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

Joseph Brule* Cyber Security Directorate National Security Agency

Michael Pease Keith Stouffer CheeYee Tang Timothy Zimmerman

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

Matthew Zopf

Strativia Largo, Maryland

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

September 2021

DRAFT

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





1 **DISCLAIMER**

- 2 Certain commercial entities, equipment, products, or materials may be identified in this document in
- 3 order to describe an experimental procedure or concept adequately. Such identification is not intended
- 4 to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE;
- 5 neither is it intended to imply that entities, equipment, products, or materials are necessarily the best
- 6 available for the purpose.
- 7 While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk
- 8 through outreach and application of standards and best practices, it is the stakeholder's responsibility to
- 9 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise,
- 10 and the impact should the threat be realized before adopting cybersecurity measures such as this
- 11 recommendation.
- 12 Domain name and IP addresses shown in this guide represent an example domain and network
- 13 environment to demonstrate the NCCoE project use case scenarios and the security capabilities.
- 14 National Institute of Standards and Technology Special Publication 1800-10C, Natl. Inst. Stand. Technol.
- 15 Spec. Publ. 1800-10C, 128 pages, September 2021

16 **FEEDBACK**

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

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

28 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

44 NIST CYBERSECURITY PRACTICE GUIDES

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

54 ABSTRACT

- 55 Today's manufacturing organizations rely on industrial control systems (ICS) to conduct their operations.
- 56 Increasingly, ICS are facing more frequent, sophisticated cyber attacks—making manufacturing the
- 57 second-most targeted industry (C. Singleton et al., X-Force Threat Intelligence Index 2021, IBM, February
- 58 2021, <u>https://www.ibm.com/security/data-breach/threat-intelligence</u>). Cyber attacks against ICS
- 59 threaten operations and worker safety, resulting in financial loss and harm to the organization's
- 60 reputation.
- 61 The architecture and solutions presented in this guide are built upon standards-based, commercially
- 62 available products, and represent some of the possible solutions. The solutions implement standard
- 63 cybersecurity capabilities, such as behavioral anomaly detection, application allowlisting, file integrity-
- 64 checking, change control management, and user authentication and authorization. The solution was
- 65 tested in two distinct lab settings: a discrete manufacturing work cell, which represents an assembly line

- 66 production, and a continuous process control system, which represents chemical manufacturing
- 67 industries.
- 68 Organizations that are interested in protecting the integrity of the manufacturing system and
- 69 information from destructive malware, insider threats, and unauthorized software should first conduct a
- 70 risk assessment and determine the appropriate security capabilities required to mitigate those risks.
- 71 Once the security capabilities are identified, the sample architecture and solution presented in this
- 72 document may be used.
- 73 The security capabilities of the example solution are mapped to NIST's Cybersecurity Framework, the
- 74 National Initiative for Cybersecurity Education Framework, and NIST Special Publication 800-53.

75 **KEYWORDS**

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

79 ACKNOWLEDGEMENTS

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

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

- 81 The Technology Partners/Collaborators who participated in this build submitted their products in
- 82 response to a notice in the Federal Register. Respondents with relevant products were invited to sign a

- 83 Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in
- 84 a consortium to build this example solution. The participants in this project were:

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)
Dragos	Dragos Platform
Forescout	eyeInspect (Formerly SilentDefense) ICS Patrol EyeSight
GreenTec	WORMdisk and ForceField
OSIsoft (now part of AVEVA)	PI System (which comprises products such as PI Server, PI Vision and others)
TDi Technologies	ConsoleWorks
<u>Tenable</u>	Tenable.ot

85 **DOCUMENT CONVENTIONS**

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

93 CALL FOR PATENT CLAIMS

- 94 This public review includes a call for information on essential patent claims (claims whose use would be
- 95 required for compliance with the guidance or requirements in this Information Technology Laboratory
- 96 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
- 97 or by reference to another publication. This call also includes disclosure, where known, of the existence
- 98 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
- 99 unexpired U.S. or foreign patents.
- 100 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in
- 101 written or electronic form, either:

- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does notcurrently intend holding any essential patent claim(s); or
- b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
- 106 publication either:
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
 or
- without compensation and under reasonable terms and conditions that are demonstrably free
 of any unfair discrimination.
- 111 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
- 112 behalf) will include in any documents transferring ownership of patents subject to the assurance,
- 113 provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,
- and that the transferee will similarly include appropriate provisions in the event of future transfers with
- 115 the goal of binding each successor-in-interest.
- 116 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
- 117 whether such provisions are included in the relevant transfer documents.
- 118 Such statements should be addressed to: <u>manufacturing nccoe@nist.gov</u>

119 **Contents**

120	1	Intr	oducti	ion	1
121		1.1	How to	o Use this Guide	1
122		1.1	Build C	Dverview	2
123		1.2	Typogr	aphic Conventions	2
124		1.3	Logical	Architecture Summary	3
125	2	Pro	duct Ir	nstallation Guides	5
126		2.1	Dispel	Remote Access	5
127			2.1.1	Host and Network Configuration	6
128			2.1.2	Installation	7
129			2.1.3	Configuration	8
130		2.2	Dragos	5	. 12
131			2.2.1	Host and Network Configuration	12
132			2.2.2	Installation	13
133			2.2.3	Configuration	13
134		2.3	Foresc	out Platform	.17
135			2.3.1	Host and Network Configuration	19
136			2.3.2	Installation	20
137			2.3.3	Configuration	22
138		2.4	Green	Гес-USA	.31
139			2.4.1	Host and Network Configuration	32
140			2.4.2	Installation	32
141			2.4.3	Configuration	33
142		2.5	Micros	oft Azure Defender for IoT	.36
143			2.5.1	Host and Network Configuration	36
144			2.5.2	Installation	36
145			2.5.3	Configuration	36
146		2.6	OSIsof	t PI Data Archive	.41
147			2.6.1	Host and Network Configuration	41
148			2.6.2	Installation	42
149			2.6.3	Configuration	43
150		2.7	Securit	y Onion	.64
151			2.7.1	Host and Network Configuration	64

152		2.7.2	Installation	65
153		2.7.3	Configuration	65
154	2.8	TDi Co	onsoleWorks	68
155		2.8.1	Host and Network Configuration	68
156		2.8.2	Installation	68
157		2.8.3	Configuration	75
158	2.9	Tenab	le.OT	97
159		2.9.1	Host and Network Configuration	97
160		2.9.2	Installation	97
161		2.9.3	Configuration	97
162	2.10	VMwa	are Carbon Black App Control	
163		2.10.1	Host and Network Configuration	105
164		2.10.2	Installation	106
165		2.10.3	Configuration	107
166	2.11	Windo	ows Software Restriction Policy	
167		2.11.1	Host and Network Configuration	114
168		2.11.2	Installation	115
169		2.11.3	Configuration	115
170	Append	A xib	List of Acronyms	
171	Append	dix B	Build Architectures Diagrams	

172 List of Figures

173	Figure 1-1: CSMS Network Architecture
174	Figure 2-1 Dispel High-level Implementation, from Remote Access for ICS
175	Figure 2-2 Mapping a Network Drive11
176	Figure 2-3 Authentication to File Server
177	Figure 2-4 Dragos OSIsoft PI Server Integration
178	Figure 2-5 Dragos PI Web API Configuration14
179	Figure 2-6 OSIsoft PI Server to Dragos Asset and Data Pairing15
180	Figure 2-7 OSIsoft PI Server and Dragos Paired Data Elements15
181	Figure 2-8 Dragos Zone Administration Page16
182	Figure 2-9 Dragos Create Zone Pop-up17
183	Figure 2-10 Forescout High-Level Components and Dataflows18
184	Figure 2-11 Forescout SecureConnector Distribution Tool21
185	Figure 2-12 Forescout Agent Download21
186	Figure 2-13 eyeInspect Sensor Admin/Overview Page – Add Sensor22
187	Figure 2-14 Adding a New SilentDefense Sensor Dialog23
188	Figure 2-15 eyeInspect ICMP Protocol/Port Scan Attempt Settings24
189	Figure 2-16 eyeInspect Sensor Configuration Options24
190	Figure 2-17 eyeInspect Portscan Detection Settings25
191	Figure 2-18 Add ICS Patrol Sensor Dialog26
192	Figure 2-19 ICS Patrol Sensor Admin Page
193	Figure 2-20 Add an ICS Patrol Scan Policy28
194	Figure 2-21 eyeSight Add Dialog – General Information
195	Figure 2-22 eyeSight Add – Command Center Credentials
196	Figure 2-23 eyeSight OT Settings
197	Figure 2-24 eyeSight Test Connection Successful Message
198	Figure 2-25 Azure Defender for IoT SSH Session for Network Configuration37
199	Figure 2-26 Azure Defender for IoT Create New Data Mining Report for AMS Protocol Information38
200	Figure 2-27 Azure Defender for IoT Custom Alert for Firmware Major Version Number Change
201	Figure 2-28 Azure Defender for IoT Custom Alert for Firmware Minor Version Number Change40
202	Figure 2-29 Azure Defender for IoT Custom Alert for Firmware Build Version Number Change40

203	Figure 2-30 Screenshot of the PI Interface Configuration Utility before the Interface is configured44
204 205	Figure 2-31 Screenshot of the PI Data Collection Manager Displaying Green Checkmarks After the PI System Connector is Properly Configured45
206 207	Figure 2-32 Screenshot of the PI Interface Configuration Utility Showing the Added Scan Class # 2 for Polling the PLC Every 60 Seconds
208 209	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
210 211	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
212 213	Figure 2-35 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Event Frame Template
214 215	Figure 2-36 Screenshot of PI System Explorer Displaying the TwinCAT Version Mismatch Event Frame Template
216 217	Figure 2-37 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Analysis Template in the PLC Element Template
218 219	Figure 2-38 Screenshot of PI System Explorer Displaying the TwinCAT Firmware Version Mismatch Analysis Template in the PLC Element Template
220	Figure 2-39 Wazuh Agent Manager
221	Figure 2-40 ossec.conf File
222	Figure 2-41 Wazuh Agent Manager User Interface67
223	Figure 2-42 Log Received After a File Change Was Detected67
224	Figure 2-43 ConsoleWorks Registration Screen
225	Figure 2-44 ConsoleWorks Offline Registration Process
226	Figure 2-45 ConsoleWorks System Backups74
227	Figure 2-46 ConsoleWorks Importing System Configurations and Components75
228	Figure 2-47 ConsoleWorks Password Settings
229	Figure 2-48 ConsoleWorks Add the Local Graphical Gateway for RDP Access77
230	Figure 2-49 ConsoleWorks Example Device Type Definition
231	Figure 2-50 ConsoleWorks List of Device Types
232	Figure 2-51 ConsoleWorks Example Device Definition
233	Figure 2-52 ConsoleWorks List of PCS (Build 1) Devices
234	Figure 2-53 ConsoleWorks List of CRS (Build 3) Devices
235	Figure 2-54 ConsoleWorks Example RDP Configuration
236	Figure 2-55 ConsoleWorks List of PCS (Build 1) RDP Connections

237	Figure 2-56 ConsoleWorks List of CRS (Build 3) RDP Connections
238	Figure 2-57 ConsoleWorks Example Console (SSH) Connection87
239	Figure 2-58 ConsoleWorks Example Console (Web Forward) Connection
240	Figure 2-59 ConsoleWorks List of PCS (Build 1) Console Connections
241	Figure 2-60 ConsoleWorks List of CRS (Build 3) Console Connections
242	Figure 2-61 ConsoleWorks List of Tags for PCS (Build 1)91
243	Figure 2-62 ConsoleWorks Example Tag Definition Screen92
244	Figure 2-63 ConsoleWorks Example Profile95
245	Figure 2-64 Tenable.OT Local Device Setting for NTP Service98
246	Figure 2-65 Tenable.OT Asset Discovery Settings99
247	Figure 2-66 Tenable.OT Controller Scans
248	Figure 2-67 Tenable.OT Network Scan Settings
249	Figure 2-68 Tenable.OT Create Asset Group Type101
250	Figure 2-69 Tenable.OT Create Asset Group Definition
251	Figure 2-70 Tenable.OT Policy Settings
252	Figure 2-71 Tenable.OT Create Policy – Event Type Options
253	Figure 2-72 Tenable.OT Create Policy - Definition104
254	Figure 2-73 Tenable.OT Create Policy - Actions
255	Figure 2-74 Excerpt from Carbon Black Documentation on Support Server Requirements108
256	Figure 2-75 IIS Configuration for Carbon Black, Server Roles109
257	Figure 2-76 Carbon Black Policy Edit110
258	Figure 2-77 Carbon Black App Control System Configuration111
259	Figure 2-78 Carbon Black App Control AD Policy Mappings112
260	Figure 2-79 Carbon Black Agent Download113
261	Figure 2-80 Carbon Black App Control Computers113
262	Figure 2-81 Carbon Black App Control File Catalog114
263	Figure 2-82 Setting Enforcement Properties
264	Figure 2-83 Setting Security Level Default
265	Figure 2-84 Additional Rules Defined for Lab Environment119
266	Figure 2-85 Menu Options for Accessing the Link an Existing GPO Option120
267	Figure 2-86 Dialog Box for Selecting GPO to Link

268	Figure B - 1 Build 1 Architecture Diagram	125
269	Figure B - 2 Build 2 Architecture Diagram	126
270	Figure B - 3 Build 3 Architecture Diagram	127
271	Figure B - 4 Build 4 Architecture Diagram	128

272 List of Tables

273	Table 2-1 Dispel Deployment	6
274	Table 2-2 Firewall Rules for Dispel	9
275	Table 2-3 Firewall Rules	10
276	Table 2-4 Dragos Deployment	12
277	Table 2-5 Forescout Deployment	19
278	Table 2-6 eyeSight Agent Deployment	19
279	Table 2-7 Firewall Rules for Forescout	20
280	Table 2-8 GreenTec-USA WORMdrive and ForceField Deployment	32
281	Table 2-9 Microsoft Azure Defender IoT Deployment	36
282	Table 2-10 OSIsoft PI Domain Hosts Deployment	41
283	Table 2-11 OSIsoft PI CRS Hosts Deployment	41
284	Table 2-12 OSIsoft PI PCS Hosts Deployment	41
285	Table 2-13 Security Onion Domain Hosts Deployment	64
286	Table 2-14 Security Onion PCS Hosts Deployment	65
287	Table 2-15 Security Onion CRS Hosts Deployment	65
288	Table 2-16 ConsoleWorks Build 1 Deployment	68
289	Table 2-17 ConsoleWorks Build 3 Deployment	68
290	Table 2-18 ConsoleWorks Device Type List	78
291	Table 2-19 ConsoleWorks PCS (Build 1) Devices	80
292	Table 2-20 ConsoleWorks CRS (Build 3) Devices	81
293	Table 2-21 ConsoleWorks PCS (Build 1) Graphical Connections	84
294	Table 2-22 ConsoleWorks CRS (Build 3) Graphical Connections	86
295	Table 2-23 ConsoleWorks PCS (Build 1) Console Connections	88
296	Table 2-24 ConsoleWorks CRS (Build 3) Console Connections	89

297	Table 2-25 Tenable.OT Appliance Details.	97
298	Table 2-26 Firewall Rules for Tenable.OT	97
299	Table 2-27 Carbon Black App Control Domain Hosts Deployment	106
300	Table 2-28 Carbon Black App Control PCS Hosts Deployment	106
301	Table 2-29 Carbon Black App Control CRS Hosts Deployment	106
302	Table 2-30 Windows SRP Domain Servers	114
303	Table 2-31 Windows SRP Build 2 Deployment	115
304	Table 2-32 Windows SRP Build 3 Deployment	115

305 **1 Introduction**

The following volume of this guide show 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.

313 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
- 316 solutions, specifically focusing on information and system integrity. This reference design is modular and
- can be deployed in whole or in part.
- 318 This guide contains three volumes:
- 319 NIST SP 1800-10A: Executive Summary
- 320 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)
- 323 Depending on your role in your organization, you might use this guide in different ways:

324 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:
- 327 challenges that enterprises face in ICS environments in the manufacturing sector
- example solution built at the NCCoE
- 329 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 3.4.1, 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.
- 346 This guide assumes that IT professionals have experience implementing security products within the 347 enterprise. While we have used a suite of commercial products to address this challenge, this guide does 348 not endorse any products. Your organization can adopt this solution or one that adheres to these 349 guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of 350 this manufacturing ICS solution. Your organization's security experts should identify the products that 351 will best integrate with your existing tools and IT system infrastructure. We hope that you will seek 352 products that are congruent with applicable standards and best practices. Section 3.5, Technologies, in 353 NIST SP 1800-10B, lists the products that we used and maps them to the cybersecurity controls provided
- by this reference solution.
- 355 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

357 success stories will improve subsequent versions of this guide. Please contribute your thoughts to

358 <u>manufacturing_nccoe@nist.gov</u>.

359 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.

367 **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

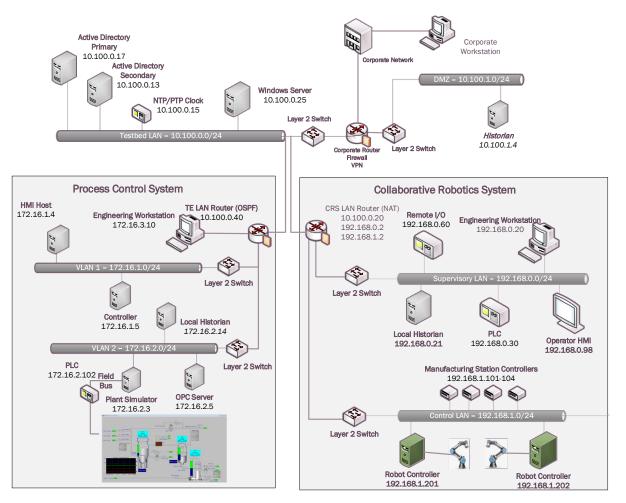
368 The following table presents typographic conventions used in this volume.

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> .

369 1.3 Logical Architecture Summary

- 370 The security mechanisms and technologies were integrated into the existing NIST Cybersecurity for
- 371 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
- 373 emulate common manufacturing environments. For more information see An Industrial Control System
- 374 *Cybersecurity Performance Testbed*, NISTIR 8089,
- 375 http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.
- 376 Typically, manufacturing organizations have unique cyber-ecosystems and specific needs for their
- 377 operations. To demonstrate the modularity and interoperability of the provided solutions, this project
- 378 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
- 381 Wazuh), native operating system features (Windows Software Restriction Policies [SRP]), and a Cisco
- 382 Adaptive Security Appliance (ASA) device configured with the AnyConnect VPN client.
- 383 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
- 386 for time synchronization. Additionally, the environment utilizes virtualized Active Directory (AD) servers
- 387 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.

390 Figure 1-1: CSMS Network Architecture



- 391 In summary, there are six networks within the CSMS architecture:
- 392 **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
- 394 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
- 397 environment.
- 398 DMZ: A demilitarized zone that separates the corporate network from the operational technology (OT)
 399 network. Many of the collaborators' products are also installed in the DMZ. The DMZ is used across the
 400 PCS and CRS environments.
- 401 PCS Virtual Local Area Network (VLAN) 1: This is the operations LAN within the PCS environment. This
 402 LAN simulates a central control room environment. The gateway interface for this network segment is
 403 172.16.1.1
- 404 **PCS VLAN 2:** This is the supervisory LAN within the PCS environment. This LAN simulates the process 405 operation/manufacturing environment, which consists of the operating plant, programmable logic

- 406 controller (PLC)s, object linking and embedding for process control (OPC) server, and data historian. The
- 407 gateway interface for this network segment is 172.16.2.1
- 408 **CRS Supervisory LAN:** This LAN is within the CRS environment. The historian, PLCs, operating human
- 409 machine interface (HMI), Engineering workstation, and remote input/output devices are connected to
- 410 this network. The gateway interface for this network segment is 192.168.0.2
- 411 **CRS Control LAN**: This LAN is within the CRS environment. The robot controllers and manufacturing
- 412 station controllers are connected to this network. The gateway interface for this network segment is
- 413 192.168.1.2
- The test bed networks used static IPv4 addresses exclusively, and the subnet masks were set to
- 415 255.255.255.0. No IPv6 addresses were used. This setup is consistent with industry practice. Specific
- 416 Internet Protocol (IP) addresses are listed for each component in the following sections.
- 417 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,
- 419 Collaborative Robotics System.

420 **2 Product Installation Guides**

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

423 2.1 Dispel Remote Access

- Dispel is a remote access tool for OT environments that provides secure remote access to the industrial
- 425 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
- 427 network. Dispel supports both user authentication and authorization, and remote access for Builds 2
- 428 and 4.

429 Virtual Desktop Interfaces (VDIs)

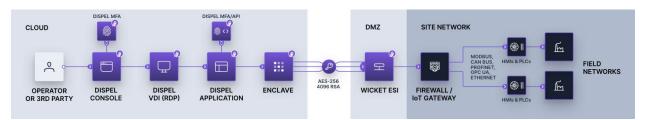
- 430 VDIs are Virtual Machines (VMs) that reside in the cloud and allow users to connect using Remote
- 431 Desktop Protocol (RDP). The VDIs establish a secure connection to the Wicket ESI located in the OT
- 432 network to provide network access to the OT devices.

433 Enclave

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

440 Wicket ESI

- 441 Wicket ESIs are on-premise components, shown in Figure 2-1, that allows users to connect to the OT
- 442 network remotely. These devices establish encrypted connections from the local OT network up to an
- 443 Enclave which, in turn, is connected to the VDI, allowing a remote user to access the OT devices.
- 444 Additional information is available in *Remote Access for Industrial Control Systems* from Dispel.io at:
- 445 <u>https://s3.amazonaws.com/downloads.dispel.io/resources/One+Pager/dispel-ics-</u>
- 446 <u>brochure_20190529.pdf</u>
- 447 Figure 2-1 Dispel High-level Implementation, from Remote Access for ICS



448 2.1.1 Host and Network Configuration

- 449 The Wicket ESI is connected to two ports within the DMZ, one for supporting outbound communications
- 450 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
- 452 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

453 Table 2-1 Dispel Deployment

454 2.1.2 Installation

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

458 After connecting the WAN and LAN network cables, configuring the Wicket ESI required connecting a

- 459 monitor, keyboard, and mouse to the unit using the available VGA and USB ports. Logging into the unit
- 460 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
- 462 performed using Sudo).
- 463 1. Update the network interfaces with the IP configuration information:

464 #> 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>
```

465 2. Update the Wicket ESI netcutter.cfg file to include the local subnet information (toward the466 bottom of the file):

467 #> 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";
});
```

468 3. Restart the Wicket services with the following command:

469 **#> service wicket restart**

- 4704. Check the log for errors and test connectivity to the Dispel environment (note: IP address will be account specific):
- 472 #> tail -f /home/ubuntu/wicket/wicket.log

473 2.1.3 Configuration

474 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

- 477 remote access to the ICS environments.
- 478 For full documentation and configuration instructions, see the Dispel documentation at
 479 https://intercom.help/dispel/en/.
- 480 Dispel created an organization named "NCCOE" with an Enclave name "NCCoE-Manufacturing" in their
- 481 pre-production staging environment. A single "user" account was created for accessing the cloud
- 482 infrastructure environment named nccoe-m-user@dispel.io. Organizations will need to plan for
- 483 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

485 separate from the user accounts used to login to the VDI environment.

- 486 The staging environment was configured without the Dispel multifactor authentication (MFA) settings
- 487 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
- 489 important for implementation and is strongly encouraged when planning the implementation. For this
- 490 effort, to reduce the risk of not having the MFA implementation, NCCoE worked with Dispel to limit
- 491 access to the cloud infrastructure and the VDI instances to only approved source IP addresses. *The*
- 492 additional protection of restricting access to the cloud infrastructure and VDI instances is also
- 493 encouraged to reduce the risks associated with the internet-accessible web and RDP services.

494 **Configure Firewall Settings**:

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

498 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

499 Notes:

500	•	Dispel's recommended rule for allowing secure shell (SSH)for installation and remote support
501		from the Dispel environment was not enabled for this effort.

- The rules implemented included 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.

506 **Configure Virtual Desktop Infrastructure (VDI):**

507 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 508 environment and then have the access to the environment configured by the device and firewall 509 510 configurations. In this effort, NCCoE implanted the VDI configuration to support Build 2 and 511 Build 4. The configuration supports the OT environment's jump server configuration (allowing 512 RDP and SSH access to systems within the PCS and CRS environment) and remote engineering 513 workstation (configuring the VDI with the tools needed to support the ICS environment). The 514 configuration for each build is detailed in the following sections.

515	1.	Build 2: P	CS Configuration
516		i.	For the PCS setup, the Dispel VDI was used in a jump server configuration. No
517			additional software was installed. The firewall and Wicket ESI configuration
518			allowed RDP and SSH connections to the PCS ICS environment. Additionally, RDP,
519			SSH, and HTTP/HTTPS access to the Cybersecurity LAN environment was
520			authorized for the remote sessions as defined in the previously described firewall
521			settings, Table 2-2.
522	2.	Build 4: Cl	RS Configuration
523		i.	For the CRS setup, the Dispel VDI was configured as a remote engineering
524			workstation. To support the Beckhoff PLC, the TwinCAT 3 XAE software was
525			installed on a VDI, and the network drive provided by the GreenTec-USA solution
526			and hosted in the DMZ environment that contained the PLC code was mapped to
527			the VDI. Additionally, RDP, SSH, and HTTP/HTTPS access to the Cybersecurity LAN
528			environment was authorized for the remote sessions as defined in the previously
529			described firewall settings, Table 2-2.
530		ii.	For the interaction with the Beckhoff PLC, the TwinCAT 3 XAE software (TC31-
531			FULL-Setup.3.1.4024.10.exe) was installed on the VDI.
532		iii.	The Dispel VPN connection does not allow split-tunneling so, once the VPN
533			connection is established from the VDI to the Wicket ESI, the VDI is disconnected
534			from the internet. Therefore, download and installation of software occurred
535			prior to connecting to the Wicket ESI.
536		iv.	Due to the NAT configuration of the RUGGEDCOM RX1510 router between the
537			Cybersecurity LAN and the CRS environment, port forwarding rules were
538			configured to allow external traffic to reach the Beckhoff CX9020 PLC.
539		٧.	The following rules (Table 2-3) were created in the RX1510 firewall to enable
540			destination network address translation (DNAT) from the firewall WAN interface
541			(10.100.0.20) to the CRS PLC (192.168.0.30)

542 Table 2-3 Firewall Rules

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.

- 5433. As described in 2.i above, the GreenTec WORMdisk (\\10.100.1.7\crs) was mapped to the544VDI to access the PLC code. The configuration to map Windows is shown in Figure 2-2545below:
- 546 Figure 2-2 Mapping a Network Drive

			×
÷	😪 Map Ne	etwork Drive	
	What ne	twork folder would you like to map?	
	Specify the	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	

5474. After clicking **Finish**, the user is prompted for credentials, as shown in Figure 2-3. An account548authorized to access the network drive must be used. This is separate from the Dispel VDI549credentials.

550 Figure 2-3 Authentication to File Server

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

551 **2.2 Dragos**

- 552 The Dragos platform implementation in Build 3 consists of two physical servers hosting the Dragos
- 553 SiteStore and the Dragos sensor to meet the behavioral anomaly detection (BAD), hardware
- 554 modification, firmware modification, and software modification capabilities. Dragos utilizes a
- 555 combination of a passive sensor and integration with the OSIsoft PI Server to monitor critical networks
- 556 for anomalies. OSIsoft PI performs active querying to retrieve information about endpoints in the CRS
- 557 environment, which is shared with Dragos.
- 558 2.2.1 Host and Network Configuration
- 559 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.

561 Table 2-4 Dragos Deployment

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

562 2.2.2 Installation

- 563 The Dragos platform, which includes the SiteStore server and the Dragos sensor, was delivered as pre-
- 564 configured 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 toguide the installation. Customers can obtain these guides from Dragos.

569 2.2.3 Configuration

- 570 In addition to the standard configuration preset by Dragos, the Dragos Platform was configured to work 571 with OSIsoft PI for alerting on certain conditions.
- 572 Configure the Dragos SiteStore Server:
- 573 1. Configure the data connection between Dragos SiteStore and OSIsoft PI Server:
- 574a. Once installation is successful, open a browser to access the configuration screen by us-575ing the URL https://<SiteStore ip address>/osisoft/#/apps. (Figure 2-4)
- 576 Figure 2-4 Dragos OSIsoft PI Server Integration

To OSISoft Integration	x +	
← → C ▲ Nota	secure 10.100.0.63/ossoft/#/apps	* 0 :
DRAGOS	to Configure ProtectualPri II Mag Elements	11 🕑 admin Đ
SysLog		
ill Geolf	Configure PIWebAPI Configure connection to OSISist Pivive-API.	Elements to Dragos Assets
CSISON.		LAUNCH
	Animent and a second se	Partition.
https://10.100.0.63/ositoft/#/Ma	adlament	

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.

582 iii. Click **Save**.

583 Figure 2-5 Dragos PI Web API Configuration

← → C ▲ Not secure 10.100.0.63/or			- •
	LAN Kang Gurrantes	D 🕒 ann	5
Carl Synt.og			
Configure PiW	API		
Avw0UEIRETaMB4XDTrvMTt A 1UEAww5UEIRETaMB5MA0 wpthlpromm42EF8ETaMB5MA0 wpthlpromm42EF9CB1058 ig/23ww6053/V9IAD0XT42X7 gwA12y58iK045050050705aM 951ETVqCBBJLURHV04Jb099 j4V/802B5J6460+HVgCJ22xxx	DivDOV.KID2IIvi-CHADELEDANETEPRAADDA1UE CARTY-VORKISTIMAMEVIV-DEQEMANEVIVE(TEPRAADD DIBIIODERAMULAANENDEDIBIIODECHINA.DANE VIIII Igibi2ADEGUIAANENDECIDIBIIODECHINA. BIRCH ALT Antometina BIRCH IGGLIDUI(T.O.) MORTI IdiDAARENgUIAAAAENERIKA LIDII JIIODECHINA.DEGUIAAAAENERIKA LIDII JIIODECHINA.DEGUIAAAAENERIKA LIDII JIIODECHINA.DEGUIAAAAENERIKA LIDII JIIODECHINA.DEGUIAAAAENERIKA LIDII JIIODECHINA.DEGUIAAAAENERIKA		
Danara			
Passand			
RESET SAVE			_
_			
	i. Select the OSIsoft Database CRS-backu	up on the left side to access the	
	from the Historian Database.		dev
	from the Historian Database.ii. Select the Default NetworkID RFC 191 assets.		
	ii. Select the Default NetworkID RFC 191 assets.iii. For each asset in the OSIsoft Database	18 and use the Filer options to fi e, select the corresponding asset	nd s
	 ii. Select the Default NetworkID RFC 191 assets. iii. For each asset in the OSIsoft Database gos asset repository and click Pair Sele 	18 and use the Filer options to fi e, select the corresponding asset ected .	nd s
	ii. Select the Default NetworkID RFC 191 assets.iii. For each asset in the OSIsoft Database	18 and use the Filer options to fi e, select the corresponding asset ected .	nd s
	 ii. Select the Default NetworkID RFC 191 assets. iii. For each asset in the OSIsoft Database gos asset repository and click Pair Sele iv. Repeat this process for each asset unt 	18 and use the Filer options to fi e, select the corresponding asset ected .	nd s
	 ii. Select the Default NetworkID RFC 191 assets. iii. For each asset in the OSIsoft Database gos asset repository and click Pair Seletiv. Repeat this process for each asset unt Data table (Figure 2-7). 	18 and use the Filer options to fi e, select the corresponding asset ected . til all paired assets are listed in t	nd s
	 ii. Select the Default NetworkID RFC 191 assets. iii. For each asset in the OSIsoft Database gos asset repository and click Pair Selectiv. Repeat this process for each asset unt Data table (Figure 2-7). 1) PLC paired to 192.168.0.30 	18 and use the Filer options to file, select the corresponding assetence, select the corresponding assetence. ected. til all paired assets are listed in the select of	nd s
	 ii. Select the Default NetworkID RFC 191 assets. iii. For each asset in the OSIsoft Database gos asset repository and click Pair Selectiv. Repeat this process for each asset unt Data table (Figure 2-7). 1) PLC paired to 192.168.0.30 2) Station 1 paired to 192.168.1.10 	 18 and use the Filer options to file, select the corresponding asset ected. all paired assets are listed in the second second	nd s

601 Figure 2-6 OSIsoft PI Server to Dragos Asset and Data Pairing

C A Not secure 10.100.0.63/osion1/#/MapElements	* 6
RAGOS Configure Private API	🖸 🕒 admin
COSISOFT Elements Part Elements P	PART ELLECTEDE

602

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

Paired Data									
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			
1	Asset 5 1176 1186 1180	Asset OSisoft Name 5 PLC 176 Station 2 180 Station 3	Asset OSisoft Name Type 5 PLC F 176 Station 2 F 180 Station 3 F	Asset OSisoft Name Type Vendor PLC Beckbeff Automation GmbH Beckbeff Automation GmbH	Asset OSisoftName Typ Vendor MAC % %C.C.C.C.C.C.C.C.C.C.C.C.C.C.C.C.C.C.C.	Assat OSisof Name Tpt Vendor MAC IP 6 P.C. Beckhoff Automation GmbH 12168.03 12168.03 170 Bation 2 C Bobscoff Automation GmbH Bobscoff Automation GmbH 2019.2168.1103_FEB0.62D5.0CFFFEF6.68B1 180 Bation 3 C C Bobscoff Automation GmbH 2019.2168.1103_FEB0.62D5.0CFFFEF6.68B1 180 Bation 3 C C Bobscoff Automation GmbH 2019.2168.1103_FEB0.62D5.0CFFFEF6.A343			

604

608

- a. Configure Zones
- 606NOTE: Zones are ordered in a similar manner to firewall rules. In other words, higher rules607have priority over lower rules.
 - i. Click **Assets** and select the **Zones** tab (Figure 2-8).

609 Figure 2-8 Dragos Zone Administration Page

Asset Explorer	♦ 11 \$\phi\$	8
ASSETS	ZONES	
Q. Search Zones	DETAILED VIEW BUM VIEW + NEW ZONE C REFRESH	NES
E DMZ	Details Asset Criteria Assets: 14 ALL: Baselined Assets: 0 IPV4 ODR Metches CIDR 10.100.10/04 Baseline Events: 0 IPV4 ODR Metches CIDR 10.100.10/04 Protocols: 2: External Communications: foise	
	EDIT	DELETE
■ Cybersecurity LAN	Details Asset: Criteria Asset: 78 ALL: Baseline Assets: 0 IPVA CIDR Matches CIDR 10.100.00/24 Baseline Communications: raise External Communications: raise	
	✓ EDIT	DELETE
CRS - Level 1 CRS Data Collection and Monitoring	Details Asset: 25 Asset: 25 ALL: Baseline Asset: 0 IPVA CIDR Matches CIDR 192 168.0.0/24 Baseline Events: 0 IPVA CIDR Matches CIDR 192 168.0.0/24 Protocols: 23 External Communications: true	
	✓ EDIT	DELETE
CRS - Level 0 CRS Robots and Controllers	Details Asset Criteria Assets: 15 ALL: Baselined Assets: 0 IPV4 CIDR Matches CIDR 192:168:1.0/24 Baseline Events: 0 IPV4 CIDR Matches CIDR 192:168:1.0/24	

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
i. Name: Testbed LAN:
1) Description: Lab Testbed LAN
2) Auto Zone Criteria (Match ALL):
a) IPV4 CIDR Matches CIDR 10.100.0.0/24
i. Name: CRS:
1) Description: Parent CRS
2) No Criteria
v. 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

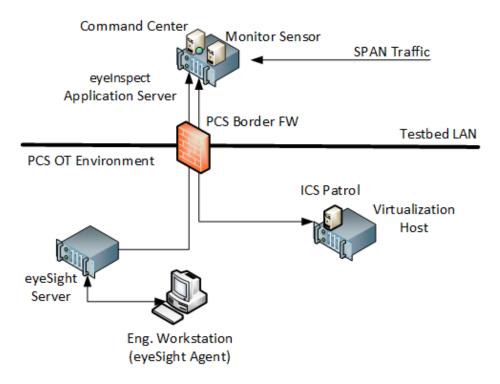
627	v. Name: CRS – Level 1:								
628	1) Description: Lab DMZ								
629	2) Parent Zone: CRS								
630	3) Auto Zone Criteria (Match ALL):								
631	a) IPV4 CIDR Matches CIDR 192.168.0.0/24								
632	Figure 2-9 Dragos Create Zone Pop-up								
	Create Zone Name* DMZ Description Lab DMZ Parent Zone Search for an existing Parent Zone, or create a new Parent Zone								
	Auto Zoning Criteria								
	Results must match ALL of the following:								

					Value		
	IPV4 CIDR	Ť	Matches CIDR.	*	10.100.1.0/24	Ē	
			+ ADD ATTR				
			T ADD AT TH	GBOTE			
Results n	nust match ANY of	the follo	wina:				
		the rone	, winig.				
			_	RIBUTE			
			_				

2.3 Forescout Platform 633

The Forescout products included in the practice guide are eyeInspect (formally SilentDefense), eyeSight, 634 635 ICS Patrol, and Forescout Console. These products are utilized in Build 2 to meet the BAD, hardware 636 modification, firmware modification, and software modification capabilities. The Forescout

- 637 implementation utilizes different components and modules installed on different devices to monitor
- 638 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.
- 640 Figure 2-10 Forescout High-Level Components and Dataflows



641 eyeInspect (formally SilentDefense)

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

647 eyeSight

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

651 ICS Patrol

- 652 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
- 654 queries and reporting results are managed through eyelnspect.
- 655 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
- 658 eyeSight server.
- 659 2.3.1 Host and Network Configuration
- 660 Forescout was installed and configured to support the PCS Environment as part of Build 2. The overall
- build architecture is provided in Figure B-2 with the Forescout specific components in Table 2-5 and the
- 662 eyeSight agents in Table 2-6.
- 663 Table 2-5 Forescout Deployment

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

664 For the lab environment, network connectivity between the components in the Testbed LAN and the

665 components in the PCS environment required the following persistent route configured on Testbed LAN 666 systems:

667 route -p ADD 172.16.0.0 MASK 255.255.252.0 10.100.0.40

- 668 The following systems were configured to utilize the eyeSight Agents.
- 669 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.

671 2.3.2 Installation

- The Forescout products included in the practice guide are eyeInspect, Forescout Console, ICS Patrol, and
- 673 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).
- 675 Table 2-7 Firewall Rules for Forescout

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

676 *2.3.2.1 eyeInspect*

- 677 eyeInspect is an appliance hosted on a Dell Embedded Box PC 5000. The unit was placed within a
- 678 standard datacenter rack unit with the eyeSight appliance and connected to the network as described in
- 679 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
- 681 after successfully logging onto the appliance.

682 2.3.2.2 Forescout Console

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

687 *2.3.2.3 eyeSight*

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

690 2.3.2.4 eyeSight SecureConnector Agent

- In a browser on a system with web connectivity to the eyeSight server, navigate to
 <u>https://172.16.2.61/sc.jsp</u> to access the SecureConnector download page (Figure 2-11) and
 follow these steps:
- 1010w these steps.
- 694a.Select Create SecureConnector for: Windows.
- b. Enable Show the SecureConnector icon on the endpoint systray.
- 696 c. Select Install Permanent As Service.
- d. Click Submit.

- 698 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.
- 702 Figure 2-11 Forescout SecureConnector Distribution Tool

Forescout SecureConnector Distribution Tool	
Use this page to download SecureConnector installers. Use these installers to distribure SecureConnector to endp	sists without direct and user interaction with the Encoded slatform
Use this page to download secure connector instanters, use these instanters to distribute secure connector to enop Use the options below to define Secure Connector deployment options.	sints without direct end user interaction with the rolescool platform.
Create SecureConnector for: Bay Windows	
O ≝ macOS / OS X ○ ∆ Linux	
Show the SecureConnector icon on the endpoint systray.	
Install Permanent As Service	
When SecureConnector runs on endpoints, it creates an encrypted and authenticated tunnel from the endpoint to i this host, the host will automatically reopen the tunnel to the managing Appliance. The tunnel created is used to re SecureConnector connects to the Appliance using a TCP connection on:	
Port 10003 for Windows SecureConnector Port 10005 for macOS / OS X SecureConnector Port 10006 for Linux SecureConnector.	
Note: the Windows SecureConnector installation file name should not be changed.	
	Submit

703 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-wKgAKScT4INyBj02vJ0UiZfHEQPNCuDINsUzyFEOorVydcsBoOoEAAEexe
Note: If your environment uses overlapping IP addresses, refer to the Forescout Working with Overlapping IP Addresses How to Guide.
Download

704 2.3.2.5 ICS Patrol

712

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

- 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
- 709 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 eyeInspect appliance.

713		b. Copy the components to the ICS Patrol VM:
714 715 716		<pre>\$ scp os_provisioning_4.1.1_install.run \ main_configuration_4.1.1_install.run \ silentdefense@172.16.2.62:/home/silentdefense</pre>
717		c. SSH to the ICS Patrol VM and execute the installation components:
718 719 720 721		<pre>\$ chmod a+x *.run \$ sudo ./os provisioning 4.1.1 install.run \$ sudo ./main_configuration_4.1.1_install.run \$ sudo reboot</pre>
722	2.3.3	Configuration

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

724 *2.3.3.1 eyeInspect*

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

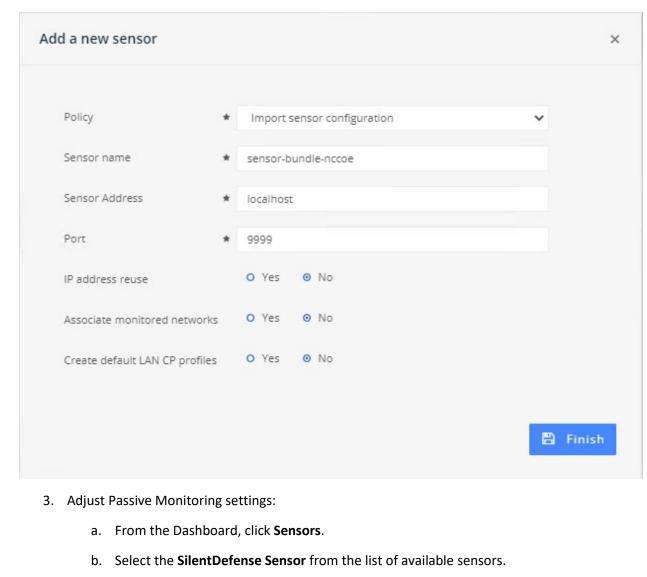
<) FORESCOUT	🚯 Dast	nboard 🚠	Network	Events 🄊	Sensors 📽 Settings	
Sensors overview	Reload	<u>Add</u> ~	Pause 🗸	IP reuse doma	ins Monitored networks	Scans 🛩
		SilentDefe	nse sensor			
SilentDefense sensors		ICS Patrol :	sensor			
0 sensors selected		PCAP repla	y sensor			

732

733

734





- 735 c. Click the **Industrial Threat Library Overview** option in the upper right corner.
- 736 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.
- 741 ii. Verify Maximum occurrences in window is set to 20.
- 742 iii. Verify **Time Window (in seconds)** is set to **60**.

743 Figure 2-15 eyeInspect ICMP Protocol/Port Scan Attempt Settings

Enable check				
Maximum occurrences in window	*	20	0	
Time window (in seconds)	*	60	0	



746 747

748

749

750

- g. Select **Portscan Detection** under Built-in Modules (Figure 2-16).
- 745 Figure 2-16 eyeInspect Sensor Configuration Options

Sensor attributes		Network whitelists Network intelligence framework	
Sensor name	sensor-bundle-nccoe	Communication patterns (LAN CP) Industrial threat library (ITL)	
State	Connected		
Address	localhost	O profiles selected O library selected	
Port	9999	ID A Name State Name	State
IP reuse domains		8 TCP communications O Detecting Industrial threat library checks	Active
Monitored networks		9 UDP communications Q Detecting	
		Custom checks (SD Scripts)	
		2 profiles	
Built-in modules		O scripts selected	
		Protocol fields (DPBI) ID • Name	State
0 modules selected		O profiles selected O cve_2019_0708_monitor	 Active
Name	State	□ 11 CVE_2020_0796_monitor v	1.0 🕑 Active
Portscan detection	Q Detecting	ID Name State	.0 📀 Active
Man-in-the-middle dete	ction Q Detecting	No profiles available. 13 ETHIP/CSP - PCCC Monitor	v0.6 🕑 Active
Malformed packet deter	tion Q Detecting	0 profiles 14 Host and Link Add-Ons v1	28 📀 Active
Frequent event aggrega	tion 📀 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	
			•
		14 scripts	
h.	Click the Settings	tab and set the following parameters (Figure 2-17):	
	i. Sensitivity	level: User defined	
	ii Numher of	Heate with foiled connections to make a distributed as	. 10
	ii. Number of	Hosts with failed connections to make a distributed sca	n: 10

iii. Detect SYN scans: Checked

- 751 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
- 755 Figure 2-17 eyeInspect Portscan Detection Settings

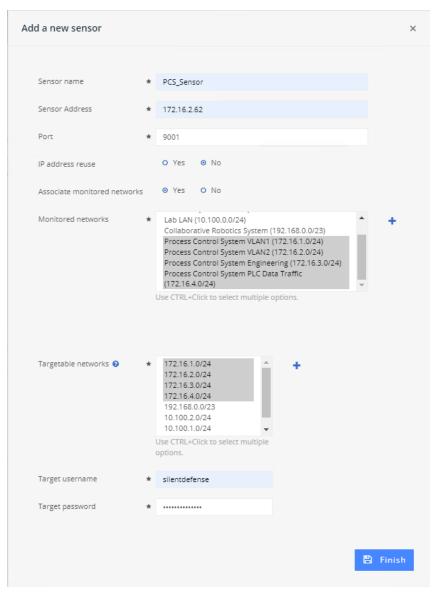
<) Command Center - Portscan dete X <	Forescout Web Client	t × +
← → C ▲ Not secure 10.100.0	.65/crypt.f2S2R1Zg	x-m8Wp0UiwMfJQ/f2Sd
<) FORESCOUT	🚯 Dashboard	🚠 Network 🔳
Portscan detection mod	Back Finish	Reset Reload
Detection sensitivity		
Sensitivity level	User defined	~
Distributed scans		
Number 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	

757 4. Register the ICS Patrol Sensor:

758

- a. From the Sensor admin page, click the menu option Add > ICS Patrol sensor.
- 759
- b. Specify the sensor parameters in the dialog box (Figure 2-18).

760 Figure 2-18 Add ICS Patrol Sensor Dialog



761

c. Define a scan policy to periodically check the PCS PLC to monitor for changes.

762 763 i. Click the PCS Sensor created in the previous step to open the sensor admin page (Figure 2-19).

764 Figure 2-19 ICS Patrol Sensor Admin Page

	FORESCOUT	🚯 Dashboard	📥 Network	Even	ts 🌒	Sensors	Sectings	
Patro	ol Sensor "PCS_Sens	Back Edit	Diagnostics	Scans 🗸				
Se	ensor Attributes							
N	ame	PCS_Sensor						
St	ate	Connected						
Ad	ddress	172.16.2.62						
Po	ort	9001						
Ta	arget networks	172.16.2.0/24, 172.16.1 172.16.3.0/24, 172.16.4						
IP	reuse domains							
м	onitored Networks	Process Control System Engineering, Process Co System PLC Data Traffic Control System VLAN2, Control System VLAN1	ontrol , Process					
	ii. 	Click the men	-	Scans > 9	Scan	Policie	s.	
	iii.	In the dialog	option (Fiរួ	gure 2-2	0) en	ter the	scanning	g pa
	111.	In the dialog of 1) Name:		gure 2-2	0) en	ter the	scanning	g þa
		_	PCS PLC	-	0) en	ter the	scanning	g þa
		1) Name:	PCS PLC ype : Ether	Net/IP		ter the	scanning	g þa
		1) Name: 2) Scan Ty	PCS PLC ype : Ether Type : Cus	Net/IP tom tar		ter the	scanning	g þa
		1) Name: 2) Scan Ty 3) Target	PCS PLC ype: Ether Type: Cus ress reuse	Net/IP tom tar; : No	get		scanning	g pa
		1) Name: 2) Scan Ty 3) Target 4) IP addr	PCS PLC ype: Ether Type: Cus ress reuse rk Addres	Net/IP tom tar; : No	get		scanning	g þá
		1) Name: 2) Scan Ty 3) Target 4) IP addr 5) Netwo	PCS PLC ype: Ether Type: Cus ress reuse rk Addres ile: Yes	Net/IP tom tar; : No s : 172.1	get		scanning	g þa
		1) Name: 2) Scan Ty 3) Target 4) IP addr 5) Netwo 6) Schedu	PCS PLC ype: Ether Type: Cus ress reuse rk Addres ile: Yes ncy: Repe	Net/IP tom tar; : No s: 172.1	get 6.2.1	02		

776	Figure	2-20	Add	an	ICS	Patrol	Scan	Policy
-----	--------	------	-----	----	-----	--------	------	--------

Add scan policy						×
Name Description	* PC	5 PLC				
Scan type	0 0 0 0	Active IPs OS/Ports OS/Ports OUT Ports OT Ports Siemens S7 EtherNet/IP O				
Target type		ustom target Yes o No	~			
Network addresses	* 173	2.16.2.102			Θ	
Schedule	٥	Yes O No				
Frequency	* Re	peat	~			
Start date	* Jun	3, 2021 12:00:00				
Interval	* 1			Hours 🗸		
					🖹 Finis	sh

777 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.

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

- 788 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.
- 791 iii. Select "443" from the TCP Port drop-down menu.
- 792 Figure 2-21 eyeSight Add Dialog General Information

4	Add Command Center - Step 1				
Add Com	nmand Center				
🖆 General	General	parameters between the Command Center and			
	Set up general communication ForeScout.	varameters between the Command Center and			
	IP Address/Name	10.100.0.65			
	TCP port	443 🗘			
	Connecting CounterACT device	172.16.2.61 ∨			
	<u>H</u> elp Pre	evio <u>u</u> s Next <u>F</u> inish Cancel			
	b. Click Next.				

- 793 794
- c. Enter the command center credentials (Figure 2-22).
- 795 d. Click Finish.

796 Figure 2-22 eyeSight Add – Command Center Credentials

Add Command Center - Step 2 of 2					
Add Command Center		enter Credentials			
🖆 Command Center Credentials					
	Credentials				
	User name	admin			
	Password	****			
	Confirm password	****			
He	lp Previo <u>u</u> s	Next Finish C	ancel		

- 5. 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 is displayed.
- 799 7. Click **Apply** to save the changes.
- 800 8. Click **Close** to close the message.

801 Figure 2-23 eyeSight OT Settings

0		Options 172.16.2	.61	_ D X
Options				
Operational	Operational Techn	ology		
🏭 Operational Technology	The Operational Technolog	y Module provides comprehensive OT asset inventory using	g passive device fingerprinting and assessment of OT device vulnerabili	ties.
	- Sensors monitor endpoin - Command Center server - The Operational Technol Typically OT networks cont		it Console. resses in the Internal Network, go to Options>Advanced>Overlapping IF omain Mapping	°s.
		er instances that report Operational Technology information		
	Search	Q		
	Address 🔺	TCP Port	Connecting CounterACT Device	<u>A</u> dd
	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

802 Figure 2-24 eyeSight Test Connection Successful Message

Operational Technology Connectivity Test	3
Communication with Command Center succeeded.	
Connectivity Test succeeded	
CONTRICTION (1997) THE SUBACTORY	Close

803 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.

807 ForceField

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

811 WORMdisk

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

816 2.4.1 Host and Network Configuration

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

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

821 2.4.2 Installation

- 822 The ForceField and WORMdisk HDDs were hosted on a hardware appliance provided by GreenTec-USA.
- 823 The unit was placed within a standard datacenter rack unit and connected to the network as shown in
- 824 <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.
- 826 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 pre-
- installed, so installation was performed via the Ubuntu Advanced Packaging Tool and the Ubuntupackage 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 executedby a user with superuser privileges or as the root user.
- 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:

838\$ sudo apt update839\$ sudo apt -y install samba840\$ sudo ufw allow samba

- 841 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.

844 *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/

851 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.

- 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:
- 858 > gt format.exe 1 /parts:120
- 859 2. In the Ubuntu OS, create the mountpoint for the WORMdisk HDD partition using the following860 command:
- 861 \$ sudo mkdir /mnt/golden
- 862 3. Add a persistent mount to the /etc/fstab file:

```
863 $ sudo echo "/dev/sdb2 /mnt/golden fuseblk
864 rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other,blksize
865 =4096 0 0" >> /etc/fstab
```

- 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:
- 869 \$ sudo /greentec/Ubuntu/wvenf /dev/sdb2

870 871 872	update	t is time to create a new "golden" partition, the partition names in the /etc/fstab file must be d to point to the correct partition. The following instructions provide an example process to the files and increment the golden partition from /dev/sdb2 to /dev/sdb3.
873 874	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:
875 876 877		<pre>\$ sudo mkdir /mnt/tmp \$ sudo mount /dev/sdb3 /mnt/tmp \$ sudo cp -R /mnt/golden /mnt/tmp</pre>
878	2.	Update the files and folders in the temporary directory, $/{\tt mnt/tmp}$, as desired.
879	3.	Unmount the temporary directory and lock the partition:
880 881		\$ sudo umount /mnt/tmp \$ sudo /greentec/Ubuntu/wvenf /dev/sdb3
882	4.	Stop the Samba service:
883		<pre>\$ sudo systemctl stop smb.service</pre>
884	5.	Unmount the golden partition:
885		\$ sudo umount /mnt/golden
886	6.	Modify the /etc/fstab file with the new partition name and save the file:
887 888 889		<pre>/dev/sdb3 /mnt/golden fuseblk rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other,blksize =4096 0 0"</pre>
890	7.	Re-mount all partitions, start the Samba service, and remove the temporary directory:
891 892 893		<pre>\$ sudo mount -a \$ sudo systemctl stop smb.service \$ sudo rmdir -r /mnt/tmp</pre>
894	2.4.3.	3 Samba
895 896	1.	Add local user accounts to the appliance for accessing the network file shares and create a password:
897 898		\$ sudo adduser nccoeuser \$ sudo smbpasswd -a nccoeuser
899 900	2.	Open the file /etc/samba/smb.conf and add the following content to the end of the file to create the individual shares:
		<pre># GreenTec-USA ForceField Share strict sync=no</pre>

```
# 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
```

- 901 3. Restart Samba:
- 902 \$ sudo systemctl restart smbd.service

903 2.4.3.4 OSIsoft PI Server and Database Backups

904 Create the scheduled backup task to backup PI Data Archive files. The script automatically inserts the905 current datetime stamp into the filename of each file copied to the ForceField drive. Follow these steps:

- 906
 91. On the server containing the PI Data Archive, open a command prompt with Administrator
 907 privileges.
- 908 2. Change to the PI\adm directory:
- 909 > cd /d "%piserver%adm"
- 910 3. Create the backup directory, and start the Windows scheduled task to perform the backup:
- 911 > pibackup h:\PIBackup -install
- 912 Create a scheduled task to copy the backup files to the ForceField HDD. Follow these steps:
- Open the Task Scheduler and create a new scheduled task to rename, timestamp, and copy the
 backup files to the ForceField HDD:
- 915 Trigger: At 3:30 AM every day
- 916 Action: Start a Program
- 917 Program/script:
- 918 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- 919 Add arguments (optional): -Command { Get-ChildItem -Path

```
920 "h:\PIBackup\arc\" | foreach { copy-item -path $($_.FullName) -
921 destination "\\10.100.1.7\ForceField\$(Get-Date -f yyyy-MM-
922 dd_HHMMss)_$($_.name)" } }
```

923 2.5 Microsoft Azure Defender for IoT

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

929 2.5.1 Host and Network Configuration

- 930 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.
- 933 Table 2-9 Microsoft Azure Defender IoT Deployment

Name	System	OS	CPU	Memory	Storage	Network
Azure Defender for loT	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

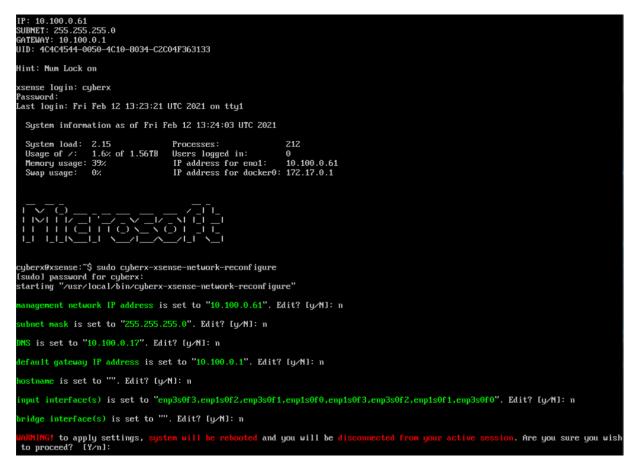
934 2.5.2 Installation

- 935 The Microsoft Azure Defender for IoT (Version 10.0.3) appliance was preinstalled with the operating
- 936 system and application. The appliance is mounted in a rack with power and network interfaces
- 937 connected to the Testbed LAN on the Eth0 port along with the SPAN connection on the expansion
- 938 network interface board.

939 2.5.3 Configuration

- 940 To configure the Microsoft Azure Defender for IoT platform, follow these steps:
- 941 1. Set the Network Configuration:
- 942a.Using either SSH, iDRAC, or the KVM Console connections on the appliance, establish943shell access to the appliance.
- 944 b. From the console, enter the following command:
- 945 \$sudo cyberx-xsense-network-reconfigure
- 946c. The system will walk through a series of network options (Figure 2-25) that are set as947follows:
- 948 i. IP Address: "10.100.0.61"
- 949 ii. **Subnet Mask:** "255.255.255.0"
- 950 iii. **DNS**: "10.100.0.17"

- 951 iv. **Default Gateway**: "10.100.0.1"
- 952 v. Hostname: Not set
- 953vi.Input Interface(s): "enp3s0f3, enp1s0f2, enp3s0f1, enp1s0f0, enp1s0f3, enp3s0f2,954enp1s0f1, enp3s0f0"
- 955 vii. Bridge Interface(s): Not Set
- 956 Figure 2-25 Azure Defender for IoT SSH Session for Network Configuration



957	2.	Create AMS Protocol report as a data mining tool:
958		a. Login to the application web interface and click Data Mining in the left menu navigation.
959 960		 b. Click the + sign and click New Report. In the Create New Report panel set the following settings (Figure 2-26):
961		i. Under Categories select AMS to automatically select the sub-elements, including:
962		1) AMS Firmware Information
963		2) AMS Index Group
964		3) AMS Index Group Offset

- 965 4) AMS Protocol Command
- 966 ii. Enter "AMS Data Analysis" as the name for the report.
- 967 iii. Click Save.
- 968 Figure 2-26 Azure Defender for IoT Create New Data Mining Report for AMS Protocol Information

Microsoft		Data Mining			
NAVIGATION		+ 💌 Main V	Create new Report		
Dashboard		_	Categories (All):	Name:	
Devices Map (82)		Suggested	Protocol Versions Unresolved Connections	AMS Data Analysis	
Device Inventory			User Access Per Protocol Windows Services	Description:	
Alerts (36)	٠	=	60870-5-104	Description	
Reports			EC-60870-5-104 ASDU Types	□ Save to Reports Page	
		Programming Com	ABB TOTALFLOW		on
	Ê	Reports	ABB Totalflow File Operations ABB Totalflow Firmware Versions ABB Totalflow Register Operations	Order By: Category Activity	
Data Mining	2		AMS	Filters: (Add)	Only results within the last Minutes 🗸
	₽		 AMS Firmware Information AMS Index Group AMS Index Group Offset AMS Protocol Command 	Device Group	
Attack Vectors	Ø	AMS	BACNET	IP Address	Ex: 10.2.1.0, 10.2.*.*
			BACNet Object Access BACNet Routes	Port	Ex: 80, HTTP, HTT*
			CAPWAP	MAC Address	
	*		Tunneling Traffic CDP		Ex: 00:10:*:ff:*:*
	\odot			•	
	\$				
Import Settings	±				Close Save

- 969 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.
- 976c. Create Custom Alert to Detect Change in PLC Firmware Major Build Number (Figure9772-27):
 - i. Enter "PLC Firmware Major Build Mismatch" as the title for the custom alert.
- 979 ii. Enter "PLC {AMS_server_ip} Firmware Major Version Build Mismatch Detected"
 980 as the message to display with the alert.
- 981 iii. Set the following conditions:

982	1) AMS_server_ip == 3232235550 (Note: this is the PLC IP address
983	192.168.0.30 in Integer format).

- 984 2) AND AMS_major ~= 3
- 985 Figure 2-27 Azure Defender for IoT Custom Alert for Firmware Major Version Number Change

AMS - Custom Alert Rules

PLC (AMS.server_ip) Firmware Major Version Build Mismatch Detected Use () to add variables to the message inditions	le	
Variable Operator Value \textcircled{AND} Variable Operator Value \textcircled{O}	PLC Firmware Major Build Mismatch	
Use () to add variables to the message Conditions Variable Operator Value Operator Operator Value Operator Value Operator Operator Value Operator O		
Variable Operator Value $$ AND Variable Operator Value $$	PLC {AMS.server_ip} Firmware Major Version Build Mismatch Detected	
	Variable Operator Value	/alue

986 987	d.	Create 2-28):	e the custom alert to detect change in PLC firmware minor build number (Figure
988 989		i.	Enter "PLC Firmware Minor Build Mismatch" as the title for the custom alert. PLC Firmware Minor Build Mismatch
990 991		ii.	Enter "PLC {AMS_server_ip} Firmware Minor Version Build Mismatch Detected" as the message to display with the alert.
992		iii.	Set the following conditions:
993 994			 AMS_server_ip == 3232235550 (Note: this is the PLC IP address 192.168.0.30 in Integer format).
995			2) AND AMS_minor ~= 1

996 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.
	Title
	PLC Firmware Minor Build Mismatch
	Message
	PLC (AMS.server_ip) Firmware Minor Build Mismatch Detected
	Use {} to add variables to the message
	Conditions
	Variable Operator Value Image: Walk of the state of t
997	CLEAR SAVE
998 999	e. Create the custom alert to detect change in the PLC Firmware Build Version (Figure 2-29):
1000	i. Enter "PLC Firmware Build Version Mismatch" as the Title for the custom alert.
1001 1002	 Enter "PLC {AMS_server_ip} Build Version Mismatch Detected" as the message to display with the alert:
1003	iii. Set the following conditions:
1004 1005	 AMS_server_ip == 3232235550 (Note: this is the PLC IP address 192.168.0.30 in Integer format).
1006	2) AND AMS_version_build ~= 4022
1007	Figure 2-29 Azure Defender for IoT Custom Alert for Firmware Build Version Number Change

AMS - Custom Alert Rules

PLC Firmware Build Ver	sion Mismatch							
ssage								
PLC {AMS.server_ip} Bu	uild Version Mismatch Detected							
Jse {} to add variables to	the message							
nditions								
/ariable	Operator Value			Variable	Operator	Value		
	oporator vatao	÷	AND				\oplus	
	× = × 323			AMS version build	~=	✓ 4022	~	
AMS.server_ip	▼ == ▼ 323	2235! Θ		AMS.version_build	~=	✓ 4022	Θ	

1009 2.6 OSIsoft PI Data Archive

1010 The OSIsoft product included in this practice guide is Process Information (PI), which is used to collect,

1011 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 whenactivity deviates from a baseline.

1014 OSIsoft PI is a suite of software applications for capturing, analyzing, and storing real-time data for

1015 industrial processes. Although the PI System is typically utilized as a process historian, the PI System is

1016 also utilized to collect, store, and manage data in real time. Interface nodes retrieve data from disparate

1017 sources to the PI Server, where the PI Data Archive resides. Data is stored in the data archive and is

1018 accessible in the assets defined in the Asset Framework (AF). Data is accessed either directly from the

1019 data archive or from the AF Server by using tools in the PI visualization suite.

1020 2.6.1 Host and Network Configuration

1021 PI was installed on virtual machines hosted on hypervisors located in the DMZ and CRS networks. The

1022 virtual machine details and resources are provided in Table 2-10, Table 2-11 and, Table 2-12. The overall

1023 build architectures utilizing PI are described in Section 4.5 in Volume B.

1024 Table 2-10 OSIsoft PI Domain Hosts Deployment

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

1025

1026 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

1027

1028 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

1030 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,*
- 1033 <u>https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf</u>. The installation for this
- 1034 project involved upgrading the existing CRS Local Historian and DMZ Historian VMs to Microsoft
- 1035 Windows Server 2016, and subsequently upgrading all the PI software components. Step-by-step
- 1036 instructions for each PI component installation are not included for brevity. Detailed instructions
- 1037 provided by the vendor can be found on the OSIsoft Live Library: <u>https://livelibrary.osisoft.com/</u>.

1038 DMZ Historian Server

- 1039 The following software is installed on the DMZ Historian server:
- 1040 Microsoft SQL Server 2019 Express 15.0.2080.9
- 1041 PI Server 2018 (Data Archive Server, Asset Framework Server)
- 1042 PI Server 2018 SP3 Patch 1
- 1043 PI Interface Configuration Utility version 1.5.1.10
- 1044 PI to PI Interface version 3.10.1.10
- 1045 PI Interface for Ramp Soak Simulator Data 3.5.1.12
- 1046 PI Interface for Random Simulator Data 3.5.1.10
- 1047 PI Connector Relay version 2.6.0.0
- 1048 PI Data Collection Manager version 2.6.0.0
- 1049 PI Web API 2019 SP1 version 1.13.0.6518
- 1050 CRS Local Historian Server (Collaborative Robotics System)
- 1051 The following software is installed on the CRS Local Historian server:
- 1052 Microsoft SQL Server 2019 Express 15.0.2080.9
- 1053 PI Asset Framework Service 2017 R2 Update 1
- 1054 PI Data Archive 2017 R2A
- 1055 PI Server 2018 SP3 Patch 1
- 1056 PI Interface Configuration Utility version 1.5.1.10
- 1057 PI to PI Interface version 3.10.1.10
- 1058
 PI Interface for Ramp Soak Simulator Data 3.5.1.12
- 1059 PI Interface for Random Simulator Data version 3.5.1.10
- 1060 PI Interface for Performance Monitor version 2.2.0.38
- 1061 PI Ping Interface version 2.1.2.49
- 1062 PI Interface for Modbus ReadWrite version 4.3.1.24
- 1063 PI Interface for SNMP ReadOnly version 1.7.0.37

- 1064 PI TCP Response Interface version 1.3.0.47
- 1065 PI Processbook 2015 R3 Patch 1 version 3.7.1.249
- 1066 PI Vision 2019 Patch 1 version 3.4.1.10
- 1067 PI System Connector version 2.2.0.1
- 1068 PCS Local Historian (Process Control System Historian)
- 1069 Rockwell FactoryTalk Historian SE version 1.00

1070 2.6.3 Configuration

1071 The following sections describe how to configure select PI components to enable the capabilities1072 described in this guide. Configurations for the other PI components are not included for brevity.

1073 2.6.3.1 Pl to Pl 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.
- 10781. On the DMZ Historian server, launch the PI Interface Configuration Utility as shown in Figure10792-30 from the Start menu and sign in with the local administrator account.

	Inte	Pl Interface Configura erface Tools Help	tion Utility	0		-	o x
	Typ De:	face: select -	×.	<undetermined></undetermined>		- PI Data server Co	Rename onnection Status
	Ge Int Se Ur	neral efface rvice iilnt Failover Health Points Performance Counters Performance Points PI SDK Disconnected Startup Debug Rate efface Status	General Point Source: Interface ID: Scan Frequency	Scan Class #	PI Host Information Server/Collective SDK Member: API Hostname: User: Type:		* * *
1081	Rea	dy					
1082 1083 1084					erface Instance from PitoPI and select the		_new.
1085 1086	4.	In the "Select Hos menu and click O		collective" dialog b	ox, select PI-DMZ fro	m the drop-do	own
1087	5.	In the left navigat	ion panel select P	PltoPl. In the Sourc	e host textbox, enter	"172.16.2.4".	
1088 1089	6.	In the left navigat button. Click Yes i	•	Service. In the "Cre	eate / Remove" sectio	on click the Cr	eate
1090 1091	7.				t stop PItoPI ir ively. Save and close		

1080 Figure 2-30 Screenshot of the PI Interface Configuration Utility before the Interface is configured.

click the green play button \blacktriangleright to start the service.

8. At the bottom of the PI Interface Configuration Utility click the Apply button. On top menu bar

- Close the PI Interface Configuration Utility. The interface is now configured to pull tags from the
 Rockwell Historian.
- 1096 2.6.3.2 Pl System Connector (CRS)
- 1097 The PI System Connector is used to duplicate process data on the DMZ Historian from the CRS Local
- 1098 Historian server. The following steps describe how to configure the PI-to-PI Interface to collect data
- 1099 from the OSIsoft PI Server.
- 1100 Figure 2-31 Screenshot of the PI Data Collection Manager Displaying Green Checkmarks After the PI
- 1101 System Connector is Properly Configured

=		р	Data Collection Manager				0	1
Components		Routing						ľ
Filter Components	Filter Options	Data Sources	Connectors	Relays	Destination:	s (4	Э	
Data Sources							^	
CRS-DS		CRS-DS	PI System Co	PI-DMZ-Relay	/ 🛁 🤡 10.10	0.1.4		
Connectors								
CRS-Connector	PI System Connector							
Relays								
PI-DMZ-Relay								
Destinations								
✓ 10.100.1.4	PI Server							

- 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:
- 1106 b. Name: PI-DMZ-Relay
- **1107** c. Address: 10.100.1.4
- **1108 d.** Port: 5460
- 1109 2. User Name: .\piconnrelay_svc
- 1110 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:
- **1113** a. Name: 10.100.1.4

1114	b. PI Data Archive Address: 10.100.1.4
1115	c. AF Server : 10.100.1.4
1116	5. Click Save Settings to add the destination.
1117 1118	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.
1119	7. Click Set up Connector to create a new connector.
1120	8. Use the following information to request registration:
1121	a. Registration Server Address: https://PI-DMZ:5460
1122	b. Registration Server User Name: piconnrelay_svc
1123	c. Registration Server Password:
1124	d. Description: Registration to PI-DMZ
1125	9. Click Request Registration to send the request to the DMZ Historian server.
1126 1127	10. On the DMZ Historian server, open the PI Data Collection Manager from the Start menu and sign in with the local administrator account.
1128 1129	11. Click Untitled Connector 1 and click Approve This Registration and Configure to approve the PI System Connector registration.
1130	12. In the Untitled Connector 1 details panel, click Edit.
1131	13. Use the following information to create the CRS-Connector connector:
1132	a. Name: CRS-Connector
1133	b. Description: Registration to PI-DMZ
1134	14. Click Save Settings to create the CRS-Connector.
1135 1136	15. Click CRS-Connector in the Connectors column. On the Overview panel click CRS-Connector : No Data Sources option to create the data source.
1137	16. On the CRS-Connector Connector Details in the Overview panel, click + Add Data Source.
1138	17. In the Data Source Settings window, use the following settings:
1139	a. Name: CRS-DS
1140	b. Source AF Server: PI-Robotics
1141	c. Source AD Database: TestbedDatabase
1142	d. Select Collect All Data from this Entire Database.
1143	18. Click Save to save the data source.

- 1144
 19. Click 10.100.1.4 in the Destination column of the Routing panel and then click Data in the
 1145
 10.100.1.4 Destination Details panel to configure the destination database for the CRS 1146
 Connector.
- 1147 20. In the 10.100.1.4 Destination Details panel, change from Change Default Settings for new
 1148 connectors to "CRS-Connector" and then click Edit Destination Data Settings.
- 1149 21. In the **10.100.1.4 Destination Details** of the **Overview** panel, use the following settings:
- 1150 a. Change the connector to **CRS-Connector**.
- 1151 b. Database: CRS-backup
- 1152 c. Click on **Elements** and it will change **<select a path using the tree below>** to **\$Elements**\
- 1153 d. Use default settings in Root AF Elements and Point Names.
- e. Create root Element CRS-Connector checkbox: Checked
- 1155 f. Prefix Point CRS-Connector checkbox: Checked
- 1156 22. Click **Save Destination Data Settings** to save the configuration.
- 1157 23. Click the white space in the **Routing** panel.
- 1158 24. Click **CRS-Connector: No Relays** in the **Overview** panel.
- 1159 25. Select the **PI-DMZ-Relay** checkbox in the **Routing** panel.
- 1160 26. Click the white space in the **Routing** panel again, then **Click PI-DMZ-Relay: No Destination** to1161 add the routing between relays and destinations.
- 1162 27. Select the **10.100.1.4** checkbox to add the routing between the relay and the destination.
- 1163 28. Click Save Configuration.
- 1164 29. In the Save Routing and Data Configuration window, select Save and Start All Components to
 1165 continue.
- 116630. Each box should now contain a green checkmark (i.e., Data Sources, Connectors, Relays, and1167Destinations). The elements in the AF database "testbeddatabase" on CRS Local Historian server1168is now replicated to AF database "CRS-backup" on the DMZ Historian server.
- 1169 31. Finally, create a Windows firewall rule to open the inbound ports 5460, 5461, 5471, and 5472.

1170 *2.6.3.3 PI Asset Template Analysis Functions and Event Frames*

- 1171 Analysis functions and event frame templates were created to generate alerts in the PLC asset template
- 1172 when their respective anomalous events are detected. When an analysis function result is TRUE, an
- 1173 event frame is generated from the event frame template and ends when the analysis function result is
- 1174 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.

1176 1177	1.	On the CRS Local Historian server, open the PI System Explorer by navigating to Start Menu > PI System > PI System Explorer.
1178	2.	On the left navigation panel, select Library.
1179	3.	In the navigation tree in the Library panel, select Templates > Event Frame Templates.
1180	4.	Right click in the whitespace of the Element Templates window and select New Template.
1181		a. Enter the following:
1182		b. Name: Station Mode Error
1183		c. Description: CRS Workcell machining station mode error
1184 1185	5.	Naming Pattern:ALARM-%ELEMENT%.%TEMPLATE%.%STARTTIME:yyyy-MM-dd HH:mm:ss.fff%
1186 1187	6.	In the navigation tree in the Library panel, select Templates > Element Templates > Machining_Station.
1188 1189	7.	In the Machining_Station panel select the Analysis Templates tab and click Create a new analysis template.
1190 1191	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 .
1192	9.	Select "Station Mode Error" in the Event Frame template drop-down menu.
1193	10	 In the Expression field for "StartTrigger1", enter the expression:
1194		<pre>'RawMode' < 0 OR 'RawMode' > 1;</pre>
1195	11	Click the Add drop-down menu and select End Trigger, and enter the expression:
1196		('RawMode' > 0 AND 'RawMode' < 1)
1197	12	. Select the "Event-Triggered" option for the Scheduling type.
1198	13	. Click the Check In button on the top menu to save all changes to the database.
1199	2.6.3	.4 PI Web API
1200 1201 1202	compl	Web API is used by Dragos to collect event frames from the DMZ Historian server. After eting the installation of the PI Web API, the "Change PI Web API Installation Configuration" dialog ys. The following steps describe how to configure the Web API on the DMZ Historian server.
1203	1.	In the Telemetry section, verify the checkbox option and click Next.

- In the Configuration Store section, select "PI-ROBOTICS" in the Asset Server drop-down menu
 and click Connect. Leave the default instance name.
- 12063. In the Listen Port section, verify port 443 is entered in the Communication Port Number1207textbox and check the Yes, please create a firewall Exception for PI Web API checkbox.

- In the Certificate section, click Next to continue and use the self-signed certificate or select
 Change to modify the certificate.
- 1210 5. In the API Service section, leave the default service NT Service\piwebapi and click Next.
- 12116. In the Crawler Service section, leave the default service NT Service\picrawler and1212click Next.
- 1213 7. In the Submit URL section, enter the URL of the DMZ Historian server Web API service:
 1214 https://pi-dmz/piwebapi/. Click Next.
- 1215 8. In the **Review Changes** section, verify all the configuration settings, check the checkbox Accept1216 all the configurations, and click **Next**.
- 1217 9. Click **Finish** to complete the configuration.

1218 2.6.3.5 Firmware Integrity Checking

- 1219 Software was developed to demonstrate the ability of PI to obtain device and firmware data from a
- 1220 Beckhoff PLC for integrity checking purposes. A new PLC task was programmed to periodically query its
- 1221 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 notmatch their expected values.
- 1224 It is important to note that this capability was developed to demonstrate a method of maintaining
- 1225 visibility of PLC hardware and firmware version numbers for integrity purposes and is not secure or
- 1226 infallible. If a malicious actor takes control of the PLC, the hardware and firmware versions provided by
- the PLC can be spoofed.
- 1228 The following steps describe how to sequentially configure this capability across multiple systems and 1229 software. Only one system or software is described in each section.

1230 Beckhoff PLC Modbus TCP Server

- 1231 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.
- 1234 1. Log in to the Windows CE Desktop of the Beckhoff PLC and open the XML file:
- 1235 \TwinCAT\Functions\TF6250-Modbus-TCP\Server\TcModbusSrv.xml
- 1236 2. Modify the <InputRegisters>... </InputRegisters> section to the following:

<in< th=""><th>putRegisters></th></in<>	putRegisters>
<m></m>	appingInfo>
	<adsport>851</adsport>
	<startaddress>32768</startaddress>
	<endaddress>32895</endaddress>
	<varname>GVL.mb_Input_Registers</varname>
<,	/MappingInfo>
<1	MappingInfo>
	<adsport>852</adsport>
	<startaddress>32896</startaddress>
	<endaddress>33023</endaddress>
	<varname>GVL.mb Input Registers</varname>
<,	/MappingInfo>
<td>nputRegisters></td>	nputRegisters>

1237

- 1238 3. Save and close the file.
- 1239 4. Restart the PLC.

1240 The Modbus TCP server will now have two register address ranges: 128 addresses for the PLC task at 1241 port 851, and 128 addresses for the PLC task at port 852.

1242 Beckhoff PLC Project

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

- 12451. On the engineering workstation, open the TwinCAT XAE Shell by navigating to Start Menu >1246Beckhoff > TwinCAT XAE Shell and open the current PLC project.
- 1247 2. In the **Solution Explorer**, right click **PLC** and select **Add New Item...**
- 12483. In the Add New Item dialog box, select Standard PLC Project, enter the name1249FirmwareIntegrityCheck in the Name textbox, and click Add.
- 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.
- 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.
- 1254 6. In the Solution Explorer, right click PLC > GVLs and click Add > Global Variable List. In the dialog
 1255 box enter the name GVL in the Name textbox and click Open.
- 1256 7. In the **Editor Window**, enter the following code:

VAR GLOBAL				
mb_Input_Register	s:	ARRAY	[0127]	OF WORD;
END_VAR				

- 1258 8. In the **Solution Explorer**, right click **PLC > FirmwareIntegrityCheck > POU** and select **Add > POU**.
- 1259 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.
- 1261 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
```

1262

1263 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
```

1264

1265 11. Save and close the POU.

1266 12. In the Solution Explorer, double click PLC > FirmwareIntegrityCheck > POUs > MAIN (PRG).

1267 13. In the Editor Window, enter the following into the Variables section (your AMS net ID may1268 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
```

1270 14. In the **Editor Window**, enter the following into the **Code** section:

1271

- 1272 15. Save and close the POU.
- 1273 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.
- 1277 17. The firmware integrity checking code is now running on the Beckhoff PLC. In the top menu
 1278 select **PLC > Logout** and close the TwinCAT XAE Shell.
- 1279 The PLC will now write the hardware serial number and firmware version numbers to the Modbus1280 TCP server registers.

1281 OSIsoft PI Points

- 1282 The following steps describe how to create the PI points and tags in the CRS Local Historian server and 1283 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.
- 1286 2. In the Interface drop-down menu, select the Modbus Interface (PIModbusE1).
- 1287 3. Select the **General** menu option. In the **Scan Classes** section, click the **New Scan Class** button.
- Set the Scan Frequency to "60" and the Scan Class # to the next sequential class number as
 shown in Figure 2-32 below.

1290 Figure 2-32 Screenshot of the PI Interface Configuration Utility Showing the Added Scan Class # 2 for

1291 Polling the PLC Every 60 Seconds

		Pl Interfa	ace Configura	ation Utility - PIM	odbusE1				-	o x
		Interface T	ools Help							
		🎦 📂 🗡		🗖 🖸 🔂 🔂	🔳 📀					
		Interface:	Robotics Mod	bus Interface (PIMo	odbusE1) -> f	PI-ROBOTICS			•	Rename
		Type:	ModbusE	▼ Modł	ous Ethernet	PLC			PI Data server Con	nection Status
		Description:							PI-ROBOTI Writeable	CS
		Versions:	PIModbusE.ex	xe version 4.3.1.24		Unilnt version	4.7.1.6		vvniceable	
		General		General				- PI Host Information		
		ModbusE Service		Point Source:	MODBUSE		슈	Server/Collective:	PI-ROBOTICS	▼ ▼
		UniInt			MODBUS	E	\mathbf{X}	SDK Member:	PI-ROBOTICS	-
		- Failover - Health Po	pints				_	API Hostname:	PI-ROBOTICS	-
			nce Counters	Interface ID:	1			User:	piadmins PIWorld	
		Performar PI SDK	nce Points	- Scan Classes				Туре:	Non-replicated - PI3	
			cted Startup			<u>*</u> ×	†	Version:	PI 3.4.435.604	
		i Debug IO Rate		Scan Frequency	/	Scan Class #	#	Port:	5450	
		Interface Sta	tus	√ 1 √ 60		1 2				
				•				- Interface Installation		
								,	86)\PIPC\Interfaces\	Modbus
								Interface Batch File PIModbusE1.bat	name	
								Ji imodbuse r.bac		
									Close	Apply
1292		Ready		Running		PIMo	dbusE1 - In	stalled		
1293										
1294	5.	Click Apply	and close	the program.						
1295	6.	On the CRS	Local Hist	orian server. d	open the	PI System I	Manage	ment Tools by	navigating to S	start
1296				PI System Mai	•	-				
1207	-		-	-	-		Deint D	بدامامير		
1297	7.	in the syste	in Manage	ement Tool pa	anel, sele	ct Points >	Point B	ullder.		
1298	8.	Create a ne	w tag for t	he PLC hardw:	vare seria	l number w	vith the	following confi	guration:	
1299		a. Nar	ne: PLC-I	HardwareSe	erialNu	umber				
1300		b. Ser	ver: PI-R	OBOTICS						
1301		c. Des	criptor: Ha	ardware se	erial 1	number o	of the	CRS Beckh	off PLC	
1302		d. Poi	nt Source:	MODBUSE						
1303		e. Poi	nt Type: I	nt16						

1304	f. Location 1:1
1305	g. Location 2: 0
1306	h. Location 3: 104
1307	i. Location 4: 2
1308	j. Location 5: 32897
1309	k. Instrument Tag: 192.168.0.30
1310	9. Create a new tag for the PLC TwinCAT build number with the following configuration:
1311	a. Name: PLC-TwinCATBuildNumber
1312	b. Server: PI-ROBOTICS
1313	c. Descriptor: Build number of the CRS PLC TwinCAT firmware.
1314	d. Point Source: MODBUSE
1315	e. Point Type: Int16
1316	f. Location 1: 1
1317	g. Location 2: 0
1318	h. Location 3: 104
1319	i. Location 4: 2
1320	j. Location 5: 32900
1321	k. Instrument Tag: 192.168.0.30
1322	10. Create a new tag for the PLC TwinCAT revision number with the following configuration:
1323	a. Name: PLC-TwinCATRevisionNumber
1324	b. Server: PI-ROBOTICS
1325	c. Descriptor: Revision number of the CRS PLC TwinCAT firmware.
1326	d. Point Source: MODBUSE
1327	e. Point Type: Int16
1328	f. Location 1: 1
1329	g. Location 2: 0
1330	h. Location 3: 104
1331	i. Location 4: 2

1332	j.	Location 5: 32899							
1333	k.	Instrument Tag: 192.168.0.30							
1334 1335									
1336	a.	Name: PLC-TwinCATVersionNumber							
1337	b.	Server: PI-ROBOTICS							
1338	С.	Descriptor: Version number of the CRS PLC TwinCAT firmware.							
1339	d.	Point Source: MODBUSE							
1340	e.	Point Type: Int16							
1341	f.	Location 1: 1							
1342	g.	Location 2: 0							
1343	h.	Location 3: 104							
1344	i.	Location 4: 2							
1345	j.	Location 5: 32898							
1346	k.	Instrument Tag: 192.168.0.30							

1347 12. Close the **PI System Management Tools** program. The PI points are now available to the DMZ1348 Historian server via the PI System Connector.

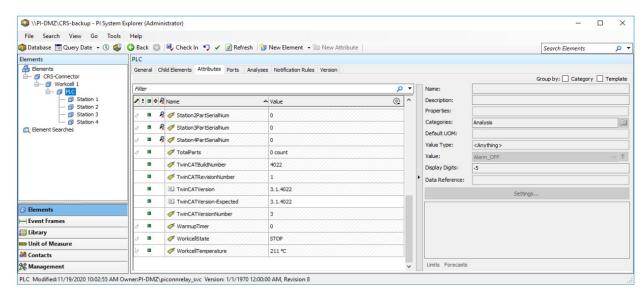
Figure 2-33 Screenshot of the PI System Management Tools Component After Configuring the PI Points
 for PLC Hardware and Firmware Version Number Integrity Checking

ervers	衬 🖬 🍕	🖻 🛃 🕜							4
arch p Servers	PI-ROBOTICS PI-ROBOTICS	Name PLC-HardwareSerialNumber PLC-TwinCATBuildNumber PLC-TwinCATRevisionNumber PLC-TwinCATVersionNumber	Stored Values Real-time data Real-time data Real-time data Real-time data	MODBUSE MODBUSE MODBUSE	Point Type Int16 Int16 Int16 Int16 Int16	Point Class classic classic classic classic	Descriptor	Point Security pladmin: A(r,w) pladmins: A(r,w) PISC: A(r,w) PIWorld: A(r) pladmin: A(r,w) pladmins: A(r,w) PISC: A(r,w) PIWorld: A(r) pladmin: A(r,w) pladmins: A(r,w) PISC: A(w) PIWorld: A(r) pladmin: A(r,w) pladmins: A(r,w) PISC: A(r,w) PIWorld: A(r)	piadmin: A(r,w) piadmins: A(r,w) PISC: A(r,w) PIWo piadmin: A(r,w) piadmins: A(r,w) PISC: A(r,w) PIWo
vatem Management Tools Varch Varma V	General Archi Location 1: Location 2: Location 3: Location 4: Location 5: Instrument Tag: Session Record		t Code:	1 Userint1: 0 Userint2: 0 UserReal	L	0 0 0 0			

1353 1354	 On the DMZ Historian server, open the PI System Explorer by navigating to Start Menu > PI System > PI System Explorer.
1355	14. On the left navigation panel, select Library.
1356 1357	15. In the navigation tree in the Library panel, select Templates > Element Templates > PLCTemplate.
1358	16. Open the Attribute Templates tab in the PLCTemplate panel.
1359 1360	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:
1361	a. Name: HardwareSerialNumber
1362	b. Description: Hardware serial number of the CRS Beckhoff PLC.
1363	c. Value Type: Int16
1364	d. Data Reference: PI Point
1365	e. Tag:\\PI-ROBOTICS\PLC-HardwareSerialNumber
1366 1367	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:
1368	a. Name: HardwareSerialNumber-Expected
1369 1370	b. Description: Expected hardware serial number of the CRS Beckhoff PLC.
1371	c. Value Type: V
1372	d. Data Reference: None
1373 1374	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:
1375	a. Name: TwinCATBuildNumber
1376	b. Description: Build number of the CRS PLC TwinCAT firmware.
1377	c. Value Type: Int16
1378	d. Data Reference: PI Point
1379	e. Tag:\\PI-ROBOTICS\PLC-TwinCATBuild
1380 1381	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:
1382	a. Name: TwinCATRevisionNumber
1383	b. Description: Revision number of the CRS PLC TwinCAT firmware.

1384	c. Value Type: Int16
1385	d. Data Reference: V
1386	e. Tag: \\PI-ROBOTICS\PLC-TwinCATRevision
1387 1388	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:
1389	a. Name: TwinCATVersionNumber
1390	b. Description: Version number of the CRS PLC TwinCAT firmware.
1391	c. Value Type: Int16
1392	d. Data Reference: PI Point
1393	e. Tag: \\PI-ROBOTICS\PLC-TwinCATVersion
1394 1395 1396	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:
1397	a. Name: TwinCATVersion
1398	b. Description: Version number of the CRS PLC TwinCAT firmware.
1399	c. Value Type: String
1400	d. Data Reference: String Builder
1401 1402 1403	<pre>e. String: 'TwinCATVersionNumber';.;'TwinCATRevisionNumber';.;'TwinCAT BuildNumber';</pre>
1404 1405 1406	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:
1407	a. Name: TwinCATVersion-Expected
1408 1409	b. Description: Expected version number of the CRS PLC TwinCAT firmware.
1410	c. Value Type: String
1411	d. Data Reference: None
1412	The PI points are now available as PLC attributes in the Asset Framework on the DMZ Historian server.

- 1413 Figure 2-34 Screenshot of PI System Explorer Displaying some Attributes of the PLC Element. Attributes
- 1414 for the TwinCAT version number are visible in the list.



1416 OSIsoft PI Analyses and Event Frames

1415

1417 The following steps describe how to create the PI analyses and event frame templates to generate event 1418 frames when the hardware or firmware version numbers do not match the expected values.

- 1419 1. In the navigation tree in the **Library** panel, select **Templates > Event Frame Templates**.
- On the top menu bar click **New Template** and enter the following configuration as shown in
 Figure 2-35:
- 1422 a. Name: Hardware Serial Number Mismatch

1423	b.	Naming pattern: %ELEMENT% %ANALYSIS% (Expected:		
1424		%@.\Elements[.] HardwareSerialNumber-Expe	ected%,	Detected:
1425		<pre>%@.\Elements[.] HardwareSerialNumber%)</pre>	%START1	TIME: yyyy-MM-
1426		dd HH:mm:ss.fff%		

1427 Figure 2-35 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Event

1428 Frame Template.

File View Go Tools	Help				
🟮 Database 🛗 Query Date	• 🕓 🤩 🔇 Back 🏐	💐 Check In 🧐 🖌 🗃 Refresh 🛛 🗃 New	Template -	Search Element Temp	lates 🔎
Library	Hardware Ser	rial Number Mismatch			
CRS-backup	∧ General Att	ribute Templates			
	es Name:	Hardware Serial Number Mismatch			
🖃 – 🦷 Event Frame Tem	nplates Description:				
BatchEventF		te: <none></none>	Severity:	Major	
HighTrouble	CallCount Categories:		Default Attribute:	<none></none>	
HighWorkcel		m: KELEMENT% %ANALYSIS% (Expected: %	A Sements [] Harr	wareSerialNumber-Expected	% Dete
	nityFault		_		nay brace
StationDoorf		Allow Extensions Can Be Acknowle		nplate Only	
StationOutO		Extended Properties (0) Location Reas	on <u>Security</u>		
	Find:	Derived Templates Event Frames	Referenced Paren		
J Elements		Derived Event Frames	Referenced Child	Templates	
- Event Frames					
Library					
Durit of Measure					
Contacts					
& Management		10-56-25 AM Owner DL DM7) nindmin			
X Management Hardware Serial Number Misr	match Modified:11/19/2020	TU: J0:2J AIVI OWNELPI-DIVIZ (plaumin			
Hardware Serial Number Misr	menu bar click Ne	w Template and enter the fo	bllowing con	figuration as sho	wn ir
Hardware Serial Number Misr 3. On the top r Figure 2-36:	menu bar click Ne		bllowing con	figuration as sho	wn in

1437 Figure 2-36 Screenshot of PI System Explorer Displaying the TwinCAT Version Mismatch Event Frame1438 Template

El. 16		(Administrator) - 🗆
File View Go		ck 💿 💐 Check In 🍤 🖌 🔊 Refresh 📓 New Template 🔹 Search Element Templates
Library		CAT Version Mismatch
		eral Attribute Templates
	hWorkcellTemperati spectionFailure	TwinCAT Version Mismatch
		cription:
- H St	ationModeError Base	e Template: <none> Severity: Major</none>
	ationOutOfSync Cate	egories: Default Attribute: None>
		ing Pattern: %ELEMENT% %ANALYSIS% (Expected: %@.\Elements[.] TwinCATVersion-Expected%, Detected:
😟 — 🎁 Transfe	r Templates	Allow Extensions Can Be Advnowledged Base Template Only
Enumeration	Viner Y	Extended Properties (0) Location Reason Security
<	> Find	
Elements		Derived Event Frames Referenced Child Templates
Event Frames		
Unit of Measure		
A Contacts		
🔆 Management		
5. In the		n on the top menu to save all changes to the database. the Library panel, select Templates > Element Templates >
	mplate	
6. Open templ		plates tab in the PLCTemplate panel and click Create a new analysis
templ	the Analysis Temp ate.	plates tab in the PLCTemplate panel and click Create a new analysi s iguration as shown in Figure 2-37:
templ	the Analysis Temp ate. the following conf	
templ 7. Enter a.	the Analysis Temp ate. the following conf Name: Hardwa Description: The	iguration as shown in Figure 2-37:
templ 7. Enter a.	the Analysis Temp ate. the following conf Name: Hardwa Description: The expected se	iguration as shown in Figure 2-37: re Serial Number Mismatch e PLC hardware serial number does not match th
templ 7. Enter a. b.	the Analysis Temp ate. the following conf Name: Hardwa Description: The expected se Analysis Type: E	iguration as shown in Figure 2-37: re Serial Number Mismatch e PLC hardware serial number does not match th crial number.
templ 7. Enter a. b. c.	the Analysis Temp ate. the following conf Name: Hardwa Description: The expected se Analysis Type: E Enable analyses	iguration as shown in Figure 2-37: re Serial Number Mismatch e PLC hardware serial number does not match therial number. vent Frame Generation

1454 8. In the **Expression** field for "StartTrigger1", enter the expression:

- 1455 'HardwareSerialNumber'<>'HardwareSerialNumber-Expected' and NOT 1456 BadVal('HardwareSerialNumber');
- 1457 9. Click **Add**... drop-down menu and select End Trigger, and enter the expression:
- 1458 'HardwareSerialNumber'='HardwareSerialNumber-Expected';
- 1459 10. Select the "Event-Triggered" option for the Scheduling type and "Any Input" for the Trigger On
 1460 drop-down menu.
- 1461 Figure 2-37 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch
- 1462 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 🔹 🕔 🥥	3 Back 🌍 🖳 Check In 🍤 🖌 👔 Refresh 🔡 New Template 👻			Search	n Element Templates	P -
Library	PLCTemplate					
CRS-backup	General Attribute Templates Ports Analysis Templates Notification Rule Templates					
- 😡 Templates		Name:	Hardware Serial Number Mismatch			
- 🔂 Machining_Station	🕼 🗃 Name	Description:	The PLC hardware serial number doe	es not match the expe	ected serial number.	
PLCTemplate	Hardware Serial Number Mismatch	Categories:				~
- Model Templates	H TwinCAT Firmware Version Mismatch	Analysis Type	Expression O Rollup	Event Frame Genera	ation O SQC	
Transfer Templates Enumeration Sets			alyses when created from template		11	
- 🕁 Reference Types		Create a new	notification rule template for Hardwa	are Serial Number Misi	match	
Tables	Example Element: CRS-Connector\Workcell 1\PLC					
						- 0
🙆 Analysis Categories	Generation Mode: Explicit Trigger v Event Frame Template:	Hardware Serial Num	ber Mismatch			×
Attribute Categories Element Categories	Add_ v				Evaluate	
Motification Rule Categories	Name Expression			True for	Severity	
🔄 Reference Type Categories	Start triggers					
_	StartTrigger1 'HardwareSerialNumber'<>'HardwareSerialNumber-Expecte	d' and NOT BadVa	l('HardwareSerialNumber')	Set (optional)	Major ~	
	End trigger				1	
	EndTrigger 'HardwareSerialNumber'='HardwareSerialNumber-Expected'				×	
					0	
🗇 Elements						
Hevent Frames						
jii Library				Advanced Ev	vent Frame Settings	
unit of Measure	Scheduling: Event-Triggered Periodic					
A Contacts						
💥 Management	Trigger on Any Input v					
PLCTemplate Modified:11/19/2020 11:11:3	2 AM Owner:PI-DMZ\piconnrelay_svc					

- 1465 11. To create a new analysis template for TwinCAT firmware version mismatch, click Create a new analysis template.1466 analysis template.
- 1467 12. Enter the following configuration as shown in Figure 2-38:
- 1468 a. Name: TwinCAT Firmware Version Mismatch
- 1469 b. Description: The TwinCAT version installed in the PLC does not1470 match the expected version.
- 1471 c. Analysis Type: Event Frame Generation
- 1472 d. Enable analyses when created from template: Checked
- 1473 e. Generation Mode: Explicit Trigger

- 1474 f. Event Frame Template: Hardware Serial Number Mismatch
- 1475 13. In the **Expression** field for "StartTrigger1", enter the expression:

1476 not Compare('TwinCATVersion', 'TwinCATVersion-Expected') and NOT 1477 BadVal('TwinCATVersion');

1478 14. Click the **Add...** drop-down menu and select **End Trigger**, and enter the expression:

1479 Compare('TwinCATVersion', 'TwinCATVersion-Expected');

- 1480 15. Select the "Event-Triggered" option for the Scheduling type and "Any Input" from the Trigger
 1481 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)					1 2	×
File View Go Tools Help							
🔕 Database 🛗 Query Date 🔹 🕔 🕌 🛛	🔇 Back 💿 💐 Check in 🍤 🖌 🛃 Refresh 🔡 New Template 👻			Search	h Element Templa	ntes 🔎	•
Library	PLCTemplate						
LUbrary Construction Constructi	General Attribute Templates Ports Analysis Templates Notification Rule Templates Image: TwinCAT Firmware Version Mismatch Description: The TwinCAT Firmware Version Mismatch Image: TwinCAT Firmware Version Mismatch Description: The TwinCAT version installed in the PLC discover and the PLC		PLC does not match) Event Frame Genera	ation O SQC			
	Name Expression Start triggers Start Trigger1 Start Trigger1 not Compare('TwinCATVersion', 'TwinCATVersion-Expected') End trigger Compare('TwinCATVersion', 'TwinCATVersion-Expected')	and NOT BadVa	l('TwinCATVersion')		Major ~	8	, a
🗊 Elements	u						
- Event Frames							
📁 Library				Advanced E	vent Frame Settin	gs	
🚥 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						

- 1486
 16. On the top menu bar click **Check In**, verify the changes in the dialog box and click the **Check In**1487
 button.
- 1488 17. On the left navigation panel, select **Elements**.
- 1489 18. In the navigation tree in the **Elements** panel, select **CRS-Connector > Workcell 1 > PLC.**
- 1490 19. Open the **Attributes** tab in the PLC panel.
- 1491 20. Select the attribute HardwareSerialNumber-Expected and enter the expected hardware serial
 1492 number (e.g., 5870) in the Value textbox.

- 1493 21. Select the attribute TwinCATVersion-Expected and enter the expected hardware serial number
 1494 (e.g., 3.1.4022) in the Value textbox.
- 1495 22. On the top menu bar and click **Check In**, verify the changes in the dialog box, and click **Check In**.
- 1496 Event frames will now be generated in the DMZ Historian if the PLC reports a hardware serial number
- 1497 that does not match the expected value or if the TwinCAT firmware version number does not match the 1498 expected value.

1499 **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.
- 1506 Note: Wazuh is a fork of the open source project OSSEC, a host-based intrusion detection system. In 1507 some places in Wazuh and this document, the term OSSEC will be used in place of Wazuh.

1508 2.7.1 Host and Network Configuration

- 1509 Wazuh is an agent-based software. For this project, an existing Security Onion server was used, and the
- 1510 Wazuh agent was installed on multiple endpoints in both the PCS and CRS environments. The tables
- 1511 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- ion Server	Hyper-V VM	Ubuntu 16.04 LTS	4	16GB	450GB	Testbed LAN 10.100.0.26
Nessus VM	Hyper-V VM	Windows 2012R2	2	6GB	65GB	Testbed LAN 10.100.0.25
Dispel VDI	Hyper-V VM	Windows 2016	2	8GB	126GB	DMZ LAN 10.100.1.61
DMZ Histo- rian	Hyper-V VM	Windows 2016	4	8GB	80GB/171GB	DMZ LAN 10.100.1.4

1513 Table 2-13 Security Onion Domain Hosts Deployment

1515 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

1516

1517 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

1518

1519 2.7.2 Installation

- 1520 Security Onion Server version 3.9 and Wazuh Agent version 3.9 were used.
- 1521 Installation of Wazuh involves setting up the central server and installing agents on hosts that needed to1522 be monitored.
- 1523 Security Onion server contains the Wazuh manager and API components as well as the Elastic Stack. The 1524 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.
- 1526 The Wazuh agent, which runs on the monitored host, is responsible for collecting system log and
- 1527 configuration data and detecting intrusions and anomalies. The collected data is then forwarded to the
- 1528 Wazuh manager for further analysis.
- 1529 The Security Onion server was already a part of the lab infrastructure prior to this effort. For the server
- 1530 component installation process, please follow the guidance from the Security Onion Installation Guide 1531 for version 3.9 available at https://documentation.wazuh.com/3.9/installation-guide/index.html.
- 1532 For information on adding agents to the server, please follow the guidance from the Security Onion
- 1532 Installation Guide for version 3.9 available at https://documentation.wazuh.com/3.9/user-
- 1534 manual/registering/index.html.

1535 2.7.3 Configuration

- 1536 1. Configure Additional Directories or Files for Wazuh Agent File Integrity Monitoring:
- 1537 a. Files and directories to be monitored are specified in the ossec.conf file on each host.

- 1538 1539
- 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.
- 1540 Figure 2-39 Wazuh Agent Manager

😽 Wazuh	zuh Agent Manager $ imes$					
Manage	View Help					
-Wazuh Agent:	View Logs View Config					
Status:	Status: Running					
-	Manager IP: 10.100.0.26 Authentication key: MDA3IFBJLURNWiAxMC4xMD/					
Save Refresh https://wazuh.com Revision 3937						

- 1542b.Selecting View Config opens the ossec.conf file in Notepad. Alternatively, the file can be1543opened in Notepad from its location in the "C:\Program Files (x86)\ossec-agent" direc-1544tory on the host machine, as shown in Figure 2-40.
- 1545 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:\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\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>
</d
```

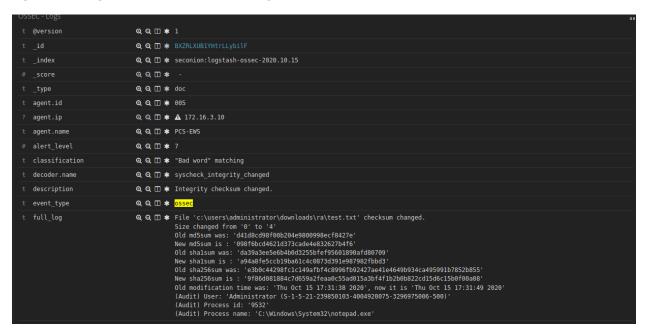
1541

1547 1548 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.

- 1549 d. Once the changes are made, save the ossec.conf file and restart the Wazuh Agent by opening the Configuration Manager, selecting "Manage", and "Restart" as shown in Fig-1550 1551 ure 2-41.
- 1552 Figure 2-41 Wazuh Agent Manager User Interface

🐳 Wazuh Agent Manager	\times
Manage View Help	
Start Stop - 10.100.1.4 Restart	
Status	
Exit Manager In: 100.0.26	
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 1554 sent to the Wazuh Manager. Figure 2-42 shows the log received after a file change was 1555 1556 detected.
- 1557 Figure 2-42 Log Received After a File Change Was Detected



1559 2.8 TDi ConsoleWorks

1560 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

1562 interface through which authenticated and authorized users receive access to graphical and shell

1563 interfaces on configured ICS components.

1564 2.8.1 Host and Network Configuration

1565 ConsoleWorks resides on a VM that was reconfigured for supporting Builds 1 and 3 as described in Table

1566 2-16 and Table 2-17 respectively.

1567 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

1568

1569 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

1570

1571 2.8.2 Installation

- 1572 ConsoleWorks version 5.3-1u3 is installed on a CentOS 7 operating system using the following
- 1573 procedures. Product installation guides and documentation are available at
- 1574 <u>https://support.tditechnologies.com/product-documentation</u>. Follow these steps for installation:
- 1575 1. Harden and configure the Operating System:
- 1576a. Log in to the system with privileged access and set the Static IP Address information by1577editing /etc/sysconfig/network-scripts/ifcfg-eth0 using the following settings:
- 1578 i. For Build 1 use the following network configuration:
- 1579 1) IP Address: 10.100.0.53
- 1580 2) Subnet Mask: **255.255.255.0**
- 1581 3) Gateway: **10.100.0.1**
- 1582 4) DNS: **10.100.0.17**
- 1583 ii. For Build 3 use the following network configuration:
- 1584 1) IP Address: **192.168.0.65**

1585	2) Subnet Mask: 255.255.255.0
1586	3) Gateway: 192.168.0.2
1587	4) DNS: 10.100.0.17
1588	iii. Restart the network service as follows:
1589	<pre># systemctl restart network</pre>
1590	b. Set the NTP Configuration as follows:
1591	i. In /etc/ntp.conf, add as the first server entry:
1592	server 10.100.0.15
1593 1594	c. Apply the following Department of Defense (DOD) Security Technology Implementation Guide (STIG) settings:
1595	i. Ensure ypserv is not installed using the following command:
1596	# yum remove ypserv
1597 1598	ii. Ensure Trivial File Transfer Protocol (TFTP) is not installed using the following command:
1599	# yum remove tftp-server
1600	iii. Ensure RSH-SERVER is not installed using the following command:
1601	# yum remove rsh-server
1602	iv. Ensure File Transfer Protocol (FTP) is not installed using the following command:
1603	# yum remove vsftpd
1604	v. Ensure TELNET-SERVER is not installed using the following command:
1605	# yum remove telnet-server
1606	vi. Configure SSH to use SSHv2 only.
1607 1608	 To disable SSHv1, ensure only Protocol 2 is allowed in the /etc/ssh/sshd_config.
1609 1610 1611 1612 1613	Protocol 2 PermitRootLogin no Ciphers aes128-ctr, aes192-ctr, aes256-ctr, aes128- cbc MACs hmac-sha2
1614	vii. Disallow authentication using an empty password as follows:
1615	1) Add PermitEmptyPasswords no to /etc/ssh/sshd_config file.

1616 1617		 Remove any instances of the nullok option in /etc/pam.d/system-auth and /etc/pam.d/password-auth files.
1618	viii.	Enable FIPS Mode as follows:
1619		1) FIPS mode can be enabled by running the command:
1620 1621		# yum install dracut # dracut -f
1622 1623		2) When step 1) is complete, add fips=1 to the /etc/default/grub file and run the command:
1624		<pre># grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg</pre>
1625		3) When step 2) completes, reboot the server with this command:
1626		# reboot
1627	ix.	Enable server auditing
1628 1629		 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:
1630		<pre># systemctl start auditd.service.</pre>
1631	х.	Configure system to only install approved digitally signed packages:
1632 1633 1634		 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.
1635	xi.	Enable the firewall:
1636		1) To enable the firewall, run the following commands:
1637		<pre># yum install firewalld and</pre>
1638		<pre># systemctl start firewalld.</pre>
1639 1640 1641 1642		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:
1643		<pre># firewall-cmdlist-all</pre>
1644		3) Add the HTTPS configuration to the firewall using the following command:
1645 1646		<pre># firewall-cmdzone=publicpermanentadd- service=https</pre>
1647	xii.	Enable SELinux and set to "targeted":

1648 1649	 Add SELINUX=enforcing and SELINUXTYPE=targeted in the /etc/selinux/config file and then reboot the server with this command:
1650	# reboot
1651	xiii. Enable Antivirus as follows:
1652 1653 1654	 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:
1655	<pre># yum install -y epel-release</pre>
1656 1657 1658 1659	<pre># yum -y install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav- scanner-systemd clamav-devel clamav-lib clamav- server-systemd</pre>
1660	2) Update SELinux policy to allow ClamAV to function
1661	# setsebool -P antivirus_can_scan_system 1
1662 1663	3) Make a backup copy of the scan.conf file and update to remove the Example string from the file using these commands:
1664	# cp /etc/clamd.d/scan.conf /etc/clamd.d/scan.conf.bk
1665	# sed -i '/^Example/d' /etc/clamd.d/scan.conf
1666	4) Uncomment the following line from /etc/clamd.d/scan.conf:
1667	LocalSocket /var/run/clamd.scan/clamd.sock
1668 1669	 Configure freshclam to automatically download updated virus definitions using these commands:
1670	# cp /etc/freshclam.conf /etc/freshclam.conf.bak
1671	# sed -i -e "s/^Example/#Example/" /etc/freshclam.conf
1672	6) Manually run freshclam to confirm the settings as follows:
1673	# freshclam
1674	7) Start and enable the clamd service with these commands:
1675	# systemctl start clamd@scan
1676	# systemctl enable clamd@scan
1677	8) Ensure log directory is available with this command:
1678	# mkdir /var/log/clamav

1679 1680	9) Create the daily scan script to scan directories of interest. Note: for the lab implementation only the /home volume was selected for scanning.
1681	# vi /etc/cron.daily/clamav_scan.sh
1682	
1683 1684 1685 1686 1687 1688	File Contents #!/bin/bash SCAN_DIR="/home" LOG_FILE="/var/log/clamav/dailyscan.log" /usr/bin/clamscan -ri \$SCAN_DIR >> \$LOG_FILE
1689	10) Set the file to have execute privilege with this command:
1690	<pre># chmod +x /etc/cron.daily/clamav_scan.sh</pre>
1691	2. Download and Install the ConsoleWorks packages
1692 1693 1694	 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.
1695 1696	 After downloading the ConsoleWorks installation package, copy it to the ConsoleWorks VM using a Secure Copy (scp) utility.
1697 1698	c. Follow the procedures from TDi ConsolWorks New Installation and Upgrade Guide for Linux Chapter 3: Automated New Installation of ConsoleWorks
1699	i. During installation, create a New Invocation named "NCCOE".
1700	ii. Create a new certificate.
1701	iii. Set the system to automatically start the ConsoleWorks Invocation.
1702	d. Login to the platform and initiate the offline registration process (Figure 2-43).
1703	e. Once the license file is obtained, complete the registration process (Figure 2-44).

1704 Figure 2-43 ConsoleWorks Registration Screen

Console <mark>Works</mark> ®	v 5.3-1u3			Unregistered Administration
⇒ FAVORITES	ADMIN: Server Man	agement: Registration		+_
No Favorites saved	Registration 🗙 Offlin	e Registration 🔀		
	ConsoleWorks Re	gistration		Complete My Offline Registration
DASHBOARDS	Contact Name:		▶ PROXY DETAILS	^
▷ CONSOLES				
▶ DEVICES	Contact Email:		► ADVANCED OPTIONS	
▶ LOGS	Telephone:			
▶ EVENTS	Facility (Site) Name:	NIST Gaithersburg		
▶ REGULATORY	Address Line 1:	100 Bureau Drive		
▶ GRAPHICAL	Address Line 2:			
▶ USERS	City:	Gaithersburg		
▶ REPORTS	State/Province:	MD		
▶ TOOLS	Zip/Postal Code:]	
▶ SECURITY				
▶ ADMIN	Country:	United States		
▶ HELP				~
		ter Offline		Cancel Save
EXTERNAL TOOLS A	Register Online Regis			Cancer Save
None Available	1			

1705

1706 Figure 2-44 ConsoleWorks Offline Registration Process

Console <mark>Works</mark>	® v 5.3-1u3 Unregist Administr	
▼ FAVORITES	▼ ADMIN: Server Management: Offline Registration	
No Favorites saved	Registration 🔀 Offline Registration 🔀	
DASHBOARDS	ConsoleWorks Offline Registration Complete My Offline Registration Please send support@tditechnologies.com an Email with:	<u>jistration</u>
CONSOLES	This <u>file attached</u> Which contains your contact info, server operating system, and ConsoleWorks version. If Email is unavailable, please contact <u>TDI St</u>	upport
DEVICES	······································	
LOGS		
> EVENTS		
REGULATORY		
GRAPHICAL		
> USERS		
> REPORTS		
> TOOLS		
SECURITY		
> ADMIN		
> HELP		
EXTERNAL TOOLS	Complete My Offline Regi	stration
None Available		

1708	f.	This completes the default installation and establishes a basic ConsoleWorks server con-
1709		figuration. For the lab implementation, ConsoleWorks support provided two additional
1710		add-on packages (XML) files to setup the environment: ONBOARDING_1-DASH-
1711		BOARDS_NCCoE.zip providing preconfigured dashboards for accelerating configurations;
1712		and NCCOE_ACRs_20210122_083645.zip providing the access control rules, tags, and

1719 1720 1721

1722

1713	automation scripts used for the dashboards. These packages are scheduled for inclusion
1714	in future releases or can be requested from ConsoleWorks.

- i. 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.

1718 Figure 2-45 ConsoleWorks System Backups

FAVORITES	 ADMIN: Database Man 	agement: Backups			+_ - X
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	N	
EVENTS	2021/03/06 03:00	Schedule:WEEKLY	Done	N	
REGULATORY	2020/12/09 10:31	CONSOLE_MANAGER	Done	N	
GRAPHICAL	2021/02/02 16:38	CONSOLE_MANAGER	Done	N	
	2021/04/24 03:00	Schedule:WEEKLY	Done	N	
USERS	2021/06/14 10:55	CONSOLE_MANAGER	Done	N	
REPORTS	2021/02/11 08:07	CONSOLE_MANAGER	Done	N	
TOOLS	2021/05/01 03:00	Schedule:WEEKLY	Done	N	
SECURITY	2021/02/13 03:00	Schedule:WEEKLY	Done	N	
ADMIN	2021/05/08 03:00	Schedule:WEEKLY	Done	N	
Server Management	2021/02/10 11:07	CONSOLE_MANAGER	Done	N	
Database Manage	2021/02/09 13:07	CONSOLE_MANAGER	Done	N	
Backups	2021/02/06 03:00	Schedule:WEEKLY	Done	N	
Restore	2021/02/20 03:00	Schedule:WEEKLY	Done	N	
XML Exports	2021/03/27 03:00	Schedule:WEEKLY	Done	N	
XML Imports	2021/04/03 03:00	Schedule:WEEKLY	Done	N	
Orphan Files	2021/01/19 14:07	CONSOLE_MANAGER	Done	N	
Template Managem	2021/02/27 03:00	Schedule:WEEKLY	Done	Ν	~
HELP	Restore	Create	Backup	Delete	Download
EXTERNAL T 🔺					
None Available					

- 1) Import the Dashboard Add-On XML file.
- 1723 2) Import the *Supporting Configuration Add-On* XML file.

Console <mark>Wo</mark>	v 5.3-1u6	Administration
FAVORITES	ADMIN: Database Management: XML Imports: Import	+_
DASHBOARDS	Import XML 🔀	
CONSOLES		
DEVICES		
LOGS		
> EVENTS		
REGULATORY		
GRAPHICAL	How would you like to provide the XML to Import?	
USERS	Upload a file	
REPORTS		
TOOLS		
> SECURITY		
Z ADMIN		
Server Management		
Database Manage		
Backups		
Restore		
XML Exports		
VML Imports		
View		
Import		
Orphan Files		Next
Femplate Managem		
HELP		
EXTERNAL T 🍐		
None Available		

1724 Figure 2-46 ConsoleWorks Importing System Configurations and Components

1725

1726 2.8.3 Configuration

1727 The ConsoleWorks implementation required the following changes to the lab Cisco VPN appliance to1728 allow remote users to access the ConsoleWorks system:

- 1729 1. Login to the Cisco Firepower Appliance.
- 1730 2. Create the Following Destination Network Objects:
- 1731 a. For Build 1:
- i. Name: ConsoleWorks
- 1733 ii. IP Address: 10.100.0.52
- 1734 b. For Build 3:
- i. Name: CRS-NAT-IP
- 1736 ii. IP Address: 10.100.0.20
- 1737 3. Create the Following VPN-Rule:

1738	a.	For B	uild 1:
1739		i.	Action: Allow
1740		ii.	Source Networks: VPN-Pool
1741		iii.	Destination Networks: ConsoleWorks
1742		iv.	Destination Ports: TCP (6): 5176; HTTPS
1743	b.	For B	uild 3:
1744		i.	Action: Allow
1745		ii.	Source Networks: VPN-Pool
1746		iii.	Destination Networks: CRS-NAT-IP
1747		iv.	Destination Ports: TCP (6): 5176; HTTPS
4740			

1748 ConsoleWorks is then configured as follows. For configuration procedures, please see the ConsoleWorks
 1749 documentation available at <u>https://support.tditechnologies.com/product-documentation</u>.

- 1750 1. Configure ConsoleWorks Password Rules (Figure 2-47):
- 1751 Figure 2-47 ConsoleWorks Password Settings

Password rules are the minimum settings for ConsoleWork User accounts, although some rules can be overridden by	
Minimum Length: 12 🗘 (1-32	characters)
Passwords Must Contain: 🔲 Spaces	
✓ Numbers	
✓ Letters	
✓ Punctuation	
Mixed Case	
Number Between	First and Last Characters
Autofill Old Password During Forced Password Changes: Yes No	
Detween Passwords.	characters)
Minimum Time Between 5 (0-43)	200 minutes)
Password Reuse After: 3 (0-10	unique passwords)
Inactive Password Expiration After: 30 (0-36	5 days)
Failed Logins Before Lockout: 4 0-10)
Account Lockout Duration: Permanent	
	Canc

1755	b. NCCOE_USER
1756 1757	3. Configure the Graphical Gateway to allow users to use RDP within ConsoleWorks following these steps (Figure 2-48):
1758	a. Name: LOCAL_GG
1759	b. Description: Local GUI Gateway
1760	c. Host: 127.0.0.1
1761	d. Port: 5172

- 1762 e. Enabled: Selected
- 1763 f. Encrypt Connection: Selected
- 1764 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	Description: Local GUI Gateway	► TAGS (0)
▶ EVENTS		7 IAU3 (0)
▶ REGULATORY	Host: 127.0.0.1	
	Port: 5172 (default: 5172	2)
View	Enabled	
Add	Encrypt Connection	
Edit		
Recordings		
Active		
View		
Add		
Edit		
▶ USERS		
▶ REPORTS		
▶ TOOLS	-	
SECURITY	I	
▶ ADMIN	Set As Default Save As	Delete Cancel Save
▶ HELP		
EXTERNAL TOOLS		
None Available		

1765 1766

1767

- 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).

1769 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
HMI	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			+_□
DASHBOARDS	View Device Types 🔀 OT_WORKSTATION 🗙			
CONSOLES	Refresh History			
DEVICES	Name: OT_WORKSTATION		► DEVICES	(1)
View	Description: Engineering Workstation		► TAGS	(0)
Add Edit	Classification:			
Device Types	Parent Device Type: WORKSTATIONS			
View	Order: 1 (relative order withi	in parent Device Type)		
Add	Path: WORKSTATIONS:OT_WORKST			
Edit	Child Count: 0			
▶ LOGS	Custom Fields			
EVENTS				
REGULATORY				
GRAPHICAL				
USERS				
REPORTS				
> TOOLS	Set As Default Save As			Delete Cancel Sa
SECURITY				
ADMIN				
▶ HELP				
EXTERNAL TOOLS A				
None Available				

1770 Figure 2-49 ConsoleWorks Example Device Type Definition

1771

1772 Figure 2-50 ConsoleWorks List of Device Types

FAVORITES	DEVICES: Device Type	s: View				+	1
DASHBOARDS	View Device Types X						
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	
Edit	OT_FWROUTER	NETWORKING:OT_FWROUTER	ICS Firewall/Router for ICS Network Segmentation		NETWORKING	1	
Device 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	
LOGS	WORKSTATIONS	WORKSTATIONS	Computers used by users to support IT/OT Operations			1	
EVENTS	HMI	WORKSTATIONS:HMI	Specialized workstation supporting Human Machine Interface		WORKSTATIONS	1	
REGULATORY	IT_WORKSTATION	WORKSTATIONS:IT_WORKSTATI.	. Computer used by user for supporting IT operations		WORKSTATIONS	1	
	OT_WORKSTATION	WORKSTATIONS:OT_WORKSTAT.	Engineering Workstation		WORKSTATIONS	1	
GRAPHICAL							
USERS							
REPORTS	<						
TOOLS		Mass Chan	je l	Delete Add	Examples Copy	Rename	E
SECURITY							_
ADMIN							
HELP							
EXTERNAL TOOLS A							

1773 1774

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

DRAFT

1775 Figure 2-51 ConsoleWorks Example Device Definition

Console Wor	ks ® v 5.3-1u3	Administration
View Add	DEVICES: Edit * View Devices X PCS_WORKSTATION * X	+_0 X
Edit Change State	Refresh History	Logs Recordings Events
VIRTUALfx	Name: PCS_WORKSTATION 5	CONSOLES (0)
Groups G	Nickname:	► GRAPHICAL CONNECTIONS * (2)
Multi-Connect Expect-Lite Scripts	Description: PCS Engineering Workstation	▼ DEVICE TYPES (1)
Usage	Status: 3 - Available	OT_WORKSTATION Add
Connection Rules		Remove
Send Command	Disable	Remove
	System Info	
View	Custom Fields	
Add	V Custom Fields	
Edit		View
Device Types		► REMEDIATION HISTORY (0)
▼ LOGS		► BASELINE RUNS (0)
View		► TAGS (0)
Active		(v)
▶ Charts		
▶ EVENTS		
	11	
View		
Add		
Edit		
Recordings	Set As Default Save As	Delete Cancel Save
Active		

1776 1777

1778

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).

1779 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

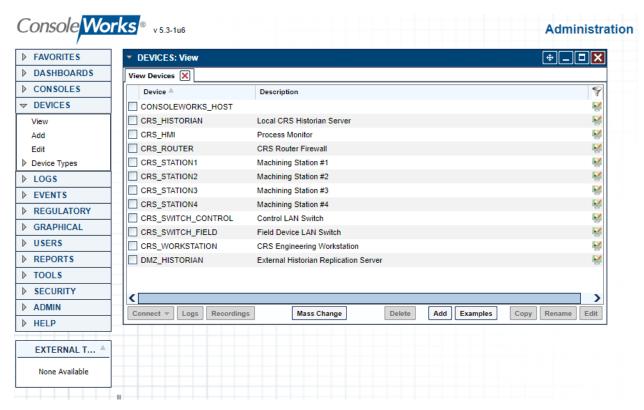
1780 Figure 2-52 ConsoleWorks List of PCS (Build 1) Devices

Console	rks [®] v 5.3-1u3 Administration	
FAVORITES	▼ DEVICES: View 🕀	
DASHBOARDS	View Devices X	
▷ CONSOLES	Device Description	9
	CONSOLEWORKS_HOST	N
View		N.
Add	PCS_HISTORIAN	N.
Edit		N.
Device Types	PCS_ROUTER	1
▶ LOGS	PCS_SWITCH_VLAN1	<u> </u>
▶ EVENTS	PCS_SWITCH_VLAN2	N.
▶ REGULATORY	PCS_WORKSTATION PCS Engineering Workstation	- Maria
▶ GRAPHICAL		
▶ USERS		
▶ REPORTS		
▶ TOOLS		
SECURITY		
▶ ADMIN		ename Edit
▶ HELP	Connect 9 Logs Recordings mass change Delete Add Lkamples Copy Re	
EXTERNAL T 🍐		
None Available		

- 1781
- 1782 1783
- 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).
- 1784 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	нмі
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

1785 Figure 2-53 ConsoleWorks List of CRS (Build 3) Devices



1786 6. Configure Graphical Connections for the PC (RDP) based devices.

1787 Figure 2-54 ConsoleWorks Example RDP Config	uration
--	---------

Console	'ori	(S [®] v 5.3-1u3	A	dministration
View	^	▼ GRAPHICAL: Edit		
Add		View Graphical Connection		
Edit		Refresh History		View Active View Recordings Connect
Change State VIRTUALfx			PCS_WORKSTATION_RDP	▼ GATEWAYS (1) △
Groups				
Multi-Connect		Description:	PCS Engineering Workstation	LOCAL_GG Add
Expect-Lite Scripts		1	PCS_WORKSTATION	Remove
Usage		Type:	RDP 👻	
Connection Rules		Host:	172.16.3.10	
Send Command		Port:	3389	
			Single Session Connection	View
View			Allow Join with Active Session	► CONSOLES (0)
Add		Status Text:		
Edit Device Types		Max Idle Time:		► TAGS (0)
V LOGS			Default Enabled	
View				
▶ Charts		Directory:	/opt/ConsoleWorks/NCCOE/graphical	
▶ EVENTS			Retain Recordings	
▶ REGULATORY		Auto-Purge:	0 0-9999 Days Old (0=disabled)	
✓ GRAPHICAL		Max Size:	0 0-99999 MB (uncompressed, 0=disabled)	
View			End Session when Max Size reached	
Add		Max Time:	0-9999 Minutes (ends Session, 0=disabled)	
Edit		Record Audio:	System Disabled 👻	
Recordings		 Authentication 		
Active		Username:	Administrator	
▶ Gateways		1		
▶ USERS	-	Password:		
▶ REPORTS		Domain:		
▼ TOOLS		Security Mode:		
CWCLIent			Disable Authentication	
Windows Event	_		Ignore Certificate Errors	
Graphical Gateway CWScripts				
 Baseline Configu 		Color Depth:		
Schedules		Display Width:	1900	
External Tools	-	Display Height:		
Mass Change				
Custom Files		DPI:		~
	~	Set As Default Save As.		Delete Cancel Save

1788 1789 1790 1791	a.	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 Table 2-21 (also shown in Figure 2-55). For each entry, the following are common settings for all graphical connections:
1792		i. Under Gateway, click Add and select LOCAL_GG.
1793		ii. Single Session Connection: Checked
1794		iii. Allow Join with Active Session: Checked
1795		iv. Under Recordings:
1796		1) Directory: /opt/ConsoleWorks/NCCOE/graphical
1797		2) Retain Records: Checked
1798		3) Auto-Purge: 0

1799	4) Max Size: 0
1800	5) End Session when Max Size Reached: Checked
1801	6) Max Time: 0
1802 v	. Authentication
1803 1804 1805	 Specify local or domain credentials, which are securely stored by ConsoleWorks, to allow complex passwords/credentials without having to share between users.
1806	2) Ignore Certificate Errors: Checked only if self-signed certificates are in use.
1807 v	i. Performance
1808	1) Display Width: 1900
1809	2) Display Height: 1200

1810 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>	v 5.3-1u3		Administra	ation	
FAVORITES	▼ GRAPHICAL: View				⊕_□
DASHBOARDS	View Graphical Connections 🔀				
CONSOLES	Graphical Connection A	Description	Туре	Status Text	Host
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
Recordings Active Gateways					
REPORTS	-				
TOOLS	<				
SECURITY	Connect View Active View Recordings	Mass Change	Delete	Add Examples	Copy Rename E
ADMIN					
HELP					
EXTERNAL T A					
None Available					

1811 Figure 2-55 ConsoleWorks List of PCS (Build 1) RDP Connections

1812 1813 1814 1815	b.	example	3 (CRS), enter the information for the graphical connections as shown in the (Figure 2-54) for each graphical connection listed in Table 2-22 (also shown in 56). For each entry, the following are common settings for all graphical connec-
1816		i.	Under Gateway, click Add and select LOCAL_GG.
1817		ii.	Under Recordings, use these settings:
1818			1) Directory /opt/ConsoleWorks/NCCOE/graphical
1819			2) Retain Records Checked
1820			3) Auto-Purge: 0
1821			4) Max Size: 0
1822			5) End Session when Max Size Reached: Checked
1823			6) Max Time: 0
1824		iii.	Authentication:
1825 1826 1827			 Specify local or domain credentials, which are securely stored by ConsoleWorks, to allow complex passwords/credentials without having to share between users.

- 1828 iv. Performance
- 1829 1) Display Width: **1900**
- 1830 2) Display Height: **1200**
- 1831 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

1833 Figure 2-56 ConsoleWorks List of CRS (Build 3) RDP Connections

onsole Works [®] v 5.3-1u6						A	dministratio	n	
FAVORITES	▼ GRAPH	HCAL: View						(_ 🗆 🔈
DASHBOARDS	View Grap	hical Connectio	ns 🗙						
CONSOLES	Graphi	ical Connection	*	Description	Туре		Status Text	Host	5
> DEVICES	CRS_H	HISTORIAN			RDP		Available	192.168.0.21	
LOGS	CRS_V	VORKSTATION			RDP		Available	192.168.0.20	
EVENTS	DMZ_H	HISTORIAN			RDP		Available	10.100.1.4	
REGULATORY									
GRAPHICAL									
View									
Add									
Edit									
Recordings									
-									
Active									
Gateways									
r Gateways View	<								
r Gateways View Add Edit	Connect	View Active	View Recordings	Mass Chang	je	Delete	Add	5 Copy Renar	
r Gateways View Add Edit		View Active	View Recordings	Mass Chan	je	Delete	Add Examples	Copy Renar	
 Gateways View Add 		View Active	View Recordings	Mass Chan	je	Delete	Add Examples	Copy Renar	ne Edit
Gateways View Add Edit VSERS REPORTS		View Active	View Recordings	Mass Chang	je	Delete	Add Examples	i Copy Renar	
Gateways View Add Edit USERS REPORTS TOOLS SECURITY		View Active	View Recordings	Mass Chan	e	Delete	Add Examples	5 Copy Renar	
Gateways View Add Edit USERS REPORTS TOOLS SECURITY ADMIN	Connect	View Active	View Recordings	Mass Chang	e	Delete	Add Examples	5 Copy Renar	
Gateways View Add Edit USERS REPORTS TOOLS SECURITY ADMIN		View Active	View Recordings	Mass Chang	e	Delete	Add Examples	5 Copy Renar	
Gateways View Add Edit USERS REPORTS TOOLS SECURITY ADMIN	Connect	View Active	View Recordings	Mass Chang	e	Delete	Add Examples	5 Copy Renar	

1834 1835

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

1836 Figure 2-57 ConsoleWorks Example Console (SSH) Connection

console <mark>Wor</mark>	ks [®] v 5.3−1u3			Administra
FAVORITES	▼ CONSOLES: Edit			+_ X
DASHBOARDS	View Consoles X PCS			
CONSOLES	Refresh History		Logs	Events Monitored Events
View				
Add	Name:	PCS_VLAN1	► GROUPS	(0)
Edit	Nickname:		► SCANS	(0)
Change State	Description:		► AUTOMATIC ACTIONS	(0)
/IRTUALfx	Status:	NORMAL Disable	► ACKNOWLEDGE ACTIONS	(0)
Groups	Device:	PCS_SWITCH =		
Aulti-Connect		SSH with Password	PURGE ACTIONS	(0)
Expect-Lite Scripts			EXPECT-LITE SCRIPTS	(0)
Jsage Connection Rules	 Connection Detail 		MULTI-CONNECT	(0)
Send Command		Priority Startup	► REMEDIATION HISTORY	(0)
DEVICES		Enable Failover		
/iew		Exclusive Connect	SCHEDULES + EVENTS	(0)
Add .	Host IP:	172.16.1.3	► TAGS	(0)
dit	Port:	(Standard: 22)	► BASELINES + SCHEDULES	(0)
Device Types	Username:	admin	► BASELINE RUNS	(0)
LOGS	Password:		GRAPHICAL CONNECTIONS	; (0)
EVENTS			► LOG TRANSFORMS	(0)
REGULATORY	Retype Password:		V LOG MANSI ONINS	
GRAPHICAL	Command:			
/iew	Min. Connect Interval:	· · ·		
dd	SSH Timeout:	(10-200 seconds)		
dit	Fingerprint:	0B:51:BF:12:DC:D1:69:09:1A:5B: C6:AB:D0:4F:F2:83:57:26:B3:13		
Recordings		Disable on Fingerprint Change		
ctive		Clear		
Bateways		Clear		
USERS	Connect			
REPORTS	Logging			
TOOLS	► Events			
SECURITY	▶ Links			
ADMIN	Special Character	ſS		
HELP	► System Info			
EXTERNAL T A	Alerts			
None Available	Custom Fields			
	Set As Default Save As			Delete Cancel Save

FAVORITES	▼ CONSOLES: Edit	⊕_□
DASHBOARDS	View Consoles X CRS_STATION1 X	
	Refresh History	Logs Events Monitored Event
View	Name: CRS_STATION1) SROUPS	(0)
Add Edit	Nickname: FCANS	(0)
Change State	Description: AUTOMATIC ACTION	NS (0)
VIRTUALfx	Status: NORMAL Disable > ACKNOWLEDGE AC	TIONS (0)
▶ Groups		
Multi-Connect		(0)
Expect-Lite Scripts	ADDITIONAL BINDS	(0)
Usage	Connection Details REMEDIATION HISTO	ORY (0)
Connection Rules	Priority Startup	NTS (0)
Send Command	Bind Name: DEFAULTWEB	
DEVICES	Host Header:	(1)
▶ LOGS	URL: http://192.168.1.101/ BASELINES + SCHE	DULES (0)
▶ EVENTS	Relative URL: /status/	(0)
▶ REGULATORY	Open F GRAPHICAL CONNE	CTIONS (0)
GRAPHICAL	Disable Standard Translations	(0)
▶ USERS		
▶ REPORTS	Log Web Traffic:	
▶ TOOLS	Profile: NCCOE_CRS	
♦ SECURITY	Traffic Processing Script:	
▶ ADMIN		
▶ HELP		
EXTERNAL T A		
None Available		
	Set As Default Save As	Delete Cancel Sav
		Delete Cancer Sav

1837 Figure 2-58 ConsoleWorks Example Console (Web Forward) Connection

183

183 184 1841 (also shown in Figure 2-59). For each entry, the following are common settings for all 1842 console connections.

1843 1844

1845

1846

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 1847

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

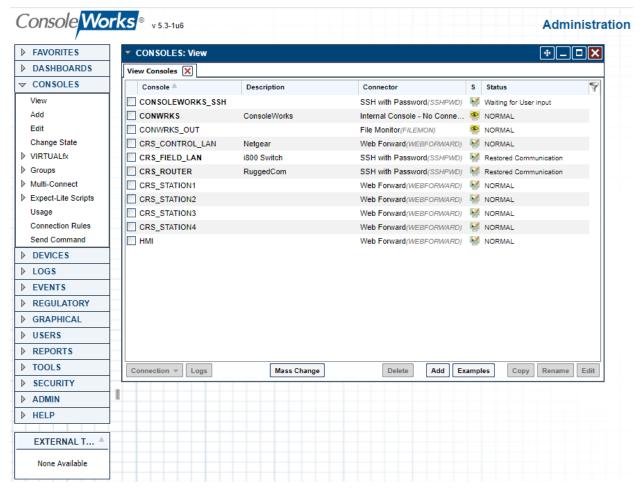
1849 Figure 2-59 ConsoleWorks List of PCS (Build 1) Console Connections

FAVORITES	CONSOLES: View			+ _	
▶ DASHBOARDS	View Consoles 🗙				
	Console A	Description	Connector	S. Status	9
View	CONSOLEWORKS_SS	зн	SSH with Password(SSHPWD)	NORMAL	
Add		ConsoleWorks	Internal Console - No Conne	. 🧟 NORMAL	
Edit	CONWRKS_OUT		File Monitor(FILEMON)	NORMAL	
Change State	PCS_ROUTER		SSH with Password(SSHPWD)	Restored Communication	
VIRTUALfx	PCS_VLAN1		SSH with Password(SSHPWD)	Restored Communication	
Groups	PCS_VLAN2		SSH with Password(SSHPWD)	Restored Communication	
Multi-Connect					
Expect-Lite Scripts					
Usage					
Connection Rules					
Send Command					
DEVICES					
▶ LOGS					
EVENTS					
REGULATORY					
GRAPHICAL					
▶ USERS					
▶ REPORTS					
▶ TOOLS					
♦ SECURITY	Connect Logs	Mass Change	Delete Add E	xamples Copy Rename	Edit
▶ HELP	✓				
**					
b.	For Build 3 (CRS), e	nter the information f	for the console conne	ections as shown in	the e
	ample (Figure 2-57	and Figure 2-58) for e	each console connect	ion listed in Table 2	2-24
		ach entry, the following			
		den entry, the following	ing are common settin		conne
	tions.				
	i. Under Conne	ection Details			
	1) Specif	y the username and p	assword. which are s	ecurely stored by (Conso
	TIJDCCII		,		
			sswords/crodontials	without boying to	charo
	Works	s, to allow complex pa en users.	sswords/credentials	without having to	share

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
HMI	CRS_HMI	Web Forward	192.168.0.98	80

1861 Figure 2-60 ConsoleWorks List of CRS (Build 3) Console Connections



- 1862 1863
- 8. Configure tags to support profiles and access controls.

FAVORITES	^	 SECURITY: Tags: View 		
DASHBOARDS		View Tags 🗙		
CONSOLES		Tag 🔺	Description	•
DEVICES		ADMIN ARCH ACCESS	Admin ARCHITECT access	
▶ LOGS		ADMIN_CONTROL_ACCESS	Admin CONTROL access	
▶ EVENTS		ADMIN_CREATE_ACCESS	Admin CREATE access	
REGULATORY		ADMIN_MODIFY_ACCESS	Admin MODIFY access	
		ADMIN_VIEW_ACCESS	Admin VIEW access	
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		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	
	H	TEST	Tag for Profile TEST	
▶ HELP		<		

1864 Figure 2-61 ConsoleWorks List of Tags for PCS (Build 1)

FAVORITES	 SECURITY: Tags: Edit 		+
DASHBOARDS	View Tags X NCCOE_CRS X		ا کا تکا گا
▶ CONSOLES	Refresh History		
▶ DEVICES	Name: NCCOE_CRS	🚎 🔻 DASHBOARDS	(1)
▶ LOGS	Description: Tag for Profile NCCOE_CRS		Add
▶ EVENTS	Custom Fields	DEMOLO	
▶ REGULATORY	Custom Fields		Remove
GRAPHICAL			
▶ USERS			
▶ REPORTS			
> TOOLS	-		View
			(1)
Access Control		DEVICE	Add
SSL Certificate			Remove
External Authenticat			
Password Rules			
View			View
Edit	-		(1)
Command Control		DEVICE	Add
Certificates		DEVICE	Add
▶ ADMIN			Remove
▶ HELP			
EXTERNAL T A			
None Available			View
	Set As Default Save As		Delete Cancel Sav
	1 (PCS) the following tags were cre of a single tag. i. Name: PCS GENERAL	eated as shown in Figure	2-61. Figure 2-62 sho
	-	sk Add and solost Doviso	c
	1) Under Dashboards , clie		5.
	2) Under Custom UI Class		
	a) DEVICE_LISTGRI	U	
	b) LISTGRID		
	3) Under Devices , click A	dd and select:	
	a) DMZ_HISTORIAN	N	
	b) PCS_HISTORIAN		
	c) PCS_HMI		

1878	i. PCS_WORKSTATION
1879	4) Under Graphical Connections, click Add and select:
1880	a) DMZ_HISTORIAN
1881	b) PCS_HISTORIAN
1882	c) PCS_HMI_RDP
1883	d) PCS_WORKSTATION_RDP
1884	ii. Name: PCS_ADMIN:
1885	1) Under Dashboards click Add and select Devices
1886	2) Under Custom UI Classes click Add and select:
1887	a) DEVICE_LISTGRID
1888	b) LISTGRID
1889	3) Under Consoles, click Add and select:
1890	a) PCS_ROUTER
1891	b) PCS_SWITCH_VLAN1
1892	c) PCS_SWITCH_VLAN2
1893	4) Under Devices, click Add and select:
1894	a) PCS_ROUTER
1895	b) PCS_SWITCH_VLAN1
1896	c) PCS_SWITCH_VLAN2
1897	b. For Build 3 (CRS) Create the following:
1898	i. Name: NCCOE_CRS
1899	1) Under Dashboards, click Add and select Devices.
1900	2) Under Custom UI Classes, click Add and select:
1901	a) DEVICE_LISTGRID
1902	b) LISTGRID
1903	3) Under Consoles, click Add and select:
1904	a) CRS_STATION1
1905	b) CRS_STATION2
1906	c) CRS_STATION3

1907		
		d) CRS_STATION4
1908		e) HMI
1909		4) Under Devices , click Add and select:
1910		a) CRS_HMI
1911		b) CRS_STATION1
1912		c) CRS_STATION2
1913		d) CRS_STATION3
1914		e) CRS_STATION4
1915		f) CRS_WORKSTATION
1916		5) Under Graphical Connections, click Add and select:
1917		a) CRS_WORKSTATION
1918		ii. Name: NCCOE_ADMIN
1919		1) Under Dashboards click Add and select Devices
1920		2) Under Custom UI Classes click Add and select:
1921		a) DEVICE_LISTGRID
1922		b) LISTGRID
1923		3) Under Consoles click Add and select:
1924		a) CRS_CONTROL_LAN
1925		b) CRS_FIELD_LAN
1926		c) CRS_ROUTER
1927		4) Under Devices click Add and select:
1928		a) CRS_SWITCH_CONTROL
1929		b) CRS_SWITCH_FIELD
1930		c) CRS_ROUTER
1931 1932	9.	Configure profiles to provide user accounts with granular access controls to available resources (Figure 2-63).

1933 Figure 2-63 ConsoleWorks Example Profile

FAVORITES	1	® v 5.3-1u6	
	-		ر الما الم
DASHBOARDS	-	VISERS: Profiles: Edit	+ _(
▶ CONSOLES	-	View Profiles X NCCOE_CRS X	
▶ DEVICES	-	Refresh History	
▶ LOGS	-	Name: NCCOE_CRS	USERS (1)
▶ EVENTS	-	Description: General Access to CRS Environmen N	CCOE_USER Add
REGULATORY	-	Custom Fields	Remove
GRAPHICAL	-		Kellove
View			
Add Edit			
Edit			View
View			TAGS (4)
Add		N	CCOE_CRS Add
Edit		Т	BA_DASHBOARD_VIEW
Change My Profile			BA_DEVICE_CONNECT
Reset Passwords		T	BA_SUBSET
Change Passwords			
Change My Password Preferences			
Sessions			View
Send Message		Set As Default Save As	Delete Cancel
▶ REPORTS	1		
▶ TOOLS			
SECURITY	1		
ADMIN			
▶ HELP			
	1		
EXTERNAL T 🔺			
None Available			
]		
a.	For E	suild 1 (PCS) the following profiles were cr	eated:
	i.	PCS_GENERAL	
		1) Under Users click Add and select	
		a) NCCOE_USER	
		2) Under Tags click Add and select	
		 2) Under Tags click Add and select a) PCS_GENERAL 	
		-	
		a) PCS_GENERAL	
		a) PCS_GENERAL b) TBA_DASHBOARD_VIEW	

1945	1) Under Users, click Add and select:
1946	a) NCCOE_ADMIN
1947	2) Under Tags, click Add and select:
1948	a) PCS_ADMIN
1949	b) TBA_DASHBOARD_VIEW
1950	c) TBA_DEVICE_CONNECT
1951	d) TBA_SUBSET
1952	e) CONSOLE_CONTROL_ACCESS
1953	f) CONSOLE_VIEW_ACCESS
1954	b. For Build 3 (CRS) create the following:
1955	i. NCCOE_CRS profile for the NCCOE_USER with access to Tags:
1956	1) Under Users, click Add and select:
1957	a) NCCOE_USER
1958	2) Under Tags click Add and select the following:
1959	a) NCCOE_CRS
1960	b) TBA_DASHBOARD_VIEW
1961	c) TBA_DEVICE_CONNECT
1962	d) TBA_SUBSET
1963	e) CONSOLE_CONTROL_ACCESS
1964	f) CONSOLE_VIEW_ACCESS
1965	ii. NCCOE_ADMIN profile for the NCCOE_USER with access to Tags:
1966	1) Under Users, click Add and select:
1967	a) NCCOE_ADMIN
1968	2) Under Tags click Add and select the following:
1969	a) NCCOE_ADMIN
1970	b) TBA_DASHBOARD_VIEW
1971	c) TBA_DEVICE_CONNECT
1972	d) TBA_SUBSET
1973	e) CONSOLE_CONTROL_ACCESS

f) CONSOLE_VIEW_ACCESS

1975 **2.9 Tenable.OT**

1976 The Tenable.OT implementation in Build 1 consists of a single appliance to meet the BAD, hardware 1977 modification, firmware modification, and software modification capabilities. Tenable.OT utilizes a 1978 combination of passive and active sensors to monitor critical networks for anomalies and active 1979 querying to retrieve information about endpoints in the PCS environment.

1980 2.9.1 Host and Network Configuration

1981 Tenable.OT is installed and configured to support the PCS environment in Build 1. The overall build 1982 architecture is described in Figure B-1, and the Tenable.OT specific components are listed in Table 2-25.

1983 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

1984 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.

1988 2.9.3 Configuration

1989 This section outlines the steps taken to configure Tenable.OT to fully integrate and support the PCS 1990 environment. These include setting NTP settings to synchronize the system time with the lab time 1991 source, configuring the scanning options for the PCS environment, and configuring network objects and 1992 policies to enhance alerting for DMZ specific remote connections.

- 1993 1. Enable connection through PCS Firewall
- 1994a. Add the following rules (Table 2-26) to the PCS Firewall to allow Tenable.OT to perform1995asset discovery and controller scanning.
- 1996 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

1997 2. Set NTP Services as follows:

```
DRAFT
```

- 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).
- 2000 c. Enter the NTP Server information: 10.100.0.15
- 2001 d. Click **Save**.

2002 Figure 2-64 Tenable.OT Local Device Setting for NTP Service

	> Assets	System Time	Set date and time manually
	> Servers		Set date and time using NTP server
	Integrations		
	System		IP1 * 10.100.0.15
	System Log		IP 2 NTP Server
	PCAP Player		
			IP 3 NTP Server
2002			Cancel Save
2003			
2004	3. Configure Sc	anning Options as follows:	
2005	a. Set A	Asset Discovery Scans:	
2006	i.	Navigate to Local Setting	s > Queries > Asset Discovery (Figure 2-65)
2007	ii.	Enable both scan options	5.
2008	iii.	Select Edit next to Asset	Discovery.
2009		1) Enter the following	g CIDR for the PCS, DMZ, and Testbed networks:
2010		a) 172.16.0.0/	22
2011		b) 10.100.0.0/	24
2012		c) 10.100.1.0/	24
2013		2) Set the scan prope	erties as follows:
2014		a) Number of A	Assets to Poll Simultaneously: 10
2015		b) Time Betwe	en Discovery Queries: 1 second
2016		c) Frequency:	Daily
2017		d) Repeats Eve	ery: 7 Days
2018		e) Repeats at:	9:00 PM

3) Click Save.

2020 Figure 2-65 Tenable.OT Asset Discovery Settings

	= tenable.ot			02:42 PM	• Thursda
	> 🌲 Events				
	Policies	Asset Discovery	IP ranges: One CIDR per line		i
	🗸 🔹 Inventory		172.16.0.0/22		
	Controllers		10.100.0.0/24 10.100.1.0/24		
	Network Assets		101100110124		
	> 🚊 Risk				
	> 🛃 Network				
	> 🏟 Groups				
	Reports		Number of Assets to Poll Simultaneously:		
	✓ o⁰ Local Settings		10 ~		
	Device		Time Between Discovery Queries:		
	User		1 second 🗸		
	Asset Custom Fields		Frequency:	1	
	API Keys		Daily		
	HTTPS		Repeats Every		
	> User Management		7 days		
	✓ Queries				
	Asset Discovery		Repeats At]	
	Controller		9:00 PM 🗸		
	Network		Cancel Save		
	> Assets				_
	> Servers	Initial Asset Enrichment	Will run SNMP, Minimal Open Port Verificat Identification, Controller Details, Controller	tion, CIP/DCP, NetBIOS, Backplane Query, Unicast State.	i
2021	Integrations				
2022	b. Set Co	ontroller Scans as follo	ows:		
2023	i.	Navigate to Local Se	ttings > Queries > Contro	ller (Figure 2-66)	
2024	ii.	Enable the following	options:		
2025		1) All Controller	Queries		
2026		2) Periodic Snaps	shots		
2027		3) Controller Dise	covery		
2028		4) Controller Sta	tus Query		
2029		5) Controller Det	ails Query		
2030		6) Backplane Qu	ery		

2031 Figure 2-66 Tenable.OT Controller Scans

				03:17 P	M • Wednesday, Dec 9,
 Policies Inventory 	All Controller Queries				0
Controllers Network Assets	Periodic Snapshots	Frequency: Every 4 days at 9:00 PM	Edi	⊛ <u>Run now</u>	1
È Risk ♣ Network	Policy Triggered Snapshots				0
Groups	Controllers Discovery	Frequency: Every 1 hour	Edi	⊛ <u>Run now</u>	٥
✓ o ^o Local Settings Device User	Controller State Query	Frequency: Every 15 Minutes	Edi	. ⊕ <u>.Run now</u>	1
User Asset Custom Fields API Keys	Diagnostic Buffer Query	Frequency: Every 4 days at 9:00 PM	Edi	. <u>Run now</u>	0
HTTPS	Controller Details Query	Frequency: Every 1 hour	Edi	. ® <u>.Run now</u>	٦
✓ Queries Asset Discovery	Backplane Query	Frequency : Every 1 hour	Edi	® <u>Run now</u>	٥
Controller Network					
> Assets	•				
> Seniers	. Set Network So	cans as follows:			
> Canvarc Version 3.8.17 Expires: Dec 9, 2021			• Queries > Network (Fi	gure 2-67)	
Cennerc Version 3.8.17 Expires: Dec 9, 2021	i. Navigate			gure 2-67)	
Senverc Version 3.8.17 Expires: Dec 9, 2021	i. Navigate ii. Enable t	e to Local Settings >		gure 2-67)	
Serverc Version 3.8.17 Expires: Dec 9, 2021	i. Navigate ii. Enable t 1) Al	e to Local Settings > he following optior Il Network Queries		gure 2-67)	
> Canvarc Version 3.8.17 Expires: Dec 9, 2021	i. Navigate ii. Enable t 1) Al 2) Di	e to Local Settings > he following optior Il Network Queries NS Query		gure 2-67)	
Serverc Version 3.8.17 Expires: Dec 9, 2021	i. Navigate ii. Enable t 1) Al 2) Di 3) Al	e to Local Settings > he following optior Il Network Queries		gure 2-67)	

2040 Figure 2-67 Tenable.OT Network Scan Settings

	■ tenable.ot Powered by Indegy					03:18 P	M • Wednesday, Dec 9, 2020	NCCOE User 🗸
	Events Policies Annentory	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		0	
	> 査 Risk > 옯 Network > 앱 Groups	SNMP Query	Frequency: SNMP V2 Community Strings: SNMP V3 Usernames:	Every 1 hour public, private	Edit	⊛ <u>Run now</u>	٢	
	 Reports v o^o Local Settings 	DNS Query					0	
	Device User	ARP Query					0	
	Asset Custom Fields API Keys	NetBIOS	Frequency: Every 1 hour		Edit		0	
	HTTPS User Management	Active Asset Tracking	Frequency: Every 5 minutes		Edit		0	
	✓ Queries Asset Discovery	WMI Query	WMI Username: WMI Frequency :	Every 1 day at 12:00 PM	<u>Edit</u> <u>Edit</u>	Run now Run Now	0	
	Controller Network	USB Connections Query	USB Frequency:	Every 1 day at 12:00 PM	Edit	<u>Run now</u>	0	
	> Assets > Cervare Version 3.8.17 Expires: Dec 9, 2021	Ripple20 Vulnerabilities Scan			Edit		0	
	4. Create	e Group Object as	follows:					
	a.	Set DMZ Group	o Object					
		i. Navigate	to Groups > Ass	et Groups				
		ii. Click Cre	ate Asset Group	to initiate the Wiz	ard process			
		1) Se	elect IP Range for	the Asset Group	Type (Figure	e 2-68) a	nd Click Nex	t.
		-		me in Name, the s in End IP (Figure 2	-			l the
)	Figure 2-68 Te	nable.OT Create	Asset Group Typ	e				

Gro	Up Type Group Defin	ition	
Asset Selection	IP Range	IP List	

	Group	×
	Group Type Group Definition	
NAME *		Î
DMZ Zone		
*		
START IP * 10.100.1.0		
END IP *		
10.100.1.254		•
∢ Back	c	ancel
5. Create	olicy to Detect External RDP Traffic:	
a.	n the left side navigation, click Policies .	
b.	Click Create Policy in the upper right corner of the steps:	page (Figure 2-70), then follow
	 For the Event Type (Figure 2-71), select as a l (Authenticated) and click Next. 	Network Events > RDP Connec
	ii. For the Policy Definition (Figure 2-72), specifNext:	y the following parameters and
	1) Policy Name: Enter "External RDP Com	imunications"
	 Source Group: Select "In" from the firs second drop-down. 	t drop-down, and "DMZ" from
	 Destination Group: Select "In" from th Asset" from the second drop-down. 	e first drop-down and select "I
	4) Schedule Group: Select "In" from the f from the second drop-down.	irst drop-down, and "In Any Ti

2050 Figure 2-69 Tenable.OT Create Asset Group Definition

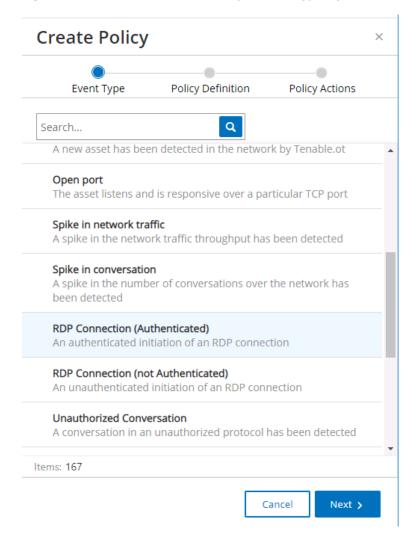
2068 Figure 2-70 Tenable.OT Policy Settings

🌲 Events								
P olicies	Policies Search	٩					Actions 🗸 🖸	Create Policy Exp
🍰 Inventory	STATUS	NAME	SEVERITY	EVENT TYPE	CATEGORY	SOURCE	DESTINATION / A	SCHEDULE
🚊 Risk	Controller Acti	ivities(105)						
A Network		SIMATIC Code Download		SIMATIC Code Do	Configuration Eve	In Any Asset	In Any Asset	In Any Time
Groups		200102 2002 2000000		Sina the code boin	comparatori crem	in any reset	invery reset	invery nine
Reports		SIMATIC Code Upload	Low	SIMATIC Code Upl	Configuration Eve	In Any Asset	In Any Asset	In Any Time
¢° Local Settings		SIMATIC Code Delete	Medium	SIMATIC Code Del	Configuration Eve	In Any Asset	In Any Asset	In Any Time
		SIMATIC Hardware Configuration Download	Medium	SIMATIC Hardwar	Configuration Eve	In Any Asset	In Any Asset	In Any Time
		SIMATIC Hardware Configuration Upload	Low	SIMATIC Hardwar	Configuration Eve	In Any Asset	In Any Asset	In Any Time
		SIMATIC Firmware Download	High	SIMATIC Firmwar	Configuration Eve	In Any Arret	In Any Asset	In Any Time

2070

2069

Figure 2-71 Tenable.OT Create Policy – Event Type Options



	0		(•
Ever	nt Type	Policy Definition		Actions
POLICY NAM	Е*			
External R	DP Commur	nications		
SOURCE GRO				
Lon.	I DMZ		~	🔶 Or
In N			·	• • •
And			· ·	• •
+ And				
And And		set	~	+ Or
And And	N*	set] -
And DESTINATION In And	N*	set] -
And DESTINATION In And SCHEDULE G	N*] -

2071 Figure 2-72 Tenable.OT Create Policy - Definition

Event Ty	ne Polic	y Definition	Policy Actions
	RDP Connect	ion (Authenti	cated)
SEVERITY *			
High	Medium	Low	None
JI SLOG			
SYSLOG			
Syslog servers are	not configured		
	not configured		
EMAIL GROUP	-		
EMAIL GROUP SMTP servers are r	not configured		
EMAIL GROUP SMTP servers are r ADDITIONAL ACTI	not configured		
EMAIL GROUP SMTP servers are r	not configured		
Syslog servers are EMAIL GROUP SMTP servers are r ADDITIONAL ACTI Disable after f	not configured		
EMAIL GROUP SMTP servers are r ADDITIONAL ACTI	not configured		

2072 Figure 2-73 Tenable.OT Create Policy - Actions

2073 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.

- 2078 2.10.1 Host and Network Configuration
- 2079 The following tables (Table 2-27, Table 2-28, and Table 2-29) detail the host and network configuration
- 2080 of the Carbon Black App Control server for PCS and CRS.

2081	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

2082 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

2083 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

2084 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>.

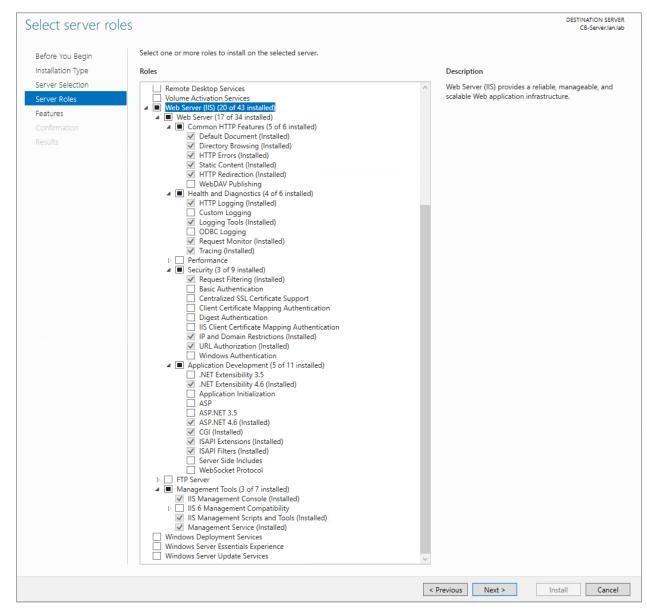
2088 1. Install Carbon Black App Control Server (fka CB_Protection) using these steps:

- a. Created 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.
- 2096 2.10.3 Configuration
- 2097 Follow these steps to configure Windows Server 2016:
- 2098 1. On the Carbon Black App Control Server, configure Windows Server 2016:
- 2099a.Based on Carbon Black documentation (Figure 2-74), Windows Server 2016 will need to2100have the following features for the Internet Information Services (IIS) role enabled for2101Carbon Black to work (Figure 2-75).

2102 Figure 2-74 Excerpt from Carbon Black Documentation on Support Server Requirements

arbon Bl	ack.							
CB Prote	ction Web	Server Platfo	orm: Supp	ort Server				
	n Requireme		onni oupp	Restrictions ®				
In the IIS configura • Commo • Stat • Defi • HTT • HTT • Applica • ASF • .NE • CGI 0 ISA • ISA • ISA • Health • HTT • Log • Req • Trac • Securit • URL • URL • URL • URL • URL • URL • ISA • ISA	Roles Manage tion: on HTTP Featu- tic Content ault Document (P Errors P Redirection tion developm P.NET (version P Extensibility PI Extensibility PI Extensions PI Filters & Diagnostics: (P Logging ging Tools (uest Monitor bing y: _ Authorization (uest Filtering ind Domain Re nance: None ement Tools: Management C	er, verify the followi ires: ent: 4.5) (version 4.5) estrictions console console coripts and Tools ice	ng	Protection AF can prevent of To configurat console an a green do can assum Otherwise, restrictions Site Binding The CB Protect address ins the list of bi IP Address If you must addresses, added to th Application CB Protect application the CB Pro credentials Authenticat You must d Authenticat	gs: otection API will not connect to localhost if a web application is bound to a specific IP stead 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 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.			
Version	Part Of O S	Current Version	Supported Architectur		Additional Notes/Requirements			
IIS 8.5	Windows 2012 Server R2 only		е x64		Common Requirements and Restrictions are listed in the table above Additional requirements: Private memory for IIS should be increased to 800 MB			
IIS 10	Windows 2016 Server		X64		Common Requirements and Restrictions are listed in the table above Additional requirements: Private memory for IIS should be increased to 800 MB			

IIS should be increased to 800 MB



2103 Figure 2-75 IIS Configuration for Carbon Black, Server Roles

- Manually update the Windows Server firewall configuration to allow inbound port 41002 traffic
 from CB App Control clients/agents.
- 2106 3. Configure Policy in the Carbon Black Console using these steps:
- 2107
- a. In the CB App Control Console, go to Rules > Policies.
- 2108b. Create a new policy with the desired enforcement level. In this case, a high enforcement2109level was chosen to actively block execution of unapproved or banned executables (Fig-2110ure 2-76).

2112

2111 Figure 2-76 Carbon Black Policy Edit

	😅 CB-Server.lan.lab Hor	ne 🕶 Reports	 Assets 	s 🕶 🛛 Rules 🕶	Tools 🔻		0
RULES O	Home » Policies » Policy Details (HighEnf	cmt_NOCOE)		200			Version 8.1.10.3
Policies							
Policies	Edit Policy HighEnform	LNCCOE					0
Mappings	Policy Name:	HighEnfcmt_NCCOE					
Notifiers	Description:	High Enforcement B		or Banned			
Software Rules							
Updaters	Mode:	Visibility Oco	ntrol ODisabled	1			
Rapid Configs	5 (Connected		Disconnected			
Publishers	Enforcement Level:	High (Block Unappr	oved) V	High (Block Unapproved) ~		
Users	Automatic Policy Assignment For New Computers:						
Directories	Set Manual Policy For Existing Computers:	There are curren	tly no computers	s in this policy.			
Files	Options:	Allow Upgrades	🗹 Track File Ch	anges			
Custom	345470447 (J) al	Load Agent in S	afe Mode 🗌 Sup	press Logo In Notifier			
Memory	Total Computers:	0					
Registry	Connected Computers:	0					
Scripts	Advanced File Rules Cust	tom Rules Memor	y Rules Regist	try Rules Publisher	Rules Rapid Config	Computers	Device Control Settings
Reputation	Name		Status	Notifiers			
Event Rules	Block writes to unapproved remo	vable devices	Active	✓ <default>: Block v</default>	vrites to unapproved remo	vable 🗸 Add E	dit
Indicator Sets	Block writes to banned removabl	e devices	Active	✓ <default>: Block v</default>	vrites to banned removable	e devi 🕶 Add E	dit
	Report reads from unapproved re	emovable devices	Report Only	▼ <none></none>		~	

2113 4. Enable AD Integration Features as follows:

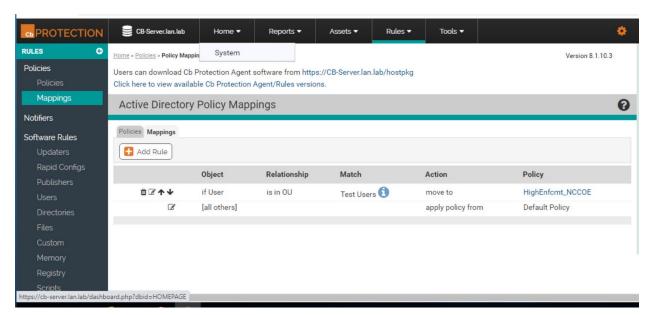
2114a.Enable AD integration features on CB App Control Console for domain user account2115login and AD-Based Policy mapping. AD-Based Policy mapping allows automatic policy2116assignment to be mapped to AD users, groups, computers, organizational units (OUs),2117etc., as configured by a CB App Control Console administrator (Figure 2-77).

2118 Figure 2-77 Carbon Black App Control System Configuration

	🥃 CB-Server.lan.lab	Home 🔻	Reports 🔻	Assets 🔻	Rules 🔻	Tools 🔻	
ADMINISTRATION G	General Events Security	Advanced Options	Mail Licensing Ext	ernal Analytics C	onnectors SAML L	ogin	
Login Accounts							
Users	General Settings						
User Roles	Server Status						
User Role	Cb Protectio	n Version: 8.1	1.10.3				
Mappings	Serve	r Address: CB	-Server.lan.lab				
System Configuration	S	erver Port: 41	002				
General	Server	Fimezone: -A	utomatic-	~			
	Database Schem	a Version: 8.1	1.10.3				
Events	Database	e Address:\S	QLEXPRESS				
Security	Database A	Auth.Type: NT	-				
Advanced Options	Data	base Size: 46	3.06 MB				
Mail	Free Local D	•	0.1 GB / 499.5 GB				
Licensing	c	L Version: 18	35				
External Analytics	Active Directory / LDAP in	tegration					
Connectors	AD-Bas	ed Logins: Er	iabled	~			
SAML Login	AD Securit	y Domain: lan	.lab				
	AD-Bas	ed Policy: Er	iabled	~			
System Health	Windows	2000 DCs: 🗌					
Update Agent/Rule Versions	Test AD Co	nnectivity: 🤇	Test Success				
	Agent Management						

- 2120 5. Add users from AD and assign policies:
- 2121a. Add "Test Users" OU from the AD to policy mapping settings and assign the "High-2122Enfcmt_NCCOE" policy (Figure 2-78).
- 2123This OU includes the "nccoeUser" and "nccoeAdmin" user accounts created for the test2124scenarios. This policy will be automatically applied to these users logged in on any com-2125puter that is running the CB Protection Agent. The "HighEnfcmt_NCCOE" policy is set to2126High Enforcement level, which will actively block all unapproved or banned files, applica-2127tions, or devices.

2128 Figure 2-78 Carbon Black App Control AD Policy Mappings



2129

2139

2130 6. Download and install CB App Control Agent from CB App Control Server

to the local host file.

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

- 2133a.Open the browser on the CRS Engineering Workstation and enter the URL to download2134the agent installer: https://CB-Server.lan.lab/hostpkg. This URL is on the Carbon Black2135server itself and is accessed on the local network. CB-Server.lan.lab is the full host name2136we gave this server during installation.2137i.If the host cannot access CB-Server.lan.lab, update the environment DNS Server2138by mapping the IP address, 10.100.0.52, to CB-Server.lan.lab or add the mapping
- 2140b. Download the Windows CB App Control Agent installer from the CB App Control Server2141and install on the CRS Engineering Workstation (Figure 2-79).

2142 Figure 2-79 Carbon Black Agent Download

Installing the Cb Protection Agent sol 1. Click the installation setup file f 2. Download the installation setup	ftware is simple: for the policy assigned to you by your netw file to a convenient location on your hard ouble-click the newly downloaded file to in	vork administrator. I-drive.			
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 U	Inapproved or Banned	Oct 27 2020 02:40:26 PM	Oct 29 2020 02:00:30 PM
1 item			Page 1/1		
			Bit9 Agent		
			Please wait while Windows configures Cb Protection Agent v8.1.8		
			Cancel		

2143

2148 2149 2150

2151 2152

- 2144c.Check the CB App Control Console to verify communication and initialization of the new2145CRS Engineering Workstation agent computer on the CB App Control Server (Figure21462-80).
- 2147 Figure 2-80 Carbon Black App Control Computers

	GB-Server.lan.lab	Home v	Reports 👻	Assets 🕶	Rules - Tools -		٠	? nccoecarbon@L	
ASSETS C	Home - Computers		-				Versio	on 8.1.10.3	
Computers									
Files File Catalog	Computers							(
Files on	Computers connected:	1 Total computer	s: 1 Current CL v	rersion: 3050 CL v	ersion for upgrade: 1328				
Computers	Saved Views:			Group By:		Days Disconnected:			
Applications	(none)	~		Add (none)	✓ Asce	nding 🗸 (none) 🗸]		
Application Catalog	Show Filters * Sho	ow Columns + Ex	port to CSV Refre	<u>sh Page</u>					
Applications on	Action - Search:			Go Clea	r				
	Computer Na	me - Connecte	d Policy Status	Upgrade Status	Connected Enforcem	Disconnected Enforcement	IP Address	Policy	
Devices		s •	Up to date	Up to date	High (Block Unappro	ved) High (Block Unapproved)	10.100.0.20	-HighEnfcmt_NCCOE-	
Device Catalog	1 item				Page 1/1			25 🗸 rows per page	
Devices on Computers									
Certificates									
	. Approve	all now t	rustod fi	ilos and n	ublichars th	at were added fro	m tha Cl	PS Engineering	
Ľ	• •			•				N3 LIIgilleelille	
	Workstation to the catalog on the CB App Control Server.								
e	e. This image (Figure 2-81) shows the Cb Protection - Files page of the CB App Control Con								
	sole.	Pc (Libur	c 2 01/3						

2153 F	Figure 2-81	Carbon	Black App	Control I	File Catalog
--------	-------------	--------	-----------	------------------	--------------

Cb Protectio	on - Files X	+							- 0
\rightarrow G	Cb-server.lan.lab/Fil	es.php?menu							Q # 8
ROTECTI	ON SCB-Server.lan.lab	Home • Reports •	Assets ▼ Rules ▼	Tools 🔻			٠	0	nccoecarbon/al.
Saved Views (none) Show Filters		Add Snapshot * Export to CSV Ref	<u> </u>	scending V	Max Age: (none) V	Show Individ	ual Files		
Action •	Showing 75 out of 38876 iter								
Select 75	First Seen Date	First Seen Name	Publisher or	Company Product N	Name	Prevalence	Trust	Threat	Global State
Q	Oct 30 2020 01:08:38 PM					0			Unapproved
OZQ	Oct 30 2020 01:04:05 PM	presentationhostdll.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	10	•	Approved
OZQ	Oct 30 2020 01:04:05 PM	penimc.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	10	۲	Approved
OZQ	Oct 30 2020 01:04:05 PM	servicemonikersupport.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	10	۲	Approved
OZQ	Oct 30 2020 01:04:05 PM	servicemonikersupport.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	9	۲	Approved
QSO	Oct 30 2020 01:04:05 PM	smconfiginstaller.exe	Microsoft Co	rporation Microsof	t® .NET Framework	1		۲	Approved
OZQ	Oct 30 2020 01:04:04 PM	system.web.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	8	۲	Approved
OZQ	Oct 30 2020 01:04:04 PM	system.web.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	1111 10	•	Approved
	Oct 30 2020 01:04:04 PM	system.web.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	8	•	Approved
Q		system.printing.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	10	0	Approved
Ogq Ogq	Oct 30 2020 01:04:04 PM						1000	-	
	Oct 30 2020 01:04:04 PM Oct 30 2020 01:04:04 PM	system.printing.dll	Microsoft Co	rporation Microsof	t® .NET Framework	1	8	0	Approved

2155 2.11 Windows Software Restriction Policy (SRP)

2156 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

2158 allow-listed. Configuring Windows SRP is done through Group Policy Object management. Windows SRP

was used for AAL in Builds 2 and 3.

2160 2.11.1 Host and Network Configuration

- 2161 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.
- 2163 Table 2-30 Windows SRP Domain Servers

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

2164

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.

2167 Build 2 supports the testing within the PCS environment. The overall build architecture is provided in

2168 Figure B-2. The Windows SRP specific components are in Table 2-31.

2169 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

2170 Build 3 supports the testing within the CRS environment. The overall build architecture is provided in

- 2171 <u>Figure B-3</u>. The Windows SRP specific components are in Table 2-32.
- 2172 Table 2-32 Windows SRP Build 3 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
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, 171 GB	CRS Supervi- sory LAN 192.168.0.21

2173 2.11.2 Installation

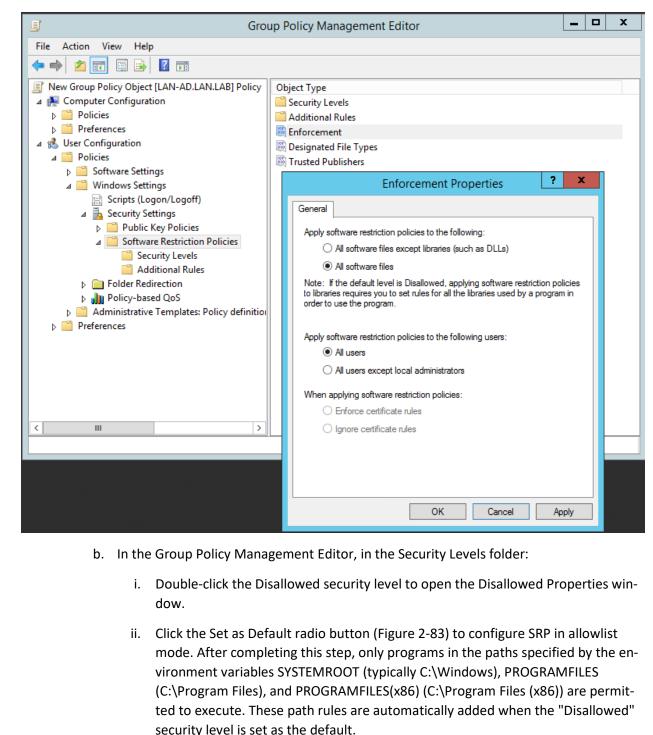
2174 Windows SRP is a feature of the Windows operating system and therefore did not require any specific 2175 installation for use in the project.

2176 2.11.3 Configuration

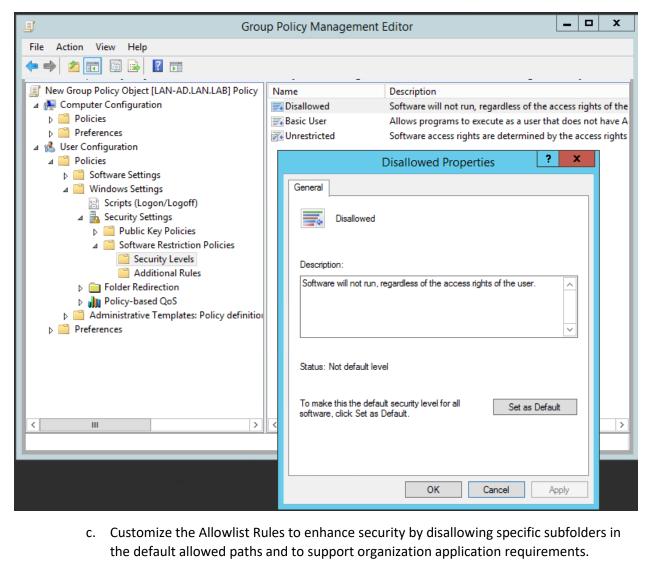
- 2177 The Windows SRP configuration required setting GPOs on the AD servers to enable the policy on all
- 2178 hosts that were part of the Windows domain. Additionally, hosts that were not part of the Windows
- 2179 Domain had GPO settings configured locally to the host. Follow these steps to configure AD with user
- 2180 accounts and set enforcement policies:

2181 2182	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.
2183 2184 2185	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 Restricted Group and include the NCCOE Admin account.
2186 2187 2188	3.	
2189 2190 2191 2192 2193 2194		Review the National Security Agency (NSA) Guidance for Application Whitelisting using Software Restriction Policies and Guidelines for Application Whitelisting ICSs available at <u>https://apps.nsa.gov/iaarchive/library/reports/application-whitelisting-using-srp.cfm</u> and <u>https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/guidelines-for-application-whitelisting-industrial-control-systems.cfm</u> respectively. Create the Windows SRP GPO with the following settings:
2195		a. From the Enforcement Properties dialog (Figure 2-82):
2196		i. Select the All Software Files radio button.
2197		ii. Select the All Users radio button.









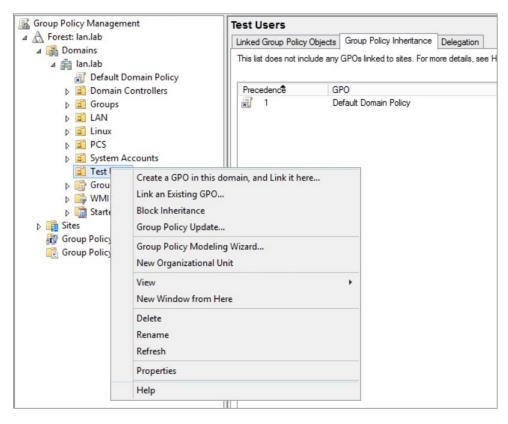
i. Click the **Additional Rules** folder and apply the rules shown in Figure 2-84. This figure combines the NSA recommended path settings in addition to lab application requirements and for disabling installers and other executable content as indicated in the comments. *Organizations should audit their environments to determine the appropriate rules to define within the policy*.

2218 Figure 2-84 Additional Rules Defined for Lab Environment

Name	Туре	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
B %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Registration	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\catroot2	Path	Disallowed	Deny execution per NSA Guidance
3%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\com\dmp	Path	Disallowed	Deny execution per NSA Guidance
SHKEY_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
SHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\spool\PRINTERS	Path	Disallowed	Deny execution per NSA Guidance
3%HKEY_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
3%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\com\dmp	Path	Disallowed	Deny execution per NSA Guidance
3%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
3 %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\tracing	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)%	Path	Unrestricted	Allow 32-bit Program Files on 64 bit systems.
SHKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Path	Unrestricted	Default Program Files Directory Allow Rule
3 %USERPROFILE%\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Path	Unrestricted	Temp rule for Workstations Allow OneDrive
SUSERPROFILE%/Forescout Console 8.2.1	Path	Unrestricted	Temporary Rule to Allow Forescout Console
ilnk	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
El\Program Files	Path	Unrestricted	Approved alternate Program Files Location
E:\Program Files (x86)	Path	Unrestricted	Approved alternate 32-bit Program Files location
nunas.exe	Path	Disallowed	Deny execution per NSA Guidance

- 2219 6. Link the GPO to the Test User OU:

- 2220
- 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).
- 2222 Figure 2-85 Menu Options for Accessing the Link an Existing GPO Option



- 2223b. In the dialog box, select the Windows SRP GPO Object from the list and click OK (Figure22242-86).
- 2225 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

2227	(Optior	al) Install GPO as the local policy on non-domain systems; for systems that are not joined		
2228	to the o	e domain, the nccoeUser and nccoeAdmin accounts are created as local user and		
2229	admini	trator accounts, respectively. Additionally, the Windows SRP GPO is manually applied to		
2230	the loca	Il system using the LGPO.exe application contained in the ZIP file from Step 3.		
2231	C.	Create a Backup of the Windows SRP GPO Object:		
2232		i. From the Group Policy Manager, select the Group Policy Objects folder and right-		
2233		click on the Windows SRP GPO object.		
2234		ii. Select the Back Up option from the pop-up menu.		
2235		iii. In the dialog box, choose a destination location such as C:\Backup GPO Folder or		
2236		some other convenient location to place the files and click Back Up .		
2237	d.	Copy the LGPO.exe along with the files created in the previous step to the non-domain		
2238		computer system.		
2239	e.	Login as an administrator on the non-domain computer and navigate to the {GUID}\Do-		
2240		mainSysvol\GPO\User folder, which should contain the registory.pol file for the GPO.		

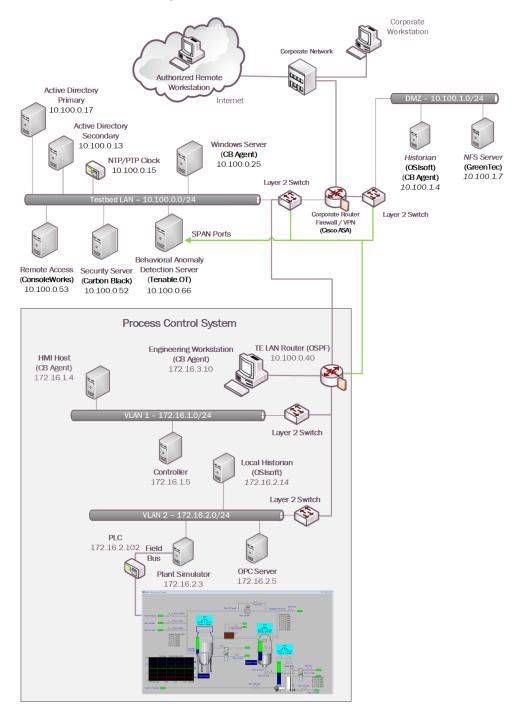
2241 2242	f.	Execute the following commands to apply the settings to the local nccoeUser and nccoeAdmin accounts:
2243		lgpo.exe /u:nccoeUser registory.pol
2244		lgpo.exe /u:nccoeAdmin registory.pol

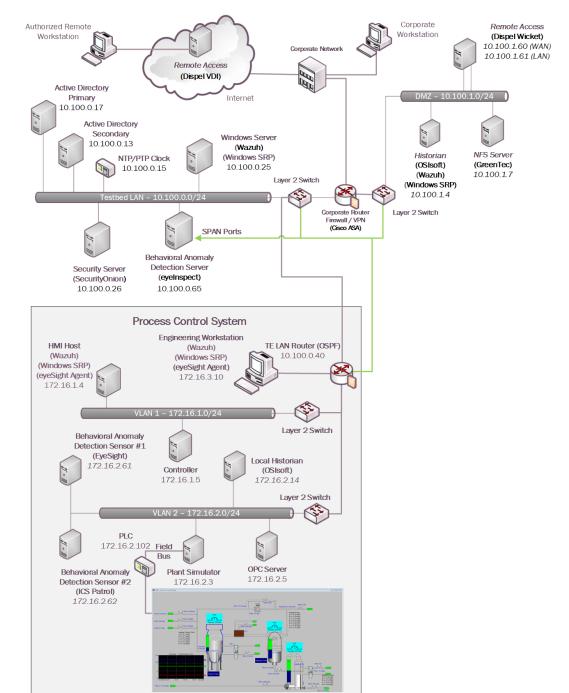
2245	Appendix A	List of Acronyms
2246	AAL	Application Allowlisting
2247	AD	Active Directory
2248	AF	Asset Framework
2249	BAD	Behavioral Anomaly Detection
2250	CRS	Collaborative Robotic System
2251	CRADA	Cooperative Research and Development Agreement
2252	CSF	NIST Cybersecurity Framework
2253	CSMS	Cybersecurity for Smart Manufacturing Systems
2254	DMZ	Demilitarized Zone
2255	DNAT	Destination Network Address Translation
2256	FOIA	Freedom of Information Act
2257	GPO	Group Policy Object
2258	HDD	Hard Disk Drive
2259	ICS	Industrial Control System
2260	IIS	Internet Information Services
2261	юТ	Internet of Things
2262	IT	Information Technology
2263	LAN	Local Area Network
2264	MFA	Multifactor Authentication
2265	MTD	Moving Target Defense
2266	NAT	Network Address Translation
2267	NCCoE	National Cybersecurity Center of Excellence
2268	NIST	National Institute of Standards and Technology
2269	NISTIR	NIST Interagency or Internal Report
2270	NSA	National Security Agency
2271	NTP	Network Time Protocol
2272	ОТ	Operational Technology

2273	OU	Organizational Unit
2274	PCS	Process Control System
2275	PI	Process Information
2276	PLC	Programmable Logic Controller
2277	RDP	Remote Desktop Protocol
2278	SP	Special Publication
2279	SPAN	Switch Port Analyzer
2280	VDI	Virtual Desktop Interface
2281	VLAN	Virtual Local Area Network
2282	VM	Virtual Machine
2283	VPN	Virtual Private Network

2284 Appendix B Build Architectures Diagrams

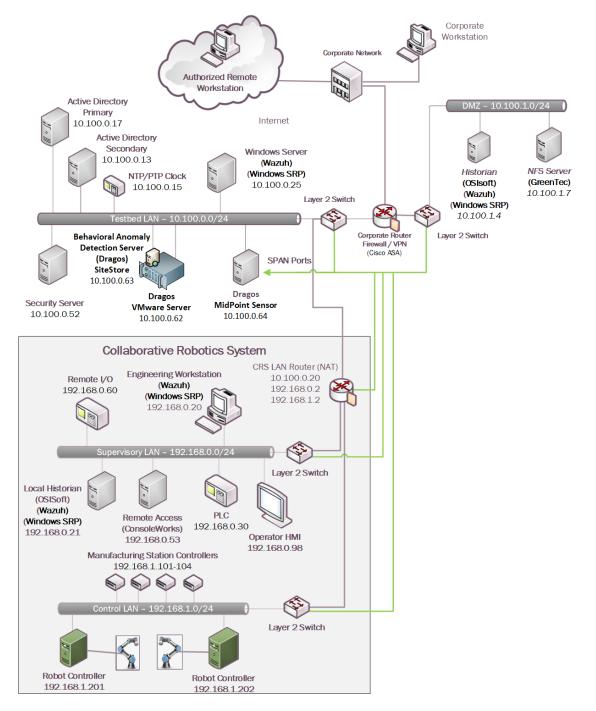
2285 Figure B-1 Build 1 Architecture Diagram

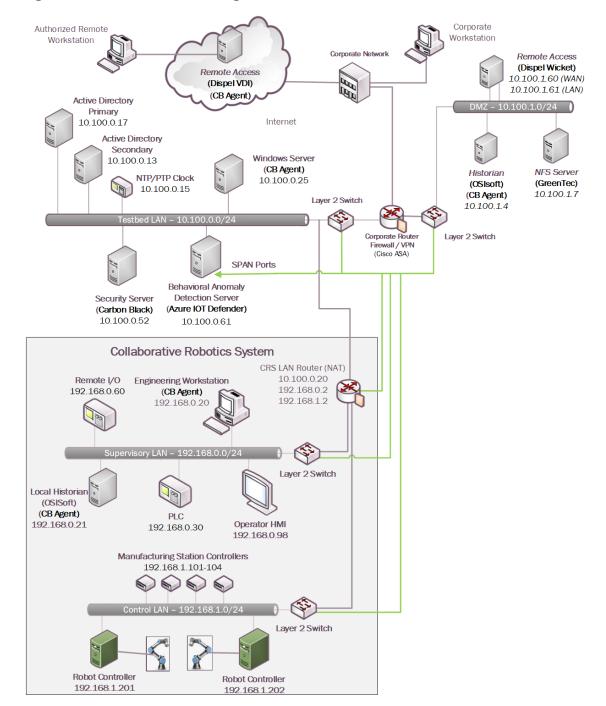




2286 Figure B-2 Build 2 Architecture Diagram

2287 Figure B-3 Build 3 Architecture Diagram





2288 Figure B-4 Build 4 Architecture Diagram