NIST SPECIAL PUBLICATION 1800-10C

Protecting Information and System Integrity in Industrial Control System Environments:

Cybersecurity for the Manufacturing Sector

Volume C: How-To Guides

Michael Powell

National Cybersecurity Center of Excellence National Institute of Standards and Technology

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

Matthew Zopf Strativia Largo, Maryland

FINAL

March 2022

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

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

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



DISCLAIMER

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

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to 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 cybersecurity measures such as this recommendation.

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

National Institute of Standards and Technology Special Publication 1800-10C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-10C, 128 pages, March 2022, CODEN: NSPUE2.

FEEDBACK

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Today's manufacturing organizations rely on industrial control systems (ICS) to conduct their operations. Increasingly, ICS are facing more frequent, sophisticated cyber attacks—making manufacturing the second-most targeted industry (C. Singleton et al., X-Force Threat Intelligence Index 2021, IBM, February 2021, <u>https://www.ibm.com/security/data-breach/threat-intelligence</u>). Cyber attacks against ICS threaten operations and worker safety, resulting in financial loss and harm to the organization's reputation.

The architecture and solutions presented in this guide are built upon standards-based, commercially available products, and represent some of the possible solutions. The solutions implement standard cybersecurity capabilities, such as behavioral anomaly detection, application allowlisting, file integrity-checking, change control management, and user authentication and authorization. The solution was tested in two distinct lab settings: a discrete manufacturing work cell, which represents an assembly line

production, and a continuous process control system (PCS), which represents chemical manufacturing industries.

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

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

KEYWORDS

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

ACKNOWLEDGEMENTS

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

Name	Organization
Dan Frechette	Microsoft
Ian 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-USA
Josh Carlson	Dragos
Alex Baretta	Dragos

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product

components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

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

DOCUMENT CONVENTIONS

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

PATENT DISCLOSURE NOTICE

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

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL. No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Contents

1	Intr	oduct	ion	.1
	1.1	How to	o Use this Guide	1
	1.1	Build C	Dverview	2
	1.2	Туроді	raphic Conventions	2
	1.3	Logica	l Architecture Summary	3
2	Pro	duct lı	nstallation Guides	5
	2.1	Dispel	Remote Access	5
		2.1.1	Host and Network Configuration	6
		2.1.2	Installation	7
		2.1.3	Configuration	8
	2.2	Dragos	5	12
		2.2.1	Host and Network Configuration	12
		2.2.2	Installation	12
		2.2.3	Configuration	12
	2.3	Foresc	out Platform	17
		2.3.1	Host and Network Configuration	19
		2.3.2	Installation	20
		2.3.3	Configuration	22
	2.4	Green	Tec-USA	31
		2.4.1	Host and Network Configuration	32
		2.4.2	Installation	32
		2.4.3	Configuration	33
	2.5	Micros	oft Azure Defender for IoT	36
		2.5.1	Host and Network Configuration	36
		2.5.2	Installation	36
		2.5.3	Configuration	36
	2.6	OSIsof	t PI Data Archive	41
		2.6.1	Host and Network Configuration	41
		2.6.2	Installation	42
		2.6.3	Configuration	43
	2.7	Securit	ty Onion	64
		2.7.1	Host and Network Configuration	64

	2.7.2	Installation	65
	2.7.3	Configuration	65
2.8	TDi Co	onsoleWorks	68
	2.8.1	Host and Network Configuration	68
	2.8.2	Installation	68
	2.8.3	Configuration	
2.9	Tenab	le.OT	97
	2.9.1	Host and Network Configuration	
	2.9.2	Installation	
	2.9.3	Configuration	
2.10	VMwa	are Carbon Black App Control	105
	2.10.1	Host and Network Configuration	105
	2.10.2	Installation	106
	2.10.3	Configuration	107
2.11	Windo	ows Software Restriction Policy	114
	2.11.1	Host and Network Configuration	114
	2.11.2	Installation	115
	2.11.3	Configuration	115
Append	lix A	List of Acronyms	123
Append	lix B	Build Architectures Diagrams	

List of Figures

Figure 1-1: CSMS Network Architecture
Figure 2-1 Dispel High-level Implementation, from Remote Access for ICS
Figure 2-2 Mapping a Network Drive
Figure 2-3 Authentication to File Server
Figure 2-4 Dragos OSIsoft PI Server Integration
Figure 2-5 Dragos PI Web API Configuration
Figure 2-6 OSIsoft PI Server to Dragos Asset and Data Pairing
Figure 2-7 OSIsoft PI Server and Dragos Paired Data Elements
Figure 2-8 Dragos Zone Administration Page
Figure 2-9 Dragos Create Zone Pop-up
Figure 2-10 Forescout High-Level Components and Dataflows
Figure 2-11 Forescout SecureConnector Distribution Tool
Figure 2-12 Forescout Agent Download21
Figure 2-13 eyeInspect Sensor Admin/Overview Page – Add Sensor
Figure 2-14 Adding a New SilentDefense Sensor Dialog
Figure 2-15 eyeInspect ICMP Protocol/Port Scan Attempt Settings
Figure 2-16 eyeInspect Sensor Configuration Options
Figure 2-17 eyeInspect Portscan Detection Settings
Figure 2-18 Add ICS Patrol Sensor Dialog
Figure 2-19 ICS Patrol Sensor Admin Page
Figure 2-20 Add an ICS Patrol Scan Policy
Figure 2-21 eyeSight Add Dialog – General Information
Figure 2-22 eyeSight Add – Command Center Credentials
Figure 2-23 eyeSight OT Settings
Figure 2-24 eyeSight Test Connection Successful Message
Figure 2-25 Azure Defender for IoT SSH Session for Network Configuration
Figure 2-26 Azure Defender for IoT Create New Data Mining Report for AMS Protocol Information 38
Figure 2-27 Azure Defender for IoT Custom Alert for Firmware Major Version Number Change
Figure 2-28 Azure Defender for IoT Custom Alert for Firmware Minor Version Number Change 40
Figure 2-29 Azure Defender for IoT Custom Alert for Firmware Build Version Number Change

Figure 2-30 Screenshot of the PI Interface Configuration Utility before the Interface is configured 44
Figure 2-31 Screenshot of the PI Data Collection Manager Displaying Green Checkmarks After the PI System Connector is Properly Configured
Figure 2-32 Screenshot of the PI Interface Configuration Utility Showing the Added Scan Class # 2 for Polling the PLC Every 60 Seconds
Figure 2-33 Screenshot of the PI System Management Tools Component After Configuring the PI Points for PLC Hardware and Firmware Version Number Integrity Checking
Figure 2-34 Screenshot of PI System Explorer Displaying some Attributes of the PLC Element. Attributes for the TwinCAT version number are visible in the list
Figure 2-35 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Event Frame Template
Figure 2-36 Screenshot of PI System Explorer Displaying the TwinCAT Version Mismatch Event Frame Template
Figure 2-37 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Analysis Template in the PLC Element Template
Figure 2-38 Screenshot of PI System Explorer Displaying the TwinCAT Firmware Version Mismatch Analysis Template in the PLC Element Template
Figure 2-39 Wazuh Agent Manager
Figure 2-40 ossec.conf File
Figure 2-41 Wazuh Agent Manager User Interface67
Figure 2-42 Log Received After a File Change Was Detected
Figure 2-43 ConsoleWorks Registration Screen73
Figure 2-44 ConsoleWorks Offline Registration Process
Figure 2-45 ConsoleWorks System Backups74
Figure 2-46 ConsoleWorks Importing System Configurations and Components
Figure 2-47 ConsoleWorks Password Settings
Figure 2-48 ConsoleWorks Add the Local Graphical Gateway for RDP Access
Figure 2-49 ConsoleWorks Example Device Type Definition79
Figure 2-50 ConsoleWorks List of Device Types
Figure 2-51 ConsoleWorks Example Device Definition
Figure 2-52 ConsoleWorks List of PCS (Build 1) Devices
Figure 2-53 ConsoleWorks List of CRS (Build 3) Devices
Figure 2-54 ConsoleWorks Example RDP Configuration
Figure 2-55 ConsoleWorks List of PCS (Build 1) RDP Connections

Figure B-1 Build 1 Architecture Diagram	125
Figure B-2 Build 2 Architecture Diagram	126
Figure B-3 Build 3 Architecture Diagram	127
Figure B-4 Build 4 Architecture Diagram	128

List of Tables

Table 2-1 Dispel Deployment 6
Table 2-2 Firewall Rules for Dispel
Table 2-3 Firewall Rules 10
Table 2-4 Dragos Deployment 12
Table 2-5 Forescout Deployment
Table 2-6 eyeSight Agent Deployment
Table 2-7 Firewall Rules for Forescout 20
Table 2-8 GreenTec-USA WORMdrive and ForceField Deployment 32
Table 2-9 Microsoft Azure Defender IoT Deployment 36
Table 2-10 OSIsoft PI Domain Hosts Deployment 41
Table 2-11 OSIsoft PI CRS Hosts Deployment
Table 2-12 OSIsoft PI PCS Hosts Deployment
Table 2-13 Security Onion Domain Hosts Deployment
Table 2-14 Security Onion PCS Hosts Deployment 65
Table 2-15 Security Onion CRS Hosts Deployment 65
Table 2-16 ConsoleWorks Build 1 Deployment 68
Table 2-17 ConsoleWorks Build 3 Deployment 68
Table 2-18 ConsoleWorks Device Type List 78
Table 2-19 ConsoleWorks PCS (Build 1) Devices 80
Table 2-20 ConsoleWorks CRS (Build 3) Devices 81
Table 2-21 ConsoleWorks PCS (Build 1) Graphical Connections
Table 2-22 ConsoleWorks CRS (Build 3) Graphical Connections 86
Table 2-23 ConsoleWorks PCS (Build 1) Console Connections 88
Table 2-24 ConsoleWorks CRS (Build 3) Console Connections 89
Table 2-25 Tenable.OT Appliance Details. 97

Table 2-26 Firewall Rules for Tenable.OT	97
Table 2-27 Carbon Black App Control Domain Hosts Deployment	106
Table 2-28 Carbon Black App Control PCS Hosts Deployment	106
Table 2-29 Carbon Black App Control CRS Hosts Deployment	106
Table 2-30 Windows SRP Domain Servers	114
Table 2-31 Windows SRP Build 2 Deployment	115
Table 2-32 Windows SRP Build 3 Deployment	115

1 Introduction

The following volume of this guide shows information technology (IT) professionals and security engineers how we implemented this example solution. We cover all the products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 How to Use this Guide

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

This guide contains three volumes:

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

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

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

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

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

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

 Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-10C*, to replicate all or parts of the build

created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse any products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of this manufacturing ICS solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.5, Technologies, in *NIST SP 1800-10B*, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to manufacturing nccoe@nist.gov.

1.1 Build Overview

The NCCoE partnered with NIST's Engineering Laboratory (EL) to provide real-world scenarios that could happen in ICS in the manufacturing sector. This collaboration spawned four unique builds: two builds within the Collaborative Robotics (CRS) environment and two builds within the Process Control System (PCS) environment. For each build, the NCCoE and the EL performed eleven scenarios. The step-by-step instructions on how each product was installed and configured in this lab environment are outlined in this document. For more information on the two environments refer to Section 4.5 in *NIST SP 1800-10B*. Additionally, Appendix B of this Volume contains the four build architecture diagrams for reference.

1.2 Typographic Conventions

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the NCCoE Style Guide.
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, on- screen computer output, sample code examples, and status codes	mkdir

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Monospace Bold	command-line user input contrasted with computer output	service sshd start
blue text	link to other parts of the doc- ument, a web URL, or an email address	All publications from NIST's NCCoE are available at <u>https://www.nccoe.nist.gov</u> .

1.3 Logical Architecture Summary

The security mechanisms and technologies were integrated into the existing NIST Cybersecurity for Smart Manufacturing Systems (CSMS) lab environment. This cybersecurity performance testbed for ICS is comprised of the PCS and the CRS environments along with additional networking capabilities to emulate common manufacturing environments. For more information see An *Industrial Control System Cybersecurity Performance Testbed*, NISTIR 8089,

http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

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

Figure 1-1 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 per vendor recommendations and standard practices as described in the detailed sections for each build.





In summary, there are six networks within the CSMS architecture:

Testbed LAN: This network is where the majority of the collaborators' products are installed. This LAN has access to the PCS and CRS environments. Other systems, such as AD, an NTP server, and a Windows server, are also located on this LAN. The Testbed LAN has three gateways to other network segments, including 10.100.0.1 to reach the DMZ and the corporate network, 10.100.0.20 as a network address translation (NAT) interface to the CRS environment, and 10.100.0.40 as the gateway to the PCS environment.

DMZ: A demilitarized zone that separates the corporate network from the operational technology (OT) network. Many of the collaborators' products are also installed in the DMZ. The DMZ is used across the PCS and CRS environments.

PCS Virtual Local Area Network (VLAN) 1: This is the operations LAN within the PCS environment. This LAN simulates a central control room environment. The gateway interface for this network segment is 172.16.1.1

PCS VLAN 2: This is the supervisory LAN within the PCS environment. This LAN simulates the process operation/manufacturing environment, which consists of the operating plant, programmable logic

controller (PLC)s, object linking and embedding for process control (OPC) server, and data historian. The gateway interface for this network segment is 172.16.2.1

CRS Supervisory LAN: This LAN is within the CRS environment. The historian, PLCs, operating human machine interface (HMI), Engineering workstation, and remote input/output devices are connected to this network. The gateway interface for this network segment is 192.168.0.2

CRS Control LAN: This LAN is within the CRS environment. The robot controllers and manufacturing station controllers are connected to this network. The gateway interface for this network segment is 192.168.1.2

The test bed networks used static IPv4 addresses exclusively, and the subnet masks were set to 255.255.255.0. No IPv6 addresses were used. This setup is consistent with industry practice. Specific Internet Protocol (IP) addresses are listed for each component in the following sections.

For an in-depth view of the architectures PCS and CRS builds, specific build architecture diagrams can be found in Volume B of this practice guide, Section 4.3, Process Control System, and Section 4.4, Collaborative Robotics System.

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all the products used to build the example solutions.

2.1 Dispel Remote Access

Dispel is a remote access tool for OT environments that provides secure remote access to the industrial networks. Dispel, implemented in Build 2 and Build 4, uses cloud-based virtual desktop interfaces (VDIs) that traverse a cloud-based Enclave to reach a Wicket ESI device that is deployed within the local OT network. Dispel supports both user authentication and authorization, and remote access for Builds 2 and 4.

Virtual Desktop Interfaces (VDIs)

VDIs are Virtual Machines (VMs) that reside in the cloud and allow users to connect using Remote Desktop Protocol (RDP). The VDIs establish a secure connection to the Wicket ESI located in the OT network to provide network access to the OT devices.

Enclave

Enclaves are single-tenanted, colorless core, moving target defense (MTD) networks. Enclaves are composed of VMs that act as traffic nodes. To create a shifting target profile, these VMs are steadily replaced by new VMs launched on different hypervisors, in different geographic regions, and/or on altogether different public or private clouds. In the case of Builds 2 and 4, the Enclaves were launched exclusively on public clouds. To provide a static set of IP addresses throughout the builds, the MTD characteristic was disabled.

Wicket ESI

Wicket ESIs are on-premise components, shown in Figure 2-1, that allow users to connect to the OT network remotely. These devices establish encrypted connections from the local OT network up to an Enclave which, in turn, is connected to the VDI, allowing a remote user to access the OT devices.

Additional information is available in *Remote Access for Industrial Control Systems* from Dispel.io at: <u>https://s3.amazonaws.com/downloads.dispel.io/resources/One+Pager/dispel-ics-brochure_20190529.pdf</u>





2.1.1 Host and Network Configuration

The Wicket ESI is connected to two ports within the DMZ, one for supporting outbound communications to the Dispel Enclave (labeled "WAN") and one for supporting communication through the local firewall to the ICS environment (labeled "LAN"). The items listed in Table 2-1 are the Wicket ESI specific device and network settings for the hardware provided to support Build 2 Figure B-2 and 4 Figure B-4.

Name	System	OS	CPU	Memory	Storage	Network
Dispel Wicket ESI	ONLOGIC, ML340G-51	Ubuntu 16.04	Intel i5- 6300U	16GB	120GB	Wicket WAN Interface 10.100.1.60 Wicket LAN Interface 10.100.1.61 DMZ
Dispel Enclave	Cloud Virtual Machines	Ubuntu 16.04	Variable	Variable	Variable	N/A
Dispel VDI	Cloud Virtual Machine	Windows Server 2016	Intel Xeon Platinum 8171M	8GB	120GB	N/A

2.1.2 Installation

Installation involves establishing an account on the Dispel cloud-infrastructure and deploying the preconfigured Wicket ESI device within the OT environment. Detailed installation information, customized to the end user's deployment, is provided by Dispel.

After connecting the WAN and LAN network cables, configuring the Wicket ESI required connecting a monitor, keyboard, and mouse to the unit using the available VGA and USB ports. Logging into the unit locally using the credentials provided by Dispel enabled configuration of the network connections using the following procedure (note: these procedures were executed using root privileges and can also be performed using Sudo).

1. Update the network interfaces with the IP configuration information:

#> vi /etc/network/interfaces

```
source-directory /etc/network/interfaces.d
# LAN
auto enp4s0
allow-hotplug enp4s0
iface enp4s0 inet static
      address 10.100.1.61
      netmask 255.255.255.0
      #gateway
      up route add -net 10.100.0.0 netmask 255.255.255.0 gw 10.100.1.1 dev
enp4s0
      up route add -net 172.16.0.0 netmask 255.255.252.0 gw 10.100.1.1 dev
enp4s0
# WAN
auto enp0s31f6
allow-hotplug enp0s31f6
iface enp0s31f6 inet static
      address 10.100.1.60
      netmask 255.255.255.0
      gateway 10.100.1.1
      dns-nameservers <ip address>
```

2. Update the Wicket ESI netcutter.cfg file to include the local subnet information (toward the bottom of the file):

#> vi /home/ubuntu/wicket/netcutter.cfg

```
...
subnets = (
    {
        name = "Default";
        value = "10.100.0.0/24";
        advertise = "false";
    },
    {
        name = "PCS";
        value = "172.16.0.0/22";
        advertise = "false";
    }
}
```

```
},
{
    name = "DMZ";
    value = "10.100.1.0/24";
    advertise = "false";
});
```

3. Restart the Wicket services with the following command:

#> service wicket restart

4. Check the log for errors and test connectivity to the Dispel environment (note: IP address will be account specific):

#> tail -f /home/ubuntu/wicket/wicket.log

2.1.3 Configuration

With the Wicket ESI connected to the lab environment, the solution may be configured by establishing an account and configuring the cloud infrastructure, configuring the corporate router/firewall to allow authorized connections to and from the Wicket ESI, and configuring the VDI environment to support the remote access to the ICS environments.

For full documentation and configuration instructions, see the Dispel documentation at <u>https://intercom.help/dispel/en/</u>.

Dispel created an organization named "NCCOE" with an Enclave name "NCCoE-Manufacturing" in their pre-production staging environment. A single "user" account was created for accessing the cloud infrastructure environment named nccoe-m-user@dispel.io. Organizations will need to plan for implementing multiple accounts for supporting the "owner" and "admin" roles in addition to the "user" roles. The "owner" and "admin" roles are for monitoring and managing the cloud infrastructure and are separate from the user accounts used to login to the VDI environment.

The staging environment was configured without the Dispel multifactor authentication (MFA) settings because personal identity verification (PIV) cards were not available as a supported mechanism, and the lab environment did not support authenticator application or security keys. However, MFA is very important for implementation and is strongly encouraged when planning the implementation. For this effort, to reduce the risk of not having the MFA implementation, NCCoE worked with Dispel to limit access to the cloud infrastructure and the VDI instances to only approved source IP addresses. *The additional protection of restricting access to the cloud infrastructure and VDI instances is also encouraged to reduce the risks associated with the internet-accessible web and RDP services*.

Configure Firewall Settings:

The Wicket ESI needs access to the internet and to the internal OT environment. Table 2-2 below describes the firewall rules implemented on the corporate router/firewall for communications on the internet-facing firewall and internal network zone firewall.

Table 2-2 Firewall Rules for Dispel

Rule Type	Source	Destination	Protocol:Port(s)	Purpose
Allow	10.100.1.60	IdAM: 159.65.111.193 Entry Node: 52.162.177.202	TCP/UDP:1194, HTTPS	Outbound Secure Web to Dis- pel Environment on the Inter- net
Allow	10.100.1.61	10.100.1.0/24	ICMP TCP/UDP:RDP, SSH, HTTP/HTTPS, SMB, NTP	PLC Controller Scans
Allow	10.100.1.61	Security Onion 10.100.0.26	TCP:1515 UDP:1514	Build 2: Communication be- tween Wazuh Agent and the server
Allow	10.100.1.61	172.16.0.0/22	TCP:RDP, HTTP/HTTPS	Build 2: Authorized Inbound Communications to PCS Envi- ronment
Allow	10.100.1.61	Carbon Black 10.100.0.52	TCP:41002	Build 4: Communication port used between Carbon Black Agent and the server
Allow	10.100.1.61	CRS NAT 10.100.0.20	TCP:48898 UDP:48899	Build 4: Inbound Automation Device Specification (ADS) Protocol for Communication with PLC Device

Notes:

- Dispel's recommended rule for allowing secure shell (SSH)for installation and remote support from the Dispel environment was not enabled for this effort.
- The rules implemented include restricting these outbound ports to Enclave specific IP addresses.
- The Enclave's MTD characteristics were disabled to keep the Enclave's IP addresses static for the duration of the project.

Configure Virtual Desktop Infrastructure (VDI):

The VDI instance is a fully functional workstation/server within the cloud environment. From the VDI instance, authorized users establish a VPN tunnel to the Wicket ESI within the OT environment and then have the access to the environment configured by the device and firewall configurations. In this effort, NCCOE implanted the VDI configuration to support Build 2 and Build 4. The configuration supports the OT environment's jump server configuration (allowing RDP and SSH access to systems within the PCS and CRS environment) and remote engineering workstation (configuring the VDI with the tools needed to support the ICS environment). The configuration for each build is detailed in the following sections:

1. Build 2: PCS Configuration

- a. For the PCS setup, the Dispel VDI was used in a jump server configuration. No additional software was installed. The firewall and Wicket ESI configuration allowed RDP and SSH connections to the PCS ICS environment. Additionally, RDP, SSH, and HTTP/HTTPS access to the Cybersecurity LAN environment was authorized for the remote sessions as defined in the previously described firewall settings, <u>Table 2-2</u>.
- 2. Build 4: CRS Configuration
 - a. For the CRS setup, the Dispel VDI was configured as a remote engineering workstation. To support the Beckhoff PLC, the TwinCAT 3 XAE software was installed on a VDI, and the network drive provided by the GreenTec-USA solution and hosted in the DMZ environment that contained the PLC code was mapped to the VDI. Additionally, RDP, SSH, and HTTP/HTTPS access to the Cybersecurity LAN environment was authorized for the remote sessions as defined in the previously described firewall settings, <u>Table 2-2</u>.
 - b. For the interaction with the Beckhoff PLC, the TwinCAT 3 XAE software (TC31-FULL-Setup.3.1.4024.10.exe) was installed on the VDI.
 - c. The Dispel VPN connection does not allow split-tunneling so, once the VPN connection is established from the VDI to the Wicket ESI, the VDI is disconnected from the internet. Therefore, download and installation of software occurred prior to connecting to the Wicket ESI.
 - d. Due to the NAT configuration of the RUGGEDCOM RX1510 router between the Cybersecurity LAN and the CRS environment, port forwarding rules were configured to allow external traffic to reach the Beckhoff CX9020 PLC.
 - e. The following rules (<u>Table 2-3</u>) were created in the RX1510 firewall to enable destination network address translation (DNAT) from the firewall WAN interface (10.100.0.20) to the CRS PLC (192.168.0.30)

Rule Type	Source	Destination	Destination Port(s)	Purpose
DNAT	10.100.1.61	192.168.0.30	UDP:48899	DNAT (10.100.0.20) - Beckhoff ADS discovery protocol used by the TwinCAT 3 software to discover ADS devices.
DNAT	10.100.1.61	192.168.0.30	TCP:48898	DNAT (10.100.0.20) - Beckhoff ADS protocol used by the TwinCAT 3 software to com- municate with the PLC.

Table 2-3 Firewall Rules

3. As described in 2.i above, the GreenTec WORMdisk (\\10.100.1.7\crs) was mapped to the VDI to access the PLC code. The configuration to map Windows is shown in Figure 2-2 below:

Figure 2-2 Mapping a Network Drive

		×
÷	Map N	letwork Drive
	What ne	etwork folder would you like to map?
	Specify the	e drive letter for the connection and the folder that you want to connect to:
	Drive:	Z: ~
	Folder:	\ <u>\10.100.1.7\crs</u>
		Example: \\server\share
		Reconnect at sign-in
		Connect using different credentials
		Connect to a Web site that you can use to store your documents and pictures.
		Finish Cancel

4. After clicking **Finish**, the user is prompted for credentials, as shown in Figure 2-3. An account authorized to access the network drive must be used. This is separate from the Dispel VDI credentials.

Figure 2-3	Authentication	to File	Server
------------	----------------	---------	--------

Windows	Security		×		
Enter i	Enter network credentials				
Enter yo	our credentials to conne	ect to: 10.100.1.7			
8	nccoeuser				
	•••••				
	Domain:				
	Remember my cr	edentials			
More ch	oices				
	ОК	Cancel			

2.2 Dragos

The Dragos platform implementation in Build 3 consists of two physical servers hosting the Dragos SiteStore and the Dragos sensor to meet the behavioral anomaly detection (BAD), hardware modification, firmware modification, and software modification capabilities. Dragos utilizes a combination of a passive sensor and integration with the OSIsoft PI Server to monitor critical networks for anomalies. OSIsoft PI performs active querying to retrieve information about endpoints in the CRS environment, which is shared with Dragos.

2.2.1 Host and Network Configuration

Dragos is installed and configured to support the CRS Environment in Build 3. The overall build architecture is shown in Figure B-3, and the Dragos specific components are listed in Table 2-4.

Name	System	OS	CPU	Memory	Storage	Network
VMware Server	Dell OEMR R740	VMware 6.7.0 Update 3	2x Intel 6130 CPU	384 GB	2x 1.5TB Mirror 6x 8TB RAID 10	Testbed LAN 10.100.0.62/24
Dragos Server	VMware	CentOS 7	48x vCPU	192 GB	215 GB 10 GB 1.5 TB 1.5 TB	Testbed LAN 10.100.0.63/24
Dragos Sensor	Dell OEM	CentOS 7	64x vCPU	128 GB	240 GB 1 TB	Testbed LAN 10.100.0.64/24

Table 2-4 Dragos Deployment

2.2.2 Installation

The Dragos platform, which includes the SiteStore server and the Dragos sensor, was delivered as preconfigured hardware appliance by Dragos with the required IP addresses already assigned. The only installation step was correctly connecting the server and the sensor management ports to the Testbed LAN and adding the switch port analyzer (SPAN) port connection to the sensor.

The Dragos Platform Administrator Guide and Dragos Platform User Guide for Release 1.7 were used to guide the installation. Customers can obtain these guides from Dragos.

2.2.3 Configuration

In addition to the standard configuration preset by Dragos, the Dragos Platform was configured to work with OSIsoft PI for alerting on certain conditions.

Configure the Dragos SiteStore Server:

1. Configure the data connection between Dragos SiteStore and OSIsoft PI Server:

a. Once installation is successful, open a browser to access the configuration screen by using the URL https://<SiteStore ip address>/osisoft/#/apps. (Figure 2-4)

Figure 2-4 Dragos OSIsoft PI Server Integration

13 OSSoft Integration	× +		×
← → C ▲ Not secure	e 10.100.0.633/ossent/#yapps		* 0 :
DRAGOS	Configure PrivateAP1 創Mop Elements	: O utrin	€
E Systog			
al	Configure PIWebAPI Configure connection to OSISOR PIWeb-API Exist mapping of OSISOR Elements to Dragos Assets		
CSISON	↔ Qu		
	LAUNCH		

- b. Click **Configuration Pi Web API** to open a screen for filling out the required information, including privacy enhanced mail (PEM) format certificate and password for secure authentication (Figure 2-5).
 - i. Upload the server public key for the HTTPS certificate.
 - ii. Specify the user credentials for the OSIsoft PI Web API interface.
 - iii. Click Save.

Figure 2-5 Dragos PI Web API Configuration

3: Offort Integration x +	- 0
← → C ▲ Not secure 10.100.053/inside/t/#/Configure	* O
	C 😧 atrin E
Goofiqure DiWebADI	
Control Migue PriveDAPI	
POSISIN POSIS	
Page Page Page Page Page Page Page Page	
Fatured	
RESET BANE	
attps://www.sessort/w/wagsiewens	

- c. Click **Map Elements** to access the interface to pair elements between OSIsoft PI Server and the Dragos Platform assets. Here, the PLC in **OSIsoft Elements** panel is paired with Beckhoff asset in the Dragos Platform asset (Figure 2-6).
 - i. Select the OSIsoft Database **CRS-backup** on the left side to access the devices list from the Historian Database.
 - ii. Select the **Default NetworkID RFC 1918** and use the Filer options to find specific assets.
 - iii. For each asset in the OSIsoft Database, select the corresponding asset in the Dragos asset repository and click **Pair Selected**.
 - iv. Repeat this process for each asset until all paired assets are listed in the **Paired Data** table (Figure 2-7).

1) PLC paired to 192.168.0.30

2) Station 1 paired to 192.168.1.101

3) Station 2 paired to 192.168.1.102

4) Station 3 paired to 192.168.1.103

5) Station 4 paired to 192.168.1.104

DRA	COTC & Configure PiWebAPi		
raLog raLog Ball eost?	OSISoft Elements Filer University OSIS And		Dragos Platform Assets Ga Ga Markit Defail Mercitin Markit
	▼ ▼ Vorkel 1 ▼ Vorkel 1 ▼ Station 2 ▼ Station 1 ▼ Station 1 ▼ Station 4 ▼ Station 3	PAR BLICTO	Asset Type Vandor MAC IP Demain Hestsame Networks 15 Ineckloff Aux 000105170001192.190.190.0 - - Default Networks 975 Definition 14/18/7726/74/C 10.100.0.30 - TEVHOSTOI Default Networks
	¥ 38801.3		

Figure 2-7 OSIsoft PI Server and Dragos Paired Data Elements

Paired Data								
Delete	Asset	OSIsoft Name	Туре	Vendor	MAC	IP	Domain	
	15	PLC		Beckhoff Automation GmbH		192.168.0.30		
	3176	Station 2			B0:D5:CC:FE:6E:B1	(2) 192.168.1.102, FE80::B2D5:CCFF:FEFE:6EB1	(2) machining-station-2.local, _tcp.local	
	3186	Station 1			B0:D5:CC:FA:70:C9	(2) 192.168.1.101, FE80::B2D5:CCFF:FEFA:70C9	(2) machining-station-1.local, _tcp.local	
	3180	Station 3			B0:D5:CC:FA:7A:43	(2) 192.168.1.103, FE80::B2D5:CCFF:FEFA:7A43	(2) machining-station-3.local, _tcp.local	
	3177	Station 4			B0:D5:CC:F4:26:EC	(2) 192.168.1.104, FE80::B2D5:CCFF:FEF4:26EC	(2) _tcp.local, machining-station-4.local	

2. Configure Zones

NOTE: Zones are ordered in a similar manner to firewall rules. In other words, higher rules have priority over lower rules.

a. Click **Assets** and select the **Zones** tab (Figure 2-8).

Figure 2-8 Dragos Zone Administration Page

TS	Asset Explorer		♦ 13 \$\frac{1}{2}\$ \$
EL Dashboard	ASSETS	2	IONES
* Map	Q, Search Zones	DETAILED VIEW SUM VIEW + NEW ZONE	C REFRESH ✔ EDIT PARENT ZONES
Assets	E DMZ Lab DMZ	Details Assets: 14 Baseline Assets: 0 Baseline Events: 0 Photocol: 2 External Communications: foise	Asset Criteria ALL: IP14 CIDR Metches CIDR 10 100 1 0/04
Notifications			EDIT DELETE
Content		Details Assette: 3 Baselined Assets: 0 Baseline Events: 0 Protocols: 13 External Communications: faise	Asset Criteria ALL: IPV4 CIDP Metches CIDP 10 100.0.0/24
Reports			P EDIT DELETE
(r) Sensors Admin	ERS - Level 1 ORS Data Collection and Montoring	Details Assets: 25 Baseline Creats: 0 Baseline Creats: 0 Protection: 100 Esternal Communications: 100	Asset Criteria ALL: IPV4 CIDP Matches CIDP 192168.0.024
			EDIT DELETE
 < > ← → 	E CRS - Level 0 CRS Robots and Controllers	Details Assets: 15 Baselined Assets: 0 Baseline Event: 0 Protocols: 10	Asset Criteria ALL: IPV4 CIDR Metches CIDR 192.168.1.0/24

- b. Click + New Zone (Figure 2-9) and define the following zones:
 - i. Name: DMZ:
 - 1) Description: Lab DMZ
 - 2) Zone Criteria (Match ALL):
 - a) IPV4 CIDR Matches CIDR 10.100.1.0/24
 - ii. Name: Testbed LAN:
 - 1) Description: Lab Testbed LAN
 - 2) Auto Zone Criteria (Match ALL):
 - a) IPV4 CIDR Matches CIDR 10.100.0.0/24
 - iii. Name: CRS:
 - 1) Description: Parent CRS
 - 2) No Criteria
 - iv. Name: CRS Level 0:
 - 1) Description: Robots and Controllers
 - 2) Parent Zone: CRS
 - 3) Auto Zone Criteria (Match ALL):
 - a) IPV4 CIDR Matches CIDR 192.168.1.0/24

v. Name: CRS – Level 1:

1) Description: Lab DMZ

2) Parent Zone: CRS

3) Auto Zone Criteria (Match ALL):

a) IPV4 CIDR Matches CIDR 192.168.0.0/24

			-		
Figuro	7 _Q	Dragoe	Crosto	Zono	Don-un
Iguic	2-3	Diagus	CICALC	LOUIC	r op-up

the follo	new Parent Zone wing:				~
the follo	new Parent Zone wing:				Ŧ
the follo	new Parent Zone wing:				Ŧ
the follo	new Parent Zone wing:				~
the follo	wing:				
the follo	wing:				
the follo	wing:				
~	Matches CIDR.	Ŧ	Value 10.100.1.0/24	Ō	
	+ ADD AT	RIBUTE			
the follo	owing:				
the f	follo	following:	following:	following:	following:

2.3 Forescout Platform

The Forescout products included in the practice guide are eyeInspect (formally SilentDefense), eyeSight, ICS Patrol, and Forescout Console. These products are utilized in Build 2 to meet the BAD, hardware modification, firmware modification, and software modification capabilities. The Forescout

implementation utilizes different components and modules installed on different devices to monitor critical networks for anomalies and active query capabilities to retrieve information about endpoints in the PCS environment. A high-level of the key server and agent components is presented in Figure 2-10.



Figure 2-10 Forescout High-Level Components and Dataflows

eyeInspect (formally SilentDefense)

The eyeInspect (Version 4.1.2) control server and monitoring sensor are installed on a single appliance with a management interface on the Testbed VLAN and network monitoring capabilities through a dedicated SPAN port. The SPAN port provides passive monitoring for network-based anomalies and retrieves information about endpoints within the network. The eyeInspect appliance also serves as the command center for supporting the ICS Patrol and eyeSight components.

eyeSight

Forescout eyeSight (Version 8.2.1) provides enhanced network monitoring and response using an agent installed on endpoints. In this build, eyeSight instances are configured through the Forescout Console to provide additional monitoring and reporting information to eyeInspect.

ICS Patrol

Forescout ICS Patrol (Version 1.1.2-4.a826b94) is a sensor that supports active queries for ICS devices to obtain status and other information such as hardware configuration and firmware version. ICS Patrol queries and reporting results are managed through eyeInspect.

Forescout Console

The Forescout Console (Version 8.2.1) is a Java-based application for configuring and managing eyeSight and eyeSight agents. The Forescout Console is installed on a computer with network access to the eyeSight server.

2.3.1 Host and Network Configuration

Forescout was installed and configured to support the PCS Environment as part of Build 2. The overall build architecture is provided in <u>Figure B-2</u> with the Forescout specific components in Table 2-5 and the eyeSight agents in Table 2-6.

Name	System	OS	CPU	Memory	Storage	Network
eyelnspect control server	Dell Embed- ded Box PC 5000	Ubuntu 16.04	Intel i7- 6820EQ	32 GB	250 GB	Testbed LAN 10.100.0.65
Forescout Console	Hyper-V VM	Windows 2012R2	2x vCPU	6 GB	65 GB	Testbed LAN 10.100.0.25
eyeSight Server	Dell R640	Ubuntu 16.04.06	Intel Xeon Sil- ver 4110	32	600 GB	PCS VLAN 2 172.16.2.61
ICS Patrol	VirtualBox VM	Ubuntu 16.04.06	2x vCPU	2 GB	40 GB	PCS VLAN 2 172.16.2.62

Table 2-5 Forescout Deployment

For the lab environment, network connectivity between the components in the Testbed LAN and the components in the PCS environment required the following persistent route configured on Testbed LAN systems:

```
route -p ADD 172.16.0.0 MASK 255.255.252.0 10.100.0.40
```

The following systems were configured to utilize the eyeSight Agents.

Table 2-6 eyeSight Agent Deployment

Name	System	OS	CPU	Memory	Storage	Network
Engineering Workstation	Dell T5610	Windows 7	Intel i5- 4570	16 GB	465 GB	PCS VLAN 3 172.16.3.10
HMI Host	Generic	Windows 7	Intel i5- 4590	8 GB	233 GB	PCS VLAN 1 172.16.1.4

Additional details for Build 2 are available in Section 4.5 of Volume B.

2.3.2 Installation

The Forescout products included in the practice guide are eyeInspect, Forescout Console, ICS Patrol, and eyeSight. These products are installed as indicated in the appropriate subsection below. To support these components, the PCS Gateway/Firewall rules were updated as follows (Table 2-7).

Rule Type	Source	Destination	Port(s)	Purpose
Allow	10.100.0.65	172.16.2.61	22 (ssh)	System Management
			9999	eyelnspect Data
			9092	eyelnspect Data
Allow	10.100.0.65	172.16.2.62	22 (ssh)	System Management
			9001	eyelnspect Data

Table 2-7 Firewall Rules for Forescout

2.3.2.1 eyeInspect

eyeInspect is an appliance hosted on a Dell Embedded Box PC 5000. The unit was placed within a standard datacenter rack unit with the eyeSight appliance and connected to the network as described in Section 2.3.1. SPAN ports from the DMZ, Testbed LAN, and PCS VLAN 1, 2, and 3 switches were routed to the appliance for passive network monitoring. Installation also required uploading the license file after successfully logging onto the appliance.

2.3.2.2 Forescout Console

Forescout Console was installed following the standard installation procedures. Instructions can be found in the Forescout Installation Guide Version 8.2.1 available at <u>https://docs.forescout.com</u>. The software is available from <u>https://forescout.force.com/support/s/downloads</u>, where current and past versions are available. Login credentials were provided by Forescout.

2.3.2.3 eyeSight

Forescout eyeSight is an appliance hosted on a 1U Dell R640 that is installed within a standard datacenter rack and connected to the network as described in the previous section.

2.3.2.4 eyeSight SecureConnector Agent

- In a browser on a system with web connectivity to the eyeSight server, navigate to https://172.16.2.61/sc.jsp to access the SecureConnector download page (Figure 2-11) and follow these steps:
 - a. Select Create SecureConnector for: Windows.
 - b. Enable Show the SecureConnector icon on the endpoint systray.
 - c. Select Install Permanent As Service.
 - d. Click Submit.

- 2. Download the Forescout Agent (Figure 2-12):
 - a. Select Version Win64.
 - b. Click Download.
- 3. Install the downloaded agent on the target systems using an administrator account.

Figure 2-11 Forescout SecureConnector Distribution Tool

prescout SecureConnector Distribution Too	
e this page to download SecureConnector installers. Use these installer e the options below to define SecureConnector deployment options.	rs to distribure SecureConnector to endpoints without direct end user interaction with the Forescout platform.
eate SecureConnector for: ₿ Windows ≧ macOS / OS X	Ç₃
A Linux Show the SecureConnector icon on the endpoint systray. Istall Permanent As Service ▼	
hen SecureConnector runs on endpoints, it creates an encrypted and au s host, the host will automatically reopen the tunnel to the managing Ap icureConnector connects to the Appliance using a TCP connection on:	uthenticated tunnel from the endpoint to this Appliance (192.168.0.41). If this Appliance is not assigned to manage pliance. The tunnel created is used to remotely inspect the host using the SecureConnector agent.
Port 10003 for Windows SecureConnector Port 10005 for macOS / OS X SecureConnector Port 10006 for Linux SecureConnector.	
ste: the Windows SecureConnector installation file name should not be o	changed. Submit

Figure 2-12 Forescout Agent Download

Forescout Agent Download	
Select Version Win32 Win64 Your SecureConnector configuration has been saved and is ready for download. Once downloaded, SecureConnector can be distributed across any network segment using standard distribution methods, for example, you can send the following link via email: https://192.168.0.41/x64/SC-wKgAKScT4INyBjO2vJ0UiZfHEQPNCuDINsUzyFEOorVydcsBoOoEAAEexe	d
Note: If your environment uses overlapping IP addresses, refer to the Forescout Working with Overlapping IP Addresses How to Guide.	
	Download

2.3.2.5 ICS Patrol

Forescout ICS Patrol (Version 1.1.2-4.a826b94) is a sensor that is deployed on an existing VirtualBox host in the PCS environment. Ubuntu 16.04.06 is required for proper installation and can be downloaded from http://old-releases.ubuntu.com/releases/xenial/ubuntu-16.04.6-server-amd64.iso. Install the operating system on a VM connected to PCS VLAN 2 following the procedures from the Silent Defense Installation and Configuration Guide 4.1.2 document Section 2.2.2, Installing the Linux Ubuntu OS.

- Install the ICS Patrol Component from the Silent Defense Installation and Configuration Guide
 4.1.2 document Sections 2.2.4 and 2.2.5 following these steps:
 - a. Establish an SSH session to the eyelnspect appliance.

b. Copy the components to the ICS Patrol VM:

```
$ scp os_provisioning_4.1.1_install.run \
main_configuration_4.1.1_install.run \
silentdefense@172.16.2.62:/home/silentdefense
```

c. SSH to the ICS Patrol VM and execute the installation components:

```
$ chmod a+x *.run
$ sudo ./os provisioning 4.1.1 install.run
$ sudo ./main_configuration_4.1.1_install.run
$ sudo reboot
```

2.3.3 Configuration

The eyeSight agents and ICS Patrol do not require specific configurations.

2.3.3.1 eyeInspect

- 1. Access the eyelnspect web interface and log in with an administrator account.
- 2. Register the local sensor for SPAN traffic monitoring:
 - a. Click the **Sensors** tab to access the Sensor Admin/Overview Page (Figure 2-13).
 - b. Click Add > SilentDefense sensor.
 - c. Specify the sensor parameters in the dialog box (Figure 2-14).

Figure 2-13 eyeInspect Sensor Admin/Overview Page – Add Sensor

<) FORESCOUT	🚯 Dash	board 🚠	Network	Events	Sensors	s 📽 Settings	
Sensors overview	Reload	<u>Add</u> ~	Pause 🛩	IP reuse	domains	Monitored networks	Scans 🗸
SilentDefense sensors		<u>SilentDefer</u> ICS Patrol s	<u>ise sensor</u> sensor				
0 sensors selected		PCAP repla	y sensor				





- 3. Adjust Passive Monitoring settings:
 - a. From the Dashboard, click **Sensors**.
 - b. Select the SilentDefense Sensor from the list of available sensors.
 - c. Click the Industrial Threat Library Overview option in the upper right corner.
 - d. Click the Security menu option on the left under Checks by Category.
 - e. Enter "ICMP" in the Search field to reduce the list of available options.
 - f. Click the **ICMP** protocol/port scan attempt to open the settings dialog box (Figure 2-15) and verify the following settings:
 - i. Verify Enable Check is selected.
 - ii. Verify Maximum occurrences in window is set to 20.
 - iii. Verify Time Window (in seconds) is set to 60.


Figure 2-15 eyelnspect ICMP Protocol/Port Scan Attempt Settings

g. Select Portscan Detection under Built-in Modules (Figure 2-16).

Figure 2-16 eyelnspect Sensor Configuration Options

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

ensor "sensor-bundle	Back Edit Import	Diagnostics	Today's alerts	Share setting	s PCAP ~						?
Sensor attributes		Networ	k whitelists				Netw	ork inte	lligence framework		
Sensor name	sensor-bundle-nccoe	Commi	unication patter	ns (LAN CP)			Indu	strial th	reat library (ITL)		
State	📀 Connected										
Address	localhost	🗌 0 pr	ofiles selected			+	0	library s	elected		
Port	9999		D 🔺 Name		State			Name		State	
IP reuse domains		8	3 TCP comm	nunications	Q Detecting			Indust	ial threat library checks	Active	
Monitored networks		9	UDP comr	nunications	Q Detecting						
		2 profile	25				Custo	om che	cks (SD Scripts)		
Built-in modules								scripts s	elected		
		Protoco	ol fields (DPBI)					ID 🔺	Name	State	
0 modules selected			- 61					10	cve_2019_0708_monitor	Active	
Name	State	L Upr	offies selected					11	CVE_2020_0796_monitor v1.	0 🥑 Active	
Portscan detection	Q Detecting		D 🔺 Name		State			12	CVE-2020-1350 Monitor v1.0	Active	
Man-in-the-middle detectio	n Q Detecting	/	Vo profiles available.					13	ETHIP/CSP - PCCC Monitor v	0.6 🕑 Active	
Malformed packet detection	n Q Detecting	0 profile	es					14	Host and Link Add-Ons v1.2	3 🥑 Active	
Frequent event aggregation	Active							15	HTTP HLI v1.4	Active	
Visual analytics	Active							17	MAC white listing v1.1	🕑 Active	
Event logging	Active							18	MODBUSTCP Monitor v0.8	Active	
								19	MS17_010 Monitor v1.1	Active	
								20	Profinet Monitor v0.3.1	Active	
								22	Ripple20 Monitor v1.0	Active	
								23	Suppress alerts on known- good IPs v1.0	🕑 Active	
								24	Vnet/IP Monitor v0.3	Active	
								25	Host and Link Add-Ons v1.3	Active	
							14 sc	ripts			

- h. Click the **Settings** tab and set the following parameters (Figure 2-17):
 - i. Sensitivity level: User defined
 - ii. Number of Hosts with failed connections to make a distributed scan: 10
 - iii. Detect SYN scans: Checked

- iv. Target detection probability: 0.99
- v. Target FP probability: 0.01
- vi. Detect ACK scans: Checked
- vii. Number of out of sequence ACK packets: 5

Figure 2-17 eyelnspect Portscan Detection Settings

Command Center - Portscan det X	Forescout	Web Client		<u>х т</u>
	Torescout	web client		
$\leftarrow \rightarrow \mathbf{C}$ A Not secure 10.100.0).65/crypt.f	f2S2R1Zg>	k-m8Wp0U	JiwMfJQ/f2Sd6
<) FORESCOUT	🕋 Dasl	hboard	🚠 Net	work 🔳 E
Portscan detection mod	Back	Finish	Reset	Reload
Detection sensitivity				
Sensitivity level	User d	efined	*	
Distributed scans				
Number of hosts with failed connections to make a distributed scan	* 10			
TCP detection options				
Detect SYN scans				
Target detection probability	* 0.99			
Target FP probability	* 0.01			
Detect ACK scans				
Number of out of sequence ACK packets to identify a scan	* 5			

- 4. Register the ICS Patrol Sensor:
 - a. From the Sensor admin page, click **Add > ICS Patrol sensor**.
 - b. Specify the sensor parameters in the dialog box (Figure 2-18).

Figure 2-18 Add ICS Patrol Sensor Dialog

A	dd a new sensor			×
	Sensor name	*	PCS_Sensor	
	Sensor Address	*	172.16.2.62	
	Port	*	9001	
	IP address reuse		O Yes 💿 No	
	Associate monitored network	S	❷ Yes O No	
	Monitored networks	*	Lab LAN (10.100.0.0/24) Collaborative Robotics System (192.168.0.0/23) Process Control System VLAN1 (172.16.1.0/24) Process Control System VLAN2 (172.16.2.0/24) Process Control System Engineering (172.16.3.0/24) Process Control System PLC Data Traffic (172.16.4.0/24) Vec CTRL-Click to select multiple options.	+
	Targetable networks 🕑	*	172.16.1.0/24 172.16.2.0/24	
			172.16.3.0/24 172.16.4.0/24 192.168.0.0/23 10.100.2.0/24 10.100.1.0/24 ▼	
			Use CTRL+Click to select multiple options.	
	Target username	*	silentdefense	
	Target password	*		
				inish

- c. Define a scan policy to periodically check the PCS PLC to monitor for changes.
 - i. Click the PCS Sensor created in the previous step to open the sensor admin page (Figure 2-19).

Figure 2-19 ICS Patrol Sensor Admin Page

) FORESCOUT	🕐 Dashboard	🕂 Network	Events	📽 Se
atrol Sensor "PCS_Sens	Back Edit I	Diagnostics	Scans 🛩	
Sensor Attributes				
Name	PCS_Sensor			
State	Connected			
Address	172.16.2.62			
Port	9001			
Target networks	172.16.2.0/24, 172.16.1.0/2 172.16.3.0/24, 172.16.4.0/2	24, 24		
IP reuse domains				
Monitored Networks	Process Control System Engineering, Process Contr System PLC Data Traffic, Pr Control System VLAN2, Pro Control System VLAN1	rol rocess ocess		

- ii. Click Scans > Scan Policies.
- iii. In the dialog option (Figure 2-20) enter the scanning parameters:
 - 1) Name: PCS PLC
 - 2) Scan Type: EtherNet/IP
 - 3) Target Type: Custom target
 - 4) IP address reuse: No
 - 5) Network Address: 172.16.2.102
 - 6) Schedule: Yes
 - 7) Frequency: Repeat
 - 8) Interval: 1 . Select "Hours" from the drop-down menu.
 - 9) Click Finish.

Figure 2-20 Add an ICS Patrol Scan Policy

Add scan policy				×
Name	* PCS PLC			
Description				11
Scan type	 Active IPS OS/Ports Custom Windows OT Ports Siemens S7 EtherNet/IP 	0		
Target type	 ★ Custom target O Yes O N 	v		
Network addresses	* 172 16 2 102			0
Schedule	© Yes O N	lo		
Frequency	* Repeat	~		
Start date	* Jun 3, 2021 12:0	00:00		
Interval	* 1		Hours 🗸	
				🖺 Finish

2.3.3.2 eyeSight

Using the Forescout Console application, users may configure, monitor, and manage the eyeSight appliance and agents. The Forescout Console is also used to test and verify connectivity to the eyeInspect server.

- 1. Login to the Forescout Console.
- 2. Select the Gear Icon in the upper right corner or the **Tools > Option** menu item to bring up the Options display.
- 3. Enter "Operational" in the search bar.
- 4. Select the **Operational Technology** tab on the left side of the screen to display the current settings.
- 5. Select the IP entry for the Command Center and select **Add** to start the workflow process.

- a. Specify General Information (Figure 2-21):
 - i. Enter the Command Center IP Address "10.100.0.65" for IP Address/Name.
 - ii. Select "172.16.2.61" from the Connecting CounterAct device drop-down menu.
 - iii. Select "443" from the TCP Port drop-down menu.

Figure 2-21 eyeSight Add Dialog – General Information

<	Add Command Center - Step 1							
Add Com	mand Center							
i General	General Set up general communication ForeScout.	parameters between the Com	mand Center and					
	IP Address/Name	10.100.0.65						
	TCP port	443 🗘						
	Connecting CounterACT device	172.16.2.61 🗸						
	<u>H</u> elp Pre	vio <u>u</u> s Next <u>I</u>	inish Cancel					

- b. Click Next.
- c. Enter the command center credentials (Figure 2-22).
- d. Click Finish.

Figure 2-22 eyeSight Add – Command Center Credentials

Add Command Center - Step 2 of 2								
Add Command Center	Command Co Enter access cred	enter Credentials entials to the Command Center.						
	Credentials							
	User name	admin						
	Password	****						
	Confirm password	*****						
Ŀ	lelp Previo <u>u</u> s	Next Finish Ca	ancel					

- 6. Select the IP address for the Command Center and Click **Test** (Figure 2-23). If the connection is successful, a message like the one shown in Figure 2-24 displays.
- 7. Click **Apply** to save the changes.
- 8. Click **Close** to close the message.

Figure 2-23 eyeSight OT Settings

0		Options 172.16	5.2.61	_ D X
Options				
Operational	Operational Tech	nology		
🛄 Operational Technology	The Operational Technol	ogy Module provides comprehensive OT asset inventory us	sing passive device fingerprinting and assessment of OT device vulnerabili	ties.
	Support for Operational T - Sensors monitor endpo - Command Center serv - The Operational Techni Typically OT networks co	echnology endpoints consists of the following components: ints in Operational Technology network segments. Irs manage Sensors and retrieve Sensor data. Jogy Module makes this information available in the Fores ntain overlapping IP addresses. To enable overlapping IP a	: cout Console. ddresses in the Internal Network, go to Options>Advanced>Overlapping IF	s.
	Manage Command Center	Integrated Sensor Standalone Sensor IP Reuse ter instances that report Operational Technology informatic	Domain Mapping	
	,			
	Search	Q		
	Address 🗢	TCP Port	Connecting CounterACT Device	Add
	10.100.0.65	443	172.16.2.61 (Module running)	<u>E</u> dit
				<u>R</u> emove
				Test
				E <u>x</u> port Certificate
				Open Command Center
				<u>S</u> ensor Scripts
				Help Apply Undo

Figure 2-24 eyeSight Test Connection Successful Message

Operational Technology Connectivity Test)
Communication with Command Center succeeded.	
Connectivity Test succeeded	
	Cinse

2.4 GreenTec-USA

The GreenTec-USA products included in this practice guide are the ForceField and WORMdisk zero trust storage devices. These products were utilized in Builds 1, 2, 3, and 4 to meet the File Integrity Checking capability by storing and protecting critical PCS and CRS data from modification and deletion.

ForceField

A ForceField hard disk drive (HDD) provides a protected write-once-read-many data storage location for historian data backups and database backups. Data is immediately protected as it is written to the HDD in real time, permanently preventing the data from modification and deletion.

WORMdisk

A WORMdisk HDD provides a protected data storage location for PLC logic, device firmware, and approved software applications for use in the manufacturing environment. Data is protected by "locking" individual partitions of the HDD using a software utility, permanently preventing the data from modification and deletion.

2.4.1 Host and Network Configuration

The WORMdisk and ForceField HDDs were installed in a rack-mount server appliance provided by GreenTec-USA and described in Table 2-8. The overall build architectures utilizing this appliance and devices are described in Section 4.5 in Volume B.

Table 2-8 GreenTec-USA WORMdrive and ForceField Deployment	

Name	System	OS	CPU	Memory	Storage	Network
GreenTec- USA Server	Supermicro x8 Series Server	Ubuntu 18.04	2x Intel Xeon E5620	16 GB	750 GB OS 1.0 TB WORMdisk 1.0 TB ForceField	DMZ 10.100.1.7

2.4.2 Installation

The ForceField and WORMdisk HDDs were hosted on a hardware appliance provided by GreenTec-USA. The unit was placed within a standard datacenter rack unit and connected to the network as shown in <u>Figure B-1</u>, <u>Figure B-2</u>, <u>Figure B-3</u>, and <u>Figure B-4</u>.

Full documentation and installation guides are provided to customers by GreenTec-USA.

NIST chose to utilize Samba as the network file sharing protocol due to the prevalence of Windows and Linux workstations within the testbed. The GreenTec-USA appliance did not come with Samba preinstalled, so installation was performed via the Ubuntu Advanced Packaging Tool and the Ubuntu package repository.

NOTE: GreenTec-USA typically provides turnkey server storage solutions. Installation and configuration of file sharing packages and other software will likely not be required.

NOTE: Many of the commands used to manage the ForceField and WORMdisk HDDs must be executed by a user with superuser privileges or as the root user.

1. Add the default gateway so the appliance can communicate to other devices on the network using the following command:

```
$ sudo route add default gw 10.100.1.1
```

2. In a terminal window on the GreenTec-USA appliance, execute these commands:

```
$ sudo apt update
$ sudo apt -y install samba
$ sudo ufw allow samba
```

2.4.3 Configuration

The appliance provided by GreenTec-USA for this project was preconfigured with the ForceField HDD as device /dev/sdc and the WORMdisk HDD as device /dev/sdb.

2.4.3.1 ForceField HDD

The ForceField HDD is configured as a mounted volume, allowing the drive to be used as a typical HDD by using native operating system commands.

- 1. Create a mount point (empty directory) for the ForceField HDD using the following command:
 - \$ sudo mkdir /mnt/forcefield
- 2. Start the ForceField WFS volume manager to mount the drive using the following command:
 - \$ sudo /opt/greentec/forcefield/bin/wfs /dev/sdc /mnt/forcefield/

2.4.3.2 WORMdisk HDD

The WORMdisk is divided into 120 partitions to enable periodic updates and revisions to the protected data (i.e., data in the "golden" directory). Once a partition is locked it cannot be modified, so the next sequential partition on the drive is used as the new "golden" directory.

1. Format the WORMdisk with 120 partitions (NOTE: this operation must be performed from the command line as administrator on a computer with the Microsoft Windows OS) using the following command:

```
> gt format.exe 1 /parts:120
```

2. In the Ubuntu OS, create the mountpoint for the WORMdisk HDD partition using the following command:

```
$ sudo mkdir /mnt/golden
```

3. Add a persistent mount to the /etc/fstab file:

```
$ sudo echo "/dev/sdb2 /mnt/golden fuseblk
rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other,blksize
=4096 0 0" >> /etc/fstab
```

- 4. Create a directory structure within the "golden" directory and copy approved files into those directories (e.g., PLC logic, device firmware, approved software).
- 5. Once all files have been copied and verified, lock the partition to protect the data:
 - \$ sudo /greentec/Ubuntu/wvenf /dev/sdb2

When it is time to create a new "golden" partition, the partition names in the /etc/fstab file must be updated to point to the correct partition. The following instructions provide an example process to update the files and increment the golden partition from /dev/sdb2 to /dev/sdb3.

1. On the GreenTec-USA appliance, create a temporary directory, mount the folder to the next unlocked WORMdisk partition, and copy existing "golden" files to the temporary directory:

```
$ sudo mkdir /mnt/tmp
$ sudo mount /dev/sdb3 /mnt/tmp
$ sudo cp -R /mnt/golden /mnt/tmp
```

- 2. Update the files and folders in the temporary directory, /mnt/tmp, as desired.
- 3. Unmount the temporary directory and lock the partition:

```
$ sudo umount /mnt/tmp
$ sudo /greentec/Ubuntu/wvenf /dev/sdb3
```

4. Stop the Samba service:

```
$ sudo systemctl stop smb.service
```

5. Unmount the golden partition:

\$ sudo umount /mnt/golden

6. Modify the /etc/fstab file with the new partition name and save the file:

```
/dev/sdb3 /mnt/golden fuseblk
rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other,blksize
=4096 0 0"
```

7. Re-mount all partitions, start the Samba service, and remove the temporary directory:

```
$ sudo mount -a
$ sudo systemctl stop smb.service
$ sudo rmdir -r /mnt/tmp
```

2.4.3.3 Samba

1. Add local user accounts to the appliance for accessing the network file shares and create a password:

```
$ sudo adduser nccoeuser
$ sudo smbpasswd -a nccoeuser
```

2. Open the file /etc/samba/smb.conf and add the following content to the end of the file to create the individual shares:

```
# GreenTec-USA ForceField Share
strict sync=no
# OSIsoft PI historian and database backups
[ForceField]
```

```
browsable = yes
guest ok = no
path = /mnt/forcefield
read only = no
writeable = yes
case sensitive = yes
# GreenTec-USA Golden WORMDisk Share
[golden]
browsable = yes
guest ok = no
path = /mnt/golden
read only = no
writeable = yes
case sensitive = yes
```

3. Restart Samba:

\$ sudo systemctl restart smbd.service

2.4.3.4 OSIsoft PI Server and Database Backups

Create the scheduled backup task to backup PI Data Archive files. The script automatically inserts the current datetime stamp into the filename of each file copied to the ForceField drive. Follow these steps:

- 1. On the server containing the PI Data Archive, open a command prompt with Administrator privileges.
- 2. Change to the PI\adm directory:

```
> cd /d "%piserver%adm"
```

3. Create the backup directory, and start the Windows scheduled task to perform the backup:

```
> pibackup h:\PIBackup -install
```

Create a scheduled task to copy the backup files to the ForceField HDD. Follow these steps:

1. Open the Task Scheduler and create a new scheduled task to rename, timestamp, and copy the backup files to the ForceField HDD:

Trigger: At 3:30 AM every day

Action: Start a Program

```
Program/script:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

```
Add arguments (optional):-Command { Get-ChildItem -Path
"h:\PIBackup\arc\" | foreach { copy-item -path $($_.FullName) -
destination "\\10.100.1.7\ForceField\$(Get-Date -f yyyy-MM-
dd HHMMss) $($ .name)" } }
```

2.5 Microsoft Azure Defender for IoT

Microsoft Azure Defender for IoT, based on technology acquired via CyberX, consists of a single appliance containing the sensor and application interface integrated into Build 4 to meet BAD, hardware modification, firmware modification, and software modification capabilities. The Microsoft Azure Defender for IoT implementation utilizes passive monitoring and protocol analysis to support cybersecurity monitoring and threat detection.

2.5.1 Host and Network Configuration

Microsoft Azure Defender for IoT was installed and configured to support the CRS environment as part of Build 4. The overall build architecture is provided in <u>Figure B-4</u>. The Microsoft Azure Defender for IoT specific components are in Table 2-9.

Name	System	OS	CPU	Memory	Storage	Network
Azure Defender for IoT	Dell OEMR XL R340	Ubuntu 18.04	Intel Xeon E- 2144G	32 GB	3x 2 TB Drives RAID-5	Testbed LAN 10.100.0.61

2.5.2 Installation

The Microsoft Azure Defender for IoT (Version 10.0.3) appliance was preinstalled with the operating system and application. The appliance is mounted in a rack with power and network interfaces connected to the Testbed LAN on the EthO port along with the SPAN connection on the expansion network interface board.

2.5.3 Configuration

To configure the Microsoft Azure Defender for IoT platform, follow these steps:

- 1. Set the Network Configuration:
 - a. Using either SSH, iDRAC, or the KVM Console connections on the appliance, establish shell access to the appliance.
 - b. From the console, enter the following command:

\$sudo cyberx-xsense-network-reconfigure

- c. The system will walk through a series of network options (Figure 2-25) that are set as follows:
 - i. IP Address: "10.100.0.61"
 - ii. Subnet Mask: "255.255.255.0"
 - iii. **DNS**: "10.100.0.17"

- iv. Default Gateway: "10.100.0.1"
- v. Hostname: Not set
- vi. Input Interface(s): "enp3s0f3, enp1s0f2, enp3s0f1, enp1s0f0, enp1s0f3, enp3s0f2, enp1s0f1, enp3s0f0"
- vii. Bridge Interface(s): Not Set

Figure 2-25 Azure Defender for IoT SSH Session for Network Configuration

IP: 10.100.0.61 SUBNET: 255.255.255.0 GATEWAY: 10.100.0.1 UID: 4C4C4544-0050-4C10-8034-C2C04F363133
Hint: Num Lock on
xsense login: cyberx Password: Last login: Fri Feb 12 13:23:21 UTC 2021 on tty1
System information as of Fri Feb 12 13:24:03 UTC 2021
System load:2.15Processes:212Usage of /:1.6% of 1.56TBUsers logged in:0Memory usage:39%IP address for eno1:10.100.0.61Swap usage:0%IP address for docker0:172.17.0.1
cyberx@xsense:~\$ sudo cyberx-xsense-network-reconfigure Isudo] password for cyberx: starting "/usr/local/bin/cyberx-xsense-network-reconfigure"
management network IP address is set to "10.100.0.61". Edit? [y/N]: n
subnet mask is set to "255.255.255.0". Edit? [y/N]: n
DNS is set to "10.100.0.17". Edit? [y/N]: n
default gateway IP address is set to "10.100.0.1". Edit? [y/N]: n
hostname is set to "". Edit? [y/N]: n
input interface(s) is set to "enp3s0f3,enp1s0f2,enp3s0f1,enp1s0f0,enp1s0f3,enp3s0f2,enp1s0f1,enp3s0f0". Edit? [y/N]: n
bridge interface(s) is set to "". Edit? [y/N]: n
WARNINGT to apply settings, system will be rebooted and you will be disconnected from your active session. Are you sure you wish to proceed? [Y/n]:

- 2. Create AMS Protocol report as a data mining tool:
 - a. Login to the application web interface and click **Data Mining** in the left menu navigation.
 - b. Click the + sign and click **New Report**. In the **Create New Report** panel set the following settings (Figure 2-26):
 - i. Under Categories select AMS to automatically select the sub-elements, including:
 - 1) AMS Firmware Information
 - 2) AMS Index Group
 - 3) AMS Index Group Offset

4) AMS Protocol Command

- ii. Enter "AMS Data Analysis" as the name for the report.
- iii. Click Save.

Figure 2-26 Azure Defender for IoT Create New Data Mining Report for AMS Protocol Information

Microsoft		Data Mining					
		+ 💌 Main V	Create new Report				
			Categories (All):		Name:		
		Suggested	Protocol Versions Unresolved Connections	•	AMS Data Analysis		
Device Inventory			User Access Per Protocol	i.	Description:		
Alorte (26)			60870-5-104	L	Description		
	-		IEC-60870-5-104 ASDU Types			1	
		Programming Com	ABB TOTALFLOW		Save to Reports Page		on Act
		Reports	ABB Totalflow File Operations ABB Totalflow Firmware Versions		Order By:		
	Ê		ABB Totalflow Register Operations		Category Activity		
Data Mining	▶.		AMS		Filters: (Add)	Only results within the last Minutes 🗸	
		=	 AMS Firmware Information AMS Index Group 		Device Group		
	A		 AMS Index Group Offset AMS Protocol Command 			· · · · · · · · · · · · · · · · · · ·	
Attack Vectors	\bigcirc	AMS	BACNET		IP Address	Ex: 10.2.1.0, 10.2.*.*	
			BACNet Object Access BACNet Routes		Port		
Custom Alarta					Port	EX: 80, HTTP; HTT^	
			Tunneling Traffic		MAC Address	Ex: 00:10:*:ff:*:*	
	÷		CDP	-			
	Õ						
	\$					Close	
	1					Close Save	

3. Create AMS – Custom Alert Rules

For this effort, the CRS PLC is configured to run using firmware version 3.1.4022 as the approved production firmware version. To detect changes to the approved version, custom alert rules are created to monitor for deviations from the approved version numbers through the AMS protocol messages over the network.

- a. Click Horizon on the left menu navigation.
- b. Select AMS > Horizon Customer Alert under the Plugin Options on the left menu.
- c. Create Custom Alert to Detect Change in PLC Firmware Major Build Number (Figure 2-27):
 - i. Enter "PLC Firmware Major Build Mismatch" as the title for the custom alert.
 - ii. Enter "PLC {AMS_server_ip} Firmware Major Version Build Mismatch Detected" as the message to display with the alert.
 - iii. Set the following conditions:

1) AMS_server_ip == 3232235550 (Note: this is the PLC IP address 192.168.0.30 in Integer format).

2) AND AMS_major ~= 3

			-			-						
Ci,	auro	2_27	Azuro	Dofondor	for IoT	Custom	Alort f	or Eirmword	Maior	Vorsion	Numbor	Change
Г Ц	guie	<u> </u>	AZUIC	Delelluel		Custom	AICIU			VEISIOII	INUITIDEL	Change

AMS - Custom Alert Rules

Trigger custom AMS alerts based o	on traffic detected on this Sensor
-----------------------------------	------------------------------------

Title				
PLC Firmware Major Build Mismatch Message				
PLC (AMS.server_ip) Firmware Major Version Build Mismatch Detec	ted			
Use {} to add variables to the message Conditions Variable Operator Value AMS.server_ip Value 3232235:	ANDAND	Variable AMS.major	Operator Value	⊕
CLEAR SAVE				

- d. Create the custom alert to detect change in PLC firmware minor build number (Figure 2-28):
 - i. Enter "PLC Firmware Minor Build Mismatch" as the title for the custom alert. PLC Firmware Minor Build Mismatch
 - ii. Enter "PLC {AMS_server_ip} Firmware Minor Version Build Mismatch Detected" as the message to display with the alert.
 - iii. Set the following conditions:
 - 1) AMS_server_ip == 3232235550 (Note: this is the PLC IP address 192.168.0.30 in Integer format).
 - 2) AND AMS_minor ~= 1

Figure 2-28 Azure Defender for IoT Custom Alert for Firmware Minor Version Number Change

AMS - Custom Alert Rules

Trigger custom AMS alerts based on traffic detected on this Sensor.

le				
PLC Firmware Minor Build Mismatch				
lessage)		
PLC {AMS.server_ip} Firmware Minor Build Mismatch Detected				
conditions				
Variable Operator Value AMS.server_ip 3232235 323223 323223 3232 3232 323 3232 323 323 323 323 323 323 323 323 323 323 32 3 32 32 3 3 32 3 3 3 32 32 3 3 3 3 3	Variable AMS.minor	Operator Value	⊕⊖	

- e. Create the custom alert to detect change in the PLC Firmware Build Version (Figure 2-29):
 - i. Enter "PLC Firmware Build Version Mismatch" as the Title for the custom alert.
 - ii. Enter "PLC {AMS_server_ip} Build Version Mismatch Detected" as the message to display with the alert:
 - iii. Set the following conditions:

1) AMS_server_ip == 3232235550 (Note: this is the PLC IP address 192.168.0.30 in Integer format).

2) AND AMS_version_build ~= 4022

Figure 2-29 Azure Defender for IoT Custom Alert for Firmware Build Version Number Change

AMS - Custom Alert Rules

ger dason And dens based on runne detected on this densor.				
Title				
PLC Firmware Build Version Mismatch				
Message				
PLC {AMS.server_ip} Build Version Mismatch Detected				
Use () to add variables to the message Conditions Variable Operator Value AMS.server_ip	ANDAND	Variable AMS.version_build	Operator Value	⊕ ⊝
CLEAR SAVE				

2.6 OSIsoft PI Data Archive

The OSIsoft product included in this practice guide is Process Information (PI), which is used to collect, store, analyze, and visualize testbed data. The product was utilized in Builds 1, 2, 3, and 4 to meet the historian capability by collecting and storing testbed data and the BAD capability by alerting when activity deviates from a baseline.

OSIsoft PI is a suite of software applications for capturing, analyzing, and storing real-time data for industrial processes. Although the PI System is typically utilized as a process historian, the PI System is also utilized to collect, store, and manage data in real time. Interface nodes retrieve data from disparate sources to the PI Server, where the PI Data Archive resides. Data is stored in the data archive and is accessible in the assets defined in the Asset Framework (AF). Data is accessed either directly from the data archive or from the AF Server by using tools in the PI visualization suite.

2.6.1 Host and Network Configuration

PI was installed on virtual machines hosted on hypervisors located in the DMZ and CRS networks. The virtual machine details and resources are provided in Table 2-10, Table 2-11 and, Table 2-12. The overall build architectures utilizing PI are described in Section 4.5 in Volume B.

Name	System	OS	CPU	Memory	Storage	Network
DMZ Histo- rian	Virtual Machine	Microsoft Windows Server 2016	4x Intel Xeon E3-1240	8 GB	Boot: 80 GB PI Data: 170 GB	DMZ 10.100.1.4

Table 2-10 OSIsoft PI Domain Hosts Deployment

Table 2-11 OSIsoft PI CRS Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
CRS Local Historian	Virtual Machine	Microsoft Windows Server 2016	4x Intel Xeon E5-2407	16 GB	Boot: 80 GB PI Data: 170 GB	CRS Supervi- sory LAN 192.168.0.21

Table 2-12 OSIsoft PI PCS Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
PCS Local	Virtual	Microsoft Windows	1x Intel i5-	2 GB	50 GB	PCS VLAN 2
Historian	Machine	Server 2008 R2	4590			172.16.2.14

2.6.2 Installation

PI was previously installed in the testbed as part of the NISTIR 8219: Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection,

<u>https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf</u>. The installation for this project involved upgrading the existing CRS Local Historian and DMZ Historian VMs to Microsoft Windows Server 2016, and subsequently upgrading all the PI software components. Step-by-step instructions for each PI component installation are not included for brevity. Detailed instructions provided by the vendor can be found on the OSIsoft Live Library: <u>https://livelibrary.osisoft.com/</u>.

DMZ Historian Server

The following software is installed on the DMZ Historian server:

- Microsoft SQL Server 2019 Express 15.0.2080.9
- PI Server 2018 (Data Archive Server, Asset Framework Server)
- PI Server 2018 SP3 Patch 1
- PI Interface Configuration Utility version 1.5.1.10
- PI to PI Interface version 3.10.1.10
- PI Interface for Ramp Soak Simulator Data 3.5.1.12
- PI Interface for Random Simulator Data 3.5.1.10
- PI Connector Relay version 2.6.0.0
- PI Data Collection Manager version 2.6.0.0
- PI Web API 2019 SP1 version 1.13.0.6518

CRS Local Historian Server (Collaborative Robotics System)

The following software is installed on the CRS Local Historian server:

- Microsoft SQL Server 2019 Express 15.0.2080.9
- PI Asset Framework Service 2017 R2 Update 1
- PI Data Archive 2017 R2A
- PI Server 2018 SP3 Patch 1
- PI Interface Configuration Utility version 1.5.1.10
- PI to PI Interface version 3.10.1.10
- PI Interface for Ramp Soak Simulator Data 3.5.1.12
- PI Interface for Random Simulator Data version 3.5.1.10
- PI Interface for Performance Monitor version 2.2.0.38
- PI Ping Interface version 2.1.2.49
- PI Interface for Modbus ReadWrite version 4.3.1.24
- PI Interface for SNMP ReadOnly version 1.7.0.37

- PI TCP Response Interface version 1.3.0.47
- PI Processbook 2015 R3 Patch 1 version 3.7.1.249
- PI Vision 2019 Patch 1 version 3.4.1.10
- PI System Connector version 2.2.0.1

PCS Local Historian (Process Control System Historian)

Rockwell FactoryTalk Historian SE version 1.00

2.6.3 Configuration

The following sections describe how to configure select PI components to enable the capabilities described in this guide. Configurations for the other PI components are not included for brevity.

2.6.3.1 PI to PI Interface (PCS)

The PCS uses the Rockwell FactoryTalk Historian to collect, store, and analyze historical process data. The PI to PI Interface is used to duplicate the process data to the DMZ Historian server. The following steps describe how to configure the PI-to-PI Interface to collect data from the Rockwell FactoryTalk Historian.

1. On the DMZ Historian server, launch the **PI Interface Configuration Utility** as shown in Figure 2-30 from the Start menu and sign in with the local administrator account.

	= 🖬 🔂 🕵 🖀 🞯	
nterface: select - Type: - none - Description: /ersions:	▼ <	PI Data server Connection Sta
General Interface Service UniInt 	General Point Source: Interface ID: Scan Classes Scan Frequency Scan Class #	PI Host Information Server/Collective: SDK Member: API Hostname: User: Type: Version: Port: Interface Installation Path Interface Batch Filename

Figure 2-30 Screenshot of the PI Interface Configuration Utility before the Interface is configured.

- 2. On the top menu, click Interface > New Windows Interface Instance from BAT File...
- 3. Navigate to E:\Program Files (x86)\PIPC\Interfaces\PItoPI and select the file PItoPI.bat_new.
- 4. In the "Select Host PI Data server/collective" dialog box, select **PI-DMZ** from the drop-down menu and click **OK**.
- 5. In the left navigation panel select **PItoPI**. In the Source host textbox, enter "172.16.2.4".
- 6. In the left navigation panel, select **Service**. In the "Create / Remove" section click the **Create** button. Click **Yes** in the dialog box.
- Enter the commands net start PItoPI and net stop PItoPI in the files pisrvsitestart.bat and pisrvsitestop.bat files, respectively. Save and close the files.
- 8. At the bottom of the **PI Interface Configuration Utility** click the **Apply** button. On top menu bar click the green play button **>** to start the service.

9. Close the **PI Interface Configuration Utility**. The interface is now configured to pull tags from the Rockwell Historian.

2.6.3.2 PI System Connector (CRS)

The PI System Connector is used to duplicate process data on the DMZ Historian from the CRS Local Historian server. The following steps describe how to configure the PI-to-PI Interface to collect data from the OSIsoft PI Server.

Figure 2-31 Screenshot of the PI Data Collection Manager Displaying Green Checkmarks After the PI System Connector is Properly Configured

PI Data Collection Manager	× +				o –		×	
\leftrightarrow \rightarrow C \cong pi-dmz:54	61/ui/config				☆		:	
PI Data Collection Manager								
Components	omponents Routing							
Filter Components	Filter Options	Data Sources	Connectors	Relays 🤆	Destinations	\oplus		
Data Sources			CDD Connector			7		
🕑 CRS-DS		CRS-DS	PI System Co	PI-DMZ-Relay	→ ♥ 10.100.1.4			
Connectors								
CRS-Connector F	Pl System Connector							
Relays								
PI-DMZ-Relay							्र	
Destinations	*							
2 10.100.1.4	PI Server							
							vlew	
					Edit Routing Configu	iration	Over	

- 1. On the DMZ Historian server, launch the **PI Data Collection Manager** as shown in Figure 2-31 from the Start menu and sign in with the local administrator account.
 - a. Click + on the Relays column to add a new connector relay. Use the following settings:
 - b. Name: PI-DMZ-Relay
 - c. Address: 10.100.1.4
 - d. Port: 5460
- 2. Username: .\piconnrelay_svc
- 3. Click Save Settings to add the connector relay.
- Click + Add Destination to add the target PI Data Archive and PI AF Server. Use the following settings:
 - a. Name: 10.100.1.4

- b. PI Data Archive Address: 10.100.1.4
- c. AF Server: 10.100.1.4
- 5. Click **Save Settings** to add the destination.
- 6. On the CRS Local Historian server, open the **PI System Connector Administration** from the Start menu and sign in with the local administrator account.
- 7. Click **Set up Connector** to create a new connector.
- 8. Use the following information to request registration:
 - a. Registration Server Address: https://PI-DMZ:5460
 - b. Registration Server Username: piconnrelay svc
 - c. Registration Server Password:
 - d. Description: Registration to PI-DMZ
- 9. Click Request Registration to send the request to the DMZ Historian server.
- 10. On the DMZ Historian server, open the **PI Data Collection Manager** from the Start menu and sign in with the local administrator account.
- 11. Click **Untitled Connector 1** and click **Approve This Registration and Configure** to approve the PI System Connector registration.
- 12. In the Untitled Connector 1 details panel, click Edit.
- 13. Use the following information to create the CRS-Connector connector:
 - a. Name: CRS-Connector
 - b. Description: Registration to PI-DMZ
- 14. Click **Save Settings** to create the CRS-Connector.
- 15. Click **CRS-Connector** in the **Connectors** column. On the **Overview** panel click **CRS-Connector**: **No Data Sources** option to create the data source.
- 16. On the CRS-Connector Connector Details in the Overview panel, click + Add Data Source.
- 17. In the Data Source Settings window, use the following settings:
 - a. Name: CRS-DS
 - b. Source AF Server: PI-Robotics
 - c. Source AD Database: TestbedDatabase
 - d. Select Collect All Data from this Entire Database.
- 18. Click **Save** to save the data source.

- Click 10.100.1.4 in the Destination column of the Routing panel and then click Data in the 10.100.1.4 Destination Details panel to configure the destination database for the CRS-Connector.
- 20. In the **10.100.1.4 Destination Details** panel, change from **Change Default Settings for new connectors** to "CRS-Connector" and then click **Edit Destination Data Settings.**
- 21. In the **10.100.1.4 Destination Details** of the **Overview** panel, use the following settings:
 - a. Change the connector to CRS-Connector.
 - b. Database: CRS-backup
 - c. Click on Elements and it will change <select a path using the tree below> to \$Elements\
 - d. Use default settings in Root AF Elements and Point Names.
 - e. Create root Element CRS-Connector checkbox: Checked
 - f. Prefix Point CRS-Connector checkbox: Checked
- 22. Click Save Destination Data Settings to save the configuration.
- 23. Click the white space in the **Routing** panel.
- 24. Click CRS-Connector: No Relays in the Overview panel.
- 25. Select the PI-DMZ-Relay checkbox in the Routing panel.
- 26. Click the white space in the **Routing** panel again, then **Click PI-DMZ-Relay: No Destination** to add the routing between relays and destinations.
- 27. Select the 10.100.1.4 checkbox to add the routing between the relay and the destination.
- 28. Click Save Configuration.
- 29. In the **Save Routing and Data Configuration** window, select **Save and Start All Components** to continue.
- 30. Each box should now contain a green checkmark (i.e., Data Sources, Connectors, Relays, and Destinations). The elements in the AF database "testbeddatabase" on CRS Local Historian server is now replicated to AF database "CRS-backup" on the DMZ Historian server.
- 31. Finally, create a Windows firewall rule to open the inbound ports 5460, 5461, 5471, and 5472.

2.6.3.3 PI Asset Template Analysis Functions and Event Frames

Analysis functions and event frame templates were created to generate alerts in the PLC asset template when their respective anomalous events are detected. When an analysis function result is TRUE, an event frame is generated from the event frame template and ends when the analysis function result is FALSE or per a user-defined function. The following steps describe how the "Station Mode Error" analysis function and event frame template were created and used in Scenario 10.

- On the CRS Local Historian server, open the PI System Explorer by navigating to Start Menu > PI System > PI System Explorer.
- 2. On the left navigation panel, select Library.
- 3. In the navigation tree in the Library panel, select Templates > Event Frame Templates.
- 4. Right click in the whitespace of the **Element Templates** window and select **New Template**.
 - a. Enter the following:
 - b. Name: Station Mode Error
 - c. Description: CRS Workcell machining station mode error
- 5. Naming Pattern: ALARM-%ELEMENT%.%TEMPLATE%.%STARTTIME:yyyy-MM-dd HH:mm:ss.fff%
- 6. In the navigation tree in the Library panel, select Templates > Element Templates > Machining_Station.
- 7. In the Machining_Station panel select the Analysis Templates tab and click Create a new analysis template.
- 8. Enter the name "Station Mode Error" in the **Name** textbox, enter a description of the analysis in the Description textbox, and select the option "Event Frame Generation" for the **Analysis Type**.
- 9. Select "Station Mode Error" in the Event Frame template drop-down menu.
- 10. In the **Expression** field for "StartTrigger1", enter the expression:

```
'RawMode' < 0 OR 'RawMode' > 1;
```

11. Click the Add... drop-down menu and select End Trigger, and enter the expression:

```
('RawMode' > 0 AND 'RawMode' < 1)
```

- 12. Select the "Event-Triggered" option for the Scheduling type.
- 13. Click the **Check In** button on the top menu to save all changes to the database.

2.6.3.4 PI Web API

The PI Web API is used by Dragos to collect event frames from the DMZ Historian server. After completing installation of the PI Web API, the "Change PI Web API Installation Configuration" dialog displays. The following steps describe how to configure the Web API on the DMZ Historian server.

- 1. In the Telemetry section, verify the checkbox option and click Next.
- 2. In the **Configuration Store** section, select "PI-ROBOTICS" in the Asset Server drop-down menu and click **Connect**. Leave the default instance name.
- 3. In the Listen Port section, verify port 443 is entered in the Communication Port Number textbox and check the Yes, please create a firewall Exception for PI Web API checkbox.

- 4. In the **Certificate** section, click **Next** to continue and use the self-signed certificate or select **Change** to modify the certificate.
- 5. In the API Service section, leave the default service NT Service \piwebapi and click Next.
- 6. In the Crawler Service section, leave the default service NT Service\picrawler and click Next.
- 7. In the Submit URL section, enter the URL of the DMZ Historian server Web API service: https://pi-dmz/piwebapi/. Click Next.
- 8. In the **Review Changes** section, verify all the configuration settings, check the checkbox Accept all the configurations, and click **Next**.
- 9. Click **Finish** to complete the configuration.

2.6.3.5 Firmware Integrity Checking

Software was developed to demonstrate the ability of PI to obtain device and firmware data from a Beckhoff PLC for integrity checking purposes. A new PLC task was programmed to periodically query its operating system for hardware and software telemetry and make it available via Modbus TCP. PI will query these Modbus registers and use analysis functions to generate event frames if any tags do not match their expected values.

It is important to note that this capability was developed to demonstrate a method of maintaining visibility of PLC hardware and firmware version numbers for integrity purposes and is not secure or infallible. If a malicious actor takes control of the PLC, the hardware and firmware versions provided by the PLC can be spoofed.

The following steps describe how to sequentially configure this capability across multiple systems and software. Only one system or software is described in each section.

Beckhoff PLC Modbus TCP Server

The base Modbus TCP server configuration file only allows one PLC task to write to the registers. The following steps describe how to modify the configuration to allow two PLC tasks to write to the Modbus TCP server input registers.

- 1. Log in to the Windows CE Desktop of the Beckhoff PLC and open the XML file: \TwinCAT\Functions\TF6250-Modbus-TCP\Server\TcModbusSrv.xml
- 2. Modify the <InputRegisters> ... </InputRegisters> section to the following:

```
<InputRegisters>
   <MappingInfo>
        <AdsPort>851</AdsPort>
        <StartAddress>32768</StartAddress>
        <EndAddress>32895</EndAddress>
        <VarName>GVL.mb_Input_Registers</VarName>
        </MappingInfo>
        <AdsPort>852</AdsPort>
        <StartAddress>32896</StartAddress>
        <EndAddress>32896</StartAddress>
        <VarName>GVL.mb_Input_Registers</varName>
        </MappingInfo>
        <AdsPort>852</AdsPort>
        <StartAddress>32896</StartAddress>
        <VarName>GVL.mb_Input_Registers</varName>
        </MappingInfo>
        </mapp
```

- 3. Save and close the file.
- 4. Restart the PLC.

The Modbus TCP server will now have two register address ranges: 128 addresses for the PLC task at port 851, and 128 addresses for the PLC task at port 852.

Beckhoff PLC Project

A new PLC task must be created to perform the integrity checking and write the data to the Modbus TCP registers. The following steps describe how to create and configure the new task.

- On the engineering workstation, open the TwinCAT XAE Shell by navigating to Start Menu > Beckhoff > TwinCAT XAE Shell and open the current PLC project.
- 2. In the Solution Explorer, right click PLC and select Add New Item...
- 3. In the Add New Item dialog box, select Standard PLC Project, enter the name FirmwareIntegrityCheck in the Name textbox, and click Add.
- 4. In the **Solution Explorer**, double click **SYSTEM > Tasks > PLCTask1**. Verify the **Auto Start** checkbox is checked and change the **Cycle Ticks** textbox to 100 ms.
- 5. In the Solution Explorer, right click PLC > FirmwareIntegrityCheck > References and click Add library... In the dialog box, select the library System > Tc2_System and click OK.
- 6. In the **Solution Explorer**, right click **PLC** > **GVLs** and click **Add** > **Global Variable List**. In the dialog box enter the name GVL in the **Name** textbox and click **Open**.
- 7. In the **Editor Window**, enter the following code:

```
VAR_GLOBAL
   mb_Input_Registers : ARRAY [0..127] OF WORD;
END_VAR
```

- In the Solution Explorer, right click PLC > FirmwareIntegrityCheck > POU (Program Organizational Unit) and select Add > POU. In the Add POU dialog box, enter the name GetSystemInfo, select the type Function Block, select the Implementation Language Structured Text (ST) and click Open.
- 9. In the Editor Window, enter the following code in the Variables section:

```
// Gathers PLC information for system integrity checking
// (e.g., PLC serial number, TwinCAT version).
FUNCTION BLOCK GetSystemInfo
VAR INPUT
     NetId : T AmsNetId; // AMS network ID of the PLC
END VAR
VAR OUTPUT
     HardwareSerialNo : WORD; // Serial number of PLC
     TwinCATVersion : WORD; // Version number of TwinCAT
     TwinCATRevision : WORD; // Revision number of
TwinCAT
     TwinCATBuild : WORD; // Build number of TwinCAT
END VAR
VAR
     DeviceData : FB GetDeviceIdentification; //PLC data
struct
     Timer : TON; // Timer to trigger the scan
     Period : TIME := T#5M; // Amount of time between
each scan
     State : INT := 0; // Function block state
END VAR
```

10. In the Editor Window, enter the following code in the Code section:

```
CASE state OF
     0:
           // Start a new request for device
identification
           DeviceData (bExecute:=TRUE, tTimeout:=T#100MS,
sNetId:=NetId);
           // Switch to the next state once the request
completes
           IF DeviceData.bBusy = FALSE THEN
                 state := 10;
           END IF
     10:
           // Store the interesting data into our internal
variables
           HardwareSerialNo :=
STRING TO WORD (DeviceData.stDevIdent.strHardwareSerialNo);
           TwinCATVersion
                           :=
STRING TO WORD(DeviceData.stDevIdent.strTwinCATVersion);
           TwinCATRevision :=
STRING TO WORD(DeviceData.stDevIdent.strTwinCATRevision);
           TwinCATBuild
                            :=
STRING TO WORD (DeviceData.stDevIdent.strTwinCATBuild);
           // Reset the timer and move to the next state
           Timer(IN:= FALSE);
           state := 20;
     20:
           // Make sure the timer is running and change to
the
         // next state once the period has been reached
           Timer(IN:=TRUE, PT:=Period);
           IF Timer.Q = TRUE THEN
                 state := 0;
           END IF
END CASE
```

- 11. Save and close the POU.
- 12. In the Solution Explorer, double click PLC > FirmwareIntegrityCheck > POUs > MAIN (PRG).
- 13. In the **Editor Window**, enter the following into the **Variables** section (your AMS net ID may differ from what is shown below):

```
PROGRAM MAIN
VAR
PLCInfo : GetSystemInfo; // Periodically collects
PLC data
SelfNetId : T_AmsNetId := '5.23.219.8.1.1'; // Local
address
END_VAR
```

14. In the Editor Window, enter the following into the Code section:

```
// Captures hardware serial numbers and TwinCAT version
// numbers from the PLC and shares them with other
// devices via Modbus TCP.
PLCInfo( NetId:=SelfNetId,
    HardwareSerialNo => GVL.mb_Input_Registers[0],
    TwinCATVersion => GVL.mb_Input_Registers[1],
    TwinCATRevision => GVL.mb_Input_Registers[2],
    TwinCATBuild => GVL.mb_Input_Registers[3]
);
```

- 15. Save and close the POU.
- 16. In the top menu, select Build > Build Project. Once the build process completes select PLC > Login. In the TwinCAT PLC Control dialog box, select Login with download, verify the Update boot project checkbox is checked, and click OK. If the PLC code is not running after the download completes, select PLC > Start in the top menu.
- 17. The firmware integrity checking code is now running on the Beckhoff PLC. In the top menu select **PLC > Logout** and close the TwinCAT XAE Shell.

The PLC will now write the hardware serial number and firmware version numbers to the Modbus TCP server registers.

OSIsoft PI Points

The following steps describe how to create the PI points and tags in the CRS Local Historian server and duplicate the tags to the DMZ Historian server.

- On the CRS Local Historian server, open the PI Interface Configuration Utility by navigating to Start > All Programs > PI System > PI Interface Configuration Utility.
- 2. In the Interface drop-down menu, select Modbus Interface (PIModbusE1).
- 3. Select the General menu option. In the Scan Classes section, click New Scan Class.
- 4. Set the **Scan Frequency** to "60" and the **Scan Class #** to the next sequential class number as shown in Figure 2-32 below.

Figure 2-32 Screenshot of the PI Interface Configuration Utility Showing the Added Scan Class # 2 for Polling the PLC Every 60 Seconds

PI Interface Configu	ration Utility - PIModbusE1		- 🗆 X		
Interface Tools Help					
🎦 🗃 🗙 🖬 🕨	= s 💫 🐘 🔳 🞯				
Interface: Robotics Mo	dbus Interface (PIModbusE1) -> PI-ROBOTICS		▼ Rename		
Type: ModbusE	PI Data server Connection Status PI-ROBOTICS				
Description:					
Versione: DIMadhus E		Vriteable			
	Unlint Version 4.7.1.6	DILL LL C. I.			
General	General	PI Host Information			
Service	Point Source: MODBUSE 라	Server/Collective	PI-ROBOTICS		
UniInt	MODBUSE	SDK Member:	PI-ROBOTICS		
- Failover		API Hostname:	PI-ROBOTICS		
Performance Counters	Interface ID: 1	User:	piadmins PIWorld		
- Performance Points	, , , , , , , , , , , , , , , , , , ,	Type:			
PI SDK	Scan Classes	Version	PI 2 4 425 604		
Disconnected Startup		Version.	F13.4.433.604		
IO Rate	Scan Frequency Scan Class #	Port:	5450		
Interface Status					
	√ 60 ∠	Interface Installation	on Path		
		E:\Program Files (x86)\PIPC\Interfaces\Modbus		
		Interface Batch Fil	ename		
		PIModbusE1 bat			
	1	J. Milododde Libur			
,			Close Apply		
Ready	Running PIModbusE1	- Installed			

- 5. Click **Apply** and close the program.
- On the CRS Local Historian server, open the PI System Management Tools by navigating to Start Menu > PI System > PI System Management Tools.
- 7. In the System Management Tool panel, select **Points > Point Builder**.
- 8. Create a new tag for the PLC hardware serial number with the following configuration:
 - a. Name: PLC-HardwareSerialNumber
 - **b.** Server: PI-ROBOTICS
 - c. Descriptor: Hardware serial number of the CRS Beckhoff PLC
 - d. Point Source: MODBUSE
 - e. Point Type: Int16

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

- f. Location 1:1
- g. Location 2: 0
- h. Location 3:104
- i. Location 4: 2
- j. Location 5: 32897
- k. Instrument Tag: 192.168.0.30
- 9. Create a new tag for the PLC TwinCAT build number with the following configuration:
 - a. Name: PLC-TwinCATBuildNumber
 - b. Server: PI-ROBOTICS
 - c. Descriptor: Build number of the CRS PLC TwinCAT firmware.
 - d. Point Source: MODBUSE
 - e. Point Type: Int16
 - f. Location 1:1
 - g. Location 2: 0
 - h. Location 3:104
 - i. Location 4: 2
 - j. Location 5: 32900
 - k. Instrument Tag: 192.168.0.30

10. Create a new tag for the PLC TwinCAT revision number with the following configuration:

- a. Name: PLC-TwinCATRevisionNumber
- b. Server: PI-ROBOTICS
- c. Descriptor: Revision number of the CRS PLC TwinCAT firmware.
- d. Point Source: MODBUSE
- e. Point Type: Int16
- f. Location 1: 1
- g. Location 2: 0
- h. Location 3:104
- i. Location 4: 2

- j. Location 5: 32899
- **k.** Instrument Tag: 192.168.0.30
- 11. Create a new tag for the PLC TwinCAT version number with the following configuration as shown in Figure 2-33:
 - a. Name: PLC-TwinCATVersionNumber
 - **b.** Server: PI-ROBOTICS
 - c. Descriptor: Version number of the CRS PLC TwinCAT firmware.
 - d. Point Source: MODBUSE
 - e. Point Type: Int16
 - f. Location 1: 1
 - g. Location 2:0
 - h. Location 3:104
 - i. Location 4: 2
 - j. Location 5: 32898
 - k. Instrument Tag: 192.168.0.30
- 12. Close the **PI System Management Tools** program. The PI points are now available to the DMZ Historian server via the PI System Connector.

Figure 2-33 Screenshot of the PI System Management Tools Component After Configuring the PI Points for PLC Hardware and Firmware Version Number Integrity Checking

🔆 Point Builder - Pl System Management Tools (Administrator) – 🗌 🗙									
File View Tools Help									
Servers	4 point								
Search P	Server	Name	Stored Values	Point Source	Point Type	Point Class	Descriptor	Point Security	Data Security
PI-ROBOTICS	PI-ROBOTICS PI-ROBOTICS PI-ROBOTICS PI-ROBOTICS	PLC-Hardware Serial Number PLC-TwinCATBuild Number PLC-TwinCATRevision Number PLC-TwinCATVersion Number	Real-time data Real-time data Real-time data Real-time data	MODBUSE MODBUSE MODBUSE MODBUSE	Int 16 Int 16 Int 16 Int 16	classic classic classic classic		padmin: A(rw) [piadmins: A(rw) [PISC. A(rw)] PIWork: A(r) padmin: A(rw) [piadmins: A(rw) [PISC. A(rw)] PIWork: A(r) padmin: A(rw) [piadmins: A(rw) [PISC. A(rw)] PIWork: A(r) piadmin: A(rw) [piadmins: A(rw) [PISC. A(rw)] PIWork: A(r)	piadmin: Afr.w) [piadmins: Afr.w) [PISC: Afr.w) [PIWold: Afr.) piadmin: Afr.w) [piadmins: Afr.w) [PISC: Afr.w) [PIWold: Afr.) piadmin: Afr.w) [piadmins: Afr.w) [PISC: Afr.w) [PIWold: Afr.) piadmin: Afr.w) [piadmins: Afr.w) [PISC: Afr.w) [PIWold: Afr.)
System Management Tools	Table C >								
Search P	General Archive Cassic Security System								
> Alarms > Alarms > Data > Interfaces > IT Points > Operation > Points > Operation > Points > Operations Point Source Equations Point Source Table Totalizers > Security	General Archive Cassic Security System Location1: 1 Conversion Factor: 1 UserInt 1: 0 Location2: 0 Files Code: 0 UserInt 1: 0 Location3: 104 Square Root Code: 0 UserReal1: 0 Location5: 32809 Total Code: 0 UserReal2: 0 Instrument Tag: 192.168.0.30								
14M nisdmin nisdmins PlWodd	Jession Necon	u							
plaurinis, Privolia									

- 13. On the DMZ Historian server, open **PI System Explorer** by navigating to **Start Menu > PI System > PI System Explorer**.
- 14. On the left navigation panel, select Library.
- 15. In the navigation tree in the **Library** panel, select **Templates > Element Templates >** PLCTemplate.
- 16. Open the **Attribute Templates** tab in the **PLCTemplate** panel.
- 17. On the top menu bar, click **New Attribute Template** and create a new attribute for the PLC hardware serial number by entering the following configuration:
 - a. Name: HardwareSerialNumber
 - b. Description: Hardware serial number of the CRS Beckhoff PLC.
 - c. Value Type: Int16
 - d. Data Reference: PI Point
 - e. Tag: \\PI-ROBOTICS\PLC-HardwareSerialNumber
- 18. On the top menu bar click **New Attribute Template** and create a new attribute for the expected hardware serial number by entering the following configuration:
 - a. Name: HardwareSerialNumber-Expected
 - **b. Description**: Expected hardware serial number of the CRS Beckhoff PLC.
 - c. Value Type: V
 - d. Data Reference: None
- 19. On the top menu bar, click **New Attribute Template** and create a new attribute for the PLC TwinCAT build number by entering the following configuration:
 - a. Name: TwinCATBuildNumber
 - b. Description: Build number of the CRS PLC TwinCAT firmware.
 - c. Value Type: Int16
 - d. Data Reference: PI Point
 - e. Tag: \\PI-ROBOTICS\PLC-TwinCATBuild
- 20. On the top menu bar, click **New Attribute Template** and create a new attribute for the PLC TwinCAT revision number by entering the following configuration:
 - a. Name: TwinCATRevisionNumber
 - b. Description: Revision number of the CRS PLC TwinCAT firmware.

- c. Value Type: Int16
- d. Data Reference: V
- e. Tag: \\PI-ROBOTICS\PLC-TwinCATRevision
- 21. On the top menu bar, click **New Attribute Template** and create a new attribute for the PLC TwinCAT version number by entering the following configuration:
 - a. Name: TwinCATVersionNumber
 - b. Description: Version number of the CRS PLC TwinCAT firmware.
 - c. Value Type: Int16
 - d. Data Reference: PI Point
 - e. Tag: \\PI-ROBOTICS\PLC-TwinCATVersion
- 22. On the top menu bar, click **New Attribute Template** and create a new attribute for the string representation of the version, revision, and build numbers by entering the following configuration:
 - a. Name: TwinCATVersion
 - b. Description: Version number of the CRS PLC TwinCAT firmware.
 - c. Value Type: String
 - d. Data Reference: String Builder
 - e. String:

'TwinCATVersionNumber';.;'TwinCATRevisionNumber';.;'TwinCAT BuildNumber';

- 23. On the top menu bar click, **New Attribute Template** and create a new attribute for the PLC expected TwinCAT version number by entering the following configuration as shown in Figure 2-34:
 - a. Name: TwinCATVersion-Expected
 - **b.** Description: Expected version number of the CRS PLC TwinCAT firmware.
 - c. Value Type: String
 - d. Data Reference: None

The PI points are now available as PLC attributes in the Asset Framework on the DMZ Historian server.

Figure 2-34 Screenshot of PI System Explorer Displaying some Attributes of the PLC Element. Attributes for the TwinCAT version number are visible in the list.



OSIsoft PI Analyses and Event Frames

The following steps describe how to create the PI analyses and event frame templates to generate event frames when the hardware or firmware version numbers do not match the expected values.

- 1. In the navigation tree in the **Library** panel, select **Templates > Event Frame Templates**.
- 2. On the top menu bar click **New Template** and enter the following configuration as shown in Figure 2-35:
 - a. Name: Hardware Serial Number Mismatch
 - b. Naming pattern: %ELEMENT% %ANALYSIS% (Expected:

```
%@.\Elements[.]|HardwareSerialNumber-Expected%, Detected:
%@.\Elements[.]|HardwareSerialNumber%) %STARTTIME:yyyy-MM-
dd HH:mm:ss.fff%
```
Figure 2-35 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Event Frame Template.

File View Go Tools Help	,				
🔕 Database 🛅 Query Date 👻 🔇 🥥	🔾 Back 🔘 💐	Check In 🧐 🖌 🛃 Refresh	🗃 New Template 🔹	Search Element	Templates 🔎
Library	Hardware Serial I	Number Mismatch			
CRS-backup	General Attribut	te Templates			
🐨 Templates	Name:	Hardware Serial Number Mismato	h		
Event Frame Templates	Description:				
BatchEventFrameTemp	Base Template:	<none></none>	Severity:	Major	~
HighTroubleCallCount	Categories:		Default Attribu	te: <none></none>	~
InspectionFailure	Naming Pattern: [%ELEMENT% %ANALYSIS% (Expected: %@. \Elements[.] HardwareSerialNumber-Expected%, Dete +				
StationDoorFault		Allow Extensions Can B	e Adknowledged 🗌 Base	Template Only	
StationOutORSunc >	0.00	Extended Properties (0) Locati	on <u>Reason</u> <u>Security</u>		
	Find:	Derived Templates Event Fram	es Referenced Pa	arent Templates	
Elements		Derived Ev	ent Frames Referenced C	niid Templates	
Event Frames					
Library					
unit of Measure					
AA -	-				
and Contacts					

- 3. On the top menu bar, click **New Template** and enter the following configuration as shown in Figure 2-36:
 - a. Name: TwinCAT Version Mismatch
 - b. Naming pattern: %ELEMENT% %ANALYSIS% (Expected: %@.\Elements[.]|TwinCATVersion-Expected%, Detected: %@.\Elements[.]|TwinCATVersion%) %STARTTIME:yyyy-MM-dd HH:mm:ss.fff%

Figure 2-36 Screenshot of PI System Explorer Displaying the TwinCAT Version Mismatch Event Frame Template

Q \\PI-DMZ\CRS-backup - PI System Ex	plorer (Administrat	tor)		- 0	×
File View Go Tools Help					
🔕 Database 🛅 Query Date 🔹 🔇 🥥	3 Back 🕤 💐	Check In 🧐 🖌 🛃 Refresh 🔡 New	Template 🔹	Search Element Templat	tes 🔎 🔻
Library	TwinCAT Version	Mismatch			
HighTroubleCallCount A	General Attribut	te Templates			
HighWorkcellTemperati	Name:	TwinCAT Version Mismatch			
RobotProximityFault	Description:				
StationDoorFault	Base Template:	<none> ~</none>	Severity:	Major	~
StationOutOfSync	Categories:	Ø	Default Attribute:	<none></none>	~
TwinCAT Version Misma	Naming Pattern:	%ELEMENT% %ANALYSIS% (Expected: %	@. \Elements[.] Twin	CATVersion-Expected%, Detect	ed: 🤊 🕨
		Allow Extensions Can Be Acknowle	dged 🗌 Base Ter	mplate Only	
Enumeration Sets		Extended Properties (0) Location Reaso	n <u>Security</u>		
< >	Find:	Derived Templates Event Frames	Referenced Paren	nt Templates	
Elements		Derived Event Frames	Referenced Child	Templates	
🔛 Library					
m Unit of Measure					
A Contacts					
🔆 Management					
TwinCAT Version Mismatch Modified:11/1	9/2020 11:00:48 AM	I Owner:PI-DMZ\piadmin			

- 4. Click **Check In** on the top menu to save all changes to the database.
- 5. In the navigation tree in the Library panel, select Templates > Element Templates > PLCTemplate.
- 6. Open the **Analysis Templates** tab in the **PLCTemplate** panel and click **Create a new analysis template**.
- 7. Enter the following configuration as shown in Figure 2-37:
 - a. Name: Hardware Serial Number Mismatch
 - b. Description: The PLC hardware serial number does not match the expected serial number.
 - c. Analysis Type: Event Frame Generation
 - d. Enable analyses when created from template: Checked
 - e. Generation Mode: Explicit Trigger
 - f. Event Frame Template: Hardware Serial Number Mismatch
- 8. In the **Expression** field for "StartTrigger1", enter the expression:

'HardwareSerialNumber'<>'HardwareSerialNumber-Expected' and NOT BadVal('HardwareSerialNumber');

9. Click Add... drop-down menu and select End Trigger, and enter the expression:

```
'HardwareSerialNumber'='HardwareSerialNumber-Expected';
```

10. Select the "Event-Triggered" option for the **Scheduling** type and "Any Input" for the **Trigger On** drop-down menu.

Figure 2-37 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Analysis Template in the PLC Element Template

INPI-DMZ\CRS-backup - PI System Ex	plorer (Administrator)				- 0	×
File View Go Tools Help						
🔕 Database 🛗 Query Date 🔹 🕔 🥥	🥝 Back 💿 🖳 Check In 🧐 🖌 👩 Refresh 📓 New Template 👻			Search	n Element Templates	· Q •
Library	PLCTemplate					
CRS-backup	General Attribute Templates Ports Analysis Templates Notification Rule Templates					
Element Templates		Name:	Hardware Serial Number Mismatch			
Machining_Station	🔕 🗷 Name	Description:	The PLC hardware serial number do	es not match the expe	cted serial number.	
PLCTemplate Event Frame Templates	Hardware Serial Number Mismatch	Categories:				~
- Model Templates	H TwinCAT Firmware Version Mismatch	Analysis Type	: 🔿 Expression 🔿 Rollup 🤅	Event Frame Generation	ation O SQC	
					match	
Tables Categories Attribute Categories Attribute Categories Attribute Categories Attribute Categories Attribute Categories Table Categories Table Categories Table Categories	Example Dement: CASt Connector WorkCell Type Generation Mode: Explicit Trigger Add Name Expression Start trigger1 Start Trigger1 'HandwareSerialNumber'<' 'HandwareSerialNumber-Expect: Endtrigger 'HandwareSerialNumber'=' HandwareSerialNumber-Expected	Create a new notification rule template for Hardware Senal Number Mismatch ame Template Hardware Senal Number Mismatch True for Sevenity ther-Expected' and NOT BadVal('HardwareSerialNumber') Set (aptional) Major ier-Expected'				
- Event Framer	•					
Library				Advanced Ev	vent Frame Settings	
m Unit of Measure						
A Contactr	Scheduling: Event-Triggered Periodic					
Management	Trigger on Any Input					
PLCTemplate Modified:11/19/2020 11:11:	sz AM Uwner:PI-UMZ\piconnrelay_svc					

- 11. To create a new analysis template for TwinCAT firmware version mismatch, click **Create a new analysis template**.
- 12. Enter the following configuration as shown in Figure 2-38:
 - a. Name: TwinCAT Firmware Version Mismatch
 - **b.** Description: The TwinCAT version installed in the PLC does not match the expected version.
 - c. Analysis Type: Event Frame Generation
 - d. Enable analyses when created from template: Checked
 - e. Generation Mode: Explicit Trigger

- f. Event Frame Template: Hardware Serial Number Mismatch
- 13. In the **Expression** field for "StartTrigger1", enter the expression:

not Compare('TwinCATVersion','TwinCATVersion-Expected') and NOT
BadVal('TwinCATVersion');

14. Click the Add... drop-down menu and select End Trigger, and enter the expression:

Compare('TwinCATVersion', 'TwinCATVersion-Expected');

15. Select the "Event-Triggered" option for the **Scheduling** type and "Any Input" from the **Trigger On** drop-down menu.

Figure 2-38 Screenshot of PI System Explorer Displaying the TwinCAT Firmware Version Mismatch Analysis Template in the PLC Element Template

*							
\\PI-DMZ\CRS-backup - PI System Ex	plorer (Administrator)				- 0	×	
File View Go Tools Help							
🔕 Database 🛅 Query Date 🔹 🕔 🗐	🔇 Back 💿 💐 Check In 🤧 🖌 🖻 Refresh 📓 New Template 👻			Search	h Element Templates	P -	
Library	PLCTemplate						
CRS-backup	General Attribute Templates Ports Analysis Templates Notification Rule Templates						
Element Templates		Name:	TwinCAT Firmware Version Mismatch				
Machining_Station	💿 🗃 Name	Description:	The TwinCAT version installed in the	PLC does not match	the expected version.		
PLCTemplate	Hardware Serial Number Mismatch	Categories:					
Model Templates	H TwinCAT Firmware Version Mismatch	Analysis Type:	○ Expression ○ Rollup ●	Event Frame Genera	ation O SQC		
1 Transfer Templates		✓ Enable and	alyses when created from template	æ			
Reference Types		Create a new	notification rule template for TwinCAT	Firmware Version M	lismatch		
- Tables	Example Element: CRS-Connector\Workcell 1\PLC						
Table Connections							
Analysis Categories	Generation Mode: Explicit Trigger v Event Frame Template: Twi	nCAT Version Misn	natch			~	
Attribute Categories	Add v				Evaluate		
····· 📺 Notification Rule Categories	Name Expression	Name Expression True for					
Reference Type Categories Table Categories	Start triggers						
Table Conceptines	StartTrigger1 not Compare('TwinCATVersion', 'TwinCATVersion-Expected') and NOT BadVal('TwinCATVersion') Set (opti						
	E End trigger						
	EndTrigger Compare('TwinCATVersion', 'TwinCATVersion-Expected')					•	
						1	
Elements							
Herent Frames							
🟭 Library				Advanced E	vent Frame Settings		
🚥 Unit of Measure						_	
A Contacts	Scheduling: Event-Triggered Periodic						
💥 Management	Trigger on Any Input v						
TwinCAT Firmware Version Mismatch Mo	dified:11/19/2020 11:27:16 AM Owner:PI-DMZ\piadmin					i	

- 16. On the top menu bar click **Check In**, verify the changes in the dialog box and click **Check In**.
- 17. On the left navigation panel, select **Elements**.
- 18. In the navigation tree in the **Elements** panel, select **CRS-Connector > Workcell 1 > PLC.**
- 19. Open the **Attributes** tab in the PLC panel.
- 20. Select the attribute **HardwareSerialNumber-Expected** and enter the expected hardware serial number (e.g., 5870) in the **Value** textbox.

- 21. Select the attribute **TwinCATVersion-Expected** and enter the expected hardware serial number (e.g., 3.1.4022) in the **Value** textbox.
- 22. On the top menu bar and click **Check In**, verify the changes in the dialog box, and click **Check In**.

Event frames will now be generated in the DMZ Historian if the PLC reports a hardware serial number that does not match the expected value or if the TwinCAT firmware version number does not match the expected value.

2.7 Security Onion

Security Onion is a Linux-based, open source security playbook. It includes numerous security tools for intrusion detection, log management, incident response, and file integrity monitoring. For this project, the tool Wazuh was used in Builds 2 and 4 for file integrity checking. Wazuh works at the host-level to detect unusual and unauthorized activity and changes to file and software configurations. Security Onion and Wazuh use Elastic Stack components, Elasticsearch, Filebeat, and Kibana to store, search, and display alert data.

Note: Wazuh is a fork of the open source project OSSEC, a host-based intrusion detection system. In some places in Wazuh and this document, the term OSSEC will be used in place of Wazuh.

2.7.1 Host and Network Configuration

Wazuh is an agent-based software. For this project, an existing Security Onion server was used, and the Wazuh agent was installed on multiple endpoints in both the PCS and CRS environments. The tables below list the network configuration for the Security Onion server (Table 2-13) and the hosts (Table 2-14 and Table 2-15) with the installed agent.

Name	System	OS	CPU	Memory	Storage	Network
Security On-	Hyper-V VM	Ubuntu 16.04	4	16GB	450GB	Testbed LAN
ion server		LIS				10.100.0.26
Nessus VM	Hyper-V VM	Windows	2	6GB	65GB	Testbed LAN
		2012R2				10.100.0.25
Dispel VDI	Hyper-V VM	Windows 2016	2	8GB	126GB	DMZ LAN
						10.100.1.61
DMZ Histo-	Hyper-V VM	Windows 2016	4	8GB	80GB/171GB	DMZ LAN
rian						10.100.1.4

Table 2-14 Security Onion PCS Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
PCS Engineer- ing Work- station	HP Z230 Tower PC	Windows 7	4	16GB	465GB	PCS LAN 3 172.16.3.10
PCS HMI Host	Supermicro Z97X-Ud5H	Windows 7	4	8GB	600GB	PCS LAN 1 172.16.1.4

Table 2-15 Security Onion CRS Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
CRS Engi- neering Workstation	Dell Preci- sion T5610	Windows 10	8	16GB	465GB	CRS Supervi- sory 192.168.0.20

2.7.2 Installation

Security Onion Server version 3.9 and Wazuh Agent version 3.9 were used.

Installation of Wazuh involves setting up the central server and installing agents on hosts that needed to be monitored.

Security Onion server contains the Wazuh manager and API components as well as the Elastic Stack. The Wazuh manager is responsible for collecting and analyzing data from deployed agents. The Elastic Stack is used for reading, parsing, indexing, and storing alert data generated by the Wazuh manager.

The Wazuh agent, which runs on the monitored host, is responsible for collecting system log and configuration data and detecting intrusions and anomalies. The collected data is then forwarded to the Wazuh manager for further analysis.

The Security Onion server was already a part of the lab infrastructure prior to this effort. For the server component installation process, please follow the guidance from the Security Onion Installation Guide for version 3.9 available at <u>https://documentation.wazuh.com/3.9/installation-guide/index.html</u>.

For information on adding agents to the server, please follow the guidance from the Security Onion Installation Guide for version 3.9 available at https://documentation.wazuh.com/3.9/user-manual/registering/index.html.

2.7.3 Configuration

- 1. Configure Additional Directories or Files for Wazuh Agent File Integrity Monitoring:
 - a. Files and directories to be monitored are specified in the ossec.conf file on each host.

i. To view or edit this file, click the **View** tab in the Wazuh Configuration Manager on the host machine and select View Config as shown in Figure 2-39.

Figure 2-39 Wazuh Agent Manager

😽 Wazuh	Agent	Manager X				
Manage	View	Help				
-Wazuh Agent:	١	/iew Logs /iew Config				
Status: Running						
Manager IP: 10.100.0.26 Authentication key: MDA3IFBJLURNWiAxMC4xMD/						
Save Refresh						
https://wa	zuh.cor	m Revision 3937				

b. Selecting View>View Config opens the ossec.conf file in Notepad. Alternatively, the file can be opened in Notepad from its location in the "C:\Program Files (x86)\ossec-agent" directory on the host machine, as shown in Figure 2-40.

Figure 2-40 ossec.conf File

```
<!-- Directories added for NCCOE Project -->
<directories check_all="yes" whodata="yes">C:\testscenarios</directories>
<directories check_all="yes" whodata="yes">C:\testscenarios</directories>
<directories check_all="yes" whodata="yes">C:\EngWorkstation_Share</directories>
<directories check_all="yes" whodata="yes">C:\EngWorkstation_Share</directories>
<directories check_all="yes" whodata="yes">C:\EngWorkstation_Share</directories>
<directories check_all="yes" whodata="yes">C:\EngWorkstation_Share</directories>
<directories check_all="yes" whodata="yes">C:\Program Files (x86)\ControlFLASH</directories>
<directories check_all="yes" whodata="yes">C:\Users\Administrator\Documents</directories>
<directories check_all="yes" whodata="yes">C:\Users\Administrator\Documents</directories>
<directories check_all="yes" whodata="yes">C:\Users\Administrator\Documents</directories>
<directories check_all="yes" whodata="yes">C:\Users\Administrator\Documents</directories>
<directories check_all="yes" whodata="yes">C:\Users\Administrator\Downloads</directories>
<directories check_all="yes">C:\Users\Administrator\Downloads</directories>
<directories check_all="yes">C:\Users\Administrator\Downloads</directories>
</directories check_all="yes">C:\Users\Administrator\Downloads</directories>
</directories check_all="yes">C:\Users\Administrator\Downloads</directories>
</dim>
```

c. To add files or directories to the default configuration, copy and modify an existing line in the ossec.conf file to ensure the proper XML syntax is used.

d. Once the changes are made, save the ossec.conf file and restart the Wazuh Agent by opening the Configuration Manager, selecting the **Manage** tab, and **Restart** as shown in Figure 2-41.

Figure 2-41 Wazuh Agent Manager User Interface

Manage View Help						
Start Stop Restart - 10.100.1.4						
Status						
Exit Manager IP: JI00.0.26						
Authentication key: MDA3IFBJLURNWiAxMC4xMD/						
Save Refresh						
https://wazuh.com Revision 3937						

e. Changes to the files or directories specified in the ossec.conf file will be detected and sent to the Wazuh Manager. Figure 2-42 shows the log received after a file change was detected.

Figure 2-42 Log Received After a File Change Was Detected

ଷ୍ୟ 🛙 ¥ 1
Q Q Ⅲ ★ BXZRLXUB1YHtrLLybilF
🝳 🔾 🖽 🗰 seconion:logstash-ossec-2020.10.15
ଷ୍ୟ∏ ★ -
Q Q II ★ doc
Q Q II # 005
Q Q 🗇 🗰 🛦 172.16.3.10
Q, Q, Ⅲ ★ PCS-EWS
Q Q II ★ 7
Q Q Ⅲ # "Bad word" matching
Q Q □ ★ syscheck_integrity_changed
Q Q Ⅲ ★ Integrity checksum changed.
Q Q Ⅲ ★ <mark>ossec</mark>
<pre>Q Q □ ★ File 'c:\users\administrator\downloads\ra\test.txt' checksum changed. Size changed from '0' to '4' Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e' New md5sum is: '098f06d4621d373cade4e832627b4f6' Old shalsum was: 'da39a3ee5e6b4b0d3255bfef95601890afd80709' New shalsum is: 'a94a6fe5ccl199a6f1c4c0873d391e987982fbbd3' Old sha256sum was: 's196d6081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08' Old modification time was: 'Thu Oct 15 17:31:38 2020', now it is 'Thu Oct 15 17:31:49 2020' (Audit) User: 'Administrator (S-1-5-21-239850103-4004920075-3296975006-500)' (Audit) Process id: '9532' (Audit) Process name: 'C:\Windows\System32\notepad.exe'</pre>

2.8 TDi ConsoleWorks

The TDi ConsoleWorks implementation in Builds 1 and 3 consists of a single VM hosted on VMWare ESXi to meet the user authentication and authorization capabilities. ConsoleWorks provides a secure web interface through which authenticated and authorized users receive access to graphical and shell interfaces on configured ICS components.

2.8.1 Host and Network Configuration

ConsoleWorks resides on a VM that was reconfigured for supporting Builds 1 and 3 as described in Table 2-16 and Table 2-17 respectively.

Table 2-16 ConsoleWorks Build 1 Deployment

Name	System	OS	CPU	Memory	Storage	Network
ConsoleWorks	VMWare VM	CentOS 7	8x vCPU	8GB	500 GB	Testbed LAN
					750 GB	10.100.0.53

Table 2-17 ConsoleWorks Build 3 Deployment

Name	System	OS	CPU	Memory	Storage	Network
ConsoleWorks	VMWare VM	CentOS 7	8x vCPU	8GB	500 GB	CRS
					750 GB	192.168.0.65

2.8.2 Installation

ConsoleWorks version 5.3-1u3 is installed on a CentOS 7 operating system using the following procedures. Product installation guides and documentation are available at https://support.tditechnologies.com/product-documentation. Follow these steps for installation:

- 1. Harden and configure the operating system:
 - a. Log in to the system with privileged access and set the Static IP Address information by editing */etc/sysconfig/network-scripts/ifcfg-eth0* using the following settings:
 - i. For Build 1 use the following network configuration:
 - 1) IP Address: 10.100.0.53
 - 2) Subnet Mask: 255.255.255.0
 - 3) Gateway: 10.100.0.1
 - 4) DNS: 10.100.0.17
 - ii. For Build 3 use the following network configuration:
 - 1) IP Address: 192.168.0.65

2) Subnet Mask: 255.255.255.0

3) Gateway: 192.168.0.2

4) DNS: 10.100.0.17

iii. Restart the network service as follows:

systemctl restart network

- b. Set the NTP Configuration as follows:
 - i. In */etc/ntp.conf*, add as the first server entry:

server 10.100.0.15

- c. Apply the following Department of Defense (DOD) Security Technology Implementation Guide (STIG) settings:
 - i. Ensure ypserv is not installed using the following command:

```
# yum remove ypserv
```

ii. Ensure Trivial File Transfer Protocol (TFTP) is not installed using the following command:

yum remove tftp-server

iii. Ensure RSH-SERVER is not installed using the following command:

```
# yum remove rsh-server
```

iv. Ensure File Transfer Protocol (FTP) is not installed using the following command:

yum remove vsftpd

v. Ensure TELNET-SERVER is not installed using the following command:

```
# yum remove telnet-server
```

vi. Configure SSH to use SSHv2 only.

```
1) To disable SSHv1, ensure only Protocol 2 is allowed in the /etc/ssh/sshd_config.
```

```
Protocol 2
PermitRootLogin no
Ciphers aes128-ctr, aes192-ctr, aes256-ctr, aes128-
cbc
MACs hmac-sha2
```

vii. Disallow authentication using an empty password as follows:

1) Add PermitEmptyPasswords no to /etc/ssh/sshd_config file.

- 2) Remove any instances of the **nullok** option in /etc/pam.d/system-auth and /etc/pam.d/password-auth files.
- viii. Enable FIPS Mode as follows:

1) FIPS mode can be enabled by running the command:

```
# yum install dracut
# dracut -f
```

2) When step 1) is complete, add **fips=1** to the /etc/default/grub file and run the command:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

3) When step 2) completes, reboot the server with this command:

reboot

ix. Enable server auditing

1) Ensure events on the server are being recorded for investigation in the event of an outage or attack. This can be enabled by running the command:

```
# systemctl start auditd.service.
```

x. Configure system to only install approved digitally signed packages:

 Configure yum to verify the Certificate Authority is from an approved organization. To enable this, ensure that gpgcheck=1 is in the /etc/yum.conf file.

xi. Enable the firewall:

1) To enable the firewall, run the following commands:

yum install firewalld and

- # systemctl start firewalld.
- 2) Check Firewall Zone and confirm only SSH and HTTPS is allowed. Note: the default zone is Public and SSH is already permitted. For the implementation, we checked the configuration using the following command:

firewall-cmd --list-all

3) Add the HTTPS configuration to the firewall using the following command:

```
# firewall-cmd --zone=public --permanent --add-
service=https
```

xii. Enable SELinux and set to "targeted":

1) Add SELINUX=enforcing and SELINUXTYPE=targeted in the /etc/selinux/config file and then reboot the server with this command:

reboot

- xiii. Enable Antivirus as follows:
 - ClamAV is used for the lab implementation using the following commands adapted from information found on https://www.clamav.net/documents/clam-antivirus-user-manual:

yum install -y epel-release

yum -y install clamav-server clamav-data clamav-update clamav-filesystem clamav clamavscanner-systemd clamav-devel clamav-lib clamavserver-systemd

2) Update SELinux policy to allow ClamAV to function

setsebool -P antivirus_can_scan_system 1

3) Make a backup copy of the scan.conf file and update to remove the Example string from the file using these commands:

cp /etc/clamd.d/scan.conf /etc/clamd.d/scan.conf.bk

sed -i '/^Example/d' /etc/clamd.d/scan.conf

4) Uncomment the following line from /etc/clamd.d/scan.conf:

LocalSocket /var/run/clamd.scan/clamd.sock

5) Configure freshclam to automatically download updated virus definitions using these commands:

cp /etc/freshclam.conf /etc/freshclam.conf.bak

sed -i -e "s/^Example/#Example/" /etc/freshclam.conf

6) Manually run freshclam to confirm the settings as follows:

freshclam

7) Start and enable the clamd service with these commands:

systemctl start clamd@scan

systemctl enable clamd@scan

8) Ensure log directory is available with this command:

mkdir /var/log/clamav

9) Create the daily scan script to scan directories of interest. Note: for the lab implementation only the /home volume was selected for scanning.

vi /etc/cron.daily/clamav_scan.sh

File Contents

#!/bin/bash
SCAN_DIR="/home"
LOG_FILE="/var/log/clamav/dailyscan.log"
/usr/bin/clamscan -ri \$SCAN_DIR >> \$LOG_FILE

10) Set the file to have execute privilege with this command:

chmod +x /etc/cron.daily/clamav_scan.sh

- 2. Download and Install the ConsoleWorks packages
 - Login to TDi Technology Support Portal (<u>https://support.tditechnologies.com/get_con-soleworks</u>) to download the ConsoleWorks for Linux 5.3-1u3 installation package. Credentials will be provided by TDi.
 - b. After downloading the ConsoleWorks installation package, copy it to the ConsoleWorks VM using a Secure Copy (scp) utility.
 - c. Follow the procedures from TDi ConsolWorks New Installation and Upgrade Guide for Linux Chapter 3: Automated New Installation of ConsoleWorks
 - i. During installation, create a New Invocation named "NCCOE".
 - ii. Create a new certificate.
 - iii. Set the system to automatically start the ConsoleWorks Invocation.
 - d. Login to the platform and initiate the offline registration process (Figure 2-43).
 - e. Once the license file is obtained, complete the registration process (Figure 2-44).

Figure 2-43 ConsoleWorks Registration Screen

Console <mark>Works</mark>	® v 5.3-1u3	Unregistered Administration
	ADMIN: Server Management: Registration	+ X
No Favorites saved	Registration X Offline Registration X	Complete My Offline Registration
DASHBOARDS	Contact Name	
▷ CONSOLES		PROAT DETAILS
▶ DEVICES	Contact Email:	ADVANCED OPTIONS
▶ LOGS	Telephone:	
▶ EVENTS	Facility (Site) Name: NIST Gaithersburg	
▶ REGULATORY	Address Line 1: 100 Bureau Drive	
▶ GRAPHICAL	Address Line 2:	7
▶ USERS	City: Gaithersburg	
▶ REPORTS	State/Province: MD	
▹ TOOLS		
SECURITY		4
> ADMIN	Country: United States	
▶ HELP		
	Register Online Register Offline	Cancel Save
EXTERNAL TOOLS		Gander
None Available	1	

Figure 2-44 ConsoleWorks Offline Registration Process

Console <mark>Works</mark>	® v 5.3-1u3	Unregistered Administration
▼ FAVORITES	▼ ADMIN: Server Management: Offline Registration	+_
No Favorites saved	Registration X Offline Registration X	
DASHBOARDS	ConsoleWorks Offline Registration Please send support@tditechnologies.com an Email with:	Complete My Offline Registration
▷ CONSOLES	 This file attached Which contains your contact info, server operating system, and ConsoleWorks version. If Email is un 	available, please contact TDI Support
▶ DEVICES		
▶ LOGS		
▶ EVENTS		
REGULATORY		
GRAPHICAL	1	
▶ USERS		
▶ REPORTS		
▶ TOOLS		
SECURITY		
ADMIN		
▶ HELP	1	
EXTERNAL TOOLS		Complete My Offline Registration
None Available		

f. This completes the default installation and establishes a basic ConsoleWorks server configuration. For the lab implementation, ConsoleWorks support provided two additional add-on packages (XML) files to setup the environment: ONBOARDING_1-DASH-BOARDS NCCoE.zip providing preconfigured dashboards for accelerating configurations; and NCCOE_ACRs_20210122_083645.zip providing the access control rules, tags, and

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

automation scripts used for the dashboards. These packages are scheduled for inclusion in future releases or can be requested from ConsoleWorks.

 Prior to installing these packages, a backup of the configuration should be made (Figure 2-45) by accessing Admin > Database Management > Backups and clicking Create Backup.

Figure 2-45 ConsoleWorks System Backups

Console Works® v 5.3-146				A	dministra
FAVORITES	ADMIN: Database Mana	agement: Backups		4	
DASHBOARDS	Backup 🗙				
CONSOLES	Start Time	User	Status	Locked	9
DEVICES	2021/05/15 03:00	Schedule:WEEKLY	Done	N	^
LOGS	2021/03/13 03:00	Schedule:WEEKLY	Done	Ν	
EVENTS	2021/03/06 03:00	Schedule:WEEKLY	Done	Ν	
	2020/12/09 10:31	CONSOLE_MANAGER	Done	Ν	
	2021/02/02 16:38	CONSOLE_MANAGER	Done	N	
RAPHICAL	2021/04/24 03:00	Schedule:WEEKLY	Done	Ν	
SERS	2021/06/14 10:55	CONSOLE_MANAGER	Done	N	
EPORTS	2021/02/11 08:07	CONSOLE_MANAGER	Done	Ν	
OOLS	2021/05/01 03:00	Schedule:WEEKLY	Done	Ν	
ECURITY	2021/02/13 03:00	Schedule:WEEKLY	Done	Ν	
DMIN	2021/05/08 03:00	Schedule:WEEKLY	Done	N	
over Management	2021/02/10 11:07	CONSOLE_MANAGER	Done	N	
atabase Manage	2021/02/09 13:07	CONSOLE_MANAGER	Done	N	
Backupe	2021/02/06 03:00	Schedule:WEEKLY	Done	N	
Dackups	2021/02/20 03:00	Schedule:WEEKLY	Done	Ν	
XML Exports	2021/03/27 03:00	Schedule:WEEKLY	Done	Ν	
XML Imports	2021/04/03 03:00	Schedule:WEEKLY	Done	N	
Ornhan Files	2021/01/19 14:07	CONSOLE_MANAGER	Done	Ν	
mplate Managem	2021/02/27 03:00	Schedule:WEEKLY	Done	N	~
ELP	Restore	Create	Backup	Delete	Download
EXTERNAL T A					

- ii. Perform the XML Imports (Figure 2-46) by accessing Admin > Database Management > XML Imports following these steps:
 - 1) Import the Dashboard Add-On XML file.
 - 2) Import the Supporting Configuration Add-On XML file.

Console <mark>Wo</mark>	orks [®] v 5.3-1u6	Administration
▶ FAVORITES	ADMIN: Database Management: XML Imports: Import	(+) – – ×
▶ DASHBOARDS	Import XML X	
▷ CONSOLES		
▶ DEVICES		
▶ LOGS		
▶ EVENTS		
▶ REGULATORY	1	
▶ GRAPHICAL	How would you like to provide the XML to Import?	
▶ USERS	Upload a file	
▶ REPORTS		
▶ TOOLS		
♦ SECURITY		
⇒ ADMIN		
Server Management	1-1	
Backups		
Restore		
XML Exports		
V XML Imports		
View		
Import		
Orphan Files		Next
Template Managem		
▶ HELP		
EXTERNAL T A		
None Available		

Figure 2-46 ConsoleWorks Importing System Configurations and Components

2.8.3 Configuration

The ConsoleWorks implementation required the following changes to the lab Cisco VPN appliance to allow remote users to access the ConsoleWorks system:

- 1. Login to the Cisco Firepower Appliance.
- 2. Create the Following Destination Network Objects:
 - a. For Build 1:
 - i. Name: ConsoleWorks
 - ii. IP Address: 10.100.0.52
 - b. For Build 3:
 - i. Name: CRS-NAT-IP
 - ii. IP Address: 10.100.0.20
- 3. Create the Following VPN-Rule:

- a. For Build 1:
 - i. Action: Allow
 - ii. Source Networks: VPN-Pool
 - iii. Destination Networks: ConsoleWorks
 - iv. Destination Ports: TCP (6): 5176; HTTPS
- b. For Build 3:
 - i. Action: Allow
 - ii. Source Networks: VPN-Pool
 - iii. Destination Networks: CRS-NAT-IP
 - iv. Destination Ports: TCP (6): 5176; HTTPS

ConsoleWorks is then configured as follows. For configuration procedures, please see the ConsoleWorks documentation available at https://support.tditechnologies.com/product-documentation.

1. Configure ConsoleWorks Password Rules (Figure 2-47):

Figure 2-47 ConsoleWorks Password Settings

 SECURITY: Password Rules 	+_□×
Password Rules 🔀	
Password rules are the minimum settings for ConsoleWorks passwords. These User accounts, although some rules can be overridden by settings on a User's f	settings apply to all Edit page.
Minimum Length: 12 🗘 (1-32 characters)	^
Passwords Must Contain: Spaces	
Vumbers	
✓ Letters	
Punctuation	
Mixed Case	
Number Between First and Last Chara	cters
Autofill Old Password During Forced Password Changes: Yes No	
Minimum Characters Changed 6 (1-32 characters)	
Minimum Time Between 5 (0-43200 minutes)	
Password Reuse After: 3 (0-10 unique passwords)	
Inactive Password Expiration After: 30 🗘 (0-365 days)	
Failed Logins Before Lockout: 4 (0-10)	
Account Lockout Duration: Permanent	~
	Cancel Save

- 2. Add user accounts:
 - a. NCCOE_ADMIN

b. NCCOE_USER

- 3. Configure the Graphical Gateway to allow users to use RDP within ConsoleWorks following these steps (Figure 2-48):
 - a. Name: LOCAL_GG
 - b. Description: Local GUI Gateway
 - c. Host: **127.0.0.1**
 - d. Port: 5172
 - e. Enabled: Selected
 - f. Encrypt Connection: Selected

Figure 2-48 ConsoleWorks Add the Local Graphical Gateway for RDP Access

Console Works ®	v 5.3-1u3	Administration
FAVORITES	▼ GRAPHICAL: Gateways: Edit	+_
DASHBOARDS	View Graphical Gateways 🔀 LOCAL_GG 🔀	
▷ CONSOLES	Refresh History	Test
▶ DEVICES	Name: LOCAL GG	► GRAPHICAL CONNECTIONS (2)
▶ LOGS		N TAGS (0)
▶ EVENTS		Y 1403 (V)
▶ REGULATORY	Host: 127.0.0.1	
	Port: 5172 (default: 5172)	
View	Enabled	
Add	Encrypt Connection	
Edit		
Recordings		
Active		
View		
Add		
Edit	-	
▶ USERS		
REPORTS		
▶ TOOLS	-	
SECURITY		
▶ ADMIN	Set As Default Save As	Delete Cancel Save
▶ HELP		
EXTERNAL TOOLS		
None Available		

- 4. Configure Device Types to organize the registered devices within the system as follows:
 - a. Enter the information for the supported device types as shown in the example device type (Figure 2-49) for each type listed in Table 2-18 (and shown in Figure 2-50).

Table 2-18 ConsoleWorks Device Type List

Name	Description	Parent Device Type	Order
NETWORKING	Devices supporting networked com- munications		1
IT_FWROUTER	Network Router/Firewall for support- ing IT Communications	NETWORKING	1
IT_SWITCH	Network switch supporting IT com- munications	NETWORKING	1
OT_FWROUTER	ICS Firewall/Router for ICS Network Separation	NETWORKING	1
OT_SWITCH	ICS Switch for supporting OT Subnets	NETWORKING	1
SERVERS	Devices for providing one or more IT/OT Services		1
IT_SERVERS	Servers providing IT Services	SERVERS	1
OT_SERVERS	Servers providing OT Services	SERVERS	1
WORKSTATIONS	Computers used to support IT/OT Operations		1
НМІ	Specialized workstation supporting human-machine interfaces	WORKSTATIONS	1
IT_WORKSTATIONS	Computers used by users to support IT Operations	WORKSTATIONS	1
OT_WORKSTATIONS	Computers used by users to support OT Operations	WORKSTATIONS	1

Console <mark>Works</mark>	® v 5.3-1u3	Administration
FAVORITES	DEVICES: Device Types: Edit	+X
DASHBOARDS	View Device Types X OT_WORKSTATION X	
▶ CONSOLES	Refresh History	
	Name: OT WORKSTATION	► DEVICES (1)
View	Description: Engineering Workstation	
Add		()
Edit	Classification:	
Device Types	Parent Device Type: WORKSTATIONS	
View	Order: 1 (relative order within parent Device Type)	
Add	Path: WORKSTATIONS:OT_WORKSTATION	
Edit	Child Count: 0	
▶ LOGS	Custom Fields	
▶ EVENTS		
REGULATORY		
▶ GRAPHICAL		
▶ USERS		
REPORTS		
▶ TOOLS	Set As Default Save As	Delete Cancel Save
SECURITY		
ADMIN		
▶ HELP		
EXTERNAL TOOLS A		
None Available		

Figure 2-49 ConsoleWorks Example Device Type Definition

Figure 2-50 ConsoleWorks List of Device Types

onsole <mark>Works</mark>	© v 5.3-1u3	Administration				
FAVORITES	DEVICES: Device Type	s: View				(+)
DASHBOARDS	View Device Types 🔀					
CONSOLES	Device Type	Path ≜	Description	Classification	Parent	Order 🐐
DEVICES	NETWORKING	NETWORKING	Devices for supporting networked communications			1
view (IT_FWROUTER	NETWORKING:IT_FWROUTER	Network Router/Firewall for supporting IT Communications		NETWORKING	1
Add	T_SWITCH	NETWORKING:IT_SWITCH	Network Switch supporting IT communications		NETWORKING	1
dit	OT_FWROUTER	NETWORKING:OT_FWROUTER	ICS Firewall/Router for ICS Network Segmentation		NETWORKING	1
evice Types	OT_SWITCH	NETWORKING:OT_SWITCH	Network Switch for supporting ICS network segement		NETWORKING	1
View	SERVERS	SERVERS	Devices for providing one or more IT/OT Services			1
Add	IT_SERVER	SERVERS:IT_SERVER	Server providing IT Services		SERVERS	1
Edit	OT_SERVER	SERVERS:OT_SERVER	Server providing OT Services		SERVERS	1
DGS	WORKSTATIONS	WORKSTATIONS	Computers used by users to support IT/OT Operations			1
/ENTS	HMI	WORKSTATIONS: HMI	Specialized workstation supporting Human Machine Interface	•	WORKSTATIONS	1
	IT_WORKSTATION	WORKSTATIONS:IT_WORKSTATI	Computer used by user for supporting IT operations		WORKSTATIONS	1
GULATORT	OT_WORKSTATION	WORKSTATIONS:OT_WORKSTAT	Engineering Workstation		WORKSTATIONS	1
PHICAL						
RS						
PORTS	<		_			
LS		Mass Change	•	Delete Add	Examples Copy	Rename Edit
URITY						
MIN						
P						
TERNAL TOOLS						
None Available						

5. Configure Devices for each system within the testbed that is accessible from ConsoleWorks.

Figure 2-51 ConsoleWorks Example Device Definition

Console <mark>Wo</mark>	rks [®] v 5.3-1u3	Administration
View Add	DEVICES: Edit *	+_ _
Edit Change State	Refresh History	Logs Recordings Events
▷ VIRTUALfx ▷ Groups	Name: PCS_WORKSTATION	CONSOLES (0)
Multi-Connect		V GRAPHICAL CONNECTIONS (2)
Expect-Lite Scripts	Description: PCS Engineering Workstation	✓ DEVICE TYPES (1)
Usage	Status: 3 - Available	OT_WORKSTATION Add
Connection Rules		Remove
Send Command	Disable	
	► System Info	
View	▶ Custom Fields	
Add		
Edit		View
Device Types		► REMEDIATION HISTORY (0)
∠LOGS		► BASELINE RUNS (0)
Active		► TAGS (0)
♦ Charts		
▶ EVENTS		
▶ REGULATORY	1	
✓ GRAPHICAL		
View		
Add		
Edit		
Recordings	Set As Default Save As	Delete Cancel Save
Active		

a. For Build 1 (PCS), enter the information for the devices as shown in the example device (Figure 2-51) for each device listed in Table 2-19 (Figure 2-52).

Table 2-19 ConsoleWorks PCS (Build 1) Devices

Name	Description	Device Type
DMZ_HISTORIAN	Historian in DMZ Subnet	IT_SERVER
PCS_HISTORIAN	Local Historian in PCS Subnet	OT_SERVER
PCS_HMI	PCS HMI Workstation	HMI
PCS_ROUTER	PCS Boundary Firewall/Router	OT_FWROUTER
PCS_SWITCH_VLAN1	PCS VLAN 1 OT Switch	OT_SWITCH
PCS_SWITCH_VLAN2	PCS VLAN 2 OT Switch	OT_SWITCH
PCS_WORKSTATION	PCS Engineering Workstation	OT_WORKSTATIONS

Figure 2-52 ConsoleWorks List of PCS (Build 1) Devices

Console Wo	rks® v 5.3-1u3 Administration	
FAVORITES	▼ DEVICES: View (+)	
▶ DASHBOARDS	View Devices X	
▷ CONSOLES	Device A Description	9
	CONSOLEWORKS_HOST	2
View	DMZ_HISTORIAN	. 😽
Add	PCS_HISTORIAN	
Edit		
Device Types	PCS_ROUTER	1
▶ LOGS	PCS_SWITCH_VLAN1	- 19
▶ EVENTS	PCS_SWITCH_VLAN2	8
▶ REGULATORY	PCS_WORKSTATION PCS Engineering Workstation	. 8
GRAPHICAL		
▶ USERS		
▶ REPORTS		
▶ TOOLS		
SECURITY		
▶ ADMIN	Connect w Long Recording Mars Change Relate Add Examples Conv. Record	Edit
▶ HELP	Connect + Logs Recordings mass change Delete Add Examples Copy Rename	Euit
EXTERNAL T 🔺		
None Available		

b. For Build 3 (CRS), enter the information for the devices as shown in the example device (Figure 2-51) for each device listed in Table 2-20 (also shown in Figure 2-53).

Table 2-20 ConsoleWorks CRS (Build 3) Devices

Name	Description	Device Type
DMZ_HISTORIAN	Historian in DMZ Subnet	IT_SERVER
CRS_HISTORIAN	Local Historian in CRS Subnet	OT_SERVER
CRS_HMI	CRS HMI Workstation	HMI
CRS_ROUTER	CRS Boundary Firewall/Router	OT_FWROUTER
CRS_SWITCH_CONTROL	OT Switch for Control Network	OT_SWITCH
CRS_SWITCH_FIELD	OT Switch for Field Network	OT_SWITCH
CRS_WORKSTATION	CRS Engineering Workstation	OT_WORKSTATIONS
CRS_STATION1	Machining Station #1	OT_WORKSTATIONS
CRS_STATION2	Machining Station #2	OT_WORKSTATIONS
CRS_STATION3	Machining Station #3	OT_WORKSTATIONS
CRS_STATION4	Machining Station #4	OT_WORKSTATIONS

ISUIC VIOI	v 5.3-1u6						Admi	nistr
VORITES	DEVICES: View						\	
SHBOARDS	View Devices 🗙							
ONSOLES	Device A	Description						9
VICES	CONSOLEWORKS_HOST							
w	CRS_HISTORIAN	Local CRS Historian Server						- N
	CRS_HMI	Process Monitor						
	CRS_ROUTER	CRS Router Firewall						<u> </u>
ice Types	CRS_STATION1	Machining Station #1						<u> </u>
GS	CRS_STATION2	Machining Station #2						<u> </u>
ENTS	CRS_STATION3	Machining Station #3						<u> </u>
	CRS_STATION4	Machining Station #4						- <u></u>
	CRS_SWITCH_CONTROL	Control LAN Switch						<u> </u>
	CRS_SWITCH_FIELD	Field Device LAN Switch						- 19
ERS	CRS_WORKSTATION	CRS Engineering Workstation						<u> </u>
PORTS	DMZ_HISTORIAN	External Historian Replication Se	rver					<u> 8</u>
OLS								
CURITY	1							
MIN		Mara Channa	Delete	(A rist	Evenueles	Carry	Deserve	
LP	Connect V Logs Recording	gs mass change	Delete	Add	Examples	Copy	Rename	Ealt
TERNAL T 🔺								
one Available								

Figure 2-53 ConsoleWorks List of CRS (Build 3) Devices

6. Configure Graphical Connections for the PC (RDP) based devices.

Console	orl	(S [®] v 5.3-1u3	A	dministration	
View	^	CRADHICAL • Edit			
Add		GIGATTICAL, EUR		L.	
Edit		View Graphical Connection			
Change State		Refresh History		View Active View Recordings	Connect
VIRTUALfx		Name:	PCS_WORKSTATION_RDP		(1)
▶ Groups		Description:	PCS Engineering Workstation	LOCAL_GG A	dd
Multi-Connect		Device:	PCS_WORKSTATION	Rem	nove
Expect-Lite Scripts		Type:	RDP =		
Connection Pulse		Host	172 16 3 10		
Send Command		indat.	174.10.0.10		
		Port	3389		
View			Single Session Connection	Vi	iew
Add			Allow Join with Active Session	► CONSOLES	(0)
Edit		Status Text:	Available Disable	► TAGS	(0)
Device Types		Max Idle Time:	0 0-999 Minutes (0=disabled)		
V LOGS		Audio:	Default Enabled		
View		- Recordings			
Active		Directory	Inti Onen Inti Inte NOODE (marking)		
▶ Charts		Directory:	/opt/console/vorks/NCCOE/graphical		
▶ EVENTS			Retain Recordings		
▶ REGULATORY		Auto-Purge:	0 0-9999 Days Old (0=disabled)		
		Max Size:	0 0-99999 MB (uncompressed, 0=disabled)		
View			End Session when Max Size reached		
Add		Max Time:	0 0-9999 Minutes (ends Session, 0=disabled)		
Edit		Record Audio:	System Disabled		
Recordings		- Authentication			
Active		Hudrendeadon	A		
Gateways		Username:	Administrator		
♦ USERS		Password:			
▶ REPORTS		Domain:			
▼ TOOLS		Security Mode:			
CWCLIent			Disable Authentication		
Windows Event			V Ignore Certificate Errors		
Graphical Gateway		- Derformance			
CWScripts					
Baseline Configu		Color Depth:			
▷ Schedules		Display Width:	1900		
External Tools		Display Height:	1200		
Custom Files		DPI:			
	~				~
< >>		Set As Default Save As		Delete Cano	Save

Figure 2-54 ConsoleWorks Example RDP Configuration

- For Build 1 (PCS), enter the information for the Graphical Connections as shown in the example (Figure 2-54) for each graphical connection listed in <u>Table 2-21</u> (also shown in <u>Figure 2-55</u>). For each entry, the following are common settings for all graphical connections:
 - i. Under Gateway, click Add and select LOCAL_GG.
 - ii. Single Session Connection: Checked
 - iii. Allow Join with Active Session: Checked
 - iv. Under Recordings:
 - 1) Directory: /opt/ConsoleWorks/NCCOE/graphical
 - 2) Retain Records: Checked
 - 3) Auto-Purge: 0

- 4) Max Size: 0
- 5) End Session when Max Size Reached: Checked
- 6) Max Time: **0**
- v. Authentication
 - Specify local or domain credentials, which are securely stored by ConsoleWorks, to allow complex passwords/credentials without having to share between users.
 - 2) Ignore Certificate Errors: Checked only if self-signed certificates are in use.
- vi. Performance
 - 1) Display Width: 1900
 - 2) Display Height: 1200

Table 2-21 ConsoleWorks PCS (Build 1) Graphical Connections

Name	Device	Туре	Host	Port
DMZ_HISTORIAN	DMZ_HISTORIAN	RDP	10.100.1.4	3389
PCS_HISTORIAN	PCS_HISTORIAN	RDP	172.16.2.14	3389
PCS_HMI_RDP	PCS_HMI	RDP	172.16.2.4	3389
PCS_WORKSTATION_RDP	PCS_WORKSTATION	RDP	172.16.3.10	3389

Console <mark>Wo</mark>	rks ® v 5.3-1u3		Administrat	ion	
FAVORITES	▼ GRAPHICAL: View				+_ ×
DASHBOARDS	View Graphical Connections				
CONSOLES	Graphical Connection	Description	Туре	Status Text	Host 9
DEVICES	DMZ_HISTORIAN		RDP	Available	10.100.1.4
LOGS	PCS_HISTORIAN		RDP	Available	172.16.2.14
EVENTS	PCS_HMI_RDP	PCS HMI Workstation	RDP	Available	172.16.1.4
REGULATORY	PCS_WORKSTATION_FACTORYTALK	PCS Engineering Wor	RDP	Available	172.16.3.10
GRAPHICAL	PCS_WORKSTATION_RDP	PCS Engineering Wor	RDP	Available	172.16.3.10
Edit Recordings Active Gateways USERS REPORTS TOOLS	=				>
SECURITY	Connect View Active View Recordings	Mass Change	Delete	dd Examples	copy Rename Edit
HELD					
EXTERNAL T A					
None Available					

Figure 2-55 ConsoleWorks List of PCS (Build 1) RDP Connections

- b. For Build 3 (CRS), enter the information for the graphical connections as shown in the example (Figure 2-54) for each graphical connection listed in <u>Table 2-22</u> (also shown in <u>Figure 2-56</u>). For each entry, the following are common settings for all graphical connections.
 - i. Under Gateway, click Add and select LOCAL_GG.
 - ii. Under Recordings, use these settings:

1) Directory /opt/ConsoleWorks/NCCOE/graphical

- 2) Retain Records Checked
- 3) Auto-Purge: 0
- 4) Max Size: 0

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

- 5) End Session when Max Size Reached: Checked
- 6) Max Time: **0**
- iii. Authentication:
 - 1) Specify local or domain credentials, which are securely stored by ConsoleWorks, to allow complex passwords/credentials without having to share between users.

iv. Performance

1) Display Width: 1900

2) Display Height: 1200

Table 2-22 ConsoleWorks CRS (Build 3) Graphical Connections

Name	Device	Туре	Host	Port
DMZ_HISTORIAN	DMZ_HISTORIAN	RDP	10.100.1.4	3389
CRS_HISTORIAN	CRS_HISTORIAN	RDP	192.168.0.21	3389
CRS_WORKSTATION	CRS_WORKSTATION	RDP	192.168.0.20	3389

Figure 2-56 ConsoleWorks List of CRS (Build 3) RDP Connections

Console <mark>Wo</mark> i	v 5.3-1u6					Adı	ministration	
FAVORITES	▼ GRAPHICAL: View						+ _	
DASHBOARDS	View Graphical Connectio	ns 🗙						
▷ CONSOLES	Graphical Connection	A	Description	Туре		Status Text	Host	9
DEVICES	CRS_HISTORIAN			RDP		Available	192.168.0.21	
▶ LOGS	CRS_WORKSTATION			RDP		Available	192.168.0.20	
▶ EVENTS	DMZ_HISTORIAN			RDP		Available	10.100.1.4	
▶ REGULATORY								
View								
Add								
Edit								
Recordings								
Active								
View								
Add								
Edit	<							>
▶ USERS	Connect View Active	View Recordings	Mass Chang	e	Delete	Add Examples	Copy Rename	Edit
▶ REPORTS								
▶ TOOLS								
♦ SECURITY								
> ADMIN								
▶ HELP								
EXTERNAL T 🍐								
None Available								

7. Configure console connections for non-graphical (e.g., SSH) interfaces to devices (Figure 2-57).



Figure 2-57 ConsoleWorks Example Console (SSH) Connection

AVORITES	CONSOLES: Edit				(A)	וצו
ASHBOARDS					C	
ONSOLES	ew consoles A CKS_				as Events Monitored Ev	onte
ew	instory					
id	Name:	CRS_STATION1		F GROUPS	(0)	Ê
lit 🛛	Nickname:			► SCANS	(0)	
nange State	Description:			► AUTOMATIC ACTIONS	(0)	
RTUALfx	Status:	NORMAL Disable		► ACKNOWLEDGE ACTION	š (0)	
roups	Device:	CRS_STATION1 ₹	Q	PURGE ACTIONS	(0)	i 🗌
nect lite Scrints	Connector:	Web Forward	-		(0)	1
age		s		P ADDITIONAL BINDS	(0)	
nnection Rules		Priority Startup	- !	REMEDIATION HISTORY	(0)	
nd Command	Bind Name:		⊤, I	SCHEDULES + EVENTS	(0)	
EVICES	Heat Header:		4	► TAGS	(1)	
DGS	nost neader.		= i	► BASELINES + SCHEDULE	S (0)	i 🗌
VENTS	URL:	http://192.168.1.101/	_ i	► BASELINE RUNS	(0)	i 🗌
EGULATORY	Relative URL:	/status/	¦		(*)	
RAPHICAL		Open		GRAPHICAL CONNECTION	NS (U)	
SERS		Disable Standard Translation	s	LOG TRANSFORMS	(0)	
EPORTS	Log Web Traffic:		-			
DOLS	Profile:	NCCOE_CRS	-			
ECURITY	raffic Processing Script:		I			
DMIN						
ELP						
XTERNAL T A						
None Available						
			77			

Figure 2-58 ConsoleWorks Example Console (Web Forward) Connection

- For Build 1 (PCS), enter the information for the Console Connections as shown in the examples (Figure 2-57 and Figure 2-58) for each console connection listed in Table 2-23 (also shown in Figure 2-59). For each entry, the following are common settings for all console connections.
 - i. Under Connection Details:

1) Specify the username and password, which are securely stored by Console-Works, to allow complex passwords/credentials without having to share between users.

Table 2-23 ConsoleWorks PCS (Build 1) Console Connections

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

Name	Device	Connector	Host	Port
PCS_ROUTER	PCS_ROUTER	SSH with Password	10.100.2.8	22
PCS_VLAN1	PCS_SWITCH_VLAN1	SSH with Password	172.16.1.3	22

Name	Device	Connector	Host	Port
PCS_VLAN2	PCS_SWITCH_VLAN2	SSH with Password	172.16.2.2	22

Figure 2-59 ConsoleWorks List of PCS (Build 1) Console Connections

/	Vorks [®] v 5.3-1u3 Administration			n	
FAVORITES CONSOLES: View				(+) <u>-</u>	
DASHBOARDS					
CONSOLES Console ≜	Description	Connector	S.	Status	9
View CONSOLEWORKS_S	SSH	SSH with Password(SSHPWD)		NORMAL	
Add CONWRKS	ConsoleWorks	Internal Console - No Conne	۹	NORMAL	
Edit CONWRKS_OUT		File Monitor(FILEMON)	G	NORMAL	
Change State PCS_ROUTER		SSH with Password(SSHPWD)	R	Restored Communication	
VIRTUALfx PCS_VLAN1		SSH with Password(SSHPWD)		Restored Communication	
Groups PCS_VLAN2		SSH with Password(SSHPWD)	R	Restored Communication	
Multi-Connect					
Expect-Lite Scripts					
Usage					
Connection Rules					
Send Command					
DEVICES					
▶ LOGS					
▶ EVENTS					
REGULATORY					
GRAPHICAL					
▶ USERS					
▶ REPORTS					
TOOLS	Mass Change	Delete Add Ex	amp	les Copy Rename	Edit
▶ SECURITY	•••		-		
ADMIN					
▶ HELP					

- b. For Build 3 (CRS), enter the information for the console connections as shown in the example (Figure 2-57 and Figure 2-58) for each console connection listed in Table 2-24 (Figure 2-60). For each entry, the following are common settings for all console connections.
 - i. Under Connection Details

1) Specify the username and password, which are securely stored by Console-Works, to allow complex passwords/credentials without having to share between users.

Table 2-24 ConsoleWorks CRS (Build 3) Console Connections

Name	Device	Connector Host		Port
CRS_CONTROL_LAN	CRS_SWITCH_CONTROL	Web Forward	192.168.0.239	80
CRS_FIELD_LAN	CRS_SWITCH_FIELD	SSH with Password	192.168.1.10	22

Name	Device	Connector	Host	Port
CRS_ROUTER	CRS_ROUTER	SSH with Password	192.168.0.2	22
CRS_STATION1	CRS_STATION1	Web Forward	192.168.1.101	80
CRS_STATION2	CRS_STATION2	Web Forward	192.168.1.102	80
CRS_STATION3	CRS_STATION3	Web Forward	192.168.1.103	80
CRS_STATION4	CRS_STATION4	Web Forward	192.168.1.104	80
НМІ	CRS_HMI	Web Forward	192.168.0.98	80

Figure 2-60 ConsoleWorks List of CRS (Build 3) Console Connections



8. Configure tags to support profiles and access controls.

Console Works v 5.3-1u3		v 5.3-1u3	Administration			
FAVORITES	^	SECURITY: Tags: View	+ 			
▶ DASHBOARDS	1	View Tags 🗙				
▶ CONSOLES	1	Tag A	Description			
▶ DEVICES	1	ADMIN_ARCH_ACCESS	Admin ARCHITECT access			
▶ LOGS	1	ADMIN_CONTROL_ACCESS	Admin CONTROL access			
▶ EVENTS		ADMIN_CREATE_ACCESS	Admin CREATE access			
		ADMIN_MODIFY_ACCESS	Admin MODIFY access			
		ADMIN_VIEW_ACCESS	Admin VIEW access			
V GRAPHICAL		CONSOLE_ACK_ACCESS	Console ACK access			
▶ USERS		CONSOLE_CONTROL_ACCESS	Console CONTROL access			
▶ REPORTS		CONSOLE_MODIFY_ACCESS	Console MODIFY access			
▶ TOOLS		CONSOLE_VIEW_ACCESS	Console VIEW access			
		PCS_ADMIN	Tag to identify PCS elements for Admin Use			
Access Control	1 1	PCS_GENERAL	Tag to identify standard PCS elements			
IP Filters		TBA_BASELINE_RUN	Run Baselines			
SSL Certificate		TBA_BASELINE_RUNVIEW	View Baselines			
External Authenti		TBA_DASHBOARD_VIEW	View Dashboards			
Password Rules		TBA_DEVICE_CONNECT	Device Connect			
		TBA_DEVICE_LOGVIEW	View Device Logs			
View		TBA_EVENT_ACKNOWLEDGE	Event acknowledge			
Add		TBA_EVENT_AWARE	Event awareness			
Edit		TBA_REPORT_OUTPUT_VIEW	View Report Outputs			
Command Contr		TBA_REPORT_RUN	Run Reports			
Certificates		TBA_SUBSET	Profile uses a subset of components			
> ADMIN	1 –	TEST	Tag for Profile TEST			
▶ HELP		<	>			
<>	~	Mass Char	Delete Add Examples Copy Rename Edit			

Figure 2-61 ConsoleWorks List of Tags for PCS (Build 1)

Figure 2-62 ConsoleWorks Example Tag Definition Screen

onsole vvorks	v 5.3-1u6		Administra
FAVORITES S	ECURITY: Tags: Edit		(+)_ _X
DASHBOARDS			
CONSOLES	fresh History		
DEVICES			(1)
LOGS		PENIOSO	
EVENTS	Description: Tag for Profile NCCOE_CRS	DEVICES	Add
REGULATORY	Custom Fields		Remove
GRAPHICAL			
USERS			
REPORTS			
TOOLS			View
SECURITY		✓ WIDGETS	(1)
Access Control		DEVICE	Add
P Filters		DEVICE	Add
SSL Certificate			Remove
External Authenticat			
Password Rules			
Tags			
Add			View
Edit		✓ WIDGET TYPES	(1)
Command Control		DEVICE	Add
Certificates		JETTOE .	
ADMIN			Remove
HELP			
EXTERNAL T			
None Available			View
	As Default	D -1	ta Canad Saus

a. For Build 1 (PCS) the following tags were created as shown in Figure 2-61. Figure 2-62 shows an example of a single tag.

i. Name: PCS_GENERAL

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

1) Under Dashboards, click Add and select Devices.

2) Under Custom UI Classes click Add and select:

a) DEVICE_LISTGRID

b) LISTGRID

3) Under Devices, click Add and select:

a) DMZ_HISTORIAN

b) PCS_HISTORIAN

c) PCS_HMI

4) Under Graphical Connections, click Add and select:

a) DMZ_HISTORIAN

b) PCS_HISTORIAN

c) PCS_HMI_RDP

d) PCS_WORKSTATION_RDP

ii. Name: PCS_ADMIN:

1) Under Dashboards click Add and select Devices

2) Under Custom UI Classes click Add and select:

a) DEVICE_LISTGRID

b) LISTGRID

3) Under Consoles, click Add and select:

a) PCS_ROUTER

b) PCS_SWITCH_VLAN1

c) PCS_SWITCH_VLAN2

4) Under Devices, click Add and select:

a) PCS_ROUTER

b) PCS_SWITCH_VLAN1

c) PCS_SWITCH_VLAN2

b. For Build 3 (CRS) Create the following:

i. Name: NCCOE_CRS

1) Under Dashboards, click Add and select Devices.

2) Under Custom UI Classes, click Add and select:

a) DEVICE_LISTGRID

b) LISTGRID

3) Under Consoles, click Add and select:

a) CRS_STATION1

b) CRS_STATION2

c) CRS_STATION3

e) HMI

4) Under Devices, click Add and select:

a) CRS_HMI

b) CRS_STATION1

c) CRS_STATION2

d) CRS_STATION3

e) CRS_STATION4

f) CRS_WORKSTATION

5) Under Graphical Connections, click Add and select:

a) CRS_WORKSTATION

ii. Name: NCCOE_ADMIN

1) Under Dashboards click Add and select Devices

2) Under Custom UI Classes click Add and select:

a) DEVICE_LISTGRID

b) LISTGRID

3) Under Consoles click Add and select:

a) CRS_CONTROL_LAN

b) CRS_FIELD_LAN

c) CRS_ROUTER

4) Under Devices click Add and select:

a) CRS_SWITCH_CONTROL

b) CRS_SWITCH_FIELD

c) CRS_ROUTER

9. Configure profiles to provide user accounts with granular access controls to available resources (Figure 2-63).

Figure 2-63 ConsoleWorks Example Profile

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

Console <mark>Wo</mark>	rks	® v 5.3-1u6				A	dminis	tration
FAVORITES]							
DASHBOARDS	1	▼ USERS: Profiles: Edit	t				(+)(
▶ CONSOLES		View Profiles X NCCO						
DEVICES		Refresh History						
▶ LOGS		Nama	NCCOF CRS				(1)	
▶ EVENTS		Name:	NUCUE_CRS		+ USEKS		("	
REGULATORY		Description:	General Access to CRS E	nvironmen	NCCOE_USER		Add	
▶ GRAPHICAL		Custom Fields					Remove	2
▼ USERS								
View								
Add								
Edit							View	
					TICO		Them	
View					▼ IAGS		(4)	
Add					NCCOE_CRS		Add	
Edit					TBA_DASHBOARD_VIEW		Remove	
Change My Profile					TBA_DEVICE_CONNECT			
Reset Passwords					TBA_SUBSET			
Change Passwords								
Change My Password	_							
Preferences							View	
Sessions		Set As Default Save As.				Delete	Cancel	Save
Send Message								
▶ REPORTS								
▶ TOOLS								
SECURITY								
ADMIN								
▶ HELP								
	1							
EXTERNAL T A								
None Available								

- a. For Build 1 (PCS) the following profiles were created:
 - i. PCS_GENERAL

1) Under Users click Add and select

a) NCCOE_USER

2) Under Tags click Add and select

- a) PCS_GENERAL
- b) TBA_DASHBOARD_VIEW
- c) TBA_DEVICE_CONNECT
- d) TBA_SUBSET
- ii. PCS_ADMIN
1) Under Users, click Add and select:

a) NCCOE_ADMIN

- 2) Under Tags, click Add and select:
 - a) PCS_ADMIN
 - b) TBA_DASHBOARD_VIEW
 - c) TBA_DEVICE_CONNECT
 - d) TBA_SUBSET
 - e) CONSOLE_CONTROL_ACCESS
 - f) CONSOLE_VIEW_ACCESS
- b. For Build 3 (CRS) create the following:
 - i. NCCOE_CRS profile for the NCCOE_USER with access to Tags:

1) Under Users, click Add and select:

a) NCCOE_USER

- 2) Under Tags click Add and select the following:
 - a) NCCOE_CRS
 - b) TBA_DASHBOARD_VIEW
 - c) TBA_DEVICE_CONNECT
 - d) TBA_SUBSET
 - e) CONSOLE_CONTROL_ACCESS
 - f) CONSOLE_VIEW_ACCESS
- ii. NCCOE_ADMIN profile for the NCCOE_USER with access to Tags:

1) Under Users, click Add and select:

a) NCCOE_ADMIN

2) Under Tags click Add and select the following:

- a) NCCOE_ADMIN
- b) TBA_DASHBOARD_VIEW
- c) TBA_DEVICE_CONNECT
- d) TBA_SUBSET
- e) CONSOLE_CONTROL_ACCESS

f) CONSOLE_VIEW_ACCESS

2.9 Tenable.OT

The Tenable.OT implementation in Build 1 consists of a single appliance to meet BAD, hardware modification, firmware modification, and software modification capabilities. Tenable.OT utilizes a combination of passive and active sensors to monitor critical networks for anomalies and active querying to retrieve information about endpoints in the PCS environment.

2.9.1 Host and Network Configuration

Tenable.OT is installed and configured to support the PCS environment in Build 1. The overall build architecture is described in Figure B-1, and the Tenable.OT specific components are listed in Table 2-25.

Table 2-25 Tenable.OT Appliance Details.

Name	System	OS	CPU	Memory	Storage	Network
Tenable.OT	Model: NCA- 4010C-IG1	CentOS 7	Intel Xeon D-1577	64 GB	64 Gb 2 TB 2 TB	Testbed LAN 10.100.0.66

2.9.2 Installation

The Tenable.OT (Version 3.8.17) appliance is installed in a rack with network connections for the Management/Query traffic on Port 1 and SPAN traffic on Port 2 of the appliance. Documentation for Tenable.OT is available at https://docs.tenable.com/Tenableot.htm.

2.9.3 Configuration

This section outlines the steps taken to configure Tenable.OT to fully integrate and support the PCS environment. These include setting NTP settings to synchronize the system time with the lab time source, configuring the scanning options for the PCS environment, and configuring network objects and policies to enhance alerting for DMZ specific remote connections.

- 1. Enable connection through PCS Firewall
 - a. Add the following rules (Table 2-26) to the PCS Firewall to allow Tenable.OT to perform asset discovery and controller scanning.

Table 2-26 Firewall Rules for Tenable.OT

Rule Type	Source	Destination	Protocol:Port(s)	Purpose
Allow	10.100.0.66	172.16.0.0/22	ICMP	Asset Discovery
Allow	10.100.0.66	172.16.2.102	TCP:44818,2222	PLC Controller Scans

2. Set NTP Services as follows:

- a. After logging into the appliance, navigate to Local Settings > Device.
- b. To the right of **System Time**, click **Edit** to display the time service options (Figure 2-64).
- c. Enter the NTP Server information: 10.100.0.15
- d. Click Save.

Figure 2-64 Tenable.OT Local Device Setting for NTP Service

> Assets		
> Servers	System Time	Set date and time manually
Integrations		Set date and time using NTP server
System		IP 1 * 10.100.0.15
System Log		IP 2 NTP Server
PCAP Player		
		IP 3 NTP Server
		Cancel Save

- 3. Configure Scanning Options as follows:
 - a. Set Asset Discovery Scans:
 - i. Navigate to Local Settings > Queries > Asset Discovery (Figure 2-65)
 - ii. Enable both scan options.
 - iii. Select Edit next to Asset Discovery.

1) Enter the following CIDR for the PCS, DMZ, and Testbed networks:

- a) **172.16.0.0/22**
- b) **10.100.0/24**
- c) **10.100.1.0/24**

2) Set the scan properties as follows:

- a) Number of Assets to Poll Simultaneously: 10
- b) Time Between Discovery Queries: 1 second
- c) Frequency: Daily
- d) Repeats Every: 7 Days
- e) Repeats at: 9:00 PM
- 3) Click Save.

Figure 2-65 Tenable.OT Asset Discovery Settings

=	tenable.ot [*]		02:42	PM • Thursd
> 🏚	Events			
ò	Policies	Asset Discovery	IP ranges:	(i)
✓ ⁰ / ₈₀	Inventory		One CIDR per line	
	Controllers		172.16.0.0/22 10.100.0.0/24	
	Network Assets		10.100.1.0/24	
> 📺	Risk			
> #	Network			
> 🇊	Groups			
	Reports		Number of Assets to Poll Simultaneously:	
~ o°	Local Settings		10 ~	
	Device		Time Between Discovery Queries:	
	User		1 second v	
	Asset Custom Fields		Frequency:	
	API Keys			
	HTTPS			
	User Management		Repeats Every	
	✓ Queries		7 days 🗸	
	Asset Discovery		Repeats At	
	Controller		9:00 PM 🗸	
	Network		Cancel Save	
1	Assets			
	Servers	Initial Asset Enrichment	Will run SNMP, Minimal Open Port Verification, CIP/DCP, NetBIOS, Backplane Query, Unicast Identification, Controller Details, Controller State.	(i)
	Integrations			

- b. Set Controller Scans as follows:
 - i. Navigate to Local Settings > Queries > Controller (Figure 2-66)
 - ii. Enable the following options:
 - 1) All Controller Queries
 - 2) Periodic Snapshots
 - 3) Controller Discovery
 - 4) Controller Status Query
 - 5) Controller Details Query
 - 6) Backplane Query

Figure 2-66 Tenable.OT Controller Scans

■ C tenable.ot					03:17 PM • V	Vednesday, Dec 9, 2020	NCCOE User 🗸
> 🌲 Events							
Policies	optroller Queries					0	
✓ ♣ Inventory	na olici gaches					Ŭ.	
Controllers						0	
Network Assets	dic Snapshots Fre	equency:	Every 4 days at 9:00 PM	Edit	© Run now	U	
> i Risk	Trianened Conselects					0	
> 🔒 Network	ringgered snapshots					U III	
> 🏟 Groups						-	
Reports Contr	rollers Discovery Fre	equency:	Every 1 hour	Edit	<u>Run now</u>	(i)	
ν φ ^o Local Settings							
Device Contr	roller State Query Fre	equency:	Every 15 Minutes	Edit	<u>Run now</u>	0	
User							
Asset Custom Fields Diagr	nostic Buffer Query Fre	equency:	Every 4 days at 9:00 PM	Edit	<u>Run now</u>	0	
API Keys							
HTTPS Contr	roller Details Query Fre	equency:	Every 1 hour	Edit	Run now	()	
> User Management							
✓ Queries Back	plane Query Fre	equency :	Every 1 hour	Edit	<u>Run now</u>	0	
Asset Discovery							
Controller							
Network							
> Assets							
Seniers *							
Version 3.8.17 Expires: Dec 9, 2021							

- c. Set Network Scans as follows:
 - i. Navigate to Local Settings > Queries > Network (Figure 2-67)
 - ii. Enable the following options:
 - 1) All Network Queries
 - 2) DNS Query
 - 3) ARP Query
 - 4) NetBIOS Query

Figure 2-67 Tenable.OT Network Scan Settings

■ () tenable.ot					03:18 PI	۷ • Wednesday, Dec 9, 2020	NCCOE User
 Events Policies Inventory 	All Network Queries					0	
Controllers Network Assets	Port Mapping	Mapping Range: Periodic mapping rate: On-demand mapping rate:	1000 most frequent ports 1 ports mapped per second 1 ports mapped per second	Edit		٥	
A State A	SNMP Query	Frequency: SNMP V2 Community Strings: SNMP V3 Usernames:	Every 1 hour public, private	Edit		3	
 Reports O^o Local Settings 	DNS Query					0	
Device User	ARP Query					3	
Asset Custom Fields API Keys	NetBIOS	Frequency: Every 1 hour		Edit		3	
HTTPS User Management	Active Asset Tracking	Frequency: Every 5 minutes		Edit		0	
✓ Queries		WMI Username:		Edit			
Controller	WMI Query	WMI Frequency :	Every 1 day at 12:00 PM	Edit	Run now Run now	١	
Network	USB Connections Query	USB Frequency:	Every 1 day at 12:00 PM	Edit	<u>Run now</u>	0	
Assets Servers Version 3.8.17 Expires: Dec 9, 2021	Ripple20 Vulnerabilities Scan			Edit		0	

- 4. Create Group Object as follows:
 - a. Set DMZ Group Object
 - i. Navigate to Groups > Asset Groups
 - ii. Click Create Asset Group to initiate the Wizard process.

1) Select IP Range for the Asset Group Type (Figure 2-68) and Click Next.

2) Enter the asset name in **Name**, the starting IP address in **Start IP**, and the ending IP Address in **End IP** (Figure 2-69) and Click **Create**.

Figure 2-68 Tenable.OT Create Asset Group Type

Asset Selection	IP Range	IP List	

Figure 2-69 Tenable.OT Create Asset Group Definition

el care / lober el oup)		×
	Group Type	Group Definition	
NAME *			Î
DMZ Zone			
START IP *			
10.100.1.0			
END IP *			
10.100.1.254			- 1

- 5. Create Policy to Detect External RDP Traffic:
 - a. In the left side navigation, click Policies.
 - b. Click **Create Policy** in the upper right corner of the page (Figure 2-70), then follow these steps:
 - For the Event Type (Figure 2-71), select as a Network Events > RDP Connection (Authenticated) and click Next.
 - ii. For the Policy Definition (Figure 2-72), specify the following parameters and click **Next**:
 - 1) Policy Name: Enter "External RDP Communications"
 - 2) **Source Group**: Select "In" from the first drop-down, and "DMZ" from the second drop-down.
 - 3) **Destination Group**: Select "In" from the first drop-down and select "In Any Asset" from the second drop-down.
 - 4) **Schedule Group**: Select "In" from the first drop-down, and "In Any Time" from the second drop-down.
 - iii. For the Policy Action (Figure 2-73), select Medium Sensitivity and click Create.

Figure 2-70 Tenable.OT Policy Settings

=Powered by Indegy	ť						09:29 AM • Monday, Jun	7, 2021 NCC	OE User 🗸
> 🌲 Events 🎗 Policies	Policies Search	٩					Actions ~	Create Policy	Export
> 🍰 Inventory > 🚊 Risk	STATUS	NAME	SEVERITY	EVENT TYPE	CATEGORY	SOURCE	DESTINATION / A	SCHEDULE	 setting
> Groups		SIMATIC Code Download SIMATIC Code Upload	Medium Low	SIMATIC Code Do SIMATIC Code Upl	Configuration Eve	In Any Asset In Any Asset	In Any Asset	In Any Time In Any Time	
> o° Local Settings		SIMATIC Code Delete SIMATIC Hardware Configuration Download	Medium	SIMATIC Code Del SIMATIC Hardwar	Configuration Eve Configuration Eve	In Any Asset In Any Asset	In Any Asset In Any Asset	In Any Time In Any Time	
		SIMATIC Hardware Configuration Upload SIMATIC Firmware Download	Low High	SIMATIC Hardwar SIMATIC Firmwar	Configuration Eve Configuration Eve	In Any Asset In Any Asset	In Any Asset In Any Asset	In Any Time	





Figure 2-72 Tenable.OT Create Policy - Definition

.

Crea	ate P	olicy					>
	Event Ty	/pe	Policy Det	finition	Policy	Actions	
POLICY	NAME *						
Exterr	nal RDP (Communi	ications				
SOURCE	GROUP	*					
In	~	DMZ			~	🔶 Or	1
	nd ATION *						
In	~	Any Asse	et		~	🕈 Or	1
∔ A	nd						
SCHEDU	JLE GROU	P *					
In	~	Any Tim	e		~		
< B	Back			Ca	ancel	Next >	

Figure 2-73 Tenable.OT Create Policy - Actions

	e Policy	Definition	Policy Actions
Evenciyp	e Policy	Demnition	Policy Actions
R	DP Connectio	on (Authenti	cated)
EVERITY *			
High	Medium	Low	None
MTP servers are no	ot configured		
ADDITIONAL ACTIO	NS		
ADDITIONAL ACTIO	NS st hit		
ADDITIONAL ACTIO	NS st hit		
ADDITIONAL ACTIO	NS 'st hit		

2.10 VMware Carbon Black App Control

VMWare Carbon Black App Control is an endpoint protection tool that provides multiple file integrity and application features, including application allow/deny listing and file modification or deletion protection. Carbon Black was used for Builds 1 and 4 as the application allowlisting (AAL) and file integrity checking tool.

2.10.1 Host and Network Configuration

The following tables (Table 2-27, Table 2-28, and Table 2-29) detail the host and network configuration of the Carbon Black App Control server for PCS and CRS.

Table 2-27 Carbon Black App Control Domain Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
Carbon Black Server	VMware ESXi VM	Windows Server 2016 Datacenter	4	8GB	500GB	Testbed LAN 10.100.0.52
Windows Server	Hyper-V VM	Windows Server 2012 R2	2	6GB	65GB	Testbed LAN 10.100.0.25
OSIsoft Pi Server	Hyper-V VM	Windows Server 2016 Standard	4	8GB	80GB/171GB	DMZ 10.100.1.4
Dispel VDI	Hyper-V VM	Windows Server 2016 Datacenter	2	8GB	126GB	N/A

Table 2-28 Carbon Black App Control PCS Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
PCS HMI Workstation	Supermicro Z97X-Ud5H	Windows 7	4	8GB	233GB	PCS 172.16.1.4
PCS Engineer- ing Work- station	Supermicro Z97X-Ud5H	Windows 7	4	16GB	465GB	PCS 172.16.3.10

Table 2-29 Carbon Black App Control CRS Hosts Deployment

Name	System	OS	CPU	Memory	Storage	Network
CRS Engi- neering Workstation	Dell Preci- sion T5610	Windows 10	8	16GB	465GB	CRS Supervi- sory 192.168.0.20
CRS OSIsoft Pi Server	Hyper-V VM	Windows Server 2016 Standard	4	16GB	80GB/171GB	CRS Supervi- sory 192.168.0.21

2.10.2 Installation

Prepare the Carbon Black App Control Server (fka CB_Protection) in accordance with the CB Protection Operating Environment Requirements v8.1.6 document that is provided for installation. This document, and all Carbon Black documentation, can be found on the website <u>https://community.carbonblack.com</u>.

1. Install Carbon Black App Control Server (fka CB_Protection) using these steps:

- a. Created the nccoeCarbon domain user account on LAN AD to be used for installation and administration of CB App Control Server and add this user to the local administrators' group on the server.
- b. Install SQL Server Express 2017 according to the CB Protection SQL Server Configuration v8.1.4 document.
- c. Install the CB App Control Server according to the CB Protection Server Install Guide v8.1.6 document.

2.10.3 Configuration

Follow these steps to configure Windows Server 2016:

- 1. On the Carbon Black App Control Server, configure Windows Server 2016:
 - Based on Carbon Black documentation (Figure 2-74), Windows Server 2016 will need to have the following features for the Internet Information Services (IIS) role enabled for Carbon Black to work (Figure 2-75).

Figure 2-74 Excerpt from Carbon Black Documentation on Support Server Requirements

bon Bl	ack.							
CB Prote	ction Web	Server Platfo	orm: Supp	ort Server				
Commo	n Requireme	ents 🛈		Restrictions [®]				
In the IIS configura Commo Stat Defi HTT HTT Applica ASF CGI ISAI Health HEALTH CGI ISAI Health HTT CGI ISAI HEALTH Req Trace Req ISA Perform Manage IIS I Mar FTP Pu	Roles Manage tion: on HTTP Featu- ic Content ault Document 'P Errors 'P Redirection tion developm P.NET (version T Extensibility PI Extensions PI Filters & Diagnostics: 'P Logging ging Tools usest Monitor big y: . Authorization usest Filtering nd Domaing nance: None ement Tools: Management Service bigshing Service	er, verify the followi ures: ent: 4.5) (version 4.5) estrictions console console conjots and Tools ice be: None	ng	Beginning with Protection AF can prevent of Onfigurat console and a green dot can assume Otherwise, restrictions: Site Binding The CB Prot the console address ins the list of bi IP Address If you must addresses, added to th Application CB Protecti application the CB Prot credentials Authenticat You must d Authenticat handles au able to log	th v8.0.0, the console relies on the CB Pl. An incorrectly configured IIS server console access. API functionality, go to System tion > Advanced Options in your current d check the "API Access Enabled" box. If appears next to the checkbox, then you e that IIS is configured correctly. make sure you meet the following : gs: tection API will not connect to localhost if : web application is bound to a specific IP tead of "*. Make sure that "*' is added to indings. and Domain Restrictions: limit console access to specific IP be sure that the IPv6 localhost address is e list. Pools: ion must be run within the DefaultAppPool pool. Using a different app pool results in tection server not having the appropriate to access the SQL Server database. ion: lisable Basic Authentication and Windows ion so that the CB Protection Server thentication. Otherwise, users will not be int to the CB Protection Server.			
Version	Part Of OS	Current Version	Supported Architectur e	Supporte d Level	Additional Notes/Requirements			
UC O F	Windows 2012		-84		③ ③ Common Requirements and Restrictions are listed in the table above			

x84

X64

Additional requirements: Private memory for IIS should be increased to 800 MB

Additional requirements: Private memory for IIS should be increased to 800 MB

① ② Common Requirements and Restrictions are listed in the table above

IIS 8.5

IIS 10

Server R2

only

Windows

2016

Server



Figure 2-75 IIS Configuration for Carbon Black, Server Roles

- 2. Manually update the Windows Server firewall configuration to allow inbound port 41002 traffic from CB App Control clients/agents.
- 3. Configure Policy in the Carbon Black Console using these steps:
 - a. In the CB App Control Console, go to Rules > Policies.
 - Create a new policy with the desired enforcement level. In this case, a high enforcement level was chosen to actively block execution of unapproved or banned executables (Figure 2-76).

Figure 2-76 Carbon Black Policy Edit

	曼 CB-Server.lan.lab Hon	ne 🕶 Repo	orts 🕶 As	sets 🕶	Rules 👻 🛛 Ta	ools 🕶		ø	
RULES O	Home » Policies » Policy Details (HighEnfe	omt_NOCOE)						Version 8.1.10.3	
Policies Policies	Edit Policy HighEnfort	_NCCOE						0	
Mappings	Policy Name:	HighEnfcmt_NC0	COE						
Notifiers	Description:	High Enforceme	nt Block Unapprov	ed or Banned		Ξ.			
Software Rules									
Updaters	Mode:	Visibility	Control O Disak	oled		_			
Rapid Configs	Enforcement Level	Connected		Disconnec	ted				
Publishers	Automotic Doline Anniorment	Нідп (вюск опа	pproved) 🗸	High (Bioc	k unapproved)	•			
Users	For New Computers:	U							
Directories	Set Manual Policy For Existing Computers:	There are cur	rently no compu	ters in this po	blicy.				
Files	Options:	🗹 Allow Upgrad	les 🔽 Track File	Changes					
Custom	20020 0 0	Load Agent i	n Safe Mode 🗔 S	Suppress Log	o In Notifier				
Memory	Total Computers:	0							
Registry	Connected Computers.	U							
Scripts	Advanced File Rules Cust	om Rules Men	nory Rules Re	gistry Rules	Publisher Rules	Rapid Configs	Computers	Device Control Settings	
Reputation	Name		Status	Notif	iers				
Event Rules	Block writes to unapproved remo	vable devices	Active	▼ <def< th=""><th>ault>: Block writes to</th><th>unapproved removab</th><th>e V Add Ed</th><th>lit</th></def<>	ault>: Block writes to	unapproved removab	e V Add Ed	lit	
Indicator Sets	Block writes to banned removable	e devices	Active	✓ <def< p=""></def<>	✓ ✓ default>: Block writes to banned removable devi ✓ Add Edit				
	Report reads from unapproved re	movable devices	Report On	v v <nor< th=""><th>18></th><th></th><th>~</th><th></th></nor<>	18>		~		

- 4. Enable AD Integration Features as follows:
 - a. Enable AD integration features on the CB App Control Console for domain user account login and AD-Based Policy mapping. AD-Based Policy mapping allows automatic policy assignment to be mapped to AD users, groups, computers, organizational units (OUs), etc., as configured by a CB App Control Console administrator (Figure 2-77).

Figure 2-77	Carbon	Black App	Control	System	Configuration
	Carbon	Didek App	Control	System	conngulation

	🧮 CB-Server.lan.lab	Home 🔻	Reports 🔻	Assets 🔻	Rules 🔻	Tools 🔻	
ADMINISTRATION G	General Events Security	Advanced Options	Mail Licensing Ext	ernal Analytics Co	onnectors SAML L	ogin	
Login Accounts			Ŭ			•	
Users	General Settings						
User Roles	Server Status						
User Role	Cb Protection	n Version: 8.1	.10.3				
Mappings	Server	r Address: CB-	Server.lan.lab				
System Configuration	Se	erver Port: 410	002				
General	Server T	imezone: -A	utomatic-	~			
Events	Database Schema	a Version: 8.1	.10.3				
	Database	Address: .\S	QLEXPRESS				
Security	Database A	uth.Type: NT					
Advanced Options	Datat	ase Size: 463	3.06 MB				
Mail	Free Local Di	SK Space: 480	J. I GB / 499.5 GB				
Licensing		L version. To:	55				
External Analytics	Active Directory / LDAP in	tegration					
Connectors	AD-Base	ed Logins: En	abled	~			
SAML Login	AD Securit	y Domain: lan.	lab				
Contained the other	AD-Bas	ed Policy: En	abled	~			
System Health	Windows	2000 DCs:					
Update Agent/Rule Versions	Test AD Con	inectivity:	Test Success				
	Agent Management						

- 5. Add users from AD and assign policies:
 - a. Add "Test Users" OU from the AD to policy mapping settings and assign the "High-Enfcmt_NCCOE" policy (Figure 2-78).

This OU includes the "nccoeUser" and "nccoeAdmin" user accounts created for the test scenarios. This policy will be automatically applied to these users logged in on any computer that is running the CB Protection Agent. The "HighEnfcmt_NCCOE" policy is set to High Enforcement level, which will actively block all unapproved or banned files, applications, or devices.

Figure 2-78 Carbon Black App Control AD Policy Mappings

	CB-Server.lan.lab	Home 🔻	Reports 🔻	Assets 🔻	Rules 🔻	Tools 🕶	٥
RULES 🕒	Home » Policies » Policy Mappin	System					Version 8.1.10.3
Policies Policies	Users can download Cb P Click here to view availabl	rotection Agent s e Cb Protection /	oftware from http: Agent/Rules versio	s://CB-Server.lan.lan.lan.lan.lan.lan.lan.la	ab/hostpkg		
Mappings	Active Directory	Policy Mapp	ings				0
Notifiers							
Software Rules	Policies Mappings						
Updaters	Add Rule						
Rapid Configs		Object	Relationship	Match		Action	Policy
Publishers	⋒⋈⋫₩	if User	is in OU	Test Users	6	move to	HighEnfort NCCOE
Users	G	[all others]	1011100	Test Users	0	apply policy from	Default Policy
Directories							
Files							
Custom							
Degistra							
Scripts							
https://cb-server.lan.lab/dashbo	pard.php?dbid=HOMEPAGE						

6. Download and install CB App Control Agent from CB App Control Server

(The process outlined below uses the CRS Engineering Workstation as an example, but the process was the same for all the agent computers.). Follow these steps:

- a. Open the browser on the CRS Engineering Workstation and enter the URL to download the agent installer: https://CB-Server.lan.lab/hostpkg. This URL is on the Carbon Black server itself and is accessed on the local network. CB-Server.lan.lab is the full host name we gave this server during installation.
 - i. If the host cannot access CB-Server.lan.lab, update the environment DNS Server by mapping the IP address, 10.100.0.52, to CB-Server.lan.lab or add the mapping to the local host file.
- b. Download the Windows CB App Control Agent installer from the CB App Control Server and install on the CRS Engineering Workstation (Figure 2-79).

Figure 2-79 Carbon Black Agent Download

Installing the Cb Protection Agent sol	ftware is simple:				
 Click the installation setup file f Download the installation setup From the download directory, do 	or the policy assigned to you by your netw file to a convenient location on your hard puble-click the newly downloaded file to in	vork administrator. I-drive. stall Cb Protection Agent.			
Cb Protection Agent Ins	tallation Setup Files				
Refresh Page					
Policy Name	Install Package	Description		Date Created 🔺	Date Modified
HighEnfomt_NCCOE	Windows, Red Hat	High Enforcement Block I	Jnapproved or Banned	Oct 27 2020 02:40:26 PM	Oct 29 2020 02:00:30 PM
1 item			Page 1/1		
			BitS Agent Preservat whe Windows configure Ob Protection Agent vib 1.8 Cancel		

c. Check the CB App Control Console to verify communication and initialization of the new CRS Engineering Workstation agent computer on the CB App Control Server (Figure 2-80).

Figure 2-80 Carbon Black App Control Computers

	GB-Server.lan.lab	Home 👻	Reports 🗸	Assets 👻	Rules 👻	Tools 👻		٠	? nccoecarbon@L. •			
ASSETS ©	Home - Computers		13					Ver	sion 8.1.10.3			
Computers												
Files	Computers								0			
Files on	Computers connected: 1	mputers connected: 1 Total computers: 1 Current CL version: 3050 CL version for upgrade: 1328										
Computers Applications	Saved Views: (none)	Saved Views: Group By: Days Disconnected: (none) Add (none) Ascending v										
Application Catalog	Show Filters * Show	Columns - Expo	ort to CSV Refre	<u>sh Page</u>								
Applications on	🚺 Action 🕶 Search:			Go Cle	ear							
computers	Computer Name	Connected	Policy Status	Upgrade Statu	s Connect	ed Enforcement	Disconnected Enforcement	IP Address	Policy			
Devices	C C LAN\POLARIS	•	Up to date	Up to date	High (Bl	ock Unapproved)	High (Block Unapproved)	10.100.0.20	-HighEnfcmt_NCCOE-			
Device Catalog	1 item				F	Page 1/1			25 V rows per page			
Computers												
Certificates												

- d. Approve all new trusted files and publishers that were added from the CRS Engineering Workstation to the catalog on the CB App Control Server.
- e. This image (Figure 2-81) shows the **CB Protection Files** page of the CB App Control Console.

Figure 2-81	Carbon	Black	Арр	Control	File	Catalog
-------------	--------	-------	-----	---------	------	---------

Cb Protectio	n - Files X	+							- 0
\rightarrow C	Cb-server.lan.lab/Fil	es.php?menu							९ ☆ 8
ROTECTIO	ON ScB-Server.lan.lab	Home - Reports -	Assets 🕶	Rules 🕶 To	ols -		0	0	nccoecarbon@L.
Saved Views (none)	:		Group By: (none)	✓ Ascending	Max Age:	Show Individ	ual Files		
Action -	Showing 75 out of 38876 iter	n(s)	resh Table						
Select 75	First Seen Date	First Seen Name	1	Publisher or Company	Product Name	Prevalence	Trust	Threat	Global State
□ 🛛 Q	Oct 30 2020 01:08:38 PM					0			Unapproved
Q	Oct 30 2020 01:04:05 PM	presentationhostdll.dll		Microsoft Corporation	Microsoft® .NET Framework	k 1	10	•	Approved
0 CQ	Oct 30 2020 01:04:05 PM	penimc.dll		Microsoft Corporation	Microsoft® .NET Framework	c 1	10	۲	Approved
0 CQ	Oct 30 2020 01:04:05 PM	servicemonikersupport.dll		Microsoft Corporation	Microsoft® .NET Framework	k 1	10	0	Approved
⊇ ⊘ Q	Oct 30 2020 01:04:05 PM	servicemonikersupport.dll		Microsoft Corporation	Microsoft® .NET Framework	k 1	9	۲	Approved
□ ♂ Q	Oct 30 2020 01:04:05 PM	smconfiginstaller.exe		Microsoft Corporation	Microsoft® .NET Framework	k 1		0	Approved
	Oct 30 2020 01:04:04 PM	system.web.dll		Microsoft Corporation	Microsoft® .NET Framework	k 1	8	۲	Approved
Q		And a state of the state of the state		Microsoft Corporation	Microsoft® .NET Framework	< 1	1111 10	0	Approved
] ₽ Q	Oct 30 2020 01:04:04 PM	system.web.dll						1.00	
030 030 030	Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM	system.web.dll		Microsoft Corporation	Microsoft® .NET Framework	< 1	8	0	Approved
0 2 q 0 2 q 0 2 q	Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM	system.web.dll system.web.dll system.printing.dll		Microsoft Corporation Microsoft Corporation	Microsoft® .NET Framework Microsoft® .NET Framework	k 1 k 1	10	0	Approved
	Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM	system.web.dll system.web.dll system.printing.dll system.printing.dll		Microsoft Corporation Microsoft Corporation Microsoft Corporation	Microsoft® .NET Framework Microsoft® .NET Framework Microsoft® .NET Framework	k 1 k 1 k 1	10 10 10 10	0	Approved Approved Approved

2.11 Windows Software Restriction Policy (SRP)

Windows SRP is a feature that is a part of the Windows operating system. It identifies applications that are running on any domain-controlled computer, and it can block any programs that have not been allow-listed. Configuring Windows SRP is done through group policy object management. Windows SRP was used for AAL in Builds 2 and 3.

2.11.1 Host and Network Configuration

Windows SRP configuration is established by Group Policy Objects (GPOs) located on the two AD servers. The domain controllers were common across all builds as detailed in Table 2-30.

Name	System	OS	CPU	Memory	Storage	Network
AD (Primary) Server	Hyper-V VM	Windows 2012R2	2x vCPU	2 GB	45 GB	Testbed LAN 10.100.0.17
AD (Second- ary) Server	Hyper-V VM	Windows 2012R2	1x vCPU	2 GB	21 GB	Testbed LAN 10.100.0.13

Table 2-30 Windows SRP Domain Servers

The following systems were configured to utilize Windows SRP for each build. Additional details for each build are available in Section 4.5 of Volume B.

Build 2 supports the testing within the PCS environment. The overall build architecture is provided in Figure B-2. The Windows SRP specific components are in Table 2-31.

Table 2-31 Windows SRP Build 2 Deployment

Name	System	OS	CPU	Memory	Storage	Network
Windows Server	Hyper-V VM	Windows 2012R2	2x vCPU	6 GB	65 GB	Testbed LAN 10.100.0.25
Dispel VDI	Hyper-V VM	Windows 2016	2x vCPU	8 GB	126 GB	DMZ LAN 10.100.1.61
DMZ Historian	Hyper-V VM	Windows 2016	4x vCPU	8 GB	80 GB, 171 GB	DMZ LAN 10.100.1.4
Engineering Workstation	HP Z230 Workstation	Windows 7	Intel i5- 4570	16 GB	465 GB	172.16.3.10
HMI Host	Generic	Windows 7	Intel i5- 4590	8 GB	233 GB	PCS VLAN 1 172.16.1.4

Build 3 supports the testing within the CRS environment. The overall build architecture is provided in <u>Figure B-3</u>. The Windows SRP specific components are in Table 2-32.

Name	System	OS	CPU	Memory	Storage	Network
Windows Server	Hyper-V VM	Windows 2012R2	2x vCPU	6 GB	65 GB	Testbed LAN 10.100.0.25
DMZ Historian	Hyper-V VM	Windows 2016	4x vCPU	8 GB	80 GB, 171 GB	DMZ LAN 10.100.1.4
Engineering Workstation	Dell T5610	Windows 10	2x Intel E3-2609 v2	16 GB	465 GB	CRS Supervi- sory LAN 192.168.0.20
CRS Local His- torian	Hyper-V VM	Windows 2016	4x vCPU	16 GB	80 GB <i>,</i> 171 GB	CRS Supervi- sory LAN 192.168.0.21

2.11.2 Installation

Windows SRP is a feature of the Windows operating system and therefore did not require any specific installation for use in the project.

2.11.3 Configuration

The Windows SRP configuration required setting GPOs on the AD servers to enable the policy on all hosts that were part of the Windows domain. Additionally, hosts that were not part of the Windows domain had GPO settings configured locally to the host. Follow these steps to configure AD with user accounts and set enforcement policies:

- 1. Set up AD with a "Test User" OU and add the NCCOE User (nccoeUser) and Admin (nccoeAdmin) accounts for this project to the OU.
- 2. To allow the NCCOE Admin account to be included as a local administrator within the environment, modify the Default Domain GPO to add administrators to the Restricted Group and include the NCCOE Admin account.
- To support applying GPOs as local settings to non-domain computers, download LGPO.zip from Microsoft Security Compliance Toolkit 1.0 available at <u>https://www.microsoft.com/en-us/download/details.aspx?id=55319</u>.
- 4. Review the National Security Agency (NSA) Guidance for Application Whitelisting using Software Restriction Policies and Guidelines for Application Whitelisting ICSs available at <u>https://www.iad.gov/iad/library/reports/application-whitelisting-using-srp.cfm</u> and <u>https://www.iad.gov/iad/library/ia-guidance/security-configuration/industrial-control-</u> <u>systems/guidelines-for-application-whitelisting-industrial-control-systems.cfm</u> respectively.
- 5. Create the Windows SRP GPO with the following settings:
 - a. From the **Enforcement Properties** dialog (Figure 2-82):
 - i. Select the All Software Files radio button.
 - ii. Select the All Users radio button.





- b. In the Group Policy Management Editor, in the Security Levels folder:
 - i. Double-click the **Disallowed** security level to open the **Disallowed Properties** window.
 - ii. Click the Set as Default radio button (Figure 2-83) to configure SRP in allowlist mode. After completing this step, only programs in the paths specified by the environment variables SYSTEMROOT (typically C:\Windows), PROGRAMFILES (C:\Program Files), and PROGRAMFILES(x86) (C:\Program Files (x86)) are permitted to execute. These path rules are automatically added when the "Disallowed" security level is set as the default.





- c. Customize the Allowlist Rules to enhance security by disallowing specific subfolders in the default allowed paths and to support organization application requirements.
 - i. Click the **Additional Rules** folder and apply the rules shown in Figure 2-84. This figure combines the NSA recommended path settings in addition to lab application requirements and for disabling installers and other executable content as indicated in the comments. *Organizations should audit their environments to determine the appropriate rules to define within the policy*.

Figure 2-84 Additional Rules Defined for Lab Environment

lame 🔺	Type	Security Level	Description
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Path	Unrestricted	Default System Root Allow Rule
] %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Debug	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\PCHEALTH\ERRORREP	Path	Disallowed	Deny execution per NSA Guidance
]%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Registration	Path	Disallowed	Deny execution per NSA Guidance
SHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\catroot2	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\com\dmp	Path	Disallowed	Deny execution per NSA Guidance
3 %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\FxsTmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\spool\drivers\c	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\spool\PRINTERS	Path	Disallowed	Deny execution per NSA Guidance
SHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\Tasks	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Systme32\spool\SERVERS	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\com\dmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\FxsTmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\Tasks	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Tasks	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Temp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\tracing	Path	Disallowed	Deny execution per NSA Guidance
3 %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)%	Path	Unrestricted	Allow 32-bit Program Files on 64 bit systems.
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Path	Unrestricted	Default Program Files Directory Allow Rule
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Path	Unrestricted	Temp rule for Workstations Allow OneDrive
%USERPROFILE%\Forescout Console 8.2.1	Path	Unrestricted	Temporary Rule to Allow Forescout Console
*Jnk	Path	Unrestricted	Allow Links to executables
*.msi	Path	Disallowed	Prevent installers from executing
\\%USERDNSDOMAIN%\Sysvol\	Path	Unrestricted	Allow Domain Login Scripts
C:\TwinCAT	Path	Unrestricted	Added to support CRS PLC Programming
E\\Program Files	Path	Unrestricted	Approved alternate Program Files Location
E:\Program Files (x86)	Path	Unrestricted	Approved alternate 32-bit Program Files locat
finanas eve	Path	Disallowed	Denv execution per NSA Guidance

- 6. Link the GPO to the Test User OU:
 - a. In the Group Policy Management tool, right click the "Test User" OU and select Link an Existing GPO from the pop-up menu (Figure 2-85).

Figure 2-85 Menu Options for Accessing the Link an Existing GPO Option

 Group Policy Management ▲ Forest: lan.lab ▲ Domains ▲ a lan.lab ☑ Default Domain Policy ▷ Domain Controllers ▷ Groups ▷ LAN ▷ Linux ▷ PCS ▷ System Accounts 		Test Users			
		Linked Group Policy	Objects	Group Policy Inheritance	Delegation
		This list does not include any GPOs linked to sites. For more details, see			
		Precedence	G	GPO	
			Default Domain Policy		
Image: Sites Image: Create a GPO in this of Group ▷ Image: Group		omain, and Link it her	e		
값 Group Polics 같은 Group Polics	Group Policy Modelin New Organizational U	g Wizard nit			
	View New Window from He	re		•	
	Delete Rename Refresh				
	Properties				
	Help				

b. In the dialog box, select the **Windows SRP GPO Object** from the list and click **OK** (Figure 2-86).

Figure 2-86 Dialog Box for Selecting GPO to Link

Select GPO	X
Look in this domain:	
lan.lab	~
Group Policy objects:	
Name	~
DoD Windows Server 2012 R2 Domain Controller STIG User v2r18 DoD Windows Server 2012 R2 Member Server STIG Computer v2 DoD Windows Server 2012 R2 Member Server STIG User v2r18 Enable Remote Desktop New Group Policy Object OPC_Security01 Process_Audit_Policy USB Disable	=
Windows SRP WSUS_Policy	~
ОК	Cancel

(Optional) Install GPO as the local policy on non-domain systems; for systems that are not joined to the domain, the nccoeUser and nccoeAdmin accounts are created as local user and administrator accounts, respectively. Additionally, the Windows SRP GPO is manually applied to the local system using the LGPO.exe application contained in the ZIP file from Step 3.

- c. Create a Backup of the Windows SRP GPO Object:
 - i. From the Group Policy Manager, select the **Group Policy Objects** folder and rightclick on the Windows SRP GPO object.
 - ii. Select the **Back Up...** option from the pop-up menu.
 - iii. In the dialog box, choose a destination location such as *C*:*Backup GPO Folder* or some other convenient location to place the files and click **Back Up**.
- d. Copy the LGPO.exe along with the files created in the previous step to the non-domain computer system.
- e. Login as an administrator on the non-domain computer and navigate to the **{GUID}\Do**mainSysvol\GPO\User folder, which should contain the **registory.pol** file for the GPO.

f. Execute the following commands to apply the settings to the local nccoeUser and nccoeAdmin accounts:

lgpo.exe /u:nccoeUser registory.pol
lgpo.exe /u:nccoeAdmin registory.pol

Appendix A List of Acronyms

AAL	Application Allowlisting
AD	Active Directory
AF	Asset Framework
BAD	Behavioral Anomaly Detection
CRS CRADA	Collaborative Robotic System Cooperative Research and Development Agreement
CSF	NIST Cybersecurity Framework
CSMS	Cybersecurity for Smart Manufacturing Systems
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
FOIA	Freedom of Information Act
GPO	Group Policy Object
HDD	Hard Disk Drive
ICS	Industrial Control System
IIS	Internet Information Services
ют	Internet of Things
ІТ	Information Technology
LAN	Local Area Network
MFA	Multifactor Authentication
MTD	Moving Target Defense
ΝΑΤ	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
NSA	National Security Agency
NTP	Network Time Protocol
от	Operational Technology

OU	Organizational Unit
PCS	Process Control System
PI	Process Information
PLC	Programmable Logic Controller
POU	Program Organizational Unit
RDP	Remote Desktop Protocol
SP	Special Publication
SPAN	Switch Port Analyzer
SRP	Software Restriction Policy
VDI	Virtual Desktop Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network

Appendix B Build Architecture Diagrams

Figure B-1 Build 1 Architecture Diagram



Figure B-2 Build 2 Architecture Diagram



Figure B-3 Build 3 Architecture Diagram



Figure B-4 Build 4 Architecture Diagram

