834	02/12/21, 02:50:02	Threat Behavior	Multiple Logons Detected	Multiple Logons Detected by edmin, 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 Logens Detected by admin, who quickly logged into at least 8	Authentication to Multiple Hosts				
		138832	02/12/21, 02.50:00	Threat Behavior	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 Logons Detected	Multiple Logens Detected by admin, who quickly logged into at least 8	Authentication to Multiple Hosts				

- New Logic Applied To PLC via Beckhoff ADS DETECTION INFORMATION ASSOCIATED ASSETS ID WHAT HAPPENED: New Logic Applied To 1 Туре Nam Engineering W 35 POLARIS VIEW ory PL OCCURRED AT: DETECTED BY: DETECTION QUAD SOURCE: ZONES: RELATED NOTIFICATIONS (0) ACTIVITY GROUP ICS ATT&CK TACTIC ID : ICS CYBER KILLCHAIN STEP ICS ATT&CK TECHNIQU QUERY-FOCUSED DATASETS: NOTIFICATION RECORD: NOTIFICATION COMPONENTS PLAYBOOKS CASES:
- 1580 Figure D-89: Dragos Alert Details for the PLC Logic File Download

# 1581 D.8.4 Build 4

- 1582 D.8.4.1 Configuration
- 1583 Behavior Anomaly Detection: Azure Defender for IoT
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.
- 1586 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.

# 1589 *D.8.4.2 Test Results*

- 1590 Figure D-90 and Figure D-91 show the connection to the CRS environment through the Dispel VDI. The
- 1591 changes to the PLC programs are detected by Azure Defender for IoT, as shown in <u>Figure D-92</u>, because
- 1592 the Dispel VDI is not an authorized programming device.

1593 Figure D-90: Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket

•3	Remote Desktop Connection				-	o ×
0	EPIER Command P	Prompt		- 🗆 X		^
Recycle Bin	TC3_AddRo Reply from 1 Reply from 1 Reply from 1 Reply from 1 Ping statist	10.100.1.7: bytes=32 time=184ms TTL=62 10.100.1.7: bytes=32 time=182ms TTL=62 10.100.1.7: bytes=32 time=181ms TTL=62 10.100.1.7: bytes=32 time=184ms TTL=62 tics for 10.100.1.7:		Ŷ		
Dispel	Packets:	Sent = 8, Received = 8, Lost = 0 (0% loss),				
e Google Chrome	Settings Help	Discel is running Disconnect	-			
	DISPEL					
OpenVPN	Available Projects	Available Entry Points	Available Exit Points		-	
GUI	NCCOE-Manufacturing	Chicago, IL (	Exit NCCOE (cutter)			
putty TC31-FULL GreenTec				Ľ		
GreenTec_D						
TC3_Remo						
<						×

1594 Figure D-91: Nested RDP Connections Showing Dispel Connection into the CRS Workstation



1595 Figure D-92: Azure Defender for IoT Alert for the Unauthorized PLC Programming

		11:36:08
Ļ	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. Source asset 10.100.1.61 performed programming on destination PLC asset 192.168.0.30.	11:36:01
	Programming chan more	
Devices		
Туре	Name	
	CX-17DB08	
	10.100.1.61	
	Filter events by related devices	
		11.36.01

# 1596 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.

1601 D.9.1 Build 1

1606

- 1602 D.9.1.1 Configuration
- 1603 Behavior Anomaly Detection: Tenable.ot
- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1605 File Integrity Checking: ForceField
  - PI Server is configured to use ForceField drive.

# 1607 *D.9.1.2 Test Results*

- 1608 Figure D-93 shows Tenable.ot detecting the remote access connections. Figure D-94 shows that
- 1609 GreenTec successfully blocks the attacker from deleting archive data.
- 1610 Figure D-93: Tenable.ot alert Showing SMB Connection from an External Workstation to the Historian

ents	All Ever	nts Se	arch	٩					Actions v Resolve All	Export
nfiguration Events			TIME	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD
ADA Events		19353	02:53:41 PM - Anr 14, 2021	Linauthorized Conversation	Low	SMB communication from Eng Station	PCS Eng. Station	172 16 3 10	LAN-AD02	10,100,0,13
ork Threats		19354	02:53:41 PM · Apr 14, 2021	Unauthorized Conversation	Low	Unauthorized SMB communication fro	PCS Eng. Station	172.16.3.10	LAN-AD02	10.100.0.13
ork Events		19351	02:51:30 PM · Apr 14, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19		HistorianDMZ	10.100.1.4
s		19352	02:51:23 PM · Apr 14, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19		HistorianDMZ	10.100.1.4
y		19350	02:50:32 PM · Apr 14, 2021	Unauthorized Conversation	Low	SMB communication from Eng Station	HMI	172.16.1.4	LAN-AD02	10.100.0.13
v		19349	02:44:46 PM · Apr 14, 2021	Unauthorized Conversation	Low	SMB communication from Eng Station	HMI	172.16.1.4		172.16.1.255
	4									
ts Settings	Items: 1-10 Event 193 Details	100 out of 1 353 02:5	7181 53:41 PM · Apr 14, 2021 Unau	thorized Conversation Low I	Not resolved				)< < Pag	e1 of 172 >
rttings	Items: 1-10 Event 193 Details Source	100 out of 1 353 02:5	7181 53:41 PM · Apr 14, 2021 Unau A conversation in an i	thorized Conversation Low I unauthorized protocol has been	Not resolved detected				K < Pag	e1 of 172 >
tings	Items 1-1 Event 193 Details Source Destinati	100 out of 1 353 02:5	7181 33:41 PM - Apr 14, 2021 Unau A conversation in an i source NAME	thorized Conversation Low I unauthorized protocol has been PCS Eng. Station	Not resolved	Why is this imp	portant?	Sugg	K < Page	e1 of 172 >
ttings	Items: 1-1 Event 193 Details Source Destinati Policy	100 out of 1 353 02:5	7181 53:41 PM - Apr 14, 2021 Unau A conversation in an I SOURCE NAME SOURCE ADDRESS	thorized Conversation Low I unauthorized protocol has been <u>PCS Eng. Station</u> 172.16.3.10	Not resolved	Why is this imp	portant?	Sugg	K < Pag	⊧1of172 > :
ttings	Items: 1-10 Event 193 Details Source Destinati Policy Status	100 out of 1 353 02:1	2181 3341 PM - Apr 14, 2021 Unau A conversation in an in Source NAME SOURCE NAME DESTINUTION NAME	thorized Conversation Low I unauthorized protocol has been PCS.ExeStation 172.16.3.10 LAN.AD02	Not resolved	Why is this imp conversations may indicate a are no despect	portant? In unauthorized protoc uspicious traffic. Some d to communicate in r	ols Che assets it is ion- con	K < Page ested Mitigation ckif this communication is s expected fraffic, then adjust	e 1 of 172 > > >
ettings	Event 192 Details Source Destinati Policy Status	100 out of 1 353 02:	A conversation in an in Source NAME Source NAME Source Address DESTINATION NAME DESTINATION ADDRESS	thorized Conversation Low I unauthorized protocol has been PCS Ene. Station 172.16.3.10 LAN.4002 10.100.0.13	Not resolved	Why is this imp conversitions are no expect standard proto the standard proto the standard proto	portant? In unauthorized protoc uspicious traffic. Some do communicate in r scols and any deviation rotocols may suggest a	cols Che assets It is ion- con from for this	K < Page ested Mitigation cki fi this communication is sepected traffic, then adjust similar communications in the spe- ormmunication is not expe-	et of 172 > > > > > > > > > > > > > > > > > > >
s ettings	Event 193 Details Source Destinati Policy Status	100 out of 1	A conversation in an in Source NAME Source NAME Source NAME Source NAME Source NAME Source NAME SOurce NAME DESTINATION NAME DESTINATION ADDRESS PHOTOCOL	thorized Conversation Low I unauthorized protocol has been PCS Ene. Station 172.16.3.10 LAN.AD02 10.100.0.13 SMB (tcp/445)	Not resolved	Why is this imp Convertations are no expect standard proto the standard pro- potential three protocols are u	portant? In unauthorized protoco gosfious traffic. Some ed to communicate in support social and any deviation rotocols may sugget a unaverse to ken but he new misecure and should he new	Sugg sols Che assets It is son- con from for for this the the sources of the sources of the the sources of the the sources of the the sources of the sources of the the sources of the sources of the the sources of the sources of the sources of the the sources of the sources of the sources of the the sources of the sources of the sources of the sources of the the sources of the sources of the sources of the sources of the the sources of the sources of the sources of the sources of the sources of the the sources of the sources of the sources of the sources of the sources of the the sources of the sourc	K < Pag ested Mitigation ckif this communication is s expected traffic, then adjust similar communications in the source asset to determine source asset to determine is communication is not expe	et of 172 > > > > > > > > > > > > > > > > > > >
s ettings	Items: 1-10 Event 193 Details Source Destinati Policy Status	100 out of 1	7181 33:41 PM - Apr 14, 2021 Unaux A conversation in an un Source NAME SOURCE NAME DESTINATION ADDRESS PHOTOCOL PORT	thorized Conversation Low I unauthorized protocol has been PCS Ene. Station 172.16.3.10 LANADO2 10.100.0.13 SMB (rcp/445) 445	Not resolved	Why is this imp Conversations may incorpect standard protocols the standard p potential three protocols are u used at all, no end assess see	portant? In unauthorized protor uspicious traffic. Some de to communicate in it coloradis may deviation unsecure and should in drafer to keep the networ ure.	Sugg cols Che assets It is non- con from for from for this the t be sou crk if th con assi	K < Page ested Mitigation of the communication is constructed raffic, then adjust similar communications in the source asset to determine we source asset to determine we communication is not expe- source asset to determine we asset to determi	expected. If the Policy generated refuture. If ted, check whether the spromised. rected, various
1611 Figure D-94: GreenTec Denies Modification and Deletion File Operations in the Protected Drive

2	Kali Linux on LANVH - Virtual Machine Connection			- 0 X
File Action Media Clipboard View Help				
(2) (0) (0) (0) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1				
	reeRDP: 10 🗉 administrato 🗈 administrato 🖻 administrato 🔳	Arc Files - Fi 03:4	орм 🗖 🜒 🎝 (	<b>0   ≙</b> G
	administrator@kali: ~/Documents/Arc Files			_ <b>–</b> ×
File Actions			Volume 100%	
File Actions	FreeRDP:10.100.1.4			- ×
[15:33:38:433] 🚽   🖓 📑 🖛   ForceField			-	o ×
[15:33:38:433] File Home Share	View			~ 0
[15:33:38:433 ← → ~ ↑ 📮 > Netwo	rk > 10.100.1.7 > ForceField	v Ö	Search ForceField	Q
[15:33:38:433]	A		Laure II	
[15:33:38:433]  Quick access	Name	×	Size	
[15:33:38:433]	2020-10-08_11	C File	1,256 KB	
[15:33:38:433]	2020-10-08_11 You need permission to perform this action	C File	65,536 KB	
[15:33:38:434]	2020-10-08_11	C File	1,256 KB	
[15:33:38:434] Documents #	2020-10-08_11 ForceField	C File	57,344 KB	
[15:33:38:434] Pictures #	2020-10-08_11	C File	8,192 KB	
[15:33:38:434] This PC	2020-10-08_11 Try Again Canc	C File	1,256 KB	
[15:33:38:434]	2020-10-08_11	C File	50,176 KB	
[15:33:38:434	2020-10-08_11	C File	15,360 KB	
[15:33:38:434]	2020-10-09_09 (V) More details	C File	1,256 KB	
[15:33:38:434]	2020-10-09_09T0V0_FT*DIVIZ_2020*00*21_17*22*13*1.arc 10/3/2020 3/0	FRIM ANC 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] Music	2020-10-09_091018_PI-DMZ_2020-08-26_17-22-15#1.arc 10/9/2020 9:12	2 AM ARC File	1,256 KB	
[15:33:38:434] E 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 Videos	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] Local Disk (C:)	2020-10-09_091039_PI-DMZ_2020-08-26_17-22-15#1.arc 10/9/2020 9:11	AM ARC File	1,256 KB	
[15:33:38:434]	2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#1.arc 10/9/2020 9:13	AM ARC File	19,456 KB	
[15:33:38:434 Archives (F)	2020-10-09_091040_PI-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:1:	AM ARC File	46,080 KB	
[15:33:38:434]	2020-10-10_131000_PI-DMZ_020-06-20_17-22-13#1.arc 10/10/20201:	IS PM ARC FILE	1,230 KB	
[15:33:38:434]	2020-10-10_131001_PI-DMZ_2020-06-27_17-22-13#1.arc 10/10/20201:	IS DMA ARC FILE	20,400 KD	
[15:33:38:535	2020-10-10_131001_P1-DMZ_2020-00-21_17-22-13#2.8fc 10/10/2020101	O DM ARC FILE	40,000 KD	
[15:33:38:535] 🛃 Network	2020_10_16_131017_DLDM7_2020_08_27_17_22_15#1 arc     10/16/2020_1:     10/16/2020_1:     10/16/2020_1:     10/16/2020_1:     10/16/2020_1:	O DM ARC File	20.480 KB	
15:33:38:618	2020-10-16 131017 PI-DMZ 2020-08-27 17-22-15#2 arc 10/16/2020 1-	9 PM ARC File	45.056 KB	
[15:33:38:661]	2020-10-16 131026 PI-DMZ 2020-08-26 17-22-15#1.arc 10/16/2020 1::	M 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 1:5	4 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 1:5	4 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 1:4	19 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 1:4	19 PM ARC File	20,480 KB	
[15:33:39:490 [15:33:39:490] 74 terms				Rea
[15:33:39:749]			2.40	DM
			^ 문 4 11/12/	/2020
Status: Running				88

# 1612 D.9.2 Build 2

1615

- 1613 D.9.2.1 Configuration
- 1614 Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1616 File Integrity Checking: ForceField
- PI Server is configured to use ForceField drive.

# 1618 *D.9.2.2 Test Results*

- 1619 Forescout detects the remote session as shown in Figure D-95. When the user attempts to alter a file on
- 1620 the protected drive, GreenTec denies the operation as shown in Figure D-96.

- 1621 Figure D-95: Forescout Alert Showing Network Connection from the Corporate Network to the
- 1622 Historian



1623 Figure D-96: GreenTec Denies Modification and Deletion File Operations in the Protected Drive

12	Kali Linux on LANVH - Virtual Machine Connection	_ <b>D</b> X
File Action Media Clipboard View Help		
2100000111 B 3 5 8		
	reeRDP: 10 🗈 administrato 🗈 administrato 🗈 administrato 🖿 Arc Files - Fi	. 03:40 PM 🗖 🜒 🏘 💿 🔒 🚱
	administrator@kali:~/Documents/Arc Files	_ = = ×
File Ashers		Volume 100%
File Actions	FreeRDP:10.100.1.4	_ ×
[15:33:38:433] 💂   🖓 🦲 🖛   ForceField		– <b>o</b> ×
[15:33:38:433] File Home Share	View	× 0
[15:33:38:433 4 > x A > x	rk > 10.100.1.7 > EorceEield	u B Cauch Encolined 0
[15:33:38:433]		V O Search Porcerieid p
[15:33:38:433]	Name Destination Folder Accers Denied - X	Size ^
[15:33:38:433] Quick access	2020-10-08 11	1.256 KB
[15:33:38:433] Desktop #	2020-10-08 11 You need permission to perform this action	65.536 KB
[15:33:38:434] University Downloads	2020-10-08 11 C File	1.256 KB
[15:33:38:434] 🗄 Documents 🖋	2020-10-08 11 ForceField C File	57,344 KB
[15:33:38:434] 📰 Pictures 📌	2020-10-08_11 CFile	8,192 KB
[15:33:38:434]	2020-10-08_11	1,256 KB
[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]	2020-10-09_09 🔗 More details C File	1,256 KB
[15:33:38:434 - Downloads	2020-10-09_09 1000_F1*DIVIZ_2020*00*21_17*22*13*1.arc 10/57 2020 5:05 AlVI AIC 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]	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-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]	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:)	2020-10-09_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] Archives (F:)	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]	2020-10-16_131016_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:59 PM ARC File	1,256 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	20,480 KB
[15:33:38:660]	2020-10-16_131017_PI-DMZ_2020-08-27_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_2020-08-26_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#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 74 items		
[15:33:39:749] [] H D []		∧ 臣 d <sub>8</sub> 3:40 PM 11/12/2020
Status: Running		≡ 8≗.

# 1624 D.9.3 Build 3

- 1625 D.9.3.1 Configuration
- 1626 Behavior Anomaly Detection: Dragos
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.
- 1629 File Integrity Checking: ForceField
- 1630 PI Server is configured to use ForceField drive.

# 1631 *D.9.3.2 Test Results*

- 1632 Dragos detects the remote session as shown in <u>Figure D-97</u>. When the user attempts to alter a file on
- 1633 the protected drive, GreenTec denies the operation as shown in Figure D-98.

1634	Figure D-97: Dragos Detection of RI	P Session from an Externa	l Network to the Historian
------	-------------------------------------	---------------------------	----------------------------

DETECTION INFORMATION		ASSOCIATED ASSETS
WHAT HAPPENED: THE ROP Negotiation Request		View         Type         ID         Name         C         D           VIEW         Image: Non-Service Statest 85         10.100.1.4         C         D         10.100.1.4         C         D
CCCURRENT: COUNT: COUN	LAT SEA LAT	NEE     Asset 84     I       COMMUNICATIONS SUMMARY       COMMUNICATIONS SUMMARY       Communication of the second conserver Microsoft Conserver in 5 100 1.4       Protect 1       Cleart 2       Server 2       Server Parts 2       TX Bytes       NO Protect 1       Cleart 2       Server 2       Server Parts 2       TX Bytes       Server 2       Serv
ID © Docurred At ©		Summary
		The Holded NordColors

1635 Figure D-98: GreenTec Denies Modification and Deletion File Operations in the Protected Drive

2	Kali Linux on LANVH - Virtual Machine Connection		-	D X
File Action Media Clipboard View Help				
2 0 0 0 0 1 b 5 5 5				_
	eeRDP: 10 🗉 administrato 🗈 administrato 🗈 administrato 💼 Arc Fil	es - Fi 03:4	орм 🗆 🔹 🚱	) 🔒 G
	administrator@kali:~/Documents/Arc Files			_ = ×
File Actions			Volume 100%	
File Actions	FreeRDP:10.100.1.4			_ ×
[15:33:38:433] .			-	
[15:33:38:433 File Home Share	View			~ <b>0</b>
[15:33:38:433 ← → ~ ↑ 📮 > Networ	x > 10.100.1.7 > ForceField	~ Õ	Search ForceField	م
[15:33:38:433			Leave 1	
[15:33:38:433]  Quick access	Name Sestination Folder Access Denied -	< <sup>ie</sup>	Size	<u> </u>
[15:33:38:433]	2020-10-08_11	C File	1,256 KB	
[15:33:38:433]	2020-10-08_11 You need permission to perform this action	C File	65,536 KB	
[15:33:38:434]	2020-10-08_11	C File	1,256 KB	
[15:33:38:434] Documents #	2020-10-08_11 ForceField	C File	57,344 KB	
[15:33:38:434] E Pictures #	2020-10-08_11	C File	8,192 KB	
[15:33:38:434] Inis PC	2020-10-08_11 Try Again Cancel	C File	1,256 KB	
[15:33:38:434]	2020-10-08_11	C File	50,176 KB	
[15:33:38:434] A Documents	2020-10-08_11	C File	15,360 KB	
[15:33:38:434]	2020-10-09_09 More details	C File	1,256 KB	
[15:33:38:434]	2020-10-09_091000_P1*DWIZ_2020*00*21_17*22*13*1:arc 10/5/2020 3:05 MIVI	HIC File	29,696 KB	
[15:33:38:434]	2020-10-09_091008_P1-DMZ_2020-08-27_17-22-15#2.arc 10/9/2020 9:09 AM	ARC File	30,840 KB	
[15:33:38:434] Music	2020-10-09_091018_PT-DMZ_2020-08-25_17-22-15#1.arc 10/9/2020 9:12 AM	ARC FILE	1,230 KB	
[15:33:38:434] E Pictures	2020-10-09_091018_PT-DMZ_2020-08-27_17-22-13+1.arc 10/9/2020 9:12 AM	ARC File	30,720 KB	
[15:33:38:434] Videos	2020-10-09_091010_PF-DM2_2020-06-27_17-22-13#2.arc 10/9/2020 912 AM	ARC File	1 255 KB	
[15:33:38:434 Local Disk (C:)	2020-10-09_091040_PL-DM7_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:)	2020-10-09_091040_PI-DIM2_2020-08-27_17-22-15#2 arc 10/9/2020_9-15_AM	ARC File	46 080 KB	
[15:33:38:434 Archives (F:)	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 (Ht)	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]	2020-10-16_131016_PI-DMZ_2020-08-26_17-22-15#1.arc 10/16/2020 1:59 PM	ARC File	1,256 KB	
L15:33:38:535	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	
[15:33:38:660]	2020-10-16_131017_PI-DMZ_2020-08-27_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_2020-08-26_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]	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 74 items				
			^ 11/12/2	M 🖵
Status: Running				<u>۵</u> 8 <u>4</u>

# 1636 D.9.4 Build 4

## 1637 D.9.4.1 Configuration

- 1638 Behavior Anomaly Detection: Azure Defender for IoT
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.
- 1641 File Integrity Checking: ForceField
- PI Server is configured to use ForceField drive.

# 1643 *D.9.4.2 Test Results*

1644 The connection to the Historian data storage was detected by Azure Defender for IoT as shown in Figure 1645 D-99. Figure D-100 shows a Windows error message after attempting to overwrite protected Historian

- 1646 files.
- 1647 Figure D-99: Azure Defender for IoT Event Timeline Showing the Remote Access Connection to the
- 1648 Historian



1649 Figure D-100: GreenTec Denies Modification and Deletion File Operations in the Protected Drive

		FreeRDP: 10.100.1.4 🗈 administrate	or@kali: ~/P 📧 ad	ministrator@l	rali: ~/P 02:59 P	M 🗆 🜒 🛕	 ۵
	down and show the	FreeRDP:10.100.1.4				_ ×	
nimize au open win	dows and show the	desktop			-		
Properties (Alt+Enter	)					~ 👩	
Show the properties	for the 0.1.7 >	ForceField		5	Search ForceField	P	
selected item.			Q				
Ouick access	Name	The State of Contract of Contr		×	Size		
Desisters	2021-01-05_0	03		C File	65,536 KB		
Desktop	2021-01-05_0	You need permission to perform this action		C File	65,536 KB		
- Downloads	2021-01-05_0	D3		C File	1,256 KB		
Documents	# 2021-01-04_0	D3 ForceField		C File	65,536 KB		
Pictures	# 2021-01-04_0	03		C File	65,536 KB		
Arc Files	# [] 2021-01-04_0	D3 Try Age	in Cancel	C File	1,256 KB		
ForceField	2021-01-03_0	03		C File	65,536 KB		
This PC	2021-01-03_0	03		C File	65,536 KB		
Dedter	2021-01-03_0	03 (  More details		C File	1,256 KB		
Desktop	2021-01-02_0	030024_F1-01012_2020-12-05_17-55-41=1.alc	1/E/E021 3.30 HIV		65,536 KB		
Documents	2021-01-02_0	033006_PI-DMZ_2020-08-27_17-22-15#1.arc	1/2/2021 3:30 AM	ARC File	65,536 KB		
Downloads	2021-01-02_0	033005_PI-DMZ_2020-08-26_17-22-15#1.arc	1/2/2021 3:30 AM	ARC File	1,256 KB		
🛫 home on kali	2021-01-01	033024_P1-DMZ_2020-12-09_17-33-41#1.arc	1/1/2021 3:30 AM	ARC FILE	03,330 KB		
Music	2021-01-01	033000_P1-DMZ_2020-00-27_17-22-13#1.arc	1/1/2021 3:30 AM	ARC FILE	1.256 V.D		
Pictures	2020-07-01	022024 PL DMZ_2020-00-20_17-22-13#1.arc	12/21/2021 3:30 AM	ARC File	1,230 KD		
Videos	2020-12-31	033006 PLDMZ 2020-12-09_17-33-41#1.arc	12/31/2020 3:30 AM	ARC File	65 536 KB		
Local Disk (C:)	2020-12-31	033005 PI-DM7 2020-08-26 17-22-15#1 arc	12/31/2020 3:30 AM	ARC File	1 256 KB		
- PI Server (E:)	2020-12-30	033024 PI-DMZ 2020-12-09 17-55-41#1.arc	12/30/2020 3:30 AM	ARC File	65 536 KB		
- Archives (E)	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		
Output (C)	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		
uueues (0:)	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_0	033006_PI-DMZ_2020-08-27_17-22-15#1.arc	12/29/2020 3:30 AM	ARC File	65,536 KB		
i 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_0	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_0	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_0	033024_PI-DMZ_2020-12-09_17-55-41#1.arc	12/27/2020 3:30 AM	ARC File	65,536 KB	~	
9 items							
	<b>A</b>				A €7 da 3:00 P	M	
					· → · · · · · · · · · · · · · · · · · ·	021	

# 1650 D.10 Executing Scenario 10: Detect Sensor Data Manipulation

1651 A sensor in the manufacturing system sends out-of-range data values to the Historian. The expected 1652 result is the behavioral anomaly detection (data historian) capability alerts on out-of-range data.

1653 D.10.1 All Builds

1656

1657

- 1654 *D.10.1.1 Configuration*
- 1655 Behavior Anomaly Detection: PI Server
  - Configured to receive process data from across the manufacturing system.
    - Configured to perform analysis on incoming data points.

# 1658 *D.10.1.2 Test Results*

1659 The Historian process monitoring capabilities provided by the PI System are able to monitor out-of-1660 range sensor readings and generate alerts. Figure D-101 shows the PI Server's event frame alerts on the 1661 out-of-range reactor pressure readings in the PCS.

- 1662 Figure D-101: PI Server's Event Frames Showing Out-of-Range Sensor Readings for the Reactor
- 1663 Pressure



# 1664 D.11 Executing Scenario 11: Detect Unauthorized Firmware Modification

1665 An authorized user accesses the system remotely and performs an unauthorized change of the firmware 1666 on a PLC. The expected result is the behavioral anomaly detection tools will alert on the new firmware.

1667 The behavior anomaly detection tools can detect changes to the firmware. Firmware change detection 1668 needs to be correlated with the maintenance management system to determine if the firmware change 1669 was authorized and approved. This was not demonstrated as part of this scenario.

- 1670 D.11.1 Build 1
- 1671 *D.11.1.1 Configuration*
- 1672 Behavior Anomaly Detection: Tenable.ot
- 1673

1675

- Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1674 Remote Access: Cisco VPN
  - Configured to allow authorized VPN users access to ConsoleWorks web interface.

- 1676 User Authentication/User Authorization: ConsoleWorks
- Configured for accessing the PCS environment.

## 1678 *D.11.1.2 Test Results*

1679 Figure D-102 depicts the list of the events detected by Tenable.ot resulting from the firmware change.

- 1680 The details of one of the alerts are shown in Figure D-103
- 1681 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											Descent Property Second Pro-
All Events	Configuration	Events Search	٩								Actions V Resolve All Export Q
Configuration Events	LOG 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	Charge in controller firmwar	Comm. Adapter #1				Unknown	4 H
Network Threats	12434	02:26:41 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 (tcp)	10
Network Events	12433	02:25:49 PM · Feb 4, 2021	Rockwell Firmwar	High	Rockwell Firmware Download	PCS Eng. Station	172.16.3.10	Corern, Adapter #1	172.16.2.102	CIIP (ttcp)	
9 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	CIIP (ttcp)	
✓ ቇ Inventory	12425	02:06:50 PM - Feb 4, 2021	Rockwell Module	Low	Rockwell Module Restart	PCS Eng. Station	172.16.3.10	Time Module	172.16.2.102	CIIP (ttep)	
Controllers	12423	02:03:55 PM · Feb 4, 2021	Rockwell Tag Dele	Low	Rockwell Delete Tax	PCS Eng. Station	172,16.3.10	olt tesim	172.16.2.102	CIIP (ttcp)	
Network Addeds	12422	02:03:55 PM · Feb 4, 2021	Rockwell Tag Cre	Low	Rockwell Create Tag	PCS Eng. Station	172.16.3.10	pic tesim	172.16.2.102	CIIP (tcp)	
P ∎ ROSK	12421	02:02:47 PM · Feb 4, 2021	Change in State	Medium	Change in controller state	olc tesim				Unknown	
> A Network	12416	01:47:47 PM · Feb 4, 2021	Change in Key Sw	High	Change in controller key state	plc tesim				CIIP (tcp)	
5 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 (tcp)	
M Reports	12413	01:46:30 PM - Feb 4, 2021	Rockwell Code Do	Medium	Rockwell Code Download	PCS Eng. Station	172.16.3.10	plc tesire	172.16.2.102	CIIP (ttcp)	
> g cocal secongs	12412	01:46:27 PM - Feb 4, 2021	Rockwell PLC Stop	High	Rockwell PLC Stop	PCS Eng. Station	172.16.3.10	plc tesm	172.16.2.102	CIIP (ttcp)	
	12410	01:45:05 PM · Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CliP (tcp)	
	12408	01:42:21 PM · Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	olc tesim	172.16.2.102	CIIP (ttcp)	
	12406	01:41:28 PM · Feb 4, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	pic tesim	172.16.2.102	CIP (tcp)	
	9133	04:33:00 PM · Jan 29, 2021	Rockwell Go Online	Low	Rockwell Online Session	PCS Eng. Station	172.16.3.10	plc tesim	172.16.2.102	CIP (tcp)	
	9121	04:02:47 PM · Jan 29, 2021	Change in Key Sw	High	Change in controller key state	plc tesim				CIIP (tcp)	
	9120	04:02:47 PM - Jan 29, 2021	Change in State	Medium	Charge in controller state	plo_tesim				Unknown	
	91.15	03:47:47 PM · Jan 29, 2021	Change in Key Sw	High	Charge in controller key state	plc tesm				CIP (ttp)	
	9114	08:47:47 PM · Jan 29, 2021	Change in State	Medium	Charge in controller state	alc tesim				Unknown	
	9110	03:38:51 PM · Jan 29, 2021	Rockwell Code Up	Low	Rockwell Code Upload	PCS Eng. Station	172.16.3.10	olc tesim	172,16.2.102	CIP (tcp)	
	Items: 1-25 out of 25										K < Page 1 of 1 -> ->
	Event 12436 02:28	:03 PM · Feb 4, 2021 Chang	e in Firmware Version	High No	t resolved						
	Details	7.6 1 1 1 1 1 1		17							
	Affected Assets	A change in the firmw	are version was detec	ied							
	Policy	SOURCE NAME	Comm. Adapte	n. 91				Why is this is	noortant?		Suggested Millipation
	Status	SOURCEADDRESS	172.16.2.102	172.16.4.102				why is unsit	riportaina		augentee minganen
			6.171.55					A change in t	the firmware version	was detected. Such a change can h obvisical access to the device.	1) Check if the change was made as part of scheduled work.
		BACKPLANE NAME	Backplane #1					an attacker i	nav use firmware ch	enter to alter the functionality of	<ol> <li>If this was not part of a planned operation, check if the network behavior of the asserbas channed.</li> </ol>
		OLD FIRMWARE VERSION	10.007					the asset. In:	sert backdoors or dis	rupt normal operations.	outsetter, of any source international
		NEW FIEMWARE VERSION	10.010								

1682 Figure D-103: Details for One of the Alerts Showing the Firmware Change

Event 12436 02:28:03 PM - Feb 4, 2021 Change in Firmware Version High Not resolved									
Details Affected Assets	A change in the firmware ver	rsion 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 alter the functionality of the asset, insert backdoors or disrupt normal operations.	behavior of the asset has changed.					
	NEW FIRMWARE VERSION	10.010							

# 1683 D.11.2 Build 2

1686

- 1684 D.11.2.1 Configuration
- 1685 Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1687 Remote Access, User Authentication/User Authorization: Dispel

1688 1689  Dispel VDI is configured to allow authorized users to access the PCS environment through the Dispel Enclave to the Dispel Wicket.

## 1690 *D.11.2.2 Test Results*

- 1691 Figure D-104 shows the activities detected by Forescout as a result of firmware change. Figure D-104,
- 1692 Figure D-105 and Figure D-106 show more details on the alerts associated with the firmware update.
- 1693 Figure D-104: Forescout Detects a Collection of Alerts Associated with the Firmware Change



1694 Figure D-105: Alert Details Detected by Forescout for the Firmware Change

<) FORESCOU	T. 🙆 Dashboard 🌲 Network 🔳 Events 🔊	Sensors 😋 Settings				🖵 🧶 🍃	admin
Alert details	Back Edit Delete Show   Y Assign to a	ase Download   ~					Help
Alert details Summary Alert ID Timestamp Sensor name Detection engine ID and name Description Security	Back     Edit     Delete     Show   ~     Assign to a state of the st	ase Download   v Source host info IP address Host name Other host names Host MAC addresses Other observed MAC addresses Reie	172.163.10 (Private IP) (gs.47031eth fgs.47031eth 40.88703.0882 (VelvetterP) Lastress Cord 23, 2020.103540 E4000308.CC2 (ResidentII) E4000308.CC2 (ResidentII) E4000308.CC2 (ResidentII) E4000308.CC2 (ResidentII) E4000308.CC2 (ResidentII) E4000308.CC2 (ResidentII) E400038.CC2 (ResidentIII) E40	•	Alert details Connance Formers update Destantion noues Models 4 User name (52-74311849/Administrator Updated firmware revision: 3.4		<ul> <li>✔ Help</li> <li>▲</li> </ul>
Severity	HILD High	Other roles	Windows workstation, Terminal server, Terminal client, Master				
Source MAC	40:AB:P0:3D:48:AE (HewlettP)	Vendor and model	Rackwell				
Destination MAC Source (P Destination (P Source port Destination (P) L2 proto L2 proto L4 pro	Ex10905484C2CD (Procovere) T272:16.3:0 (gr-strain) 50753 44918 Ethernet: IP TCP ETHP Not analyzed Address VAN IDs	Client protocols	DCGM (TCP 13), 54/153, 54/153, DMS (DDF 31, 3353) DMS (DDF 31, 3353) ETH4P (TC 24401) ETH4P (TC 24401) ETH4P (TC 24401) ATTD (TC 2400, 3530) MTP (LOP 240), MTP (LOP 240), MTP (LOP 120) MTP (LOP 120) MTP (LOP 120) MTP (LOP 120) MSB (DCP 130) SSDP (UCP 130) SSDP				
Name	Address VLAN IDs		NMC (TCD 6195)				

#### 1695 Figure D-106: ICS Patrol Scan Results Showing a Change Configuration was Made

Scan	details						×
Scan	ID	15		Started on	Oct 15, 2020 11:14:28		
Scan	type	Ether	Net/IP	Duration	01m37s		
Scan	targets	172.1	6.2.102	Scan status	📀 Completed		
Scan	ning sensors	PCS_	Sensor	Scanned IPs	1		
Scan	policy			Responding hosts	1		
Initia	ted by	Admi	n User	Updated hosts	1		
0	items selected					¥	c
	Target IP 🔺		Scanning sensor	Scan status	Host status		
		0	PCS_Sensor 🗸	(Not set)	(Not set)		
	172.16.2.102		PCS_Sensor	📀 Completed	Updated		
1 to 1	l items of 1						
Result	lt t is not available.						

# 1696 D.11.3 Build 3

- 1697 *D.11.3.1 Configuration*
- 1698 Remote Access: Cisco VPN
- Configured to allow authorized VPN users to access only the ConsoleWorks web interface.
- 1700 User Authentication/User Authorization: ConsoleWorks
- Configured to allow remote access to hosts in manufacturing environment.
- 1702 Behavior Anomaly Detection: Dragos
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and
   Control LAN.

## 1705 *D.11.3.2 Test Results*

- 1706 Dragos detects the change to the firmware as shown on the dashboard in Figure D-107 with details
- 1707 shown in Figure D-108.



1708 Figure D-107: Dragos Dashboard Showing an Alert for Firmware Change

## 1709 Figure D-108: Details for Firmware Change Alert

DETECTION INFORMATION		ASSOCIATED ASSETS		c
WHAT HAPPENED: (021.6) released Teppelies by Station 2 on Accel 2125		View T Type T 10 T Name	: Die :	0
OCCUBRED AT: 04/29/21.12/14/070	LAST BED: 04/29/21, 15:14:000			
COUNT:	STATE: URESOURD	COMMUNICATIONS SUMMARY		0
DETECTED BY: Osion Event-rane Notification DFD	SOURCE: IN Type Land			
DETECTION QUAD: Modeling	ZONES: URB Level1	- No bomina i catoli o soni ma p		
ACTIVITY GROUP:	ICS CYBER KILLCHAIN STEP:			
MITEL ATTACK TACTIC: , Formate Code Execution	MTRE ATTACK TECHNIQUE:			
QUERY FOCUSED DATAGETS:	NOTIFICATION RECORD:			
PLATEOCKE: No Associated Phytopics	NOTIFICATION COMPONENTS: No Associated Components			
CASES: AN COSES CAREO				0
RELATED NOTIFICATIONS		fermov		
				TECTER
		No Rotato Notificaters.		
	private bit of policy	10	FIRST PREVIOUS NEET 1181	

# 1710 D.11.4 Build 4

# 1711 D.11.4.1 Configuration

1712	•	Behavior Anomaly Detection: Azure Defender for IoT
1713 1714		<ul> <li>Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN</li> </ul>
1715	•	Remote Access, User Authentication/User Authorization: Dispel
1716 1717		• Dispel VDI is configured as the engineering workstation to connect through the Dispel Enclave to the Dispel Wicket to manage the Beckhoff PLC.

# 1718 *D.11.4.2 Test Results*

- 1719 Azure Defender for IoT alerts on the firmware update as shown below in Figure D-109.
- 1720 Figure D-109: Azure Defender for IoT Alert Showing a Version Mismatch in the Firmware Build

Microsoft		Alerts			e
		Free Search Q Adv		📋 🗈 🖡 🗶 Main View + 🛛 Export All	Alerts
			Version Build Mismatch		
		Important Alerts (72)	The PLC Version Build was not the expected result		
		POLICY Unauthorized Internet Co VIOLATION An asset defined in your intern		No Alerts	
Alerts (72)		POLICY Unauthorized Internet Co	•		
		POLICY Unauthorized Internet Co	Supervisory Eng PLC Wor	ngineering orkstation	
		VIOLATION An asset defined in your laters			
		VIOLATION An ausert defined in your intern	Manage this Event		
		POLICY Unauthorized Internet Co VIOLATION An asset defined in year intern	<ul> <li>This is a Horizon custom alert that provides information resolved by a required, contact your security administrator for more details.</li> </ul>	y a proprietary protocol plugin. If	
		POLICY Unauthorized Internet Co VIOLATION As asset defend in your intern			
		POLICY Unauthorized Internet Co		Acknowledge	10
		VIOLATION An easier defined in your interv		POLICY Version Build Mismatch	-
		VIOLATION As asset defined in your internal ne	book is communicating with addresses on the internet. These addresses have not been lea	VIOLATION The PLC Version Baild was not the expected result	00
		POLICY Unauthorized Internet Conne VIOLATION An exect defined in your internal ne	ectivity Detected   1 month ago work is communicating with addresses on the Internet. These addresses have not been les	OPERATIONAL Device is Suspected to be Disconnected (Unresponsive) Device 192.168.0.30 (s suspected to be disconnected (unresponsive) Jan 6.13.	58
		POLICY Unauthorized Internet Conne VIOLATION An exact defined in your internal ne	ectivity Detected   1 month ago have to communication with addresses on the Internet. These addresses have not then be	OPERATIONAL Suspicion of Unresponsive MODBUS Device Jan 6 13: Outstation device 192.168.8.30 (Protocol Address 255) secrets to be Unresponsive to MODBUS requests.	57
		POLICY Unauthorized Internet Conne	ectivity Detected (1 month ago	OPERATIONAL HTTP Client Error Jan 6 13:	21
		VIOLATION An esset defined in your internal ne	work is communicating with addresses on the interact. These addresses have not been lea	Policy Unauthorized Internet Connectivity Detected	
		VIOLATION An asset defined in your intensit ne	ectivity Detected   1 month ago twork to communicating with addresses on the Internet. These addresses have not been lea	VIOLATION An esset defined in your internal network is communicating with addresses on the Internet. These addresses but	10
		POLICY Unauthorized Internet Conne VIOLATION An asset defined in your internal no	ectivity Detected   1 month ago	OPERATIONAL Device is Suspected to be Disconnected (Unresponsive)     Jan 5 17:     Device 192.168.0.98 (a suspected to be disconnected (unresponsive).	26 .
	ø				
Azure Defender for Version 3.1.1	rloT				

# Appendix E Benefits of IoT Cybersecurity Capabilities

The National Institute of Standards and Technology's (NIST's) <u>Cybersecurity for the Internet of Things (IoT)</u> 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; 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 the **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 Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	<ul> <li>Ability to uniquely identify the IoT device logically.</li> <li>Ability to uniquely identify a remote IoT device.</li> <li>Ability for the device to support a unique device ID.</li> <li>Ability to configure IoT device access control policies using IoT device identity.</li> <li>Ability to verify the identity of an IoT 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 IoT device.</li> <li>Ability to create 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 establish organizationally defined user actions for accessing the IoT device and/or device interface.</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> </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 and critical system 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>	AC-2 IA-2 IA-4 IA-5 IA-8 IA-12
PR.AC-3: Remote access is managed.	<ul> <li>Ability to configure IoT device access control policies using IoT device identity.         <ul> <li>Ability for the IoT device to differentiate between authorized and unauthorized remote users.</li> </ul> </li> </ul>	N/A	AC-17 AC-19 AC-20

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>Ability to authenticate external users and systems.</li> <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 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, including:         <ul> <li>usage restrictions</li> <li>configuration requirements</li> <li>manufacturer established requirement</li> </ul> </li> <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> <li>Ability to control the IoT device's logical interface (e.g., locally or remotely).</li> <li>Ability to detect remote activation attempts.</li> </ul>		
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).         <ul> <li>Ability to establish user accounts to support role-based logical access privileges.</li> <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> </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 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>	AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24

Framework v1.1 Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	800-53
Subcategory		Rev. 5
<ul> <li>Ability to apply least privilege to user accounts.         <ul> <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 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> <li>Ability to reate organizationally defined accounts that support privileged roles with automated expiration conditions.</li> </ul> </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 restrict the use of shared/group accounts on the IoT device.</li> <li>Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on:</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 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> <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 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 enforce authorized access at the system level.</li> <li>Providing education and supporting materials explaining how to establish role 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> </ul>	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	<ul> <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 establish limits on authorized concurrent device sessions.</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> <li>Ability to revoke access to the IoT device.</li> </ul>	<ul> <li>Providing education and supporting materials for how to establish roles to support IoT device policies, procedures, and associated documentation.</li> </ul>	
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 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 authenticate external users and systems.</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 protected.	<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> <li>Ability to store encryption keys securely.</li> <li>Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.</li> <li>Ability to support data encryption and signing to prevent data from being altered in device storage.</li> <li>Ability to secure data stored locally on the device.</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 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> </ul>	SC-28 MP-2 MP-4 MP-5

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	<ul> <li>Ability to secure data stored in remote storage areas (e.g., cloud, server).</li> <li>Ability to utilize separate storage partitions for system and user data.</li> <li>Ability to protect the audit information through mechanisms such as:         <ul> <li>encryption</li> <li>digitally signing audit files</li> <li>securely sending audit files to another device</li> <li>other protections created by the device manufacturer</li> </ul> </li> </ul>		
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	<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> <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>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> <li>Providing 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>	SC-16 SI-7 MP-4 MP-5
PR.IP-4: Backups of information are conducted, maintained, and tested.	N/A	<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>	CP-4 CP-9

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities 800 Rev	ST SP 0-53 ev. 5
		<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> <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>	
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	N/A	<ul> <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 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 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> <li>Providing details necessary for IoT device customers to implement only organizationally approved IoT device diagnostic tools within their system.</li> <li>Providing the details and instructions to perform necessary IoT device maintenance activities.</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. If such comprehensive IoT device maintenance operations documentation describing maintenance operations documentation describing maintenance operations that the IoT device customer is required to perform. If such comprehensive IoT device maintenance operations documentation describing maintenance operations</li> </ul>	-2 -3 -5 -6

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		<ul> <li>clearly communicate to IoT device customers that the user must perform these operations themselves.</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 the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> <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> <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 loT 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> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <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 supporting entities, to follow.</li> </ul>	
		manufacturer to ask questions or obtain help related to the IoT device configuration settings.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities 800 Rev	ST SP 0-53 ev. 5
		<ul> <li>Providing information to allow for in-house support from within the IoT device customer organization.</li> <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> <li>Providing education for how to scan for critical software updates and patches.</li> <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>	
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	N/A	<ul> <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 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 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> <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 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> </ul>	-4

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established	N/A	<ul> <li>Providing the details necessary for maintaining records for nonlocal IoT device maintenance and diagnostic activities.</li> <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> <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 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> <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> </ul>	AC-4 CA-3 CM-2 SI-4
and managed.			
DE.AE-2: Detected events are analyzed to understand attack 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 collected and correlated 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 information can be checked to allow for review, analysis, and reporting).</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

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SF 800-53 Rev. 5
DE.CM-1: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	<ul> <li>Ability to keep an accurate internal system time.</li> <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> </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>	SI-4 AU-12 CA-7 CM-3 SC-7 SI-4
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	N/A	N/A	AC-2 AU-12 CA-7 CM-3 SC-5 SC-7 SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	<ul> <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 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 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>	AC-2 AU-12 AU-13 CA-7 CM-10 CM-11

# **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.

Table E-2 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 CSF 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.

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

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

Scenario ID and		
Description with	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
	<ul> <li>(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>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 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 heing launched.</li> </ul>
Scenario 2: Protect	<ul> <li>Ability to identify software loaded on the IoT</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement</li> </ul>
Host from Malware	device based on IoT device identity.	management and operational controls to protect data obtained from IoT devices and
via Network Vector:	<ul> <li>Ability to verify digital signatures.</li> </ul>	associated systems from unauthorized access, modification, and deletion.
This test will	<ul> <li>Ability to run hashing algorithms.</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement</li> </ul>
demonstrate the	<ul> <li>Ability to perform authenticated encryption</li> </ul>	management and operational controls to protect IoT device data integrity and
detection of	algorithms.	associated systems data integrity.
malware	<ul> <li>Ability to compute and compare hashes.</li> </ul>	<ul> <li>Providing IoT device customers with the details necessary to support secure</li> </ul>
introduction from	<ul> <li>Ability to utilize one or more capabilities to</li> </ul>	implementation of the IoT device and associated systems data integrity controls.
the network.	protect transmitted data from unauthorized	Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and housts use them. If there are used in the integrity
	access and modification.	controls built into the IoT device and now to use them. If there are no data integrity
	- Ability to valuate the integrity of data	customers the ways to achieve IoT device data integrity
DE AF-2	<ul> <li>Ability to verify software undates come from</li> </ul>	<ul> <li>Providing details for how to review and undate the IoT device and associated systems.</li> </ul>
DE.AE-3	valid sources by using an effective method	while preserving data integrity.
DE.CM-1	(e.g., digital signatures, checksums,	<ul> <li>Providing instructions and documentation describing the physical and logical access</li> </ul>
DE.CM-3	certificate validation).	capabilities necessary to the IoT device to perform each type of maintenance activity.
DE.CM-7	<ul> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>

Scenario ID and		
Description with	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> <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>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 drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul> <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 documented descriptions of the specific maintenance procedures for defined maintenance tasks.</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 device behavior indicators that could occur when an attack is being launched.</li> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device.</li> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring service of the manufacturer's supporting entity.</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 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 describing thetials necessary to identify unauthorized use of IoT device.</li> </ul>
Scenario 3: Protect	Ability to uniquely identify the IoT device	<ul> <li>Providing details for how to establish unique identification for each IoT device</li> </ul>
Host from Malware	logically.	associated with the system and critical system components within which it is used.
via Remote Access	<ul> <li>Ability to uniquely identify a remote IoT</li> </ul>	Providing communications and documentation detailing how to perform account
Connections:	device.	management activities, using the technical IoT device capabilities, or through
This test will	<ul> <li>Ability for the device to support a unique</li> </ul>	supporting systems and/or tools.
demonstrate	device ID.	Providing the details necessary to establish and implement unique identification for
blocking malware	<ul> <li>Ability to configure IoT device access control</li> </ul>	each IoT device associated with the system and critical system components within
attempting to infect	policies using IoT device identity.	which it is used.

Scenario ID and		
Description with	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
manufacturing	<ul> <li>Ability to verify the identity of an IoT device.</li> </ul>	<ul> <li>Providing the tools, assistance, instructions, and other types of information to</li> </ul>
system through	<ul> <li>Ability to add a unique physical identifier at</li> </ul>	support establishing a hierarchy of role-based privileges within the IoT device.
authorized remote	an external or internal location on the	<ul> <li>Providing details about the specific types of manufacturer's needs to access the IoT</li> </ul>
access connections.	device authorized entities can access.	device interfaces, such as for specific support, updates, ongoing maintenance, and
PR.AC-1	<ul> <li>Ability to set and change authentication</li> </ul>	other purposes.
PR.AC-3	configurations, policies, and limitations	<ul> <li>Providing education explaining how to control access to IoT devices implemented</li> </ul>
PR.AC-4	settings for the IoT device.	within IoT device customer information systems.
PR.AC-7	<ul> <li>Ability to revoke access to the device.</li> </ul>	<ul> <li>Providing education explaining how to enforce authorized access at the system level.</li> </ul>
PR.MA-1	<ul> <li>Ability to create unique IoT device user</li> </ul>	<ul> <li>Providing detailed instructions and guidance for establishing activities performed by</li> </ul>
PR.MA-2	accounts.	the IoT device that do not require identification or authentication.
DE.CM-3	<ul> <li>Ability to identify unique IoT device user</li> </ul>	<ul> <li>Providing documentation describing the specific IoT platforms used with the device to</li> </ul>
DE.CM-7	accounts.	support required IoT authentication control techniques.
	<ul> <li>Ability to create organizationally defined</li> </ul>	<ul> <li>Providing documentation with details describing external authentication by IoT</li> </ul>
	accounts that support privileged roles with	platforms and associated authentication methods that can be used with the IoT
	automated expiration conditions.	device.
	<ul> <li>Ability to configure IoT device access control</li> </ul>	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT</li> </ul>
	policies using IoT device identity.	device diagnostics activities.
	<ul> <li>Ability to authenticate external users and</li> </ul>	<ul> <li>Providing the details and instructions to perform necessary IoT device maintenance</li> </ul>
	systems.	activities and repairs.
	<ul> <li>Ability to securely interact with authorized</li> </ul>	<ul> <li>Providing details about the types of, and situations that trigger, local and/or remote</li> </ul>
	external, third-party systems.	maintenance activities required once the device is purchased and deployed in the
	<ul> <li>Ability to identify when an external system</li> </ul>	organization's digital ecosystem or within an individual consumer's home.
	meets the required security requirements	<ul> <li>Providing documented descriptions of the specific maintenance procedures for</li> </ul>
	for a connection.	defined maintenance tasks.
	<ul> <li>Ability to establish secure communications</li> </ul>	Providing appropriate tools, assistance, instructions, or other details describing the
	with internal systems when the device is	capabilities for monitoring the IoT device and/or for the IoT device customer to
	operating on external networks.	report actions to the monitoring service of the manufacturer's supporting entity.
	<ul> <li>Ability to establish requirements for remote</li> </ul>	<ul> <li>Providing the details necessary to monitor io i devices and associated systems.</li> <li>Description description describing details necessary to identify any statistic description.</li> </ul>
	access to the IOT device and/or IOT device	<ul> <li>Providing documentation describing details necessary to identify unauthorized use of Int devices and their associated systems.</li> </ul>
	Interface.	Ior devices and their associated systems.
	<ul> <li>Ability to enforce the established local and remote access requirements</li> </ul>	<ul> <li>Providing documentation that describes indicators of unauthorized use of the lot device.</li> </ul>
	Ability to provent external access to the let	
	<ul> <li>Ability to prevent external access to the IOT dovice management interface.</li> </ul>	
	Ability to assign roles to lot device user	
	- Ability to assign roles to for device user	

Scenario ID and		
Description with	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
	<ul> <li>Ability to support a hierarchy of logical access privileges for the IoT device based on roles.</li> <li>Ability to apply least privilege to user accounts.</li> <li>Ability to enable automation and reporting of account management activities.</li> <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).</li> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</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>	
Scenario 4: Protect	<ul> <li>Ability to identify software loaded on the IoT</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement</li> </ul>
Host from	device based on IoT device identity.	management and operational controls to protect data obtained from IoT devices and
Unauthorized	<ul> <li>Ability to verify digital signatures.</li> </ul>	associated systems from unauthorized access, modification, and deletion.
Application	<ul> <li>Ability to run hashing algorithms.</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement</li> </ul>
Installation:	<ul> <li>Ability to perform authenticated encryption</li> </ul>	management and operational controls to protect IoT device data integrity and
This test will	algorithms.	associated systems data integrity.
demonstrate	<ul> <li>Ability to compute and compare hashes.</li> </ul>	<ul> <li>Providing IoT device customers with the details necessary to support secure</li> </ul>
blocking the	<ul> <li>Ability to utilize one or more capabilities to</li> </ul>	implementation of the IoT device and associated systems data integrity controls.
installation and	protect transmitted data from unauthorized	<ul> <li>Providing IoT device customers with documentation describing the data integrity</li> </ul>
execution of	access and modification.	controls built into the IoT device and how to use them. If there are no data integrity
This test will demonstrate blocking the installation and execution of unauthorized	<ul> <li>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>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</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
applications on	<ul> <li>Ability to validate the integrity of data</li> </ul>	controls built into the IoT device, include documentation explaining to IoT device
workstation in the	transmitted.	customers the ways to achieve IoT device data integrity.
manufacturing	<ul> <li>Ability to verify software updates come from</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems</li> </ul>
system.	valid sources by using an effective method	while preserving data integrity.
PR.DS-6	(e.g., digital signatures, checksums,	<ul> <li>Providing instructions and documentation describing the physical and logical access</li> </ul>
PR.MA-1	certificate validation).	capabilities necessary to the IoT device to perform each type of maintenance activity.
DE.AE-1	<ul> <li>Ability to verify and authenticate any update</li> </ul>	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT</li> </ul>
DE.AE-2	before installing it.	device diagnostics activities.
DE.AE-3	<ul> <li>Ability to store the operating environment</li> </ul>	Providing the details and instructions to perform necessary IoT device maintenance
DE.CM-1	(e.g., firmware image, software,	activities and repairs.
DE.CM-3	applications) in read-only media (e.g., Read	<ul> <li>Providing communications and comprehensive documentation describing the IOT</li> <li>device resistance according to a formation of the second but the manufactures and the</li> </ul>
DE.CIVI-7	Only Memory).	device maintenance operations performed by the manufacturer and the
	<ul> <li>Ability to provide a physical indicator of sensor use</li> </ul>	manufacturer's supporting entities.
	Selisor use.	<ul> <li>Providing communications and comprehensive documentation describing maintenance operations that the IoT device suctomer is required to perform</li> </ul>
	- Ability to send requested adult logs to all	Browiding communications that include details for the recommended events that will
	(e.g. where its auditing information can be	trigger IoT device system reviews and/or maintenance by the manufacturer
	checked to allow for review analysis and	Providing communications and documentation detailing how to perform
	reporting)	recommended local and/or remote maintenance activities
	<ul> <li>Ability to keep an accurate internal system</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for</li> </ul>
	time.	defined maintenance tasks.
	<ul> <li>Ability to support a monitoring process to</li> </ul>	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>
	check for disclosure of organizational	<ul> <li>Providing documentation describing how to implement and securely deploy</li> </ul>
	information to unauthorized entities.	monitoring devices and tools for IoT devices and associated systems.
	<ul> <li>Ability to monitor changes to the</li> </ul>	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur</li> </ul>
	configuration settings.	when an attack is being launched.
	<ul> <li>Ability to detect remote activation attempts.</li> </ul>	<ul> <li>Providing documentation describing the types of usage and environmental systems</li> </ul>
	<ul> <li>Ability to detect remote activation of</li> </ul>	data that can be collected from the IoT device.
	sensors.	<ul> <li>Providing appropriate tools, assistance, instructions, or other details describing the</li> </ul>
	<ul> <li>Ability to take organizationally defined</li> </ul>	capabilities for monitoring the IoT device and/or for the IoT device customer to
	actions when unauthorized hardware and	report actions to the monitoring service of the manufacturer's supporting entity.
	software components are detected (e.g.,	<ul> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> </ul>
	disallow a flash drive to be connected even if	<ul> <li>Providing documentation describing details necessary to identify unauthorized use of</li> </ul>
	a Universal Serial Bus [USB] port is present).	IoT devices and their associated systems.
		<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT</li> </ul>
		device.

Scenario ID and				
Description with		Device Cybersecurity Capabilities		Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		· · · ·		
Scenario 5: Protect		Ability to identify software loaded on the IoT		Providing documentation and/or other communications describing how to implement
from Unauthorized		device based on IoT device identity.		management and operational controls to protect data obtained from IoT devices and
Addition of a		Ability to verify digital signatures.		associated systems from unauthorized access, modification, and deletion.
Device:		Ability to run hashing algorithms.		Providing communications to IoT device customers describing how to implement
This test will		Ability to perform authenticated encryption		management and operational controls to protect IoT device data integrity and
demonstrate the		algorithms.		associated systems data integrity.
detection of an		Ability to compute and compare hashes.		Providing IoT device customers with the details necessary to support secure
unauthorized device	•	Ability to utilize one or more capabilities to		implementation of the IoT device and associated systems data integrity controls.
connecting to the		protect transmitted data from unauthorized		Providing IoT device customers with documentation describing the data integrity
manufacturing		access and modification.		controls built into the IoT device and how to use them. If there are no data integrity
system.	•	Ability to validate the integrity of data		controls built into the IoT device, include documentation explaining to IoT device
PR.DS-6		transmitted.		customers the ways to achieve IoT device data integrity.
PR.MA-1		Ability to verify software updates come from		Providing details for how to review and update the IoT device and associated systems
DE.AE-1		valid sources by using an effective method		while preserving data integrity.
DE.AE-2		(e.g., digital signatures, checksums,		Providing instructions and documentation describing the physical and logical access
DE.AE-3		certificate validation).		capabilities necessary to the IoT device to perform each type of maintenance activity.
DE.CM-1		Ability to verify and authenticate any update		Providing detailed documentation describing the tools manufacturers require for IoT
DE.CM-3		before installing it.		device diagnostics activities.
DE.CM-7	•	Ability to store the operating environment		Providing the details and instructions to perform necessary IoT device maintenance
		(e.g., firmware image, software,		activities and repairs.
		applications) in read-only media (e.g., Read		Providing communications and comprehensive documentation describing the IoT
		Only Memory).		device maintenance operations performed by the manufacturer and the
		Ability to provide a physical indicator of		manufacturer's supporting entities.
		sensor use.		Providing communications and comprehensive documentation describing
		Ability to send requested audit logs to an		maintenance operations that the IoT device customer is required to perform.
		external audit process or information system	- C	Providing communications that include details for the recommended events that will
		(e.g., where its auditing information can be	_	trigger IoT device system reviews and/or maintenance by the manufacturer.
		checked to allow for review, analysis, and		Providing communications and documentation detailing how to perform
	_	reporting).	_	recommended local and/or remote maintenance activities.
		Ability to keep an accurate internal system	- T-	Providing documented descriptions of the specific maintenance procedures for
	_	time.	_	defined maintenance tasks.
		Ability to support a monitoring process to		Providing education for now to scan for critical software updates and patches.
		information to unputhorized entities		monitoring dovisor and tools for IoT dovisor and according dovisors
		Ability to monitor changes to the		monitoring devices and tools for for devices and associated systems.
		configuration settings		when an attack is being launched

Scenario ID and Description with CSF Subcategories		Device Cybersecurity Capabilities		Manufacturer Nontechnical Supporting Capabilities
	2	Ability to detect remote activation attempts. Ability to detect remote activation of	•	Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.
		sensors.		Providing appropriate tools, assistance, instructions, or other details describing the
	•	Ability to take organizationally defined		capabilities for monitoring the IoT device and/or for the IoT device customer to
		actions when unauthorized hardware and		report actions to the monitoring service of the manufacturer's supporting entity.
		software components are detected (e.g.,		Providing the details necessary to monitor IoT devices and associated systems.
		disallow a flash drive to be connected even if		Providing documentation describing details necessary to identify unauthorized use of
		a Universal Serial Bus [USB] port is present).		IoT devices and their associated systems.
				Providing documentation that describes indicators of unauthorized use of the IoT
				device.
Scenario 6: Detect		Ability to identify software loaded on the IoT		Providing documentation and/or other communications describing how to implement
Unauthorized		device based on IoT device identity.		management and operational controls to protect data obtained from IoT devices and
Device-to-Device		Ability to verify digital signatures.		associated systems from unauthorized access, modification, and deletion.
Communications:		Ability to run hashing algorithms.	÷.,	Providing communications to IoT device customers describing how to implement
This test will		Ability to perform authenticated encryption		management and operational controls to protect IoT device data integrity and
demonstrate the		algorithms.		associated systems data integrity.
detection of		Ability to compute and compare hashes.		Providing IoT device customers with the details necessary to support secure
unauthorized		Ability to utilize one or more capabilities to		implementation of the IoT device and associated systems data integrity controls.
communications		protect transmitted data from unauthorized		Providing IoT device customers with documentation describing the data integrity
between devices.	_	access and modification.		controls built into the IoT device and now to use them. If there are no data integrity
PR.DS-6 PR.MA-1		Ability to validate the integrity of data transmitted		controls built into the IOT device, include documentation explaining to IOT device
DF.AF-1		Ability to verify software undates come from		Providing details for how to review and undate the IoT device and associated systems
DE.AE-2		valid sources by using an effective method		while preserving data integrity.
DE.AE-3		(e.g., digital signatures, checksums,		Providing instructions and documentation describing the physical and logical access
DE.CM-1		certificate validation).		capabilities necessary to the IoT device to perform each type of maintenance activity.
DE.CM-3	•	Ability to verify and authenticate any update		Providing detailed documentation describing the tools manufacturers require for IoT
DE.CM-7		before installing it.		device diagnostics activities.
	•	Ability to store the operating environment		Providing the details and instructions to perform necessary IoT device maintenance
		(e.g., firmware image, software,		activities and repairs.
		applications) in read-only media (e.g., Read		Providing communications and comprehensive documentation describing the IoT
		Only Memory).		device maintenance operations performed by the manufacturer and the
	•	Ability to provide a physical indicator of		manufacturer's supporting entities.
		sensor use.		Providing communications and comprehensive documentation describing
	•	Ability to send requested audit logs to an		maintenance operations that the IoT device customer is required to perform.
		external audit process or information system		

Scenario ID and		
Description with	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories	<ul> <li>(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 drive to be connected even if a Universal Serial Bus [USB] port is present).</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> <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 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> </ul>
Scenario 7: Protect from Unauthorized Modification and Deletion of Files: This test will demonstrate protection of files from unauthorized deletion both locally and on network file share. PR.DS-1 PR.DS-6 PR.IP-4 PR.MA-1	<ul> <li>Ability to execute cryptographic mechanisms of appropriate strength and performance.</li> <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 store passwords at rest, as well as device identity and other authentication data.</li> <li>Ability to support data encryption and signing to prevent data from being altered in device storage.</li> <li>Ability to secure data stored locally on the device.</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 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 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	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
DE.AE-2	<ul> <li>Ability to secure data stored in remote storage areas (e.g., cloud, server).</li> <li>Ability to utilize separate storage partitions for system and user data.</li> <li>Ability to protect the audit information through mechanisms such as:         <ul> <li>encryption</li> <li>digitally signing audit files</li> <li>securely sending audit files to another device</li> <li>other protections created by the device manufacturer</li> </ul> </li> <li>Ability to verify digital signatures.</li> <li>Ability to verify digital signatures.</li> <li>Ability to verify digital signatures.</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 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>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, 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 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> <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> <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> <li>Providing detailed documentation describing the physical and logical access capabilities necessary to the IoT device to perform necessary IoT device maintenance activity.</li> <li>Providing the details and instructions to perform necessary IoT device maintenance activity.</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 activities and 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 details proved the perform recommended local and/or remote maintenance activities.</li> <li>Providing communications and documentation details of the recommended events that will trigger</li></ul>

Scenario ID and		
Description with	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
Scenario 8: Detect	<ul> <li>Ability to configure IoT device access control</li> </ul>	Providing detailed instructions and guidance for establishing activities performed by
Unauthorized	policies using IoT device identity.	the IoT device that do not require identification or authentication.
Modification of PLC	<ul> <li>Ability to authenticate external users and</li> </ul>	<ul> <li>Providing documentation describing the specific IoT platforms used with the device to</li> </ul>
Logic:	systems.	support required IoT authentication control techniques.
This test will	<ul> <li>Ability to securely interact with authorized</li> </ul>	<ul> <li>Providing documentation with details describing external authentication by IoT</li> </ul>
demonstrate the	external, third-party systems.	platforms and associated authentication methods that can be used with the IoT
detection of PLC	<ul> <li>Ability to identify when an external system</li> </ul>	device.
logic modification.	meets the required security requirements	Providing documentation and/or other communications describing how to implement
PR.AC-3	for a connection.	management and operational controls to protect data obtained from IoT devices and
PR.AC-7	<ul> <li>Ability to establish secure communications</li> </ul>	associated systems from unauthorized access, modification, and deletion.
PR.DS-6	with internal systems when the device is	<ul> <li>Providing communications to IoT device customers describing how to implement</li> </ul>
PR.MA-1	operating on external networks.	management and operational controls to protect IoT device data integrity and
PR.MA-2	<ul> <li>Ability to establish requirements for remote</li> </ul>	associated systems data integrity.
DE.AE-1	access to the IoT device and/or IoT device	<ul> <li>Providing IoT device customers with the details necessary to support secure</li> </ul>
DE.AE-2	interface.	implementation of the IoT device and associated systems data integrity controls.
DE.AE-3	<ul> <li>Ability to enforce the established local and</li> </ul>	<ul> <li>Providing IoT device customers with documentation describing the data integrity</li> </ul>
DE.CM-1	remote access requirements.	controls built into the IoT device and how to use them. If there are no data integrity
DE.CM-3	<ul> <li>Ability to prevent external access to the IoT</li> </ul>	controls built into the IoT device, include documentation explaining to IoT device
DE.CM-7	device management interface.	customers the ways to achieve IoT device data integrity.
	<ul> <li>Ability for the IoT device to require</li> </ul>	<ul> <li>Providing details for how to review and update the IoT device and associated systems</li> </ul>
	authentication prior to connecting to the	while preserving data integrity.
	device.	<ul> <li>Providing instructions and documentation describing the physical and logical access</li> </ul>
	<ul> <li>Ability for the IoT device to support a</li> </ul>	capabilities necessary to the IoT device to perform each type of maintenance activity.
	second, or more, authentication method(s).	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT</li> </ul>
	<ul> <li>Ability to identify software loaded on the IoT</li> </ul>	device diagnostics activities.
	device based on IoT device identity.	Providing the details and instructions to perform necessary IoT device maintenance
	Ability to verify digital signatures.	activities and repairs.
	Ability to run hashing algorithms.	Providing communications and comprehensive documentation describing the IoT
	<ul> <li>Ability to perform authenticated encryption</li> </ul>	device maintenance operations performed by the manufacturer and the
	algorithms.	manufacturer's supporting entities.
	<ul> <li>Ability to compute and compare nashes.</li> <li>Ability to utilize one or more compalities to</li> </ul>	<ul> <li>Providing communications and comprehensive documentation describing</li> <li>maintenance operations that the IoT device systemer is required to perform</li> </ul>
	<ul> <li>Ability to utilize one of more capabilities to protect transmitted data from unauthorized</li> </ul>	Browiding communications that include details for the recommended events that will
	access and modification	<ul> <li>Froming communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> </ul>
	Ability to validate the integrity of data	Providing communications and documentation detailing how to perform
	transmitted	recommended local and/or remote maintenance activities
Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
--	---	---
	<ul> <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> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</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 drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing education for how to scan for critical software updates and patches.</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 documentation describing how to implement and securely deploy monitoring devices and tools for 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 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 describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> </ul>
Scenario 9: Protect from Modification of Historian Data:	<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> </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	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
This test will demonstrate the blocking of modification of historian archive data. PR.DS-6 PR.MA-1 DE.AE-2	<ul> <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>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, 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 detaile 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 and documentation details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing documentation description IoT device behavior indicators that could occur when an attack is being launche</li></ul>
Scenario 10: Detect	<ul> <li>Ability to identify software loaded on the IoT</li> </ul>	<ul> <li>Providing education to IoT device customers covering the instructions and details</li> </ul>
Sensor Data	device based on IoT device identity.	necessary for them to create accurate backups and to recover the backups when
Manipulation:	<ul> <li>Ability to verify digital signatures.</li> </ul>	necessary.
This test will	<ul> <li>Ability to run hashing algorithms.</li> </ul>	<ul> <li>Providing education to IoT device customers that includes instructions describing how</li> </ul>
demonstrate		to back up data from systems where IoT device data is stored.

Scenario ID and		
Description with	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
CSF Subcategories		
detection of atypical	<ul> <li>Ability to perform authenticated encryption</li> </ul>	<ul> <li>Providing awareness reminders and tips to IoT device customers (e.g., directly in</li> </ul>
data reported to the	algorithms.	person, in videos, in an online webinar) for various aspects involved with backing up
historian.	<ul> <li>Ability to compute and compare hashes.</li> </ul>	the IoT device data.
PR.IP-4	<ul> <li>Ability to utilize one or more capabilities to</li> </ul>	<ul> <li>Providing documentation and/or other communications describing how to implement</li> </ul>
PR.DS-6	protect transmitted data from unauthorized	management and operational controls to protect data obtained from IoT devices and
PR.MA-1	access and modification.	associated systems from unauthorized access, modification, and deletion.
DE.AE-1	<ul> <li>Ability to validate the integrity of data</li> </ul>	<ul> <li>Providing communications to IoT device customers describing how to implement</li> </ul>
DE.AE-2	transmitted.	management and operational controls to protect IoT device data integrity and
DE.AE-3	<ul> <li>Ability to verify software updates come from</li> </ul>	associated systems data integrity.
DE.CM-1	valid sources by using an effective method	<ul> <li>Providing IoT device customers with the details necessary to support secure</li> </ul>
DE.CM-3	(e.g., digital signatures, checksums,	implementation of the IoT device and associated systems data integrity controls.
DE.CM-7	certificate validation).	<ul> <li>Providing IoT device customers with documentation describing the data integrity</li> </ul>
	<ul> <li>Ability to verify and authenticate any update</li> </ul>	controls built into the IoT device and how to use them. If there are no data integrity
	before installing it.	controls built into the IoT device, include documentation explaining to IoT device
	<ul> <li>Ability to store the operating environment</li> </ul>	customers the ways to achieve IoT device data integrity.
	(e.g., firmware image, software,	<ul> <li>Providing details for how to review and update the IoT device and associated systems</li> </ul>
	applications) in read-only media (e.g., Read	while preserving data integrity.
	Only Memory).	<ul> <li>Providing instructions and documentation describing the physical and logical access</li> </ul>
	<ul> <li>Ability to provide a physical indicator of</li> </ul>	capabilities necessary to the IoT device to perform each type of maintenance activity.
	sensor use.	<ul> <li>Providing detailed documentation describing the tools manufacturers require for IoT</li> </ul>
	<ul> <li>Ability to send requested audit logs to an</li> </ul>	device diagnostics activities.
	external audit process or information system	Providing the details and instructions to perform necessary IoT device maintenance
	(e.g., where its auditing information can be	activities and repairs.
	checked to allow for review, analysis, and	<ul> <li>Providing communications and comprehensive documentation describing the iol         device resistance executions and the second by the respective and the     </li> </ul>
	reporting).	device maintenance operations performed by the manufacturer and the
	<ul> <li>Ability to keep an accurate internal system</li> </ul>	Braviding communications and communication describing
	Ability to support a monitoring process to	<ul> <li>Providing communications and comprehensive documentation describing</li> <li>maintenance operations that the IoT device suctementic required to perform</li> </ul>
	- Ability to support a monitoring process to	Browiding communications that include details for the recommended events that will
	information to unauthorized entities	trigger IoT device system reviews and/or maintenance by the manufacturer
	<ul> <li>Ability to monitor changes to the</li> </ul>	<ul> <li>Providing communications and documentation detailing how to perform</li> </ul>
	configuration settings	recommended local and/or remote maintenance activities
	<ul> <li>Ability to detect remote activation attempts</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for</li> </ul>
	<ul> <li>Ability to detect remote activation of</li> </ul>	defined maintenance tasks.
	sensors.	<ul> <li>Providing education for how to scan for critical software updates and patches.</li> </ul>

Scenario ID and Description with CSF Subcategories	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>	<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>
Scenario 11: Detect Unauthorized Firmware Modification: This test will demonstrate the detection of device firmware modification 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> <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>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> <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 the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul> <li>Ability to provide a physical indicator of sensor use.</li> </ul>	Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the
	<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 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> </ul>
	<ul> <li>Ability to keep an accurate internal system time.</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 support a monitoring process to check for disclosure of organizational information to unauthorized entities</li> </ul>	<ul> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing education for how to scap for critical software updates and patches</li> </ul>
	<ul> <li>Ability to monitor changes to the configuration settings.</li> </ul>	<ul> <li>Providing education for now to scan for critical software updates and patches.</li> <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><li>Ability to detect remote activation of</li></ul>	<ul> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
	<ul><li>sensors.</li><li>Ability to take organizationally defined</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>
	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).	<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> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and the size and the size associated systems.</li> </ul>
		<ul> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>