

# NIST SPECIAL PUBLICATION 1800-10

---

## Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector

---

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

**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

<https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics>

NIST SPECIAL PUBLICATION 1800-10

**Protecting Information and System Integrity in Industrial Control  
System Environments:  
Cybersecurity for the Manufacturing Sector**

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B);  
and How-To Guides (C)*

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*

DRAFT

September 2021



U.S. Department of Commerce  
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology  
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce  
for Standards and Technology & Director, National Institute of Standards and Technology*

NIST SPECIAL PUBLICATION 1800-10A

# Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector

## Volume A: Executive Summary

**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

<https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics>

# 1 Executive Summary

2 Many manufacturing organizations rely on industrial control systems (ICS) to monitor and control their  
3 machinery, production lines, and other physical processes that produce goods. To stay competitive,  
4 manufacturing organizations are increasingly connecting their operational technology (OT) systems to  
5 their information technology (IT) systems to enable and expand enterprise-wide connectivity and  
6 remote access for enhanced business processes and capabilities.

7 Although the integration of IT and OT networks is helping manufacturers boost productivity and gain  
8 efficiencies, it has also provided malicious actors, including nation states, common criminals, and insider  
9 threats, a fertile landscape where they can exploit cybersecurity vulnerabilities to compromise the  
10 integrity of ICS and ICS data to reach their end goal. The motivations behind these attacks can range  
11 from degrading manufacturing capabilities to financial gain, to causing reputational harm.

12 Once malicious actors gain access, they can harm an organization by compromising data or system  
13 integrity, hold ICS and/or OT systems ransom, damage ICS machinery, or cause physical injury to  
14 workers. The statistics bear this out. The [X-Force Threat Intelligence Index 2021 \(ibm.com\)](https://www.ibm.com) stated that  
15 manufacturing was the second-most-attacked industry in 2020, up from eighth place in 2019.

16 One particular case study illustrates the long-lasting effects and damage a single cyber attack can inflict  
17 on an organization. It was reported that a global pharmaceutical manufacturer suffered a cyber attack  
18 that caused temporary production delays at a facility making a key vaccination. More than 30,000 laptop  
19 and desktop computers, along with 7,500 servers, sat idle. Although the company claimed that its  
20 operations were back to normal within six months of the incident, at this writing, news reports stated  
21 that the organization is locked in a legal battle with its insurers and is looking to reclaim expenses that  
22 include repairing its computer networks and the costs associated with interruptions to its operations.  
23 They are seeking more than \$1.3 billion in damages.

24 To address the cybersecurity challenges facing the manufacturing sector, the National Institute of  
25 Standards and Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE) launched this  
26 project in partnership with NIST's Engineering Laboratory (EL) and cybersecurity technology providers.  
27 Together, we have built example solutions that manufacturing organizations can use to mitigate ICS  
28 integrity risks, strengthen the cybersecurity of OT systems, and protect the data that these systems  
29 process.

## 30 CHALLENGE

31 The manufacturing industry is critical to the economic well-being of our nation, and is constantly seeking  
32 ways to modernize its systems, boost productivity, and raise efficiency. To meet these goals,  
33 manufacturers are modernizing their OT systems by making them more interconnected and integrated  
34 with other IT systems and introducing automated methods to strengthen their overall OT asset  
35 management capabilities.

36 As OT and IT systems become increasingly interconnected, manufacturers have become a major target  
37 of more widespread and sophisticated cybersecurity attacks, which can disrupt these processes and

38 cause damage to equipment and/or injuries to workers. Furthermore, these incidents could significantly  
 39 impact productivity and raise operating costs, depending on the extent of a cyber attack.

**This practice guide can help your organization:**

- detect and prevent unauthorized software installation
- protect ICS networks from potentially harmful applications
- determine changes made to a network using change management tools
- detect unauthorized use of systems
- continuously monitor network traffic
- leverage malware tools

## 40 **SOLUTION**

41 The NCCoE, in conjunction with the NIST EL, collaborated with cybersecurity technology providers to  
 42 develop and implement example solutions that demonstrate how manufacturing organizations can  
 43 protect the integrity of their data from destructive malware, insider threats, and unauthorized software  
 44 within manufacturing environments that rely on ICS.

45 The example solutions use technologies and security capabilities from the project collaborators listed in  
 46 the table below. These technologies were implemented in two distinct manufacturing lab environments  
 47 that emulate discrete and continuous manufacturing systems. This project takes a modular approach in  
 48 demonstrating two unique builds in each of the lab environments.

49 The following is a list of the project's collaborators.

Collaborator	Component
 <b>DISPEL</b>	Provides secure remote access with authentication and authorization support.
 <b>DRAGOS</b>	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
 <b>ForeScout</b>	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
 <b>GreenTec™</b> www.GreenTec-USA.com	Offers secure data storage on-prem.
 <b>Microsoft</b>	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
 <b>OSIsoft.</b> is now part of AVEVA	Real-time data management software that enables detection of behavior anomalies and modifications to hardware, firmware, and software capabilities.

Collaborator	Component
	Access control platform that secures connections and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke
	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
	Provides host-based application allowlisting (the blocking of unauthorized activities that have the potential to pose a harmful attack) and file integrity monitoring.

50 While the NCCoE used a suite of commercial products to address this challenge, this guide does not  
 51 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your  
 52 organization's information security experts should identify the products that will best integrate with  
 53 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that  
 54 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
 55 implementing parts of a solution.

## 56 **HOW TO USE THIS GUIDE**

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

58 **Business decision makers, including chief information security and technology officers**, can use this  
 59 part of the guide, *NIST SP 1800-10A: Executive Summary*, to understand the drivers for the guide, the  
 60 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could  
 61 benefit your organization.

62 **Technology, security, and privacy program managers** who are concerned with how to identify,  
 63 understand, assess, and mitigate risk can use *NIST SP 1800-10B: Approach, Architecture, and Security  
 64 Characteristics*. It describes what we built and why, including the risk analysis performed and the  
 65 security/privacy control mappings.

66 **IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-10C: How-  
 67 To Guides*. It provides specific product installation, configuration, and integration instructions for  
 68 building the example implementation, allowing you to replicate all or parts of this project.

## 69 **SHARE YOUR FEEDBACK**

70 You can view or download the preliminary draft guide at <https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics>. Help the NCCoE make this guide better by sharing your thoughts with us. There will be at least 45 additional days for the comment period for this guide.

73 Once the example implementation is developed, you can adopt this solution for your own organization.  
 74 If you do, please share your experience and advice with us. We recognize that technical solutions alone  
 75 will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned  
 76 and best practices for transforming the processes associated with implementing this guide.

77 To provide comments, join the community of interest, or to learn more about the project and example  
78 implementation, contact the NCCoE at [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov).

---

79 **COLLABORATORS**

80 Collaborators participating in this project submitted their capabilities in response to an open call in the  
81 Federal Register for all sources of relevant security capabilities from academia and industry (vendors  
82 and integrators). Those respondents with relevant capabilities or product components signed a  
83 Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to  
84 build this example solution.

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

## NIST SPECIAL PUBLICATION 1800-10B

# Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector

**Volume B:**  
Approach, Architecture, and Security Characteristics

**Michael Powell**

National Cybersecurity Center of Excellence  
National Institute of Standards and Technology

**Joseph Brule\***

Cyber Security Directorate  
National Security Agency

**Michael Pease**

Keith Stouffer

CheeYee Tang

Timothy Zimmerman

Engineering Laboratory

National Institute of Standards and Technology

**Chelsea Deane**

**John Hoyt**

**Mary Raguso**

**Aslam Sherule**

**Kangmin Zheng**

The MITRE Corporation  
McLean, Virginia

**Matthew Zopf**

Strativia

Largo, Maryland

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

September 2021

DRAFT

This publication is available free of charge from

<https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics>



1    **DISCLAIMER**

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

8    While NIST and NCCoE address goals of improving the management of cybersecurity and privacy risk  
9    through outreach and application of standards and best practices, it is the stakeholder's responsibility to  
10   fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise  
11   and the impact should the threat be realized before adopting cyber security measures such as this  
12   recommendation.

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

15   National Institute of Standards and Technology Special Publication 1800-10B, Natl. Inst. Stand. Technol.  
16   Spec. Publ. 1800-10B, 170 pages, (September 2021), CODEN: NSPUE2

17   **FEEDBACK**

18   You can improve this guide by contributing feedback. As you review and adopt this solution for your  
19   own organization, we ask you and your colleagues to share your experience and advice with us.

20   Comments on this publication may be submitted to: [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov).

21   Public comment period: September 23, 2021 through November 07, 2021

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

23                              National Cybersecurity Center of Excellence  
24                              National Institute of Standards and Technology  
25                              100 Bureau Drive  
26                              Mailstop 2002  
27                              Gaithersburg, MD 20899  
28                              Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

## 29 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 45 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 55 **ABSTRACT**

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

60 The architecture and solutions presented in this guide are built upon standards-based, commercially  
61 available products, and represent some of the possible solutions. The solutions implement standard  
62 cybersecurity capabilities such as behavioral anomaly detection (BAD), application allowlisting, file  
63 integrity-checking, change control management, and user authentication and authorization. The  
64 solution was tested in two distinct lab settings: a discrete manufacturing workcell, which represents an  
65 assembly line production, and a continuous process control system, which represents chemical  
66 manufacturing industries.

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

72 The security capabilities of the example solution are mapped to the [NIST Cybersecurity Framework](#), the  
 73 [National Initiative for Cybersecurity Education Framework](#), and [NIST Special Publication 800-53](#).

## 74 KEYWORDS

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

## 78 ACKNOWLEDGEMENTS

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

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

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

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

## 84 **DOCUMENT CONVENTIONS**

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

## 92 **CALL FOR PATENT CLAIMS**

93 This public review includes a call for information on essential patent claims (claims whose use would be  
 94 required for compliance with the guidance or requirements in this Information Technology Laboratory  
 95 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication  
 96 or by reference to another publication. This call also includes disclosure, where known, of the existence  
 97 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant  
 98 unexpired U.S. or foreign patents.

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

103 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring  
104 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft  
105 publication either:

- 106     1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;  
107         or  
108     2. without compensation and under reasonable terms and conditions that are demonstrably free  
109         of any unfair discrimination

110 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its  
111 behalf) will include in any documents transferring ownership of patents subject to the assurance,  
112 provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,  
113 and that the transferee will similarly include appropriate provisions in the event of future transfers with  
114 the goal of binding each successor-in-interest.

115 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of  
116 whether such provisions are included in the relevant transfer documents.

117 Such statements should be addressed to: [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov)

## 118 **Contents**

119	<b>1 Summary.....</b>	<b>1</b>
120	1.1 Challenge .....	2
121	1.2 Solution.....	3
122	1.2.1 Relevant Standards and Guidance .....	3
123	1.3 Benefits.....	4
124	<b>2 How to Use This Guide .....</b>	<b>4</b>
125	2.1 Typographic Conventions.....	6
126	<b>3 Approach .....</b>	<b>6</b>
127	3.1 Audience.....	6
128	3.2 Scope .....	7
129	3.3 Assumptions .....	7
130	3.4 Risk Assessment .....	8
131	3.4.1 Threats .....	8
132	3.4.2 Vulnerabilities .....	9
133	3.4.3 Risk.....	10
134	3.4.4 Security Control Map .....	10
135	3.5 Technologies.....	13
136	<b>4 Architecture .....</b>	<b>14</b>
137	4.1 Manufacturing Process and Control System Description .....	15
138	4.2 Cybersecurity for Smart Manufacturing Systems Architecture .....	15
139	4.3 Process Control System .....	16
140	4.4 Collaborative Robotics System (CRS) .....	19
141	4.5 Logical Network and Security Architectures .....	21
142	4.5.1 Build 1 .....	21
143	4.5.2 Build 2 .....	25
144	4.5.3 Build 3 .....	28
145	4.5.4 Build 4 .....	30
146	<b>5 Security Characteristic Analysis.....</b>	<b>32</b>
147	5.1 Assumptions and Limitations .....	32
148	5.2 Example Solution Testing .....	32
149	5.2.1 Scenario 1: Protect Host from Malware Infection via USB .....	33

150	5.2.2	Scenario 2: Protect Host from Malware Infection via Network Vector .....	34
151	5.2.3	Scenario 3: Protect Host from Malware via Remote Access Connections .....	35
152	5.2.4	Scenario 4: Protect Host from Unauthorized Application Installation .....	36
153	5.2.5	Scenario 5: Protect from Unauthorized Addition of a Device .....	38
154	5.2.6	Scenario 6: Detect Unauthorized Device-to-Device Communications .....	39
155	5.2.7	Scenario 7: Protect from Unauthorized Deletion of Files.....	40
156	5.2.8	Scenario 8: Detect Unauthorized Modification of PLC Logic.....	41
157	5.2.9	Scenario 9: Protect from Modification of Historian Data .....	42
158	5.2.10	Scenario 10: Detect Sensor Data Manipulation.....	44
159	5.2.11	Scenario 11: Detect Unauthorized Firmware Modification.....	44
160	5.3	Scenarios and Findings .....	46
161	5.3.1	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.....	46
162	5.3.2	PR.AC-3: Remote access is managed .....	46
163	5.3.3	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.....	46
164	5.3.4	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).....	47
165	5.3.5	PR.DS-1: Data-at-rest is protected.....	47
166	5.3.6	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.....	47
167	5.3.7	PR.IP-4: Backups of information are conducted, maintained, and tested .....	47
168	5.3.8	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools .....	47
169	5.3.9	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access .....	48
170	5.3.10	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.....	48
171	5.3.11	DE.AE-2: Detected events are analyzed to understand attack targets and methods .....	48
172	5.3.12	DE.AE-3: Event data are collected and correlated from multiple sources and sensors .....	48
173	5.3.13	DE.CM-1: The network is monitored to detect potential cybersecurity events.....	49
174	5.3.14	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events .....	49
175	5.3.15	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.....	49

186	<b>6 Future Build Considerations .....</b>	<b>50</b>
187	<b>Appendix A List of Acronyms.....</b>	<b>51</b>
188	<b>Appendix B Glossary .....</b>	<b>53</b>
189	<b>Appendix C References .....</b>	<b>57</b>
190	<b>Appendix D Scenario Execution Results.....</b>	<b>59</b>
191	D.1 Executing Scenario 1: Protect Host from Malware via USB.....	59
192	D.1.1 Build 1 .....	59
193	D.1.2 Build 2 .....	61
194	D.1.3 Build 3 .....	61
195	D.1.4 Build 4 .....	62
196	D.2 Executing Scenario 2: Protect Host from Malware via Network Vector.....	63
197	D.2.1 Build 1 .....	64
198	D.2.2 Build 2 .....	67
199	D.2.3 Build 3 .....	73
200	D.2.4 Build 4 .....	77
201	D.3 Executing Scenario 3: Protect Host from Malware via Remote Access Connections.....	81
202	D.3.1 Build 1 .....	81
203	D.3.2 Build 2 .....	83
204	D.3.3 Build 3 .....	85
205	D.3.4 Build 4 .....	87
206	D.4 Executing Scenario 4: Protect Host from Unauthorized Application Installation.....	89
207	D.4.1 Build 1 .....	89
208	D.4.2 Build 2 .....	91
209	D.4.3 Build 3 .....	93
210	D.4.4 Build 4 .....	96
211	D.5 Executing Scenario 5: Protect from Unauthorized Addition of a Device.....	99
212	D.5.1 Build 1 .....	100
213	D.5.2 Build 2 .....	101
214	D.5.3 Build 3 .....	102
215	D.5.4 Build 4 .....	106
216	D.6 Executing Scenario 6: Detect Unauthorized Device-to-Device Communications.....	108
217	D.6.1 Build 1 .....	108

219	D.6.2	Build 2 .....	109
220	D.6.3	Build 3 .....	110
221	D.6.4	Build 4 .....	111
222	D.7	Executing Scenario 7: Protect from Unauthorized Deletion of Files .....	112
223	D.7.1	Build 1 .....	112
224	D.7.2	Build 2 .....	113
225	D.7.3	Build 3 .....	114
226	D.7.4	Build 4 .....	115
227	D.8	Executing Scenario 8: Detect Unauthorized Modification of PLC Logic.....	116
228	D.8.1	Build 1 .....	116
229	D.8.2	Build 2 .....	119
230	D.8.3	Build 3 .....	123
231	D.8.4	Build 4 .....	126
232	D.9	Executing Scenario 9: Protect from Modification of Historian Data.....	128
233	D.9.1	Build 1 .....	128
234	D.9.2	Build 2 .....	130
235	D.9.3	Build 3 .....	132
236	D.9.4	Build 4 .....	134
237	D.10	Executing Scenario 10: Detect Sensor Data Manipulation .....	136
238	D.10.1	All Builds.....	136
239	D.11	Executing Scenario 11: Detect Unauthorized Firmware Modification .....	137
240	D.11.1	Build 1 .....	137
241	D.11.2	Build 2 .....	138
242	D.11.3	Build 3 .....	141
243	D.11.4	Build 4 .....	142
244	<b>Appendix E Benefits of IoT Cybersecurity Capabilities .....</b>	<b>144</b>	
245	E.1	Device Capabilities Mapping .....	144
246	E.2	Device Capabilities Supporting Functional Test Scenarios.....	155

## 247 List of Figures

248	<a href="#">Figure 4-1: CSMS Network Architecture .....</a>	16
249	<a href="#">Figure 4-2: Simplified Tennessee Eastman Process Model .....</a>	17
250	<a href="#">Figure 4-3: HMI Screenshot for the PCS Showing the Main Components in the Process .....</a>	18
251	<a href="#">Figure 4-4: PCS Network.....</a>	19
252	<a href="#">Figure 4-5: The CRS Workcell .....</a>	20
253	<a href="#">Figure 4-6: CRS Network.....</a>	21
254	<a href="#">Figure 4-7: Build 1, PCS Complete Architecture with Security Components .....</a>	24
255	<a href="#">Figure 4-8: Build 2, PCS Complete Architecture with Security Components .....</a>	27
256	<a href="#">Figure 4-9: Build 3, CRS Complete Architecture with Security Components .....</a>	29
257	<a href="#">Figure 4-10: Build 4, CRS Complete Architecture with Security Components .....</a>	31
258	<a href="#">Figure D-1: An Alert from Carbon Black Showing that Malware (1.exe) was Blocked from Executing ..</a>	60
259	<a href="#">Figure D-2: Carbon Black's Server Provides Additional Details and Logs of the Event.....</a>	60
260	<a href="#">Figure D-3: Carbon Black's Server Log of the Event.....</a>	61
261	<a href="#">Figure D-4: Windows 7 Alert as a Result of Windows SRP Blocking the Execution of 1.exe.....</a>	61
262	<a href="#">Figure D-5: Windows 10 Alert as a Result of Windows SRP Blocking the Execution of 1.exe.....</a>	62
263	<a href="#">Figure D-6: Carbon Black Blocks the Execution of 1.exe for Build 4.....</a>	63
264	<a href="#">Figure D-7: Tenable.ot Dashboard Showing the Events that were Detected .....</a>	64
265	<a href="#">Figure D-8: Detected RDP Session Activity from External System to DMZ System .....</a>	65
266	<a href="#">Figure D-9: Event Detection Detail for the RDP Connection from the External System to the Historian in the DMZ .....</a>	65
268	<a href="#">Figure D-10: Tenable.ot Detected VNC Connection Between the DMZ and the Testbed LAN.....</a>	65
269	<a href="#">Figure D-11: Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in the Testbed LAN.....</a>	66
271	<a href="#">Figure D-12: Detected RDP from a DMZ system to a Testbed LAN system .....</a>	66
272	<a href="#">Figure D-13: Tenable.ot Event Detail Showing the RDP Connection Between the Historian in the DMZ to a Workstation in the Testbed LAN .....</a>	66
274	<a href="#">Figure D-14: Attempt to Execute 1.exe Failed.....</a>	67
275	<a href="#">Figure D-15: Alert Dashboard Showing Detection of an RDP Session.....</a>	68
276	<a href="#">Figure D-16: Details of the Detected RDP Session Activity from an External System to DMZ System ...</a>	69

277	<b>Figure D-17: Detection of Scanning Traffic and RDP Connection into Manufacturing Environment.....</b>	70
278	<b>Figure D-18: Details of One of the Port Scan Alerts.....</b>	71
279	<b>Figure D-19: Details of Alert for RDP Connection into Manufacturing Environment.....</b>	72
280	<b>Figure D-20: Dialog Message Showing 1.exe was Blocked from Executing .....</b>	73
281	<b>Figure D-21: Windows SRP blocked 1.exe From Executing .....</b>	74
282	<b>Figure D-22: Log of Alerts Detected by Dragos.....</b>	74
283	<b>Figure D-23: Detail of RDP Session Activity Between an External System and a DMZ System .....</b>	75
284	<b>Figure D-24: Detail for Network Scanning Alert .....</b>	76
285	<b>Figure D-25: Detail of RDP Session Activity Between a DMZ System and a Testbed LAN System .....</b>	76
286	<b>Figure D-26: Azure Defender for IoT “info” Event Identified the Remote Access Connection to the DMZ .....</b>	77
288	<b>Figure D-27: Alert for Scanning Activity.....</b>	78
289	<b>Figure D-28: Details for the Scanning Alert.....</b>	79
290	<b>Figure D-29: Detection of RDP Connection into the Manufacturing Environment .....</b>	80
291	<b>Figure D-30: Carbon Black Shows an Alert for Blocking File 1.exe.....</b>	81
292	<b>Figure D-31: Secured VPN Connection to Environment with Cisco AnyConnect .....</b>	82
293	<b>Figure D-32: Remote Access is Being Established Through ConsoleWorks .....</b>	83
294	<b>Figure D-33: Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket ESI....</b>	84
295	<b>Figure D-34: Nested RDP Session Showing Dispel Connection into the PCS Workstation.....</b>	85
296	<b>Figure D-35: VPN Connection to Manufacturing Environment.....</b>	86
297	<b>Figure D-36: Remote Access is Being Established Through ConsoleWorks .....</b>	87
298	<b>Figure D-37: Dispel VDI Showing Interface for Connecting Through Dispel Enclave to Dispel Wicket ...</b>	88
299	<b>Figure D-38: Nested RDP Session Showing Dispel Connection into the CRS Workstation.....</b>	88
300	<b>Figure D-39: Carbon Black Blocks the Execution of putty.exe and Other Files.....</b>	90
301	<b>Figure D-40: Tenable.ot alert Showing the SMB Connection Between the HMI and the GreenTec Server.....</b>	91
303	<b>Figure D-41: Tenable.ot Alert Details of the SMB Connection Between the HMI and the network file system (NFS) Server in the DMZ .....</b>	91
305	<b>Figure D-42: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration.....</b>	92
306	<b>Figure D-43: putty-64bit-0.74-installer.msi is blocked by Windows SRP .....</b>	92
307	<b>Figure D-44: Forescout Alert on the File Transfer Activity .....</b>	93
308	<b>Figure D-45: Forescout Alert Details for the File Transfer Activity .....</b>	93

309	<b>Figure D-46: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration .....</b>	94
310	<b>Figure D-47: putty-64bit-0.74-installer.msi is Blocked by Windows SRP .....</b>	94
311	<b>Figure D-48: Dragos Alert on the File Transfer Activity.....</b>	95
312	<b>Figure D-49: Dragos Alert Details of the File Transfer Alert.....</b>	96
313	<b>Figure D-50: Carbon Black Alert Showing that putty.exe is Blocked from Executing.....</b>	97
314	<b>Figure D-51: Carbon Black Alert Showing the Execution of putty-64bit-0.74-installer.msi Being Blocked .....</b>	98
316	<b>Figure D-52: Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity .....</b>	98
317	<b>Figure D-53: Azure Defender for IoT Alert Details Showing RPC Connection Between the DMZ and the Testbed LAN .....</b>	99
319	<b>Figure D-54: Azure Defender for IoT Event Alert Timeline Showing the File Transfer .....</b>	99
320	<b>Figure D-55: Tenable.ot Event Showing a New Asset has Been Discovered.....</b>	101
321	<b>Figure D-56: Tenable.ot Event Showing Unauthorized SSH Activities .....</b>	101
322	<b>Figure D-57: Forescout Alert on the DNS Request from the New Device.....</b>	102
323	<b>Figure D-58: Forescout alert showing the SSH connection .....</b>	102
324	<b>Figure D-59: Detailed Forescout alert of the Unauthorized SSH Connection .....</b>	102
325	<b>Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network Scanning.....</b>	104
327	<b>Figure D-61: Details of Network Scanning Activity.....</b>	104
328	<b>Figure D-62: Additional Details of Network Scanning Activity .....</b>	105
329	<b>Figure D-63: Alert for New Asset on the Network.....</b>	105
330	<b>Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset....</b>	106
331	<b>Figure D-65: Azure Defender for IoT Detects New Asset in the Environment .....</b>	107
332	<b>Figure D-66: Azure Defender for IoT Alert Management Options .....</b>	107
333	<b>Figure D-67: Details for Network Scanning Alert.....</b>	108
334	<b>Figure D-68: Tenable.ot Event Log Showing the Unapproved SSH Traffic.....</b>	109
335	<b>Figure D-69: Forescout Alert Showing the Unapproved SSH Traffic .....</b>	110
336	<b>Figure D-70: Dragos Alert Showing the Unapproved SSH Connection Between Devices .....</b>	111
337	<b>Figure D-71: Azure Defender for IoT Event Identified the Unauthorized SSH Connection .....</b>	112
338	<b>Figure D-72 Event Messages from Carbon Black Showing File Deletion Attempts .....</b>	113
339	<b>Figure D-73: Security Onion Wazuh Alert Showing a File Has Been Deleted.....</b>	114
340	<b>Figure D-74: Alert from Security Onion for a File Deletion .....</b>	115

341	<b>Figure D-75: Carbon Black Alerts Showing That a File Has Been Deleted .....</b>	116
342	<b>Figure D-76: Remote Access to Systems in PCS Network is Being Established Through ConsoleWorks.....</b>	117
344	<b>Figure D-77: Remote Session into Studio 5000 to Perform PLC File Operations.....</b>	117
345	<b>Figure D-78: Tenable.ot Detected the Transfer of PLC Logic File to the Rockwell PLC .....</b>	118
346	<b>Figure D-79: Tenable.ot PLC Stop alert details .....</b>	118
347	<b>Figure D-80: Tenable.ot PLC Program Download Alert Details.....</b>	119
348	<b>Figure D-81: Remote Access to Systems in PCS Network is Being Established Through Dispel .....</b>	120
349	<b>Figure D-82: Modifying the Parameters for the Allen-Bradley PLC Controller Using Studio 5000 .....</b>	121
350	<b>Figure D-83: Forescout Alerts Showing It Detected the Traffic Between the Engineering Workstation and the PLC.....</b>	122
352	<b>Figure D-84: Forescout Alert Details for the Stop Command Issued to the PLC .....</b>	122
353	<b>Figure D-85: Forescout Alert Details for the Configuration Download Command.....</b>	123
354	<b>Figure D-86: VPN Connection to the Manufacturing Environment.....</b>	124
355	<b>Figure D-87: Remote Access is Being Established through ConsoleWorks .....</b>	124
356	<b>Figure D-88: Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the Beckhoff PLC.....</b>	125
358	<b>Figure D-89: Dragos Alert Details for the PLC Logic File Download .....</b>	126
359	<b>Figure D-90: Dispel VDI with Interface for Connecting Through Dispel Enclave to Dispel Wicket .....</b>	127
360	<b>Figure D-91: Nested RDP Connections Showing Dispel Connection into the CRS Workstation .....</b>	127
361	<b>Figure D-92: Azure Defender for IoT Alert for the Unauthorized PLC Programming.....</b>	128
362	<b>Figure D-93: Tenable.ot alert Showing SMB Connection from an External Workstation to the Historian.....</b>	129
364	<b>Figure D-94: GreenTec Denies Modification and Deletion File Operations in the Protected Drive.....</b>	130
365	<b>Figure D-95: Forescout Alert Showing Network Connection from the Corporate Network to the Historian.....</b>	131
367	<b>Figure D-96: GreenTec Denies Modification and Deletion File Operations in the Protected Drive.....</b>	132
368	<b>Figure D-97: Dragos Detection of RDP Session from an External Network to the Historian.....</b>	133
369	<b>Figure D-98: GreenTec Denies Modification and Deletion File Operations in the Protected Drive.....</b>	134
370	<b>Figure D-99: Azure Defender for IoT Event Timeline Showing the Remote Access Connection to the Historian.....</b>	135
372	<b>Figure D-100: GreenTec Denies Modification and Deletion File Operations in the Protected Drive....</b>	136
373	<b>Figure D-101: PI Server's Event Frames Showing Out-of-Range Sensor Readings for the Reactor Pressure .....</b>	137

375	<b>Figure D-102: Tenable.ot Detects a Collection of Events Generated by a Firmware Change .....</b>	<b>138</b>
376	<b>Figure D-103: Details for One of the Alerts Showing the Firmware Change.....</b>	<b>138</b>
377	<b>Figure D-104: Forescout Detects a Collection of Alerts Associated with the Firmware Change .....</b>	<b>139</b>
378	<b>Figure D-105: Alert Details Detected by Forescout for the Firmware Change.....</b>	<b>140</b>
379	<b>Figure D-106: ICS Patrol Scan Results Showing a Change Configuration was Made .....</b>	<b>141</b>
380	<b>Figure D-107: Dragos Dashboard Showing an Alert for Firmware Change.....</b>	<b>142</b>
381	<b>Figure D-108: Details for Firmware Change Alert.....</b>	<b>142</b>
382	<b>Figure D-109: Azure Defender for IoT Alert Showing a Version Mismatch in the Firmware Build.....</b>	<b>143</b>

## 383 **List of Tables**

384	<b>Table 3-1: Security Control Map .....</b>	<b>11</b>
385	<b>Table 3-2: Products and Technologies.....</b>	<b>13</b>
386	<b>Table 4-1: Summary of What Products Were Used in Each Build .....</b>	<b>15</b>
387	<b>Table 4-2: Build 1 Technology Stack to Capabilities Map.....</b>	<b>22</b>
388	<b>Table 4-3: Build 2 Technology Stack to Capabilities Map.....</b>	<b>25</b>
389	<b>Table 4-4: Build 3 Technology Stack to Capabilities Map.....</b>	<b>28</b>
390	<b>Table 4-5: Build 4 Technology Stack to Capabilities Map.....</b>	<b>30</b>
391	<b>Table E-1: Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities to NIST Cybersecurity Framework Subcategories of the ICS Project.....</b>	<b>145</b>
393	<b>Table E-2 Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities that Map to Each of the Functional Test Scenarios .....</b>	<b>155</b>

## 1 Summary

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

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

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

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

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

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

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

- destructive malware
- insider threats
- unauthorized software
- unauthorized remote access
- loss of historical data
- anomalies network traffic
- unauthorized modification of systems

429 This document contains the following sections:

430 [Section 1, Summary](#), presents the challenges addressed by the NCCoE project, with a look at the  
431 solutions demonstrated to address the challenge, as well as benefits of the solutions.

432 [Section 2, How to Use This Guide](#), explains how readers—business decision makers, program managers,  
433 control system engineers, cybersecurity practitioners, and IT professionals (e.g., systems  
434 administrators)— might use each volume of this guide.

435 [Section 3, Approach](#), offers a description of the intended audience and the scope of the project. This  
436 section also describes the assumptions on which the security architecture and solution development  
437 was based, the risk assessment that informed architecture development, the NIST *Cybersecurity*  
438 *Framework* functions supported by each component of the architecture and reference design, and  
439 which industry collaborators contributed support in building, demonstrating, and documenting the  
440 solutions. This section also includes a mapping of the NIST *Cybersecurity Framework* subcategories to  
441 other industry guidance, and identifies the products used to address each subcategory.

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

446 [Section 5, Security Characteristic Analysis](#), summarizes the scenarios and findings that were employed to  
447 demonstrate the example implementations' functionality. Each of the scenarios is mapped to the  
448 relevant NIST *Cybersecurity Framework* functions and subcategories and the security capabilities of the  
449 products that were implemented. Additionally, it briefly describes how the security capabilities that  
450 were used in the solution implementation help detect cyber attacks and protect the integrity of the  
451 manufacturing systems and information.

452 [Section 6, Future Build Considerations](#), identifies additional areas that should be reviewed in future  
453 practice guides.

454 [Section Appendix D, Scenario Execution Results](#), describes, in detail, the test results of the scenarios,  
455 including screenshots from the security products captured during the tests.

## 456 **1.1 Challenge**

457 Manufacturing organizations that rely on ICS to monitor and control physical processes face risks from  
458 malicious and non-malicious insiders along with external threats in the form of increasingly  
459 sophisticated cyber attacks. A compromise to system or information integrity may very well pose a  
460 significant threat to human safety and can adversely impact an organization's operations, resulting in  
461 financial loss and harming production for years to come.

462 Manufacturing organizations may be the targets of malicious cyber actors or may be incidentally  
463 impacted by a broader malware event such as ransomware attacks. ICS components remain vulnerable  
464 to cyber attacks for numerous reasons, including adoption and integration of enhanced connectivity,  
465 remote access, the use of legacy technologies, flat network topologies, lack of network segmentation,

466 and the lack of cybersecurity technologies (e.g., anti-virus, host-based firewalls, encryption) typically  
467 found on IT systems.

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

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

## 482 **1.2 Solution**

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

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

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

- 491     ■ application allowlisting
- 492     ■ behavior anomaly detection (BAD)
- 493     ■ file integrity
- 494     ■ user authentication and authorization
- 495     ■ remote access

### 496 **1.2.1 Relevant Standards and Guidance**

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

- 499     ■ NIST Special Publication (SP) 800-167: *Guide to Application Whitelisting* [\[2\]](#)
- 500     ■ Department of Homeland Security, *Critical Manufacturing Sector Cybersecurity Framework  
501 Implementation Guidance* [\[3\]](#)

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

### 517 1.3 Benefits

518 This NCCoE practice guide can help organizations:

- 519     ▪ mitigate cybersecurity risk  
520     ▪ reduce downtime to operations  
521     ▪ provide a reliable environment that can detect cyber anomalies  
522     ▪ respond to security alerts through automated cybersecurity-event products  
523     ▪ develop and execute an OT cybersecurity strategy for which continuous OT cybersecurity monitoring is a foundational building block  
524     ▪ implement current cybersecurity standards and best practices

## 526 2 How to Use This Guide

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

531 This guide contains three volumes:

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

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

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

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

543 **Technology or security program managers** might share the *Executive Summary*, NIST SP 1800-10A, with 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.

547 **Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-10B (this document), which describes what we did and why. [Section 3.4.4](#), which maps the security characteristics of the example solutions to cybersecurity standards and best practices, will be of particular interest:

- 551     ▪ **IT and OT professionals** who want to implement an approach like this will find the whole practice guide useful, particularly the how-to portion, NIST SP 1800-10C, which provides step-by-step details to replicate all, or parts of the example solutions created in our lab. Volume C does not re-create the product manufacturers' documentation, which is generally widely available. Rather, Volume C shows how we integrated the products together to create an example solution.

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

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

569 This document provides initial guidance. We seek feedback on its contents and welcome your input. 570 Comments, suggestions, and success stories will improve subsequent versions of this guide. Please 571 contribute your thoughts to [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov).

## 572 2.1 Typographic Conventions

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

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

## 574 3 Approach

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

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

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

### 587 3.1 Audience

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

### 593 3.2 Scope

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

597 The scope of this project is to protect the integrity of information and systems, which includes:

- 598     ▪ securing the data historians
- 599     ▪ preventing the execution or installation of unapproved software
- 600     ▪ detecting anomalous behavior on the network that affects system or information integrity
- 601     ▪ detecting hardware, software, or firmware modification
- 602     ▪ enabling secure remote access
- 603     ▪ authenticating and authorizing users

604 Organizational cybersecurity policies and procedures, as well as response and recovery functions, are  
605 out of scope for this document.

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

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

### 623 3.3 Assumptions

624 This project makes the following assumptions:

- 625     ▪ Each solution is comprised of several readily available products. The modularity of the solutions  
626       might allow organizations to consider swapping one or more products, depending on their  
627       specific requirements.

- 628     ▪ A cybersecurity stakeholder might implement all or part of a solution in a manner that is  
629        compatible with their existing environment.
- 630     ▪ Organizations will test and evaluate the compatibility of the solutions with their ICS devices  
631        prior to production implementation and deployment. Response and recovery functions are  
632        beyond the scope of this guide.

### 633    **3.4 Risk Assessment**

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

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

#### 647    **3.4.1 Threats**

648    A threat is “any circumstance or event with the potential to adversely impact organizational operations”  
649    [11]. Within an IT environment, threats are typically thought of in terms of threats to confidentiality,  
650    integrity, or availability.

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

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

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

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

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

### 680     3.4.2 Vulnerabilities

681     A vulnerability as defined in [NISTIR 7298, Glossary of Key Information Security Terms \[12\]](#) is a “weakness  
682         in an information system, system security procedures, internal controls, or implementation that could  
683         be exploited by a threat source.”

684     As indicated in [Section 1](#) of this document, when IT and OT environments are integrated, each domain  
685         inherits the vulnerabilities of the other. Increasing complexity of the interfaces typically results in the  
686         vulnerability of the overall system being much greater than the sum of the vulnerabilities of the  
687         subsystems.

688     [NIST SP 800-82](#) categorizes ICS vulnerabilities into the following categories with examples [\[14\]](#):

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

699     The first step in understanding the vulnerabilities and securing an organization’s ICS infrastructure is  
700         knowledge of deployed assets and their interfaces. The knowledge of an asset’s location and baselining  
701         of its behavior enable detection of anomalous behavior, via network monitoring, that may be the result  
702         of a successfully exploited vulnerability. The ability to reliably detect changes in asset behavior and  
703         knowing an asset’s attributes are key in responding to potential cybersecurity incidents.

704 

### 3.4.3 Risk

705 The risk to an organization is the intersection of:

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

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

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

721 

### 3.4.4 Security Control Map

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

727 The subset of NIST *Cybersecurity Framework* Functions, Categories, and Subcategories that are  
728 supported by this example solution are listed below in [Table 3-1](#), along with the subset of mappings to  
729 [NIST SP 800-53 Rev. 5](#) and to the [National Initiative for Cybersecurity Education \(NICE\) Workforce  
730 Framework](#). [NIST SP 800-53 Rev 5: Security and Privacy Controls for Information Systems and  
731 Organizations](#) provides a list of controls for protecting operations, assets, and individuals. The controls  
732 detail requirements necessary to meet organizational needs. The [NICE Cybersecurity Workforce  
733 Framework](#) identifies knowledge, skills, and abilities (KSAs) needed to perform cybersecurity tasks. It is a  
734 reference guide on how to recruit and retain talent for various cybersecurity roles.

735 For more information on the security controls, the *NIST SP 800-53 Rev.5, Security and Privacy Controls  
736 for Information Systems and Organizations* is available at  
737 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

738 For more information about NICE and resources that are available to employers, education and training  
739 providers, students, and job seekers, the *NIST SP-181 Rev. 1, NICE Cybersecurity Workforce Framework*,  
740 and other NICE resources are available at [https://nist.gov/itl/applied-cybersecurity/nice/nice-  
741 framework-resource-center](https://nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center).

742 **Table 3-1: Security Control Map**

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IA-2, IA-4, IA-5, IA-7, IA-9, IA-10, IA-12	SP-DEV-001, OM-ADM-001, OV-PMA-003
		PR.AC-3: Remote access is managed	AC-17, AC-19	SP-SYS-001, OM-ADM-001, PR-INF-001
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-14, AC-24	OM-STS-001, OM-ADM-001
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	AC-14, IA-2, IA-4, IA-5	OM-STS-001, OM-ADM-001
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	MP-7, SC-28	SP-DEV-002, SP-SYS-002, OM-DTA-001
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	OM-DTA-001
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes,	PR.IP-4: Backups of information are conducted, maintained, and tested	CP-9	SP-SYS-001, SP-SYS-002, OM-DTA-001

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
	and procedures are maintained and used to manage protection of information systems and assets.			
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	MA-3	SP-SYS-001, OM-ANA-001
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	MA-4	SP-SYS-001, OM-ANA-001
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	CM-2, SI-4	SP-ARC-001, PR-CDA-001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	CA-7, SI-4 RA-5	OM-DTA-002, PR-CDA-001, CO-OPS-001
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	CA-7, SI-4	OM-DTA-002, PR-CDA-001, PR-CIR-001, CO-OPS-001
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	AU-12, CA-7, CM-3, SC-7, SI-4	OM-NET-001, PR-CDA-001, PR-CIR-001
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AU-12, CA-7, CM-11	PR-CDA-001, AN-TWA-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, SI-4	PR-CDA-001, PR-CIR-001, AN-TWA-001, CO-OPS-001

### 743 3.5 Technologies

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

747 **Table 3-2: Products and Technologies**

Capability	Product	Function	NIST <i>Cybersecurity Framework</i> Subcategories Mapping
<b>Application Allowlisting (AAL)</b>	VMWare Carbon Black	Allow approved ICS applications to execute.	DE.AE-2, DE.AE-3, DE.CM-3, DE.CM-7
	Windows Software Restriction Policies (SRP) (Note: This component was not provided by collaborator. It is a feature of the Windows operating system product.)		
<b>File Integrity Checking</b>	GreenTec WORMdisk and ForceField	Provides immutable storage for data, system, and configuration files.	PR.DS-1, PR.IP-4, PR.MA-1
	VMWare Carbon Black	Provides integrity checks for files and software.	PR.DS-6, PR.MA-1, DE.AE-2, DE.CM-3
<b>BAD, Hardware/Software/Firmware Modification Detection</b>	Wazuh Security Onion (Note: This component was not provided by collaborator. It is an open source product.)		
	Microsoft Azure Defender for IoT	Passively scans the OT network to create a baseline of devices and network traffic.  Alerts when activity deviates from the baseline.	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
	Dragos Platform		
	Forescout eyeInspect (formerly SilentDefense)		
	Tenable Tenable.ot		

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

## 748 4 Architecture

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

754 Typically, manufacturing organizations have unique cyber-ecosystems and specific needs for their  
 755 operation. To demonstrate the modularity and interoperability of the provided solutions, this project  
 756 used available CRADA partner technologies to assemble four “builds” deployed across both the PCS and  
 757 CRS. Additionally, to increase the diversity of technologies between builds, two of the builds also utilized  
 758 open source solutions (Security Onion Wazuh), native operating system features (Windows Software  
 759 Restriction Policies [SRP]), and a Cisco Adaptive Security Appliance (ASA) device configured with the  
 760 AnyConnect VPN client.

761 This modular approach, focusing on specific products and outcomes, demonstrates how solutions might  
 762 be tailored to the operating environment. [Table 4-1](#) provides a summary of the four builds and how the

763 products were distributed across them. Detailed descriptions of the installation, configuration, and  
 764 integration of these builds are included in Volume C of this guide.

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

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

766 [Sections 4.1, 4.2, 4.3, and 4.4](#), present descriptions of the manufacturing processes and control systems  
 767 of the testbed that are used for demonstrating the security capabilities required for protecting  
 768 information and system integrity in ICS environments. [Section 4.5](#) describes the network and security  
 769 architectures that are used to implement the above security capabilities.

## 770 **4.1 Manufacturing Process and Control System Description**

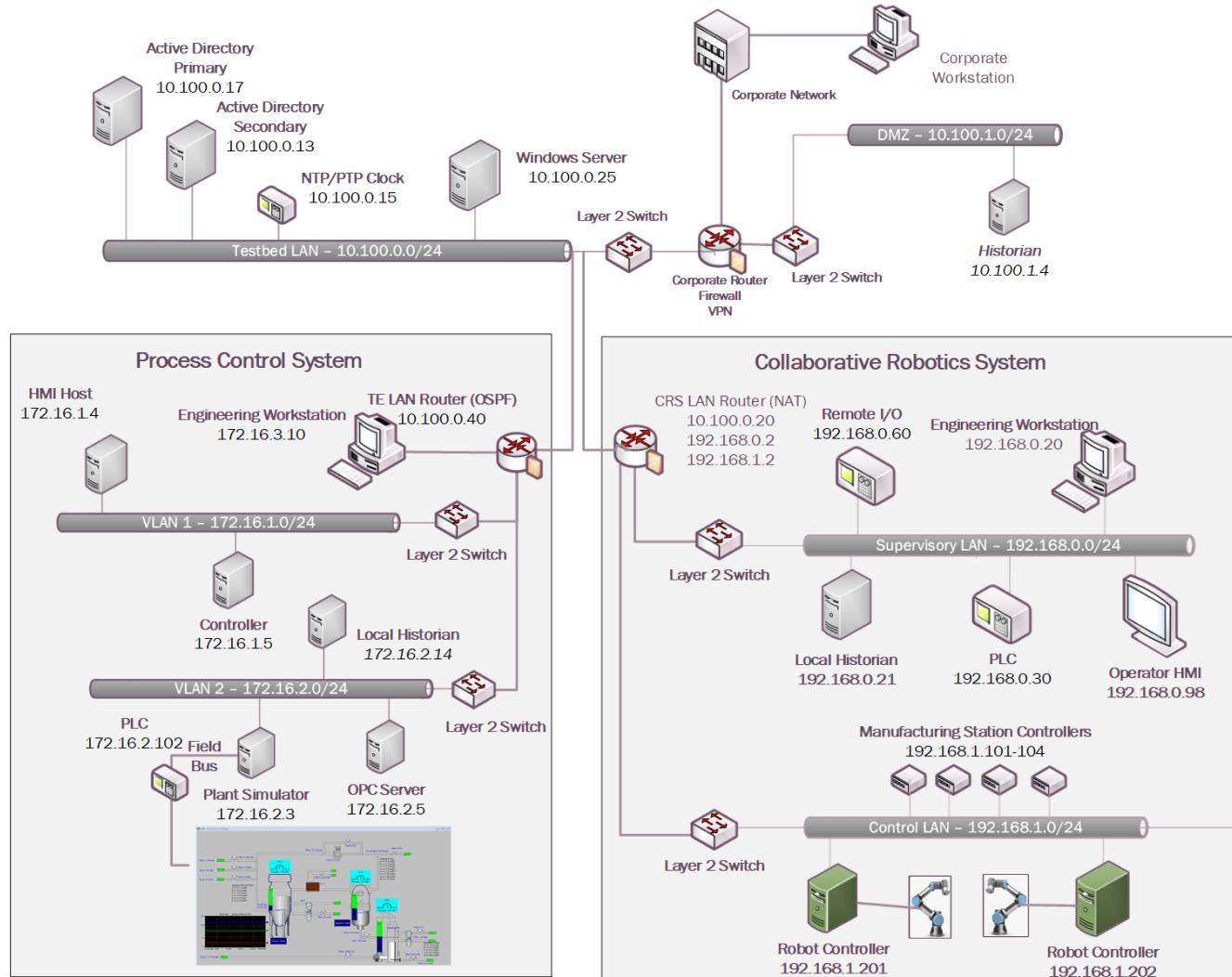
771 The CSMS demonstration environment emulates real-world manufacturing processes and their ICS by  
 772 using software simulators and commercial off-the-shelf (COTS) hardware in a laboratory environment  
 773 [\[8\]](#). The CSMS environment was designed to measure the performance impact on ICS that is induced by  
 774 cybersecurity technologies. For this effort, the CSMS and the integrated PCS and CRS are used to  
 775 demonstrate the information and system integrity capabilities and are described in [Sections 4.3](#) and [4.4](#).

## 776 **4.2 Cybersecurity for Smart Manufacturing Systems Architecture**

777 [Figure 4-1](#) depicts a high-level architecture for the demonstration environment consisting of a testbed  
 778 local area network (LAN), a demilitarized zone (DMZ), the PCS, and the CRS. The environment utilizes a  
 779 combination of physical and virtual systems and maintains a local network time protocol (NTP) server  
 780 for time synchronization. Additionally, the environment utilizes virtualized Active Directory (AD) servers  
 781 for domain services. The tools used to support information and system integrity are deployed and

782 integrated in the DMZ, Testbed LAN, PCS, and CRS according to vendor recommendations and standard  
 783 practices as described in the detailed sections for each build.

784 **Figure 4-1: CSMS Network Architecture**



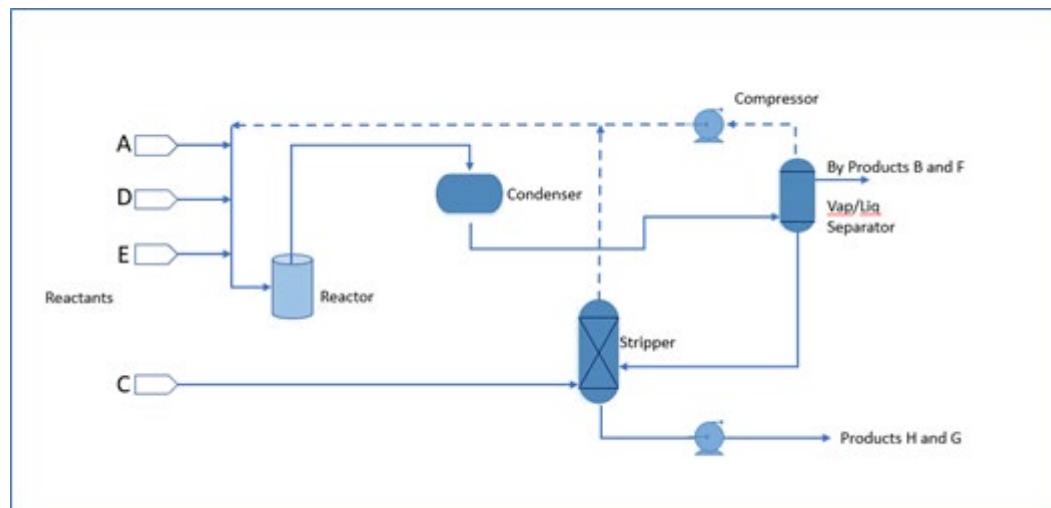
### 785 **4.3 Process Control System**

786 A continuous manufacturing process is a type of manufacturing process that produces or processes  
 787 materials continuously and in which the materials are continuously moving, going through chemical  
 788 reactions, or undergoing mechanical or thermal treatment. Continuous manufacturing usually implies a  
 789 24-hours a day, seven days a week (24/7) operation with infrequent maintenance shutdowns. Examples  
 790 of continuous manufacturing systems are chemical production, oil refining, natural gas processing, and  
 791 wastewater treatment.

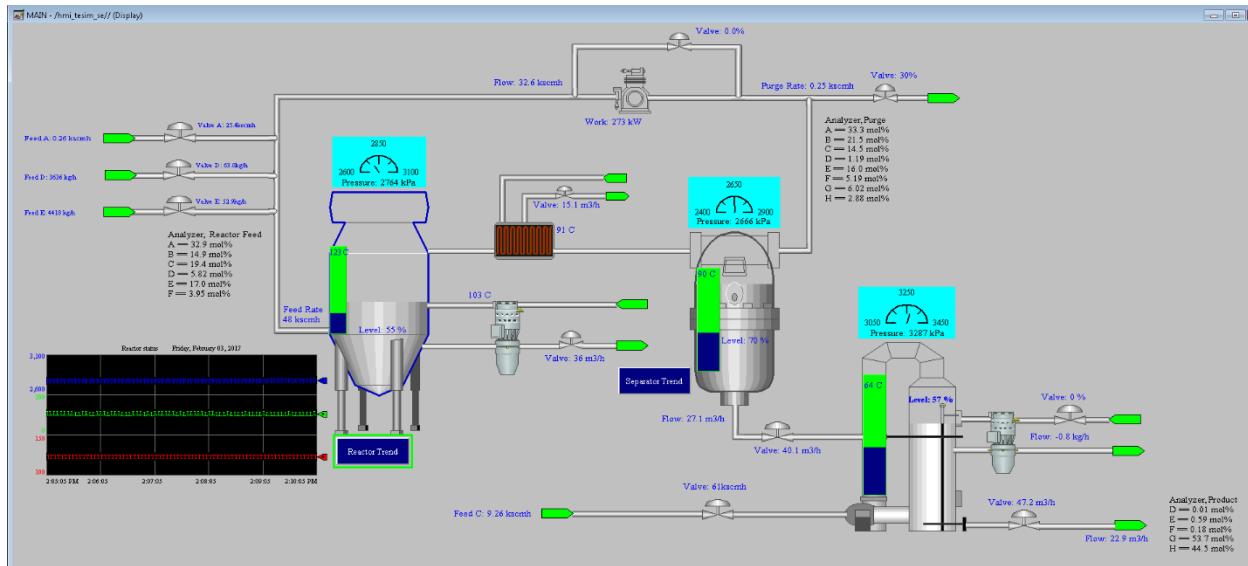
792 The PCS emulates the Tennessee-Eastman (TE) chemical reaction process. The TE problem, presented by  
 793 Downs and Vogel [15], is a well-known process-control problem in continuous chemical manufacturing.  
 794 A control loop is required in the PCS to maintain a steady and stable chemical production. The PCS  
 795 presents a real-world scenario in which a cybersecurity attack could represent a real risk to human  
 796 safety, environmental safety, and economic viability. This allows the PCS to be used to assess the impact  
 797 of cybersecurity attacks on the continuous process manufacturing environment.

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

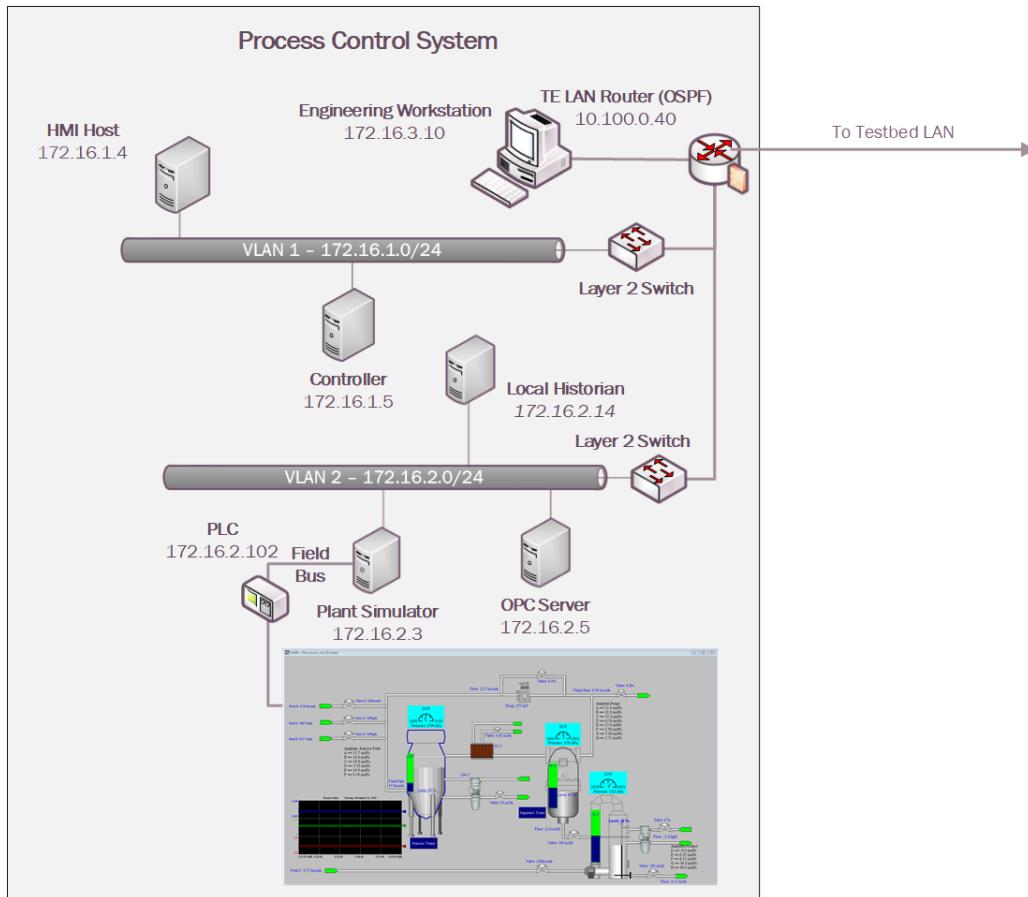
810 **Figure 4-2: Simplified Tennessee Eastman Process Model**



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



- 812 The PCS network architecture is shown in [Figure 4-4](#). The PCS network is connected to the Testbed LAN via a boundary router. The boundary router is an Allen-Bradley Stratix 8300. All network traffic is going through the boundary router to access the Testbed LAN and the DMZ. The PCS environment is segmented into three local networks, namely the engineering LAN, Operations LAN (VLAN1), and the Supervisory LAN (VLAN2). Each of these local networks is connected using an industrial network switch, an Allen-Bradley Stratix 5700. The engineering workstation is hosted in the engineering LAN. The HMI and the Plant Controller are hosted in the operations LAN. The Plant Simulator is hosted in the supervisory LAN along with the Local Historian, OPC Server, and the Supervisory PLC.
- 820 The Operations LAN (VLAN1) simulates a central control room environment. The supervisory LAN (VLAN2) simulates the process operation/ manufacturing environment, which typically consists of the operating plant, PLCs, OPC server, and data historian.
- 823 An OPC DA server is the main data gateway for the PLC and the simulated controller. The PLC reads in the manufacturing process sensor data from the Plant Simulator using the DeviceNet connection and communicates the data to the OPC DA server. The PLC also retrieves actuator information from the controller through the OPC DA and transmits to the Plant Simulator. The controller uses a MATLAB Simulink interface to communicate with the OPC DA server directly.

828 **Figure 4-4: PCS Network**829 **4.4 Collaborative Robotics System (CRS)**

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

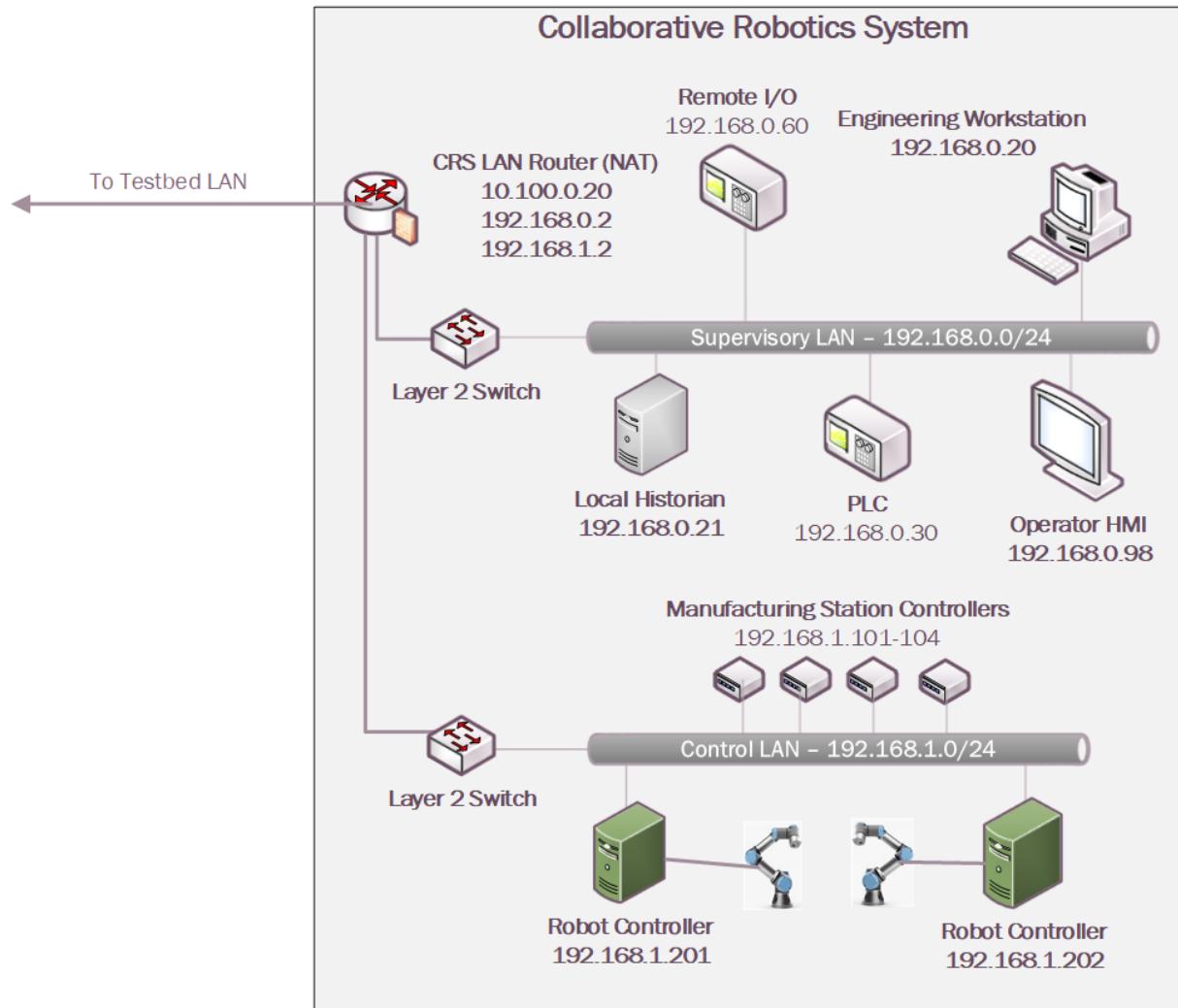
835 Parts are transported by two Universal Robots UR3e robotic arms through four simulated machining  
 836 stations. Each station communicates with the Supervisory PLC (a Beckhoff CX9020) over the workcell  
 837 network, which monitors and controls all aspects of the manufacturing process. An HMI (Red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

839 Figure 4-5: The CRS Workcell



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

847 Figure 4-6: CRS Network

848 

## 4.5 Logical Network and Security Architectures

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

852 

### 4.5.1 Build 1

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

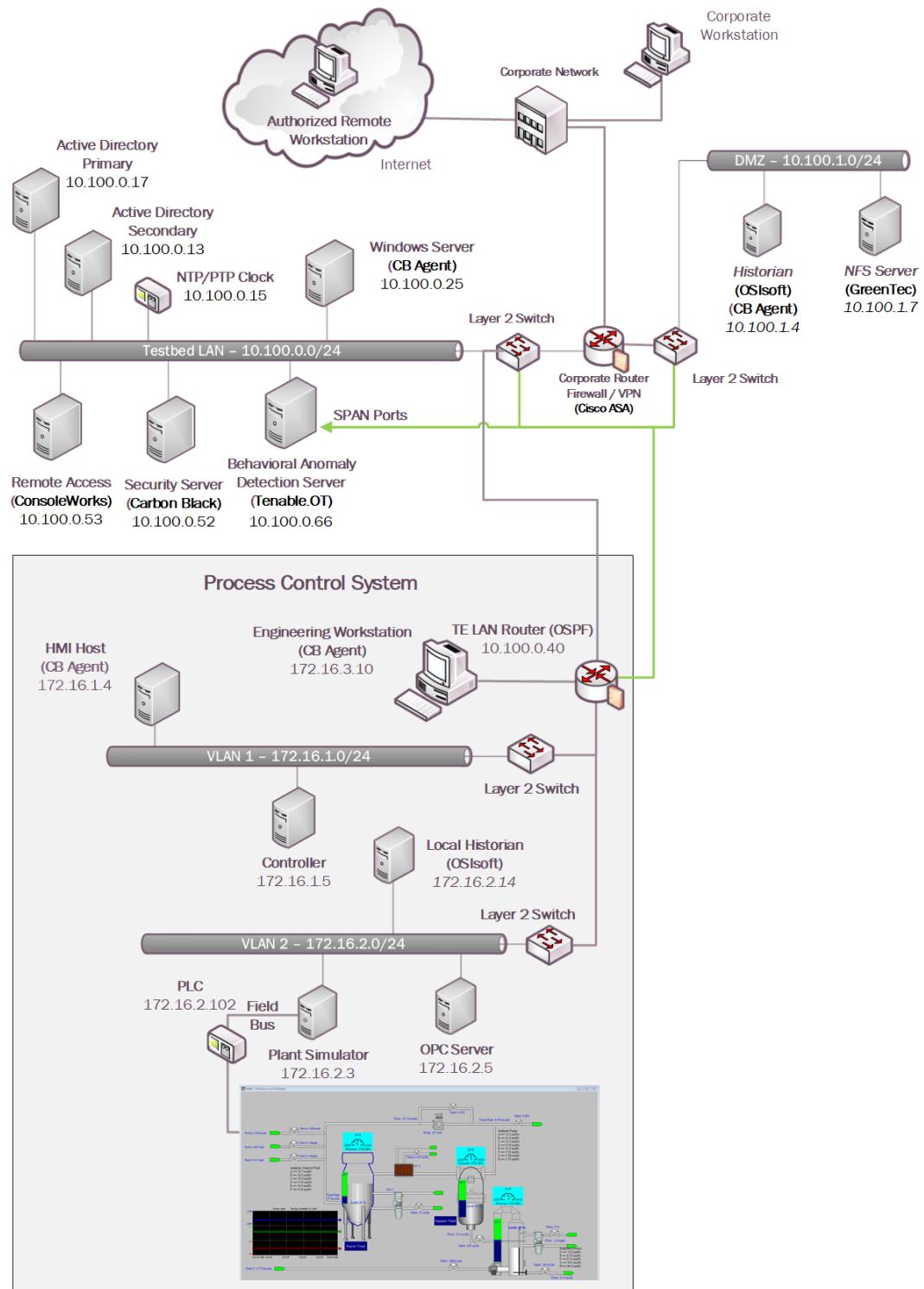
855 Table 4-2: Build 1 Technology Stack to Capabilities Map

Capability	Products	Description
<b>Application Allowlisting</b>	Carbon Black	Carbon Black Server is deployed within the Testbed LAN with the Carbon Black Agents installed on key workstations and servers in the Testbed LAN, PCS environment, and DMZ to control application execution.
<b>Behavior Anomaly Detection, Hardware/Software/Firmware Modification Detection</b>	PI Server	Deployed in the DMZ and PCS environments, the PI Server provides the historian repository for process data through its Data Archive and generates Event Frames upon detection of abnormal manufacturing system behavior.
	Tenable.ot	Passively monitors the PCS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports, and is also configured to capture detailed asset information for supporting inventory, change via both passive and active scanning.
<b>File Integrity Checking</b>	Carbon Black	Deployed within the Testbed LAN environment with the Carbon Black Agents installed on key workstations and servers to monitor the integrity of local files.
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ environment and configured with both a ForceField and WORM drive to provide a protected archive for the historian data and the approved versions of configuration, source (PLC Programs), and executable files for the ICS environment.
<b>User Authentication and Authorization</b>	ConsoleWorks	Deployed to centralize the access and management of the systems and credentials. ConsoleWorks is deployed to the Testbed LAN to allow connections to the PCS environment.

Capability	Products	Description
Remote Access	AnyConnect	Supports authenticated VPN connections to the environment with limited access to only the TDI ConsoleWorks web interface.

The technology was integrated into the lab environment as shown in [Figure 4-7](#).

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



857 **4.5.2 Build 2**

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

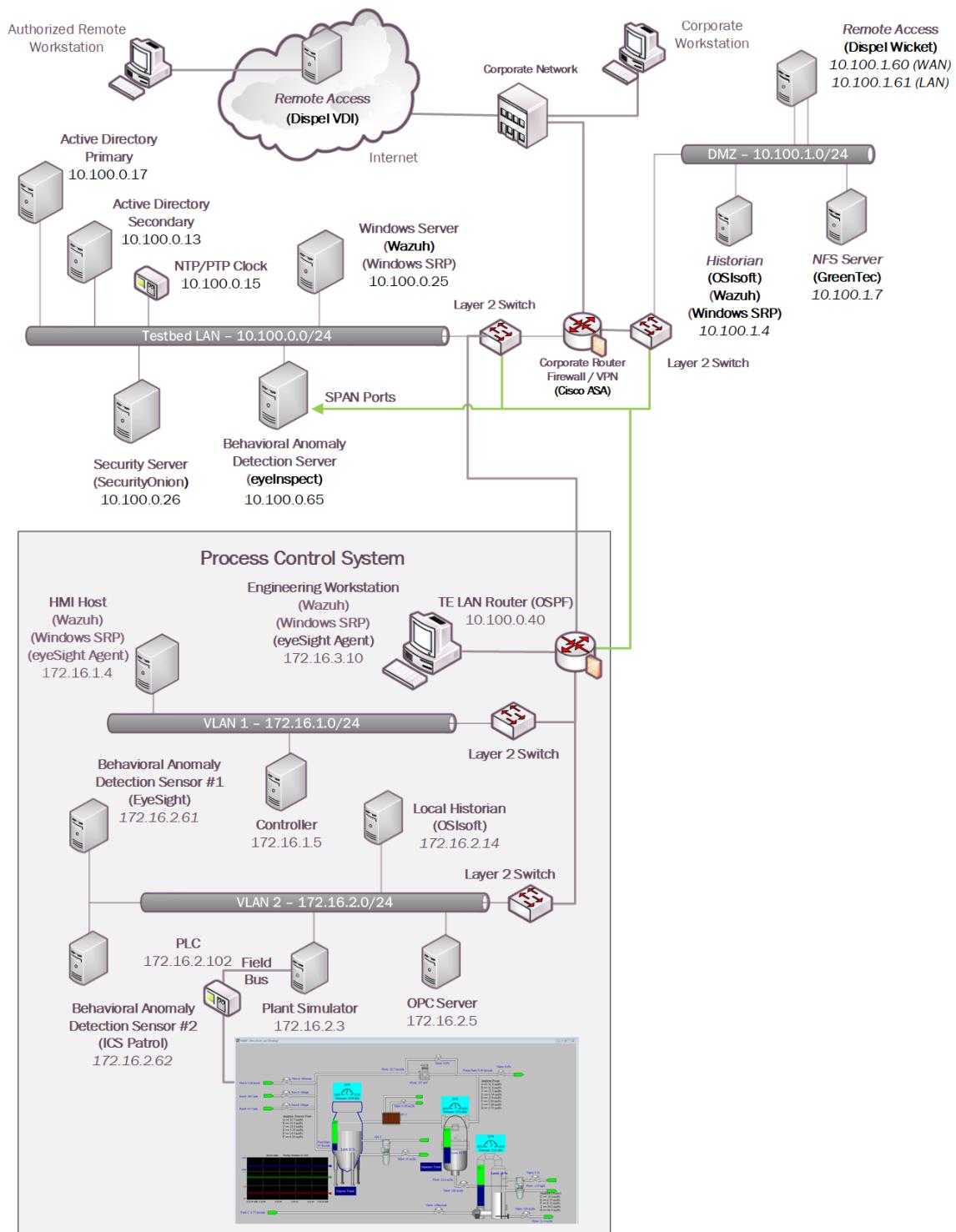
860 **Table 4-3: Build 2 Technology Stack to Capabilities Map**

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

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

- 861 The technology was integrated into the lab environment as shown in [Figure 4-8](#).

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



863 **4.5.3 Build 3**

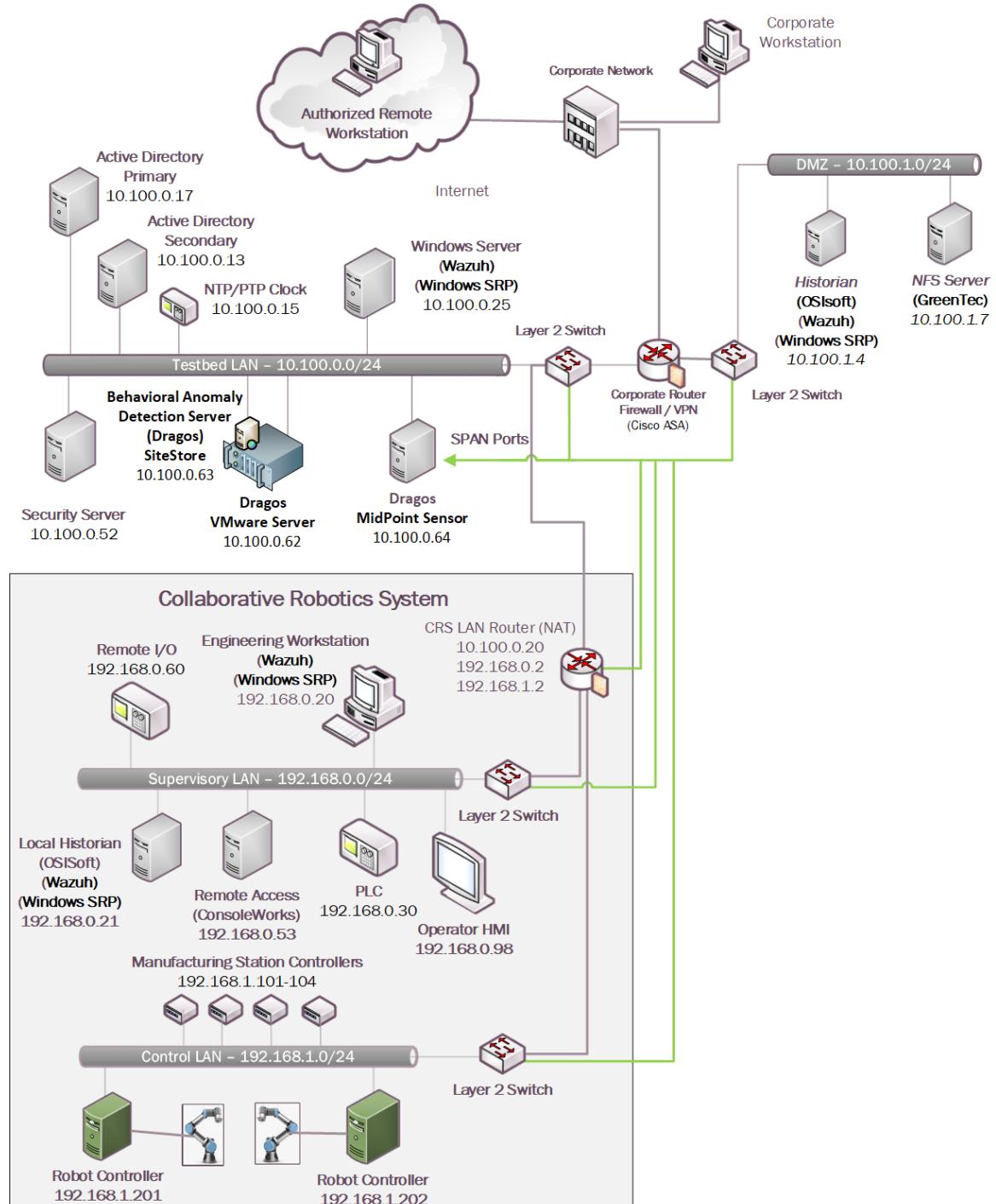
864 The technologies in Table 4-4 were integrated into the CRS for Build 3 to enhance system and data  
 865 integrity capabilities.

866 **Table 4-4: Build 3 Technology Stack to Capabilities Map**

Capability	Products	Description
<b>Application Allowlisting</b>	Windows SRP	AD Group Policy Objects (GPOs) are used to configure and administer the Windows Software Restriction Policy (SRP) capabilities within the Testbed LAN environment and CRS environments.
<b>Behavior Anomaly Detection, Hardware/Software/Firmware Modification Detection</b>	PI Server	Deployed in the DMZ and CRS environments, the PI Server provides the historian repository for process data through its Data Archive and generates Event Frames upon detection of abnormal manufacturing system behavior
	Dragos	Passively monitors the CRS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports and receives Event Frames from the DMZ PI system through the PI Web API interface.
<b>File Integrity Checking</b>	Wazuh	The Security Onion server is used to manage and monitor the integrity of local files using the Wazuh agents deployed on the DMZ, Testbed LAN, and CRS.
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ environment and configured with both a ForceField and WORM drive to provide a protected archive for the historian data and the approved versions of configuration and coding files for the ICS environment.
<b>User Authentication and Authorization</b>	ConsoleWorks	Deployed to centralize the access and management of the systems and credentials. ConsoleWorks is deployed to allow connections within the CRS environment.
<b>Remote Access</b>	AnyConnect	Supports authenticated VPN connections to the environment with limited access to only the TDI ConsoleWorks web interface.

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

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



869 **4.5.4 Build 4**

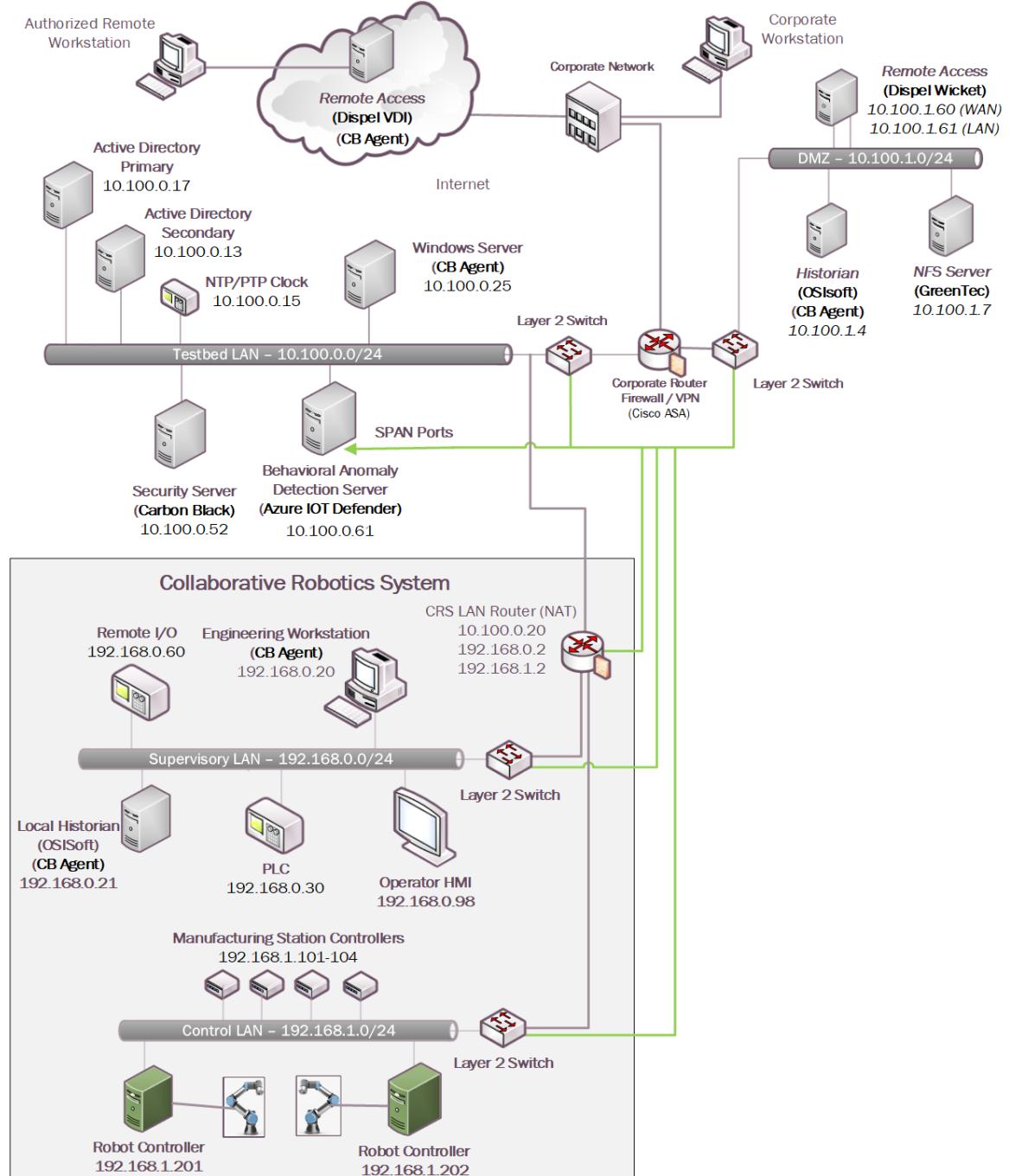
870 For Build 4, the technologies in Table 4-5 were integrated into the CRS, Testbed LAN, and DMZ segments  
 871 of the testbed environment to enhance system and data integrity capabilities.

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

Capability	Products	Description
<b>Application Allowlisting</b>	Carbon Black	Deployed within the Testbed LAN environment with the Carbon Black agents installed on key workstations and servers to control application execution.
<b>Behavior Anomaly Detection, Hardware/Software/Firmware Modification Detection</b>	PI Server	Deployed in the DMZ and CRS environments, the PI Server provides the historian repository for process data through its Data Archive and generates Event Frames upon detection of abnormal manufacturing system behavior.
	Azure Defender for IoT	Passively monitors the CRS network, Testbed LAN, and DMZ for abnormal network activity via SPAN ports and is also configured to capture detailed asset information for supporting inventory and change management capabilities.
<b>File Integrity Checking</b>	Carbon Black	Deployed within the Testbed LAN environment with the Carbon Black agents installed on key workstations and servers to monitor the integrity of local files.
	ForceField, WORMdisk	A GreenTec fileserver is added to the DMZ environment and configured with both a ForceField and WORM drive to provide a protected archive for the historian data and the approved versions of configuration and coding files for the ICS environment.
<b>User Authentication and Authorization</b>	Dispel	The Dispel Wicket is deployed to the DMZ environment and integrated with the Dispel cloud-based environment to provide a virtual desktop interface (VDI) with a secure remote connection to the testbed environment. Through this connection, authorized users are permitted to access resources in both the Testbed LAN and CRS environment.
<b>Remote Access</b>		

- 873 The technology was integrated into the lab environment as shown in [Figure 4-10](#).

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



## 874 5 Security Characteristic Analysis

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

### 878 5.1 Assumptions and Limitations

879 The security characteristic analysis has the following limitations:

- 880     ▪ It is neither a comprehensive test of all security components nor a red-team exercise.
- 881     ▪ It cannot identify all weaknesses.
- 882     ▪ It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these  
883        devices would reveal only weaknesses in implementation that would not be relevant to those  
884        adopting this reference architecture.

### 885 5.2 Example Solution Testing

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

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

900 Additional information for each scenario such as screenshots captured during the execution of the test  
901 procedures and detailed results from the security capabilities are presented in [Appendix D](#).

## 902 5.2.1 Scenario 1: Protect Host from Malware Infection via USB

<b>Objective</b>	This test demonstrates blocking the introduction of malware through physical access to a workstation within the manufacturing environment.
<b>Description</b>	An authorized user transports executable files into the manufacturing system via a USB flash drive that contains malware.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-6, PR.MA-2, DE.AE-2
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ User does not have administrative privileges on the target machine.</li> <li>▪ User has physical access to the target machine.</li> </ul>
<b>Security Capabilities and Products</b>	Build 1: <ul style="list-style-type: none"> <li>▪ Carbon Black: Application Allowlisting</li> </ul> Build 2: <ul style="list-style-type: none"> <li>▪ Windows SRP: Application Allowlisting</li> </ul> Build 3: <ul style="list-style-type: none"> <li>▪ Windows SRP: Application Allowlisting</li> </ul> Build 4: <ul style="list-style-type: none"> <li>▪ Carbon Black: Application Allowlisting</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. Attempt to execute malware on the target machine.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The application allowlisting tool will detect and stop the malware upon execution.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The application allowlisting technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> </ul>
<b>Overall Result</b>	PASS

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

<b>Objective</b>	This test demonstrates the detection of malware introduced from the network.
<b>Description</b>	An attacker pivoting from the corporate network into the manufacturing environment attempts to insert malware to establish persistence in the manufacturing environment.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ The attacker has completed reconnaissance and initial access, gaining the ability to pivot into the manufacturing environment.</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Carbon Black: Application Allowlisting</li> <li>▪ Tenable.ot: Behavioral Anomaly Detection</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ Windows SRP: Application Allowlisting</li> <li>▪ Forescout eyeInspect: Behavioral Anomaly Detection</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Windows SRP: Application Allowlisting</li> <li>▪ Dragos: Behavioral Anomaly Detection</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Carbon Black: Application Allowlisting</li> <li>▪ Azure Defender for IoT: Behavioral Anomaly Detection</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. Attacker pivots into the manufacturing environment.</li> <li>2. Attacker copies malware to the server in Testbed LAN.</li> <li>3. Attacker attempts to execute malware on server in Testbed LAN.</li> </ol>

<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The application allowlisting capabilities installed on target systems will block execution of the malicious code.</li> <li>▪ The behavioral anomaly detection tool will capture the suspicious traffic and generate an alert.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The application allowlisting technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> <li>▪ The BAD tool is able to detect and alert on activity pivoting into manufacturing systems.</li> </ul>
<b>Overall Result</b>	PASS

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

<b>Objective</b>	This test demonstrates blocking malware that is attempting to infect the manufacturing system through authorized remote access connections.
<b>Description</b>	A remote workstation authorized to use a remote access connection has been infected with malware. When the workstation is connected to the manufacturing environment through the remote access connection, the malware attempts to pivot and spread to vulnerable host(s).
<b>Relevant NIST <i>Cybersecurity Framework</i> Subcategories</b>	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-7, PR.MA-1, PR.MA-2, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ Infection of the remote workstation occurs prior to remote access session.</li> </ul>

<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Cisco VPN: Remote Access</li> <li>▪ ConsoleWorks: User Authentication and User Authorization</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ Dispel: User Authentication and User Authorization, and Remote Access</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Cisco VPN: Remote Access</li> <li>▪ ConsoleWorks: User Authentication and User Authorization</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. Authorized remote user connects to the manufacturing environment.</li> <li>2. Malware on remote host attempts to pivot into the manufacturing environment.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ Malware will be blocked from propagation by the remote access capabilities.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ Remote access connection blocks malware attempts to pivot into the manufacturing environment.</li> </ul>
<b>Overall Result</b>	PASS

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

<b>Objective</b>	This test demonstrates blocking installation and execution of unauthorized applications on a workstation in the manufacturing system.
<b>Description</b>	An authorized user copies downloaded software installation files from a shared network drive accessible from the workstation in the manufacturing system. The user then attempts to install the unauthorized software on the workstation.

<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ User does not have administrative privileges on the target machine.</li> <li>▪ Applications to be installed are unapproved applications.</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Carbon Black: Application Allowlisting</li> <li>▪ Tenable.ot: Behavioral Anomaly Detection</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ Windows SRP: Application Allowlisting</li> <li>▪ eyeInspect: Behavioral Anomaly Detection</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Windows SRP: Application Allowlisting</li> <li>▪ Dragos: Behavioral Anomaly Detection</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Carbon Black: Application Allowlisting</li> <li>▪ Azure Defender for IoT: Behavioral Anomaly Detection</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. The user copies software to a host in the manufacturing environment.</li> <li>2. The user attempts to install the software on the host.</li> <li>3. The user attempts to execute software that does not require installation.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The application allowlisting tool will detect and stop the execution of the software installation or executable file.</li> <li>▪ The BAD tool will capture the suspicious traffic and generate an alert.</li> </ul>

<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The application allowlisting technology successfully blocks and alerts on the execution of the application on the workstation in all builds.</li> <li>▪ The BAD tool is able to detect and alert on activity in the manufacturing system.</li> </ul>
<b>Overall Result</b>	PASS

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

<b>Objective</b>	This test demonstrates detection of an unauthorized device connecting to the manufacturing system.
<b>Description</b>	An individual authorized to access the physical premises connects and uses an unauthorized device on the manufacturing network.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ Ports on switch are active and available.</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Tenable.ot: Behavioral Anomaly Detection</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ eyeInspect: Behavioral Anomaly Detection</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Dragos: Behavioral Anomaly Detection</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Azure Defender for IoT: Behavioral Anomaly Detection</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. The individual connects the unauthorized device to the manufacturing network.</li> <li>2. The individual uses an unauthorized device to access other devices on the manufacturing network.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The behavioral anomaly detection tool will capture the suspicious traffic and generate an alert.</li> </ul>

<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The behavioral anomaly detection tool is able to detect and alert on activity in the manufacturing system.</li> </ul>
<b>Overall Result</b>	PASS

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

<b>Objective</b>	This test demonstrates detection of unauthorized communications between devices.
<b>Description</b>	A device authorized to be on the network attempts to establish an unapproved connection.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ The environment has a predictable communications pattern.</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Tenable.ot: Behavioral Anomaly Detection.</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ eyeInspect: Behavioral Anomaly Detection.</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Dragos: Behavioral Anomaly Detection.</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Azure Defender for IoT: Behavioral Anomaly Detection.</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. The device attempts to establish an unapproved connection.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The BAD tool will capture the suspicious traffic and generate an alert.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The BAD tool is able to detect and alert on activity in manufacturing systems.</li> </ul>
<b>Overall Result</b>	PASS

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

<b>Objective</b>	This test demonstrates protection of files from unauthorized deletion both locally and on network file share.
<b>Description</b>	An authorized user attempts to delete files on an engineering workstation and a shared network drive within the manufacturing system.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-1, PR.DS-6, PR.IP-4, PR.MA-1, DE.AE-2
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ User does not have administrative privileges on the target machine.</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Carbon Black: File Integrity Checking.</li> <li>▪ WORMdisk: File Integrity Protection.</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ Security Onion: File Integrity Checking.</li> <li>▪ WORMdisk: File Integrity Protection.</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Security Onion: File Integrity Checking.</li> <li>▪ WORMdisk: File Integrity Protection.</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Carbon Black: File Integrity Checking.</li> <li>▪ WORMdisk: File Integrity Protection.</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. User attempts to delete files located on a workstation in the manufacturing system.</li> <li>2. User attempts to delete files from the network file share containing the golden images for the manufacturing system.</li> </ol>

<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ Deletion of files on the workstation will be detected and alerted on by the file integrity checking tool.</li> <li>▪ Deletion of files on the network file share will be prevented by the file integrity checking tool.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ Host-based file integrity checking is able to detect and alert on deletion of files.</li> <li>▪ Protected network file share is able to prevent deletion of files on the network file share.</li> </ul>
<b>Overall Result</b>	PASS

## 909 5.2.8 Scenario 8: Detect Unauthorized Modification of PLC Logic

<b>Objective</b>	This test demonstrates detection of PLC logic modification.
<b>Description</b>	An authorized user performs an unapproved or unauthorized modification of the PLC logic from an engineering workstation.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.AC-3, PR.AC-7, PR.DS-6, PR.MA-1, PR.MA-2, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>• None</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Tenable.ot: Behavioral Anomaly Detection and Software Modification</li> <li>▪ Cisco VPN: Remote Access</li> <li>▪ ConsoleWorks: User Authentication, User Authorization, and Remote Access</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ eyeInspect: Behavioral Anomaly Detection and Software Modification</li> <li>▪ Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>

	<p><b>Build 3:</b></p> <ul style="list-style-type: none"> <li>▪ Dragos: Behavioral Anomaly Detection and Software Modification</li> <li>▪ Cisco VPN: Remote Access</li> <li>▪ ConsoleWorks: User Authentication, User Authorization, and Remote Access</li> </ul> <p><b>Build 4:</b></p> <ul style="list-style-type: none"> <li>▪ Azure Defender for IoT: Behavioral Anomaly Detection and Software Modification</li> <li>▪ Dispel: User Authentication and User Authorization, and Remote Access</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. The authorized user remotely connects to a manufacturing environment.</li> <li>2. The user modifies and downloads a logic file to the PLC.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The behavioral anomaly detection tool will capture the suspicious traffic and generate an alert.</li> <li>▪ The user authentication/authorization/remote access is able to remotely access the engineering systems as intended.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The behavioral anomaly detection tool is able to detect and alert on activity accessing the PLC.</li> </ul>
<b>Overall Result</b>	PASS

### 910 5.2.9 Scenario 9: Protect from Modification of Historian Data

<b>Objective</b>	This test demonstrates blocking of modification of historian archive data.
<b>Description</b>	An attacker coming from the corporate network pivots into the manufacturing environment and attempts to modify historian archive data.
<b>Relevant NIST Cybersecurity Framework Subcategories</b>	PR.DS-6, PR.MA-1, DE.AE-2

<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ The attacker has completed reconnaissance and initial access, gaining the ability to pivot into the manufacturing environment.</li> </ul>
<b>Security Capabilities and Products</b>	<p>Build 1:</p> <ul style="list-style-type: none"> <li>▪ Tenable.ot: Behavioral Anomaly Detection.</li> <li>▪ ForceField WFS: File Integrity Protection.</li> </ul> <p>Build 2:</p> <ul style="list-style-type: none"> <li>▪ eyeInspect: Behavioral Anomaly Detection.</li> <li>▪ ForceField WFS: File Integrity Protection.</li> </ul> <p>Build 3:</p> <ul style="list-style-type: none"> <li>▪ Dragos: Behavioral Anomaly Detection.</li> <li>▪ ForceField WFS: File Integrity Protection.</li> </ul> <p>Build 4:</p> <ul style="list-style-type: none"> <li>▪ Azure Defender for IoT: Behavioral Anomaly Detection.</li> <li>▪ ForceField WFS: File Integrity Protection.</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. Attacker pivots into the manufacturing environment from the corporate network.</li> <li>2. Attacker attempts to delete historian archive data file.</li> <li>3. Attacker attempts to replace historian archive data file.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The file operations will be blocked by the file integrity checking tool.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ File integrity checking tool is able to prevent file operations on the protected files.</li> </ul>
<b>Overall Result</b>	PASS

## 911 5.2.10 Scenario 10: Detect Sensor Data Manipulation

<b>Objective</b>	This test demonstrates detection of atypical data reported to the historian.
<b>Description</b>	A sensor in the manufacturing system begins sending atypical data values to the historian.
<b>Relevant NIST <i>Cybersecurity Framework</i> Subcategories</b>	PR.IP-4, PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ Devices in the manufacturing system (HMI and PLCs) are not validating sensor data.</li> </ul>
<b>Security Capabilities and Products</b>	<ul style="list-style-type: none"> <li>▪ PI Server: Behavioral Anomaly Detection</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. A sensor sends invalid data to the historian.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>▪ The behavioral anomaly detection capability will detect atypical sensor data and generate alerts.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>▪ The behavioral anomaly detection tool is able to detect atypical data and create an event frame.</li> </ul>
<b>Overall Result</b>	PASS

## 912 5.2.11 Scenario 11: Detect Unauthorized Firmware Modification

<b>Objective</b>	This test demonstrates detection of device firmware modification.
<b>Description</b>	An authorized user performs a change of the firmware on a PLC.
<b>Relevant NIST <i>Cybersecurity Framework</i> Subcategories</b>	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
<b>Assumptions</b>	<ul style="list-style-type: none"> <li>▪ None</li> </ul>

<b>Security Capabilities and Products</b>	<p><b>Build 1:</b></p> <ul style="list-style-type: none"> <li>■ Cisco VPN: Remote Access.</li> <li>■ ConsoleWorks: Remote Access, User Authentication, and User Authorization.</li> <li>■ Tenable.ot: Behavioral Anomaly Detection and Firmware Modification.</li> </ul> <p><b>Build 2:</b></p> <ul style="list-style-type: none"> <li>■ Dispel: Remote Access, User Authentication, and User Authorization.</li> <li>■ eyeInspect and ICSPatrol: Behavioral Anomaly Detection and Firmware Modification.</li> </ul> <p><b>Build 3:</b></p> <ul style="list-style-type: none"> <li>■ Cisco VPN: Remote Access.</li> <li>■ ConsoleWorks: Remote Access, User Authentication, and User Authorization.</li> <li>■ Dragos: Behavioral Anomaly Detection and Firmware Modification.</li> </ul> <p><b>Build 4:</b></p> <ul style="list-style-type: none"> <li>■ Dispel: Remote Access, User Authentication, and User Authorization.</li> <li>■ Azure Defender for IoT: Behavioral Anomaly Detection and Firmware Modification.</li> </ul>
<b>Test Procedures</b>	<ol style="list-style-type: none"> <li>1. Authorized remote user connects to manufacturing environment.</li> <li>2. The user changes firmware on the PLC component.</li> </ol>
<b>Expected Results</b>	<ul style="list-style-type: none"> <li>■ The behavioral anomaly detection tool will identify the change to the PLC and generate an alert for review.</li> </ul>
<b>Actual Test Results</b>	<ul style="list-style-type: none"> <li>■ The behavioral anomaly tool is able to detect and generate alerts for updates to PLC component firmware.</li> </ul>
<b>Overall Result</b>	PASS

913 **5.3 Scenarios and Findings**

914 One aspect of our security evaluation involved assessing how well the reference design addresses the  
915 security characteristics that it was intended to support. The NIST *Cybersecurity Framework*  
916 Subcategories were used to provide structure to the security assessment by consulting the specific  
917 sections of each standard that are cited in reference to a Subcategory. The cited sections provide  
918 validation points that the example solution would be expected to exhibit. Using the NIST *Cybersecurity*  
919 *Framework* Subcategories as a basis for organizing our analysis allowed us to systematically consider  
920 how well the reference design supports the intended security characteristics.

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

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

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

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

932 **5.3.3 PR.AC-4: Access permissions and authorizations are managed,  
933 incorporating the principles of least privilege and separation of duties**

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

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

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

949   **5.3.5 PR.DS-1: Data-at-rest is protected**

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

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

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

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

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

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

967   This NIST *Cybersecurity Framework* Subcategory is supported by a combination of tools including  
968   application allowlisting, the user authentication and user authorization tools, and the behavior anomaly  
969   detection tools. User authentication and user authorization tools provide a controlled environment for  
970   authorized users to interact with the manufacturing environment. Behavior anomaly detection tools  
971   provide a means to detect maintenance activities in the environment such as PLC logic modification or

972 PLC firmware updates via the network. This information can be combined with data from a  
973 computerized maintenance management system to ensure that all maintenance activities are  
974 appropriately approved and logged. Also, application allowlisting prevents unapproved software from  
975 running on systems to ensure that only approved tools are used for maintenance activities.

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

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

982 **5.3.10 DE.AE-1: A baseline of network operations and expected data flows for  
983 users and systems is established and managed**

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

987 **5.3.11 DE.AE-2: Detected events are analyzed to understand attack targets and  
988 methods**

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

995 **5.3.12 DE.AE-3: Event data are collected and correlated from multiple sources and  
996 sensors**

997 This NIST *Cybersecurity Framework* Subcategory is supported by all the capabilities included in the  
998 solutions. Each tool detects different aspects of the scenarios from diverse perspectives. Although not  
999 demonstrated in these solutions, a data aggregation and correlation tool such as a security information  
1000 and event management (SIEM) tool would enhance the detection capability of the solution.

1001    5.3.13 DE.CM-1: The network is monitored to detect potential cybersecurity  
1002    events

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

1011    5.3.14 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity  
1012    events

1013    This NIST *Cybersecurity Framework* Subcategory is supported by the authentication and authorization  
1014    tools that allow for monitoring personnel activity while connected through these tools. Further,  
1015    application allowlisting and file integrity checking tools provide the ability to monitor user actions on  
1016    hosts. Additionally, behavioral anomaly detection tools monitor and record events associated with  
1017    personnel actions traversing network traffic. Each tool provides a different perspective in monitoring  
1018    personnel activity within the environment. The resulting alerts and logs from these tools can be  
1019    monitored individually or collectively to support investigations for potential malicious or unauthorized  
1020    activity within the environment.

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

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

## 1032 6 Future Build Considerations

1033 This guide has presented technical solutions for maintaining and monitoring system and information  
1034 integrity, which will help detect and prevent incidents in a manufacturing environment. Future builds  
1035 should demonstrate methods and techniques for fusing event and log data from multiple platforms into  
1036 a security operations center (SOC) to improve monitoring and detection capabilities for an organization.  
1037 Future builds should also demonstrate how to recover from a loss of system or information integrity  
1038 such as a ransomware attack for ICS environments.

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

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

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

**1076 Appendix B Glossary**

<b>Access Control</b>	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).  SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009
<b>Architecture</b>	A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).  SOURCE: FIPS 201-2
<b>Authentication</b>	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.  SOURCE: FIPS 200
<b>Authorization</b>	The right or a permission that is granted to a system entity to access a system resource.  SOURCE: NIST SP 800-82 Rev. 2
<b>Backup</b>	A copy of files and programs made to facilitate recovery if necessary.  SOURCE: NIST SP 800-34 Rev. 1
<b>Continuous Monitoring</b>	Maintaining ongoing awareness to support organizational risk decisions.  SOURCE: NIST SP 800-137
<b>CRADA</b>	Collaborative Research and Development Agreement  SOURCE: NIST SP 1800-5b, NIST SP 1800-5c

<b>Cybersecurity</b>	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
	SOURCE: CNSSI 4009-2015 (NSPD-54/HSPD-23)
<b>Cyber Attack</b>	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
	SOURCE: NIST SP 800-30 Rev. 1
<b>Data</b>	A subset of information in an electronic format that allows it to be retrieved or transmitted.
	SOURCE: CNSSI-4009
<b>Data Integrity</b>	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
	SOURCE: CNSSI-4009
<b>File Integrity Checking</b>	Software that generates, stores, and compares message digests for files to detect changes made to the files.
	SOURCE: NIST SP 800-115
<b>Firmware</b>	Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs.
	SOURCE: CNSSI 4009-2015
<b>Industrial Control Systems</b>	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution.
	SOURCE: NIST SP 800-30 Rev. 1

<b>Information Security</b>	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
	SOURCE: FIPS 199 (44 U.S.C., Sec. 3542)
<b>Information System</b>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
	SOURCE: FIPS 200 (44 U.S.C., Sec. 3502)
<b>Information Technology</b>	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
	SOURCE: FIPS 200
<b>Log</b>	A record of the events occurring within an organization's systems and networks.
	SOURCE: NIST SP 800-92
<b>Malware</b>	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
	SOURCE: NIST SP 800-111
<b>Network Traffic</b>	Computer network communications that are carried over wired or wireless networks between hosts.
	SOURCE: NIST SP 800-86
<b>Operational Technology</b>	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).
	SOURCE: NIST SP 800-37 Rev. 2
<b>Privacy</b>	Assurance that the confidentiality of, and access to, certain information about an entity is protected.
	SOURCE: NIST SP 800-130

<b>Remote Access</b>	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).  SOURCE: NIST SP 800-128 under Remote Access from NIST SP 800-53
<b>Risk</b>	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.  SOURCE: FIPS 200
<b>Risk Assessment</b>	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.  SOURCE: NIST SP 800-63-2
<b>Risk Management Framework</b>	The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.  SOURCE: NIST SP 800-82 Rev. 2 (NIST SP 800-37)
<b>Security Control</b>	A protection measure for a system  SOURCE: NIST SP 800-123
<b>Virtual Machine</b>	Software that allows a single host to run one or more guest operating systems  SOURCE: NIST SP 800-115

## 1077 Appendix C References

- 1078 [1] C. Singleton et al., X-Force Threat Intelligence Index 2021, IBM, February 2021,  
1079 <https://www.ibm.com/security/data-breach/threat-intelligence>
- 1080 [2] A Sedgewick et al., *Guide to Application Whitelisting*, NIST SP 800-167, NIST, Oct. 2015.  
1081 Available: <http://dx.doi.org/10.6028/NIST.SP.800-167>.
- 1082 [3] Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework  
1083 Implementation Guidance, 2015. Available:  
1084 <https://www.cisa.gov/sites/default/files/publications/critical-manufacturingcybersecurity->  
1085 <framework-implementation-guide-2015-508.pdf>.
- 1086 [4] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD201300091,  
1087 Feb. 12, 2013. Available: <https://obamawhitehouse.archives.gov/the-press->  
1088 <office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
- 1089 [5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, V1.1 April 16, 2018.  
1090 Available: <https://doi.org/10.6028/NIST.CSWP.04162018>.
- 1091 [6] J. McCarthy et al., Securing Manufacturing Industrial Control Systems: Behavioral Anomaly  
1092 Detection, NIST Interagency Report (NISTIR) 8219, NIST, Nov. 2018. Available:  
1093 <https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf>.
- 1094 [7] K. Stouffer et al., Cybersecurity Framework Manufacturing Profile, NIST Internal Report 8183,  
1095 NIST, May 2017. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf>.
- 1096 [8] R. Candell et al., An Industrial Control System Cybersecurity Performance Testbed, NISTIR 8089,  
1097 NIST, Nov. 2015. Available: <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf>.
- 1098 [9] Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53  
1099 Revision 5, NIST, Apr. 2013. Available: <https://doi.org/10.6028/NIST.SP.800-53r5>.
- 1100 [10] W. Newhouse et al., National Initiative for Cybersecurity Education (NICE) Cybersecurity  
1101 Workforce Framework, NIST SP 800-181, Aug. 2017. Available:  
1102 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>.
- 1103 [11] J. Cawthra et al., Data Integrity: Identifying and Protecting Assets Against Ransomware and  
1104 Other Destructive Events, NIST Special Publication 1800-25 Dec. 2020,  
1105 <https://doi.org/10.6028/NIST.SP.1800-25>.
- 1106 [12] Celia Paulsen, Robert Byers, Glossary of Key Information Security Terms NISTIR 7298,  
1107 <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf>.

- 1108 [13] U.S.-Canada Power Systems Outage Task Force, Final Report on the August 14, 2003 Blackout in  
1109 the United States and Canada: Causes and Recommendations. Available:  
1110 [https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/Outage\\_Task\\_Force\\_-\\_DRAFT\\_Report\\_on\\_Implementation.pdf](https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/Outage_Task_Force_-_DRAFT_Report_on_Implementation.pdf)
- 1112 [14] K. Stouffer et al., Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Revision 2,  
1113 NIST, June 2015, Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- 1115 [15] J. J. Downs and E. F. Vogel, "A Plant-wide Industrial Problem Process," Comput. Chem. Eng., vol.  
1116 17, no. 3, 1993, pp. 245–255.

## 1117 **Appendix D Scenario Execution Results**

1118 The following section provides details regarding the execution and results from each scenario. Details  
1119 such as usernames, filenames, IP addresses, etc. are specific to the NCCoE lab environment and are  
1120 provided for reference only.

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

1122 An authorized user inserts a USB storage device containing a malware file (1.exe) into a system in the  
1123 manufacturing environment (e.g., an engineering workstation). After insertion, the malware file (1.exe)  
1124 attempts to execute. The expected outcome is that the application allowlisting technology blocks the  
1125 execution of the file.

#### 1126 **D.1.1 Build 1**

##### 1127 *D.1.1.1 Configuration*

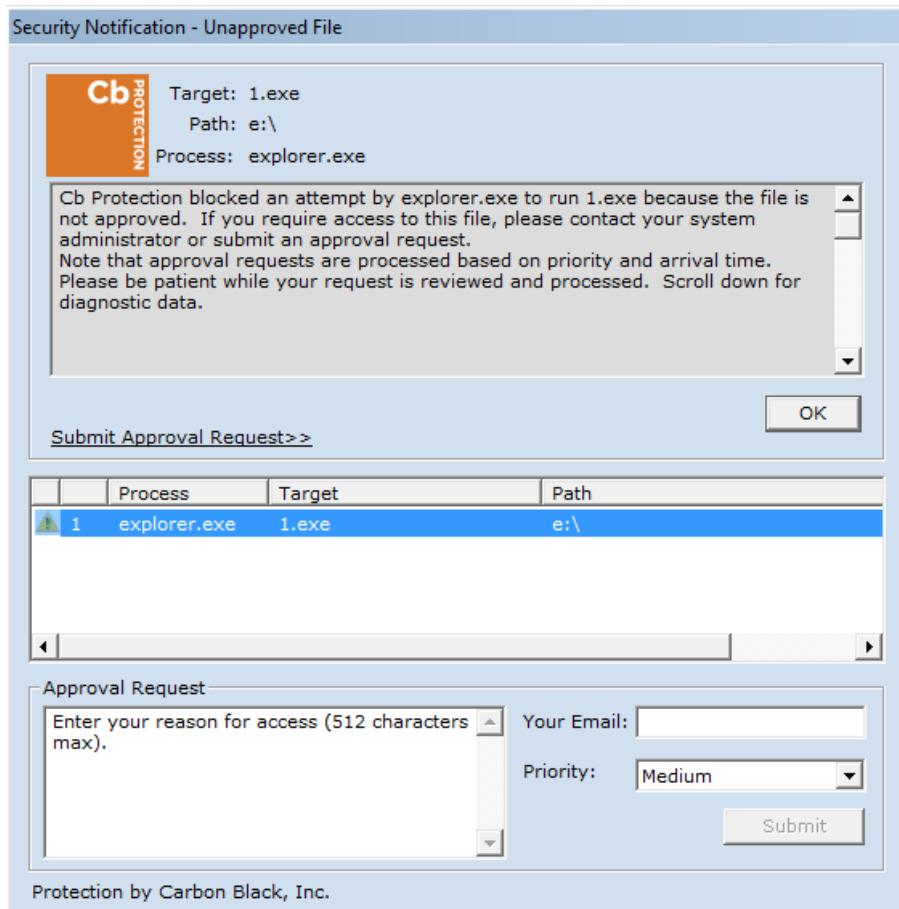
- 1128     ▪ Application Allowlisting: Carbon Black
  - 1129         • Agent installed on an HMI Workstation and configured to communicate to the Carbon  
1130             Black Server.

##### 1131 *D.1.1.2 Test Results*

1132 Carbon Black successfully detects and blocks the malware (1.exe) from running as shown in [Figure D-1](#).  
1133 [Figure D-2](#) shows Carbon Black's server log. The log provides more detail on the activity detected by  
1134 Carbon Black.

DRAFT

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



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

Timestamp	Severity	Type	Subtype	Source	Description	IP Address	User
Apr 7 2021 02:51:09 PM	Notice	Discovery	New unapproved file to computer	LANIFGS-61338HH	Computer LANIFGS-61338HH discovered new file 'e:\1.exe' [2D2CB..A1224]. DiscoveredBy[Kernel.Execute] FileCreated@[24/2020 2:23:10 PM] Discovered@[4/7/2021 6:51:09 PM (Hash: 4/7/2021 6:51:09 PM)] YaraClassifyVersion@2 Rules@{eExe,IsDepthIncompatibleExe}	172.16.1.4	LAN\nccoeUser
Apr 7 2021 02:51:09 PM	Notice	Policy Enforcement	Execution block (unapproved file)	LANIFGS-61338HH	File 'e:\1.exe' [2D2CB..A1224] was blocked because it was unapproved.	172.16.1.4	LAN\nccoeUser
Apr 7 2021 02:47:35 PM	Notice	Discovery	New unapproved file to computer	LANIFGS-61338HH	Computer LANIFGS-61338HH discovered new file 'e:\1.exe' [2D2CB..A1224]. DiscoveredBy[Kernel.Execute] FileCreated@[24/2020 2:23:10 PM] Discovered@[4/7/2021 6:47:35 PM (Hash: 4/7/2021 6:47:35 PM)] YaraClassifyVersion@2 Rules@{eExe,IsDepthIncompatibleExe}	172.16.1.4	LAN\nccoeUser
Apr 7 2021 01:43:52 PM	Notice	Policy Enforcement	Execution block (unapproved file)	LANIPOLARIS	File 'e:\1.exe' [2D2CB..A1224] was blocked because it was unapproved.	10.100.0.20	LAN\nccoeUser
Apr 7 2021 01:43:52 PM	Notice	Discovery	New unapproved file to computer	LANIPOLARIS	Computer LANIPOLARIS discovered new file 'e:\1.exe' [2D2CB..A1224]. DiscoveredBy[Kernel.Execute] FileCreated@[24/2020 2:23:10 PM] Discovered@[4/7/2021 5:43:52 PM (Hash: 4/7/2021 5:43:52 PM)] YaraClassifyVersion@2 Rules@{eExe,IsDepthIncompatibleExe}	10.100.0.20	LAN\nccoeUser

1137 **Figure D-3: Carbon Black's Server Log of the Event**

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

1138 **D.1.2 Build 2**

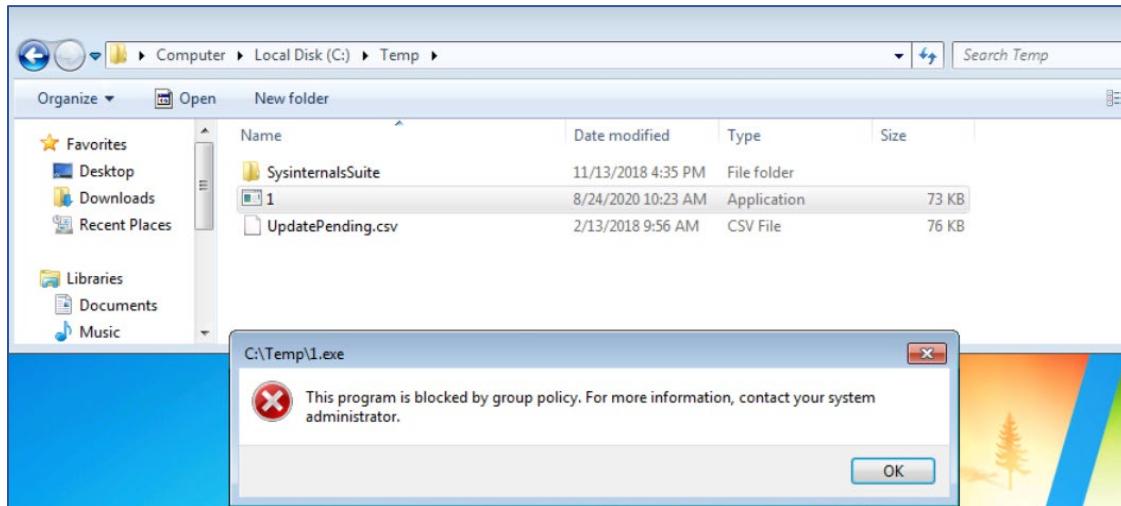
#### 1139 *D.1.2.1 Configuration*

- 1140     ▪ Application Allowlisting: windows SRP
  - 1141         • Allowlisting policies are applied to HMI Workstation.

#### 1142 *D.1.2.2 Test Results*

1143 The execution of 1.exe is blocked successfully when Windows SRP is enforced as shown in Figure D-4.

1144 **Figure D-4: Windows 7 Alert as a Result of Windows SRP Blocking the Execution of 1.exe**



1145 **D.1.3 Build 3**

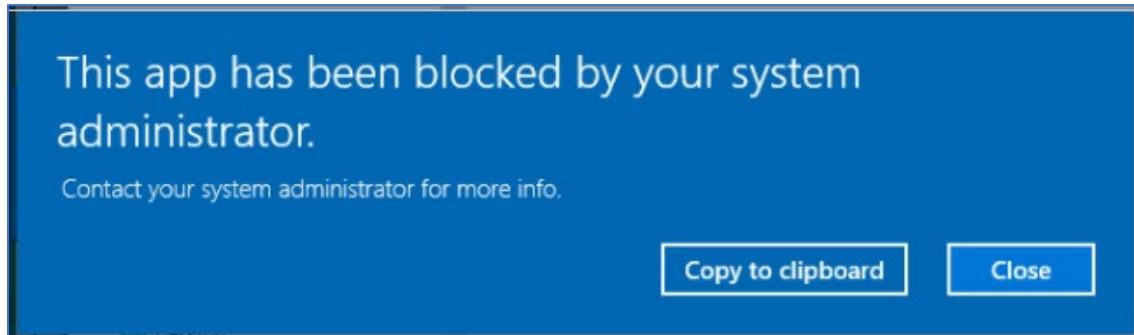
#### 1146 *D.1.3.1 Configuration*

- 1147     ▪ Application Allowlisting: Windows SRP
  - 1148         • Allowlisting policies are applied to Engineering Workstation.

#### 1149 *D.1.3.2 Test Results*

1150 For Build 3, Windows SRP application allowlisting is enabled in the Collaborative Robotics environment.  
 1151 [Figure D-5](#) shows that the executable is blocked on the CRS workstation.

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



1153    **D.1.4 Build 4**

1154    ***D.1.4.1 Configuration***

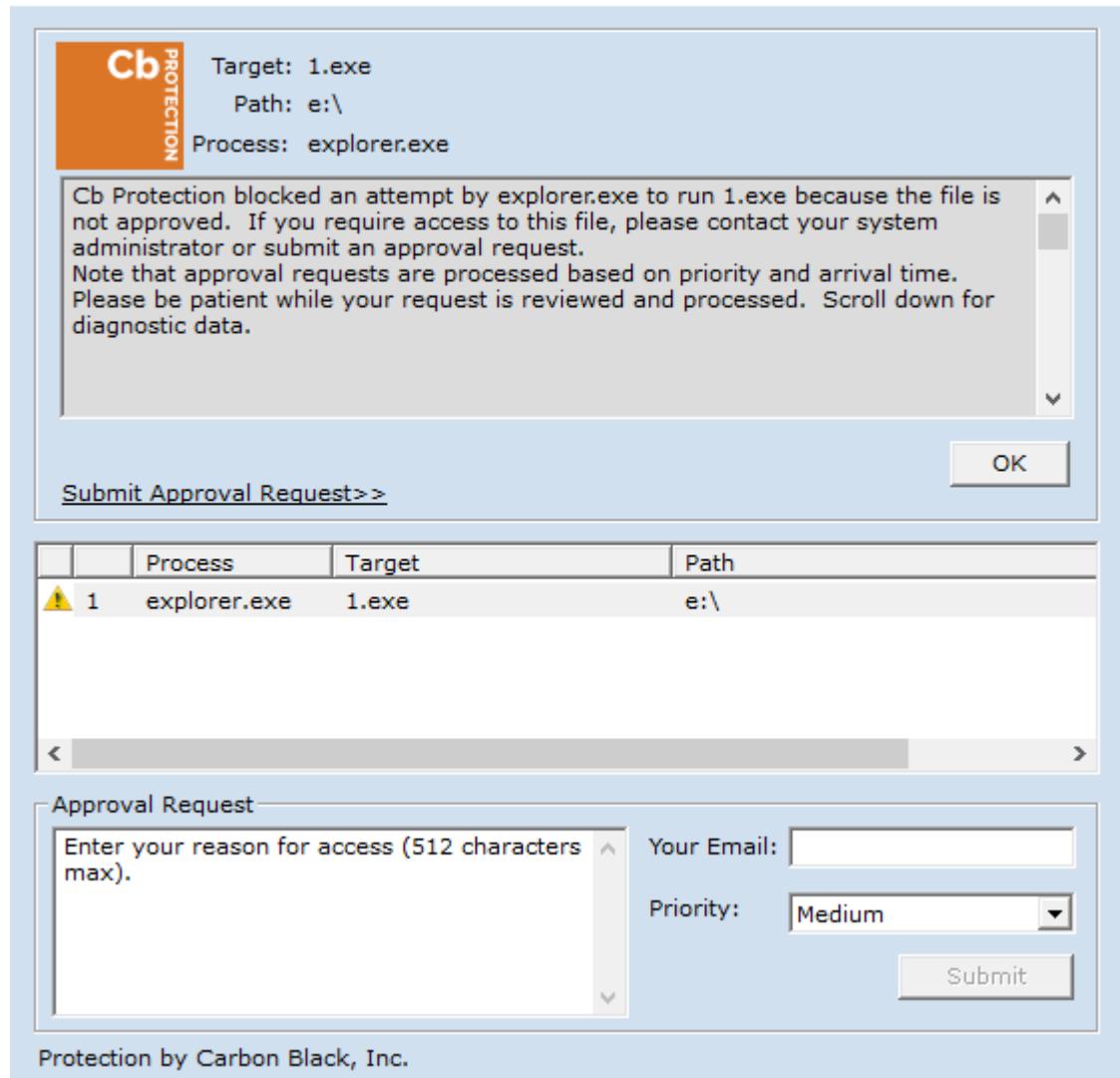
- 1155        ▪ Application Allowlisting : Carbon Black
- 1156            • Agent installed on Engineering Workstation and configured to communicate to the Carbon  
1157            Black Server.

1158    ***D.1.4.2 Test Results***

1159    Carbon Black successfully detects and blocks the malicious file as shown by the Carbon Black notification  
1160    in [Figure D-6](#).

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

Security Notification - Unapproved File

1162 **D.2 Executing Scenario 2: Protect Host from Malware via Network Vector**

1163 An attacker who has already gained access to the corporate network attempts to pivot into the ICS  
 1164 environment through the DMZ. From a system in the DMZ, the attacker scans for vulnerable systems in  
 1165 the Testbed LAN environment to continue pivoting toward the ICS environments. In an attempt to  
 1166 establish a persistent connection into the ICS environment, the malicious file (1.exe) is copied to a  
 1167 system in the Testbed LAN environment and executed. The expected outcome is that the malicious file is  
 1168 blocked by the application allowlisting tool, and the RDP and scanning network activity is observed by  
 1169 the behavioral anomaly detection tool.

1170 **D.2.1 Build 1**1171 **D.2.1.1 Configuration**

- 1172     ▪ Application Allowlisting: Carbon Black
- 1173         • Agent installed on systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2 and configured  
1174         to communicate to the Carbon Black Server.
- 1175     ▪ Behavior Anomaly Detection: Tenable.ot
- 1176         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

1177 **D.2.1.2 Test Results**

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

1185 **Figure D-7: Tenable.ot Dashboard Showing the Events that were Detected**

The screenshot shows the Tenable.ot dashboard interface. At the top, there's a header bar with the Tenable logo, the date and time (01:54 PM • Tuesday, Apr 13, 2021), and a user name (NCCOE User). Below the header is a navigation menu with items like Configuration Events, SCADA Events, Network Threats, Network Events, Policies, Inventory, Controllers, Network Assets, Risk, Network, Groups, Reports, and Local Settings. The main area has tabs for 'Events' (selected), 'All Events' (selected), and a search bar. A table lists 100 out of 17135 events. The columns include Log ID, Time, Event Type, Severity, Policy Name, Source Asset, Source Address, Destination Asset, and Destination Address. Most events are categorized as 'SYN Scan Detected' with 'High' severity. Below the table, a specific event (Event 19308) is selected, showing its details: 'A Port scan is a probe to reveal what ports are open and listening on a given asset'. It lists the source as 'OPC Server' and the destination as 'Server #22'. A 'Why is this important?' section notes that port scans are part of mapping communication channels to an asset, and a 'Suggested Mitigation' section advises being familiar with the source of the port scan and monitoring devices in the network.

1186 **Figure D-8: Detected RDP Session Activity from External System to DMZ System**

LOG ID	TIME ↓	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD...
<input type="checkbox"/> 19251	02:18:57 PM · Apr 12, 2021	Unauthorized Conversation	Medium	<a href="#">Communication from External Network</a>	Work Station #19		HistorianDMZ	
<input type="checkbox"/> 19250	02:18:45 PM · Apr 12, 2021	Unauthorized Conversation	Medium	<a href="#">Communication from External Network</a>	Work Station #19		HistorianDMZ	

1187 **Figure D-9: Event Detection Detail for the RDP Connection from the External System to the Historian in the DMZ**

Event 19251 02:18:57 PM · Apr 12, 2021 Unauthorized Conversation Medium Not resolved

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

1189 **Figure D-10: Tenable.ot Detected VNC Connection Between the DMZ and the Testbed LAN**

Event 19273 02:54:32 PM · Apr 12, 2021 Intrusion Detection Medium Not resolved

Details	Intrusion Detection events may indicate malicious communications based on known traffic patterns	Why is this important?	Suggested Mitigation
Rule Details	SOURCE NAME <a href="#">HistorianDMZ</a>	Intrusion detection events may indicate that the network has been compromised and is exposed to malicious entities. It is important to be aware of any such traffic that may indicate reconnaissance activity, attacks on the network or propagation of a threat to/from other subnets of the network.	Make sure that the source and destination assets are familiar to you. In addition, depending on the suspicious traffic, you may consider updating anti-virus definitions, firewall rules or other security patches. You can open the Rule Details panel to view additional details about this particular rule.
Source	SOURCE ADDRESS 10.100.1.4		
Destination	DESTINATION NAME <a href="#">Stratix8300 FA2</a>		
Policy	DESTINATION ADDRESS 10.100.0.40   172.16.2.1		
Status	PROTOCOL rfb (tcp/5900)		
	PORT 5900		
	RULE MESSAGE ET SCAN Potential VNC Scan 5900-5920		
	SID 2002911		

1190    **Figure D-11: Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in  
1191 the Testbed LAN**

The screenshot shows the Tenable.ot event detail interface for an event ID 19288. The event occurred at 02:55:24 PM on April 12, 2021, and is categorized as a 'Port Scan' with a 'High' severity level and 'Not resolved' status.

**Details:** A Port scan is a probe to reveal what ports are open and listening on a given asset.

SOURCE NAME	<a href="#">HistorianDMZ</a>
SOURCE ADDRESS	10.100.1.4
DESTINATION NAME	<a href="#">Laptop</a>
DESTINATION ADDRESS	10.100.0.101   192.168.0.205
PROTOCOL	tcp
PORT	

**Why is this important?** Port scans are part of mapping communication channels to an asset. Some port scans are legitimate and done by monitoring devices in the network. However, such mapping may also be done in the early stages of an attack, in order to detect vulnerable and accessible ports for malicious communication.

**Suggested Mitigation:** Make sure that you are familiar with the source of the port scan and that this port scan was expected. In case you are not familiar with the source check with the source asset owner to see whether this was a planned and expected port scan. If not, check which other assets have been scanned by the source asset and consider isolating the source asset to decrease network exposure while you investigate further.

1192    **Figure D-12: Detected RDP from a DMZ system to a Testbed LAN system**

The screenshot shows the Tenable.ot event detail interface for an event ID 19299. The event occurred at 03:01:39 PM on April 12, 2021, and is categorized as an 'RDP Connection (Authenticated)' with a 'Medium' severity level and 'Not resolved' status.

SOURCE NAME	<a href="#">HistorianDMZ</a>
SOURCE ADDRESS	10.100.1.4
DESTINATION NAME	<a href="#">NESSUSVM</a>
DESTINATION ADDRESS	10.100.0.25
PROTOCOL	Rdstls
COOKIE	Cookie: mstshash=ncceouser

1193    **Figure D-13: Tenable.ot Event Detail Showing the RDP Connection Between the Historian in the DMZ  
1194 to a Workstation in the Testbed LAN**

The screenshot shows the Tenable.ot event detail interface for an event ID 19299. The event occurred at 03:01:39 PM on April 12, 2021, and is categorized as an 'RDP Connection (Authenticated)' with a 'Medium' severity level and 'Not resolved' status.

**Details:** An authenticated initiation of an RDP connection.

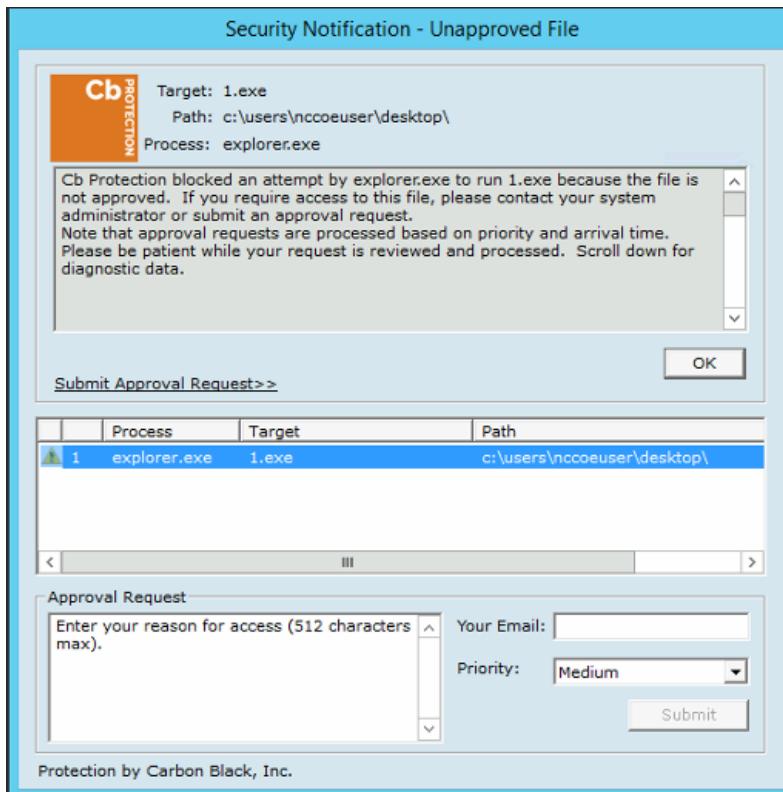
SOURCE NAME	<a href="#">HistorianDMZ</a>
SOURCE ADDRESS	10.100.1.4
DESTINATION NAME	<a href="#">NESSUSVM</a>
DESTINATION ADDRESS	10.100.0.25
PROTOCOL	Rdstls
COOKIE	Cookie: mstshash=ncceouser

**Why is this important?** Remote access to a workstation is a common way for cyber threats to propagate towards their target. Often system administrators prefer to limit use of such protocols to unique support cases so that they can identify the use of such protocols as anomalies.

**Suggested Mitigation:**

1. Check if this communication was approved.
2. Investigate if it was done by an authorized employee.
3. Check for potential initiation of such a communication by malware.

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



1196 **D.2.2 Build 2**

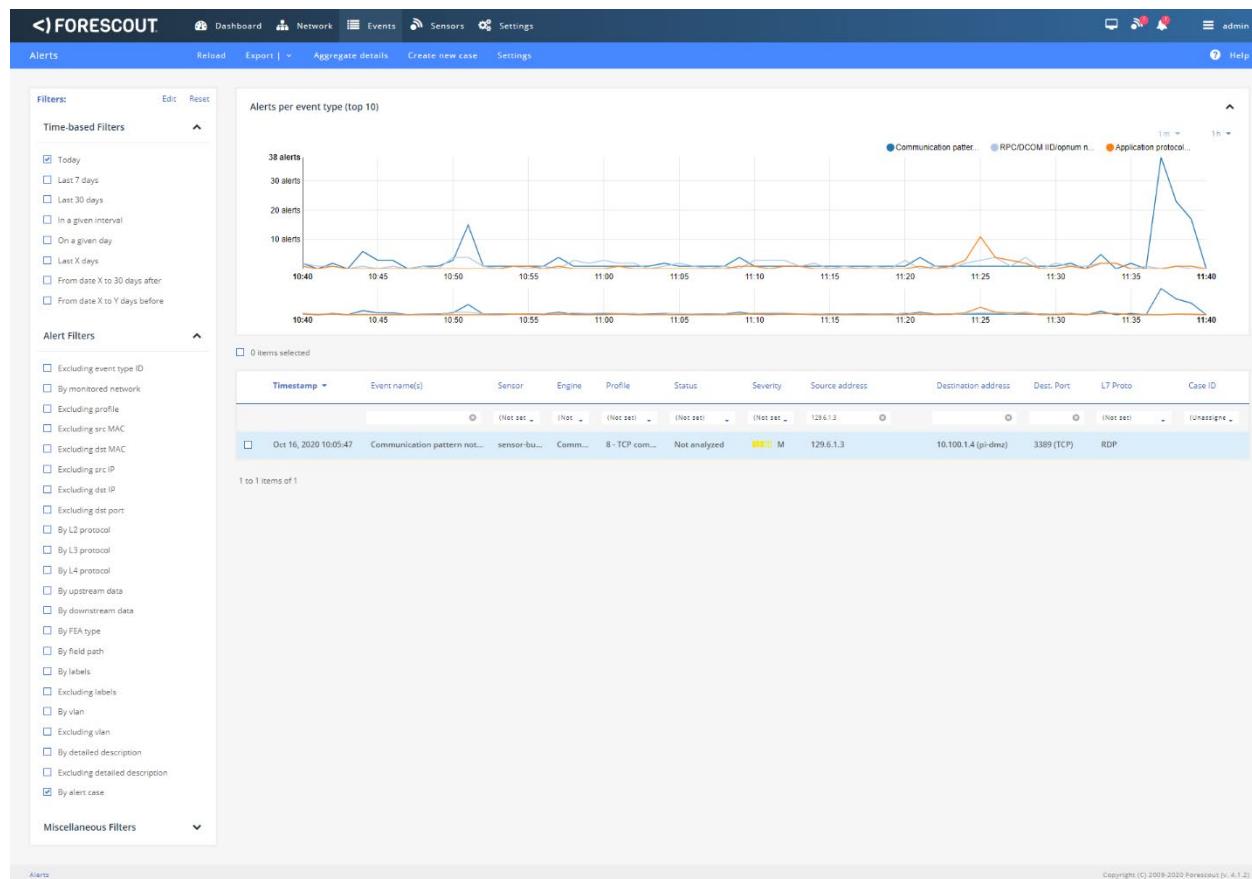
### 1197 *D.2.2.1 Configuration*

- 1198     ▪ Application Allowlisting: Windows SRP
  - 1199         • Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1201     ▪ Behavior Anomaly Detection: eyeInspect
  - 1202         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

### 1203 *D.2.2.2 Test Results*

1204 [Figure D-15](#) shows the RDP alert for connection into the DMZ while [Figure D-16](#) shows the details of the  
 1205 alert. [Figure D-17](#) shows a collection of suspicious activity detected by Forescout eyeInspect when  
 1206 scanning and an RDP connection is executed. [Figure D-18](#) and [Figure D-19](#) show details of a port  
 1207 scanning alert and the second RDP connection into the manufacturing environment, respectively. The  
 1208 attempt to execute malware (1.exe) is blocked by Windows SRP as shown in [Figure D-20](#).

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



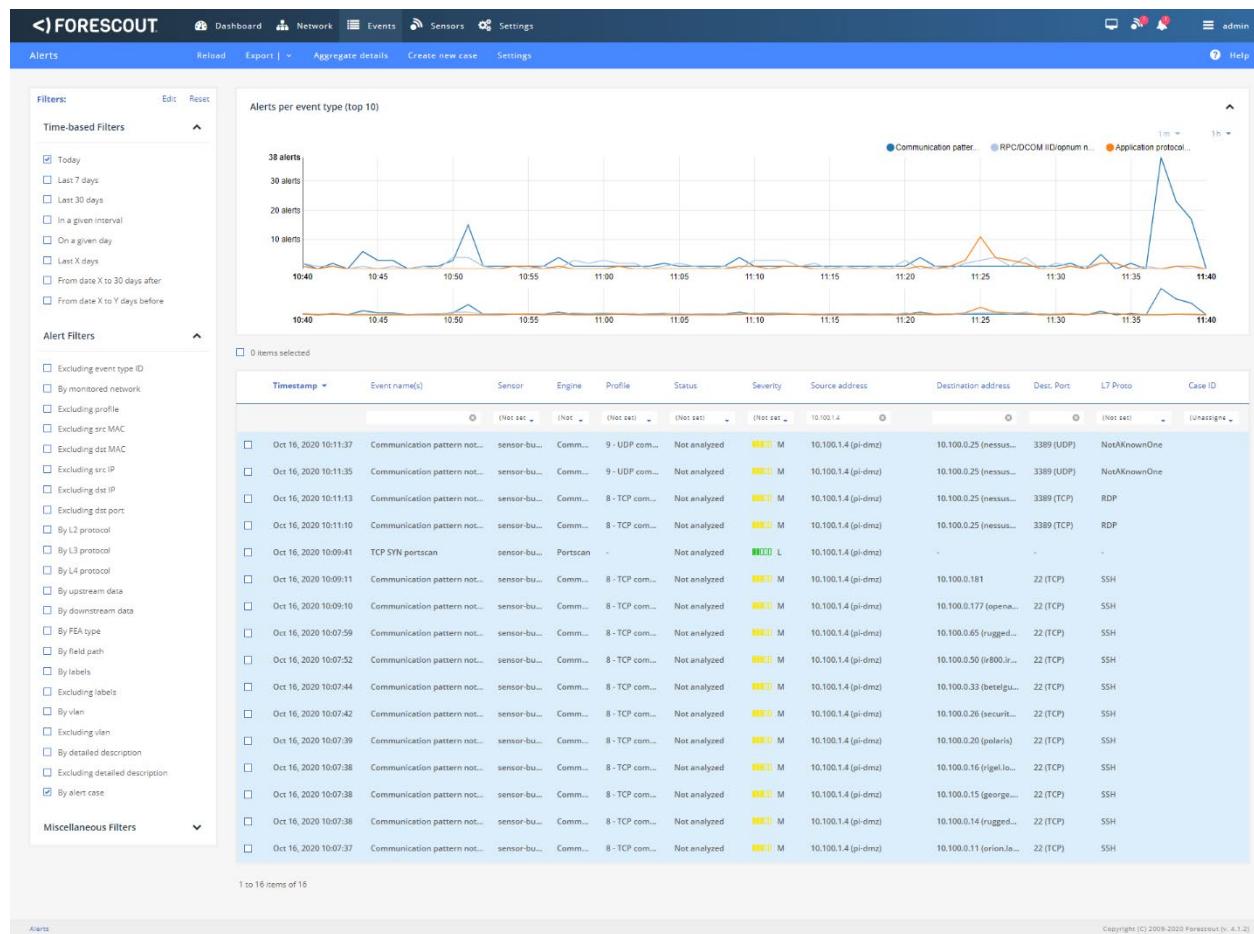
1210 Figure D-16: Details of the Detected RDP Session Activity from an External System to DMZ System

The screenshot displays the FORESCOUT web-based security management platform. The top navigation bar includes links for Dashboard, Network, Events, Sensors, Settings, and Admin. The main content area is divided into several sections:

- Alert details:** Shows an alert with ID 203138, timestamp Oct 16, 2020 10:05:47, and a summary of the detected communication pattern.
- Source host info:** Details about the source host, including IP address (Public IP), Host MAC addresses (Unknown), Other observed MAC addresses (Rockwell, Cisco), Role (Terminal client), Vendor and model (Rockwell), Client protocols (RDP (TCP 3389)), Server protocols (NotKnownOrOne (TCP 4444)), Purdue level (4 - Site business network), Security Risk (3.3), Operational Risk (0.0), Criticality (L), Known vulnerabilities (0), and Related alerts (6 (Show)). It also shows First seen (Oct 14, 2020 11:56:54) and Last seen (Oct 16, 2020 10:16:45).
- Destination host info:** Details about the destination host, including IP address (Private IP), Host name (pi-dmz), Other host names (Microsoft), Host MAC addresses (Last seen: Oct 16, 2020 10:44:57), Other observed MAC addresses (Rockwell, Ruggedized, Cisco), Role (Terminal server), Other roles (Windows workstation, Terminal client), OS version (Windows 10 or Windows Server 2016), Client protocols (AFP (TCP 445), DCOM (TCP 135), DNS (UDP 53, 5353, 5355), FailedConnection (TCP 21, 71, 98, 110, 389, 8834, 49179, 49195, 54128, 62331, 62532, 62841, 62899), HTTP (TCP 80, 445, 8530), Kerberos (TCP 464), LDAP (TCP 445), MSSQL (TCP 445), NTP (UDP 123), NetBIOS (UDP 137), NoData (TCP 139), NoKnownOrOne (TCP 445), NoKnownOrOne (UDP 442, 1434, 1514, 3389, 32904, 43463, 43724, 43734, 43789, 44102, 44690), OsiIsoPPI (TCP 5450), RDP (TCP 3389), SMB (TCP 445), SMB (UDP 138), SSDP (UDP 1900), SSH (TCP 22), SSL (TCP 443, 445), SunRPC (TCP 445), WS\_Discovery (UDP 3702), FailedConnection (TCP 1542, 1574, 1577, 1585, 2311, 28860, 49690, 49694), NetBIOS (TCP 139), RDP (TCP 3389), SMB (TCP 445), SSL (TCP 5671, 5672)), Server protocols (SMB (TCP 445), SMB (UDP 138), SSL (TCP 5671, 5672)), Labels (vlan\_id=1), Purdue level (3 - Site operations and control), Security Risk (6.0), Operational Risk (2.0), Criticality (L), Known vulnerabilities (0), and Related alerts (922 (Show)). It also shows First seen (Sep 3, 2020 16:47:58) and Last seen (Oct 16, 2020 11:45:43).
- Monitored networks:** A table showing monitored networks, including DMZ LAN with address 10.100.1.0/24 and VLAN IDs any.
- Alert Details:** Shows the ID and name (lan\_cp\_cnv\_c - Communication pattern not whitelisted), Description (Communication pattern not whitelisted; the source and destination hosts are whitelisted in zone communication rule, but not with this combination), and Triggering rule/default action (alert).

## DRAFT

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





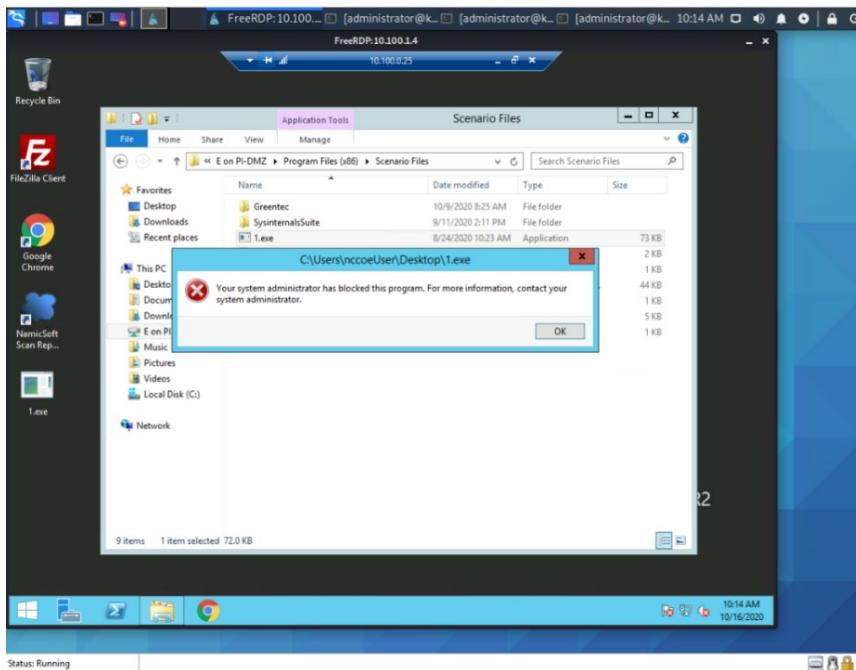
1213 Figure D-19: Details of Alert for RDP Connection into Manufacturing Environment

The screenshot displays the FORESCOUT web-based security management platform. The top navigation bar includes links for Dashboard, Network, Events, Sensors, Settings, and Help, along with a user account icon for 'admin'.

The main content area is divided into several sections:

- Alert details:** Shows the alert ID (203188), timestamp (Oct 16, 2020 10:11:10), sensor name (sensor-bundle-mcoce), detection engine (Communication patterns (LAN CP)), profile (8-TCP communicators), severity (Medium), and source MAC (00:15:5D:02:00:03 (Microsoft)).
- Summary:** Contains monitored networks information, showing two entries: DMZ LAN (10.100.1.0/24) and Lab LAN (10.100.0.0/24), both with 'any' VLAN IDs.
- Source host info:** Details about the source host, including IP address (10.100.1.4 (Private IP)), host name (pi-dmz), other host names (ruggedcom.mgmt.lab), host MAC addresses (00:15:5D:02:D0:D3 (Microsoft)), and other observed MAC addresses (E4:90:99:1B:C5:27 (Redmond), 94:BB:C5:0E:11:9F (Ruggged)), among others.
- Alert Details:** Describes the alert pattern as 'lan\_cp\_cmw\_c - Communication pattern not whitelisted'. It states that communication between source and destination hosts is not whitelisted in some rules but is present here. The triggering rule/default action is set to 'alert'.
- Monitored networks:** A table showing network monitoring details for DMZ LAN and Lab LAN.
- Destination host info:** Details about the destination host, including IP address (10.100.0.25 (Private IP)), host name (nessusvm), other host names (ruggedcom.mgmt.lab), host MAC addresses (00:15:5D:02:D0:D6 (Microsoft)), and other observed MAC addresses (94:BB:C5:0E:11:9F (Ruggged), 7C:0E:CE:67:89:03 (Cisco)), among others.
- Labels:** Includes Purdue level (3-Site operations and control), Security Risk (6.0), Operational Risk (2.0), Criticality (L), Known vulnerabilities (0), and Related alerts (923 (Show)).
- Purdue level:** 3-Site operations and control.
- Security Risk:** 6.0.
- Operational Risk:** 2.0.
- Criticality:** L.
- Known vulnerabilities:** 0.
- Related alerts:** 923 (Show).
- First seen:** Sep 3, 2020 16:47:58.
- Last seen:** Oct 16, 2020 11:48:50.

At the bottom of the interface, there are navigation links for 'Alerts / Alert details' and a copyright notice: 'Copyright (C) 2009-2020 ForeScout (v. 4.1.2)'.

1214 **Figure D-20: Dialog Message Showing 1.exe was Blocked from Executing**1215 **D.2.3 Build 3**1216 ***D.2.3.1 Configuration***

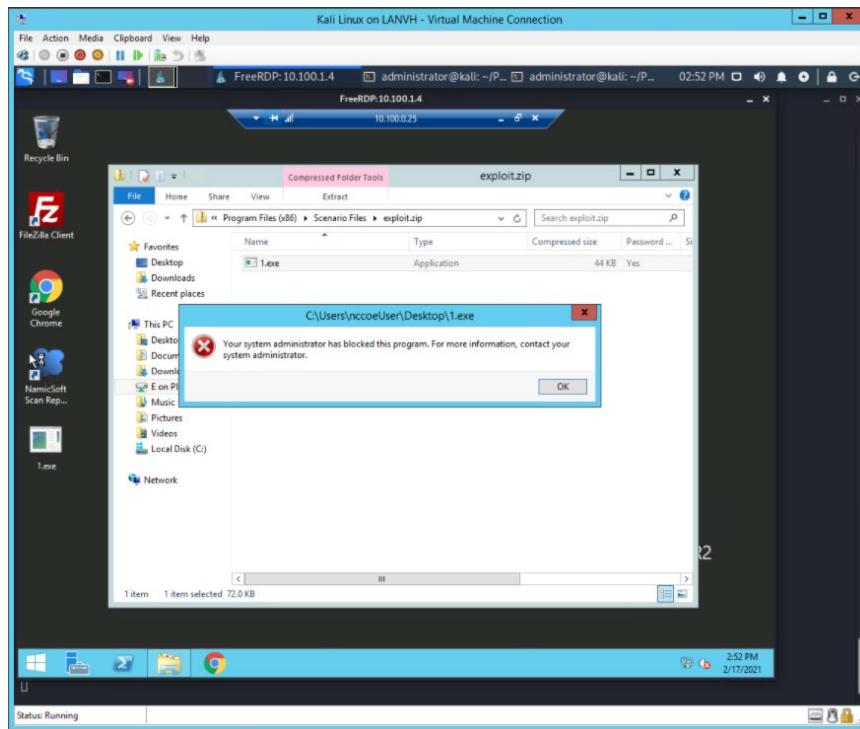
- 1217     ▪ Application Allowlisting: Windows SRP
  - 1218         • Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and Supervisory LAN
- 1219     ▪ Behavior Anomaly Detection: Dragos
  - 1220         • Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

1222 ***D.2.3.2 Test Results***

1223 Windows SRP blocks the attempted execution of 1.exe ([Figure D-21](#)). [Figure D-22](#) shows the alerts  
 1224 generated by Dragos when it detected the remote connection to the target. [Figure D-23](#) depicts the  
 1225 detected RDP session from an external system to the DMZ system. [Figure D-24](#) depicts network scanning  
 1226 alert details. [Figure D-25](#) depicts the RDP session from a DMZ system to the Testbed LAN system.

## DRAFT

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



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

		View	Sever...	ID	Occurred At	Detection Quadrants	Summary	Message	Detected By	Asset IDs	Source IPv4	Dest. IPv4	Other IPv4
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148546	02/17/21, 07:39:49...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 85 (IP: ) connected to Asset...	Network Device Access	85, 96			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148545	02/17/21, 07:37:59...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 85 (IP: ) connected to Asset...	Network Device Access	85, 96			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148544	02/17/21, 07:38:14...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148543	02/17/21, 07:42:57...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 85 (IP: ) connected to Asset...	Network Device Access	85, 96			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148542	02/17/21, 07:42:40...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148541	02/17/21, 07:43:46...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148540	02/17/21, 07:44:33...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148539	02/17/21, 07:40:27...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">0</span>	148538	02/17/21, 07:46:11...	Indicator	Default Community Signature Fired	Activity that meets the criteria of a default co...	Short Community Rules	85, 844			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">0</span>	148537	02/17/21, 07:46:11...	Indicator	Default Community Signature Fired	Activity that meets the criteria of a default co...	Short Community Rules	85, 844			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">0</span>	148536	02/17/21, 07:46:11...	Threat Behavior	RDP Negotiation Request	RDP Negotiation Request	RDP Port Mismatch	85, 844			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148531	02/17/21, 07:36:02...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148530	02/17/21, 07:36:15...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			
<input type="checkbox"/>	<input type="checkbox"/>	<span style="color: #00AEEF;">VIEW</span>	<span style="color: #00AEEF;">1</span>	148529	02/17/21, 07:37:08...	Threat Behavior	Administrative Access to a Network Device D...	Asset: 1807 (IP: ) connected to ...	Network Device Access	1807, 94			

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

The screenshot displays a detailed view of an RDP Negotiation Request event. The main panel shows 'DETECTION INFORMATION' with fields like 'WHAT HAPPENED:', 'OCCURRED AT:', 'COUNT:', 'DETECTED BY:', 'DETECTION QUAD:', 'ACTIVITY GROUP:', 'MITRE ATT&CK FOR ICS TACTIC', 'QUERY-FOCUSED DATASETS', 'PLAYBOOKS:', and 'CASES:'. Below this is a 'COMMUNICATIONS SUMMARY' diagram showing a connection between a 'Windows Server Microsoft Corporation pi-dmz' and an 'Asset' over SSL. A table titled 'ASSOCIATED ASSETS' lists two entries: 'Windows Server' (ID 85) and 'Asset 844'. At the bottom, there's a 'RELATED NOTIFICATIONS' section with a table showing no results.

DRAFT

1230 Figure D-24: Detail for Network Scanning Alert

The screenshot shows a detailed view of a network scanning alert. The top header includes a navigation bar with 'Dashboard', 'Scan', 'Assets', 'Data', 'Notifications', 'Content' (selected), 'Reports', 'Sensors', and 'Admin'. A sidebar on the left lists 'Dashboard', 'Map', 'Assets', 'Data', 'Notifications', 'Content' (selected), 'Reports', 'Sensors', and 'Admin'. The main content area has a title 'Sequential Scan Detected' with ID 148604. It contains sections for 'DETECTION INFORMATION' (WHAT HAPPENED: Sequential ICMP Sweep Detected, OCCURRED AT: 02/17/21, 02:50 PM EST, COUNT: 1, DETECTED BY: Scan Sequential, DETECTION QUAD: Threat Behavior, ACTIVITY GROUP: ELECTRUM, MITRE ATT&CK FOR ICS TACTIC: Discovery), 'ASSOCIATED ASSETS' (Windows Serv 85 Asset 85, 10.100.1.4 other), and 'COMMUNICATIONS SUMMARY' (No Communications Summary). Below these are sections for 'PLAYBOOKS' (Network Address Scanning Activity Detected), 'NOTIFICATION RECORD' (No Associated Record), 'NOTIFICATION COMPONENTS' (No Associated Components), and 'CASES' (No Cases Linked). A 'RELATED NOTIFICATIONS' section shows no results. At the bottom are buttons for 'CREATE A RULE' and 'CREATE CASE'.

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

The screenshot shows a detailed view of RDP session activity. The top header includes a navigation bar with 'Dashboard', 'Scan', 'Assets', 'Data', 'Notifications' (selected), 'Content', 'Reports', 'Sensors', and 'Admin'. A sidebar on the left lists 'Dashboard', 'Map', 'Assets', 'Data', 'Notifications' (selected), 'Content', 'Reports', 'Sensors', and 'Admin'. The main content area has a title 'RDP Negotiation Request' with ID 148547. It contains sections for 'DETECTION INFORMATION' (WHAT HAPPENED: RDP Negotiation Request, OCCURRED AT: 02/17/21, 19:51 UTC, COUNT: 1, DETECTED BY: RDP Port Mismatch, DETECTION QUAD: Threat Behavior, ACTIVITY GROUP: XECUTE, MITRE ATT&CK FOR ICS TACTIC: Command And Control), 'ASSOCIATED ASSETS' (Windows Serv 85 Asset 85, 10.100.1.4 src, Vulnerability S 37 Asset 37, 10.100.0.25 dst), and 'COMMUNICATIONS SUMMARY' (A diagram showing a connection between 'Windows Server, Microsoft Corporation' (10.100.1.4) and 'General Use Desktop, Microsoft Corporation' (10.100.0.25) via ICMP, SSL, and UDP. Below the diagram is a table of communication logs: ICMP (10.100.1.4 to 10.100.0.25, 10.100.0.25 to 10.100.1.4), ICMP (10.100.0.25 to 10.100.1.4), SSL (10.100.1.4 to 10.100.0.25, 10.100.0.25 to 10.100.1.4), and UDP (10.100.1.4 to 10.100.0.25, 10.100.0.25 to 10.100.1.4)). Below these are sections for 'PLAYBOOKS' (No Associated Playbooks), 'NOTIFICATION RECORD' (No Associated Record), 'NOTIFICATION COMPONENTS' (View in Kibana), and 'CASES' (No Cases Linked). A 'RELATED NOTIFICATIONS' section shows no results. At the bottom are buttons for 'CREATE A RULE' and 'CREATE CASE'.

1232 **D.2.4 Build 4**1233 ***D.2.4.1 Configuration***

- 1234     ▪ Application Allowlisting: Carbon Black
- 1235         • Agent installed on systems in the DMZ, Testbed LAN, and Supervisory LAN and configured  
1236         to communicate to the Carbon Black Server.
- 1237     ▪ Behavior Anomaly Detection: Azure Defender for IoT
- 1238         • Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and  
1239         Control LAN.

1240 ***D.2.4.2 Test Results***

1241 Azure Defender for IoT is able to detect the remote access connection to the DMZ as seen in [Figure D-26](#). [Figure D-27](#) shows detection of scanning activity, while [Figure D-28](#) shows details of the scan. The  
1242 RDP connection into the manufacturing environment is seen in [Figure D-29](#). Carbon Black blocks 1.exe  
1243 from executing as shown in [Figure D-30](#).

1245 **Figure D-26: Azure Defender for IoT “info” Event Identified the Remote Access Connection to the DMZ**

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

The screenshot shows the Azure Defender for IoT Event Timeline interface. The left sidebar contains navigation links for Asset Map, Asset Inventory, Alerts (68), Reports, ANALYSIS (Event Timeline, Data Mining, Investigation, Risk Assessment, Attack Vectors), and ADMINISTRATION (Custom Alerts, Users, Forwarding, System Settings). The main area displays the Event Timeline with several events listed:

- Device Connection Detected** (Jan 5, 2021 1:54:03 PM) - Connected devices 10.100.0.62 and 10.100.1.4
- Grouped Events** (Jan 5, 2021 1:54:03 PM) - Connected devices 10.100.0.50 and 10.100.1.4
- Alert Detected** (Jan 5, 2021 1:53:45 PM) - Address scan detected. Scanning address: 10.100.1.4. Scanned subnet: 10.100.0.0/16. Scanned addresses: 10.100.0.10, 10.100.0.11, 10.100.0.12, 10.100.0.13, 10.100.0.14, 10.100.0.15, 10.100.0.16, 10.100.0... (with a 'more' link)
- PCAP file** (link to download)
- Remote Access Connection Established** (Jan 5, 2021 1:53:05 PM) - 24 notifications
- Grouped Events** (Jan 5, 2021 1:53:05 PM)

The bottom status bar shows the date (1/5/2021) and time (2:08 PM).

1247 Figure D-28: Details for the Scanning Alert

The screenshot shows a web-based interface for managing network security alerts. At the top left, it says 'ID: 183'. On the right side, there are several small icons for file operations like download, delete, and refresh. The main title is 'Address Scan Detected' in bold. Below it, the text 'Anomaly | Jan 5, 2021 1:53:44 PM ( 12 minutes ago )' is displayed. The alert message states: 'Address scan detected. Scanning address: 10.100.1.4. Scanned subnet: 10.100.0.0/16. Scanned addresses: 10.100.0.10, 10.100.0.11, 10.100.0.12, 10.100.0.13, 10.100.0.14, 10.100.0.15, 10.100.0.16, 10.100.0.17, 10.100.0.18, 10.100.0.19... It is recommended to notify the security officer of the incident.' Below this, there is a small icon of a document with a list. To its right, the text 'PI-DMZ' is visible. Under the heading 'Manage this Event', there is a bulleted list: '● Multiple scans in the network can be an indication for a new device in the network, a new functionality of an existing device, improper configuration of an application (for example: due to a firmware update, or a new deployment), or malicious activity in the network, such as reconnaissance.' and '● During the reconnaissance phase, a tool usually collects system configuration data, including data about any installed antivirus applications and steals data on the computer systems themselves, which is then sent back to the attackers.' At the bottom right, there are two blue buttons labeled 'Learn' and 'Acknowledge'.

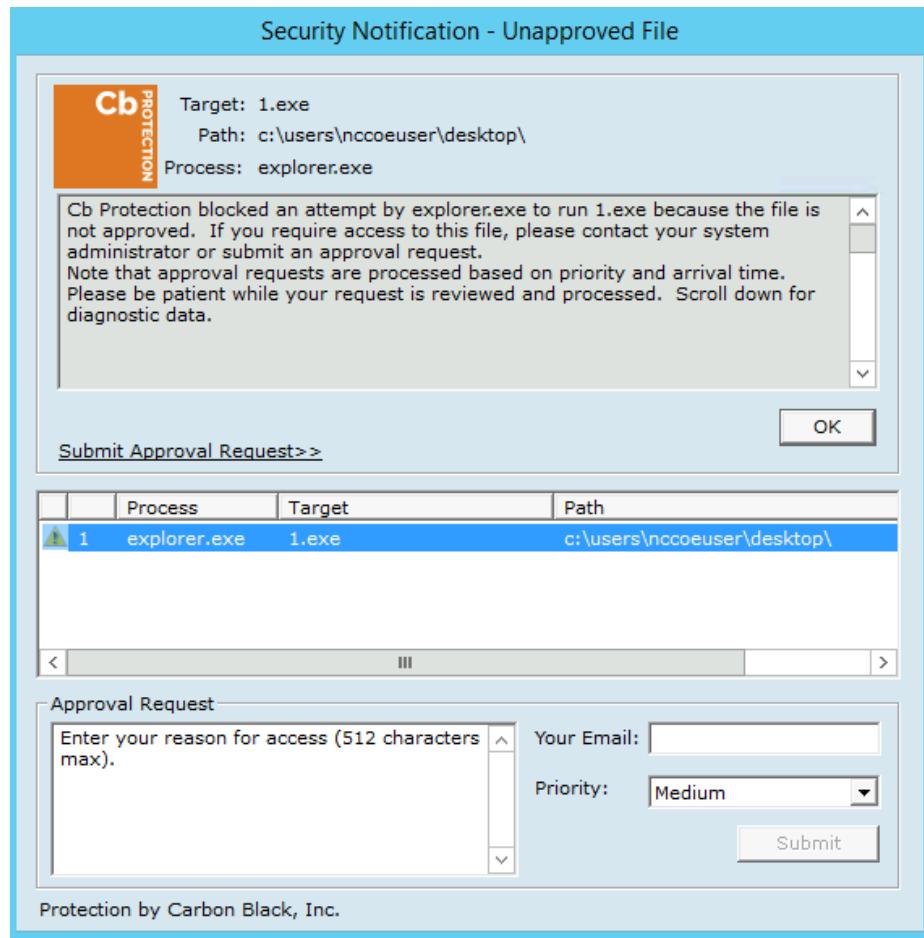
1248 **Figure D-29: Detection of RDP Connection into the Manufacturing Environment**

The screenshot shows the Azure Defender for IoT interface with the 'Event Timeline' tab selected. The timeline displays the following events:

- File Transfer Detected** at 14:04:19 on Jan 5, 2021. Details: HTTP File transfer from client IP: [REDACTED] to Server: [REDACTED]. Content type application/octet-stream. Status: Notice.
- Remote Access Connection Established** at 13:59:30 on Jan 5, 2021. Details: Connection detected from ' [REDACTED]' to ' [REDACTED]' using Remote Desktop. Status: Info.
- File Transfer Detected** at 13:58:08 on Jan 5, 2021. Details: HTTP File transfer from client IP: [REDACTED] to Server: [REDACTED]. Content type application/vnd.ms-cab-compressed. Status: Notice.
- Device Connection Detected** at 13:56:03 on Jan 5, 2021. Details: Connected devices [REDACTED] and [REDACTED]. Status: Info. A blue circle with the number '3' indicates three grouped events.

The left sidebar includes links for Asset Map (95), Asset Inventory, Alerts (68), Reports, ANALYSIS (Event Timeline, Data Mining, Investigation, Risk Assessment, Attack Vectors), ADMINISTRATION (Custom Alerts, Users, Forwarding, System Settings), and the footer notes Version 3.1.1.

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

1250 **D.3 Executing Scenario 3: Protect Host from Malware via Remote Access  
Connections**

1252 An authorized user with an authorized remote workstation, infected with a worm-type malware,  
 1253 connects via remote access capabilities to the manufacturing environments. The malware on the remote  
 1254 host attempts to scan the manufacturing environment to identify vulnerable hosts. The expected result  
 1255 is that the remote access tools effectively stop the worm-type malicious code from propagating to the  
 1256 manufacturing environment from the infected remote workstation.

1257 **D.3.1 Build 1**1258 **D.3.1.1 Configuration**

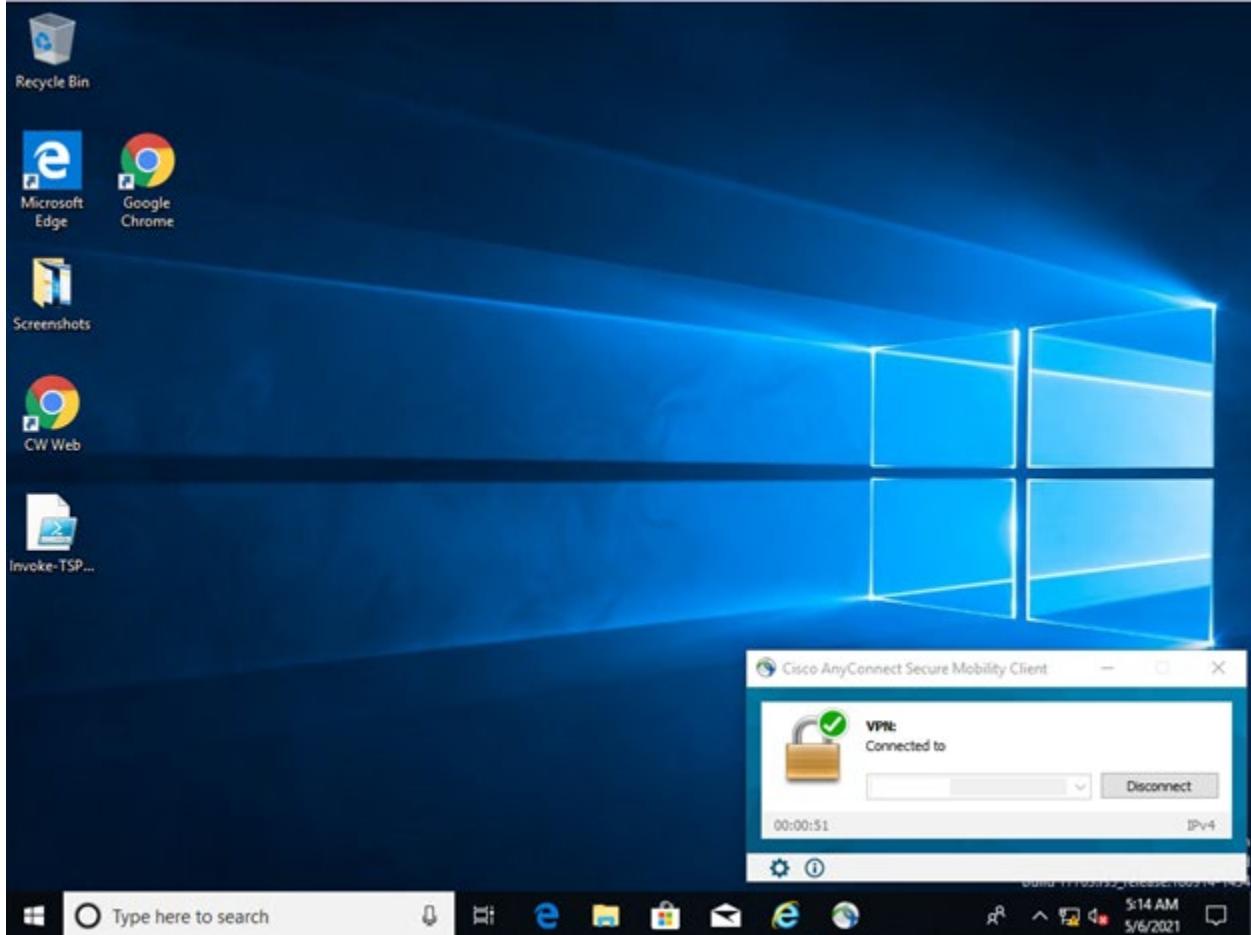
- 1259     ■    Remote Access: Cisco VPN
  - 1260         ●    Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- 1261     ■    User Authentication/User Authorization: ConsoleWorks

1262       • Configured for access PCS environment.

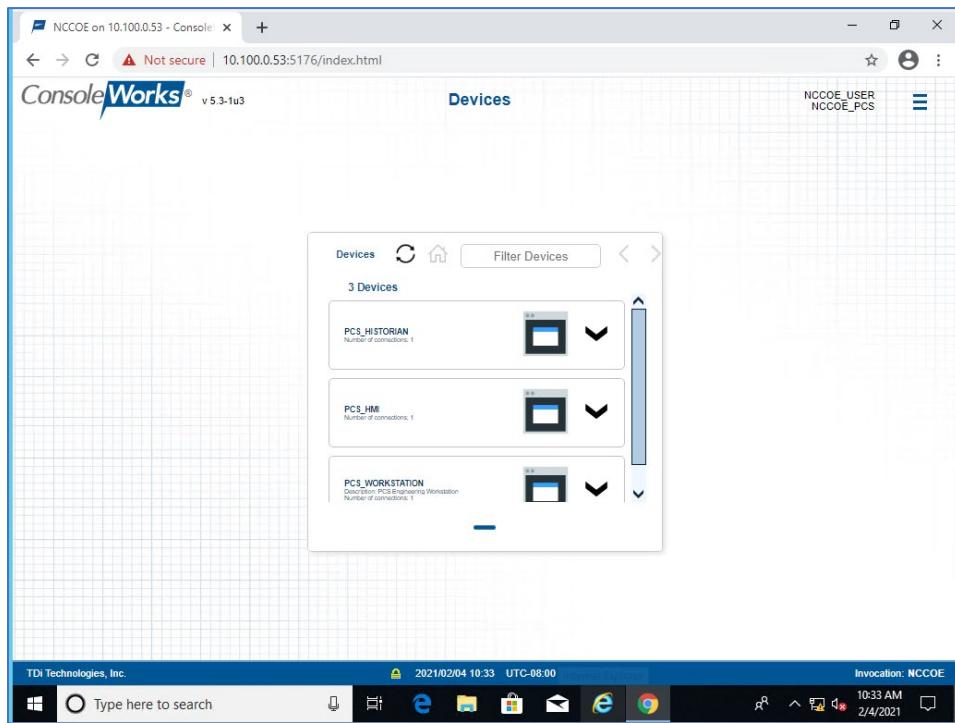
1263 *D.3.1.2 Test Results*

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

1268 **Figure D-31: Secured VPN Connection to Environment with Cisco AnyConnect**



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



1270 **D.3.2 Build 2**

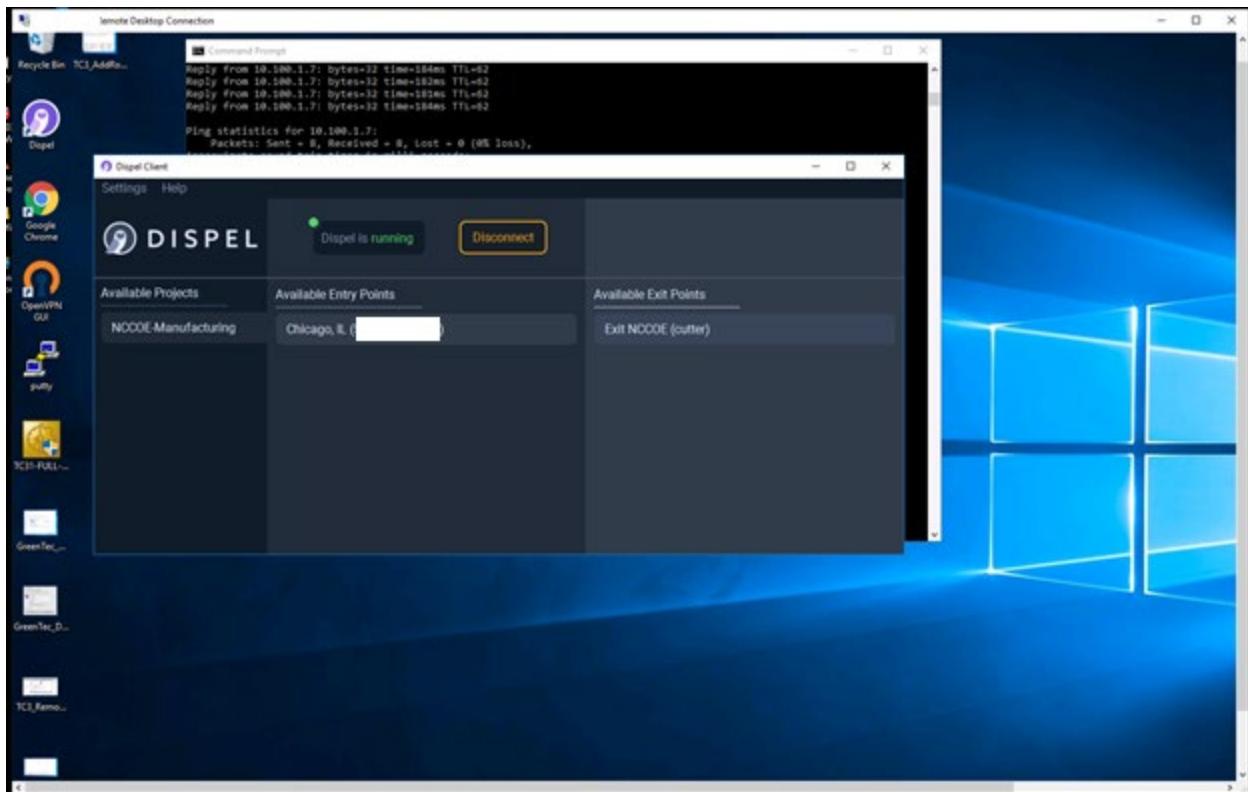
1271 *D.3.2.1 Configuration*

- 1272   ■ Remote Access, User Authentication/User Authorization: Dispel
- 1273       ● Dispel VDI is configured to allow authorized users to access PCS environment through the  
1274       Dispel Enclave to the Dispel Wicket.

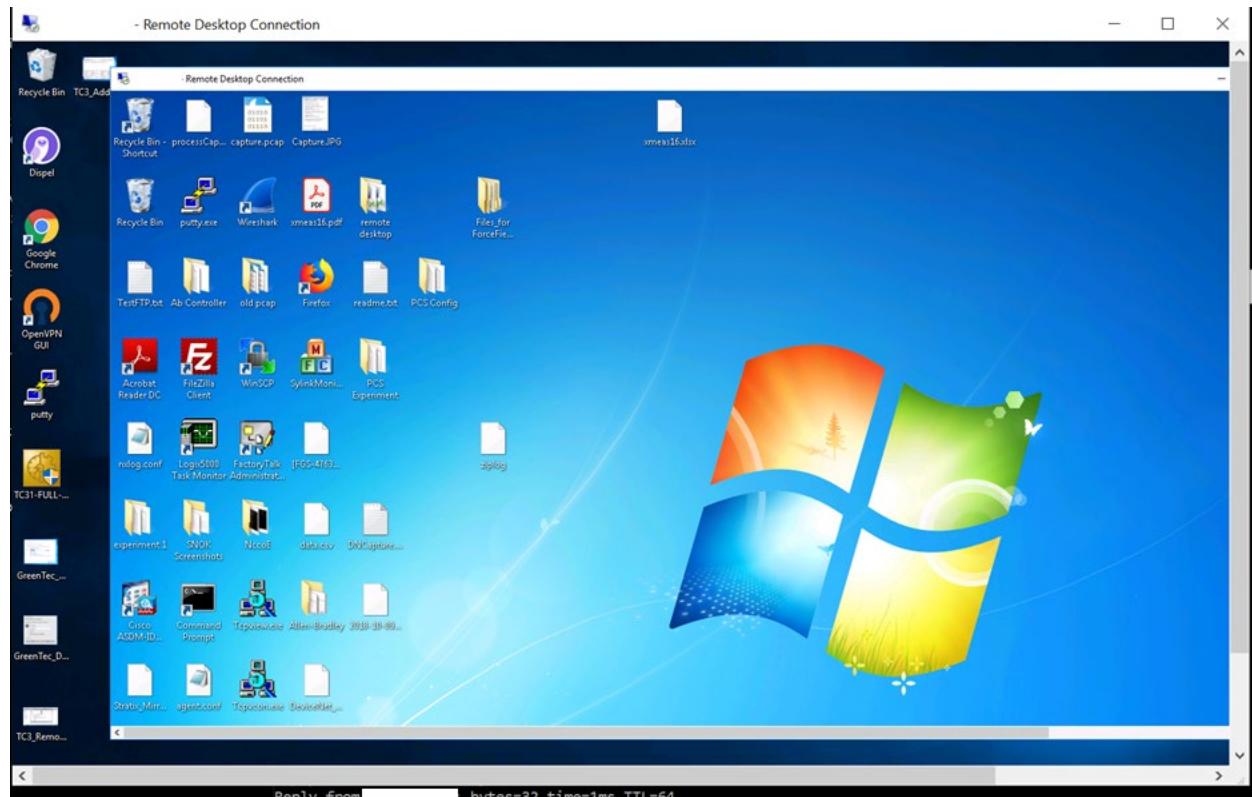
1275 *D.3.2.2 Test Results*

1276 The user connects to the Dispel VDI as shown in [Figure D-33](#) and then connects to the PCS workstation  
1277 as shown in [Figure D-34](#). Once a connection to the NCCOE environment was established, the simulated  
1278 worm attack was executed on the remote PC to scan the target network. The scan was successfully  
1279 blocked by the Dispel VDI configuration.

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



1281 **Figure D-34: Nested RDP Session Showing Dispel Connection into the PCS Workstation**



1282 **D.3.3 Build 3**

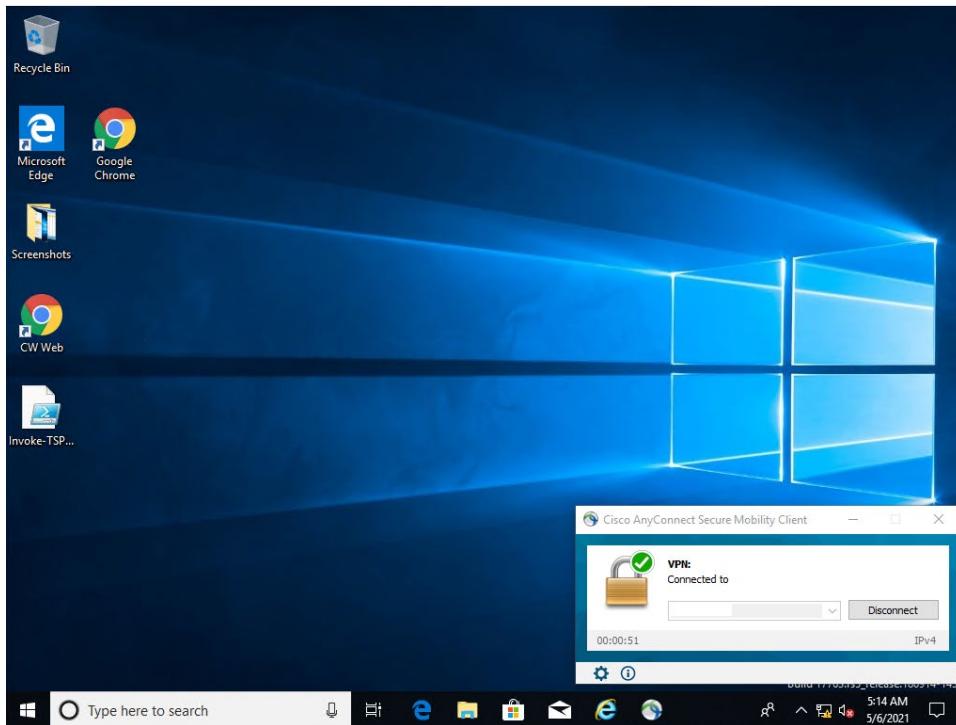
1283 ***D.3.3.1 Configuration***

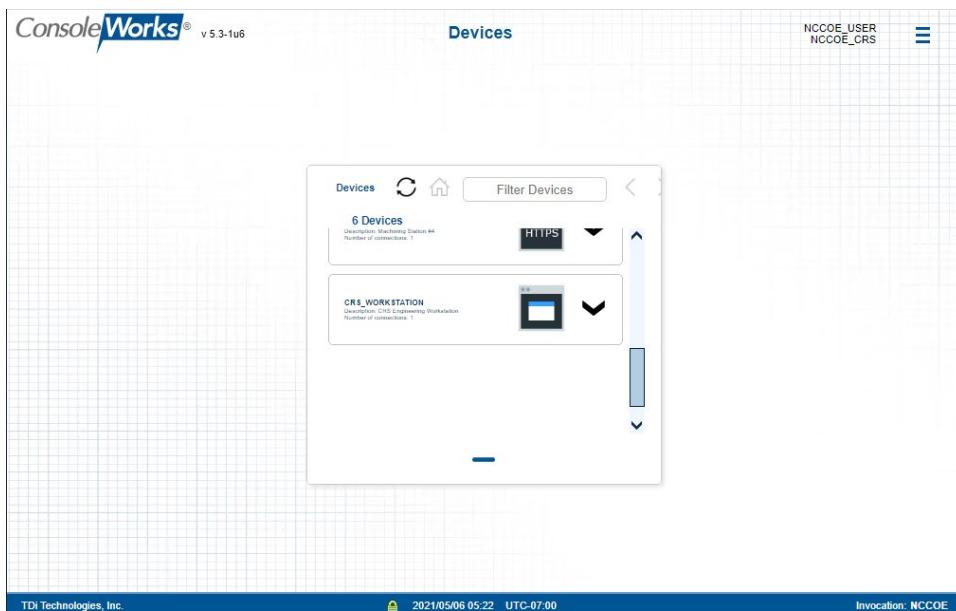
- 1284     ■    Remote Access: Cisco VPN
  - 1285         ●    Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- 1286     ■    User Authentication/User Authorization: ConsoleWorks
  - 1287         ●    Configured for access CRS environment.

1288 ***D.3.3.2 Test Results***

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

1293 **Figure D-35: VPN Connection to Manufacturing Environment**



1294 **Figure D-36: Remote Access is Being Established Through ConsoleWorks**1295 **D.3.4 Build 4**1296 ***D.3.4.1 Configuration***

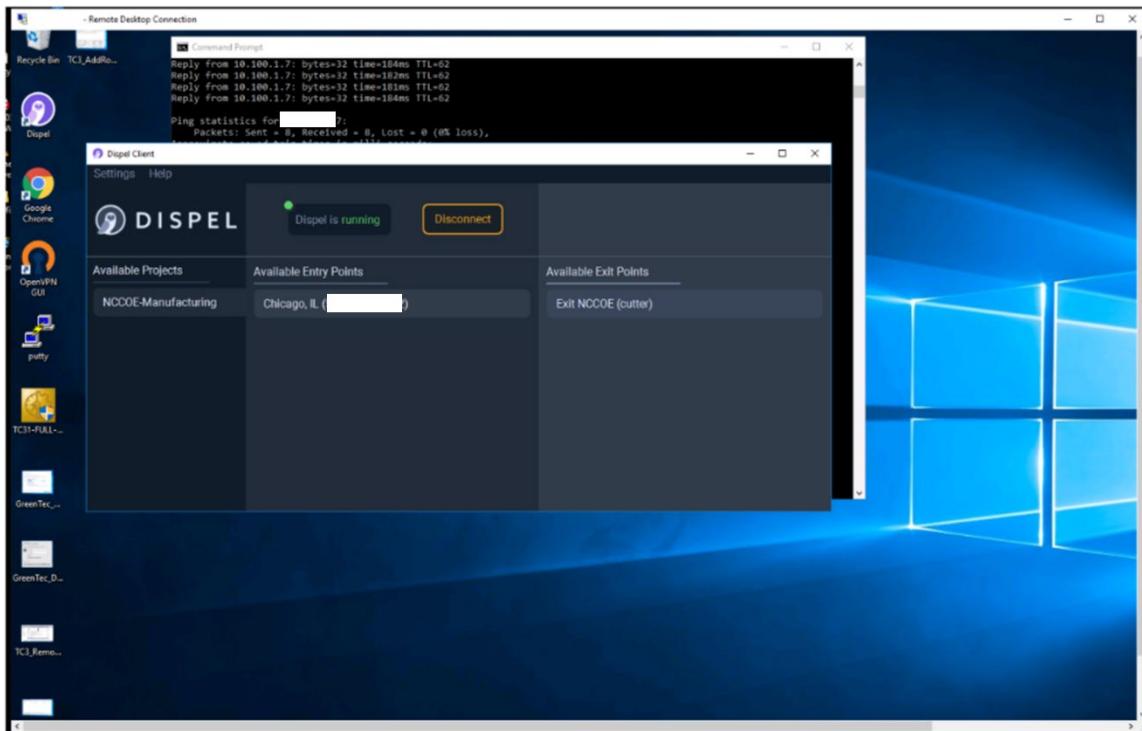
- 1297     ▪    Remote Access, User Authentication/User Authorization: Dispel
  - 1298         •    Dispel VDI is configured to allow authorized users to access the PCS environment through the Dispel Enclave to the Dispel Wicket.

1300 ***D.3.4.2 Test Results***

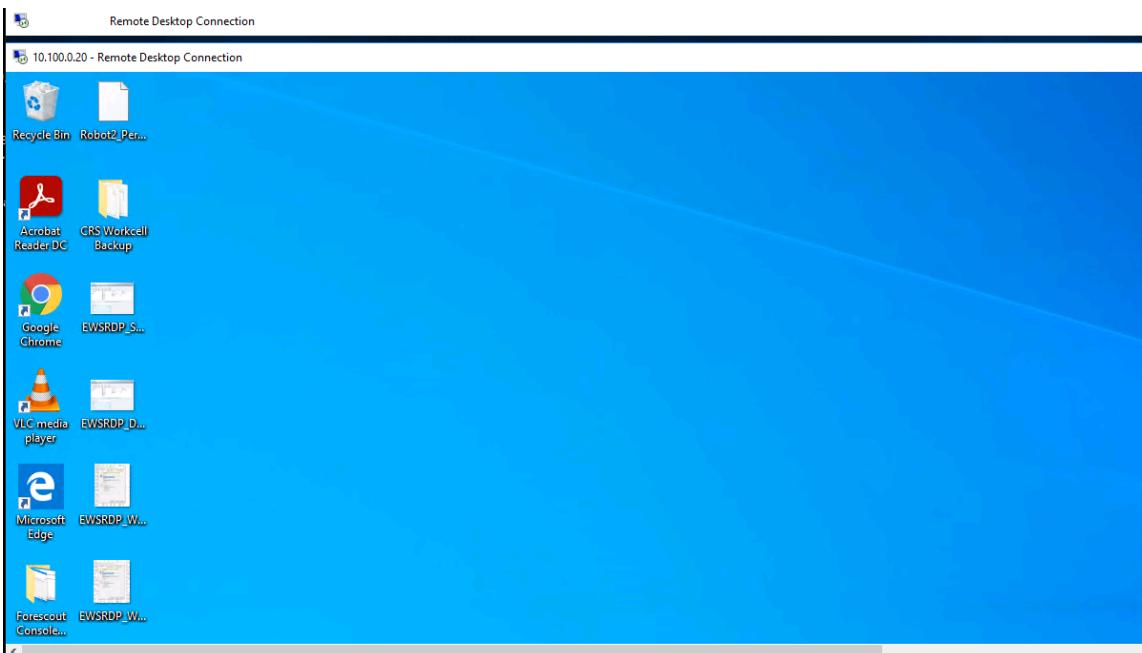
1301 [Figure D-37](#) shows the Dispel VDI desktop, which allows a connection to the CRS workstation in  
 1302 [Figure D-38](#). Once a connection to the NCCOE environment was established, the simulated worm attack  
 1303 was executed on the remote PC to scan the target network. The scan was successfully blocked by the  
 1304 use of the Dispel VDI.

DRAFT

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



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



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

1309     An authorized user copies downloaded software installation files and executable files from a shared  
1310     network drive to a workstation. The user attempts to execute or install the unauthorized software on  
1311     the workstation. The expected result is that the application allowlisting tool prevents execution or  
1312     installation of the software. Also, the behavioral anomaly detection identifies file transfer activity in the  
1313     manufacturing environment.

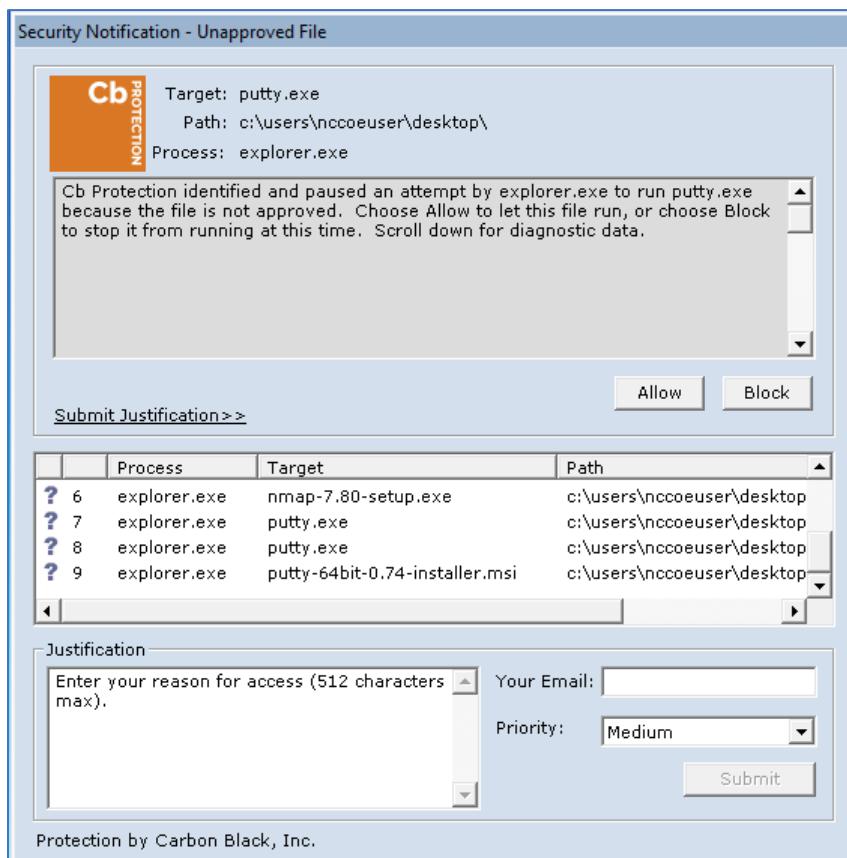
1314     **D.4.1 Build 1**

1315         ***D.4.1.1 Configuration***

- 1316             ▪ Application Allowlisting: Carbon Black
- 1317                 • Agent installed on systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2 and configured  
1318                 to communicate to the Carbon Black Server.
- 1319             ▪ Behavior Anomaly Detection: Tenable.ot
- 1320                 • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

1321         ***D.4.1.2 Test Results***

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

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

DRAFT

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

The screenshot shows the Tenable.ot web interface. The left sidebar includes sections for Events (All Events, Configuration Events, SCADA Events, Network Threats, Network Events), Policies, Inventory (Controllers, Network Assets), Risk, Network, Groups, Reports, and Local Settings. The main content area displays an alert titled "All Events" for log ID 19333. The alert details an "Unauthorized Conversation" from "SMB communication from Eng Station..." (HMI) to "GreenTec" (172.16.1.4) at 02:10:04 PM on April 14, 2021. The severity is Low and it is Not resolved. The alert message states: "A conversation in an unauthorized protocol has been detected". It provides source and destination information: SOURCE NAME HMI, SOURCE ADDRESS 172.16.1.4, DESTINATION NAME GreenTec, DESTINATION ADDRESS 10.100.1.7, PROTOCOL SMB (tcp/445), PORT 445, and PROTOCOL GROUP In SMB. A "Why is this important?" section explains that conversations in unauthorized protocols may indicate suspicious traffic. A "Suggested Mitigation" section advises checking if the communication is expected and adjusting policy conditions if necessary. The top right shows the time as 02:10 PM on Wednesday, April 14, 2021, and the user as NCCOE User.

1327  
1328 **Figure D-41: Tenable.ot Alert Details of the SMB Connection Between the HMI and the network file system (NFS) Server in the DMZ**

The screenshot shows the Tenable.ot web interface. The left sidebar includes sections for Events (All Events, Configuration Events, SCADA Events, Network Threats, Network Events), Policies (selected), Inventory (Controllers, Network Assets), Risk, Network, Groups, Reports, and Local Settings. The main content area displays a policy titled "SMB communication from Eng Station Detected" under the "Unauthorized Conversation" category. The "Details" tab is selected, showing the "Policy Definition" section with the following details:

- NAME: SMB communication from Eng Station Detected
- SOURCE: (In ENG. Stations) or (In HMIs)
- DESTINATION / AFFECTED ASSET: In Any Asset
- PROTOCOL GROUP: In SMB
- SCHEDULE: In Any Time

The "Policy Actions" section shows:

- SEVERITY: Low
- SYSLOG
- EMAIL
- DISABLE AFTER HIT

The "General" section shows:

- CATEGORY: Network Events
- DISABLED: Enabled

A "STATUS" button and an "Actions" dropdown are visible in the top right corner. The top right shows the time as 02:10 PM on Wednesday, April 14, 2021, and the user as NCCOE User.

1329 **D.4.2 Build 2**

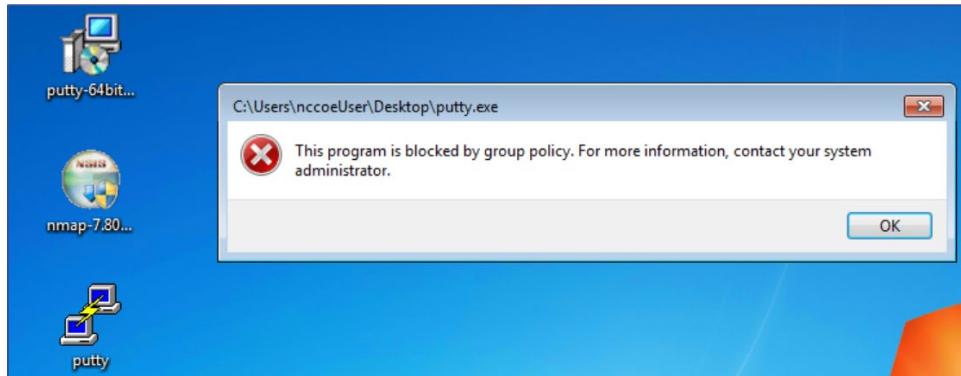
1330 **D.4.2.1 Configuration**

- 1331     ■ Application Allowlisting: Windows SRP
- 1332         ● Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1334     ■ Behavior Anomaly Detection: eyeInspect
- 1335         ● Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

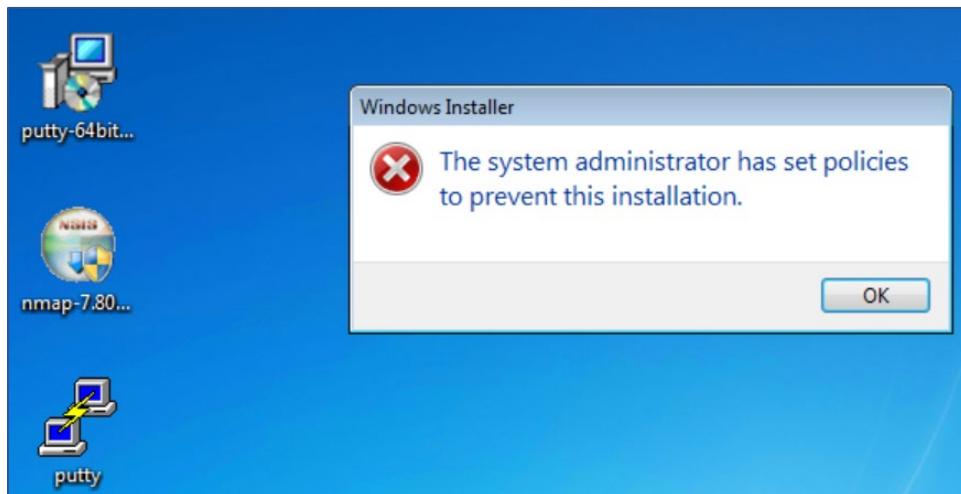
1336 *D.4.2.2 Test Results*

1337 With Windows SRP enabled, putty.exe is not allowed to execute because it is not a permitted  
1338 application under group policy, as shown in Figure D-42. Windows SRP also blocks the user's attempt to  
1339 run putty-64bit-0.74-installer.msi. (Figure D-43). Forescout detected the file transfer activity ([Figure D-  
1340 44](#)). [Figure D-45](#) shows a detailed description of the alert that was generated for the file transfer activity.

1341 **Figure D-42: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration**



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



DRAFT

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

The screenshot shows the Forescout web interface under the 'Alerts' tab. A single alert is listed in the main pane. The alert details are as follows:

Timestamp	Event name(s)	Sensor	Engine	Profile	Status	Severity	Source address	Destination address	Dest. Port	L7 Proto	Case ID
Oct 7, 2020 09:12:30	Communication pattern ...	sensor-B...	Com...	8-TCP co...	Not analyzed	Yellow M	172.16.1.4	10.100.1.7	0	(Port 445) SMB	130391

On the left sidebar, there are several filter options under 'Alert Filters':

- From date X to 30 days after
- From date X to Y days before
- Excluding event type ID
- By monitored network
- Excluding profile
- Excluding src MAC
- Excluding dst MAC
- Excluding src IP
- Excluding dst IP
- Excluding dst port
- Excluding L2 protocol
- By L3 protocol

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

The screenshot shows the 'Alert details' page for the alert from Figure D-44. The summary pane on the left contains the following information:

Alert ID	130391
Timestamp	Oct 7, 2020 09:12:30
Sensor name	sensor-Bundle-ecose
Detection engine	Communication patterns (SAN CP)
Profile	8-TCP communications
Severity	Yellow Medium
Source MAC	0CC47A670A4A7 (SuperMicro)
Destination MAC	E480B93B0C21 (Rockwell)
Source IP	172.16.1.4 (ipg-012304)
Destination IP	10.100.1.7 (greenie server)
Source port	49783
Destination port	445
U2 proto	Ethernet
U3 proto	IP
U4 proto	TCP
U7 proto	SMB
TCP stream opened in hot start mode	N/A
Status	Not analyzed
Labels	
User notes	

The source host info and alert details panes on the right provide more detailed information about the communication pattern.

## 1345 **D.4.3 Build 3**

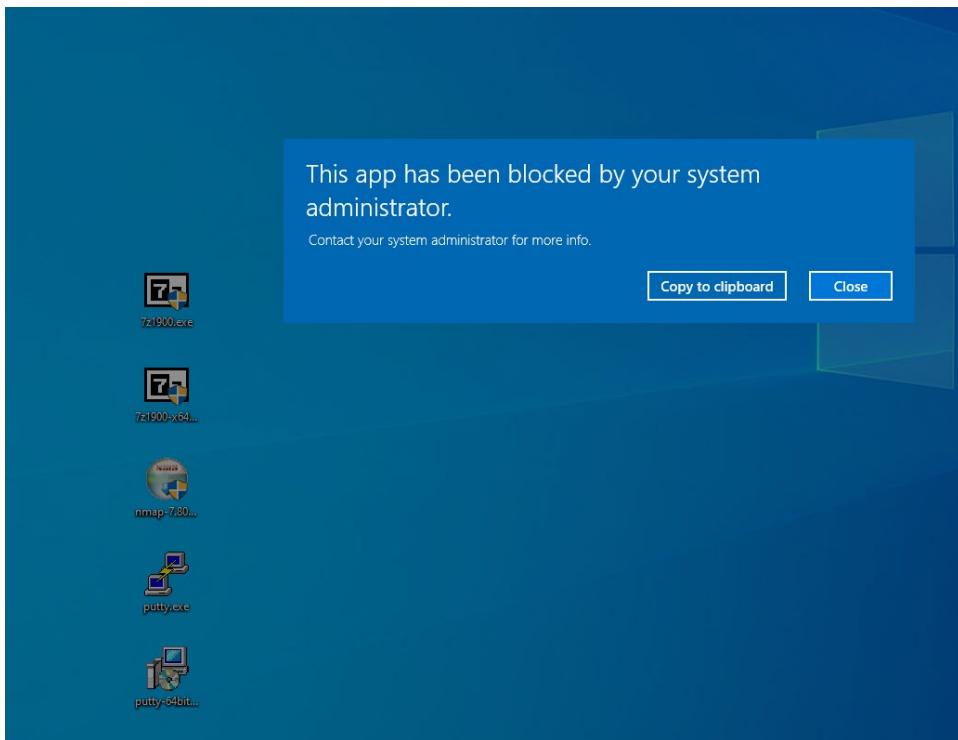
### 1346 *D.4.3.1 Configuration*

- 1347     ■ Application Allowlisting : Windows SRP
  - 1348         ● Settings are applied to systems in the DMZ, Testbed LAN, and Supervisory LAN
- 1349     ■ Behavior Anomaly Detection: Dragos
  - 1350         ● Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

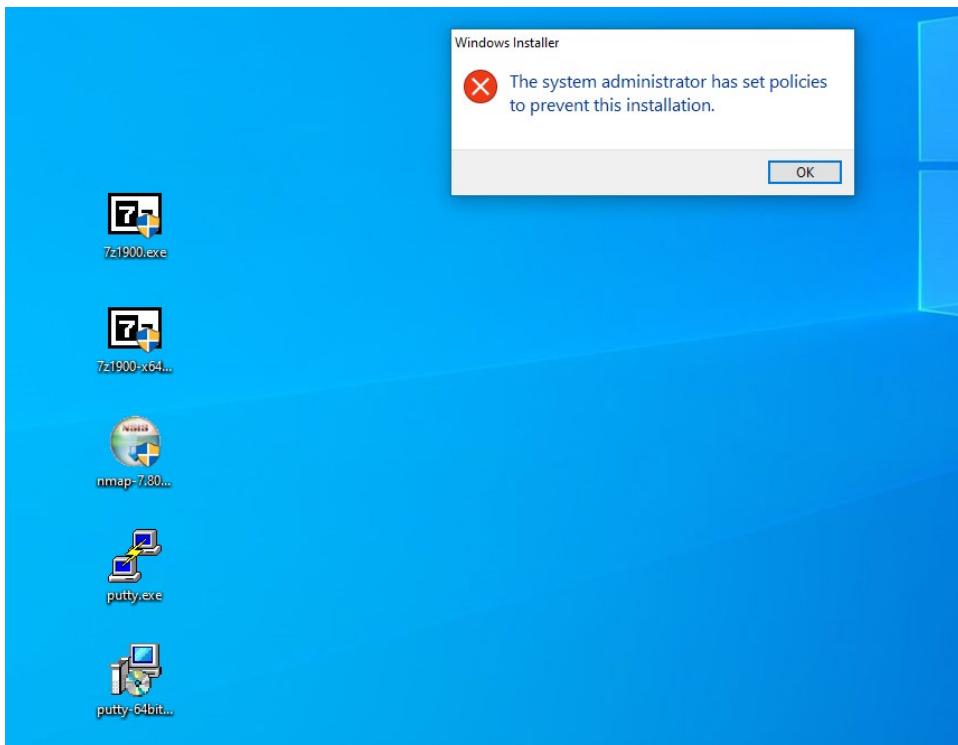
### 1352 *D.4.3.2 Test Results*

- 1353 With Windows SRP enabled, putty.exe is not allowed to execute because it is not a permitted application under group policy, as shown in [Figure D-46](#). Windows SRP also blocks the user's attempt to run putty-64bit-0.74-installer.msi ([Figure D-47](#)). Dragos detected the file transfer activity ([Figure D-48](#)). [Figure D-49](#) shows a detailed description of the alert that was generated for the file transfer activity.

1357 **Figure D-46: Putty.exe is Not Permitted to Run Based on the Windows SRP Configuration**



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



## DRAFT

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

The screenshot shows the Dragos Notification Manager interface. On the left, there is a sidebar with navigation links: Dashboard, Map, Assets, Data, Notifications (selected), Context, Reports, Sensors, and Admin. The main area is titled "Notification Manager" and contains two tabs: "ASSET NOTIFICATIONS" and "SYSTEM ALERTS". The "ASSET NOTIFICATIONS" tab is active, displaying a list of 28 notifications from February 17, 2021, at 19:43 UTC to 21:00 UTC. The columns include: View, Severity, ID, Occurred At, Type, Summary, Message, Detected By, Asset ID, Source IPv4, Dest. IPv4, and Other IPv4. The notifications are mostly of type "Communication" and involve assets downloading files with suspicious hashes. The "SYSTEM ALERTS" tab is visible but empty. The top right corner shows a user icon and the text "admin".

View	Severity	ID	Occurred At	Type	Summary	Message	Detected By	Asset ID	Source IPv4	Dest. IPv4	Other IPv4
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148575	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148574	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148573	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148572	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2.20	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148571	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2.20	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148570	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148569	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148568	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148567	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148566	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2.20	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148565	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_raw_size	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148564	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2.20	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148563	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148562	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148561	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148560	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 5ba...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148559	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2.20	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148558	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2...	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148557	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	151, 96	10.100.1.7	192.168.0.2.20	
<a href="#">VIEW</a>	<span style="color: green;">INFO</span>	148556	02/17/21, 19:43 UTC	Communication	A Downloaded file hit on: suspicious_pe_sections	Asset 96 downloaded a file with sha256 hash of 43d...	File Transfer of Suspicious PE	80, 96	10.100.1.7	192.168.0.2...	

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

**Detection Information:**

- WHAT HAPPENED: Asset 80 downloaded a file with sha256 hash of c3d5460ea7b99c3f6198fa5b7749f5c27176a65190ba0119e511a30c1ca from 80 which matched the suspicious\_raw\_size file.
- OCCURRED AT: 02/17/21, 19:43 UTC
- COUNT: 1
- DETECTED BY: File Transfer of Suspicious PE
- DETECTION QUAD: Thread Behavior
- ACTIVITY GROUP: None
- ICS CYBER KILLCHAIN STEP: Stage 1 - Delivery
- MITRE ATT&CK FOR ICS TACTIC: External Movement
- NOTIFICATION RECORD: View in Killbase
- NOTIFICATION COMPONENTS: View in Killbase
- CASES: No Cases Linked

**Associated Assets:**

Name	Type	ID	Dir.
16.190.1.7	General Use D	80	Asset 80
192.168.0.2	Router	96	Asset 96

**Communications Summary:**

Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
SMB	10.100.0.20	-	10.100.1.7	-	42.9 KB	43.0 KB
NTLM	10.100.0.20	-	10.100.1.7	-	120.1 KB	121.7 KB
DCE RPC	10.100.0.20	-	10.100.1.7	-	2.1 MB	65.5 MB

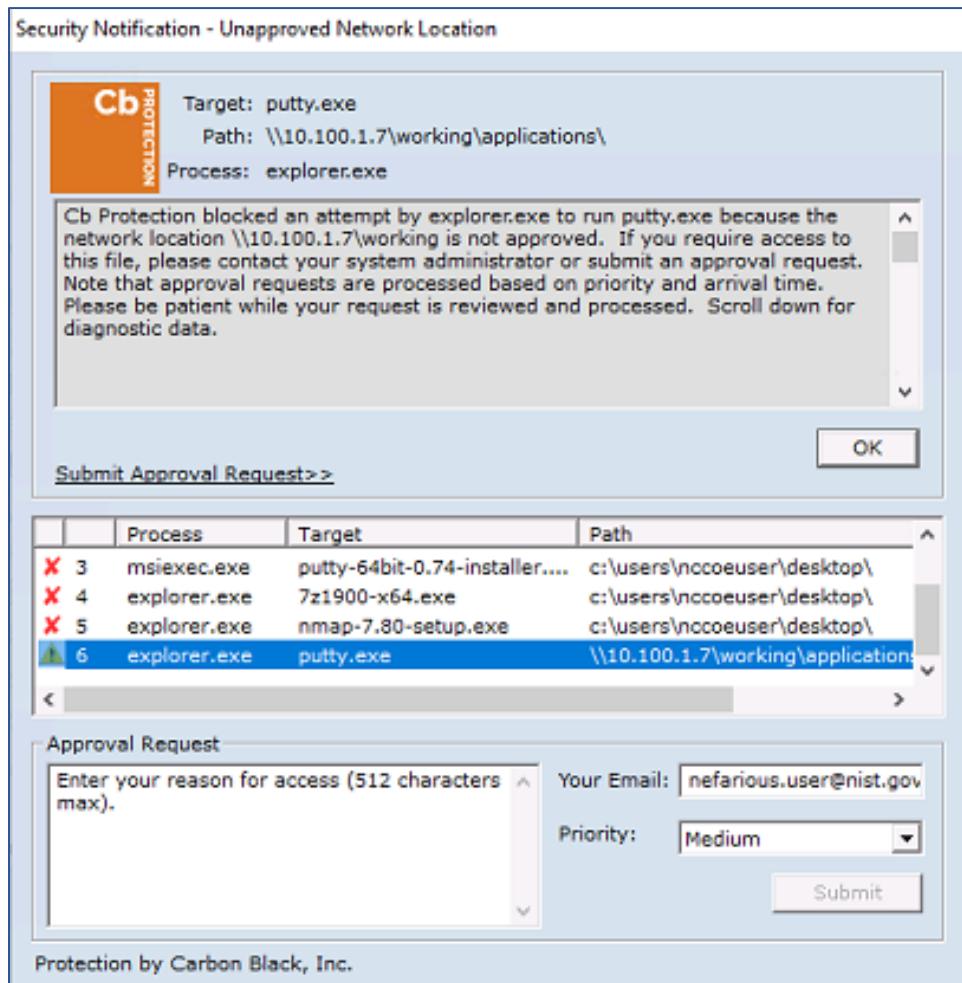
1361 **D.4.4 Build 4**1362 **D.4.4.1 Configuration**

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

1369 **D.4.4.2 Test Results**

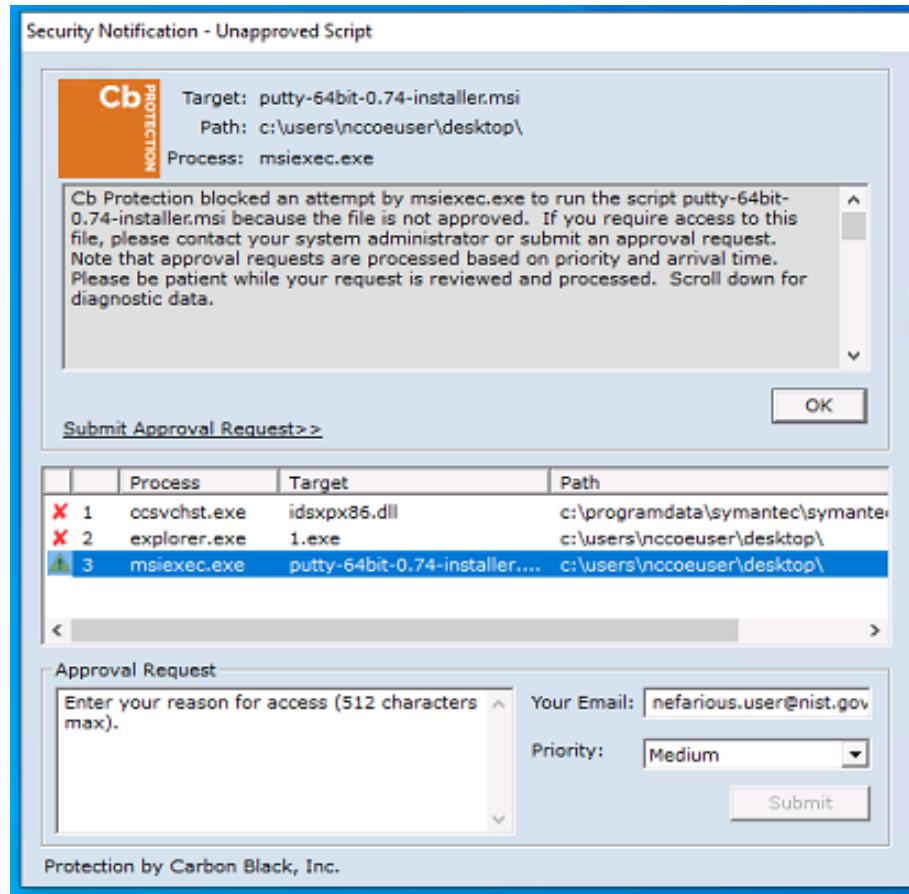
1370 Carbon Black was able to block the execution of putty.exe ([Figure D-50](#)) and the installation of putty-64bit-0.74-installer.msi ([Figure D-51](#)). [Figure D-52](#) is the alert dashboard for Azure Defender for IoT that shows new activity has been detected. The detailed alert in [Figure D-53](#)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

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



## DRAFT

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

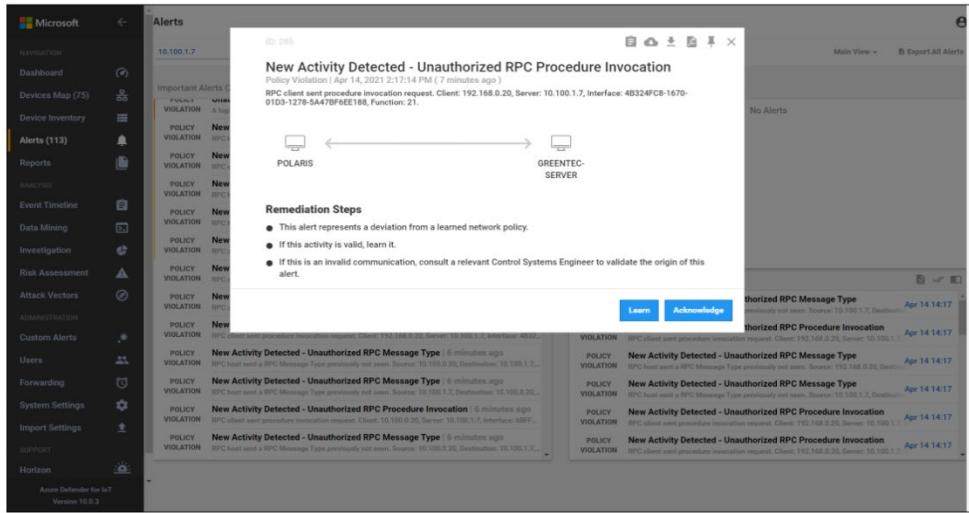


1377 Figure D-52: Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity

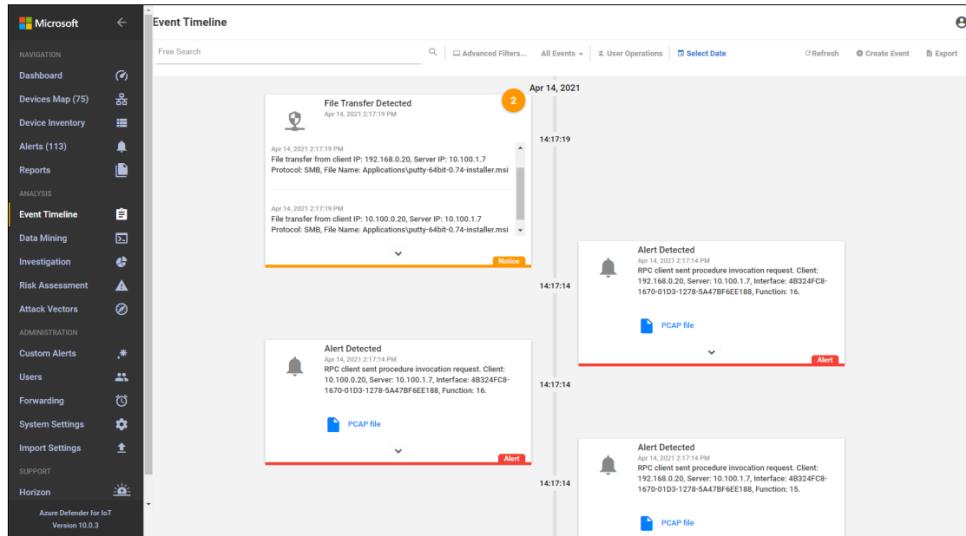
The screenshot shows the Azure Defender for IoT Alert Dashboard. The left sidebar includes navigation links such as Dashboard, Devices Map, Device Inventory, Reports, ANALYSIS, Event Timeline, Data Mining, Investigation, Risk Assessment, Attack Vectors, ADMINISTRATION, Custom Alerts, Users, Forwarding, System Settings, Import Settings, SUPPORT, and Horizon. The main area displays a list of alerts under 'Important Alerts (26)' and 'Recent Alerts (26)'. Both sections show multiple entries for 'New Activity Detected - Unauthorized RPC Message Type' and 'New Activity Detected - Unauthorized RPC Procedure Invocation' occurring over the last 6 minutes.

DRAFT

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



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



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

1382 An authorized individual with physical access connects an unauthorized device on the manufacturing  
1383 network and then uses it to connect to devices and scan the network. The expected result is behavioral  
1384 anomaly detection identifies the unauthorized device.

1385 D.5.1 Build 1

1386 *D.5.1.1 Configuration*

- 1387     ▪ Behavior Anomaly Detection: Tenable.ot
- 1388         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

1389 *D.5.1.2 Test Results*

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

DRAFT

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

The screenshot shows the Tenable.ot web interface. The left sidebar contains navigation links for Events, Configuration Events, SCADA Events, Network Threats, Network Events, Policies, Inventory, Controllers, Network Assets, Risk, Network (Network Summary, Packet Captures, Conversations, Assets Map), Groups, Reports, and Help. The main content area is titled "All Events" with a search bar for "172.16.1.30". A table lists events with columns: LOG ID, TIME, EVENT TYPE, SEVERITY, POLICY NAME, SOURCE ASSET, and SOURCE ADDRESS. One event is highlighted: Event 9069 from 02:42:23 PM on Jan 29, 2021, with the type "New asset discovered", severity "Low", policy "New Asset Discovered", source asset "Endpoint #61", and source address "172.16.1.30". Below the table, a detailed view for Event 9069 shows the following information:

Details	
Affected Assets	A new asset has been detected in the network by Tenable.ot
Policy	SOURCE NAME: Endpoint #61
Status	SOURCE ADDRESS: 172.16.1.30
DESTINATION NAME	It is important to know what assets exist in your network. New assets can indicate unexpected network connections, third party connectivity or potential threats to the network.
DESTINATION ADDRESS	Make sure that the asset is expected to be at this IP and is familiar to other asset owners. If you are not familiar with the asset, contact the relevant network admin to check if

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

The screenshot shows the Tenable.ot web interface. The left sidebar contains navigation links for Events, Configuration Events, SCADA Events, Network Threats, Network Events, Policies, Inventory, Controllers, Network Assets, Risk, Network (Network Summary, Packet Captures, Conversations, Assets Map), Groups, Reports, and Help. The main content area is titled "All Events" with a search bar for "SSH". A table lists events with columns: LOG ID, TIME, EVENT TYPE, SEVERITY, POLICY NAME, SOURCE ASSET, and SOURCE ADDRESS. Two events are listed: Event 9086 from 03:10:50 PM on Jan 29, 2021, and Event 9085 from 03:06:01 PM on Jan 29, 2021, both with the type "Unauthorized Conversation", severity "Medium", and policy "SSH Communications to Engineering S...". Below the table, a detailed view for Event 9086 shows the following information:

Details	
Source	A conversation in an unauthorized protocol has been detected
Destination	SOURCE NAME: Endpoint #61
Policy	SOURCE ADDRESS: 172.16.1.30
Status	DESTINATION NAME: Stratix5700 VLAN1
	Conversations in unauthorized protocols may indicate suspicious traffic. Some assets are not expected to communicate in non-standard protocols and any deviation from the
	Check if this communication is expected. If it is unexpected, then review the Policy conditions so that Events aren't generated for similar communications in the future. If this

## 1396 **D.5.2 Build 2**

### 1397 **D.5.2.1 Configuration**

- 1398     ▪ Behavior Anomaly Detection: eyelnspect

- 1399         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

### 1400 **D.5.2.2 Test Results**

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

DRAFT

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

The screenshot shows the Forescout alert details interface. The alert ID is 169436, timestamped Oct 13, 2020 13:39:55. The source host info includes an IP address of 172.16.2.30 (Private IP), host name 'stochastic', and host MAC addresses 00:09:5B:AA:E9:29 (Netgear). Other observed MAC addresses include E4:90:69:3B:C2:C3 (Rockwell) and E4:90:69:3B:C2:C0 (Rockwell). The role is SNMP manager, and other roles include Windows workstation, Web server, Terminal client. Client protocols listed are DNS (UDP 53), FailedConnection (TCP 80, 7000, 7001, 7002, 7004, 7005, 7006, 7007, 7008, 7009, 52311), LDAP (UDP 389), and NotKnownOne (UDP 443, 19000). The alert details show an ID and name 'lan\_cp\_enw\_c - Communication pattern not whitelisted' and a description stating 'Communication pattern not whitelisted: the source and destination hosts are whitelisted in some communication rule, but not with this combination'. The triggering rule/default action is set to 'alert'.

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

This screenshot shows a portion of the Forescout alert timeline. It displays a single event entry for an SSH connection. The event details are: Date: Oct 13, 2020, Time: 13:24:58, Communication type: sens... (Sensor bundle), Co... (Communication pattern), Profile: 8 - TCP communications, Severity: 1 (Medium), Source IP: 172.16.2.30 (stochastic), Destination IP: 172.16.2.2 (strat1@300-mgmt-lab), Source port: 22, Destination port: 22, and Protocol: SSH (TCP).

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

This detailed screenshot of the Forescout alert interface shows an unauthorized SSH connection. The alert ID is 169373, timestamped Oct 13, 2020 13:24:58. The source host info includes an IP address of 172.16.2.30 (Private IP), host name 'stochastic', and host MAC addresses 00:09:5B:AA:E9:29 (Netgear). Other observed MAC addresses include E4:90:69:3B:C2:C3 (Rockwell) and E4:90:69:3B:C2:C0 (Rockwell). The role is SNMP manager, and other roles include Windows workstation, Web server, Terminal client. Client protocols listed are DNS (UDP 53), FailedConnection (TCP 80, 7000, 7001, 7002, 7004, 7005, 7006, 7007, 7008, 7009, 52311), LDAP (UDP 389), and NotKnownOne (UDP 443, 19000). The alert details show an ID and name 'lan\_cp\_enw\_c - Communication pattern not whitelisted' and a description stating 'Communication pattern not whitelisted: the source and destination hosts are whitelisted in some communication rule, but not with this combination'. The triggering rule/default action is set to 'alert'.

## 1408 **D.5.3 Build 3**

### 1409 **D.5.3.1 Configuration**

- 1410     ■ Behavior Anomaly Detection: Dragos
  - 1411         • Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
  - 1412

1413    *D.5.3.2 Test Results*

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

DRAFT

1417 **Figure D-60: Dragos Dashboard Showing Alerts Generated upon Detecting New Device and Network**  
 1418 **Scanning**

The screenshot shows the Dragos Notification Manager interface. On the left, a sidebar lists navigation options: Dashboard, Map, Assets, Data, Notifications (selected), Content, Reports, Sensors, and Admin. The main area is divided into three tabs: ASSET NOTIFICATIONS, SYSTEM ALERTS, and RULES.

- ASSET NOTIFICATIONS:** Shows 5 notifications from 02/17/21, 20:59 UTC to 02/17/21, 21:00 UTC. The first four are communication-related (NewSourcePort Detected, NewDestPort Detected, NewCommunication Detected, NewCommunication Peering) and the last one is an ICMP Scan Detected (ICMP scan observed from asset 85). A search bar at the top right shows "Search 0.205".
- SYSTEM ALERTS:** Shows 1 alert: "Asset 2799 seen as the ethernet source for the first time" (Detected by New Source Ethernet Address Detection).
- RULES:** Shows 1 rule: "ICMP Scan Detected" (Asset IDs 102, 85; Source IPv4 192.168.0.205; Dest IPv4 10.100.1.4; Other IPv4 10.100.1.4).

At the bottom, it says "Showing 1 to 5 of 5 Notifications" and "Result per page 500".

1419 **Figure D-61: Details of Network Scanning Activity**

This screenshot shows the details of an ICMP Scan Detected alert (ID 148592) on the Dragos Notification Manager. The left sidebar is identical to Figure D-60.

**DETECTION INFORMATION:**

- WHAT HAPPENED:** ICMP scan observed from asset 85, 10.100.1.4, scanned at least 214 unique hosts (that did not respond) via ICMP type 8 requests in 200ms. Addresses were incrementing (179 times out of 1970 (100.00%)). A max size of 1 occurred 1970 times (100.00%). Top psh sizes were: 1 (1792). The longest run of contiguous addresses was 240 long. All destination addresses were incrementing (179 times out of 1970 (100.00%)).
- LAST SEEN:** 02/17/21, 21:00 UTC
- COUNT:** 1
- DETECTED BY:** ICMP sweep
- DETECTION QUAD:** Threat Behavior
- ACTIVITY GROUP:** Common
- MITRE ATT&CK FOR ICS TACTIC:** Discovery
- PLAYBOOKS:** Known Address Scanning Activity Detected
- CASES:** No Cases Linked

**ASSOCIATED ASSETS:** Shows 1 asset: Windows Serv 85 Asset 85 (Name 10.100.1.4, OS Win).

**COMMUNICATIONS SUMMARY:** Shows "No Communications Summary".

On the right, there is a sidebar titled "admin" showing network scanning activity with IP ranges 0.205 and 2.205, and a count of 4.

## DRAFT

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

**DETECTION INFORMATION**

**WHAT HAPPENED:**  
Scan 2799 detected 6 new communication between 2021-02-17T20:55:21.899Z and 2021-02-17T20:59:46.234Z.

**OCCURRED AT:** 2021/02/17, 20:59 UTC

**COUNT:** 1

**DETECTED BY:** New Communication Piping

**DETECTION QUAD:** No Applicable Detection Quad

**ACTIVITY GROUP:** No Applicable Activity Group

**MITRE ATT&CK TECHNIQUE:** No Applicable MITRE ATT&CK Technique

**QUERY-FOCUSED DATASETS:** No Applicable Query-Focused Dataset

**PLAYBOOKS:** No Related Playbooks

**CASES:** No Cases Linked

**NOTIFICATION RECORD:** View in Kibana

**SOURCE:** 2021/02/17-20:59:46.234Z-439c3d9e961965ba, F02c5d39-485a-4492-860a-3009a4707fb8, 8119150a-327b-46f7-8032-8C8705D98841, 0ea83595-f11a-42fe-9217-049732a32794c, 979302a5-12b6-46f7-af58-152db29f7fa, f5560ef1-122e-4a26-988e-0274e0118fb0

**ZONES:** IFC10, Cybersecurity LAN

**ICS CYBER KILLCHAIN STEP:** None

**MITRE ATT&CK TACTIC:** No Applicable MITRE ATT&CK Tactic

**NOTIFICATION COMPONENTS:** View in Kibana

**RELATED NOTIFICATIONS**

ID	Occurred At

No Related Notifications.

**ASSOCIATED ASSETS**

View	Type	ID	Name	Dir.
VIS-W	Asset	2791	Asset 2791	baddr
VIS-W	General Use ID	102	Asset 102	f6899000597110de85705121
VIS-W	Router	96	Asset 96	192.168.0.2

**COMMUNICATIONS SUMMARY**

No Communications Summary.

**LAST**

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

**DETECTION INFORMATION**

**WHAT HAPPENED:**  
Asset 2799 seen as the ethernet source for the first time.

**OCCURRED AT:** 2021/02/17, 02:39 UTC

**COUNT:** 1

**DETECTED BY:** New Source Ethernet Address Detection

**DETECTION QUAD:** Comprehensive

**ACTIVITY GROUP:** None

**MITRE ATT&CK TECHNIQUE:** None

**QUERY-FOCUSED DATASETS:** None

**PLAYBOOKS:** New Source Ethernet or IP Address Detected

**CASES:** No Cases Linked

**NOTIFICATION RECORD:** View in Kibana

**SOURCE:** 00402d43-596c-46b7-a379-ekh961965ba

**ZONES:** DSC\_1 - level 1

**ICS CYBER KILLCHAIN STEP:** None

**MITRE ATT&CK TACTIC:** None

**NOTIFICATION COMPONENTS:** View in Kibana

**RELATED NOTIFICATIONS**

ID	Occurred At

No Related Notifications.

**ASSOCIATED ASSETS**

View	Type	ID	Name	Dir.
VIS-W	Server	2799	Asset 2799	192.168.0.205

**COMMUNICATIONS SUMMARY**

No Communications Summary.

**LAST**

1422 **D.5.4 Build 4**1423 ***D.5.4.1 Configuration***

- 1424     ▪ Behavior Anomaly Detection: Azure Defender for IoT
- 1425         • Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and  
1426         Control LAN.

1427 ***D.5.4.2 Test Results***

1428 A “New Asset Detected” alert is shown on Azure Defender for IoT dashboard (Figure D-64) and on the  
1429 Alert screen ([Figure D-65](#)). [Figure D-66](#) shows the alert management options in Azure Defender for IoT.  
1430 The details of the network scanning alert are shown in [Figure D-67](#).

1431 **Figure D-64: Azure Defender for IoT Dashboard Showing the Alerts, Including for the New Asset**

The screenshot displays the Azure Defender for IoT Dashboard. On the left, a navigation sidebar lists various sections like Dashboard, Asset Map, Asset Inventory, Alerts (62), Reports, Event Timeline, Data Mining, Investigation, Risk Assessment, Attack Vectors, Custom Alerts, Users, Forwarding, System Settings, Import Settings, SUPPORT, Horizon, and Support. The main dashboard area shows four summary cards: 'Welcome back, [User]' (21 Critical), '19 Major', 'No Minor' (23 Warnings), and '63 All'. Below these are two large numerical displays: '2,998 PPS' and '63 UA'. To the right, a detailed alert card for 'Access Violation' is shown, stating 'Device Discovered Unexpectedly'. It includes a magnifying glass icon over a network diagram and a list of related alerts, including 'New Asset Detected' (just now) and 'Violation' (A new asset was detected on the network). A 'Devices' section shows a table with one entry (Type: 192.168.0.205) and a 'Show Devices' button. Another alert card for 'Policy Violation' is partially visible below it.

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

The screenshot shows the Azure Defender for IoT interface under the 'Alerts' section. On the left is a navigation sidebar with various options like Dashboard, Asset Inventory, Reports, ANALYTICS, Data Mining, Investigation, Risk Assessment, Attack Vectors, ADMINISTRATION, Custom Alerts, Users, Forwarding, System Settings, SUPPORT, Horizon, and Support. The main area is titled 'Important Alerts (2)' and lists two items:

- POLICY VIOLATION** Unauthorized Internet Connectivity Detected | just now: An asset defined in your internal network is communicating with addresses on the Internet. These addresses have not been learned.
- POLICY VIOLATION** New Asset Detected | just now: A new asset was detected on the network. Asset 192.168.0.205 was added to your network. Verify that this is a valid network asset.

Below this is a 'Pinned Alerts (0)' section labeled 'No Alerts'. At the bottom is a 'Recent Alerts (2)' section with the same two alert entries, each with a timestamp of 'Jan 6 14:36'.

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

The screenshot shows the details of a specific alert titled 'New Asset Detected' with ID 232. The alert information includes:

- Policy Violation | Jan 6, 2021 2:36:03 PM ( 2 minutes ago )
- A new asset was detected on the network. Asset 192.168.0.205 was added to your network.
- Verify that this is a valid network asset.

Below this is a section titled 'Manage this Event' with the following options:

- Approve this asset as a valid network device.
- Select Acknowledge to save the alert. Another alert will trigger if the event is detected again.
- Disconnect the asset from the network. Select Delete Asset. This asset will not be analyzed by the sensor unless it is detected again.

At the bottom are three buttons: 'Delete Asset' (blue), 'Approve' (blue), and 'Acknowledge' (blue).

1434 **Figure D-67: Details for Network Scanning Alert**

**Device Connection Detected**  
Jan 6, 2021 2:36:03 PM

**Grouped Events**

- Jan 6, 2021 2:36:03 PM  
Connected devices 192.168.1.103 and 192.168.0.205
- Jan 6, 2021 2:36:03 PM  
Connected devices 192.168.0.205 and 192.168.1.101
- Jan 6, 2021 2:36:03 PM  
Connected devices 192.168.0.205 and 10.100.0.17

**Assets**

Type	Name
Station 2	
LAN-AD	
Station 4	
Station 3	
Station 1	
CRS Supervisory LAN Gateway	
192.168.0.205	

**Info**

1435 **D.6 Executing Scenario 6: Detect Unauthorized Device-to-Device Communications**  
14361437 An authorized device that is installed on the network attempts to establish an unapproved connection  
1438 not recorded in the baseline. The expected result is the behavioral anomaly detection products alert on  
1439 the non-baseline network traffic.1440 **D.6.1 Build 1**1441 **D.6.1.1 Configuration**

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

1444 **D.6.1.2 Test Results**

1445 The unapproved SSH traffic is detected by Tenable.ot as shown in Figure D-68.

1446 **Figure D-68: Tenable.ot Event Log Showing the Unapproved SSH Traffic**

The screenshot shows the Tenable.ot web interface with the following details:

- Header:** Shows the Tenable logo, navigation links like 'Events', 'Configuration Events', 'SCADA Events', etc., and a search bar with 'ssh'.
- Event List:** A table with columns: LOG ID, TIME, EVENT TYPE, SEVERITY, POLICY NAME, SOURCE ASSET, and SOURCE ADDRESS. It lists two events:
  - Event 9097: Unauthorized Conversation, Medium severity, Policy SSH Communications, Source Asset PCS\_Eng\_Station, Source Address 172.16.3.10, Time 03:22:51 PM - Jan 29, 2021.
  - Event 9093: Unauthorized Conversation, Medium severity, Policy SSH Communications, Source Asset PCS\_Eng\_Station, Source Address 172.16.3.10, Time 03:20:44 PM - Jan 29, 2021.
- Event Detail View:** For Event 9093, it shows:
  - Details:** A conversation in an unauthorized protocol has been detected.
  - Source:** SOURCE NAME: PCS\_Eng\_Station, SOURCE ADDRESS: 172.16.3.10.
  - Destination:** DESTINATION: Stratis5700 VLAN1, NAME: 172.16.1.3, ADDRESS: 172.16.1.3.
  - Protocol:** PROTOCOL: SSH (tcp/22), PORT: 22.
  - Why is this important?** Conversations in unauthorized protocols may indicate suspicious traffic. Some assets are not expected to communicate in non-standard protocols and any deviation from the standard protocols may suggest a potential threat. In addition, some protocols are insecure and should not be used at all, in order to prevent unauthorized access.
  - Suggested Mitigation:** Check if this communication is expected. If it is expected traffic, then adjust the Policy conditions so that Events aren't generated for similar communications in the future. If this communication is not expected, check the source asset to determine whether the source asset itself has been compromised. If this

1447 **D.6.2 Build 2**

1448 **D.6.2.1 Configuration**

- 1449     ■ Behavior Anomaly Detection: eyeInspect
  - 1450         ● Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.

1451 **D.6.2.2 Test Results**

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

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

The screenshot shows the Forescout interface with the following details:

**Alert details**

- Summary**:
  - Alert ID: 139850
  - Timestamp: Oct 7, 2023 12:06:19
  - Sensor name: sensor-bundle-noise
  - Description engine: Communication pattern (LAN CP)
  - Profile: 0 - TCP communications
  - Severity: ! ! Medium
  - Source MAC: 0C:6A:7A:31:40:47 (SuperM)
  - Destination MAC: F4:D6:33:2F:0E:C1 (Rockwell)
  - Source IP: 172.16.1.4 (gs-01389n)
  - Destination IP: 172.16.1.3 (plant)
  - Source port: 5850
  - Destination port: 22
  - L2 proto: Ethernet
  - L3 proto: IP
  - L4 proto: TCP
  - L7 proto: SSH
  - TCP streams opened in host start mode: False
  - Status: Not analyzed
  - Labels:
  - User notes:
- Source host info**:
  - IP address: 172.16.1.4 (Private IP)
  - Host name: fpo-01389n
  - Other host names: fpo-01389n.lan.lab
  - Host MAC address: 0C:6A:7A:31:40:47 (SuperM)
  - Other observed MAC addresses: E4:09:69:0B:02:C3 (Rockwell), E4:09:69:0B:02:C4 (Rockwell), E4:09:69:0B:02:C5 (Rockwell), 7C:08:CE:67:80:88 (Cisco), 7C:08:CE:67:80:89 (Cisco)
  - Role: Terminal server
  - Other roles: Windows workstation
  - Vendor and model: Rockwell
  - OS version: Windows 7 or Windows Server 2008 R2
  - Client protocols: DCCP (TCP 125, 40155, 49159), DNS (TCP 53), DNS (UDP 53), DNS (UD 5385), FaileConnection (TCP 23, 80, 139), HTTP (TCP 80), HTTP (TCP 443), LDAP (TCP 389), LDAP (UDP 389), LDAP (TCP 389), LDAP (UDP 389), Telnet (TCP 23), Telnet (TCP 137), NetWare (TCP 50005), NetBIOSNameQuery (TCP 132, 2502, 2504, 10000), NetBIOSNameReq (TCP 134), SMB (TCP 445), SMB (UDP 139), SMB (UDP 446), SSH (TCP 22), SSL (TCP 443, 10000), SyNc (UDP 514), TFTP (TCP 157, 631)
- Alert Details**:
  - ID and name: Ian\_cpx\_cme\_x - Communication pattern not whitelisted
  - Description: Communication pattern not whitelisted. The source and destination hosts are whitelisted in some communication rule, but not with this combination.
  - Triggering rule/default action: alert

1455 

## D.6.3 Build 3

1456 

### D.6.3.1 Configuration

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

1460 

### D.6.3.2 Test Results

- 1461 Dragos detected the non-baseline SSH traffic as shown in [Figure D-70](#).

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

**DETECTION INFORMATION**

**WHAT HAPPENED:** New Communication from host 192.168.1.104 to host 192.168.1.101 over SSH on port [22] for the first time.

**\_OCCURRED\_AT:** 14:07:27, 10-10 UTC

**COUNT:** 1

**STATE:** UNRESOLVED

**SOURCE:** [Asset 3177 \(192.168.1.104\)](#)

**ZONES:** [Zone - Level 0](#)

**ACTIVITY GROUP:** No Applicable Activity Group

**ICS CYBER KILLCHAIN STEP:** [No Applicable ICS Cyber Killchain Step](#)

**MITRE ATTACK TACTIC:** [No Applicable MITRE Attack Tactic](#)

**MITRE ATTACK TECHNIQUE:** [No Applicable MITRE Attack Technique](#)

**QUERY-FOCUSED DATASETS:** No Applicable Query-Focused Datasets

**PLAYBOOKS:** No Associated Playbooks

**CASES:** No Cases Linked

**RELATED NOTIFICATIONS**

ID	Occurred At
...	...

No Related Notifications.

**ASSOCIATED ASSETS**

Name	Dir.
192.168.1.104	src
192.168.1.101	dest

**COMMUNICATIONS SUMMARY**

SSH AND ARP traffic between Texas Instruments hosts.

Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
SSH	192.168.1.104	48736	192.168.1.101	22	2.6 kB	1.0 kB
SSH	B0:D5:CC:F4:26:E0	48736	B0:D5:CC:FA:70:C9	22	2.6 kB	1.0 kB
ARP	B0:D5:CC:F4:26:E0	-	B0:D5:CC:FA:70:C9	-	60.0 bytes	0 bytes
ARP	B0:D5:CC:FA:70:C9	-	B0:D5:CC:F4:26:E0	-	0 bytes	60.0 bytes

1463 

## D.6.4 Build 4

1464 

### D.6.4.1 Configuration

- 1465
- Behavior Anomaly Detection: Azure Defender for IoT

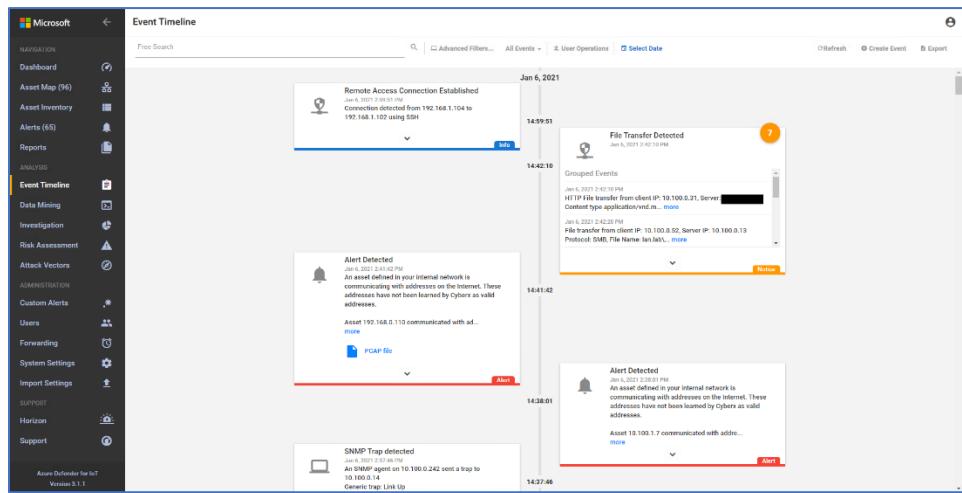
- 1466
- Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

1468 

### D.6.4.2 Test Results

- 1469 A device attempts to establish a remote access connection via SSH. Azure Defender for IoT was able to
- 
- 1470 detect this activity as shown in
- [Figure D-71](#)
- .

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



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

1473 An authorized user attempts to delete files on an engineering workstation and a shared network drive  
 1474 within the manufacturing system. The expected result is the file integrity checking tools in the  
 1475 environment alert on the deletion or prevent deletion entirely.

### 1476 **D.7.1 Build 1**

#### 1477 ***D.7.1.1 Configuration***

- 1478     ▪ File Integrity Checking: Carbon Black
  - 1479         • Agent installed on workstations and configured to communicate to the Carbon Black Server.
- 1481     ▪ File Integrity Checking: WORMdisk
  - 1482         • Network file share on server is configured to use WORMdisk.

#### 1483 ***D.7.1.2 Test Results***

1484 Carbon Black reports file deleting activities as shown in [Figure D-72](#). GreenTec protects the files on its  
 1485 drive from being deleted.

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

Timestamp	Se...	Type	Subtype	Source	Description	IP Address	User	Process Na...
Feb 3 2021 01:35:55 PM	Info	Policy Enforcement	Report write (Custom Rule)	LAN\FGS-47631EHH	'C:\users\administrator\downloads\va\nccoe_test_file.txt' was deleted by FGS-47631EHH\Administrator	172.16.3.10	FGS-47631EHH\Administr...	explorer.exe
Feb 3 2021 01:35:50 PM	Info	Policy Enforcement	Report write (Custom Rule)	LAN\FGS-47631EHH	'C:\users\administrator\downloads\va\tests\scenarios\nccoe_test_file.txt' was deleted by FGS-47631EHH\Administrator	172.16.3.10	FGS-47631EHH\Administr...	explorer.exe
Feb 3 2021 01:35:35 PM	Info	Policy Enforcement	Report write (Custom Rule)	LAN\FGS-47631EHH	'C:\users\administrator\documents\test\im\nccoe_test_file.txt' was deleted by FGS-47631EHH\Administrator	172.16.3.10	FGS-47631EHH\Administr...	explorer.exe

1487 **D.7.2 Build 2**1488 ***D.7.2.1 Configuration***1489 **▪ File Integrity Checking: Security Onion**

- 1490     • The agent is installed on workstations and configured to communicate to the Security  
1491       Onion Server.

1492 **▪ File Integrity Checking: WORMdisk**

- 1493     • Network file share on server is configured to use WORMdisk.

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

1495 Security Onion Wazuh alerts on file deletion as shown in [Figure D-73](#). Files stored on a storage drive  
1496 protected by GreenTec are protected from deletion.

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

```

@timestamp          | October 15th 2020, 13:05:33.753
@version           | 1
_id                | JXY5LXUB1YHtrLLyWhk
_index             | seconion:logstash-ossec-2020.10.15
_score              |
_type               | doc
agent.id            | 005
agent.ip            | ▲ 172.16.3.10
agent.name          | PCS-EWS
alert_level         | 7
classification      | "Bad word" matching
decoder.name        | syscheck_integrity_changed
description         | File deleted.
event_type          | ossec
full_log            |
| File 'c:\users\administrator\downloads\ra\testscenarios\test_file.txt' was deleted.
| (Audit) User: 'Administrator (5-1-5-21-239850103-4004920075-3296975006-500)'
| (Audit) Process id: '6056'
| (Audit) Process name: 'C:\Windows\explorer.exe'
host                | gateway
id                 | 1602781532.2062049
location            | syscheck
logstash_time       | 0.002

```

1498 [D.7.3 Build 3](#)

#### 1499 [D.7.3.1 Configuration](#)

- 1500     ▪ File Integrity Checking: Security Onion
  - 1501         • Agent installed on workstations and configured to communicate to the Security Onion Server.
- 1503     ▪ File Integrity Checking: WORMdisk
  - 1504         • Network file share on server is configured to use WORMdisk.

#### 1505 [D.7.3.2 Test Results](#)

1506 Security Onion Wazuh detected the deletion of the files as shown in the Security Onion Server log in  
 1507 [Figure D-74](#). Files stored on a storage drive protected by GreenTec are protected from deletion.

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

```

{
  "@timestamp": "Feb 12, 2021 @ 10:41:45.589",
  "@version": "1",
  "_id": "Mhrlnuc8lvk0Opavc9g",
  "_index": "seconion:logstash-ossec-2021.02.12",
  "_score": "-",
  "_type": ".doc",
  "agent.id": "003",
  "agent.ip": "192.168.0.20",
  "agent.name": "CRS-EWS",
  "alert.level": 7,
  "classification": "Bad word" matching,
  "decoder.name": "syscheck_integrity_changed",
  "description": "File deleted.",
  "event.type": "ossec",
  "full.log": "File 'c:\\users\\nccoeuser\\documents\\twinCAT projects\\crs workcell\\boot\\twinCAT ce7 (armv7)\\plc\\port_851.oce' was deleted.",
  "host": "gateway",
  "id": "1613144584.13813845",
  "location": "syscheck",
  "logstash.time": "0.007",
  "manager.name": "seconion",
  "message": {
    "@timestamp": "2021-02-12T15:41:44.769+0000",
    "rule": {
      "level": 7,
      "description": "File deleted."
    },
    "id": "553",
    "firetime": -60,
    "mail": true,
    "groups": [
      "ossec",
      "syscheck"
    ],
    "pci_dss": [
      "II.5.1"
    ],
    "ppid": [
      "4.31"
    ],
    "ppr": [
      "II.5.1"
    ],
    "agent": {
      "id": "003",
      "name": "CRS-EWS",
      "ip": "192.168.0.20",
      "manager": {
        "name": "seconion"
      },
      "id": "1613144584.13813845"
    },
    "full.log": "File 'c:\\users\\nccoeuser\\documents\\twinCAT projects\\crs workcell\\boot\\twinCAT ce7 (armv7)\\plc\\port_851.oce' was deleted.\n",
    "syscheck": {
      "path": "c:\\users\\nccoeuser\\documents\\twinCAT projects\\crs workcell\\boot\\twinCAT ce7 (armv7)\\plc\\port_851.oce",
      "event": "deleted"
    }
  },
  "port": 36884,
  "syscheck.event": "deleted",
  "syscheck.path": "c:\\users\\nccoeuser\\documents\\twinCAT projects\\crs workcell\\boot\\twinCAT ce7 (armv7)\\plc\\port_851.oce"
}

```

1509 **D.7.4 Build 4**1510 ***D.7.4.1 Configuration***

- 1511     ▪ File Integrity Checking: Carbon Black
  - 1512         • Agent installed on workstations and configured to communicate to the Carbon Black Server.
- 1514     ▪ File Integrity Checking: WORMdisk
  - 1515         • Network file share on server is configured to use WORMdisk.

1516 ***D.7.4.2 Test Results***

- 1517 The attempts to delete a file are detected by Carbon Black as shown in [Figure D-75](#). Files stored on a storage drive protected by GreenTec are protected from deletion.

1519 **Figure D-75: Carbon Black Alerts Showing That a File Has Been Deleted**

Timestamp	Severity	Type	Subtype	Source	Description	IP Address	User	Process Name
Jan 6 2021 02:25:56 PM	Notice	Computer Management	Agent deleted events	WORKGROUP\eee...	'Computer WORKGROUP\eee93e4e44od-vm' deleted 508 events.	10.100.1.61		
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs\workcell\untitled2_old_v1mp3\j\twinsafe\group1\twinsafe\group1.sal' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs\workcell\untitled2_old_v1mp3\j\untitled2.splproj' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs\workcell\untitled2_old_v1mp3\j\untitled2.splproj' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs\workcell\untitled2_old_v1mp3\j\twinsafe\group1\twinsafe\group1.alias.devices\term 4 (el2904) - module 1 (fsoes).sds' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs\workcell\untitled2_old_v1mp3\j\twinsafe\group1\twinsafe\group1.alias.devices\alias devices' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe

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

1521 An authorized user performs an unapproved or unauthorized modification of the PLC logic through the  
 1522 secure remote access tools. The expected result is the behavioral anomaly detection tools will detect  
 1523 and capture the activity, flagging it for review.

1524 The behavior anomaly detection tools can detect program downloads to the PLC. Program download  
 1525 detection needs to be correlated with the maintenance management system to determine if the  
 1526 download was authorized and approved. This was not demonstrated as part of this scenario.

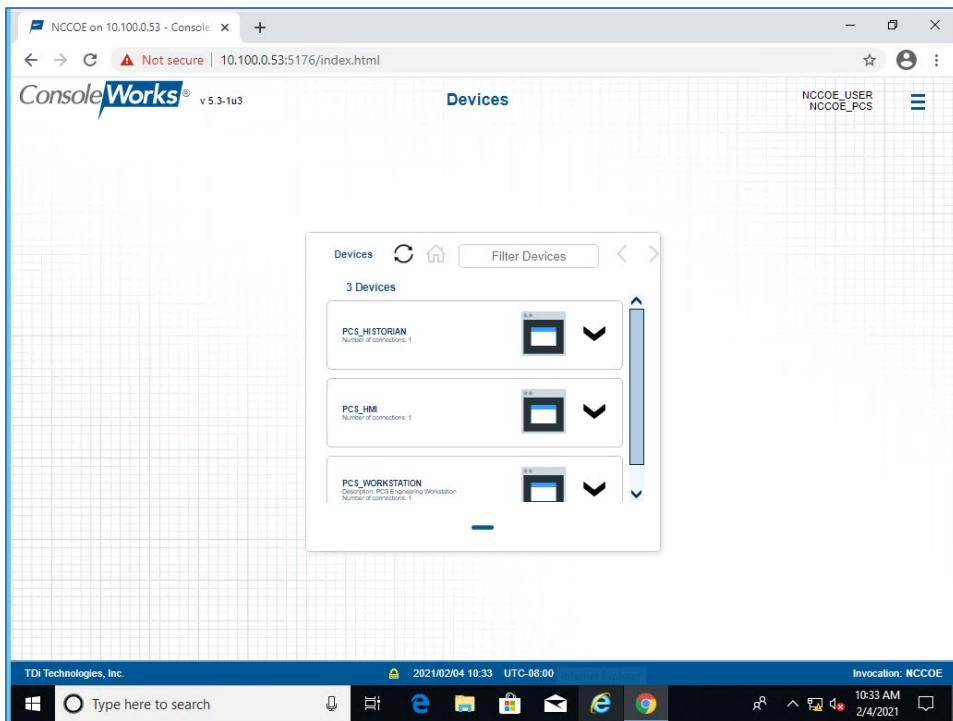
1527 **D.8.1 Build 1**1528 **D.8.1.1 Configuration**

- 1529     ▪ Behavior Anomaly Detection: Tenable.ot
  - 1530         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1531     ▪ Remote Access: Cisco VPN
  - 1532         • Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- 1533     ▪ User Authentication/User Authorization: ConsoleWorks
  - 1534         • Configured for accessing the PCS environment

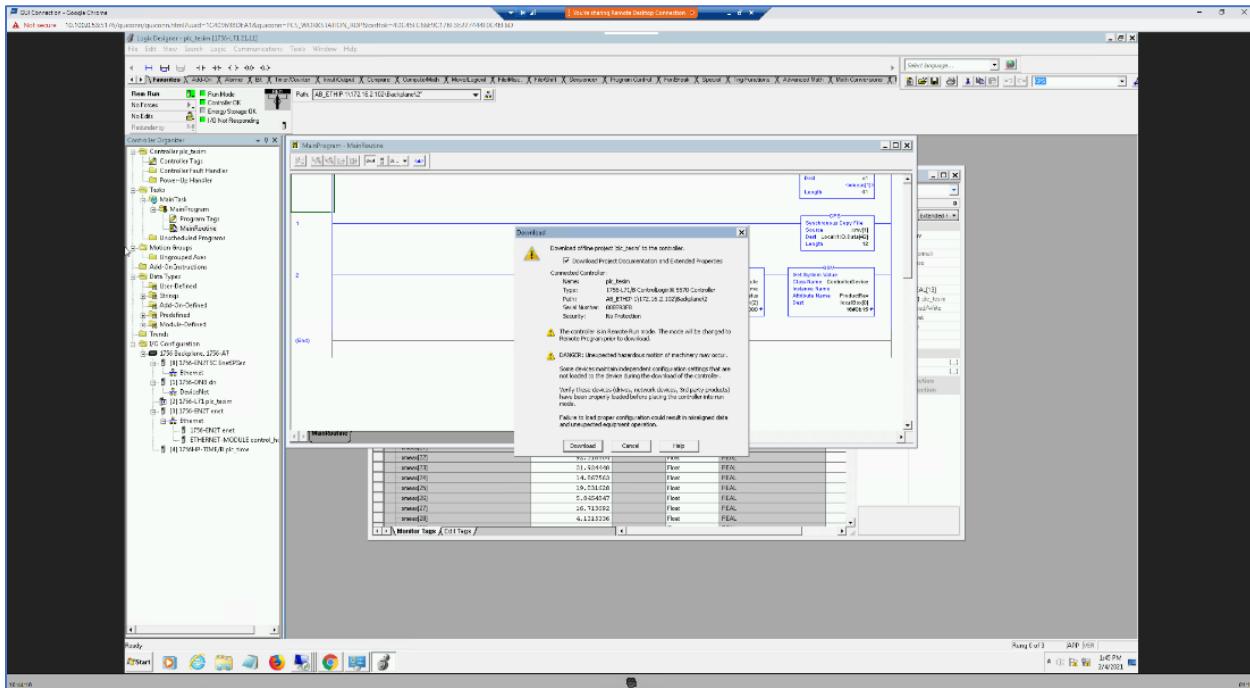
1535 **D.8.1.2 Test Results**

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

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



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



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

All Events		Search...	Actions ▾	Resolve All	Export
LOG ID	TIME ▾	EVENT TYPE	SEVERITY	POLICY NAME	
<input type="checkbox"/> 12416	01:47:47 PM · Feb 4, 2021	Change in Key Sw...	High	<a href="#">Change in controller key state</a>	
<input type="checkbox"/> 12414	01:46:52 PM · Feb 4, 2021	Rockwell PLC Start	Low	<a href="#">Rockwell PLC Start</a>	
<input type="checkbox"/> 12413	01:46:30 PM · Feb 4, 2021	Rockwell Code Do...	Medium	<a href="#">Rockwell Code Download</a>	
<input type="checkbox"/> 12412	01:46:27 PM · Feb 4, 2021	Rockwell PLC Stop	High	<a href="#">Rockwell PLC Stop</a>	
<input type="checkbox"/> 12410	01:45:05 PM · Feb 4, 2021	Rockwell Go Online	Low	<a href="#">Rockwell Online Session</a>	
<input type="checkbox"/> 12409	01:44:38 PM · Feb 4, 2021	RDP Connection (...)	Medium	<a href="#">RDP Communication to an Engineerin...</a>	

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

 Rockwell PLC Stop  
Rockwell PLC Stop

Status  Actions ▾

Category Configuration Events

Details	Triggered Events	Exclusions																					
Items: 1-1 out of 1	Event 12412 01:46:27 PM · Feb 4, 2021 Rockwell PLC Stop High Not resolved																						
		<p>Details</p> <p>The controller state was changed to Stop</p> <table border="1"> <tr> <td>SOURCE <a href="#">PCS Eng. Station</a></td> <td>Why is this important?</td> <td>Suggested Mitigation</td> </tr> <tr> <td>NAME</td> <td></td> <td>1) Check whether the state change was made as part of scheduled maintenance work and</td> </tr> <tr> <td>SOURCE 172.16.3.10</td> <td></td> <td></td> </tr> <tr> <td>ADDRESS</td> <td></td> <td></td> </tr> <tr> <td>DESTINATION <a href="#">plc_tesim</a></td> <td></td> <td></td> </tr> <tr> <td>NAME</td> <td></td> <td></td> </tr> <tr> <td>DESTINATION 172.16.2.102</td> <td></td> <td></td> </tr> </table>	SOURCE <a href="#">PCS Eng. Station</a>	Why is this important?	Suggested Mitigation	NAME		1) Check whether the state change was made as part of scheduled maintenance work and	SOURCE 172.16.3.10			ADDRESS			DESTINATION <a href="#">plc_tesim</a>			NAME			DESTINATION 172.16.2.102		
SOURCE <a href="#">PCS Eng. Station</a>	Why is this important?	Suggested Mitigation																					
NAME		1) Check whether the state change was made as part of scheduled maintenance work and																					
SOURCE 172.16.3.10																							
ADDRESS																							
DESTINATION <a href="#">plc_tesim</a>																							
NAME																							
DESTINATION 172.16.2.102																							

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

The screenshot shows a software interface titled "Rockwell Code Download" under the "Configuration Events" category. A specific event is selected: "Event 12413 01:46:30 PM · Feb 4, 2021 · Rockwell Code Download · Medium · Not resolved". The event details indicate that code was downloaded from an engineering station to a controller. The "Why is this important?" section notes a change in controller code. The "Suggested Mitigation" section provides a check for scheduled work and source of the change.

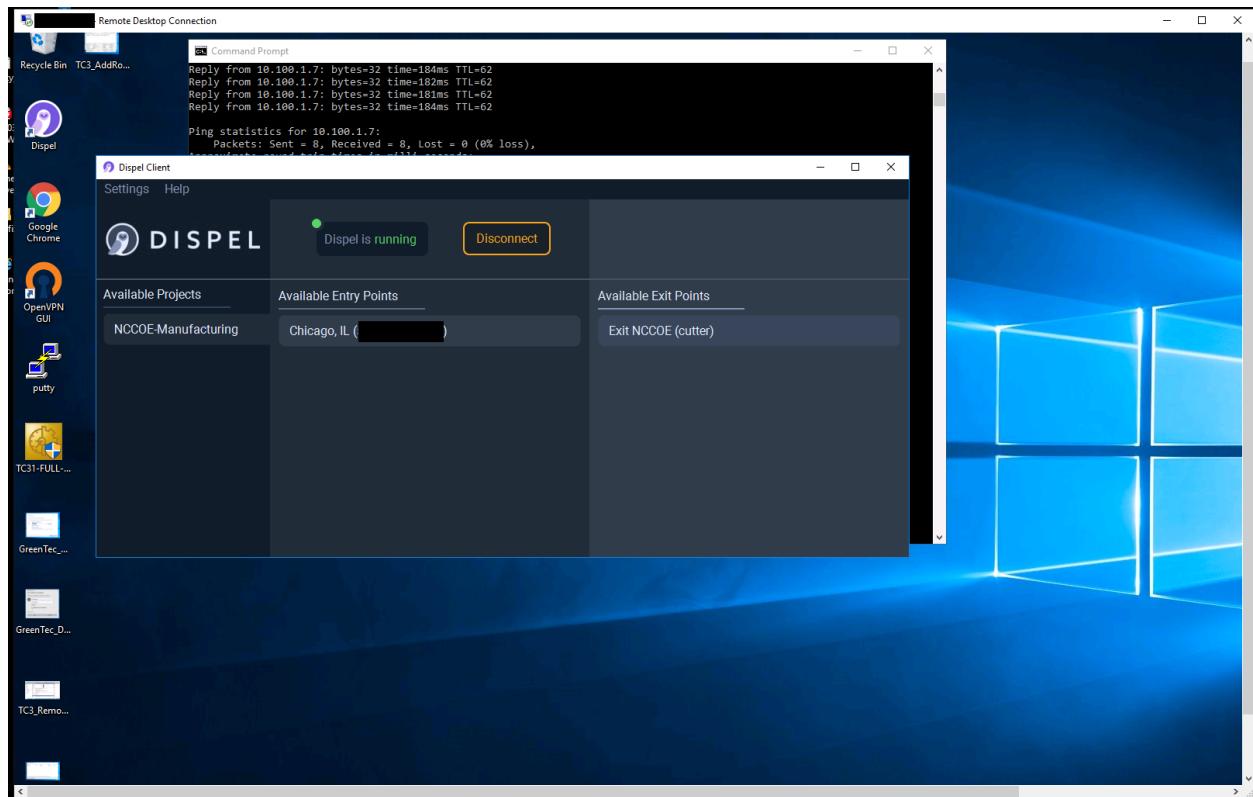
Code	SOURCE <a href="#">PCS Eng_Station</a> NAME	Why is this important?	Suggested Mitigation
Source	SOURCE 172.16.3.10 ADDRESS	The system detected a change in the controller code that was made	1) Check whether the change was made as part of scheduled work and whether the source of the
Destination	DESTINATION <a href="#">plc_tesim</a> NAME		
Policy	DESTINATION 172.16.2.102		
Status			

1544 **D.8.2 Build 2**1545 **D.8.2.1 Configuration**

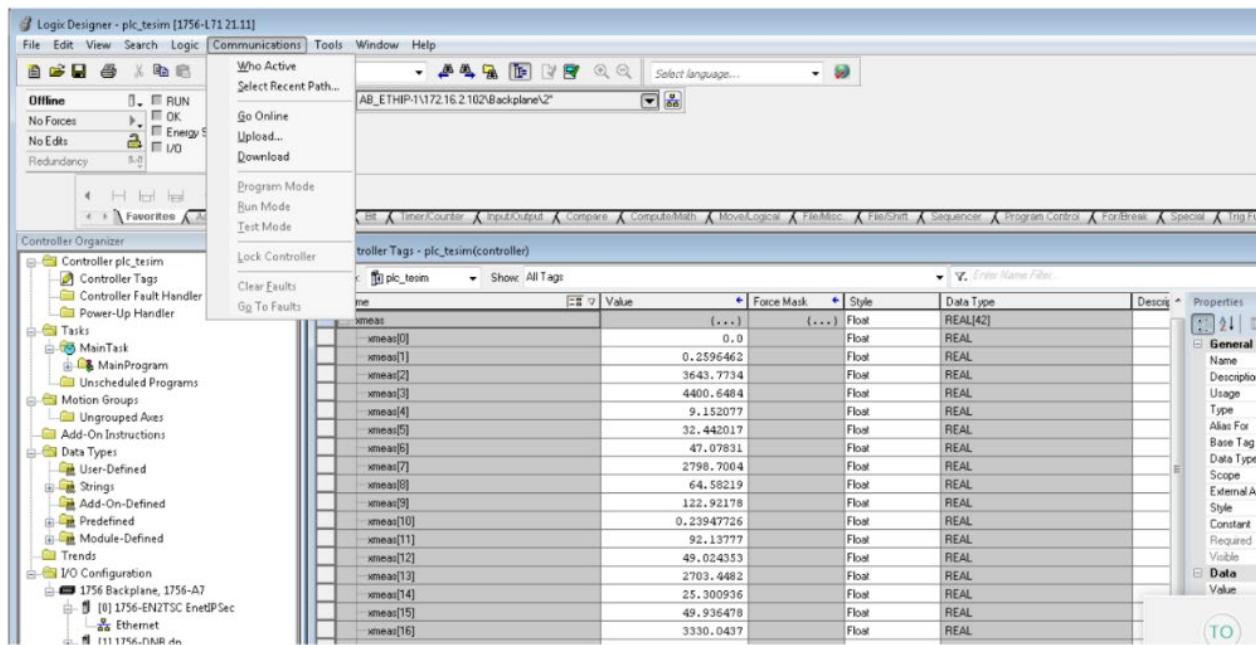
- Behavior Anomaly Detection: eyeInspect
  - Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- Remote Access, User Authentication/User Authorization: Dispel
  - Dispel VDI is configured to allow authorized users to access PCS environment through the Dispel Enclave to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

1551 **D.8.2.2 Test Results**

1552 As shown in [Figure D-81](#) the authorized user establishes a session into the manufacturing environment using the Dispel VDI. The user connects to the engineering workstation and launches the Studio 5000 Logix Designer as shown in [Figure D-82](#) to modify the PLC logic. [Figure D-83](#), [Figure D-84](#) and [Figure D-85](#) show that Forescout is able to detect the traffic between the engineering workstation and the PLC, including details of the Stop command and Download command.

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

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



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

The screenshot shows the Forescout interface with the 'Alerts' tab selected. The table lists ten alerts, all of which are for Oct 13, 2020, at 13:47:52. The alerts describe FEA Exit messages from a sensor to a Co... engine. The source address is 172.16.3.10 and the destination address is 172.16.2.102. The L7 Proto is ETHIP (TCP) and the Case ID is 44818. The severity is Not analyzed.

Timestamp	Event name(s)	Sensor	Engine	Profile	Status	Severity	Source address	Destination address	Dest. Port	L7 Proto	Case ID
Oct 13, 2020 13:47:52	(FEA Exit) Message t...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:47:52	(FEA Exit) Message t...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:47:52	(FEA Exit) Message t...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:47:52	(FEA Exit) Message t...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:47:52	(FEA Exit) Message t...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:47:52	(FEA Exit) Message t...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:46:49	ETHIP controller star...	senso...	Indu...	-	Not analy...	■■■■■ L	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:46:49	Message type not w...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP
Oct 13, 2020 13:46:49	Message type not w...	senso...	Co...	8 - TCP c...	Not analy...	■■■■■ M	172.16.3.10 (fg...	172.16.2.102 (...	44818	(TCP)	ETHIP

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

The screenshot shows the Forescout interface with the 'Alert details' tab selected. The alert summary indicates an ID of 169537, timestamp of Oct 13, 2020 13:46:10, and a potentially dangerous ETHIP operation. The source host info shows the IP address is 172.16.3.10 (Private IP), host name is fgs-47631ehh, and other host names are fgs-47631ehh.lan.lab. The alert details pane shows the command was 'Stop controller' issued by user 'FGS-47631EHH\Administrator'.

Summary	Source host info	Alert details
Alert ID: 169537 Timestamp: Oct 13, 2020 13:46:10 Sensor name: sensor.bundle-nccoe Detection engine: Industrial threat library (ITL) ID and name: id_ops_ddos_ethip_controller_stop - ETHIP controller stop command Description: Potentially dangerous ETHIP operation: the ETHIP master or an operator has requested a PLC to stop. This operation may be part of regular maintenance but can also be used in a Denial of Service attack. Severity: ■■■■■ High Source MAC: 40:AB:F0:3D:4B:AE (HewlettP) Destination MAC: E4:90:69:3B:C2:C0 (Rockwell) Source IP: 172.16.3.10 (fgs-47631ehh) Destination IP: 172.16.2.102 (pic_tesim) Source port: 58324 Destination port: 44818	IP address: 172.16.3.10 (Private IP) Host name: fgs-47631ehh Other host names: fgs-47631ehh.lan.lab Host MAC addresses: 40:AB:F0:3D:4B:AE (HewlettP) Last seen: Oct 12, 2020 12:52:01 Other observed MAC addresses: E4:90:69:3B:C2:C3 (Rockwell) E4:90:69:3B:C2:C2 (Rockwell) E4:90:69:3B:C2:C1 (Rockwell) 7C:0E:CE:67:86:83 (Cisco) Role: EWS Other roles: Windows workstation, Terminal server, Terminal client, Master Vendor and model: Rockwell DCOM (TCP 135, 49155, 49159) DNS (TCP 53) DNS (UDP 53, 5355) ETHIP (TCP 44818) ETHIP (UDP 44818) FailedConnection (TCP 23, 80, 139, 1332, 8000, 8443)	Command: Stop controller Destination route: Module 2 User name: FGS-47631EHH\Administrator

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

The screenshot shows the Forescout alert details for a configuration download command. The alert ID is 169543, timestamped Oct 13, 2020 13:46:20. The detection engine is Industrial threat library (ITL) and the ID and name is `itl_ops_dop_ether_download - EtherIP configuration download command`. The description notes a potentially dangerous EtherIP operation where a master or operator has requested a PLC to initiate a configuration download, which may be part of regular maintenance but can also be used in a cyber attack. The severity is High. The source host info includes IP address 172.16.3.10, host name fgs-47631ehh, and other host names fgs-47631ehh.lan.lab. The source MAC address is 40:AB:F0:3D:48:AE (HewlettP). The destination MAC is E4:90:69:3B:C2:C0 (Rockwell). The source IP is 172.16.3.10 (fgs-47631ehh). The destination IP is 172.16.2.102 (pic\_tesim). The source port is 58324. The alert details pane shows the command was Configuration download, user was FGS-47631EHH\Administrator, and the downloaded items included Program:MainProgram, User Tasks: TaskMainTask, I/O Maps: MapPic\_Uptime, MapControl\_host\_eip, and MapNetwork.

1563 

### D.8.3 Build 3

1564 

#### D.8.3.1 Configuration

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

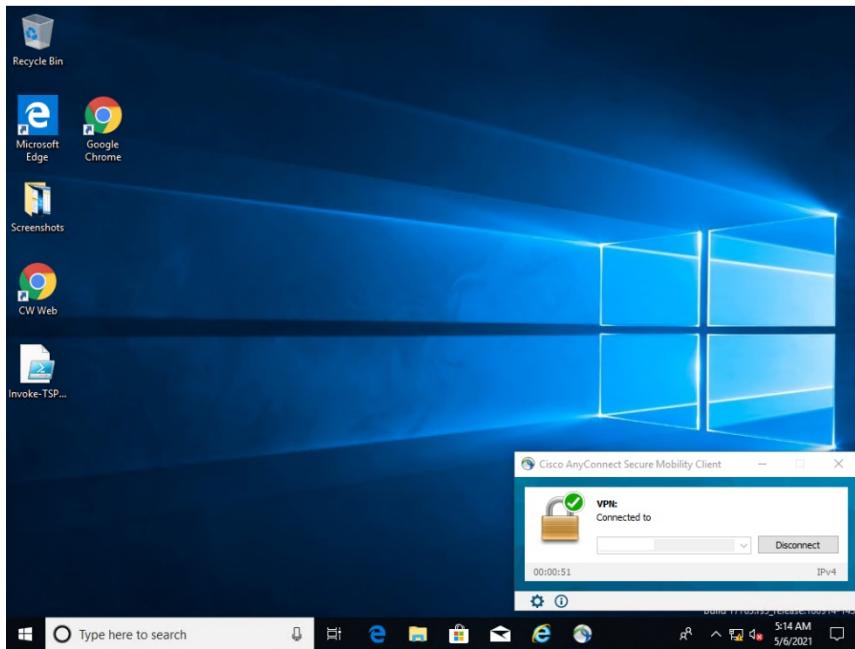
1572 

#### D.8.3.2 Test Results

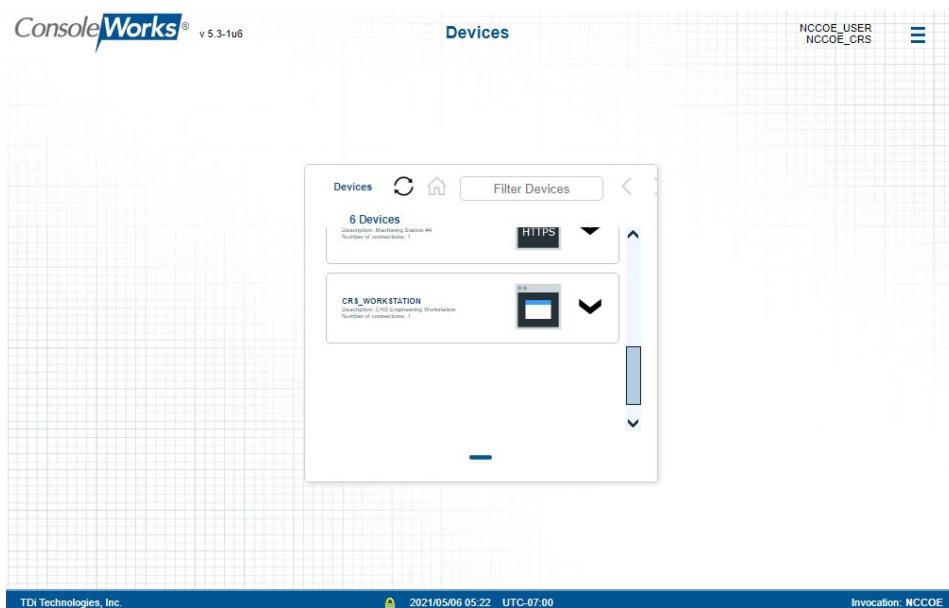
1573 In this build, a remote session to the CRS workstation is established to perform PLC file operations as  
 1574 shown in [Figure D-86](#) and [Figure D-87](#). Dragos is able to detect the PLC file modifications as shown in  
 1575 [Figure D-88](#) with details shown in [Figure D-89](#).

DRAFT

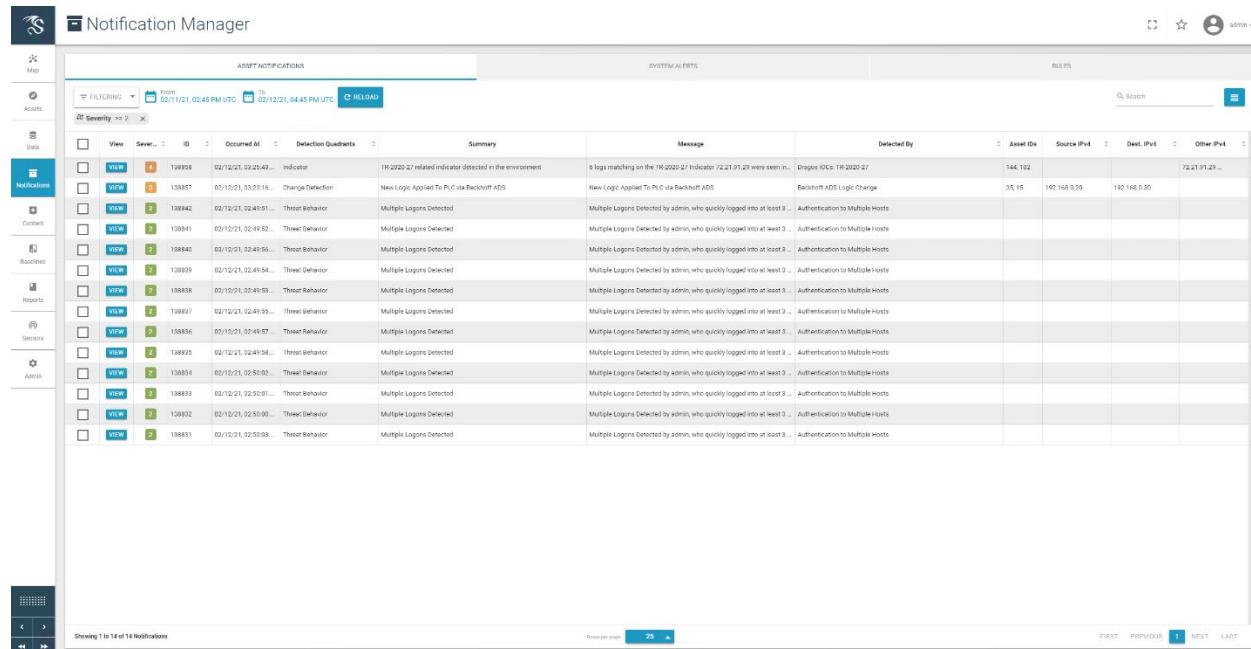
1576 **Figure D-86: VPN Connection to the Manufacturing Environment**



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



1578 **Figure D-88: Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the**  
 1579 **Beckhoff PLC**



The screenshot shows the Dragos Notification Manager interface. The left sidebar includes links for Map, Assets, Data, Notifications (selected), Context, Business, Reports, Sensors, and Admin. The main area has tabs for 'ARMY NOTIFICATIONS' (selected) and 'SYSTEM ALERTS'. A search bar at the top right shows 'admin'. The 'ARMY NOTIFICATIONS' tab displays a table of 14 notifications. The columns are: View, Severity, ID, Occurred At, Detection Quadrant, Summary, Message, Detected By, Asset ID, Source IP, Dest IP, and Other IP. The notifications detail various detection points such as 'Indicator', 'Change Detection', and 'Threat Behavior' across different dates and times. Most notifications are categorized under 'Multiple Logins Detected' or 'Threat Behavior'. The 'Detected By' column includes entries like 'Dragos IOC: IR-2020-27', 'Beckhoff AD5 Logic Change', and 'Authentication to Multiple Hosts'. The 'Source IP' and 'Dest IP' columns show network addresses like '192.168.0.20' and '192.168.0.30'. The bottom of the table shows pagination with 'Showing 1 to 14 of 14 Notifications' and a '25' button.

View	Severity	ID	Occurred At	Detection Quadrant	Summary	Message	Detected By	Asset ID	Source IP	Dest IP	Other IP
VIEW	INFO	138898	02/12/21, 02:45:42...	Indicator	IR-2020-27 related indicator detected in the environment	8 logs matching on the IR-2020-27 Indicator 72.21.91.29 were seen in the last 24 hours	Dragos IOC: IR-2020-27	144,112		72.21.91.29...	
VIEW	INFO	138857	02/12/21, 03:23:16...	Change Detection	New Logic Applied To PLC via Beckhoff AD5	New Logic Applied To PLC via Beckhoff AD5	Beckhoff AD5 Logic Change	35,15	192.168.0.20	192.168.0.30	
VIEW	INFO	138842	02/12/21, 02:49:51...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138841	02/12/21, 02:49:52...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138840	02/12/21, 02:49:59...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138839	02/12/21, 02:49:54...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138838	02/12/21, 02:49:53...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138837	02/12/21, 02:49:55...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138836	02/12/21, 02:49:57...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138835	02/12/21, 02:49:59...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138834	02/12/21, 02:50:02...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138833	02/12/21, 02:50:01...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138832	02/12/21, 02:50:00...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				
VIEW	INFO	138831	02/12/21, 02:50:08...	Threat Behavior	Multiple Logins Detected	Multiple Logins Detected by admin, who quickly logged into at least 3...	Authentication to Multiple Hosts				

1580 **Figure D-89: Dragos Alert Details for the PLC Logic File Download**

The screenshot shows the Dragos Alert Details interface for a specific alert. The alert details are as follows:

- WHAT HAPPENED:** New Logic Applied To PLC via Beckhoff ADS.
- OCCURRED AT:** 02/12/2021, 03:23 PM UTC.
- SOURCE:** Network Traffic.
- ZONES:** CRS - Level 1.
- ACTIVITY GROUP:** N/A.
- ICS CYBER KILLCHAIN STEP:** None.
- ICSA ATTACK TACTIC:** Execution.
- ICSA ATTACK TECHNIQUE:** Change Program State.
- QUERY-FOCUSED DATASETS:** No Applicable Query-Focused Datasets.
- POLYBOOKS:** No Associated Polybooks.
- CASES:** No Cases Linked.
- NOTIFICATION RECORD:** No Associated Record.
- NOTIFICATION COMPONENTS:** View in Kibana.

**ASSOCIATED ASSETS**

View	Type	ID	Name	Dic.
VIEW	Engineering View	35	POLARIS	192.168.0.20 src
VIEW	Process Supervision	15	Supervisory PLC	192.168.0.20 dst

**RELATED NOTIFICATIONS (0)**

ID	Occurred At	Summary
No related notifications.		

Buttons at the bottom include: < PREV, CLOSE, MARK AS READ, CREATE A RULE, CREATE CASE, and NEXT >.

1581 

## D.8.4 Build 4

1582 

### D.8.4.1 Configuration

- 1583     ■ Behavior Anomaly Detection: Azure Defender for IoT
  - 1584         ● Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- 1586     ■ Remote Access, User Authentication/User Authorization: Dispel
  - 1587         ● Dispel VDI is configured to allow authorized users to access the PCS environment through the Dispel Enclave to the Dispel Wicket.

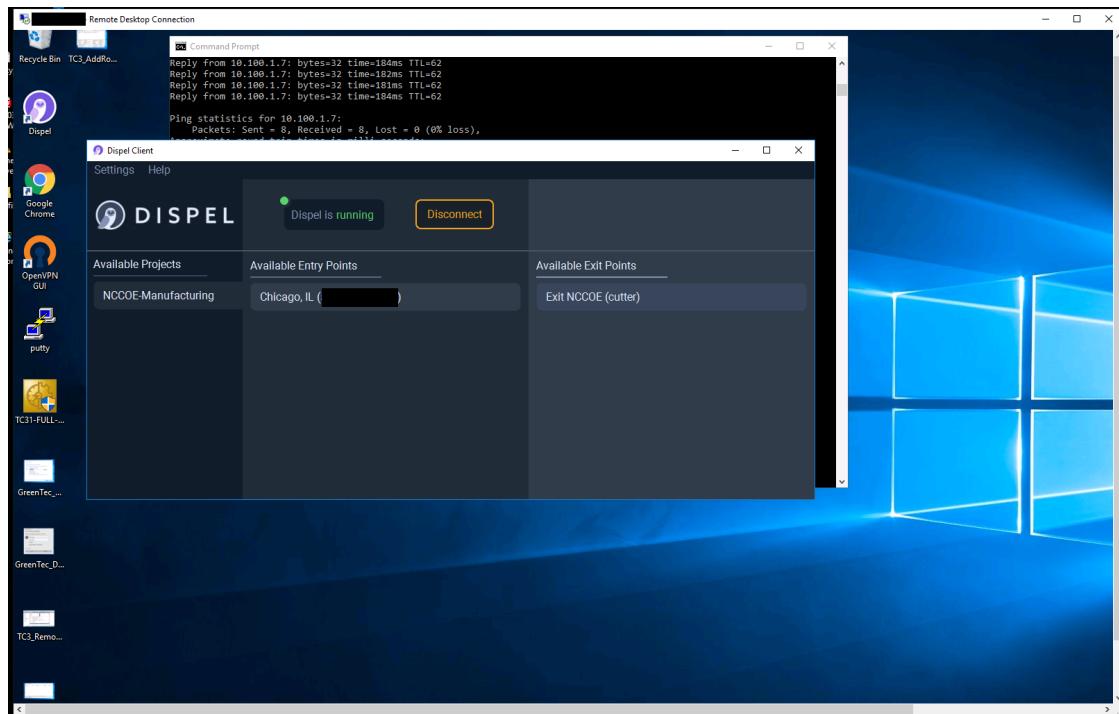
1589 

### D.8.4.2 Test Results

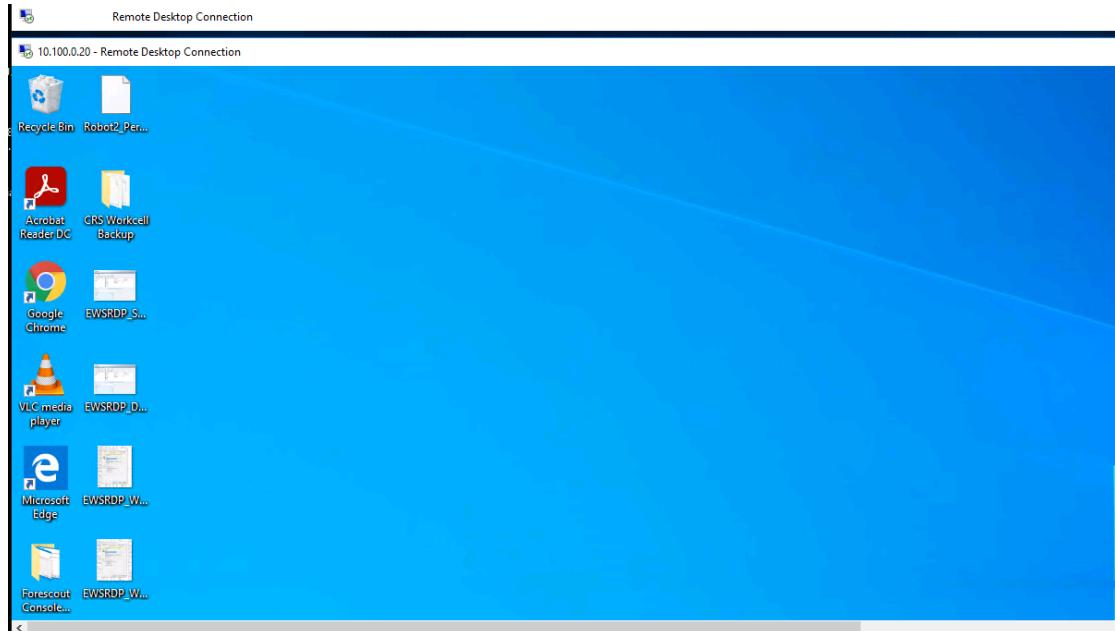
1590 [Figure D-90](#) and [Figure D-91](#) show the connection to the CRS environment through the Dispel VDI. The  
 1591 changes to the PLC programs are detected by Azure Defender for IoT, as shown in [Figure D-92](#), because  
 1592 the Dispel VDI is not an authorized programming device.

DRAFT

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



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



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

The screenshot shows an 'Alert Detected' message from Mar 17, 2021, at 11:36:01 AM. It states that an asset not defined as a programming device performed a programming change on a PLC. The source asset is 10.100.1.61 and the destination PLC asset is 192.168.0.30. Below this, a table lists two devices: CX-17DB08 and 10.100.1.61. A red bar at the bottom indicates the alert status.

Type	Name
CX-17DB08	
10.100.1.61	

[Filter events by related devices](#)

**Alert**

## 1596 D.9 Executing Scenario 9: Protect from Modification of Historian Data

1597 An attacker who has already gained access to the corporate network attempts to modify historian  
 1598 archive data located in the DMZ. The expected result is the behavioral anomaly detection products  
 1599 detect the connection to the historian archive. File modification is prevented by the file integrity  
 1600 checking capability.

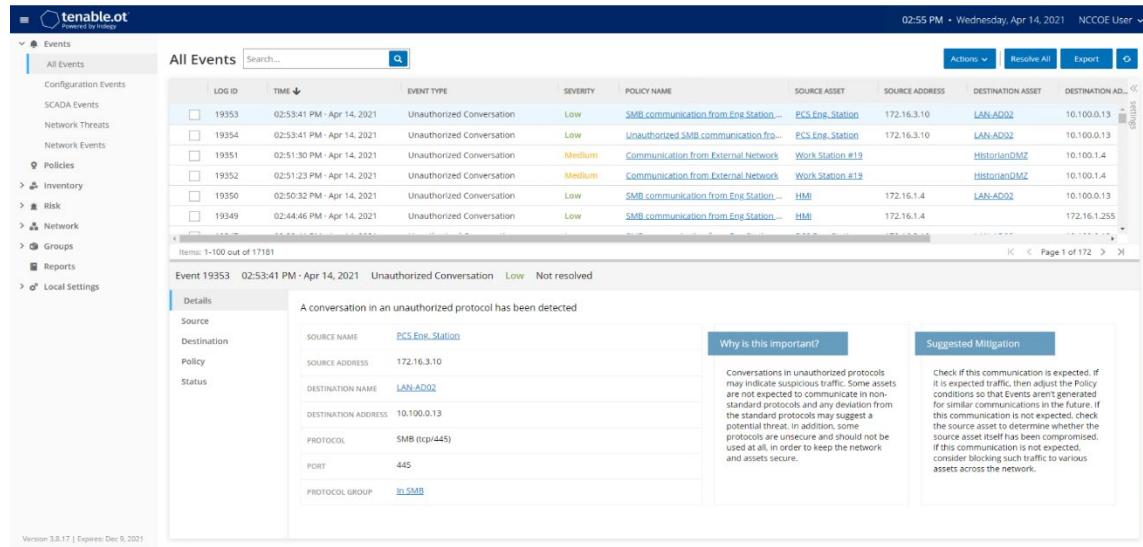
### 1601 D.9.1 Build 1

#### 1602 D.9.1.1 Configuration

- 1603     ▪ Behavior Anomaly Detection: Tenable.ot
  - 1604         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1605     ▪ File Integrity Checking: ForceField
  - 1606         • PI Server is configured to use ForceField drive.

### 1607 *D.9.1.2 Test Results*

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



The screenshot shows the Tenable.ot web interface with the following details:

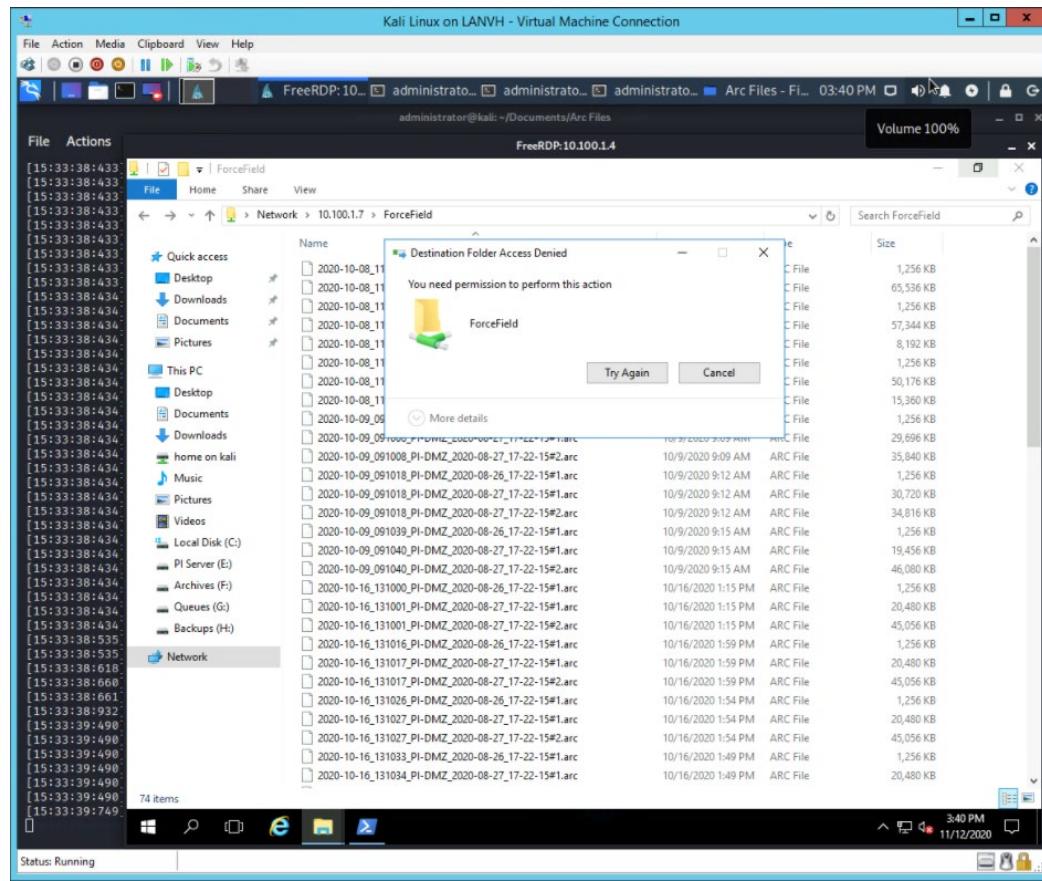
- Header:** 02:55 PM • Wednesday, Apr 14, 2021 NCCOE User
- Left Sidebar:** Events, All Events, Configuration Events, SCADA Events, Network Threats, Network Events, Policies, Inventory, Risk, Network, Groups, Reports, Local Settings.
- Main Content:**
  - Table:** All Events
 

LOG ID	TIME	EVENT TYPE	SEVERITY	POLICY NAME	SOURCE ASSET	SOURCE ADDRESS	DESTINATION ASSET	DESTINATION AD...
19353	02:53:41 PM - Apr 14, 2021	Unauthorized Conversation	Low	SMB communication from Eng_Station...	PCS_Eng_Station	172.16.3.10	LAN-AD02	10.100.0.13
19354	02:53:41 PM - Apr 14, 2021	Unauthorized Conversation	Low	Unauthorized SMB communication fro...	PCS_Eng_Station	172.16.3.10	LAN-AD02	10.100.0.13
19351	02:51:30 PM - Apr 14, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19	172.16.1.4	HistorianDMZ	10.100.1.4
19352	02:51:23 PM - Apr 14, 2021	Unauthorized Conversation	Medium	Communication from External Network	Work Station #19	172.16.1.4	HistorianDMZ	10.100.1.4
19350	02:50:32 PM - Apr 14, 2021	Unauthorized Conversation	Low	SMB communication from Eng_Station...	HMI	172.16.1.4	LAN-AD02	10.100.0.13
19349	02:44:46 PM - Apr 14, 2021	Unauthorized Conversation	Low	SMB communication from Eng_Station...	HMI	172.16.1.4		172.16.1.255
  - Event Detail:** Event 19353 - 02:53:41 PM - Apr 14, 2021 Unauthorized Conversation Low Not resolved
 

Details	
A conversation in an unauthorized protocol has been detected	
Source	SOURCE NAME: PCS_Eng_Station
Destination	SOURCE ADDRESS: 172.16.3.10
Policy	DESTINATION NAME: LAN-AD02
Status	DESTINATION ADDRESS: 10.100.0.13
	PROTOCOL: SMB (tcp/445)
	PORT: 445
	PROTOCOL GROUP: to_SMB
  - Why is this important?** Conversations in unauthorized protocols may indicate that the network assets are not expected to communicate in non-standard protocols and any deviation from the standard protocols may suggest a potential threat. In addition, some protocols are unsecure and should not be used at all, in order to keep the network and assets secure.
  - Suggested Mitigation:** Check if this communication is expected. If it is expected, update the Policy conditions so that Events aren't generated for similar communications in the future. If this communication is not expected, check the source asset to determine whether the source asset has been compromised. If this communication is not expected, consider blocking such traffic to various assets across the network.

DRAFT

1611 **Figure D-94: GreenTec Denies Modification and Deletion File Operations in the Protected Drive**



1612 **D.9.2 Build 2**

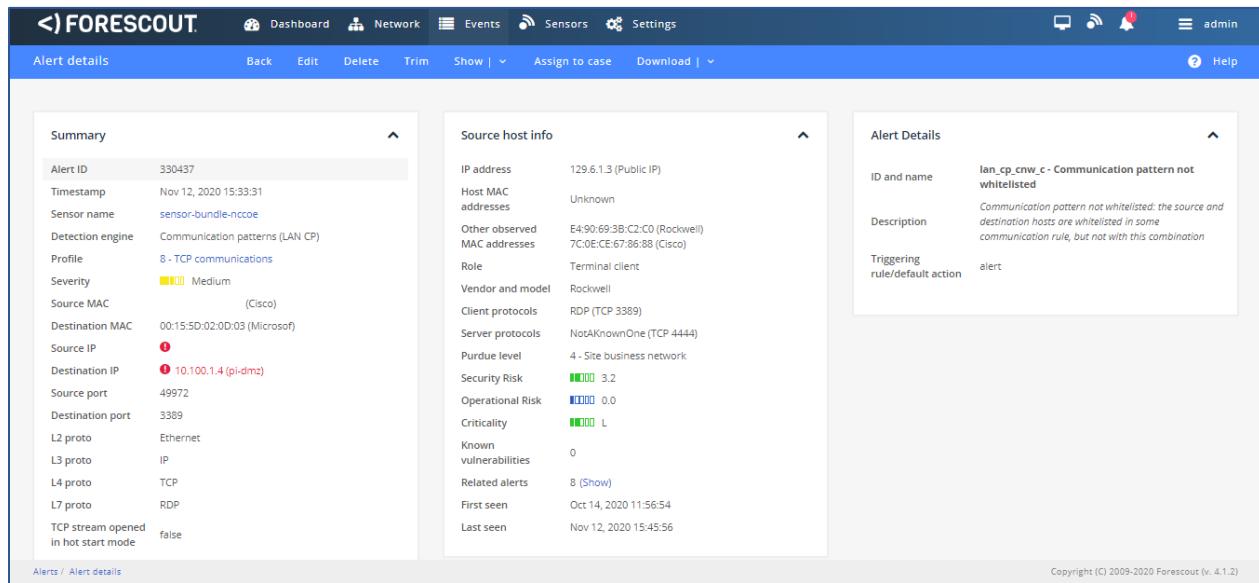
1613 **D.9.2.1 Configuration**

- 1614     ▪ Behavior Anomaly Detection: eyeInspect
- 1615         • Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1616     ▪ File Integrity Checking: ForceField
- 1617         • PI Server is configured to use ForceField drive.

1618 **D.9.2.2 Test Results**

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

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



The screenshot shows the Forescout alert details interface. The top navigation bar includes links for Dashboard, Network, Events, Sensors, Settings, and admin. Below the navigation is a toolbar with Back, Edit, Delete, Trim, Show | ▾, Assign to case, Download | ▾, Help, and a question mark icon.

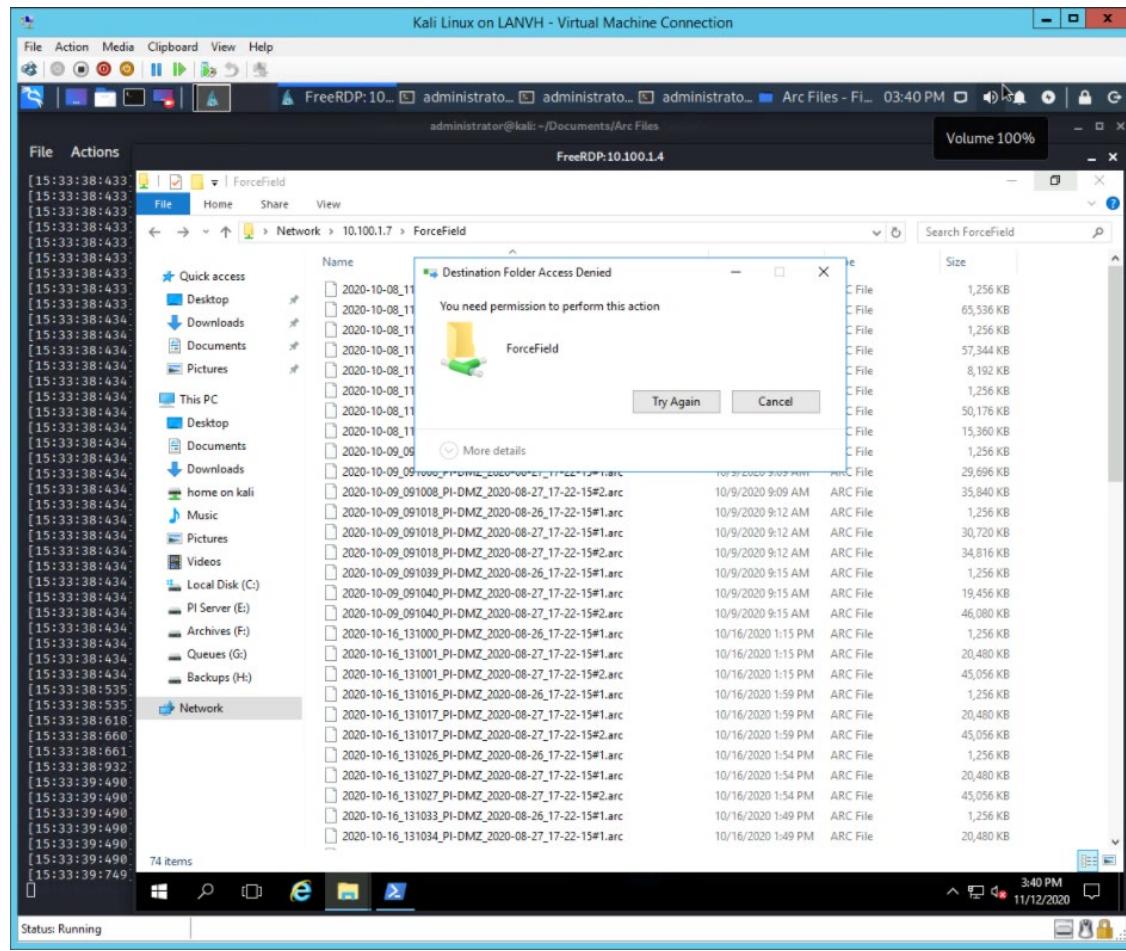
The main content area is divided into three panels:

- Summary:** Contains alert details such as Alert ID (330437), Timestamp (Nov 12, 2020 15:33:31), Sensor name (sensor-bundle-nccoe), Detection engine (Communication patterns (LAN CP)), Profile (8 - TCP communications), Severity (Medium), Source MAC (Unknown), Destination MAC (00:15:5D:02:D0:03 (Microsoft)), Source IP (10.100.1.4), Destination IP (10.100.1.4 (pl-dmz)), Source port (49972), Destination port (3389), L2 proto (Ethernet), L3 proto (IP), L4 proto (TCP), L7 proto (RDP), and TCP stream opened in hot start mode (false).
- Source host info:** Lists host details like IP address (129.6.1.3 (Public IP)), Host MAC addresses (Unknown), Other observed MAC addresses (E4:90:69:3B:C2:C0 (Rockwell) 7C:0E:CE:67:86:88 (Cisco)), Role (Terminal client), Vendor and model (Rockwell), Client protocols (RDP (TCP 3389)), Server protocols (NotAKnownOne (TCP 4444)), Purdue level (4 - Site business network), Security Risk (Medium 3.2), Operational Risk (Low 0.0), Criticality (Low L), Known vulnerabilities (0), and Related alerts (8 (Show)).
- Alert Details:** Shows the alert ID and name (lan\_cp\_cnw\_c - Communication pattern not whitelisted), Description (Communication pattern not whitelisted: the source and destination hosts are whitelisted in some communication rule, but not with this combination), and Triggering rule/default action (alert).

At the bottom left is a breadcrumb navigation (Alerts / Alert details). At the bottom right is a copyright notice: Copyright (C) 2009-2020 Forescout (v. 4.1.2).

DRAFT

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



1624 **D.9.3 Build 3**

1625 **D.9.3.1 Configuration**

- 1626     ▪ Behavior Anomaly Detection: Dragos
- 1627         • Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- 1628
- 1629     ▪ File Integrity Checking: ForceField
- 1630         • PI Server is configured to use ForceField drive.

1631 **D.9.3.2 Test Results**

- 1632 Dragos detects the remote session as shown in [Figure D-97](#). When the user attempts to alter a file on
- 1633 the protected drive, GreenTec denies the operation as shown in [Figure D-98](#).

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

The screenshot displays the Dragos Security Platform's incident details page for an 'RDP Negotiation Request'.

**DETECTION INFORMATION:**

- WHAT HAPPENED: RDP Negotiation Request
- OCCURRED AT: 01/17/23, 19:48 UTC
- COUNT: 1
- DETECTED BY: RDP Port Monitor
- DETECTION QUAD: None Detected
- ACTIVITY GROUP: KENO/NAME
- MITRE ATTACK FOR ICS TACTIC: Command And Control
- QUERY-FOCUSED DATASETS: No Applicable Query-Focused Datasets
- PLAYBOOKS: No Associated Playbooks
- CASES: No Cases Linked

**LAST SEEN:** 01/17/23, 19:48 UTC

**STATE:** Unresolved

**SOURCE:** Network Traffic

**ZONE:** DMZ\_NIST

**ICS CYBER KILLCHAIN STEP:** Stage 1 - Act on Objectives

**MITRE ATTACK FOR ICS TECHNIQUE:** T1089: Commonly Used Port

**NOTIFICATION RECORD:** No Associated Record

**NOTIFICATION COMPONENTS:** View in Xpanse

**ASSOCIATED ASSETS:**

Type	ID	Name	IP
Windows Serv	85	Asset 85	10.100.1.4
Asset	844	Asset 844	10.100.1.4

**COMMUNICATIONS SUMMARY:**

Diagram illustrating a communication flow between a Windows Server (Microsoft Corporation, pid=drz) at 10.100.1.4 and an Asset (10.100.1.4). The connection is labeled 'SSL'.

Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
SSL			10.100.1.4		2.1 MB	15.9 MB

**RELATED NOTIFICATIONS:**

No Related Notifications.

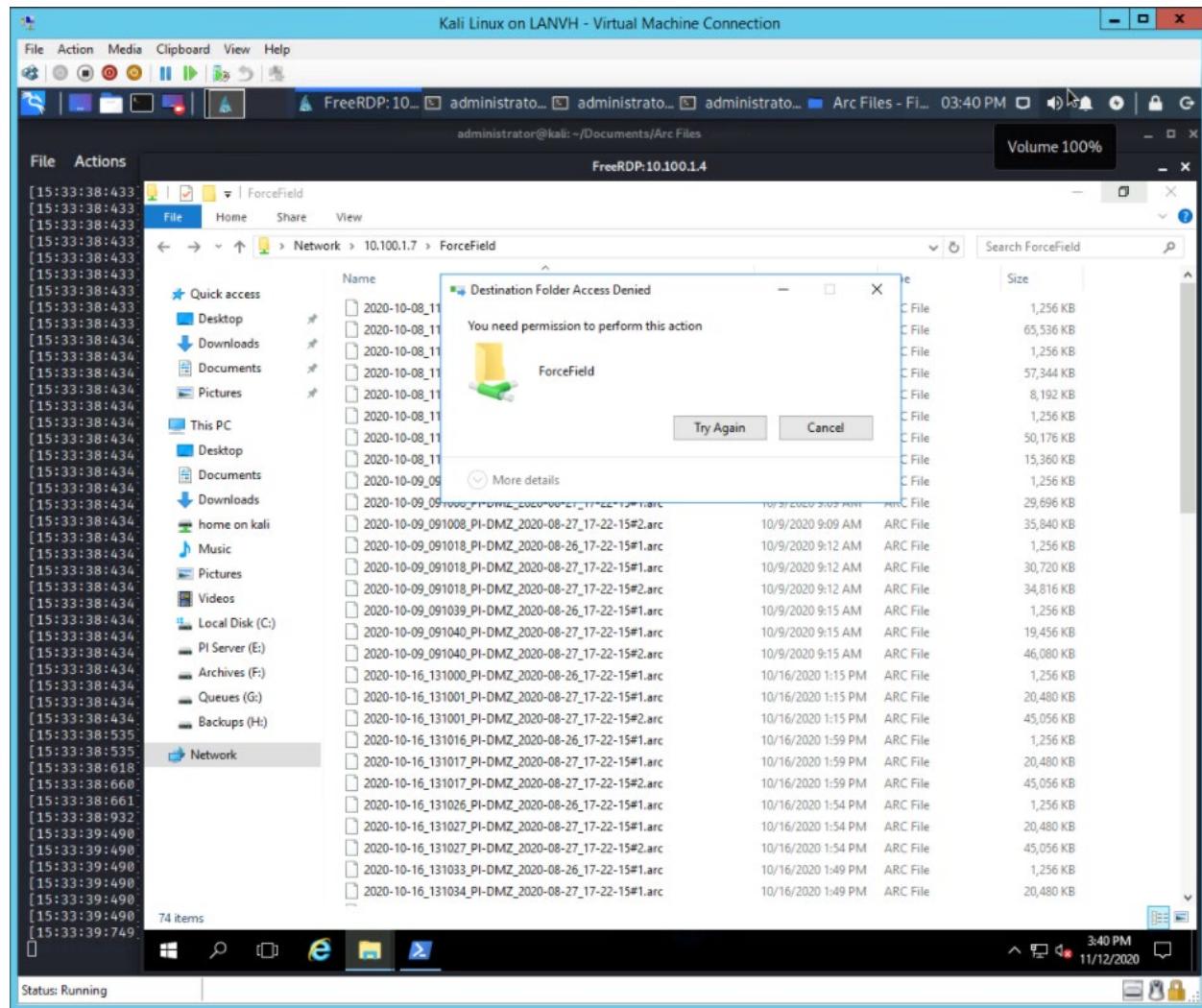
ROWS PER PAGE: 10

FIRST PREVIOUS PREVIOUS LAST NEXT > LAST >

CREATE A RULE CREATE CASE

DRAFT

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



1636 **D.9.4 Build 4**

1637 **D.9.4.1 Configuration**

- 1638     ■ Behavior Anomaly Detection: Azure Defender for IoT
  - 1639         ● Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.
- 1641     ■ File Integrity Checking: ForceField
  - 1642         ● PI Server is configured to use ForceField drive.

#### 1643 *D.9.4.2 Test Results*

1644 The connection to the Historian data storage was detected by Azure Defender for IoT as shown in Figure  
1645 D-99. [Figure D-100](#) shows a Windows error message after attempting to overwrite protected Historian  
1646 files.

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

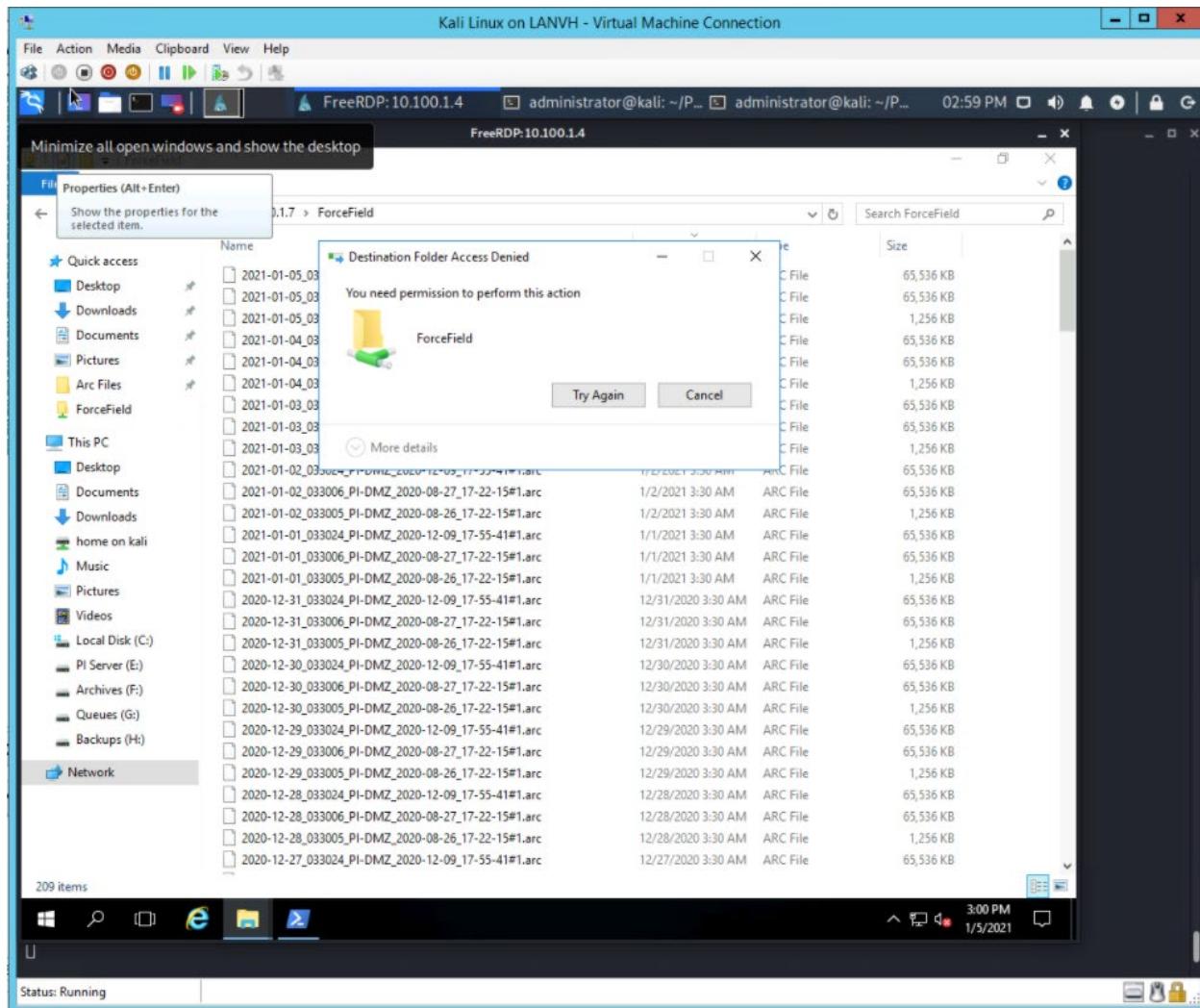
The screenshot shows the Azure Defender for IoT Event Timeline interface. The left sidebar includes options like Dashboard, Devices Map, Device Inventory, Alerts, Reports, Data Mining, Investigation, Risk Assessment, Attack Vectors, Administration, Custom Alerts, and Azure Defender for IoT Version 10.0.3. The main area displays the Event Timeline for April 14, 2021. Three events are listed:

- File Transfer Detected**: April 14, 2021 2:43:13 PM. HTTP File transfer from client IP: 10.100.1.4, Server: Content type application/vnd.ms-cab-compressed. Status: Notice.
- Remote Access Connection Established**: April 14, 2021 2:41:47 PM. Connection detected from to 10.100.1.4 using Remote Desktop.
- Alert Detected**: April 14, 2021 2:36:43 PM. A new asset was detected on the network. Asset 10.100.0.61 was added to your network. Status: Info. A note says: Verify that this is a valid network asset.

A sidebar on the right shows a list of devices: Type (PI-DMZ), Name (Internet). A link "Filter events by related devices" is also present.

DRAFT

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



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

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

### 1653 **D.10.1 All Builds**

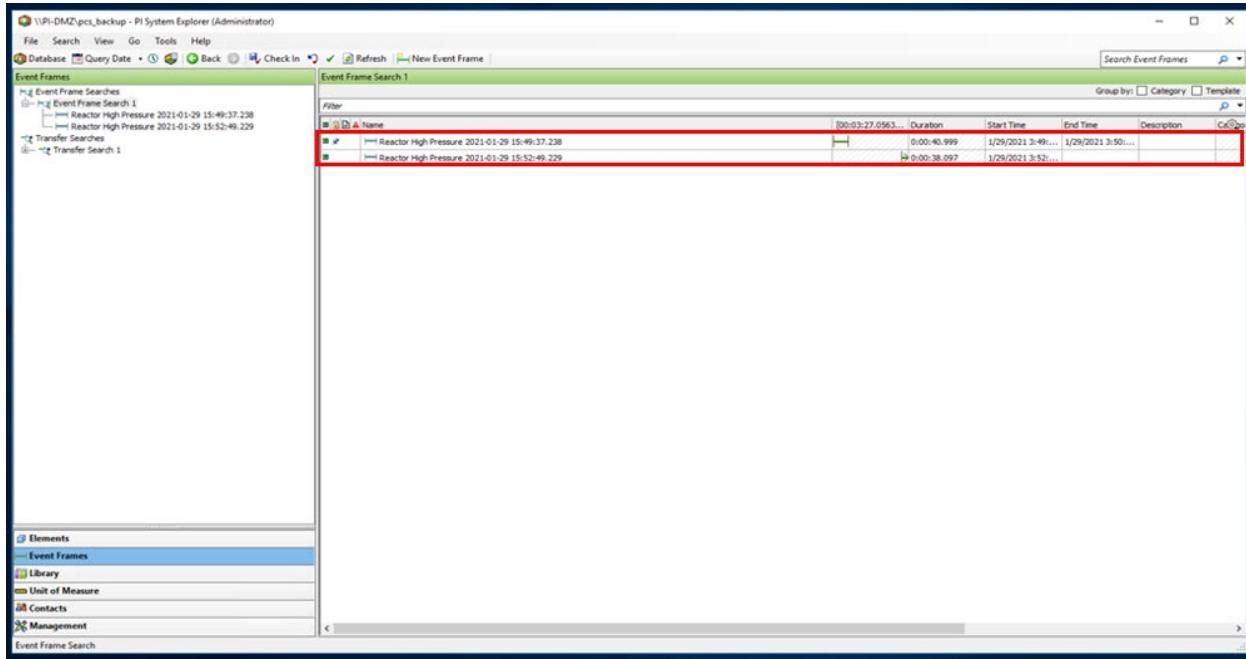
#### 1654 **D.10.1.1 Configuration**

- 1655     ■ Behavior Anomaly Detection: PI Server
  - 1656         ● Configured to receive process data from across the manufacturing system.
  - 1657         ● Configured to perform analysis on incoming data points.

1658 **D.10.1.2 Test Results**

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

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

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

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

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

1670 **D.11.1 Build 1**1671 **D.11.1.1 Configuration**

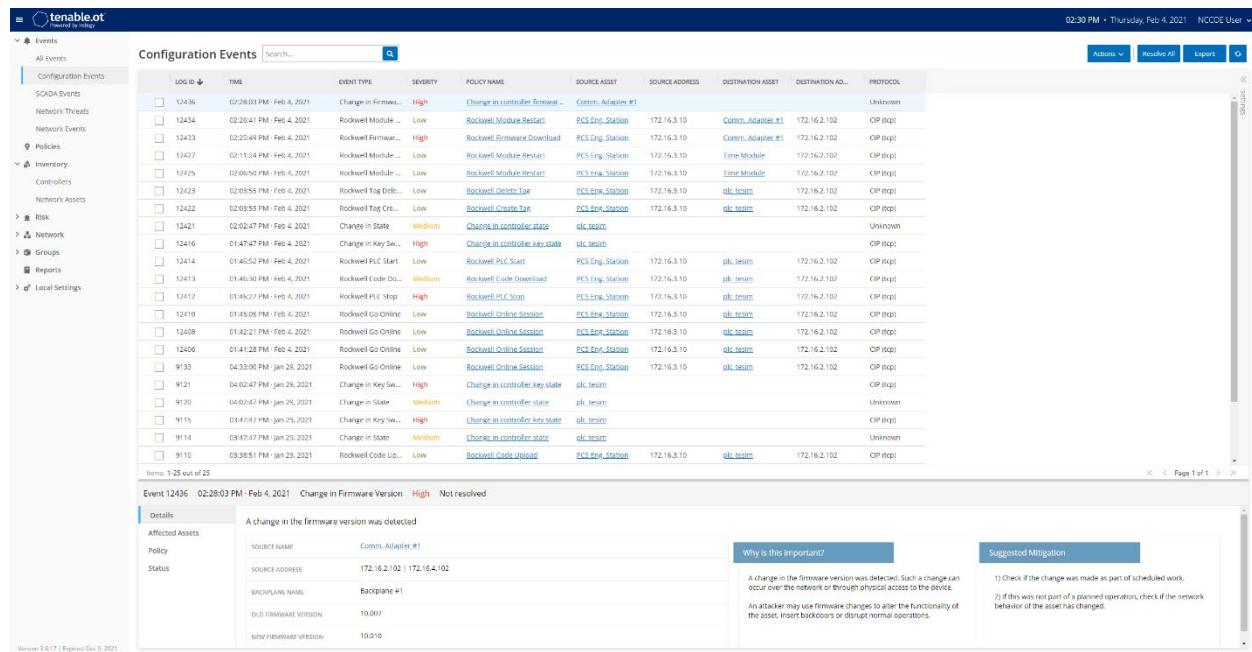
- 1672     ■ Behavior Anomaly Detection: Tenable.ot
  - 1673         ● Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.
- 1674     ■ Remote Access: Cisco VPN
  - 1675         ● Configured to allow authorized VPN users access to ConsoleWorks web interface.

- 1676     ■ User Authentication/User Authorization: ConsoleWorks  
 1677         ● Configured for accessing the PCS environment.

### 1678 *D.11.1.2 Test Results*

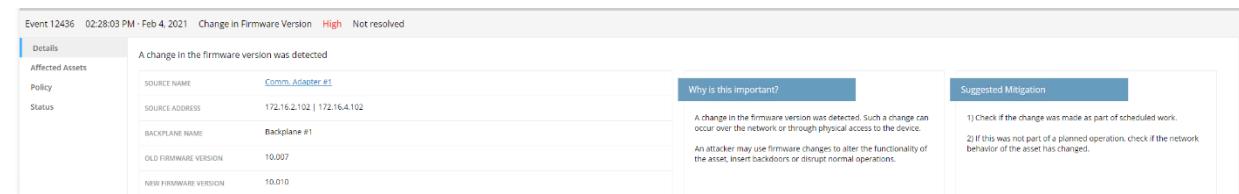
1679 Figure D-102 depicts the list of the events detected by Tenable.ot resulting from the firmware change.  
 1680 The details of one of the alerts are shown in Figure D-103

1681 **Figure D-102: Tenable.ot Detects a Collection of Events Generated by a Firmware Change**



The screenshot shows the Tenable.ot interface with the title 'Configuration Events'. The left sidebar includes sections for Events, Configuration Events, SODA Events, Network Threats, Network Events, Policies, Inventory, Controllers, and Network Assets. The main area displays a table of events with columns: LOG ID, TIME, EVENT TYPE, SEVERITY, POLICY NAME, SOURCE ASSET, SOURCE ADDRESS, DESTINATION ASSET, DESTINATION AD., and PROTOCOL. One event is highlighted in blue: Event ID 12436 at 02:28:03 PM - Feb 4, 2021, with a severity of High and policy name 'Change in controller firmware -'. The source asset is 'Comm\_Adapter #1' and the destination asset is 'UnKnown'. The protocol is 'Unknown'. Other events listed include changes in key state, PLC start, and online sessions.

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



This screenshot shows the detailed view for the event from Figure D-102. The event is identified as 'Event 12436 02:28:03 PM - Feb 4, 2021 Change in Firmware Version High Not resolved'. The 'Details' tab is selected, showing that a change in the firmware version was detected. The 'Affected Assets' section lists the source name as 'Comm\_Adapter #1' and the source address as '172.16.2.102 | 172.16.4.102'. The 'Policy' section shows the policy name as 'Change in controller key state'. The 'Status' section provides the old and new firmware versions: 'OLD FIRMWARE VERSION' is 10.0007 and 'NEW FIRMWARE VERSION' is 10.0110. A 'Why is this important?' box states: 'A change in the firmware version was detected. Such a change can occur over the network or through physical access to the device.' A 'Suggested Mitigation' box contains two items: '1) Check if the change was made as part of scheduled work.' and '2) If this was not part of a planned operation, check if the network behavior of the asset has changed.'

1683 **D.11.2 Build 2**

### 1684 *D.11.2.1 Configuration*

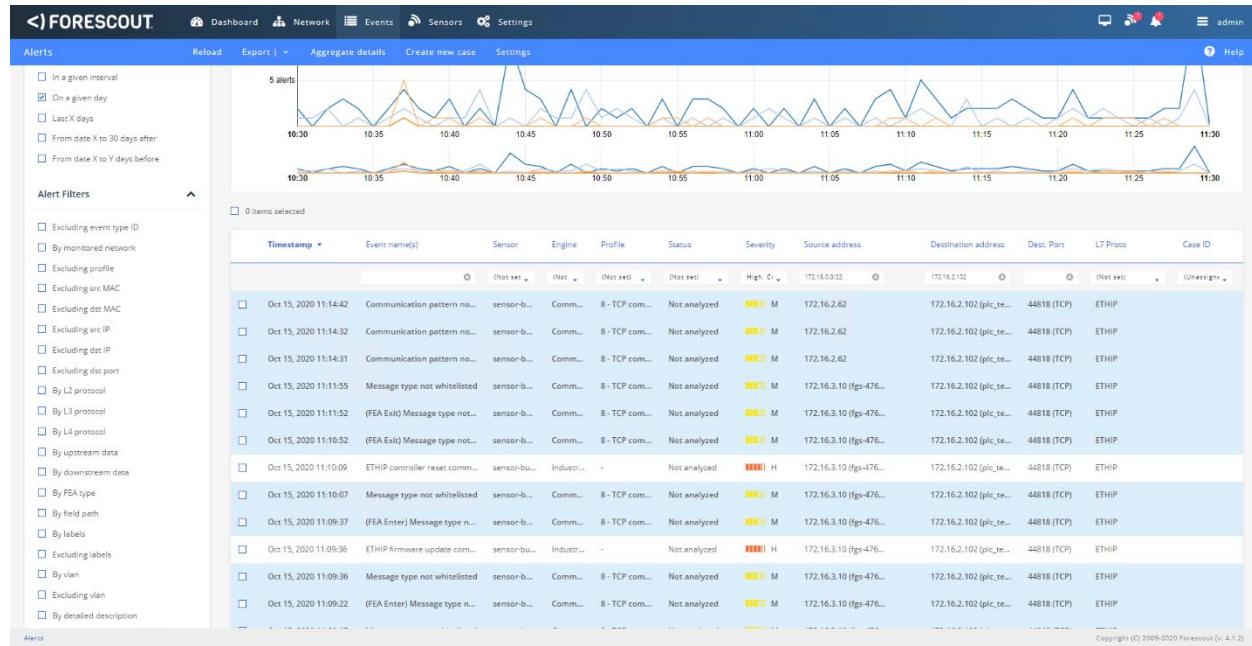
- 1685     ■ Behavior Anomaly Detection: eyelnspect  
 1686         ● Configured to receive packet streams from DMZ, Testbed LAN, and PCS VLAN 1 and 2.  
 1687     ■ Remote Access, User Authentication/User Authorization: Dispel

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

1690 **D.11.2.2 Test Results**

1691 Figure D-104 shows the activities detected by Forescout as a result of firmware change. Figure D-104,  
 1692 [Figure D-105](#) and [Figure D-106](#) show more details on the alerts associated with the firmware update.

1693 **Figure D-104: Forescout Detects a Collection of Alerts Associated with the Firmware Change**



## DRAFT

1694

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

The screenshot shows the Forescout alert details interface. The top navigation bar includes links for Dashboard, Network, Events, Sensors, Settings, and Admin. The main content area is divided into several sections:

- Alert details** (top left): Shows Alert ID 188671, Timestamp Oct 15, 2020 11:09:36, and Sensor name sensor-bundle-rcosse.
- Summary** (left panel): Contains detailed information about the alert, including Detection engine (Industrial threat library (ITL)), ID and name (il\_esp\_dspdp\_ethip\_firmware\_update - ETHIP firmware update command), and Description (Potentially dangerous ETHIP operation: the ETHIP master or an operator has requested a PLC to initiate a firmware update. This operation may be part of regular maintenance but can also be used in a cyber attack.). It also lists Severity (High), Source MAC (40:AB:F0:3D:4B:AE (HewlettP)), Destination MAC (E4:90:69:3B:C2:C0 (Rockwell)), Source IP (172.16.3.10 (gs-47631ehh)), Destination IP (172.16.2.102 (plc\_resin)), Source port (50753), Destination port (44818), L2 proto (Ethernet), L3 proto (IP), L4 proto (TCP), L7 proto (ETHIP), Status (Not analyzed), Labels, and User notes.
- Source host info** (middle left): Lists IP address (172.16.3.10 (Private IP)), Host name (fgv-47631ehh), Other host names (fgv-47631ehh.lan.lab), Host MAC addresses (40:AB:F0:3D:4B:AE (HewlettP) Last seen: Oct 19, 2020 10:35:40), Other observed MAC addresses (E4:90:69:3B:C2:C3 (Rockwell) E4:90:69:3B:C2:C2 (Rockwell) E4:90:69:3B:C2:C1 (Rockwell) 7C:0E:CE:67:86:88 (Cisco) 7C:0E:CE:67:86:83 (Cisco)), Role (EWS), Other roles (Windows workstation, Terminal server, Terminal client, Master), Vendor and model (Rockwell), and Client protocols (DCOM (TCP 135, 49155, 49159) DNS (TCP 53) DNS (UDP 53) DNS (TCP 5355) DNS (UDP 5355) ETHIP (TCP 44818) ETHIP (UDP 44818) FailedConnection (TCP 23, 80, 139, 1332, 8000, 8443) HTTP (TCP 8000, 8530) Kerberos (TCP 88) LDAP (TCP 389) LDAP (UDP 389) NTP (UDP 123) NetBIOS (UDP 137) NetKnownOne (TCP 2500, 2501, 4444, 10005) NetKnownOne (UDP 1514) RDP (TCP 3389) SMB (TCP 445) SMB (UDP 138) SSDP (UDP 1900) SSH (TCP 22) SSL (TCP 443, 3389, 10003, 10005) Syslog (UDP 514) DCOM (TCP 135, 6160) FailedConnection (TCP 139, 445, 11731) VMFS (TCP 6194))
- Alert details** (right panel): Displays Command: Firmware update, Destination route: Module 4, User name: FGS-47631EH\Administrator, and Updated firmware revision: 3.4.

At the bottom left is a breadcrumb navigation: Alerts / Alert details. At the bottom right is a copyright notice: Copyright (C) 2009-2020 Forescout (v. 8.1.2).

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

The screenshot shows a 'Scan details' interface with two main sections: 'Scan details' and a table of results.

**Scan details:**

Scan ID	15	Started on	Oct 15, 2020 11:14:28
Scan type	EtherNet/IP	Duration	01m37s
Scan targets	172.16.2.102	Scan status	Completed
Scanning sensors	PCS_Sensor	Scanned IPs	1
Scan policy		Responding hosts	1
Initiated by	Admin User	Updated hosts	1

**Result:**

Target IP	Scanning sensor	Scan status	Host status
172.16.2.102	PCS_Sensor	Completed	Updated

1 to 1 items of 1

**Result:**  
Result is not available.

### 1696 **D.11.3 Build 3**

#### 1697 **D.11.3.1 Configuration**

- 1698     ▪ Remote Access: Cisco VPN
  - 1699         • Configured to allow authorized VPN users to access only the ConsoleWorks web interface.
- 1700     ▪ User Authentication/User Authorization: ConsoleWorks
  - 1701         • Configured to allow remote access to hosts in manufacturing environment.
- 1702     ▪ Behavior Anomaly Detection: Dragos
  - 1703         • Configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN.

#### 1705 **D.11.3.2 Test Results**

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

DRAFT

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

The Dragos dashboard displays four main sections: MODEL, THREAT BEHAVIOR, CONFIGURATION, and INDICATOR. The MODEL section shows a large orange circle with the number '1' and a message about an OSisoft Event Frame of StationModeError. The THREAT BEHAVIOR section shows a green checkmark icon with the message 'NO KNOWN MALICIOUS BEHAVIOR DETECTED'. The CONFIGURATION section shows a large green circle with the number '2' and a message about Medium Description Code. The INDICATOR section shows a green checkmark icon with the message 'NO TECHNICAL ELEMENTS OF KNOWN MALICIOUS ACTIVITY DETECTED'. A sidebar on the right lists various navigation options.

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

This screenshot shows the detailed view of a firmware change alert. The left panel contains 'DETECTION INFORMATION' with fields like 'WHAT HAPPENED:', 'OCCURRED AT:', 'DETECTED BY:', 'ACTIVITY GROUP:', and 'RELATED NOTIFICATIONS'. The right panel shows 'ASSOCIATED ASSETS' (a table with one row), 'COMMUNICATIONS SUMMARY' (empty), and 'NOTIFICATION RECORDS' (empty). A sidebar on the right provides navigation links.

## 1710 **D.11.4 Build 4**

### 1711 **D.11.4.1 Configuration**

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

1718 *D.11.4.2 Test Results*

1719 Azure Defender for IoT alerts on the firmware update as shown below in Figure D-109.

1720 **Figure D-109: Azure Defender for IoT Alert Showing a Version Mismatch in the Firmware Build**

The screenshot shows the Azure Defender for IoT interface. On the left, there's a navigation sidebar with various options like Dashboard, Asset Map, Asset Inventory, Alerts (72), Reports, ANALYZE, Event Timeline, Data Mining, Investigation, Risk Assessment, Attack Vectors, ADMINISTRATION, Custom Alerts, Users, Forwarding, System Settings, Import Settings, SUPPORT, Horizon, and Support. The 'Alerts (72)' option is selected.

The main area is titled 'Alerts' and shows a list of alerts. One alert is highlighted with a red border:

- Version Build Mismatch**
- Policy Violation | Jan 6, 2021 2:00:37 PM (just now)
- The PLC Version Build was not the expected result
- Supervisory PLC ↔ Engineering Workstation
- Manage this Event**
- This is a Horizon custom alert that provides information resolved by a proprietary protocol plugin. If required, contact your security administrator for more details.
- Acknowledge**

Below this, there's a list of other alerts:

- POLICY VIOLATION Version Build Mismatch (Jan 6 14:00)
- OPERATIONAL Device is Suspected to be Disconnected (Unresponsive) (Jan 6 13:58)
- OPERATIONAL Suspicion of Unresponsive MODBUS Device (Jan 6 13:57)
- OPERATIONAL HTTP Client Error (Jan 6 13:21)
- POLICY VIOLATION Unauthorized Internet Connectivity Detected (Jan 6 07:10)
- OPERATIONAL Device is Suspected to be Disconnected (Unresponsive) (Jan 5 17:26)

## Appendix E Benefits of IoT Cybersecurity Capabilities

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

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

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

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

### E.1 Device Capabilities Mapping

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

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

**Table E-1: Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities to NIST Cybersecurity Framework Subcategories of the ICS Project**

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	<ul style="list-style-type: none"> <li>▪ Ability to uniquely identify the IoT device logically.</li> <li>▪ Ability to uniquely identify a remote IoT device.</li> <li>▪ Ability for the device to support a unique device ID.</li> <li>▪ Ability to configure IoT device access control policies using IoT device identity.</li> <li>▪ Ability to verify the identity of an IoT device.</li> <li>▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.</li> <li>▪ Ability to set and change authentication configurations, policies, and limitations settings for the IoT device.</li> <li>▪ Ability to create unique IoT device user accounts.</li> <li>▪ Ability to identify unique IoT device user accounts.</li> <li>▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions.</li> <li>▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface.</li> <li>▪ Ability to enable automation and reporting of account management activities.</li> <li>▪ Ability to establish conditions for shared/group accounts on the IoT device.</li> <li>▪ Ability to administer conditions for shared/group accounts on the IoT device.</li> <li>▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.</li> <li>▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.</li> <li>▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.</li> <li>▪ Providing the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used.</li> <li>▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources.</li> <li>▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.</li> <li>▪ Providing education explaining how to enforce authorized access at the system level.</li> </ul>	AC-2 IA-2 IA-4 IA-5 IA-8 IA-12
PR.AC-3: Remote access is managed.	<ul style="list-style-type: none"> <li>▪ Ability to configure IoT device access control policies using IoT device identity.           <ul style="list-style-type: none"> <li>○ Ability for the IoT device to differentiate between authorized and unauthorized remote users.</li> </ul> </li> </ul>	N/A	AC-17 AC-19 AC-20

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
	<ul style="list-style-type: none"> <li>■ Ability to authenticate external users and systems.</li> <li>■ Ability to securely interact with authorized external, third-party systems.</li> <li>■ Ability to identify when an external system meets the required security requirements for a connection.</li> <li>■ Ability to establish secure communications with internal systems when the device is operating on external networks.</li> <li>■ Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including: <ul style="list-style-type: none"> <li>○ usage restrictions</li> <li>○ configuration requirements</li> <li>○ connection requirements</li> <li>○ manufacturer established requirement</li> </ul> </li> <li>■ Ability to enforce the established local and remote access requirements.</li> <li>■ Ability to prevent external access to the IoT device management interface.</li> <li>■ Ability to control the IoT device's logical interface (e.g., locally or remotely).</li> <li>■ Ability to detect remote activation attempts.</li> <li>■ Ability to detect remote activation of sensors.</li> </ul>		
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	<ul style="list-style-type: none"> <li>■ Ability to assign roles to IoT device user accounts.</li> <li>■ Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary). <ul style="list-style-type: none"> <li>○ Ability to establish user accounts to support role-based logical access privileges.</li> <li>○ Ability to administer user accounts to support role-based logical access privileges.</li> <li>○ Ability to use organizationally defined roles to define each user account's access and permitted device actions.</li> <li>○ Ability to support multiple levels of user/process account functionality and roles for the IoT device.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.</li> <li>■ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces, such as for specific support, updates, ongoing maintenance, and other purposes.</li> <li>■ Providing documentation with instructions for the IoT device customer to follow for how to restrict interface connections that enable specific activities.</li> <li>■ Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis.</li> </ul>	AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
	<ul style="list-style-type: none"> <li>■ Ability to apply least privilege to user accounts.           <ul style="list-style-type: none"> <li>○ Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege.</li> <li>○ Ability to apply least privilege settings within the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions).</li> <li>○ Ability to limit access to privileged device settings that are used to establish and administer authorization requirements.</li> <li>○ Ability for authorized users to access privileged settings.</li> </ul> </li> <li>■ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions.</li> <li>■ Ability to enable automation and reporting of account management activities.</li> <li>■ Ability to establish conditions for shared/group accounts on the IoT device.</li> <li>■ Ability to administer conditions for shared/group accounts on the IoT device.</li> <li>■ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.</li> <li>■ Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on:           <ul style="list-style-type: none"> <li>○ run-time access control decisions facilitated by dynamic privilege management.</li> <li>○ organizationally defined actions to access/use device.</li> </ul> </li> <li>■ Ability to allow information sharing capabilities based upon the type and/or role of the user attempting to share the information.</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis.</li> <li>■ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>■ Providing a detailed description of the other types of devices and systems that will access the IoT device during customer use of the device, and how they will access it.</li> <li>■ Providing communications and detailed instructions for implementing a hierarchy of privilege levels to use with the IoT device and/or necessary associated information systems.</li> <li>■ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.</li> <li>■ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources.</li> <li>■ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.</li> <li>■ Providing education explaining how to enforce authorized access at the system level.</li> <li>■ Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that communicate or interface with the device.</li> <li>■ Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device.</li> </ul>	

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
	<ul style="list-style-type: none"> <li>■ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization.</li> <li>■ Ability to establish limits on authorized concurrent device sessions.</li> <li>■ Ability to restrict updating actions to authorized entities.</li> <li>■ Ability to restrict access to the cybersecurity state indicator to authorized entities.</li> <li>■ Ability to revoke access to the IoT device.</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing education and supporting materials for how to establish roles to support IoT device policies, procedures, and associated documentation.</li> </ul>	
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	<ul style="list-style-type: none"> <li>■ Ability for the IoT device to require authentication prior to connecting to the device.</li> <li>■ Ability for the IoT device to support a second, or more, authentication method(s) such as: <ul style="list-style-type: none"> <li>○ temporary passwords or other one-use log-on credentials</li> <li>○ third-party credential checks</li> <li>○ biometrics</li> <li>○ hard tokens</li> </ul> </li> <li>■ Ability to authenticate external users and systems.</li> <li>■ Ability to verify and authenticate any update before installing it.</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.</li> <li>■ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.</li> <li>■ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.</li> </ul>	AC-7 AC-8 AC-9 AC-12 AC-14 IA-2 IA-3 IA-4 IA-5 IA-8 IA-11
PR.DS-1: Data-at-rest is protected.	<ul style="list-style-type: none"> <li>■ Ability to execute cryptographic mechanisms of appropriate strength and performance.</li> <li>■ Ability to obtain and validate certificates.</li> <li>■ Ability to perform authenticated encryption algorithms.</li> <li>■ Ability to change keys securely.</li> <li>■ Ability to generate key pairs.</li> <li>■ Ability to store encryption keys securely.</li> <li>■ Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.</li> <li>■ Ability to support data encryption and signing to prevent data from being altered in device storage.</li> <li>■ Ability to secure data stored locally on the device.</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device.</li> <li>■ Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.</li> </ul>	SC-28 MP-2 MP-4 MP-5

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
	<ul style="list-style-type: none"> <li>■ Ability to secure data stored in remote storage areas (e.g., cloud, server).</li> <li>■ Ability to utilize separate storage partitions for system and user data.</li> <li>■ Ability to protect the audit information through mechanisms such as:           <ul style="list-style-type: none"> <li>○ encryption</li> <li>○ digitally signing audit files</li> <li>○ securely sending audit files to another device</li> <li>○ other protections created by the device manufacturer</li> </ul> </li> </ul>		
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	<ul style="list-style-type: none"> <li>■ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>■ Ability to verify digital signatures.</li> <li>■ Ability to run hashing algorithms.</li> <li>■ Ability to perform authenticated encryption algorithms.</li> <li>■ Ability to compute and compare hashes.</li> <li>■ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>■ Ability to validate the integrity of data transmitted.</li> <li>■ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>■ Ability to verify and authenticate any update before installing it.</li> <li>■ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>■ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>■ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>■ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>■ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>	SC-16 SI-7 MP-4 MP-5
PR.IP-4: Backups of information are conducted, maintained, and tested.	N/A	■ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary.	CP-4 CP-9

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
		<ul style="list-style-type: none"> <li>■ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.</li> <li>■ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.</li> </ul>	
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	N/A	<ul style="list-style-type: none"> <li>■ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home.</li> <li>■ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>■ Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used.</li> <li>■ Providing the details necessary for IoT device customers to implement only organizationally approved IoT device diagnostic tools within their system.</li> <li>■ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>■ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>■ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>■ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. If such comprehensive IoT device maintenance operations documentation does not exist, the manufacturer should</li> </ul>	MA-2 MA-3 MA-5 MA-6

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
		<p>clearly communicate to IoT device customers that the user must perform these operations themselves.</p> <ul style="list-style-type: none"> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> <li>▪ Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel.</li> <li>▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.</li> <li>▪ Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing the details necessary for customers to document attempts to obtain IoT device components or IoT device information system service documentation when such documentation is either unavailable or nonexistent, and documenting the appropriate response for manufacturer employees, or supporting entities, to follow.</li> <li>▪ Providing a process for IoT device customers to contact the manufacturer to ask questions or obtain help related to the IoT device configuration settings.</li> </ul>	

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
		<ul style="list-style-type: none"> <li>▪ Providing information to allow for in-house support from within the IoT device customer organization.</li> <li>▪ Providing education explaining how to inspect IoT device and/or use maintenance tools to ensure the latest software updates and patches are installed.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing education that explains the legal requirements governing IoT device maintenance responsibilities or how to meet specific types of legal requirements when using the IoT device.</li> </ul>	
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	N/A	<ul style="list-style-type: none"> <li>▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> </ul>	MA-4

<b>Cybersecurity Framework v1.1 Subcategory</b>	<b>Device Cybersecurity Capabilities</b>	<b>Manufacturer Nontechnical Supporting Capabilities</b>	<b>NIST SP 800-53 Rev. 5</b>
		<ul style="list-style-type: none"> <li>▪ Providing the details necessary for maintaining records for nonlocal IoT device maintenance and diagnostic activities.</li> <li>▪ Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel.</li> <li>▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.</li> <li>▪ Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> </ul>	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	N/A	<ul style="list-style-type: none"> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> </ul>	AC-4 CA-3 CM-2 SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	N/A	<ul style="list-style-type: none"> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>	AU-6 CA-7 IR-4 SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	<ul style="list-style-type: none"> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> </ul>	AU-6 AU-12 CA-7 IR-4 IR-5

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	<ul style="list-style-type: none"> <li>■ Ability to keep an accurate internal system time.</li> </ul>		SI-4
DE.CM-1: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	<ul style="list-style-type: none"> <li>■ Ability to monitor specific actions based on the IoT device identity.</li> <li>■ Ability to access information about the IoT device's cybersecurity state and other necessary data.</li> <li>■ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.</li> <li>■ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check).</li> <li>■ Ability to monitor communications traffic.</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information.</li> <li>■ Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools.</li> <li>■ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>■ Providing documentation describing how to perform monitoring activities.</li> </ul>	AU-12 CA-7 CM-3 SC-7 SI-4
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	N/A	N/A	AC-2 AU-12 CA-7 CM-3 SC-5 SC-7 SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	<ul style="list-style-type: none"> <li>■ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check).</li> <li>■ Ability to monitor changes to the configuration settings.</li> <li>■ Ability to detect remote activation attempts.</li> <li>■ Ability to detect remote activation of sensors.</li> <li>■ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>■ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>■ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>■ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>■ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>	AC-2 AU-12 AU-13 CA-7 CM-10 CM-11

## E.2 Device Capabilities Supporting Functional Test Scenarios

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

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

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

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

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

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<b>Scenario 1: Protect Host from Malware via USB:</b> This test will demonstrate blocking the introduction of malware through physical access to a workstation within the manufacturing system. <b>PR.DS-6</b> <b>PR.MA-2</b> <b>DE.AE-2</b>	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>(e.g., digital signatures, checksums, certificate validation).</li> <li>Ability to verify and authenticate any update before installing it.</li> <li>Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul style="list-style-type: none"> <li>Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> <li>Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
<b>Scenario 2: Protect Host from Malware via Network Vector:</b> This test will demonstrate the detection of malware introduction from the network. <b>PR.DS-6</b> <b>PR.MA-1</b> <b>DE.AE-1</b> <b>DE.AE-2</b> <b>DE.AE-3</b> <b>DE.CM-1</b> <b>DE.CM-3</b> <b>DE.CM-7</b>	<ul style="list-style-type: none"> <li>Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>Ability to verify digital signatures.</li> <li>Ability to run hashing algorithms.</li> <li>Ability to perform authenticated encryption algorithms.</li> <li>Ability to compute and compare hashes.</li> <li>Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>Ability to validate the integrity of data transmitted.</li> <li>Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>Ability to verify and authenticate any update before installing it.</li> </ul>	<ul style="list-style-type: none"> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>▪ Ability to keep an accurate internal system time.</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
<b>Scenario 3: Protect Host from Malware via Remote Access Connections:</b> This test will demonstrate blocking malware attempting to infect	<ul style="list-style-type: none"> <li>▪ Ability to uniquely identify the IoT device logically.</li> <li>▪ Ability to uniquely identify a remote IoT device.</li> <li>▪ Ability for the device to support a unique device ID.</li> <li>▪ Ability to configure IoT device access control policies using IoT device identity.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.</li> <li>▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.</li> <li>▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<p>manufacturing system through authorized remote access connections.</p> <p><b>PR.AC-1</b></p> <p><b>PR.AC-3</b></p> <p><b>PR.AC-4</b></p> <p><b>PR.AC-7</b></p> <p><b>PR.MA-1</b></p> <p><b>PR.MA-2</b></p> <p><b>DE.CM-3</b></p> <p><b>DE.CM-7</b></p>	<ul style="list-style-type: none"> <li>▪ Ability to verify the identity of an IoT device.</li> <li>▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.</li> <li>▪ Ability to set and change authentication configurations, policies, and limitations settings for the IoT device.</li> <li>▪ Ability to revoke access to the device.</li> <li>▪ Ability to create unique IoT device user accounts.</li> <li>▪ Ability to identify unique IoT device user accounts.</li> <li>▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions.</li> <li>▪ Ability to configure IoT device access control policies using IoT device identity.</li> <li>▪ Ability to authenticate external users and systems.</li> <li>▪ Ability to securely interact with authorized external, third-party systems.</li> <li>▪ Ability to identify when an external system meets the required security requirements for a connection.</li> <li>▪ Ability to establish secure communications with internal systems when the device is operating on external networks.</li> <li>▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface.</li> <li>▪ Ability to enforce the established local and remote access requirements.</li> <li>▪ Ability to prevent external access to the IoT device management interface.</li> <li>▪ Ability to assign roles to IoT device user accounts.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.</li> <li>▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces, such as for specific support, updates, ongoing maintenance, and other purposes.</li> <li>▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.</li> <li>▪ Providing education explaining how to enforce authorized access at the system level.</li> <li>▪ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.</li> <li>▪ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.</li> <li>▪ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles.</li> <li>▪ Ability to apply least privilege to user accounts.</li> <li>▪ Ability to enable automation and reporting of account management activities.</li> <li>▪ Ability for the IoT device to require authentication prior to connecting to the device.</li> <li>▪ Ability for the IoT device to support a second, or more, authentication method(s).</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	
<b>Scenario 4: Protect Host from Unauthorized Application Installation:</b> This test will demonstrate blocking the installation and execution of unauthorized	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<p>applications on workstation in the manufacturing system.</p> <p><b>PR.DS-6</b></p> <p><b>PR.MA-1</b></p> <p><b>DE.AE-1</b></p> <p><b>DE.AE-2</b></p> <p><b>DE.AE-3</b></p> <p><b>DE.CM-1</b></p> <p><b>DE.CM-3</b></p> <p><b>DE.CM-7</b></p>	<ul style="list-style-type: none"> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>▪ Ability to keep an accurate internal system time.</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<p>controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</p> <ul style="list-style-type: none"> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<b>Scenario 5: Protect from Unauthorized Addition of a Device:</b> This test will demonstrate the detection of an unauthorized device connecting to the manufacturing system. <b>PR.DS-6</b> <b>PR.MA-1</b> <b>DE.AE-1</b> <b>DE.AE-2</b> <b>DE.AE-3</b> <b>DE.CM-1</b> <b>DE.CM-3</b> <b>DE.CM-7</b>	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>▪ Ability to keep an accurate internal system time.</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
<b>Scenario 6: Detect Unauthorized Device-to-Device Communications:</b> This test will demonstrate the detection of unauthorized communications between devices. <b>PR.DS-6</b> <b>PR.MA-1</b> <b>DE.AE-1</b> <b>DE.AE-2</b> <b>DE.AE-3</b> <b>DE.CM-1</b> <b>DE.CM-3</b> <b>DE.CM-7</b>	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>(e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>Ability to keep an accurate internal system time.</li> <li>Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>Ability to monitor changes to the configuration settings.</li> <li>Ability to detect remote activation attempts.</li> <li>Ability to detect remote activation of sensors.</li> <li>Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>Providing education for how to scan for critical software updates and patches.</li> <li>Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>Providing the details necessary to monitor IoT devices and associated systems.</li> <li>Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
<b>Scenario 7: Protect from Unauthorized Modification and Deletion of Files:</b> This test will demonstrate protection of files from unauthorized deletion both locally and on network file share. <b>PR.DS-1</b> <b>PR.DS-6</b> <b>PR.IP-4</b> <b>PR.MA-1</b>	<ul style="list-style-type: none"> <li>Ability to execute cryptographic mechanisms of appropriate strength and performance.</li> <li>Ability to obtain and validate certificates.</li> <li>Ability to change keys securely.</li> <li>Ability to generate key pairs.</li> <li>Ability to store encryption keys securely.</li> <li>Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.</li> <li>Ability to support data encryption and signing to prevent data from being altered in device storage.</li> <li>Ability to secure data stored locally on the device.</li> </ul>	<ul style="list-style-type: none"> <li>Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device.</li> <li>Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.</li> <li>Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
DE.AE-2	<ul style="list-style-type: none"> <li>▪ Ability to secure data stored in remote storage areas (e.g., cloud, server).</li> <li>▪ Ability to utilize separate storage partitions for system and user data.</li> <li>▪ Ability to protect the audit information through mechanisms such as:           <ul style="list-style-type: none"> <li>○ encryption</li> <li>○ digitally signing audit files</li> <li>○ securely sending audit files to another device</li> <li>○ other protections created by the device manufacturer</li> </ul> </li> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary.</li> <li>▪ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.</li> <li>▪ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<b>Scenario 8: Detect Unauthorized Modification of PLC Logic:</b> This test will demonstrate the detection of PLC logic modification. <b>PR.AC-3</b> <b>PR.AC-7</b> <b>PR.DS-6</b> <b>PR.MA-1</b> <b>PR.MA-2</b> <b>DE.AE-1</b> <b>DE.AE-2</b> <b>DE.AE-3</b> <b>DE.CM-1</b> <b>DE.CM-3</b> <b>DE.CM-7</b>	<ul style="list-style-type: none"> <li>▪ Ability to configure IoT device access control policies using IoT device identity.</li> <li>▪ Ability to authenticate external users and systems.</li> <li>▪ Ability to securely interact with authorized external, third-party systems.</li> <li>▪ Ability to identify when an external system meets the required security requirements for a connection.</li> <li>▪ Ability to establish secure communications with internal systems when the device is operating on external networks.</li> <li>▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface.</li> <li>▪ Ability to enforce the established local and remote access requirements.</li> <li>▪ Ability to prevent external access to the IoT device management interface.</li> <li>▪ Ability for the IoT device to require authentication prior to connecting to the device.</li> <li>▪ Ability for the IoT device to support a second, or more, authentication method(s).</li> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication.</li> <li>▪ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques.</li> <li>▪ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.</li> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>▪ Ability to keep an accurate internal system time.</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities.</li> <li>▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.</li> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
<b>Scenario 9: Protect from Modification of Historian Data:</b>	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<p>This test will demonstrate the blocking of modification of historian archive data.</p> <p><b>PR.DS-6</b> <b>PR.MA-1</b> <b>DE.AE-2</b></p>	<ul style="list-style-type: none"> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> </ul>
<p><b>Scenario 10: Detect Sensor Data Manipulation:</b> This test will demonstrate</p>	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary.</li> <li>▪ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
<p>detection of atypical data reported to the historian.</p> <p><b>PR.IP-4</b></p> <p><b>PR.DS-6</b></p> <p><b>PR.MA-1</b></p> <p><b>DE.AE-1</b></p> <p><b>DE.AE-2</b></p> <p><b>DE.AE-3</b></p> <p><b>DE.CM-1</b></p> <p><b>DE.CM-3</b></p> <p><b>DE.CM-7</b></p>	<ul style="list-style-type: none"> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>▪ Ability to keep an accurate internal system time.</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.</li> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>
<p><b>Scenario 11: Detect Unauthorized Firmware Modification:</b> This test will demonstrate the detection of device firmware modification</p> <p><b>PR.DS-6</b> <b>PR.MA-1</b> <b>DE.AE-1</b> <b>DE.AE-2</b> <b>DE.AE-3</b> <b>DE.CM-1</b> <b>DE.CM-3</b> <b>DE.CM-7</b></p>	<ul style="list-style-type: none"> <li>▪ Ability to identify software loaded on the IoT device based on IoT device identity.</li> <li>▪ Ability to verify digital signatures.</li> <li>▪ Ability to run hashing algorithms.</li> <li>▪ Ability to perform authenticated encryption algorithms.</li> <li>▪ Ability to compute and compare hashes.</li> <li>▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.</li> <li>▪ Ability to validate the integrity of data transmitted.</li> <li>▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).</li> <li>▪ Ability to verify and authenticate any update before installing it.</li> <li>▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.</li> <li>▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.</li> <li>▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls.</li> <li>▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.</li> <li>▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.</li> <li>▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.</li> <li>▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.</li> <li>▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.</li> </ul>

Scenario ID and Description with CSF Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	<ul style="list-style-type: none"> <li>▪ Ability to provide a physical indicator of sensor use.</li> <li>▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).</li> <li>▪ Ability to keep an accurate internal system time.</li> <li>▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.</li> <li>▪ Ability to monitor changes to the configuration settings.</li> <li>▪ Ability to detect remote activation attempts.</li> <li>▪ Ability to detect remote activation of sensors.</li> <li>▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.</li> <li>▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform.</li> <li>▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer.</li> <li>▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.</li> <li>▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.</li> <li>▪ Providing education for how to scan for critical software updates and patches.</li> <li>▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.</li> <li>▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.</li> <li>▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.</li> <li>▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.</li> <li>▪ Providing the details necessary to monitor IoT devices and associated systems.</li> <li>▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.</li> <li>▪ Providing documentation that describes indicators of unauthorized use of the IoT device.</li> </ul>

## 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 <https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics>



## 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: [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov).

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: [nccoe@nist.gov](mailto:nccoe@nist.gov)

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

## 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, <https://www.ibm.com/security/data-breach/threat-intelligence>). 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  
77 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
Ian Schmertzler	Dispel
Ben Burke	Dispel
Chris Jensen	Tenable
Bethany Brower	VMWare
Dennis Hui	OSIsoft (now part of AVEVA)
John Matranga	OSIsoft (now part of AVEVA)
Michael A. Piccalo	Forescout
Tim Jones	Forescout
Yejin Jang	Forescout
Samantha Pelletier	TDI Technologies
Rusty Hale	TDI Technologies
Steve Petruzzo	GreenTec-USA
Josh Carlson	Dragos
Alex Baretta	Dragos

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

102 a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not  
103 currently intend holding any essential patent claim(s); or

104 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring  
105 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft  
106 publication either:

107 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;  
108 or

109 2. without compensation and under reasonable terms and conditions that are demonstrably free  
110 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,  
114 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: [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov)

## 119 **Contents**

120	<b>1 Introduction .....</b>	<b>1</b>
121	1.1 How to Use this Guide.....	1
122	1.1 Build Overview .....	2
123	1.2 Typographic Conventions.....	2
124	1.3 Logical Architecture Summary .....	3
125	<b>2 Product Installation Guides .....</b>	<b>5</b>
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.....	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 Forescout 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 GreenTec-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 Microsoft 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 OSIsoft 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 Security 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 ConsoleWorks .....	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 Tenable.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 VMware Carbon Black App Control.....	105
163	2.10.1 Host and Network Configuration.....	105
164	2.10.2 Installation .....	106
165	2.10.3 Configuration .....	107
166	2.11 Windows Software Restriction Policy .....	114
167	2.11.1 Host and Network Configuration.....	114
168	2.11.2 Installation .....	115
169	2.11.3 Configuration .....	115
170	<b>Appendix A List of Acronyms .....</b>	<b>123</b>
171	<b>Appendix B Build Architectures Diagrams .....</b>	<b>125</b>

## 172 List of Figures

173	<b>Figure 1-1: CSMS Network Architecture .....</b>	4
174	<b>Figure 2-1 Dispel High-level Implementation, from Remote Access for ICS .....</b>	6
175	<b>Figure 2-2 Mapping a Network Drive .....</b>	11
176	<b>Figure 2-3 Authentication to File Server .....</b>	12
177	<b>Figure 2-4 Dragos OSIsoft PI Server Integration .....</b>	13
178	<b>Figure 2-5 Dragos PI Web API Configuration.....</b>	14
179	<b>Figure 2-6 OSIsoft PI Server to Dragos Asset and Data Pairing.....</b>	15
180	<b>Figure 2-7 OSIsoft PI Server and Dragos Paired Data Elements.....</b>	15
181	<b>Figure 2-8 Dragos Zone Administration Page.....</b>	16
182	<b>Figure 2-9 Dragos Create Zone Pop-up .....</b>	17
183	<b>Figure 2-10 Forescout High-Level Components and Dataflows .....</b>	18
184	<b>Figure 2-11 Forescout SecureConnector Distribution Tool .....</b>	21
185	<b>Figure 2-12 Forescout Agent Download .....</b>	21
186	<b>Figure 2-13 eyeInspect Sensor Admin/Overview Page – Add Sensor .....</b>	22
187	<b>Figure 2-14 Adding a New SilentDefense Sensor Dialog .....</b>	23
188	<b>Figure 2-15 eyeInspect ICMP Protocol/Port Scan Attempt Settings .....</b>	24
189	<b>Figure 2-16 eyeInspect Sensor Configuration Options.....</b>	24
190	<b>Figure 2-17 eyeInspect Portscan Detection Settings .....</b>	25
191	<b>Figure 2-18 Add ICS Patrol Sensor Dialog .....</b>	26
192	<b>Figure 2-19 ICS Patrol Sensor Admin Page.....</b>	27
193	<b>Figure 2-20 Add an ICS Patrol Scan Policy.....</b>	28
194	<b>Figure 2-21 eyeSight Add Dialog – General Information.....</b>	29
195	<b>Figure 2-22 eyeSight Add – Command Center Credentials.....</b>	30
196	<b>Figure 2-23 eyeSight OT Settings.....</b>	31
197	<b>Figure 2-24 eyeSight Test Connection Successful Message.....</b>	31
198	<b>Figure 2-25 Azure Defender for IoT SSH Session for Network Configuration .....</b>	37
199	<b>Figure 2-26 Azure Defender for IoT Create New Data Mining Report for AMS Protocol Information ...</b>	38
200	<b>Figure 2-27 Azure Defender for IoT Custom Alert for Firmware Major Version Number Change.....</b>	39
201	<b>Figure 2-28 Azure Defender for IoT Custom Alert for Firmware Minor Version Number Change.....</b>	40
202	<b>Figure 2-29 Azure Defender for IoT Custom Alert for Firmware Build Version Number Change .....</b>	40

203	<b>Figure 2-30 Screenshot of the PI Interface Configuration Utility before the Interface is configured.....</b>	44
204	<b>Figure 2-31 Screenshot of the PI Data Collection Manager Displaying Green Checkmarks After the PI System Connector is Properly Configured .....</b>	45
206	<b>Figure 2-32 Screenshot of the PI Interface Configuration Utility Showing the Added Scan Class # 2 for Polling the PLC Every 60 Seconds .....</b>	54
208	<b>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.....</b>	56
210	<b>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. ....</b>	59
212	<b>Figure 2-35 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Event Frame Template.....</b>	60
214	<b>Figure 2-36 Screenshot of PI System Explorer Displaying the TwinCAT Version Mismatch Event Frame Template .....</b>	61
216	<b>Figure 2-37 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Analysis Template in the PLC Element Template .....</b>	62
218	<b>Figure 2-38 Screenshot of PI System Explorer Displaying the TwinCAT Firmware Version Mismatch Analysis Template in the PLC Element Template .....</b>	63
220	<b>Figure 2-39 Wazuh Agent Manager.....</b>	66
221	<b>Figure 2-40 ossec.conf File.....</b>	66
222	<b>Figure 2-41 Wazuh Agent Manager User Interface .....</b>	67
223	<b>Figure 2-42 Log Received After a File Change Was Detected .....</b>	67
224	<b>Figure 2-43 ConsoleWorks Registration Screen .....</b>	73
225	<b>Figure 2-44 ConsoleWorks Offline Registration Process .....</b>	73
226	<b>Figure 2-45 ConsoleWorks System Backups.....</b>	74
227	<b>Figure 2-46 ConsoleWorks Importing System Configurations and Components .....</b>	75
228	<b>Figure 2-47 ConsoleWorks Password Settings .....</b>	76
229	<b>Figure 2-48 ConsoleWorks Add the Local Graphical Gateway for RDP Access .....</b>	77
230	<b>Figure 2-49 ConsoleWorks Example Device Type Definition.....</b>	79
231	<b>Figure 2-50 ConsoleWorks List of Device Types .....</b>	79
232	<b>Figure 2-51 ConsoleWorks Example Device Definition .....</b>	80
233	<b>Figure 2-52 ConsoleWorks List of PCS (Build 1) Devices .....</b>	81
234	<b>Figure 2-53 ConsoleWorks List of CRS (Build 3) Devices .....</b>	82
235	<b>Figure 2-54 ConsoleWorks Example RDP Configuration .....</b>	83
236	<b>Figure 2-55 ConsoleWorks List of PCS (Build 1) RDP Connections .....</b>	85

237	<b>Figure 2-56 ConsoleWorks List of CRS (Build 3) RDP Connections .....</b>	86
238	<b>Figure 2-57 ConsoleWorks Example Console (SSH) Connection .....</b>	87
239	<b>Figure 2-58 ConsoleWorks Example Console (Web Forward) Connection .....</b>	88
240	<b>Figure 2-59 ConsoleWorks List of PCS (Build 1) Console Connections .....</b>	89
241	<b>Figure 2-60 ConsoleWorks List of CRS (Build 3) Console Connections .....</b>	90
242	<b>Figure 2-61 ConsoleWorks List of Tags for PCS (Build 1).....</b>	91
243	<b>Figure 2-62 ConsoleWorks Example Tag Definition Screen.....</b>	92
244	<b>Figure 2-63 ConsoleWorks Example Profile .....</b>	95
245	<b>Figure 2-64 Tenable.OT Local Device Setting for NTP Service .....</b>	98
246	<b>Figure 2-65 Tenable.OT Asset Discovery Settings.....</b>	99
247	<b>Figure 2-66 Tenable.OT Controller Scans.....</b>	100
248	<b>Figure 2-67 Tenable.OT Network Scan Settings .....</b>	101
249	<b>Figure 2-68 Tenable.OT Create Asset Group Type.....</b>	101
250	<b>Figure 2-69 Tenable.OT Create Asset Group Definition .....</b>	102
251	<b>Figure 2-70 Tenable.OT Policy Settings .....</b>	103
252	<b>Figure 2-71 Tenable.OT Create Policy – Event Type Options .....</b>	103
253	<b>Figure 2-72 Tenable.OT Create Policy - Definition.....</b>	104
254	<b>Figure 2-73 Tenable.OT Create Policy - Actions.....</b>	105
255	<b>Figure 2-74 Excerpt from Carbon Black Documentation on Support Server Requirements .....</b>	108
256	<b>Figure 2-75 IIS Configuration for Carbon Black, Server Roles.....</b>	109
257	<b>Figure 2-76 Carbon Black Policy Edit .....</b>	110
258	<b>Figure 2-77 Carbon Black App Control System Configuration .....</b>	111
259	<b>Figure 2-78 Carbon Black App Control AD Policy Mappings.....</b>	112
260	<b>Figure 2-79 Carbon Black Agent Download.....</b>	113
261	<b>Figure 2-80 Carbon Black App Control Computers .....</b>	113
262	<b>Figure 2-81 Carbon Black App Control File Catalog .....</b>	114
263	<b>Figure 2-82 Setting Enforcement Properties .....</b>	117
264	<b>Figure 2-83 Setting Security Level Default .....</b>	118
265	<b>Figure 2-84 Additional Rules Defined for Lab Environment .....</b>	119
266	<b>Figure 2-85 Menu Options for Accessing the Link an Existing GPO Option .....</b>	120
267	<b>Figure 2-86 Dialog Box for Selecting GPO to Link .....</b>	121

268	<a href="#">Figure B - 1 Build 1 Architecture Diagram</a>	125
269	<a href="#">Figure B - 2 Build 2 Architecture Diagram</a>	126
270	<a href="#">Figure B - 3 Build 3 Architecture Diagram</a>	127
271	<a href="#">Figure B - 4 Build 4 Architecture Diagram</a>	128

## 272 **List of Tables**

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

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

## 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.*

### 1.1 How to Use this Guide

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

This guide contains three volumes:

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

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

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

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

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

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

- Section 3.4.1, 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

341 of the build created in our lab. This How-To portion of the guide provides specific product  
 342 installation, configuration, and integration instructions for implementing the example solution.  
 343 We do not recreate the product manufacturers' documentation, which is generally widely  
 344 available. Rather, we show how we incorporated the products together in our environment to  
 345 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  
 354 by this reference solution.

355 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a  
 356 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 [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov).

## 359 1.1 Build Overview

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

## 367 1.2 Typographic Conventions

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

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

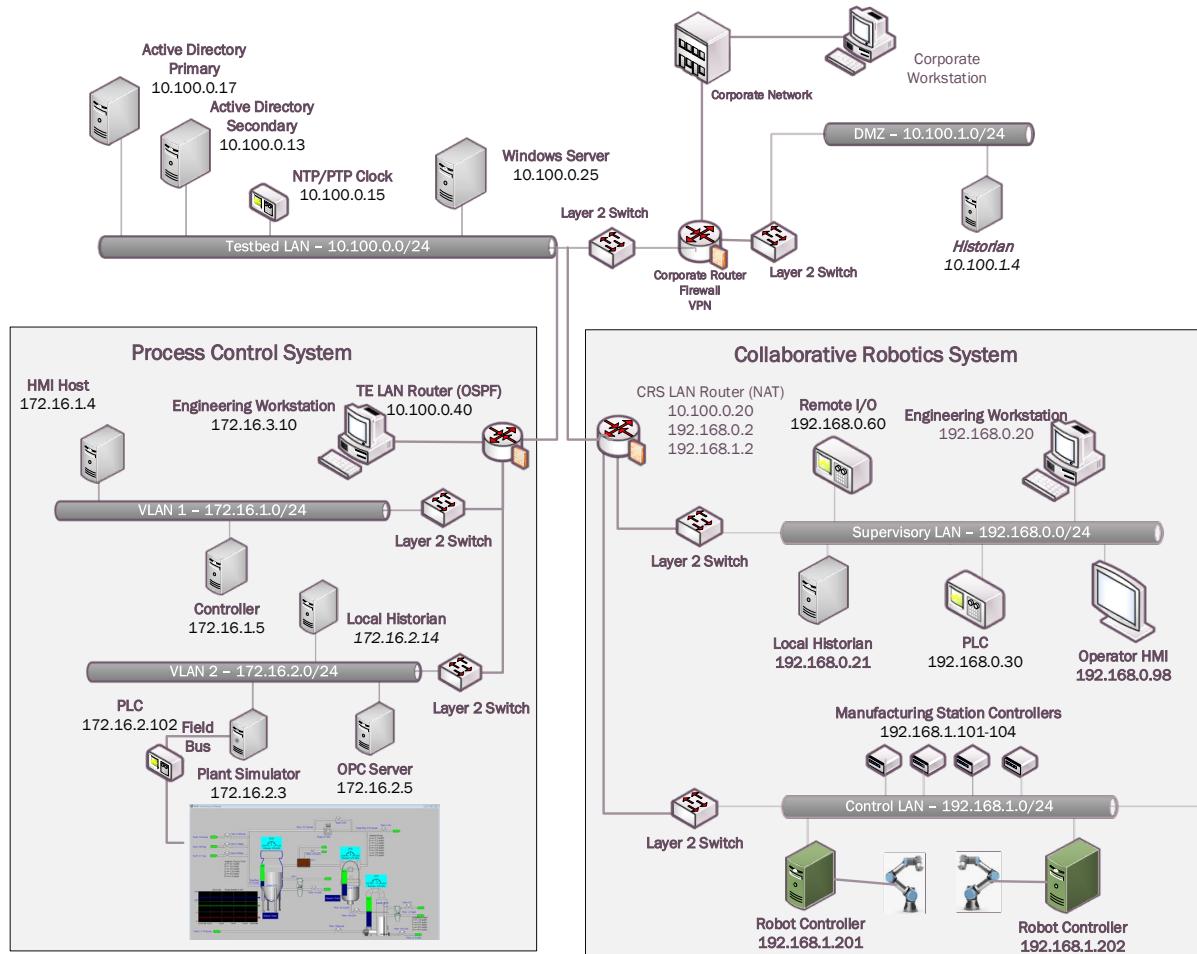
Typeface/Symbol	Meaning	Example
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<code>service sshd start</code>
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov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

### 1.3 Logical Architecture Summary

The security mechanisms and technologies were integrated into the existing NIST Cybersecurity for Smart Manufacturing Systems (CSMS) lab environment. This cybersecurity performance testbed for ICS is comprised of the PCS and the CRS environments along with additional networking capabilities to emulate common manufacturing environments. For more information see An *Industrial Control System Cybersecurity Performance Testbed*, NISTIR 8089, <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf>.

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

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

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 server, are also located on this LAN. The Testbed LAN has three gateways to other network segments, including 10.100.0.1 to reach the DMZ and the corporate network, 10.100.0.20 as a network address translation (NAT) interface to the CRS environment, and 10.100.0.40 as the gateway to the PCS environment.

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

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

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

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

414 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  
418 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**

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

### 423 **2.1 Dispel Remote Access**

424 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)  
426 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.

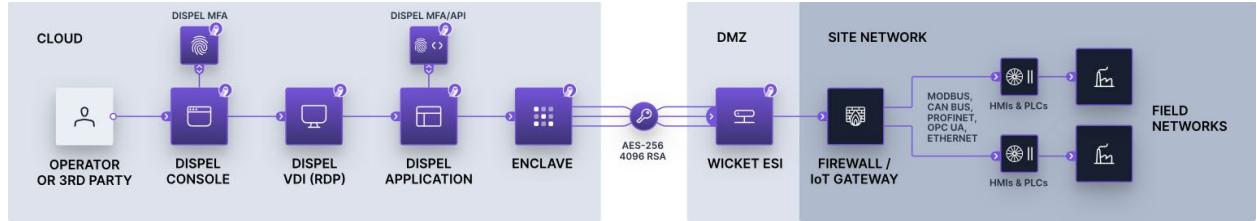
#### 433 **Enclave**

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 [https://s3.amazonaws.com/downloads.dispel.io/resources/One+Pager/dispel-ics-brochure\\_20190529.pdf](https://s3.amazonaws.com/downloads.dispel.io/resources/One+Pager/dispel-ics-brochure_20190529.pdf)  
 446

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  
 451 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](#).

453 **Table 2-1 Dispel Deployment**

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

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  
 461 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 the  
 466 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**

470     4. Check the log for errors and test connectivity to the Dispel environment (note: IP address will be  
471       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  
475       an account and configuring the cloud infrastructure, configuring the corporate router/firewall to allow  
476       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”  
484       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  
488       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 Dispel Environment on the Internet
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 between 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 Environment
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.
- 502     ▪ The rules implemented included restricting these outbound ports to Enclave specific IP  
503       addresses.
- 504     ▪ The Enclave's MTD characteristics were disabled to keep the Enclave's IP addresses static for the  
505       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  
508       VDI instance, authorized users establish a VPN tunnel to the Wicket ESI within the OT  
509       environment and then have the access to the environment configured by the device and firewall  
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.

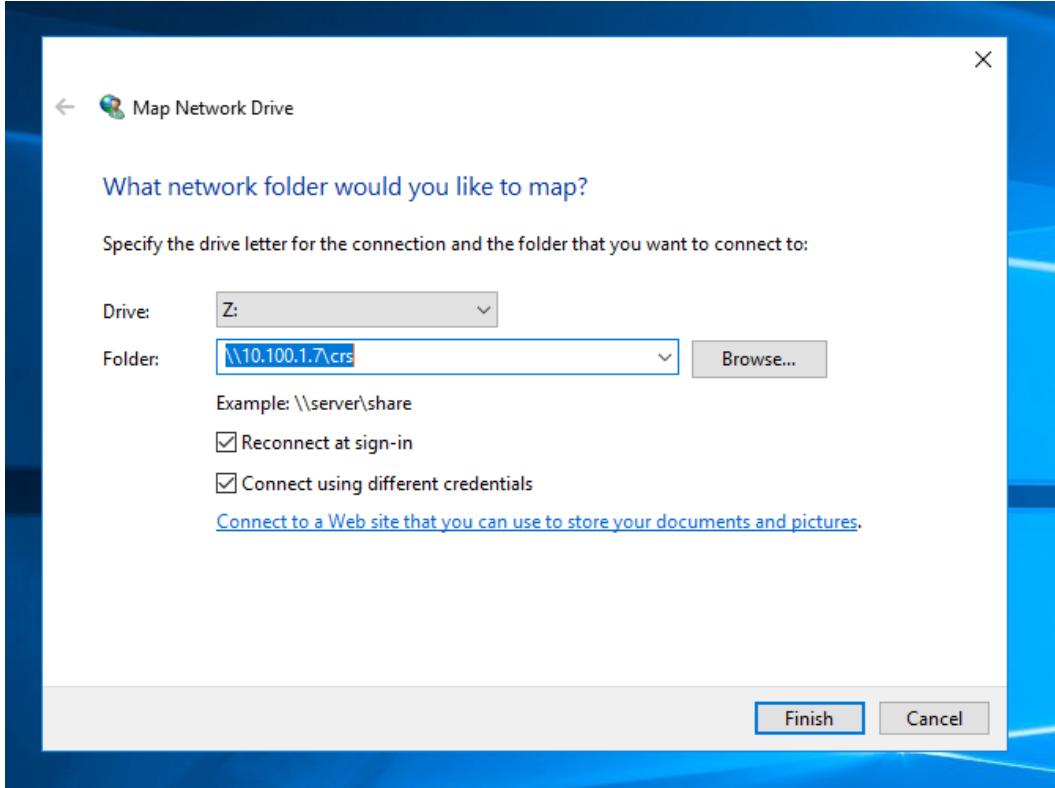
- 515            1. Build 2: PCS Configuration  
 516            i. For the PCS setup, the Dispel VDI was used in a jump server configuration. No  
 517            additional software was installed. The firewall and Wicket ESI configuration  
 518            allowed RDP and SSH connections to the PCS 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: CRS 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            v. 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**

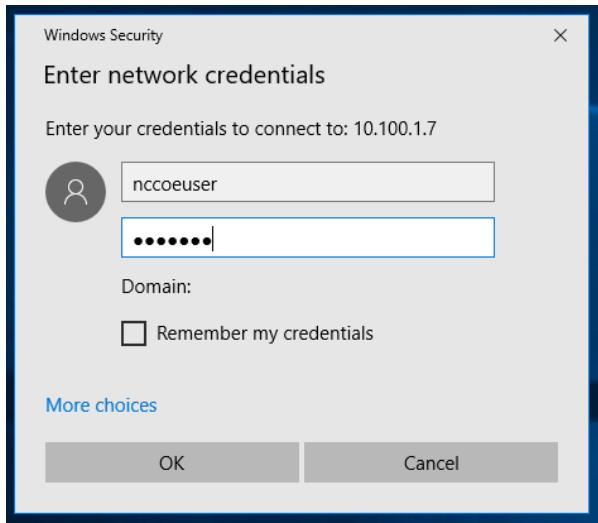
Rule Type	Source	Destination	Destination Port(s)	Purpose
DNAT	10.100.1.61	192.168.0.30	UDP:48899	DNAT (10.100.0.20) - Beckhoff ADS discovery protocol used by the TwinCAT 3 software to discover ADS devices.
DNAT	10.100.1.61	192.168.0.30	TCP:48898	DNAT (10.100.0.20) - Beckhoff ADS protocol used by the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

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

546       **Figure 2-2 Mapping a Network Drive**



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

550 **Figure 2-3 Authentication to File Server**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  
 560 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  
565 installation step was correctly connecting the server and the sensor management ports to the Testbed  
566 LAN and adding the switch port analyzer (SPAN) port connection to the sensor.

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

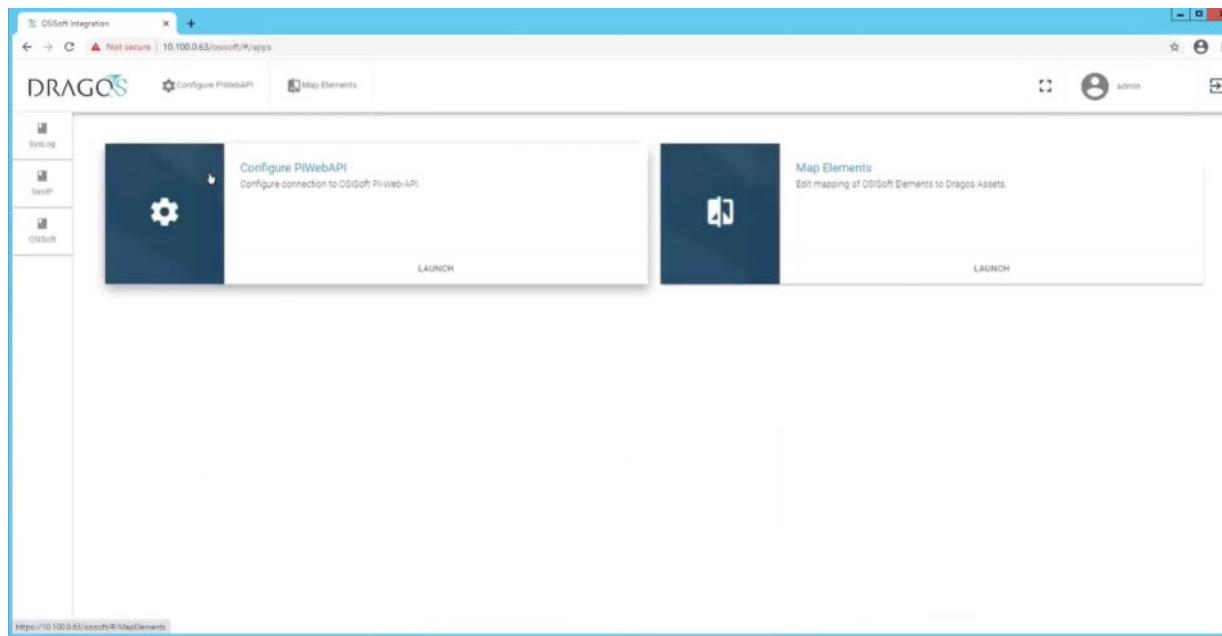
## 569 2.2.3 Configuration

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

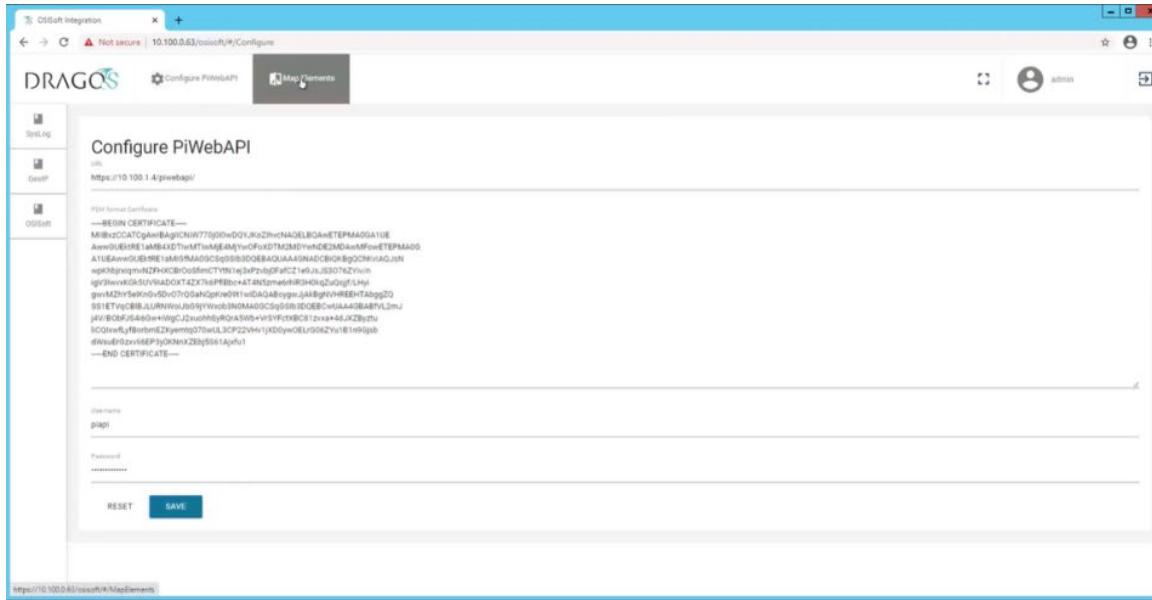
576 **Figure 2-4 Dragos OSIsoft PI Server Integration**



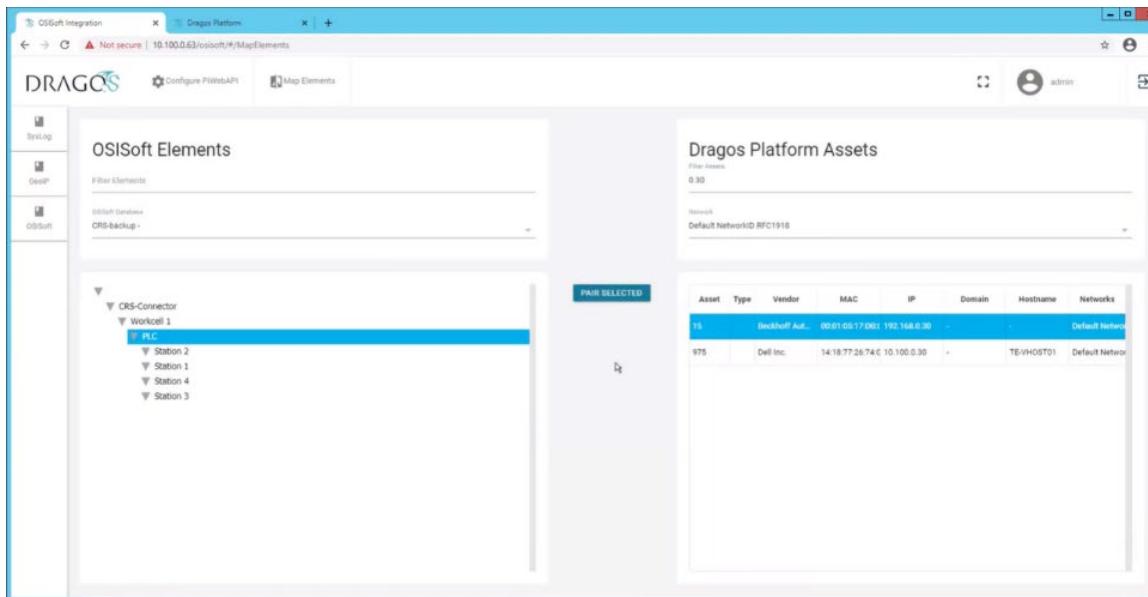
- 577 b. Click **Configuration Pi Web API** to open a screen for filling out the required information,  
578 including privacy enhanced mail (PEM) format certificate and password for secure  
579 authentication (Figure 2-5).
  - 580 i. Upload the server public key for the HTTPS certificate.
  - 581 ii.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

582                             iii. Click **Save**.

583   **Figure 2-5 Dragos PI Web API Configuration**



- 584
- 585                             c. Click **Map Elements** to access the interface to pair elements between OSIsoft PI Server  
586                             and the Dragos Platform assets. Here, the PLC in **OSIsoft Elements** panel is paired with  
587                             Beckhoff asset in the Dragos Platform asset (Figure 2-6).
- 588                             i. Select the OSIsoft Database **CRS-backup** on the left side to access the devices list  
589                             from the Historian Database.
- 590                             ii. Select the **Default NetworkID RFC 1918** and use the Filer options to find specific  
591                             assets.
- 592                             iii. For each asset in the OSIsoft Database, select the corresponding asset in the Dra-  
593                             gos asset repository and click **Pair Selected**.
- 594                             iv. Repeat this process for each asset until all paired assets are listed in the **Paired  
595                             Data** table (Figure 2-7).
- 596                             1) PLC paired to 192.168.0.30
- 597                             2) Station 1 paired to 192.168.1.101
- 598                             3) Station 2 paired to 192.168.1.102
- 599                             4) Station 3 paired to 192.168.1.103
- 600                             5) Station 4 paired to 192.168.1.104

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

602

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

Delete	Asset	OSIsoft Name	Type	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_...top.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_...top.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_...top.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

604

## 605      a. Configure Zones

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

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

609 **Figure 2-8 Dragos Zone Administration Page**

The screenshot shows the Dragos Asset Explorer interface. The left sidebar has a navigation menu with options: Dashboard, Map, Assets (selected), Data, Notifications, Content, Reports, Sensors, Admin, and a bottom section with navigation icons. The main area is titled 'Asset Explorer' and has tabs for 'ASSETS' and 'ZONES'. A search bar 'Search Zones' is at the top. Below it are buttons for 'DETAILED VIEW', 'SLIM VIEW', '+ NEW ZONE', 'REFRESH', 'EDIT PARENT ZONES', and a menu icon. The 'ZONES' tab is selected, showing four entries:

- DMZ**: Description: Lab DMZ. Details: Assets: 14, Baseline Assets: 0, Baseline Events: 0, Protocols: 2, External Communications: false. Asset Criteria: ALL: IPv4 CIDR Matches CIDR 10.100.1.0/24.
- Cybersecurity LAN**: Description: Data Collection and Monitoring. Details: Assets: 75, Baseline Assets: 0, Baseline Events: 0, Protocols: 13, External Communications: false. Asset Criteria: ALL: IPv4 CIDR Matches CIDR 10.100.0.0/24.
- CRS - Level 1**: Description: Robots and Controllers. Details: Assets: 25, Baseline Assets: 0, Baseline Events: 0, Protocols: 23, External Communications: true. Asset Criteria: ALL: IPv4 CIDR Matches CIDR 192.168.0.0/24.
- CRS - Level 0**: Description: Robots and Controllers. Details: Assets: 15, Baseline Assets: 0, Baseline Events: 0, Protocols: 10, External Communications: true. Asset Criteria: ALL: IPv4 CIDR Matches CIDR 192.168.1.0/24.

610 b. Click + New Zone (Figure 2-9) and define the following zones:

611 i. Name: **DMZ**:

612 1) Description: Lab DMZ

613 2) Zone Criteria (Match ALL):

614 a) IPV4 CIDR Matches CIDR 10.100.1.0/24

615 ii. Name: Testbed LAN:

616 1) Description: Lab Testbed LAN

617 2) Auto Zone Criteria (Match ALL):

618 a) IPV4 CIDR Matches CIDR 10.100.0.0/24

619 iii. Name: CRS:

620 1) Description: **Parent CRS**

621 2) No Criteria

622 iv. Name: CRS – Level 0:

623 1) Description: Robots and Controllers

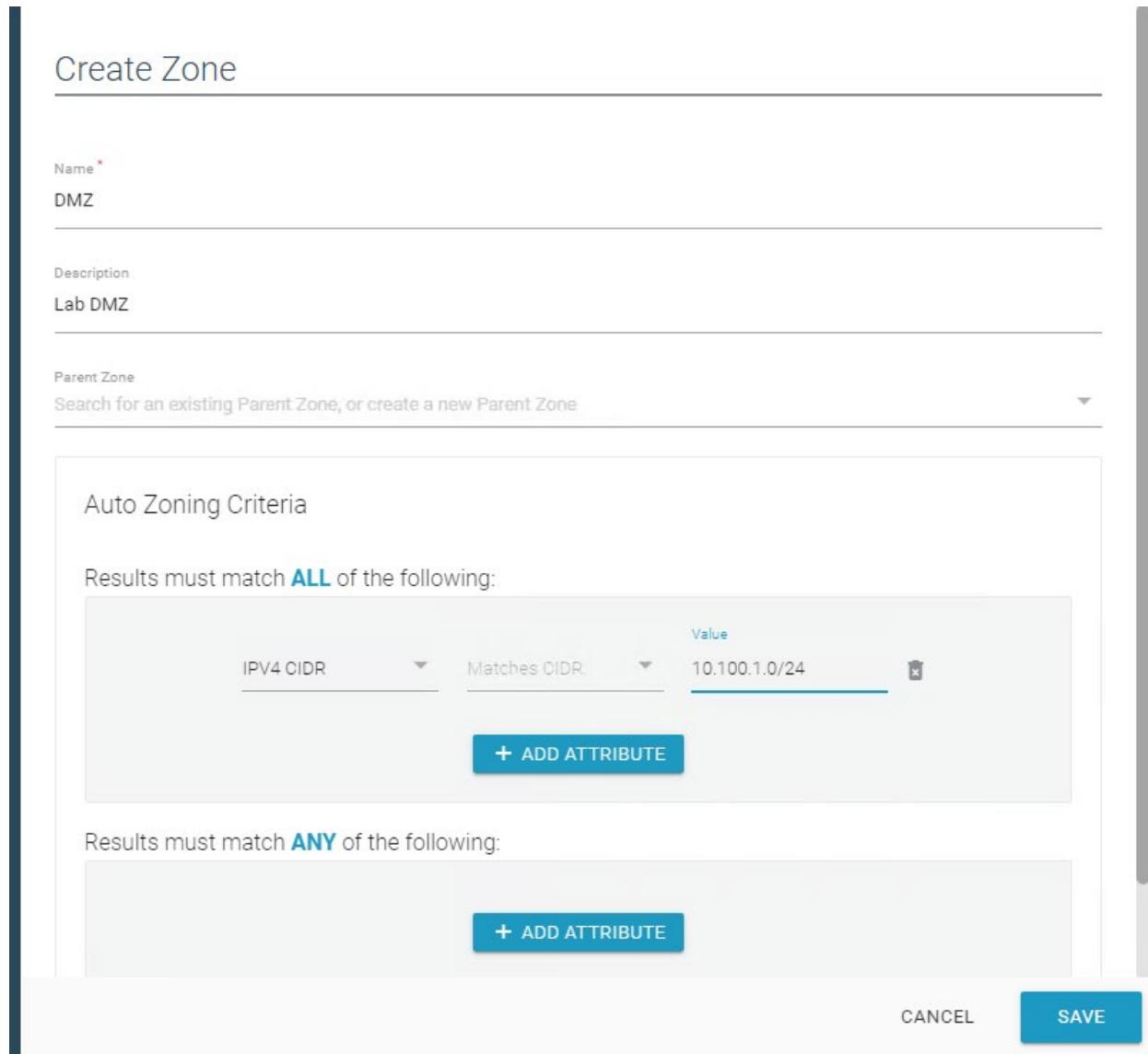
624 2) Parent Zone: **CRS**

625 3) Auto Zone Criteria (Match **ALL**):

626 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**

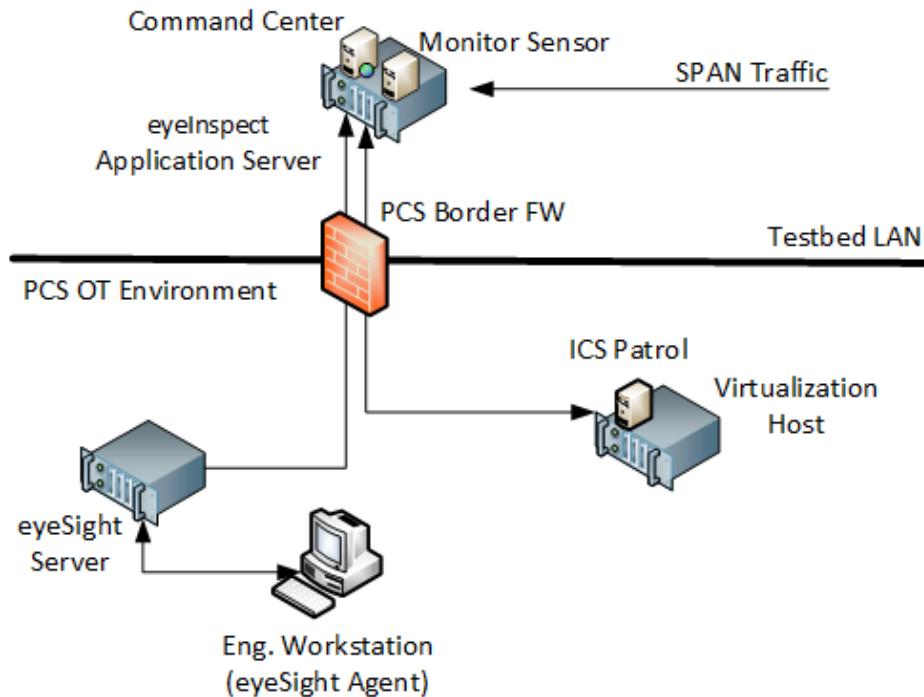


### 633 **2.3 Forescout Platform**

634 The Forescout products included in the practice guide are eyeInspect (formally SilentDefense), eyeSight,  
 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  
 639 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  
 653 obtain status and other information such as hardware configuration and firmware version. ICS Patrol  
 654 queries and reporting results are managed through eyeInspect.

655 **Forescout Console**

656 The Forescout Console (Version 8.2.1) is a Java-based application for configuring and managing eyeSight  
 657 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  
 661 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 Embedded 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 Silver 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

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

671 **2.3.2 Installation**

672 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  
 674 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) 9999 9092	System Management eyeInspect Data eyeInspect Data
Allow	10.100.0.65	172.16.2.62	22 (ssh) 9001	System Management eyeInspect 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  
 680 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 <https://forescout.force.com/support/s/downloads>, where current and past  
 686 versions are available. Login credentials were provided by Forescout.

687 **2.3.2.3 eyeSight**

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

690 **2.3.2.4 eyeSight SecureConnector Agent**

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

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

702 **Figure 2-11 Forescout SecureConnector Distribution Tool**

703 **Figure 2-12 Forescout Agent Download**

704 ***2.3.2.5 ICS Patrol***

- 705        Forescout ICS Patrol (Version 1.1.2-4.a826b94) is a sensor that is deployed on an existing VirtualBox host  
 706        in the PCS environment. Ubuntu 16.04.06 is required for proper installation and can be downloaded  
 707        from <http://old-releases.ubuntu.com/releases/xenial/ubuntu-16.04.6-server-amd64.iso>. Install the  
 708        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.  
 710        1. Install the ICS Patrol Component from the Silent Defense Installation and Configuration Guide  
 711        4.1.2 document Sections 2.2.4 and 2.2.5 following these steps:  
 712            a. Establish an SSH session to the eyeInspect appliance.

713           b. Copy the components to the ICS Patrol VM:

714           \$ scp os\_provisioning\_4.1.1\_install.run \  
715           main\_configuration\_4.1.1\_install.run \  
716           silentdefense@172.16.2.62:/home/silentdefense

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

718           \$ chmod a+x \*.run  
719           \$ sudo ./os provisioning 4.1.1 install.run  
720           \$ sudo ./main\_configuration\_4.1.1\_install.run  
721           \$ sudo reboot

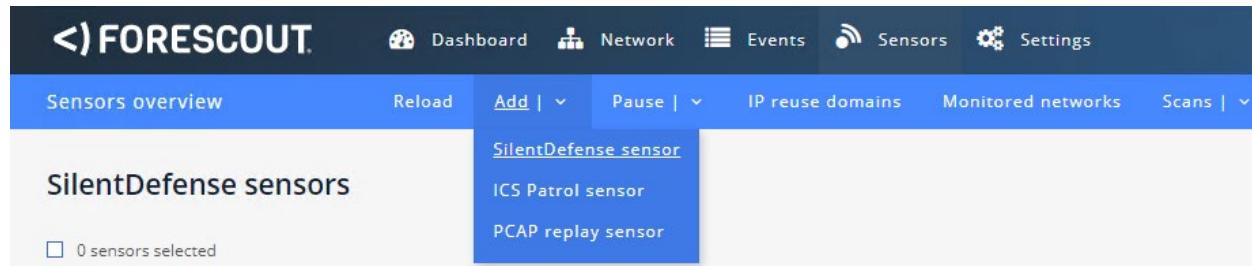
### 722 2.3.3 Configuration

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

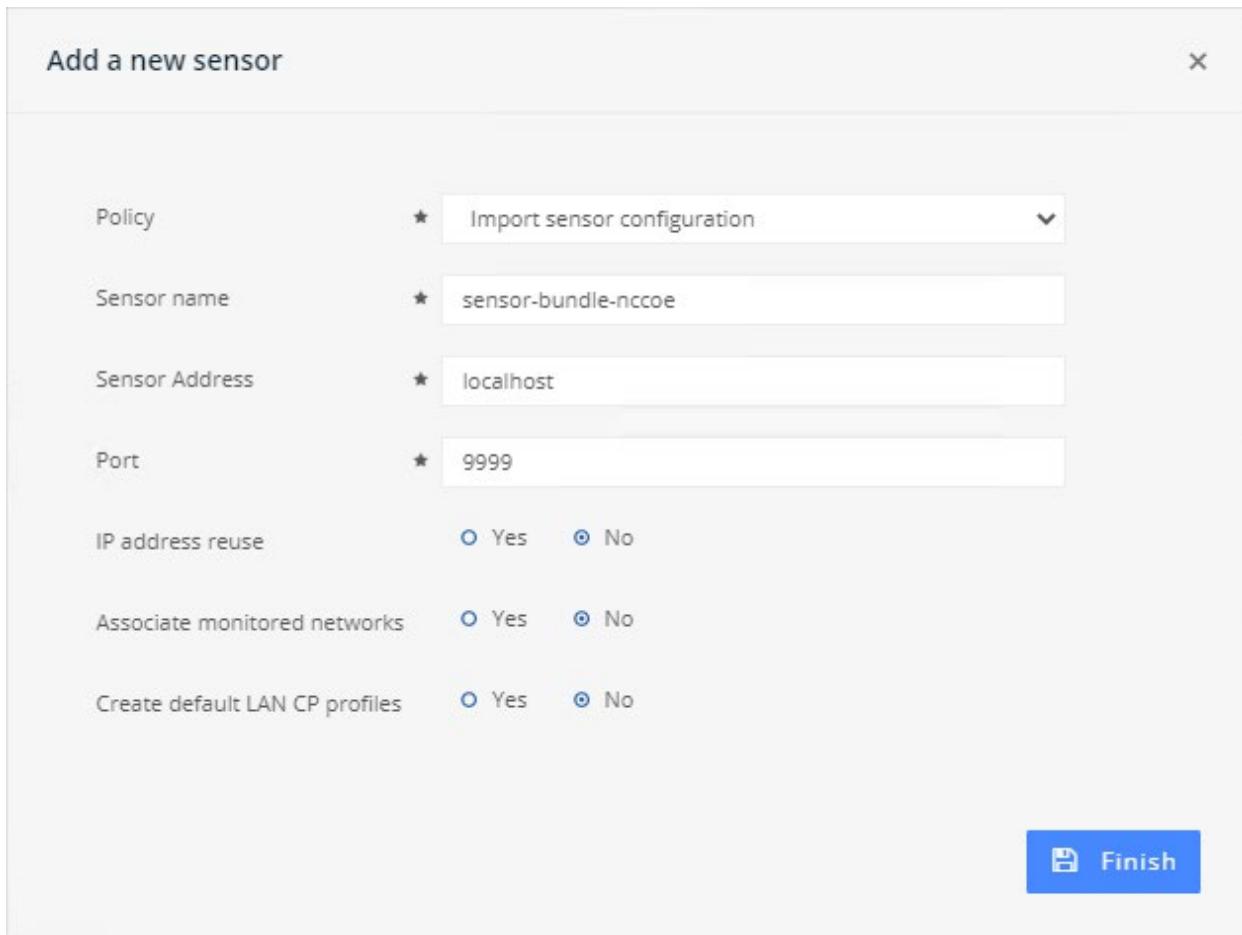
#### 724 2.3.3.1 *eyeInspect*

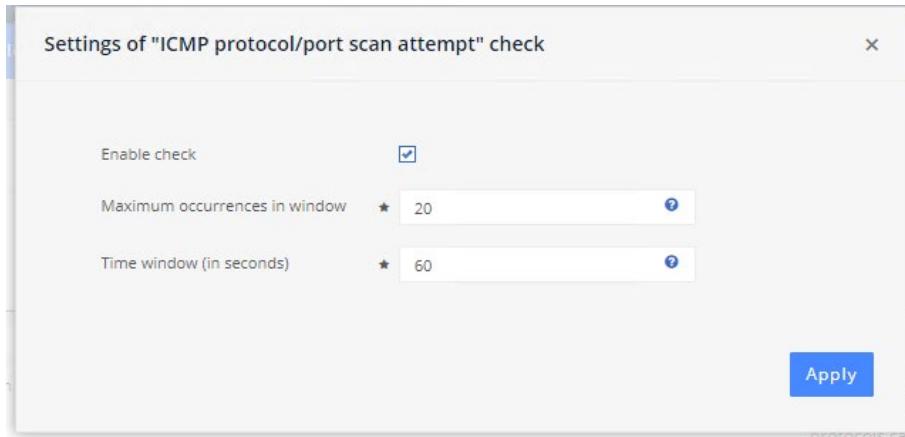
- 725       1. Access the eyeInspect web interface and log in with an administrator account.
- 726       2. Register the local sensor for SPAN traffic monitoring:
  - 727           a. Click the **Sensors** option to access the Sensor Admin/Overview Page (Figure 2-13).
  - 728           b. Click the menu 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



731 Figure 2-14 Adding a New SilentDefense Sensor Dialog



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

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

745 **Figure 2-16 eyeInspect Sensor Configuration Options**

The screenshot shows the configuration interface for a sensor named "sensor-bundle-ncoe". The top navigation bar includes Back, Edit, Import, Diagnostics, Today's alerts, Share settings, PCAP, and Help. The main content is divided into several sections:

- Sensor attributes:** Shows the sensor name as "sensor-bundle-ncoe", state as "Connected", address as "localhost", port as "9999", and monitored networks.
- Built-in modules:** Shows a list of modules with their names and states:
 

Name	State
Portscan detection	Detecting
Man-in-the-middle detection	Detecting
Malformed packet detection	Detecting
Frequent event aggregation	Active
Visual analytics	Active
Event logging	Active
- Network whitelists:** Shows communication patterns (LAN CP) with profiles for TCP and UDP communications, both in a Detecting state.
- Protocol fields (DPBI):** Shows no profiles available.
- Network intelligence framework:** Shows the Industrial threat library (ITL) with one entry: "Industrial threat library checks" (Active).
- Custom checks (SD Scripts):** Shows a list of 25 scripts, all in an Active state:
 

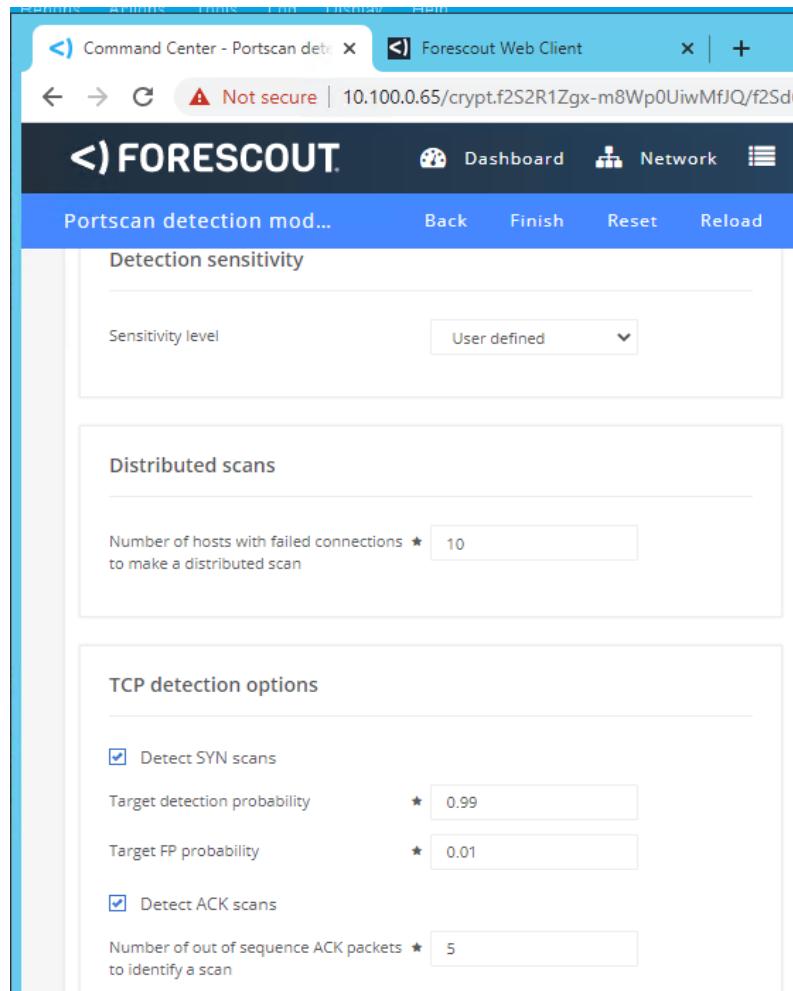
ID	Name	State
10	cve_2019_0708_monitor	Active
11	CVE_2020_0796_monitor v1.0	Active
12	CVE-2020-1350 Monitor v1.0	Active
13	ETHIP/CSP - PCCC Monitor v0.6	Active
14	Host and Link Add-Ons v1.28	Active
15	HTTP HLI v1.4	Active
17	MAC white listing v1.1	Active
18	MODBUSTCP Monitor v0.8	Active
19	MS17_010 Monitor 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 v1.30	Active

746

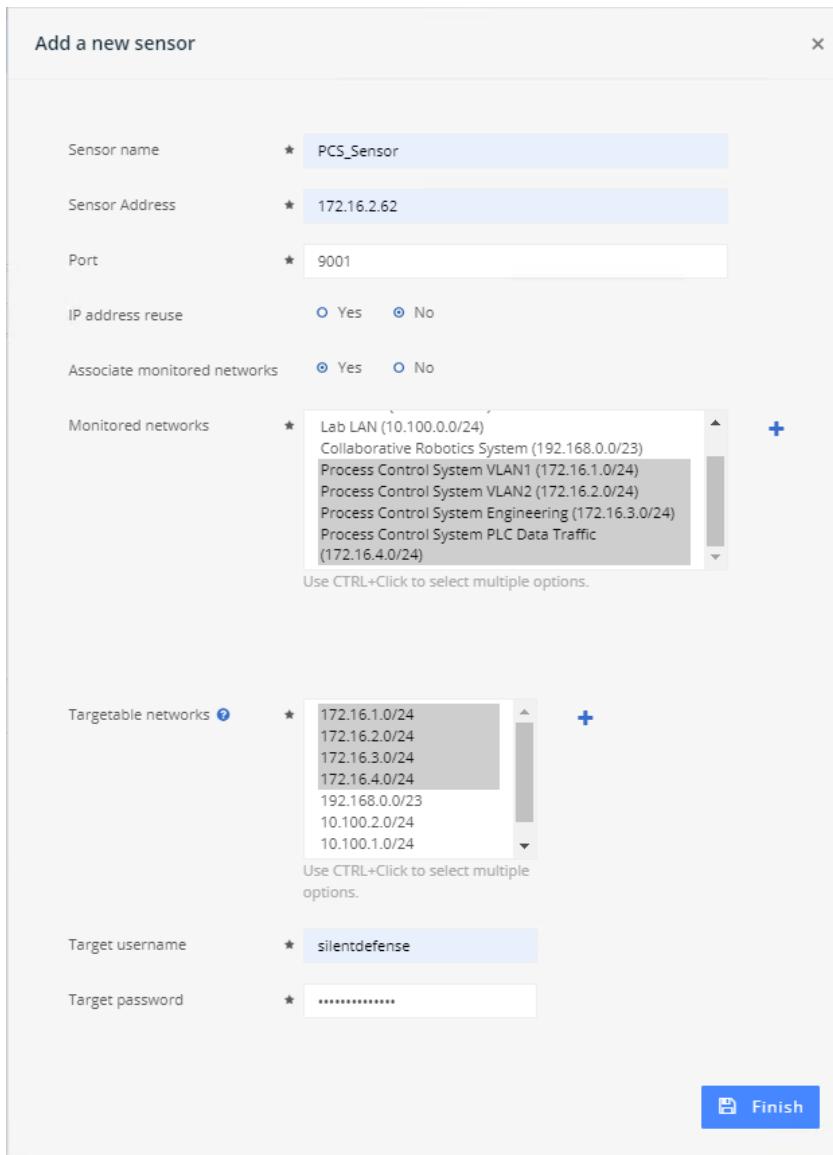
747 h. Click the **Settings** tab and set the following parameters (Figure 2-17):748 i. **Sensitivity level:** User defined749 ii. **Number of Hosts with failed connections to make a distributed scan:** 10750 iii. **Detect SYN scans:** Checked

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

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



- 756  
 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       i. Click the PCS Sensor created in the previous step to open the sensor admin page (Figure 2-19).
- 763

764 **Figure 2-19 ICS Patrol Sensor Admin Page**

The screenshot shows the 'Sensor Attributes' section of the FORESCOUT interface. The sensor name is 'PCS\_Sensor'. It is connected to the network at address 172.16.2.62 on port 9001. The target networks listed are 172.16.2.0/24, 172.16.1.0/24, 172.16.3.0/24, and 172.16.4.0/24. The monitored networks include Process Control System, Engineering, Process Control, System PLC Data Traffic, Process Control System VLAN2, Process Control System VLAN1.

Sensor Attributes	
Name	PCS_Sensor
State	Connected
Address	172.16.2.62
Port	9001
Target networks	172.16.2.0/24, 172.16.1.0/24, 172.16.3.0/24, 172.16.4.0/24
IP reuse domains	
Monitored Networks	Process Control System Engineering, Process Control System PLC Data Traffic, Process Control System VLAN2, Process Control System VLAN1

765 ii. Click the menu option **Scans > Scan Policies**.

766 iii. In the dialog option (Figure 2-20) enter the scanning parameters:

767 1) **Name:** PCS PLC768 2) **Scan Type:** EtherNet/IP769 3) **Target Type:** Custom target770 4) **IP address reuse:** No771 5) **Network Address:** 172.16.2.102772 6) **Schedule:** Yes773 7) **Frequency:** Repeat774 8) **Interval:** 1 . Select "Hours" from the drop-down menu.775 9) Click **Finish**.

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

Add scan policy

Name \* PCS PLC

Description

Scan type \*  Active IPs ?  
 OS/Ports ?  
 Custom ?  
 Windows ?  
 OT Ports ?  
 Siemens S7 ?  
 EtherNet/IP ?

Target type \* Custom target

IP address reuse  Yes  No

Network addresses \* 172.16.2.102

Schedule  Yes  No

Frequency \* Repeat

Start date \* Jun 3, 2021 12:00:00

Interval \* 1 Hours

**Finish**

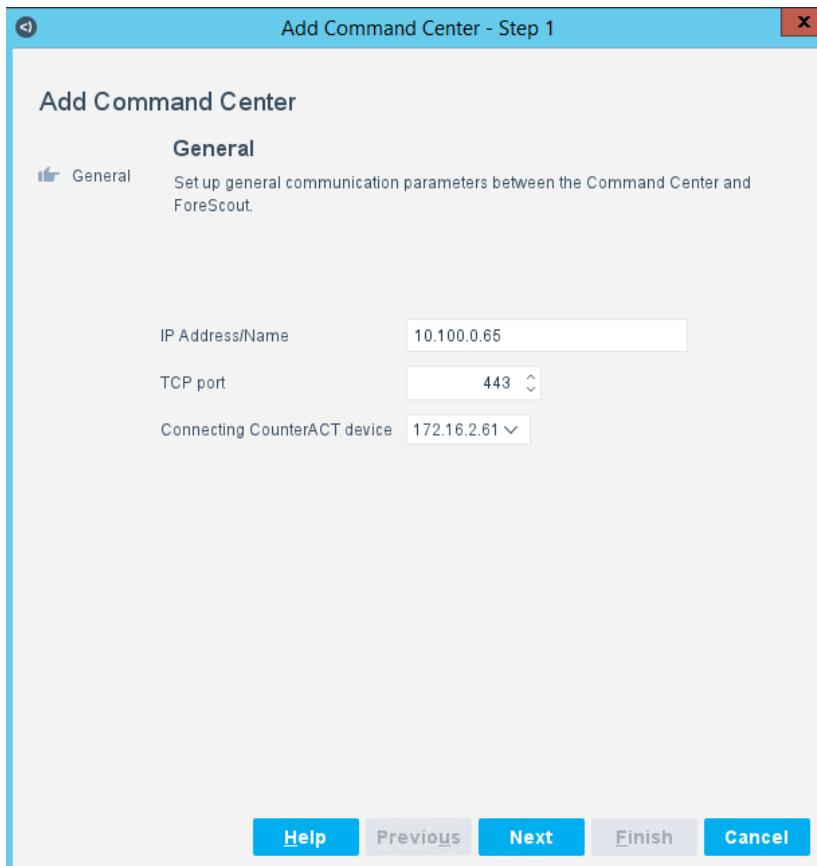
777 **2.3.3.2 eyeSight**

778 Using the Forescout Console application, users may configure, monitor, and manage the eyeSight  
 779 appliance and agents. The Forescout Console is also used to test and verify connectivity to the  
 780 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 Options display.
- 783 3. Enter "Operational" in the search bar.
- 784 4. Select the **Operational Technology** tab on the left side of the screen to display the current settings.
- 785 5. Select the IP entry for the Command Center and select **Add** to start the workflow process.

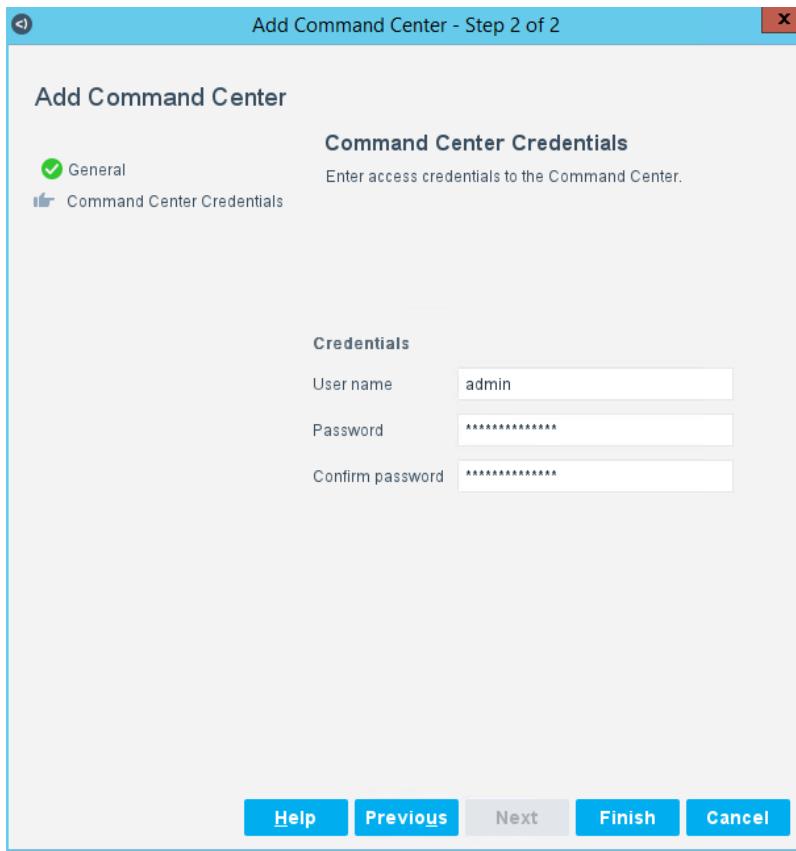
- 788           a. Specify General Information (Figure 2-21):  
789              i. Enter the Command Center IP Address "10.100.0.65" for IP Address/Name.  
790              ii. Select "172.16.2.61" from the **Connecting CounterAct device** drop-down menu.  
791              iii. Select "443" from the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

792       **Figure 2-21 eyeSight Add Dialog – General Information**

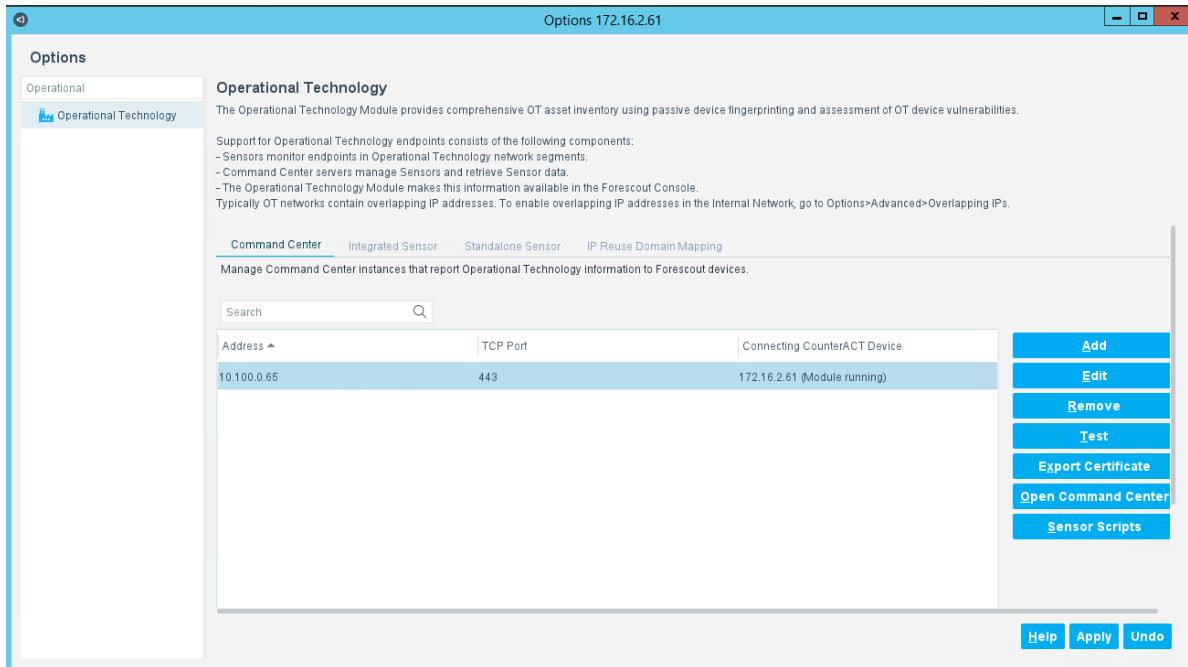
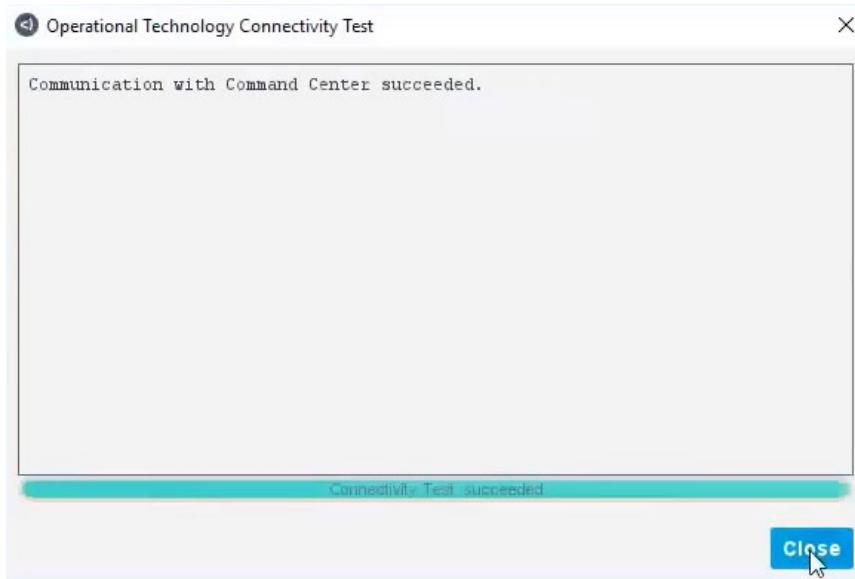


- 793           b. Click **Next**.  
794           c. Enter the command center credentials (Figure 2-22).  
795           d. Click **Finish**.

796 Figure 2-22 eyeSight Add – Command Center Credentials



- 797     6. Select the IP address for the Command Center and Click **Test** (Figure 2-23). If the connection is successful, a message like the one shown in Figure 2-24 is displayed.
- 798
- 799     7. Click **Apply** to save the changes.
- 800     8. Click **Close** to close the message.

801 **Figure 2-23 eyeSight OT Settings**802 **Figure 2-24 eyeSight Test Connection Successful Message****2.4 GreenTec-USA**

804 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**

812 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- USA Server	Supermicro x8 Series Server	Ubuntu 18.04	2x Intel Xeon E5620	16 GB	750 GB OS 1.0 TB WORMdisk 1.0 TB ForceField	DMZ 10.100.1.7

#### 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 [Figure B-1](#), [Figure B-2](#), [Figure B-3](#), and [Figure B-4](#).

825 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  
 827 Linux workstations within the testbed. The GreenTec-USA appliance did not come with Samba pre-  
 828 installed, so installation was performed via the Ubuntu Advanced Packaging Tool and the Ubuntu  
 829 package repository.

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

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

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

836 \$ sudo route add default gw 10.100.1.1

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

838            \$ sudo apt update  
839            \$ sudo apt -y install samba  
840            \$ sudo ufw allow samba

### 841        2.4.3 Configuration

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

#### 844        2.4.3.1 ForceField HDD

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

847        1. Create a mount point (empty directory) for the ForceField HDD using the following command:

848            \$ sudo mkdir /mnt/forcefield

849        2. Start the ForceField WFS volume manager to mount the drive using the following command:

850            \$ sudo /opt/greentec/forcefield/bin/wfs /dev/sdc /mnt/forcefield/

#### 851        2.4.3.2 WORMdisk HDD

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

855        1. Format the WORMdisk with 120 partitions (NOTE: this operation must be performed from the  
856        command line as administrator on a computer with the Microsoft Windows OS) using the  
857        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 following  
860        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

866        4. Create a directory structure within the “golden” directory and copy approved files into those  
867        directories (e.g., PLC logic, device firmware, approved software).

868        5. Once all files have been copied and verified, lock the partition to protect the data:

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

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

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

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

878 2. Update the files and folders in the temporary directory, /mnt/tmp, as desired.

879 3. Unmount the temporary directory and lock the partition:

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

882 4. Stop the Samba service:

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

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     /dev/sdb3 /mnt/golden fuseblk
888     rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other,blksize
889     =4096 0 0"
```

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

```
891     $ sudo mount -a
892     $ sudo systemctl start smb.service
893     $ sudo rmdir -r /mnt/tmp
```

#### 894 *2.4.3.3 Samba*

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

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

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

```
# GreenTec-USA ForceField Share
strict sync=no

# OSIsoft PI historian and database backups
[ForceField]
```

```

browsable = yes
guest ok = no
path = /mnt/forcefield
read only = no
writeable = yes
case sensitive = yes

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

```

901       3. Restart Samba:

902           \$ sudo systemctl restart smbd.service

#### *2.4.3.4 OS/soft PI Server and Database Backups*

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

906       1. 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:

913       1. Open the Task Scheduler and create a new scheduled task to rename, timestamp, and copy the  
914       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  
 931 of Build 4. The overall build architecture is provided in [Figure B-4](#). The Microsoft Azure Defender for IoT  
 932 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 IoT	Dell OEMR XL R340	Ubuntu 18.04	Intel Xeon E-2144G	32 GB	3x 2 TB Drives RAID-5	Testbed LAN 10.100.0.61

### 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:

942 a. Using either SSH, iDRAC, or the KVM Console connections on the appliance, establish  
 943 shell access to the appliance.

944 b. From the console, enter the following command:

945 `$sudo cyberx-xsense-network-reconfigure`

946 c. The system will walk through a series of network options (Figure 2-25) that are set as  
 947 follows:

948 i. **IP Address:** "10.100.0.61"

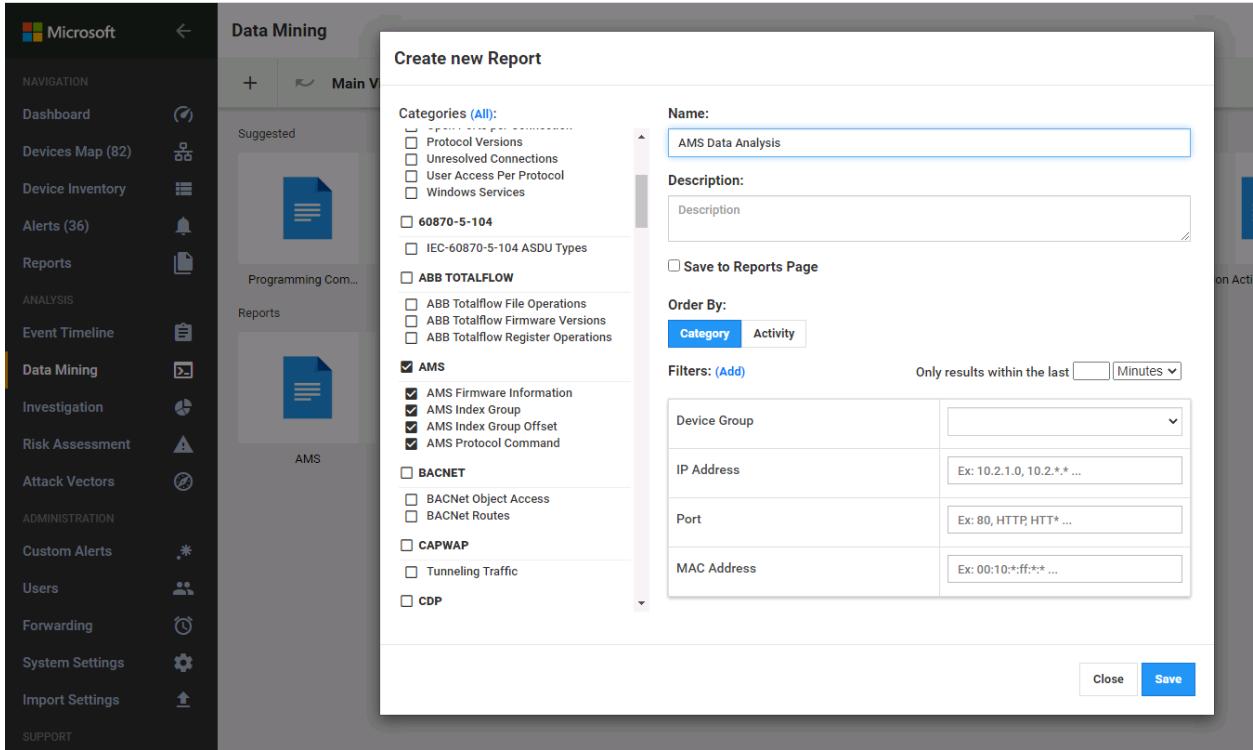
949 ii. **Subnet Mask:** "255.255.255.0"

950 iii. **DNS:** "10.100.0.17"



- 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**



- 969                                  3. Create AMS – Custom Alert Rules  
 970                                  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.  
 971                                  a. Click **Horizon** on the left menu navigation.  
 972                                  b. Select **AMS > Horizon Customer Alert** under the Plugin Options on the left menu.  
 973                                  c. Create Custom Alert to Detect Change in PLC Firmware Major Build Number (Figure 2-27):  
 974                                  i. Enter "PLC Firmware Major Build Mismatch" as the title for the custom alert.  
 975                                  ii. Enter "PLC {AMS\_server\_ip} Firmware Major Version Build Mismatch Detected" as the message to display with the alert.  
 976                                  iii. Set the following conditions:  
 977

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

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

The screenshot shows the 'AMS - Custom Alert Rules' configuration page. It includes fields for 'Title' (PLC Firmware Major Build Mismatch), 'Message' (PLC {AMS.server\_ip} Firmware Major Version Build Mismatch Detected), and two 'Conditions' blocks. Each condition block contains a variable dropdown (e.g., AMS.server\_ip or AMS.major), an operator dropdown (e.g., == or ~=), and a value input field (e.g., 3232235550 or 3). An 'AND' connector is used between the two conditions. At the bottom are 'CLEAR' and 'SAVE' buttons.

986          d. Create the custom alert to detect change in PLC firmware minor build number (Figure  
 987                 2-28):

988               i. Enter "PLC Firmware Minor Build Mismatch" as the title for the custom alert. PLC  
 989                 Firmware Minor Build Mismatch

990               ii. Enter "PLC {AMS\_server\_ip} Firmware Minor Version Build Mismatch Detected"  
 991                 as the message to display with the alert.

992               iii. Set the following conditions:

993                **1) AMS\_server\_ip == 3232235550** (Note: this is the PLC IP address  
 994                 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 AND Variable Operator Value  
 AMS.server\_ip == 32322355 AND AMS.minor ~= 1

**CLEAR** **SAVE**

997

- 998 e. Create the custom alert to detect change in the PLC Firmware Build Version (Figure  
 999 2-29):

- 1000 i. Enter "PLC Firmware Build Version Mismatch" as the Title for the custom alert.
- 1001 ii. Enter "PLC {AMS\_server\_ip} Build Version Mismatch Detected" as the message to  
 1002 display with the alert:
- 1003 iii. Set the following conditions:
- 1004 1) **AMS\_server\_ip == 3232235550** (Note: this is the PLC IP address  
 1005 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**

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

**Title**  
PLC Firmware Build Version Mismatch

**Message**  
PLC {AMS.server\_ip} Build Version Mismatch Detected

Use {} to add variables to the message

**Conditions**

Variable Operator Value AND Variable Operator Value  
 AMS.server\_ip == 32322355 AND AMS.version\_build ~= 4022

**CLEAR** **SAVE**

1008

## 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  
 1012 Historian capability by collecting and storing testbed data and the BAD capability by alerting when  
 1013 activity 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
DMZ Historian	Virtual Machine	Microsoft Windows Server 2016	4x Intel Xeon E3-1240	8 GB	Boot: 80 GB PI Data: 170 GB	DMZ 10.100.1.4

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 Supervisory LAN 192.168.0.21

1027

1028 **Table 2-12 OSIsoft PI PCS Hosts Deployment**

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

1029

1030 **2.6.2 Installation**

1031 PI was previously installed in the testbed as part of the *NISTIR 8219: Securing Manufacturing Industrial*  
1032 *Control Systems: Behavioral Anomaly Detection*,  
1033 <https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf>. 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: <https://livelibrary.osisoft.com/>.

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**

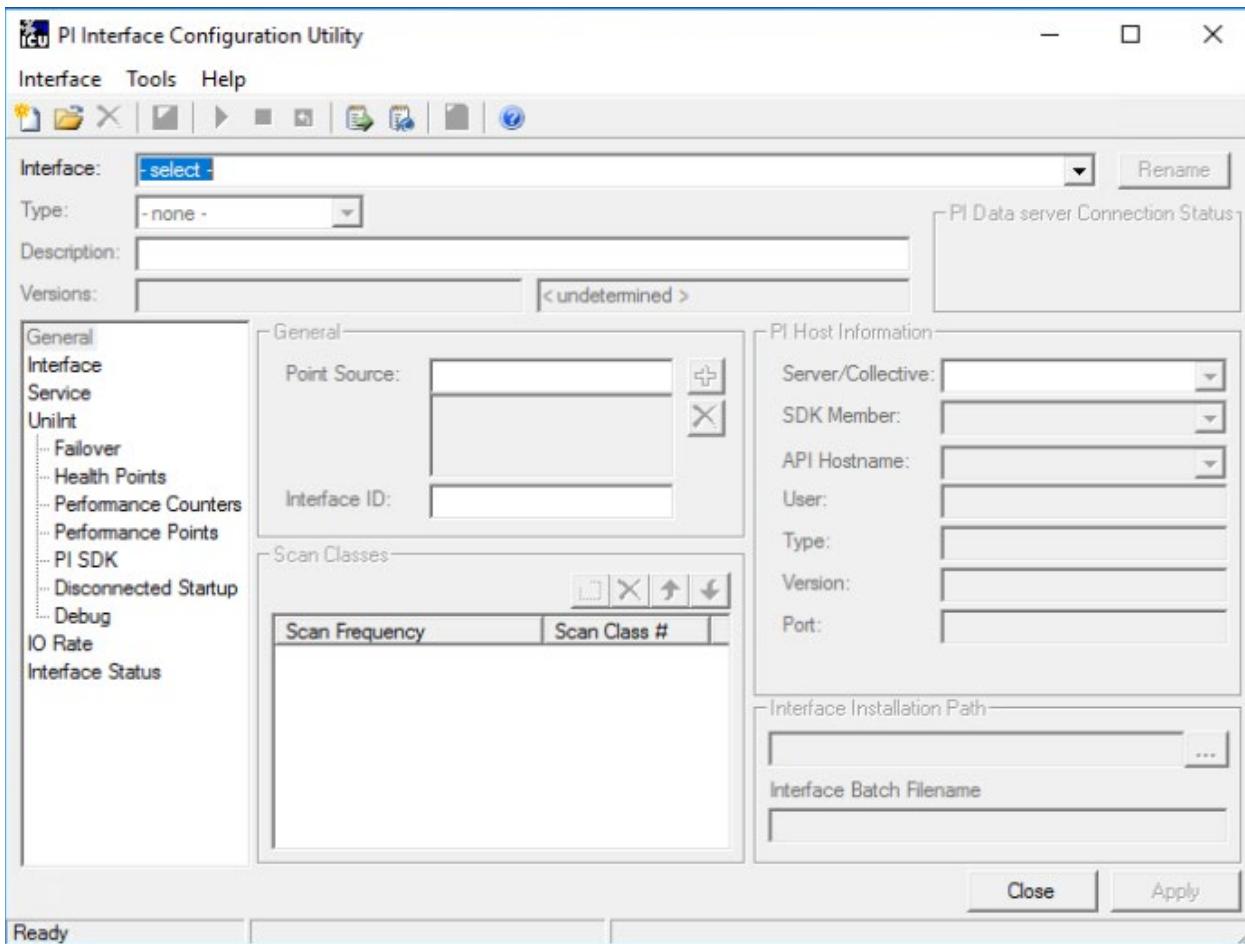
1071 The following sections describe how to configure select PI components to enable the capabilities  
1072 described in this guide. Configurations for the other PI components are not included for brevity.

1073 ***2.6.3.1 PI to PI Interface (PCS)***

1074 The PCS uses the Rockwell FactoryTalk Historian to collect, store, and analyze historical process data.  
1075 The PI to PI Interface is used to duplicate the process data to the DMZ Historian server. The following  
1076 steps describe how to configure the PI to PI Interface to collect data from the Rockwell FactoryTalk  
1077 Historian.

- 1078       1. On the DMZ Historian server, launch the **PI Interface Configuration Utility** as shown in Figure  
1079           2-30 from the Start menu and sign in with the local administrator account.

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



1081 Ready

1082

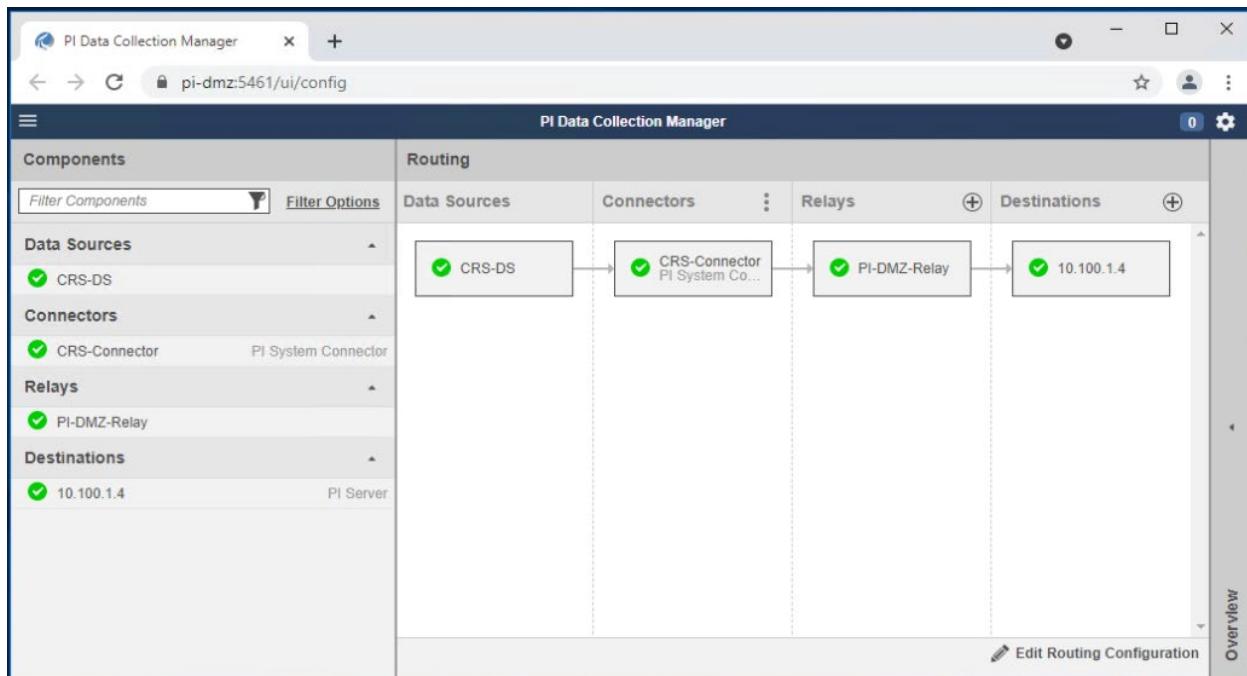
- 1083 2. On the top menu, click **Interface > New Windows Interface Instance from BAT File...**
- 1084 3. Navigate to **E:\Program Files (x86)\PIPC\Interfaces\PItoPI** and select the file **PItoPI.bat\_new**.
- 1085 4. In the “Select Host PI Data server/collective” dialog box, select **PI-DMZ** from the drop-down menu and click **OK**.
- 1086
- 1087 5. In the left navigation panel select **PItoPI**. In the Source host textbox, enter "172.16.2.4".
- 1088 6. In the left navigation panel, select **Service**. In the “Create / Remove” section click the **Create** button. Click **Yes** in the dialog box.
- 1089
- 1090 7. Enter the commands **net start PItoPI** and **net stop PItoPI** in the files **pisrvsitestart.bat** and **pisrvsitestop.bat** files, respectively. Save and close the files.
- 1091
- 1092 8. At the bottom of the **PI Interface Configuration Utility** click the **Apply** button. On top menu bar click the green play button ➤ to start the service.
- 1093

1094        9. Close the **PI Interface Configuration Utility**. The interface is now configured to pull tags from the  
 1095        Rockwell Historian.

1096        **2.6.3.2 PI 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**



1102        1. On the DMZ Historian server, launch the **PI Data Collection Manager** as shown in Figure 2-31  
 1103        from the Start menu and sign in with the local administrator account.

1104            a. Click **+** on the Relays column to add a new connector relay. Use the following settings:

1105            b. Name: PI-DMZ-Relay

1106            c. Address: 10.100.1.4

1107            d. Port: 5460

1108        2. User Name: .\piconnrelay\_svc

1109        3. Click **Save Settings** to add the connector relay.

1110        4. Click **+ Add Destination** to add the target PI Data Archive and PI AF Server. Use the following  
 1111        settings:

1112            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        6. On the CRS Local Historian server, open the **PI System Connector Administration** from the Start  
1118        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        10. On the DMZ Historian server, open the **PI Data Collection Manager** from the Start menu and  
1127        sign in with the local administrator account.
- 1128        11. Click **Untitled Connector 1** and click **Approve This Registration and Configure** to approve the PI  
1129        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        15. Click **CRS-Connector** in the **Connectors** column. On the **Overview** panel click **CRS-Connector: No  
1136        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**.  
1154            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** to  
1161            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.
- 1166        30. Each box should now contain a green checkmark (i.e., Data Sources, Connectors, Relays, and  
1167            Destinations). The elements in the AF database "testbeddatabase" on CRS Local Historian server  
1168            is 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"  
1175            analysis function and event frame template were created and used in Scenario 10.

- 1176     1. On the CRS Local Historian server, open the **PI System Explorer** by navigating to **Start Menu > PI**  
1177       **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     5. Naming Pattern: ALARM-%ELEMENT%.%TEMPLATE%.%STARTTIME:yyyy-MM-dd  
1185       HH:mm:ss.fff%
- 1186     6. In the navigation tree in the **Library** panel, select **Templates > Element Templates >**  
1187       **Machining\_Station**.
- 1188     7. In the **Machining\_Station** panel select the **Analysis Templates** tab and click **Create a new**  
1189       **analysis template**.
- 1190     8. Enter the name “Station Mode Error” in the **Name** textbox, enter a description of the analysis in  
1191       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       'RawMode' < 0 OR 'RawMode' > 1;
- 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   The PI Web API is used by Dragos to collect event frames from the DMZ Historian server. After  
1201   completing the installation of the PI Web API, the “Change PI Web API Installation Configuration” dialog  
1202   displays. 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**.
- 1204     2. In the **Configuration Store** section, select "PI-ROBOTICS" in the Asset Server drop-down menu  
1205       and click Connect. Leave the default instance name.
- 1206     3. In the **Listen Port** section, verify port 443 is entered in the **Communication Port Number**  
1207       textbox and check the **Yes, please create a firewall Exception for PI Web API** checkbox.

- 1208        4. In the **Certificate** section, click **Next** to continue and use the self-signed certificate or select  
1209        **Change** to modify the certificate.
- 1210        5. In the **API Service** section, leave the default service NT Service\piwebapi and click **Next**.
- 1211        6. In the **Crawler Service** section, leave the default service NT Service\picrawler and  
1212        click **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 Accept  
1216        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  
1222        query these Modbus registers and use analysis functions to generate event frames if any tags do not  
1223        match 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  
1227        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  
1232        following steps describe how to modify the configuration to allow two PLC tasks to write to the Modbus  
1233        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:

```

<InputRegisters>
  <MappingInfo>
    <AdsPort>851</AdsPort>
    <StartAddress>32768</StartAddress>
    <EndAddress>32895</EndAddress>
    <VarName>GVL.mb_Input_Registers</VarName>
  </MappingInfo>
  <MappingInfo>
    <AdsPort>852</AdsPort>
    <StartAddress>32896</StartAddress>
    <EndAddress>33023</EndAddress>
    <VarName>GVL.mb_Input_Registers</VarName>
  </MappingInfo>
</InputRegisters>

```

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**1243 A new PLC task must be created to perform the integrity checking and write the data to the Modbus TCP  
1244 registers. The following steps describe how to create and configure the new task.1245 1. On the engineering workstation, open the **TwinCAT XAE Shell** by navigating to **Start Menu >**  
1246 **Beckhoff > TwinCAT XAE Shell** and open the current PLC project.1247 2. In the **Solution Explorer**, right click **PLC** and select **Add New Item...**1248 3. In the **Add New Item** dialog box, select **Standard PLC Project**, enter the name  
1249 **FirmwareIntegrityCheck** in the **Name** textbox, and click **Add**.1250 4. In the **Solution Explorer**, double click **SYSTEM > Tasks > PLCTask1**. Verify the **Auto Start**  
1251 checkbox is checked and change the **Cycle Ticks** textbox to 100 ms.1252 5. In the **Solution Explorer**, right click **PLC > FirmwareIntegrityCheck > References** and click **Add**  
1253 **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_Registers : ARRAY [0..127] OF WORD;
END_VAR

```

1257

- 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**,  
1260            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 may  
1268 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

```

1269

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

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

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.

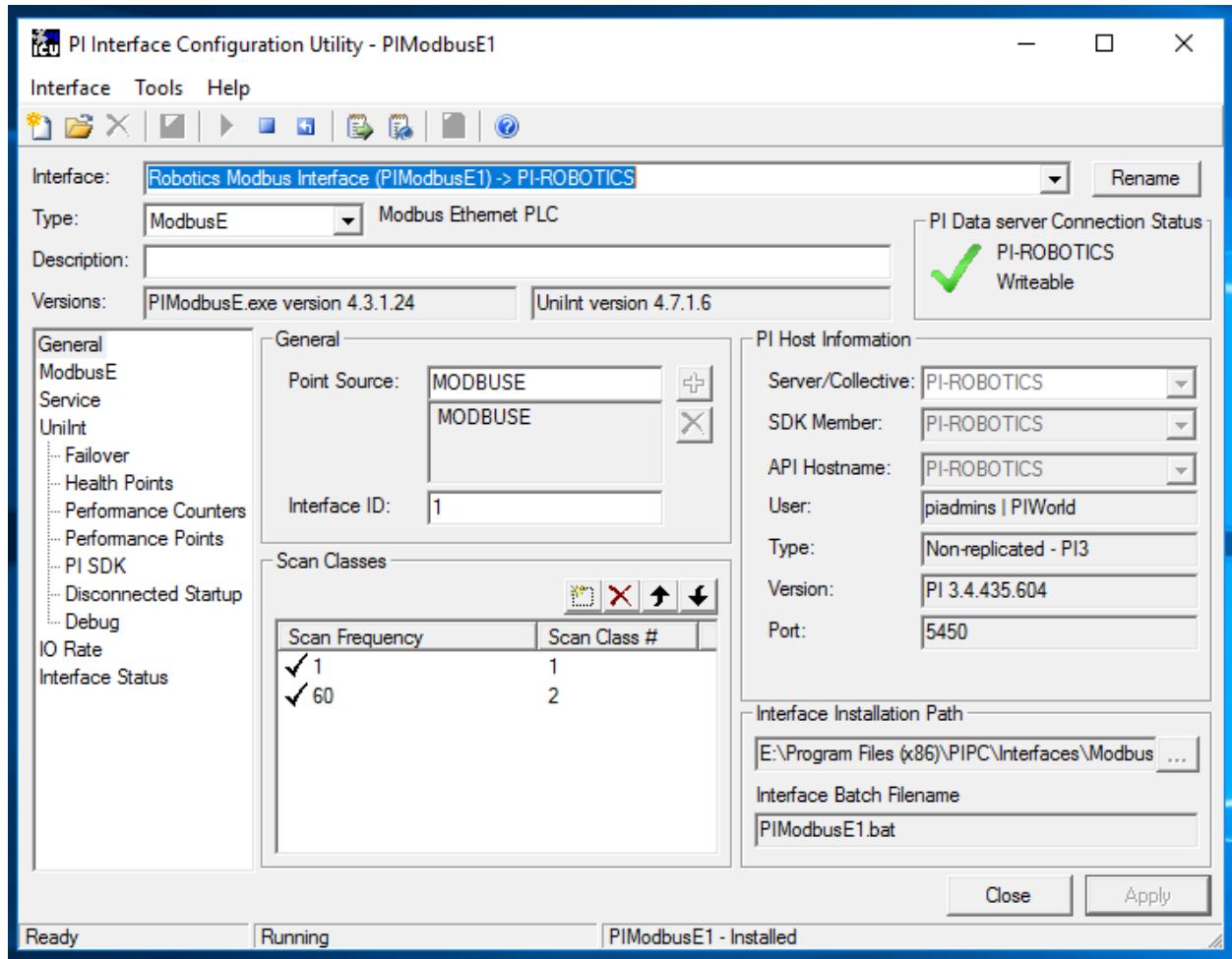
1279      The PLC will now write the hardware serial number and firmware version numbers to the Modbus  
1280      TCP server registers.

## 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.

- 1284      1. On the CRS Local Historian server, open the PI Interface Configuration Utility by navigating to  
1285      **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.
- 1288      4. Set the **Scan Frequency** to "60" and the **Scan Class #** to the next sequential class number as  
1289      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**



1292

1293

- 1294    5. Click **Apply** and close the program.
- 1295    6. On the CRS Local Historian server, open the **PI System Management Tools** by navigating to **Start Menu > PI System > PI System Management Tools**.
- 1296    7. In the System Management Tool panel, select **Points > Point Builder**.
- 1297    8. Create a new tag for the PLC hardware serial number with the following configuration:
  - 1299    a. Name: PLC-HardwareSerialNumber
  - 1300    b. Server: PI-ROBOTICS
  - 1301    c. Descriptor: Hardware serial number of the CRS Beckhoff PLC
  - 1302    d. Point Source: MODBUSE
  - 1303    e. Point Type: Int16

- 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 11. Create a new tag for the PLC TwinCAT version number with the following configuration as shown  
1335 in Figure 2-33:

1336 a. Name: PLC-TwinCATVersionNumber

1337 b. Server: PI-ROBOTICS

1338 c. 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

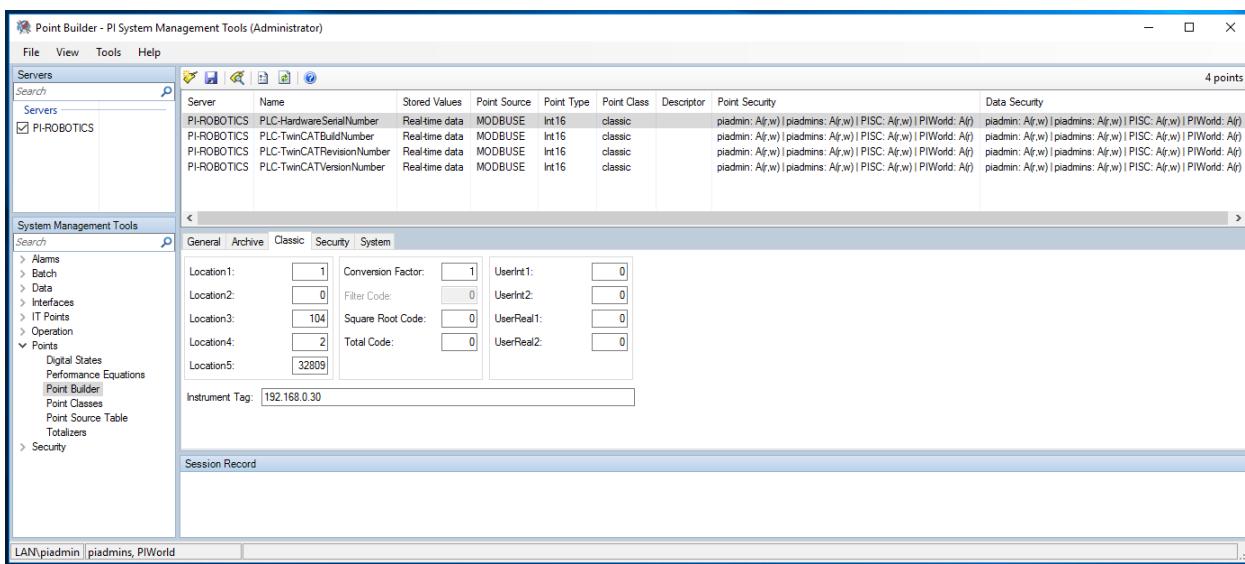
1344 i. Location 4: 2

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 DMZ  
1348 Historian server via the PI System Connector.

1349 **Figure 2-33 Screenshot of the PI System Management Tools Component After Configuring the PI Points  
1350 for PLC Hardware and Firmware Version Number Integrity Checking**



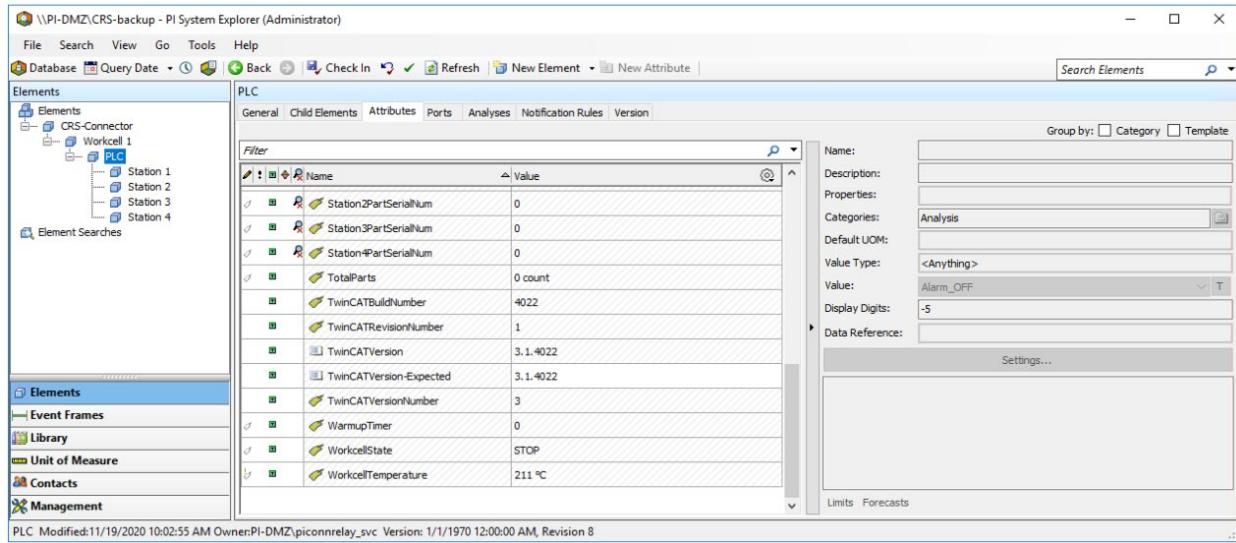
1351

1352

- 1353        13. On the DMZ Historian server, open the **PI System Explorer** by navigating to **Start Menu > PI**  
1354        **System > PI System Explorer**.
- 1355        14. On the left navigation panel, select **Library**.
- 1356        15. In the navigation tree in the **Library** panel, select **Templates > Element Templates >**  
1357        **PLCTemplate**.
- 1358        16. Open the **Attribute Templates** tab in the **PLCTemplate** panel.
- 1359        17. On the top menu bar, click **New Attribute Template** and create a new attribute for the PLC  
1360        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        18. On the top menu bar click **New Attribute Template** and create a new attribute for the expected  
1367        hardware serial number by entering the following configuration:
- 1368            a. Name: HardwareSerialNumber-Expected
- 1369            b. Description: Expected hardware serial number of the CRS Beckhoff  
1370            PLC.
- 1371            c. Value Type: V
- 1372            d. Data Reference: None
- 1373        19. On the top menu bar click New Attribute Template and create a new attribute for the PLC  
1374        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        20. On the top menu bar click New Attribute Template and create a new attribute for the PLC  
1381        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       21. On the top menu bar click New Attribute Template and create a new attribute for the PLC  
1388                   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       22. On the top menu bar click New Attribute Template and create a new attribute for the string  
1395                   representation of the version, revision, and build numbers by entering the following  
1396                   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                   e. String:  
1402                    'TwinCATVersionNumber';.;'TwinCATRevisionNumber';.;'TwinCAT  
1403                    BuildNumber';
- 1404       23. On the top menu bar click New Attribute Template and create a new attribute for the PLC  
1405                   expected TwinCAT version number by entering the following configuration as shown in Figure  
1406                   2-34:
- 1407                   a. Name: TwinCATVersion-Expected  
1408                   b. Description: Expected version number of the CRS PLC TwinCAT  
1409                   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.**



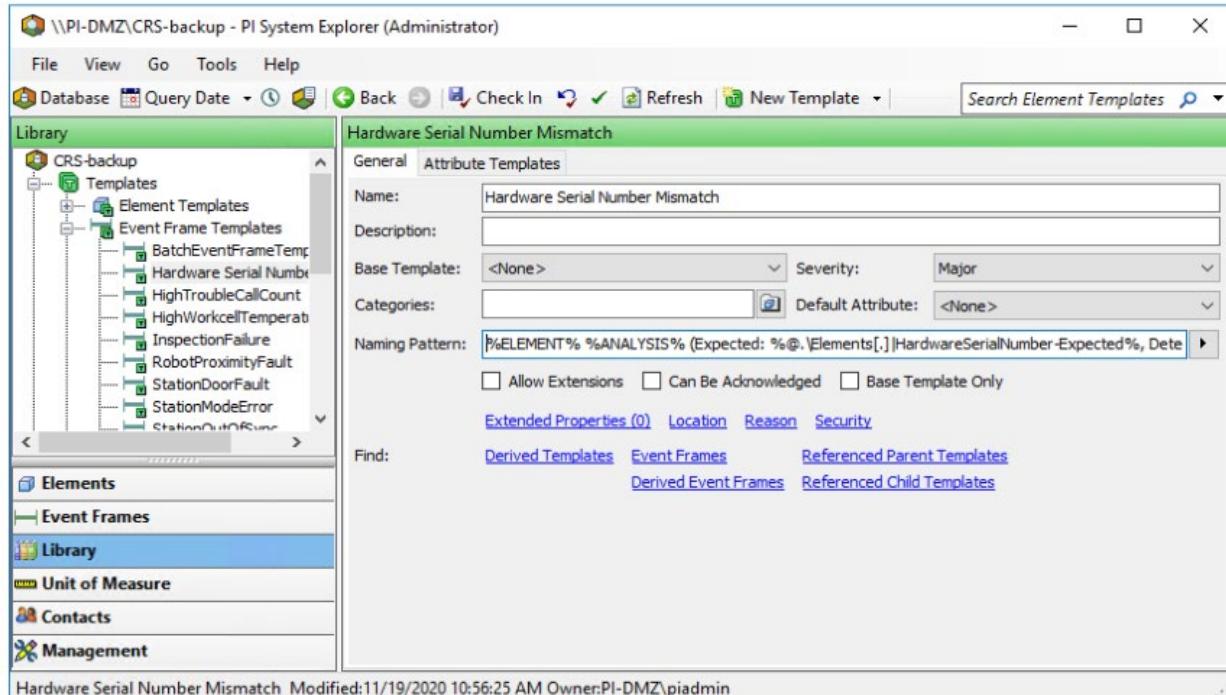
1415    PLC Modified:11/19/2020 10:02:55 AM Owner:PI-DMZ\piconnrelay\_svc Version: 1/1/1970 12:00:00 AM, Revision 8

## 1416    OSIsoft PI Analyses and Event Frames

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.

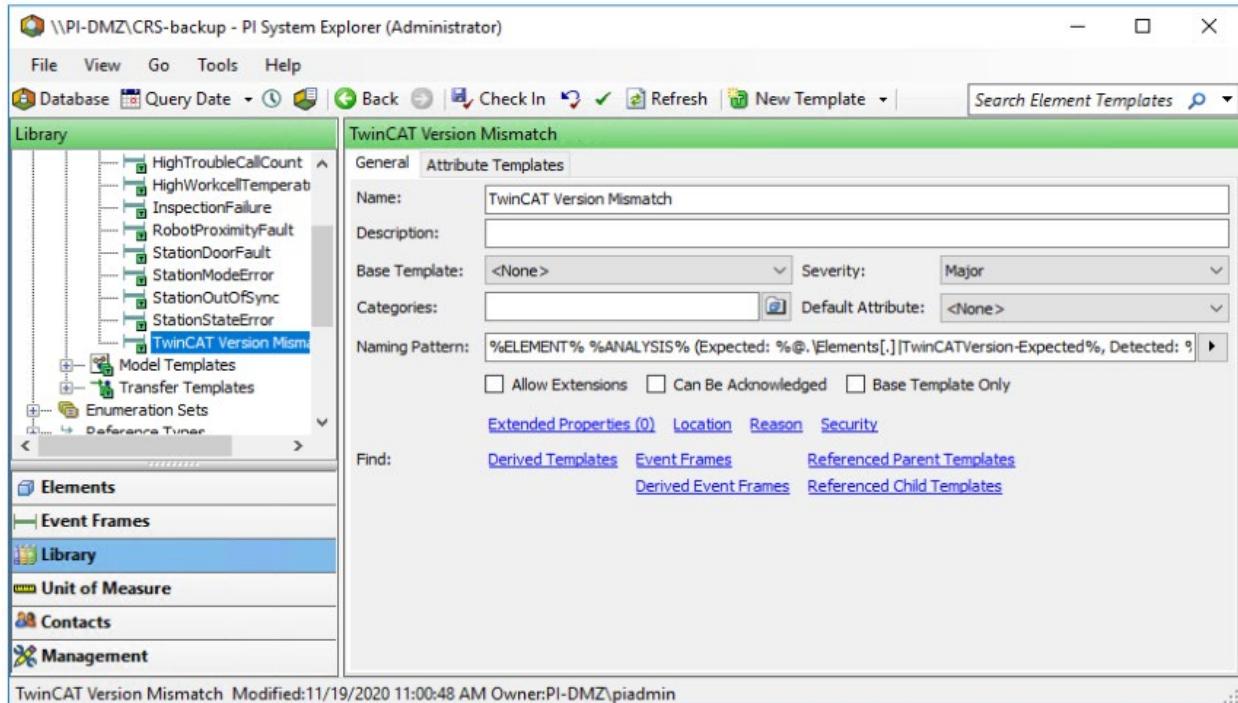
- 1419        1. In the navigation tree in the **Library** panel, select **Templates > Event Frame Templates**.
- 1420        2. On the top menu bar click **New Template** and enter the following configuration as shown in  
 1421        Figure 2-35:
  - 1422            a. Name: Hardware Serial Number Mismatch
  - 1423            b. Naming pattern: %ELEMENT% %ANALYSIS% (Expected:  
 1424              %@.\Elements[.]|HardwareSerialNumber-Expected%, Detected:  
 1425              %@.\Elements[.]|HardwareSerialNumber%) %STARTTIME:yyyy-MM-  
 1426              dd HH:mm:ss.ffff%

1427    **Figure 2-35 Screenshot of PI System Explorer Displaying the Hardware Serial Number Mismatch Event  
1428    Frame Template.**



- 1429  
1430    3. On the top menu bar click **New Template** and enter the following configuration as shown in  
1431    Figure 2-36:  
1432        a. Name: TwinCAT Version Mismatch  
1433        b. Naming pattern: %ELEMENT% %ANALYSIS% (Expected:  
1434                    %@.\Elements[.]|TwinCATVersion-Expected%, Detected:  
1435                    %@.\Elements[.]|TwinCATVersion%) %STARTTIME:yyyy-MM-dd  
1436                    HH:mm:ss.fff%

1437    **Figure 2-36 Screenshot of PI System Explorer Displaying the TwinCAT Version Mismatch Event Frame  
1438    Template**



1439

1440

- 1441        4. Click the **Check In** button on the top menu to save all changes to the database.
- 1442        5. In the navigation tree in the **Library** panel, select **Templates > Element Templates > PLCTemplate**.
- 1443        6. Open the **Analysis Templates** tab in the **PLCTemplate** panel and click **Create a new analysis template**.
- 1444        7. Enter the following configuration as shown in Figure 2-37:
  - 1447            a. **Name:** Hardware Serial Number Mismatch
  - 1448            b. **Description:** The PLC hardware serial number does not match the expected serial number.
  - 1449            c. **Analysis Type:** Event Frame Generation
  - 1450            d. **Enable analyses when created from template:** Checked
  - 1451            e. **Generation Mode:** Explicit Trigger
  - 1452            f. **Event Frame Template:** Hardware Serial Number Mismatch
- 1453        8. In the **Expression** field for "StartTrigger1", enter the expression:

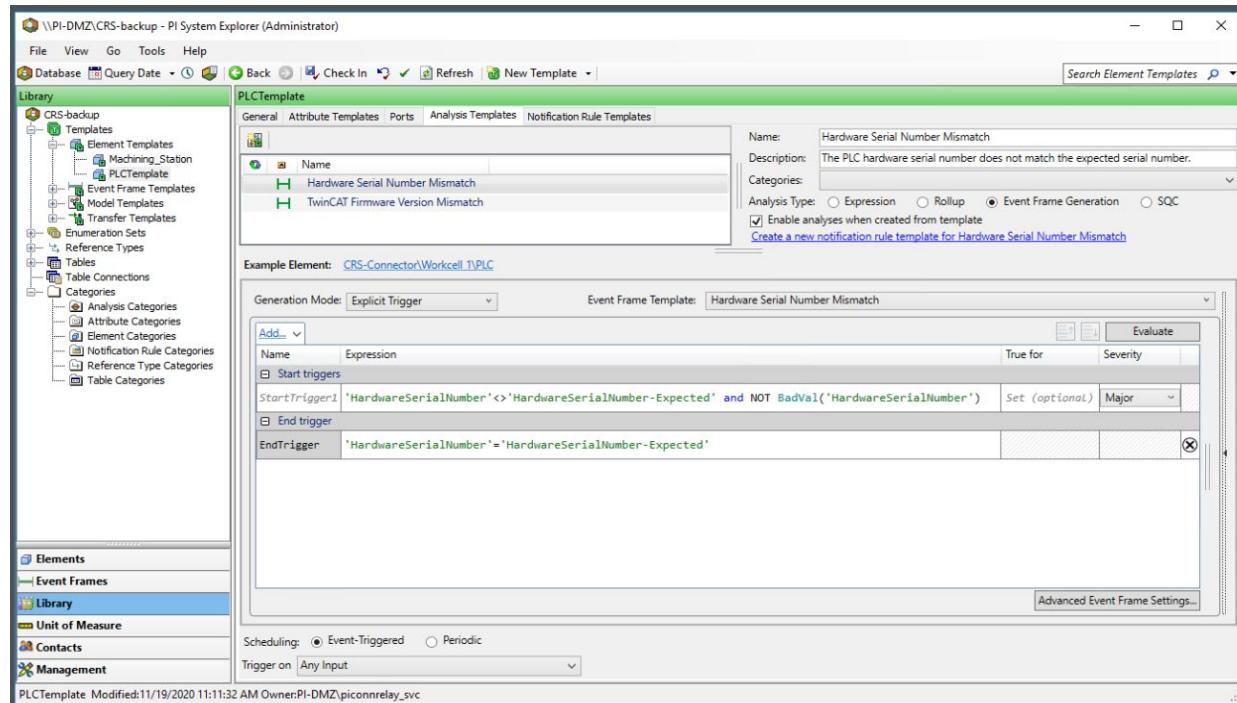
1455                   'HardwareSerialNumber'<>'HardwareSerialNumber-Expected' and NOT  
 1456                   BadVal('HardwareSerialNumber') ;

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**



1463     PLCTemplate Modified:11/19/2020 11:11:32 AM Owner:PI-DMZ\piconrelay\_svc

1464

1465     11. To create a new analysis template for TwinCAT firmware version mismatch, click **Create a new**  
 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 not  
 1470                   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:

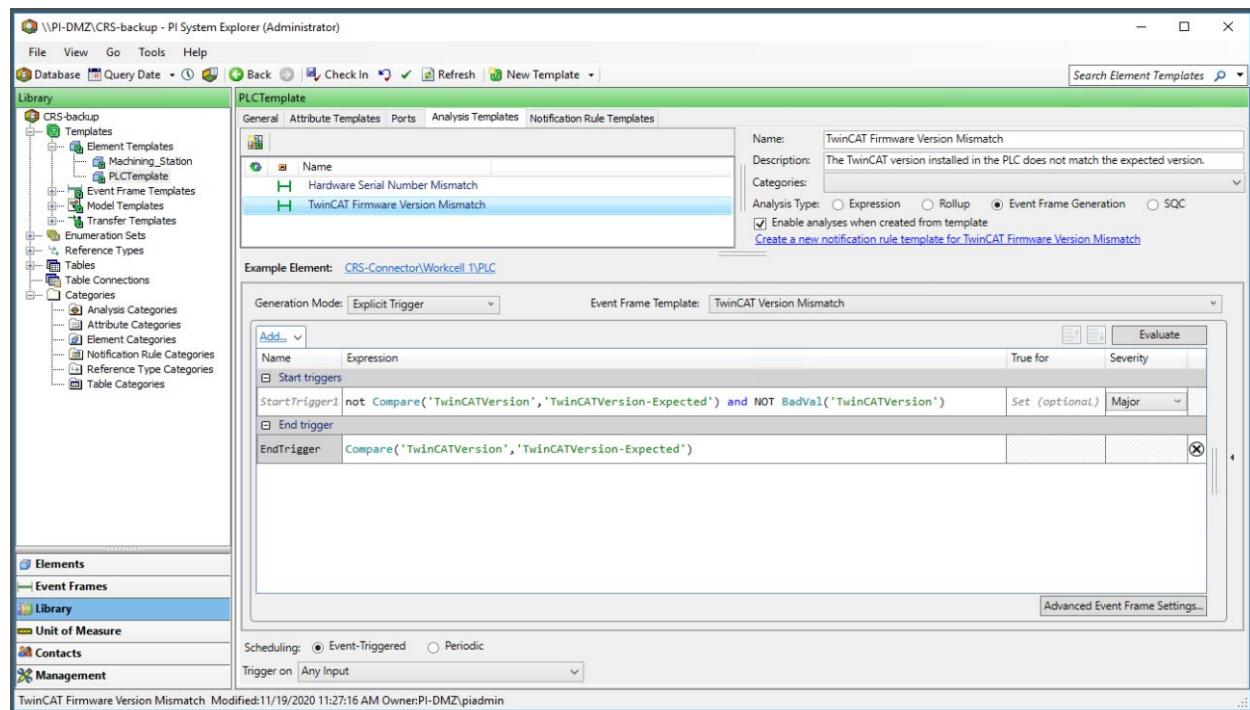
```
1476     not Compare('TwinCATVersion','TwinCATVersion-Expected') and NOT  
1477     BadVal('TwinCATVersion');
```

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.

1482 **Figure 2-38 Screenshot of PI System Explorer Displaying the TwinCAT Firmware Version Mismatch**  
1483 **Analysis Template in the PLC Element Template**



1484

1485

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

1500        Security Onion is a Linux-based, open source security playbook. It includes numerous security tools for  
 1501        intrusion detection, log management, incident response, and file integrity monitoring. For this project,  
 1502        the tool Wazuh was used in Builds 2 and 4 for file integrity checking. Wazuh works at the host-level to  
 1503        detect unusual and unauthorized activity and changes to file and software configurations. Security  
 1504        Onion and Wazuh use Elastic Stack components, Elasticsearch, Filebeat, and Kibana to store, search, and  
 1505        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  
 1512        and Table 2-15) with the installed agent.

1513        **Table 2-13 Security Onion Domain Hosts Deployment**

Name	System	OS	CPU	Memory	Storage	Network
Security Onion 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 Historian	Hyper-V VM	Windows 2016	4	8GB	80GB/171GB	DMZ LAN 10.100.1.4

1514

1515 **Table 2-14 Security Onion PCS Hosts Deployment**

Name	System	OS	CPU	Memory	Storage	Network
PCS Engineering Workstation	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 Engineering Workstation	Dell Precision T5610	Windows 10	8	16GB	465GB	CRS Supervisory 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 to  
1522 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  
1525 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  
1533 Installation Guide for version 3.9 available at <https://documentation.wazuh.com/3.9/user-manual/registering/index.html>.

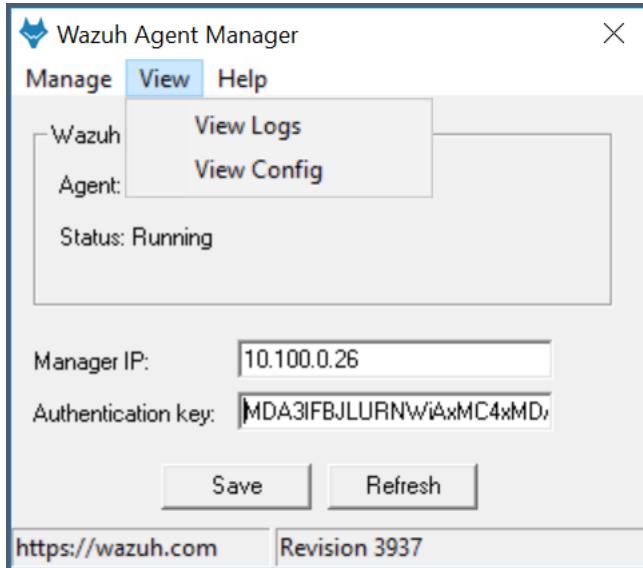
## 1535 [2.7.3 Configuration](#)

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                   i. To view or edit this file, click the View tab in the Wazuh Configuration Manager  
 1539                   on the host machine and select View Config as shown in Figure 2-39.

1540 **Figure 2-39 Wazuh Agent Manager**



1541  
 1542                   b. Selecting View Config opens the ossec.conf file in Notepad. Alternatively, the file can be  
 1543                   opened in Notepad from its location in the "C:\Program Files (x86)\ossec-agent" direc-  
 1544                   tory 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:\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>

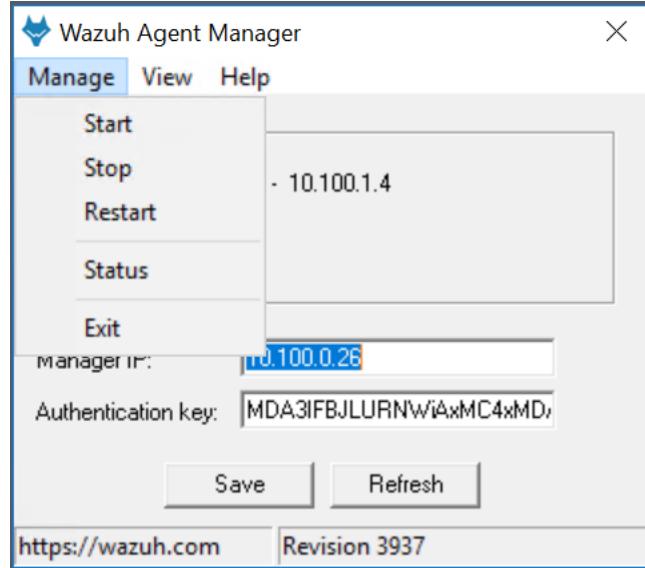
<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evt$</ignore>
```

1546  
 1547                   c. To add files or directories to the default configuration, copy and modify an existing line  
 1548                   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  
 1550           opening the Configuration Manager, selecting "Manage", and "Restart" as shown in Fig-  
 1551           ure 2-41.

1552 **Figure 2-41 Wazuh Agent Manager User Interface**



1553  
 1554           e. Changes to the files or directories specified in the ossec.conf file will be detected and  
 1555           sent to the Wazuh Manager. Figure 2-42 shows the log received after a file change was  
 1556           detected.

1557 **Figure 2-42 Log Received After a File Change Was Detected**

```
OSSEC-Logs
t @version          Q, Q, □ * 1
t _id               Q, Q, □ * BXZRLXUB1YHtrLLybilF
t _index             Q, Q, □ * seconion:logstash-ossec-2020.10.15
# _score             Q, Q, □ * -
t _type              Q, Q, □ * doc
t agent.id           Q, Q, □ * 005
? agent.ip           Q, Q, □ * ▲ 172.16.3.10
t agent.name         Q, Q, □ * PCS-EWS
# alert_level        Q, Q, □ * 7
t classification     Q, Q, □ * "Bad word" matching
t decoder.name       Q, Q, □ * syscheck_integrity_changed
t description         Q, Q, □ * Integrity checksum changed.
t event_type          Q, Q, □ * ossec
t full_log            Q, Q, □ * File 'c:\users\administrator\downloads\ra\test.txt' checksum changed.
                                         Size changed from '0' to '4'
                                         Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e'
                                         New md5sum is : '098ff6bcd4621d373cade4e832627b4f6'
                                         Old sha1sum was: 'da39a3ee5e6b400d325bfe95601890afdf80709'
                                         New sha1sum is : 'a94a8feccb19ba1c4c0873d391e987982fbdb3'
                                         Old sha256sum was: 'e3b0c44298fc1c149afbf4c8996fb92427ae1a4649b934ca495991b7852b855'
                                         New sha256sum is : '9f86d081884c7d659a2fea0c55ad015a3bf4fib2b0b822cd15d6c15b0f00a08'
                                         Old modification time was: 'Thu Oct 15 17:31:38 2020', now it is 'Thu Oct 15 17:31:49 2020'
                                         (Audit) User: 'Administrator (S-1-5-21-239850103-4004920075-3296975006-500)'
                                         (Audit) Process id: '9532'
                                         (Audit) Process name: 'C:\Windows\System32\notepad.exe'
```

1558

## 1559 2.8 TDi ConsoleWorks

1560 The TDi ConsoleWorks implementation in Builds 1 and 3 consists of a single VM hosted on VMWare ESXi  
 1561 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 750 GB	Testbed LAN 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 750 GB	CRS 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 <https://support.tditechnologies.com/product-documentation>. Follow these steps for installation:

1575 1. Harden and configure the Operating System:

1576 a. Log in to the system with privileged access and set the Static IP Address information by  
 1577 editing `/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                                 **# systemctl restart network**  
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                         c. Apply the following Department of Defense (DOD) Security Technology Implementation  
1594                         Guide (STIG) settings:  
1595                                 i. Ensure ypserv is not installed using the following command:  
1596   **# yum remove ypserv**  
1597                                 ii. Ensure Trivial File Transfer Protocol (TFTP) is not installed using the following  
1598                                 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                                 1) To disable SSHv1, ensure only Protocol 2 is allowed in the  
1608   */etc/ssh/sshd\_config*.  
1609   **Protocol 2**  
1610   **PermitRootLogin no**  
1611   **Ciphers aes128-ctr, aes192-ctr, aes256-ctr, aes128-  
1612   cbc**  
1613   **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                   2) Remove any instances of the **nullok** option in /etc/pam.d/system-auth and  
1617                   /etc/pam.d/password-auth files.

1618               viii. Enable FIPS Mode as follows:

1619                   1) FIPS mode can be enabled by running the command:

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

1622                   2) When step 1) is complete, add **fips=1** to the /etc/default/grub file and run  
1623                   the command:

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

1625                   3) When step 2) completes, reboot the server with this command:

```
# reboot
```

1627               ix. Enable server auditing

1628                   1) Ensure events on the server are being recorded for investigation in the  
1629                   event of an outage or attack. This can be enabled by running the command:

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

1631               x. Configure system to only install approved digitally signed packages:

1632                   1) Configure yum to verify the Certificate Authority is from an approved  
1633                   organization. To enable this, ensure that **gpgcheck=1** is in the  
1634                   /etc/yum.conf file.

1635               xi. Enable the firewall:

1636                   1) To enable the firewall, run the following commands:

```
# yum install firewalld and  
# systemctl start firewalld.
```

1639                   2) Check Firewall Zone and confirm only SSH and HTTPS is allowed. Note: the  
1640                   default zone is Public and SSH is already permitted. For the  
1641                   implementation, we checked the configuration using the following  
1642                   command:

```
# firewall-cmd --list-all
```

1644                   3) Add the HTTPS configuration to the firewall using the following command:

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

1647               xii. Enable SELinux and set to "targeted":

1648                   1) Add SELINUX=enforcing and SELINUXTYPE=targeted in the  
1649                   /etc/selinux/config file and then reboot the server with this command:  
1650                   **# reboot**

1651                 xiii. Enable Antivirus as follows:

1652                   1) ClamAV is used for the lab implementation using the following commands  
1653                   adapted from information found on  
1654                   <https://www.clamav.net/documents/clam-antivirus-user-manual>:

1655                   **# yum install -y epel-release**

1656                   **# yum -y install clamav-server clamav-data**  
1657                   **clamav-update clamav-filesystem clamav clamav-**  
1658                   **scanner-systemd clamav-devel clamav-lib clamav-**  
1659                   **server-systemd**

1660                   2) Update SELinux policy to allow ClamAV to function

1661                   **# setsebool -P antivirus\_can\_scan\_system 1**

1662                   3) Make a backup copy of the scan.conf file and update to remove the  
1663                   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                   5) Configure freshclam to automatically download updated virus definitions  
1669                   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                   9) Create the daily scan script to scan directories of interest. Note: for the lab  
1680                   implementation only the /home volume was selected for scanning.

1681                   # vi /etc/cron.daily/clamav\_scan.sh

1682

1683                   **File Contents**

1684

```
1685                   #!/bin/bash
1686                   SCAN_DIR="/home"
1687                   LOG_FILE="/var/log/clamav/dailyscan.log"
1688                   /usr/bin/clamscan -ri $SCAN_DIR >> $LOG_FILE
```

1689                   10) Set the file to have execute privilege with this command:

1690                   # chmod +x /etc/cron.daily/clamav\_scan.sh

1691                  2. Download and Install the ConsoleWorks packages

1692                  a. Login to TDi Technology Support Portal ([https://support.tditechnologies.com/get\\_consoleworks](https://support.tditechnologies.com/get_consoleworks)) to download the ConsoleWorks for Linux 5.3-1u3 installation package. Credentials will be provided by TDi.

1695                  b. After downloading the ConsoleWorks installation package, copy it to the ConsoleWorks  
1696                  VM using a Secure Copy (scp) utility.

1697                  c. Follow the procedures from TDi ConsolWorks New Installation and Upgrade Guide for  
1698                  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

The screenshot shows the 'ConsoleWorks' interface with a version of 'v 5.3-1u3'. The main title bar says 'unregistered Administration'. On the left, there's a sidebar with 'FAVORITES' (No Favorites saved), 'DASHBOARDS', 'CONSOLES', 'DEVICES', 'LOGS', 'EVENTS', 'REGULATORY', 'GRAPHICAL', 'USERS', 'REPORTS', 'TOOLS', 'SECURITY', 'ADMIN', and 'HELP'. Below this is an 'EXTERNAL TOOLS' section with 'None Available'. The main content area is titled 'ADMIN: Server Management: Registration' with tabs for 'Registration' (selected) and 'Offline Registration'. It contains fields for 'Contact Name', 'Contact Email', 'Telephone', 'Facility (Site) Name' (set to 'NIST Gaithersburg'), 'Address Line 1' (set to '100 Bureau Drive'), 'Address Line 2', 'City' (set to 'Gaithersburg'), 'State/Province' (set to 'MD'), 'Zip/Postal Code' (set to '20879'), and 'Country' (set to 'United States'). To the right are sections for 'PROXY DETAILS' and 'ADVANCED OPTIONS'. At the bottom are 'Register Online' and 'Register Offline' buttons, along with 'Cancel' and 'Save' buttons.

1705

1706 Figure 2-44 ConsoleWorks Offline Registration Process

The screenshot shows the 'ConsoleWorks' interface with a version of 'v 5.3-1u3'. The main title bar says 'Unregistered Administration'. The sidebar is identical to Figure 2-43. The main content area is titled 'ADMIN: Server Management: Offline Registration' with tabs for 'Registration' (selected) and 'Offline Registration'. It contains instructions: 'Please send [support@tditechnologies.com](mailto:support@tditechnologies.com) an Email with:' followed by a bullet point '• This file attached'. Below this is a note: 'Which contains your contact info, server operating system, and ConsoleWorks version. If Email is unavailable, please contact [TDI Support](#)'. At the bottom is a 'Complete My Offline Registration' button.

1707

- 1708 f. This completes the default installation and establishes a basic ConsoleWorks server configuration. For the lab implementation, ConsoleWorks support provided two additional add-on packages (XML) files to setup the environment: ONBOARDING\_1-DASH-  
 1709 BOARDS\_NCCoE.zip providing preconfigured dashboards for accelerating configurations;  
 1710  
 1711 and NCCOE\_ACRs\_20210122\_083645.zip providing the access control rules, tags, and  
 1712

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

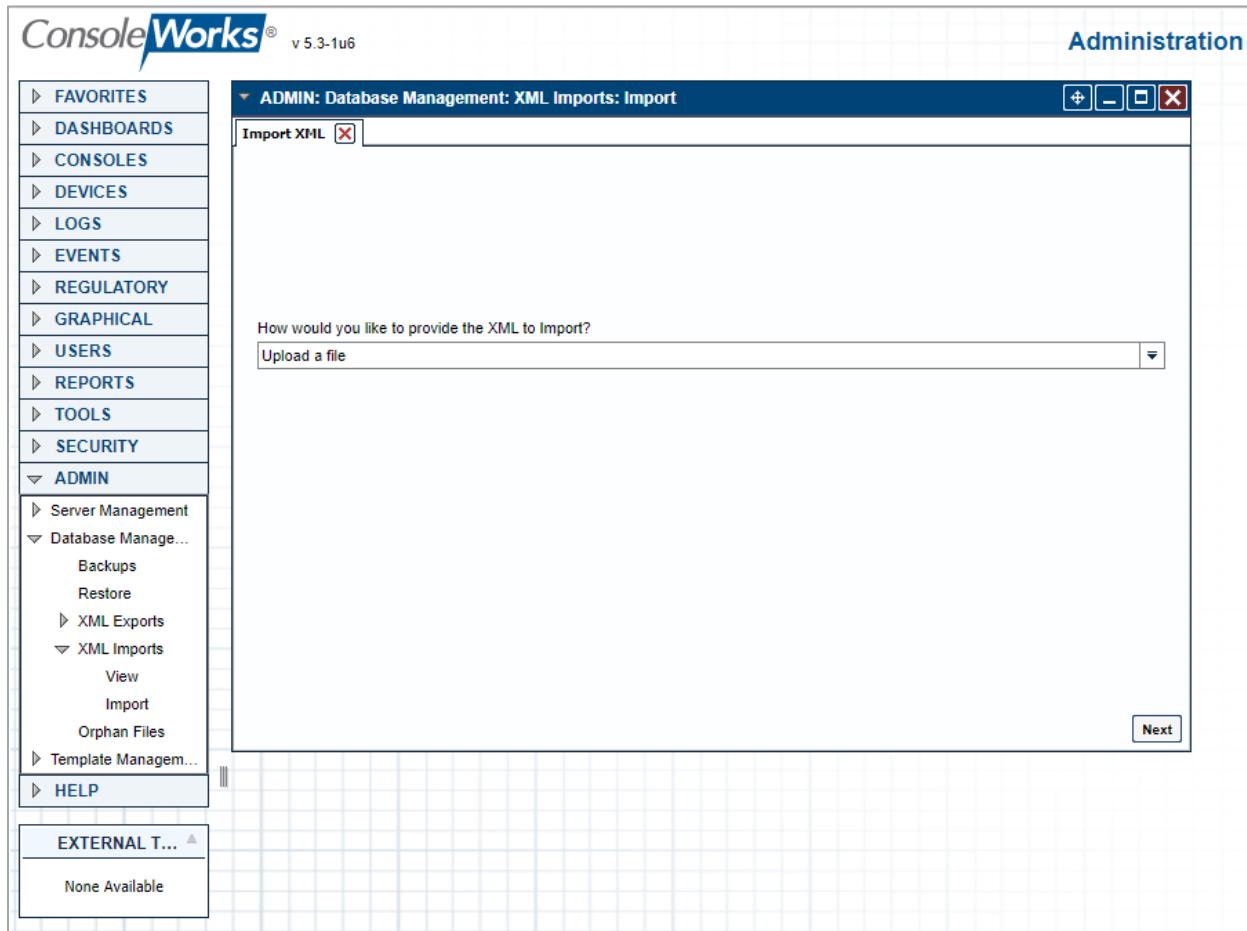
1715                    i. Prior to installing these packages, a backup of the configuration should be made  
 1716                    (Figure 2-45) by accessing **Admin > Database Management > Backups** and click-  
 1717                    ing **Create Backup**.

1718                  **Figure 2-45 ConsoleWorks System Backups**

Start Time	User	Status	Locked
2021/05/15 03:00	Schedule:WEEKLY	Done	N
2021/03/13 03:00	Schedule:WEEKLY	Done	N
2021/03/06 03:00	Schedule:WEEKLY	Done	N
2020/12/09 10:31	CONSOLE_MANAGER	Done	N
2021/02/02 16:38	CONSOLE_MANAGER	Done	N
2021/04/24 03:00	Schedule:WEEKLY	Done	N
2021/06/14 10:55	CONSOLE_MANAGER	Done	N
2021/02/11 08:07	CONSOLE_MANAGER	Done	N
2021/05/01 03:00	Schedule:WEEKLY	Done	N
2021/02/13 03:00	Schedule:WEEKLY	Done	N
2021/05/08 03:00	Schedule:WEEKLY	Done	N
2021/02/10 11:07	CONSOLE_MANAGER	Done	N
2021/02/09 13:07	CONSOLE_MANAGER	Done	N
2021/02/06 03:00	Schedule:WEEKLY	Done	N
2021/02/20 03:00	Schedule:WEEKLY	Done	N
2021/03/27 03:00	Schedule:WEEKLY	Done	N
2021/04/03 03:00	Schedule:WEEKLY	Done	N
2021/01/19 14:07	CONSOLE_MANAGER	Done	N
2021/02/27 03:00	Schedule:WEEKLY	Done	N

1719                    ii. Perform the XML Imports (Figure 2-46) by accessing **Admin > Database Management > XML Imports** following these steps:  
 1720                    1) Import the *Dashboard Add-On XML* file.  
 1721                    2) Import the *Supporting Configuration Add-On XML* file.  
 1722  
 1723

1724 Figure 2-46 ConsoleWorks Importing System Configurations and Components



1725

### 1726 2.8.3 Configuration

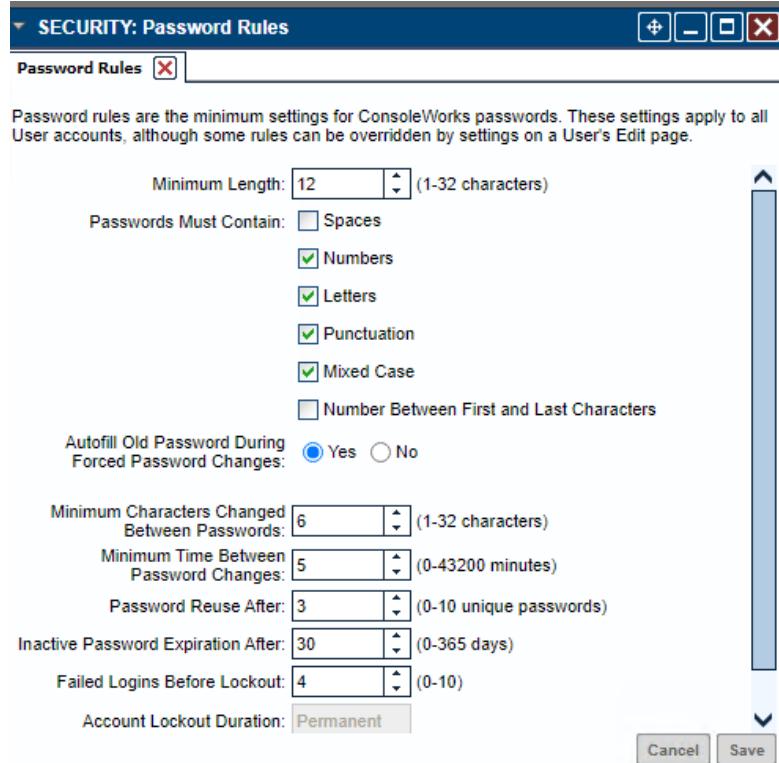
1727 The ConsoleWorks implementation required the following changes to the lab Cisco VPN appliance to  
1728 allow remote users to access the ConsoleWorks system:

- 1729 1. Login to the Cisco Firepower Appliance.
- 1730 2. Create the Following Destination Network Objects:
  - 1731 a. For Build 1:
    - 1732 i. Name: ConsoleWorks
    - 1733 ii. IP Address: 10.100.0.52
  - 1734 b. For Build 3:
    - 1735 i. Name: CRS-NAT-IP
    - 1736 ii. IP Address: 10.100.0.20
- 1737 3. Create the Following VPN-Rule:

- 1738            a. For Build 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 Build 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
- 1748        ConsoleWorks is then configured as follows. For configuration procedures, please see the ConsoleWorks  
 1749        documentation available at <https://support.tditechnologies.com/product-documentation>.

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

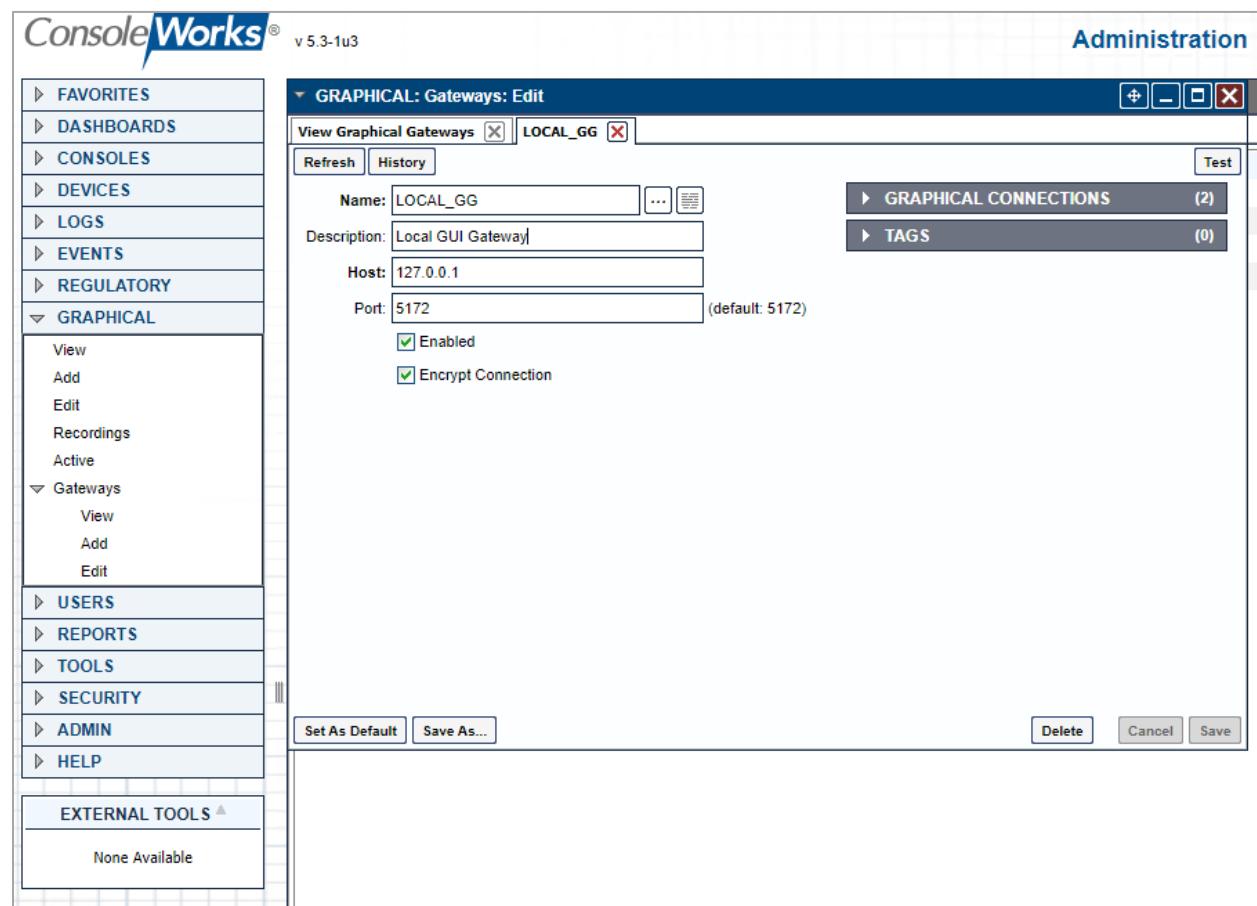
1751 **Figure 2-47 ConsoleWorks Password Settings**



- 1752        2. Add user accounts:
- 1753            a. **NCCOE\_ADMIN**

- 1755                   b. **NCCOE\_USER**
- 1756           3. Configure the Graphical Gateway to allow users to use RDP within ConsoleWorks following  
1757           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

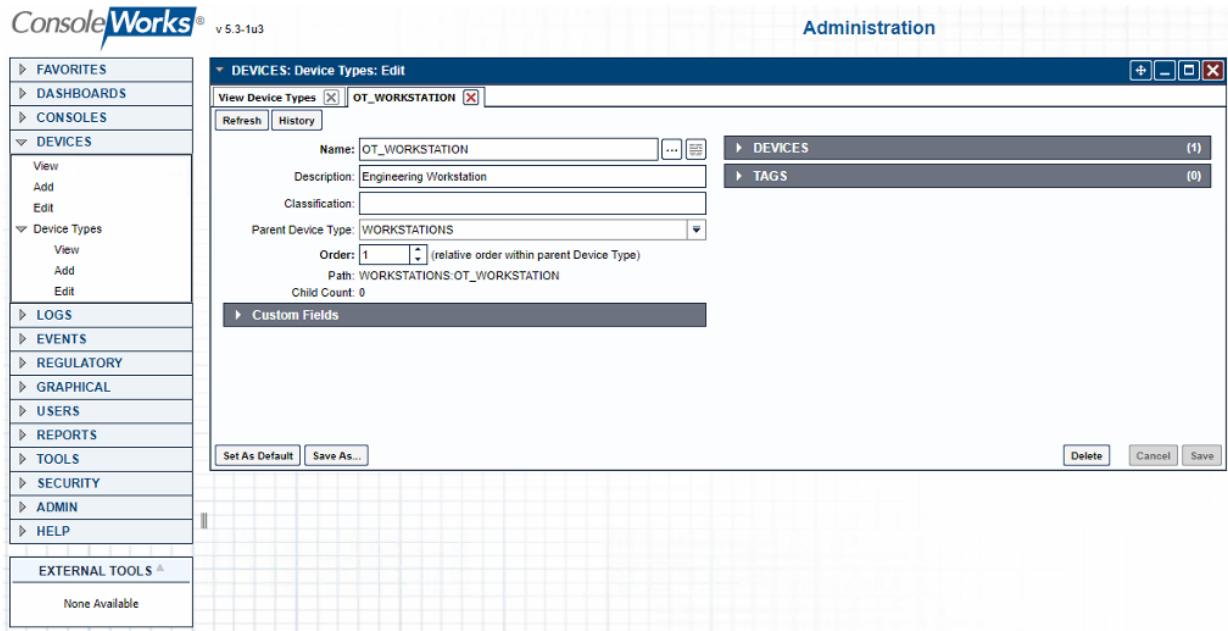


- 1765
- 1766          4. Configure Device Types to organize the registered devices within the system as follows:
- 1767           a. Enter the information for the supported device types as shown in the example device  
1768           type (Figure 2-49) for each type listed in Table 2-18 (and shown in Figure 2-50).

1769 **Table 2-18 ConsoleWorks Device Type List**

Name	Description	Parent Device Type	Order
NETWORKING	Devices supporting networked communications		1
IT_FWROUTER	Network Router/Firewall for supporting IT Communications	NETWORKING	1
IT_SWITCH	Network switch supporting IT communications	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

1770 Figure 2-49 ConsoleWorks Example Device Type Definition



1771

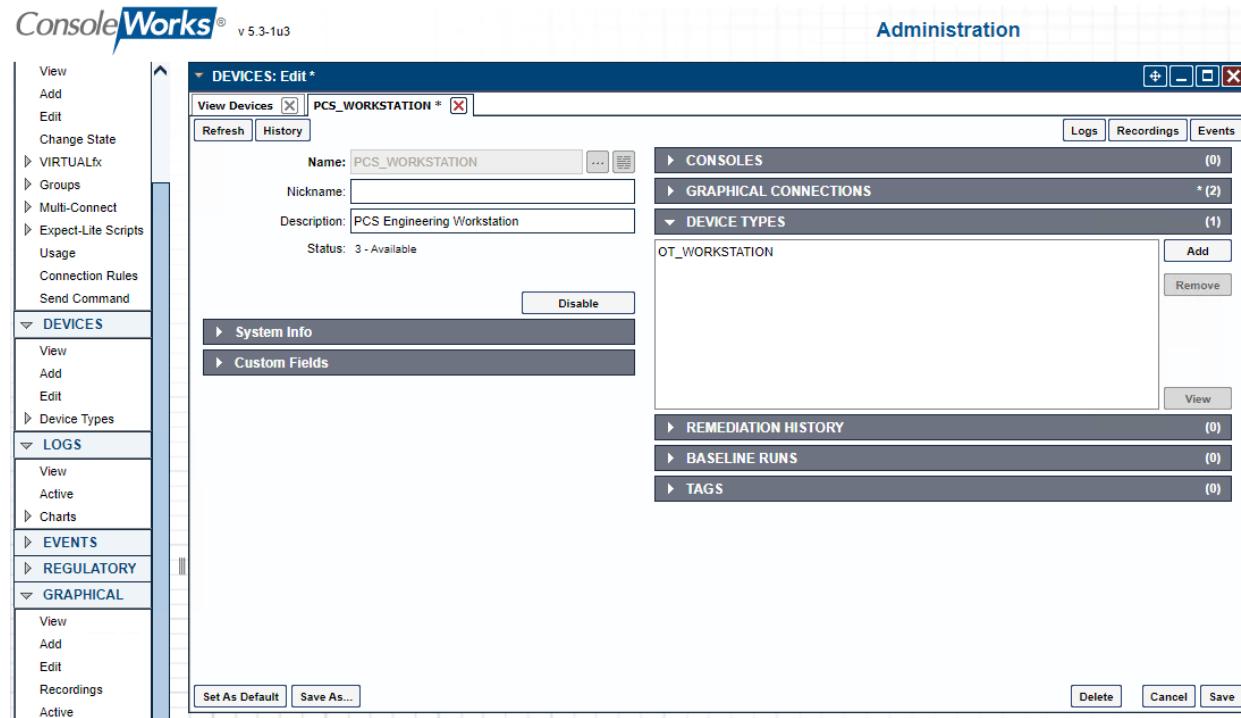
1772 Figure 2-50 ConsoleWorks List of Device Types

Device Type	Path	Description	Classification	Parent	Order
NETWORKING	NETWORKING	Devices for supporting networked communications			1
IT_FWROUTER	NETWORKING.IT_FWROUTER	Network Router/Firewall for supporting IT Communications	NETWORKING		1
IT_SWITCH	NETWORKING.IT_SWITCH	Network Switch supporting IT communications	NETWORKING		1
OT_FWROUTER	NETWORKING.OT_FWROUTER	ICS Firewall/Router for ICS Network Segmentation	NETWORKING		1
OT_SWITCH	NETWORKING.OT_SWITCH	Network Switch for supporting ICS network segment	NETWORKING		1
SERVERS	SERVERS	Devices for providing one or more IT/OT Services			1
IT_SERVER	SERVERS.IT_SERVER	Server providing IT Services	SERVERS		1
OT_SERVER	SERVERS.OT_SERVER	Server providing OT Services	SERVERS		1
WORKSTATIONS	WORKSTATIONS	Computers used by users to support IT/OT Operations			1
HMI	WORKSTATIONS.HMI	Specialized workstation supporting Human Machine Interface	WORKSTATIONS		1
IT_WORKSTATION	WORKSTATIONS.IT_WORKSTATION	Computer used by user for supporting IT operations	WORKSTATIONS		1
OT_WORKSTATION	WORKSTATIONS.OT_WORKSTATION	Engineering Workstation	WORKSTATIONS		1

1773

1774 5. Configure Devices for each system within the testbed that is accessible from ConsoleWorks.

1775 Figure 2-51 ConsoleWorks Example Device Definition



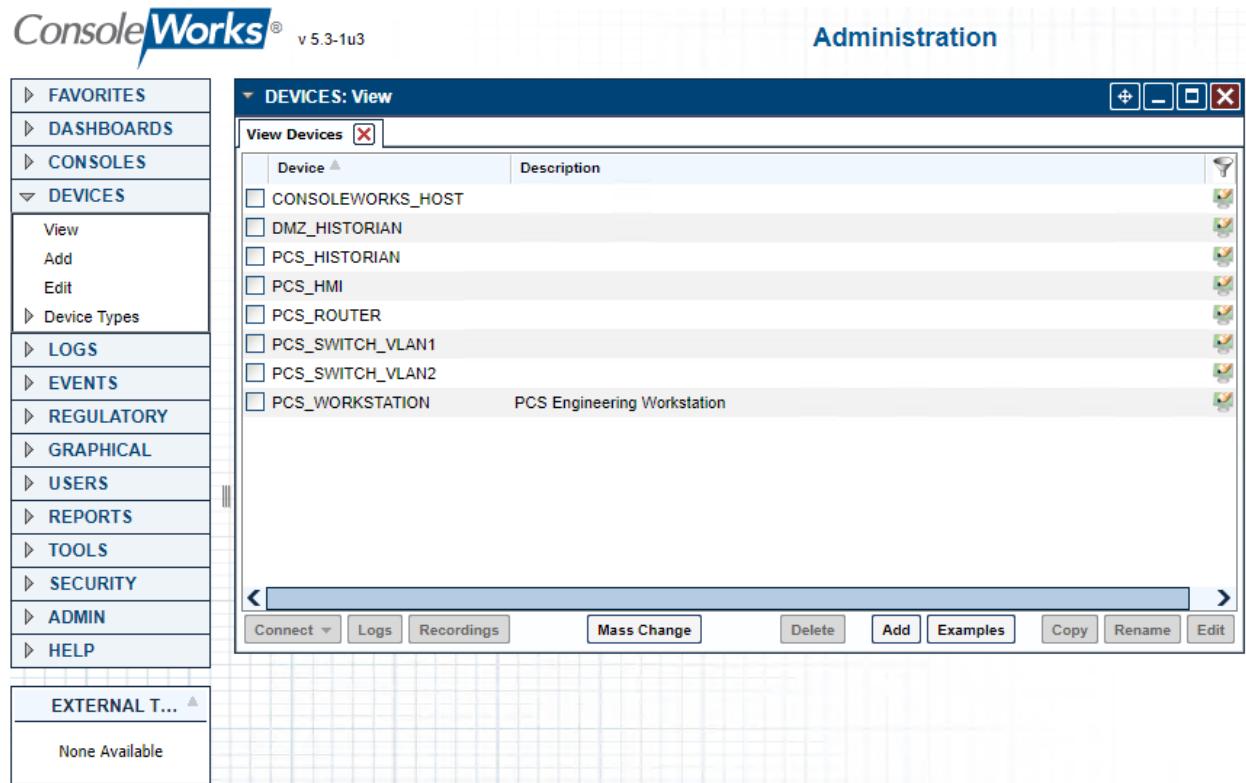
1776

- 1777        a. For Build 1 (PCS), enter the information for the devices as shown in the example device  
 1778              (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



1781

- 1782 b. For Build 3 (CRS) , enter the information for the devices as shown in the example device  
1783 (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	HMI
CRS_ROUTER	CRS Boundary Firewall/Router	OT_FWROUTER
CRS_SWITCH_CONTROL	OT Switch for Control Network	OT_SWITCH
CRS_SWITCH_FIELD	OT Switch for Field Network	OT_SWITCH
CRS_WORKSTATION	CRS Engineering Workstation	OT_WORKSTATIONS
CRS_STATION1	Machining Station #1	OT_WORKSTATIONS
CRS_STATION2	Machining Station #2	OT_WORKSTATIONS
CRS_STATION3	Machining Station #3	OT_WORKSTATIONS
CRS_STATION4	Machining Station #4	OT_WORKSTATIONS

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

**DEVICES: View**

Device	Description
CONSOLEWORKS_HOST	Local CRS Historian Server
CRS_HISTORIAN	Process Monitor
CRS_HMI	CRS Router Firewall
CRS_ROUTER	Machining Station #1
CRS_STATION1	Machining Station #2
CRS_STATION2	Machining Station #3
CRS_STATION3	Machining Station #4
CRS_STATION4	Control LAN Switch
CRS_SWITCH_CONTROL	Field Device LAN Switch
CRS_SWITCH_FIELD	CRS Engineering Workstation
CRS_WORKSTATION	External Historian Replication Server
DMZ_HISTORIAN	

View Devices

Device

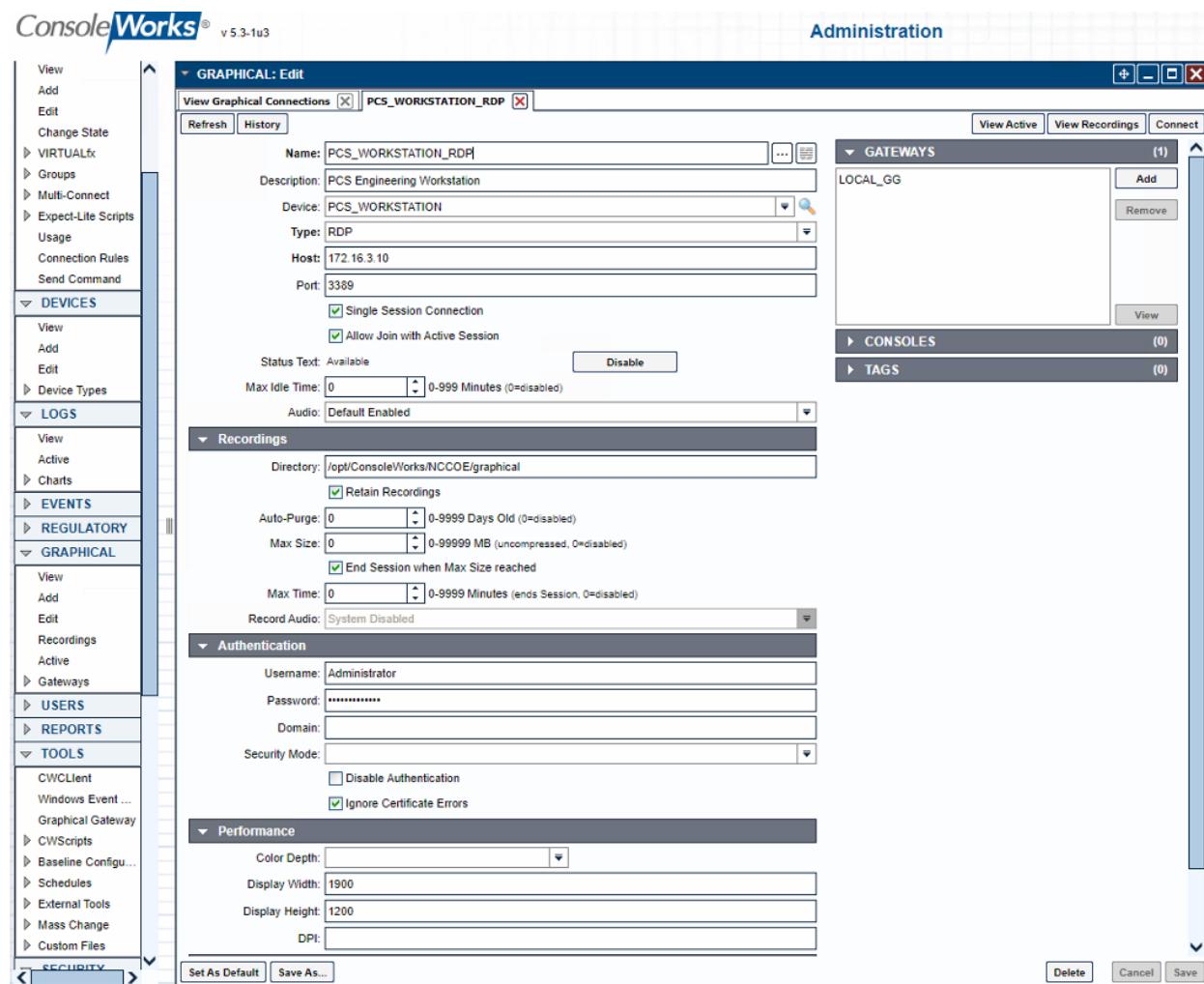
Connect

EXTERNAL T...

Administration

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

1787 Figure 2-54 ConsoleWorks Example RDP Configuration



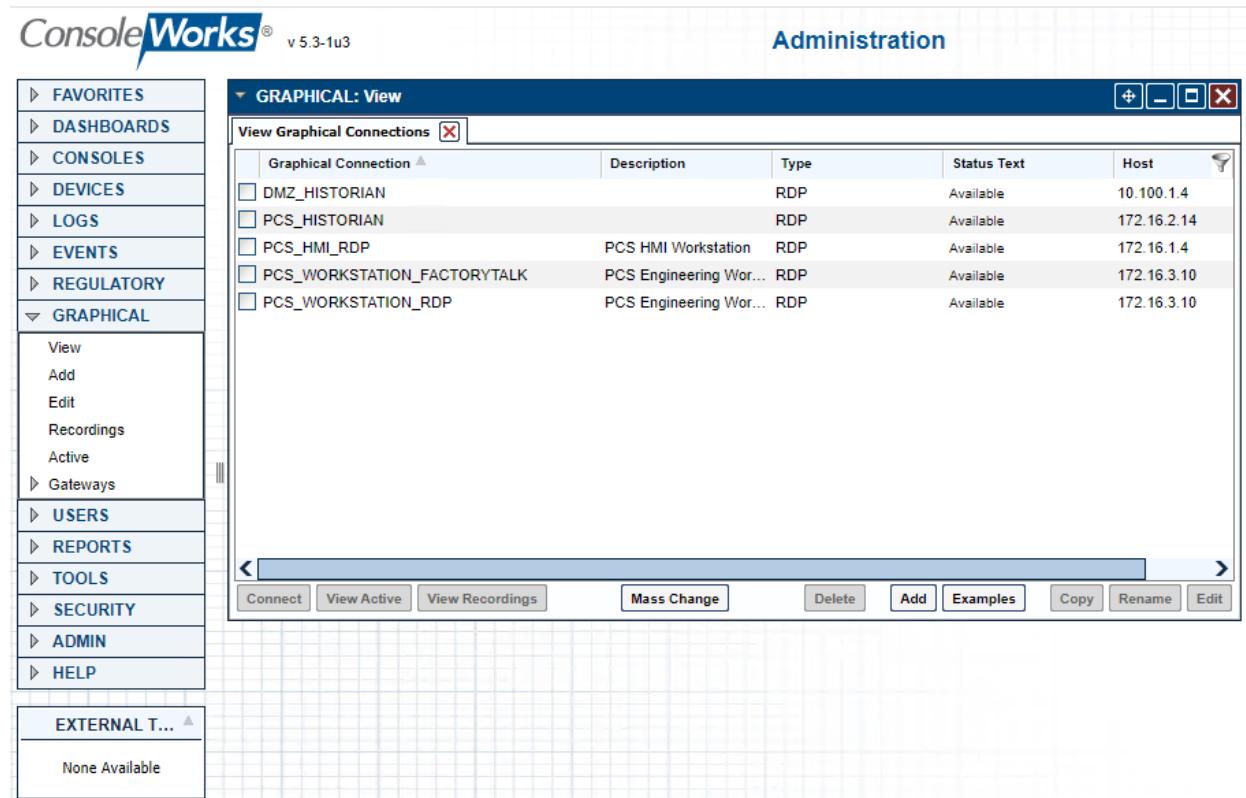
- 1788 a. For Build 1 (PCS), enter the information for the Graphical Connections as shown in the  
 1789 example (Figure 2-54) for each graphical connection listed in Table 2-21 (also shown in  
 1790 Figure 2-55). For each entry, the following are common settings for all graphical connec-  
 1791 tions:
- 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                          1) Specify local or domain credentials, which are securely stored by  
1804                          ConsoleWorks, to allow complex passwords/credentials without having to  
1805                          share between users.
- 1806                          2) Ignore Certificate Errors: Checked only if self-signed certificates are in use.
- 1807                          vi. Performance
- 1808                          1) Display Width: **1900**
- 1809                          2) Display Height: **1200**

1810 **Table 2-21 ConsoleWorks PCS (Build 1) Graphical Connections**

Name	Device	Type	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

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



- 1812 b. For Build 3 (CRS), enter the information for the graphical connections as shown in the example (Figure 2-54) for each graphical connection listed in Table 2-22 (also shown in Figure 2-56). For each entry, the following are common settings for all graphical connections.
- 1813 i. Under Gateway, click **Add** and select **LOCAL\_GG**.
- 1814 ii. Under Recordings, use these settings:
- 1815     1) Directory **/opt/ConsoleWorks/NCCOE/graphical**
- 1816     2) Retain Records **Checked**
- 1817     3) Auto-Purge: **0**
- 1818     4) Max Size: **0**
- 1819     5) End Session when Max Size Reached: **Checked**
- 1820     6) Max Time: **0**
- 1821 iii. Authentication:
- 1822     1) 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	Type	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

1832

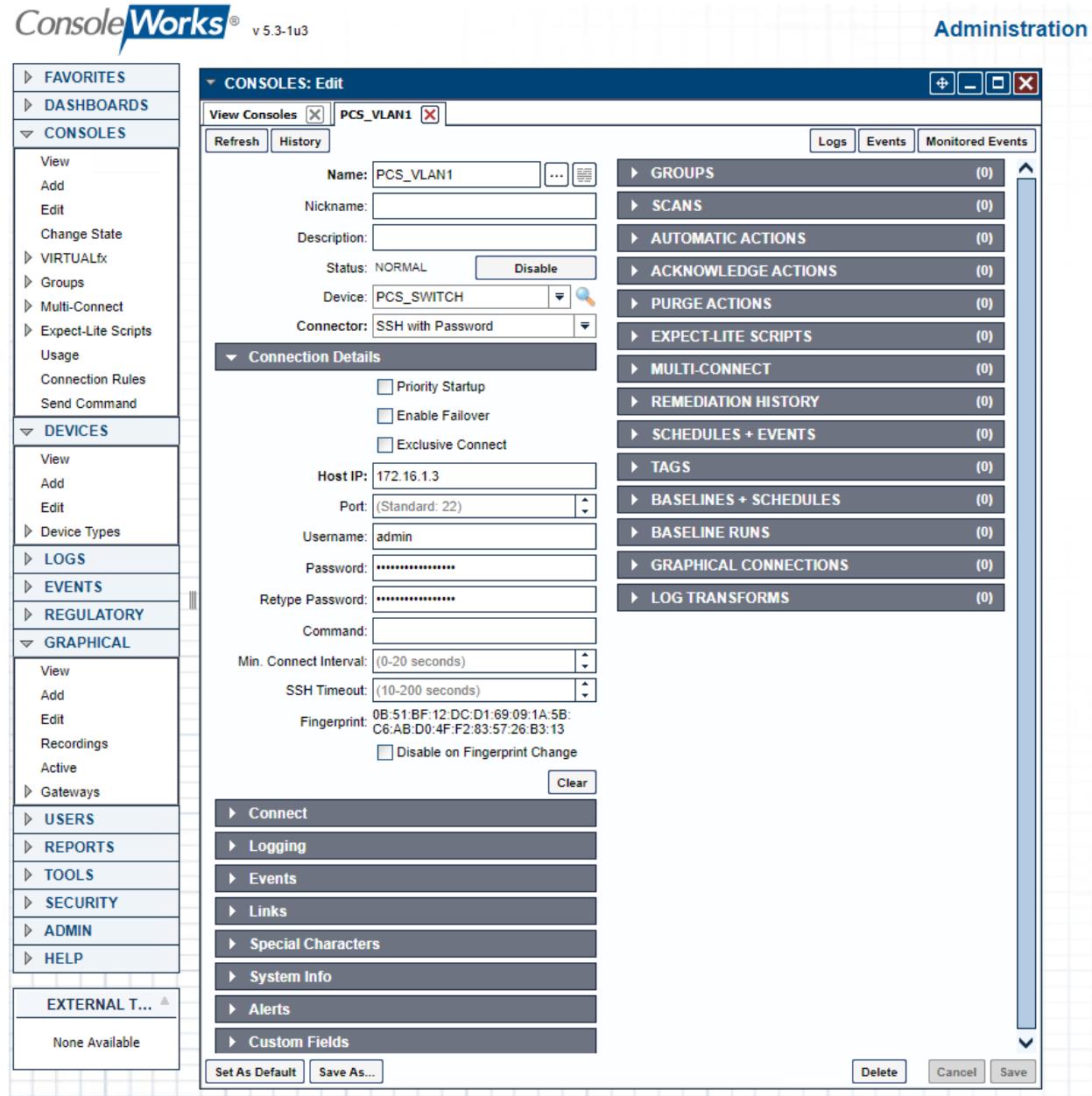
1833 **Figure 2-56 ConsoleWorks List of CRS (Build 3) RDP Connections**

Graphical Connection	Description	Type	Status Text	Host
CRS_HISTORIAN		RDP	Available	192.168.0.21
CRS_WORKSTATION		RDP	Available	192.168.0.20
DMZ_HISTORIAN		RDP	Available	10.100.1.4

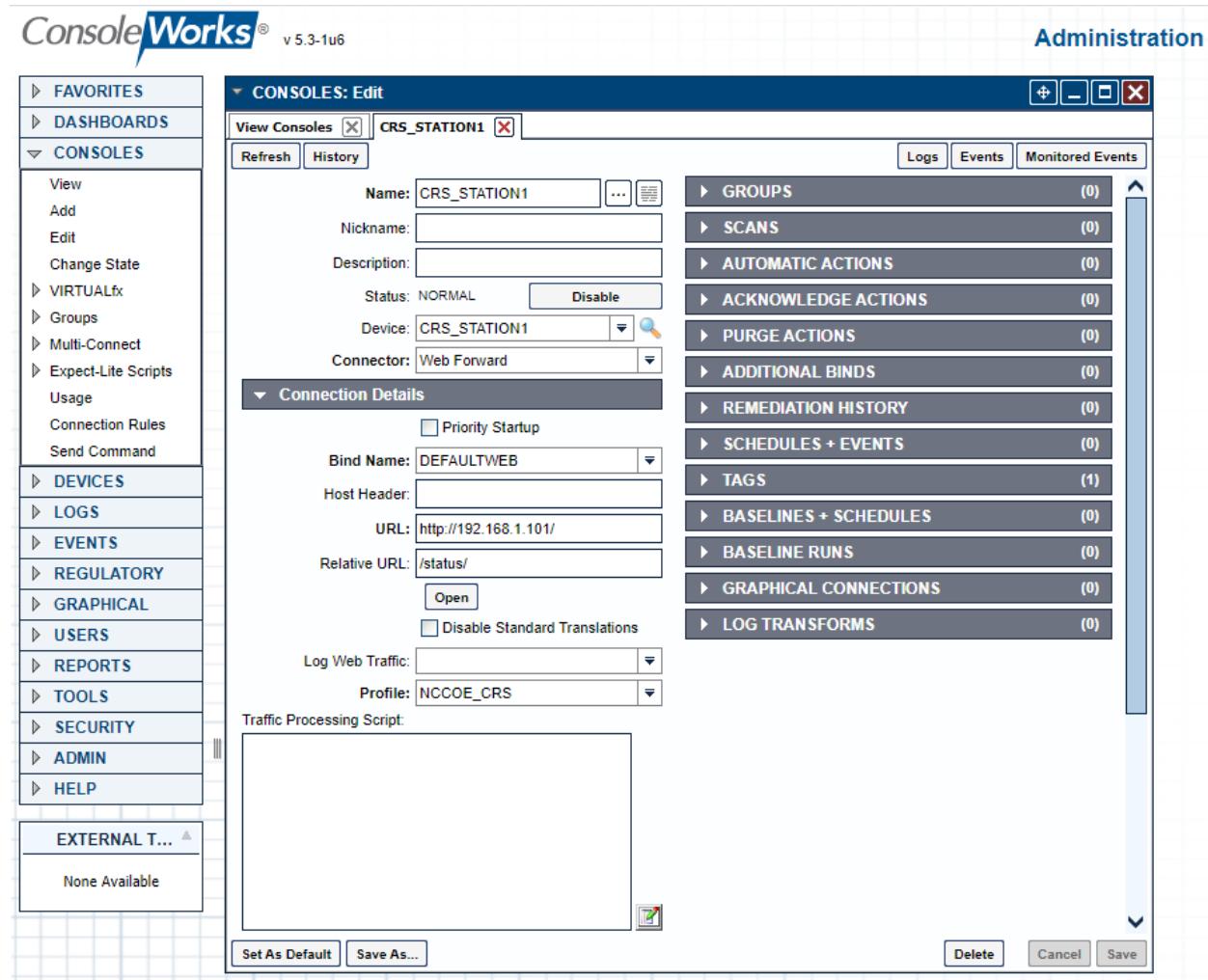
1834

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



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



1838

1839       a. For Build 1 (PCS), enter the information for the Console Connections as shown in the examples (Figure 2-57 and Figure 2-58) for each console connection listed in Table 2-23 (also shown in Figure 2-59). For each entry, the following are common settings for all console connections.

1843           i. Under **Connection Details**:

1844              1) Specify the username and password, which are securely stored by Console-  
1845                Works, to allow complex passwords/credentials without having to share  
1846                between users.

1847 Table 2-23 ConsoleWorks PCS (Build 1) Console Connections

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

1848

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

Console	Description	Connector	Status
CONSOLEWORKS_SSH		SSH with Password(SSHPWD)	NORMAL
CONWRKS	ConsoleWorks	Internal Console - No Conne...	NORMAL
CONWRKS_OUT		File Monitor(FILEMON)	NORMAL
PCS_ROUTER		SSH with Password(SSHPWD)	Restored Communication
PCS_VLAN1		SSH with Password(SSHPWD)	Restored Communication
PCS_VLAN2		SSH with Password(SSHPWD)	Restored Communication

1850

- 1851 b. For Build 3 (CRS), enter the information for the console connections as shown in the ex-  
 1852 ample (Figure 2-57 and Figure 2-58) for each console connection listed in Table 2-24  
 1853 (Figure 2-60). For each entry, the following are common settings for all console connec-  
 1854 tions.

1855 i. Under **Connection Details**

- 1856 1) Specify the username and password, which are securely stored by Console-  
 1857 Works, to allow complex passwords/credentials without having to share  
 1858 between users.

1859 Table 2-24 ConsoleWorks CRS (Build 3) Console Connections

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

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

1860

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

The screenshot shows the 'ConsoleWorks' application interface. The title bar reads 'ConsoleWorks® v 5.3-1u6'. The main window is titled 'CONSOLES: View' and contains a table of connected devices. The table columns are 'Console', 'Description', 'Connector', and 'Status'. The status column includes icons for signal strength and battery level. Below the table are buttons for 'Connection', 'Logs', 'Mass Change', 'Delete', 'Add', 'Examples', 'Copy', 'Rename', and 'Edit'.

Console	Description	Connector	Status
CONSOLEWORKS_SSH	ConsoleWorks	SSH with Password(SSHPWD)	Waiting for User input
CONWRKS	ConsoleWorks	Internal Console - No Conn...	NORMAL
CONWRKS_OUT		File Monitor(FILEMON)	NORMAL
CRS_CONTROL_LAN	Netgear	Web Forward(WEBFORWARD)	NORMAL
CRS_FIELD_LAN	i800 Switch	SSH with Password(SSHPWD)	Restored Communication
CRS_ROUTER	RuggedCom	SSH with Password(SSHPWD)	Restored Communication
CRS_STATION1		Web Forward(WEBFORWARD)	NORMAL
CRS_STATION2		Web Forward(WEBFORWARD)	NORMAL
CRS_STATION3		Web Forward(WEBFORWARD)	NORMAL
CRS_STATION4		Web Forward(WEBFORWARD)	NORMAL
HMI		Web Forward(WEBFORWARD)	NORMAL

Navigation links on the left include: FAVORITES, DASHBOARDS, CONSOLES (View, Add, Edit, Change State), VIRTUALfx, Groups, Multi-Connect, Expect-Lite Scripts, Usage, Connection Rules, Send Command, DEVICES, LOGS, EVENTS, REGULATORY, GRAPHICAL, USERS, REPORTS, TOOLS, SECURITY, ADMIN, and HELP. The EXTERNAL T... section at the bottom says 'None Available'.

1862

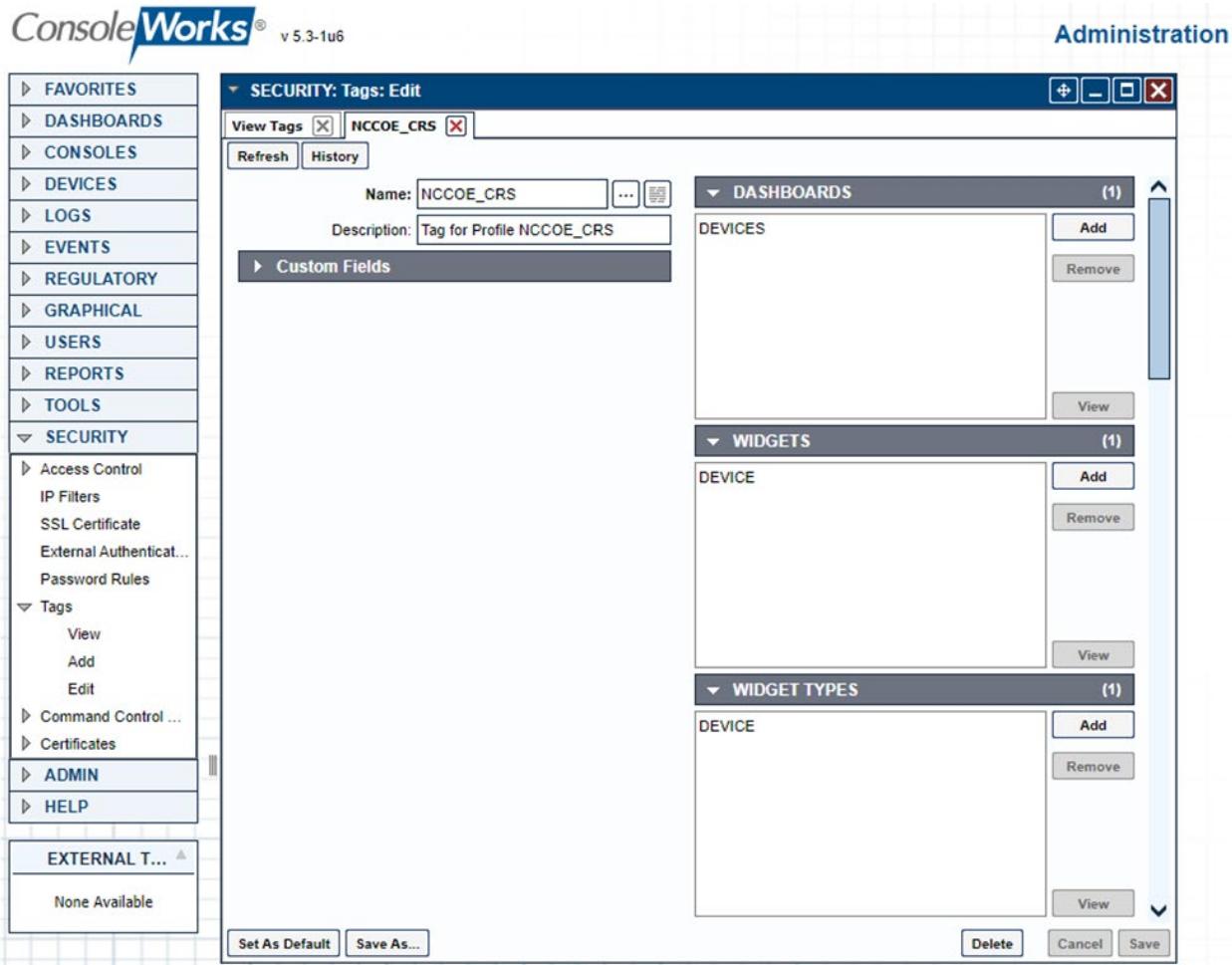
1863 8. Configure tags to support profiles and access controls.

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

The screenshot shows the ConsoleWorks Administration interface with the title "Administration" at the top right. On the left is a vertical navigation menu with sections like FAVORITES, DASHBOARDS, CONSOLES, DEVICES, LOGS, EVENTS, REGULATORY, GRAPHICAL, USERS, REPORTS, TOOLS, and SECURITY. Under SECURITY, there are sub-options for Access Control, IP Filters, SSL Certificate, External Authenti..., Password Rules, Tags (with sub-options for View, Add, Edit), Command Contr..., Certificates, ADMIN, and HELP. The main window is titled "SECURITY: Tags: View" and contains a table with two columns: "Tag" and "Description". The table lists various tags with their descriptions, such as ADMIN\_ARCH\_ACCESS (Admin ARCHITECT access), ADMIN\_CONTROL\_ACCESS (Admin CONTROL access), and TEST (Tag for Profile TEST). At the bottom of the table are buttons for Mass Change, Delete, Add, Examples, Copy, Rename, and Edit.

Tag	Description
ADMIN_ARCH_ACCESS	Admin ARCHITECT access
ADMIN_CONTROL_ACCESS	Admin CONTROL access
ADMIN_CREATE_ACCESS	Admin CREATE access
ADMIN MODIFY_ACCESS	Admin MODIFY access
ADMIN_VIEW_ACCESS	Admin VIEW access
CONSOLE_ACK_ACCESS	Console ACK access
CONSOLE_CONTROL_ACCESS	Console CONTROL access
CONSOLE MODIFY_ACCESS	Console MODIFY access
CONSOLE_VIEW_ACCESS	Console VIEW access
PCS_ADMIN	Tag to identify PCS elements for Admin Use
PCS_GENERAL	Tag to identify standard PCS elements
TBA_BASELINE_RUN	Run Baselines
TBA_BASELINE_RUNVIEW	View Baselines
TBA_DASHBOARD_VIEW	View Dashboards
TBA_DEVICE_CONNECT	Device Connect
TBA_DEVICE_LOGVIEW	View Device Logs
TBA_EVENT_ACKNOWLEDGE	Event acknowledge
TBA_EVENT_AWARE	Event awareness
TBA_REPORT_OUTPUT_VIEW	View Report Outputs
TBA_REPORT_RUN	Run Reports
TBA_SUBSET	Profile uses a subset of components
TEST	Tag for Profile TEST

1865 Figure 2-62 ConsoleWorks Example Tag Definition Screen



1866

1867 a. For Build 1 (PCS) the following tags were created as shown in Figure 2-61. Figure 2-62 shows an  
1868 example of a single tag.

1869 i. Name: **PCS\_GENERAL**

1870 1) Under **Dashboards**, click **Add** and select **Devices**.

1871 2) Under **Custom UI Classes** click **Add** and select:

1872 a) **DEVICE\_LISTGRID**

1873 b) **LISTGRID**

1874 3) Under **Devices**, click **Add** and select:

1875 a) **DMZ\_HISTORIAN**

1876 b) **PCS\_HISTORIAN**

1877 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:

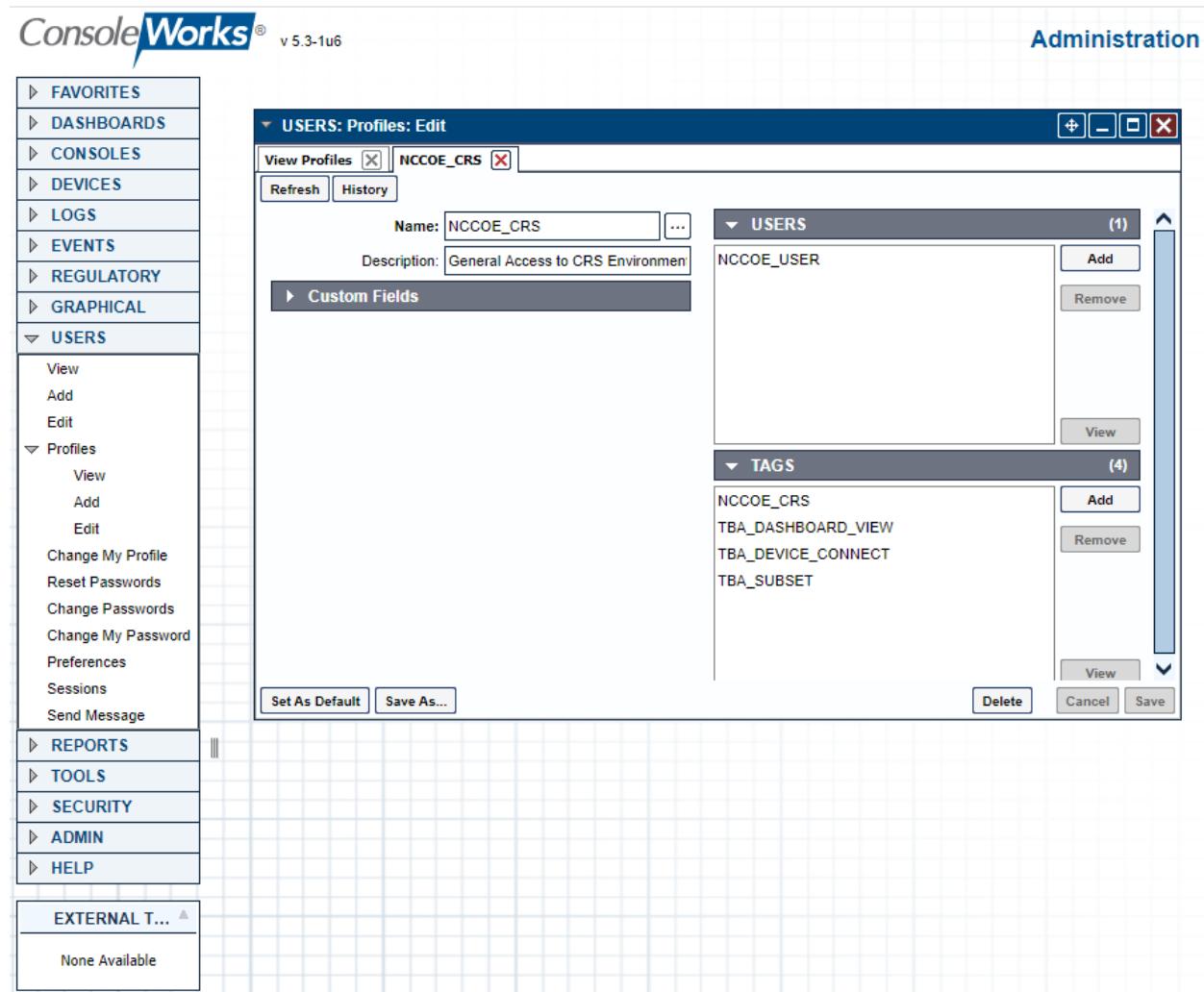
1904 a) CRS\_STATION1

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 9. Configure profiles to provide user accounts with granular access controls to available resources  
1932 (Figure 2-63).

1933 Figure 2-63 ConsoleWorks Example Profile



1934

1935 a. For Build 1 (PCS) the following profiles were created:

1936 i. **PCS\_GENERAL**

1937 1) Under Users click Add and select

1938 a) NCCOE\_USER

1939 2) Under Tags click Add and select

1940 a) PCS\_GENERAL

1941 b) TBA\_DASHBOARD\_VIEW

1942 c) TBA\_DEVICE\_CONNECT

1943 d) TBA\_SUBSET

1944 ii. **PCS\_ADMIN**

- 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

1974 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**

1985 The Tenable.OT (Version 3.8.17) appliance is installed in a rack with network connections for the  
 1986 Management/Query traffic on Port 1 and SPAN traffic on Port 2 of the appliance. Documentation for  
 1987 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

1994         a. Add the following rules (Table 2-26) to the PCS Firewall to allow Tenable.OT to perform  
 1995 asset discovery and controller scanning.

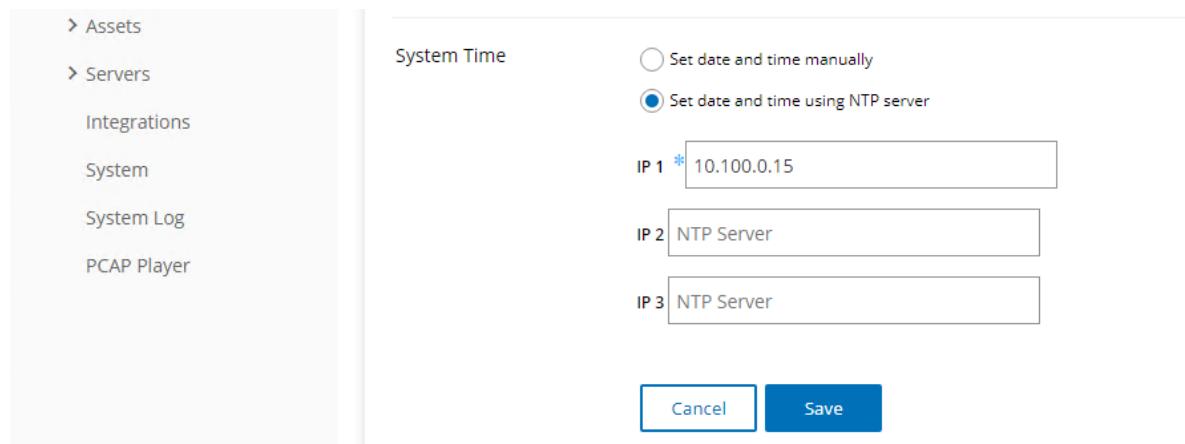
1996 **Table 2-26 Firewall Rules for Tenable.OT**

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:

- 1998            a. After logging into the appliance, navigate to **Local Settings > Device**.
- 1999            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**



- 2003
- 2004            3. Configure Scanning Options as follows:
- 2005            a. Set Asset Discovery Scans:
- 2006            i. Navigate to **Local Settings > Queries > Asset Discovery** (Figure 2-65)
- 2007            ii. Enable both scan options.
- 2008            iii. Select **Edit** next to Asset Discovery.
- 2009            1) Enter the following 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 properties as follows:
- 2014            a) Number of Assets to Poll Simultaneously: **10**
- 2015            b) Time Between Discovery Queries: **1 second**
- 2016            c) Frequency: **Daily**
- 2017            d) Repeats Every: **7 Days**
- 2018            e) Repeats at: **9:00 PM**
- 2019            3) Click **Save**.

2020 Figure 2-65 Tenable.OT Asset Discovery Settings

The screenshot shows the Tenable.OT web interface. The left sidebar includes links for Events, Policies, Inventory (with sub-links for Controllers and Network Assets), Risk, Network, Groups, Reports, Local Settings (with sub-links for Device, User, Asset Custom Fields, API Keys, and HTTPS), User Management, Queries (with sub-links for Asset Discovery, Controller, Network, Assets, Servers, and Integrations), and a bottom section for Initial Asset Enrichment. The main content area is titled "Asset Discovery" and contains a "IP ranges:" field with three entries: "172.16.0.0/22", "10.100.0.0/24", and "10.100.1.0/24". Below this are fields for "Number of Assets to Poll Simultaneously:" (set to 10), "Time Between Discovery Queries:" (set to 1 second), "Frequency:" (set to Daily), "Repeats Every" (set to 7 days), and "Repeats At" (set to 9:00 PM). A "Save" button is at the bottom right. A note below the IP ranges states: "Will run SNMP, Minimal Open Port Verification, CIP/DCP, NetBIOS, Backplane Query, Unicast Identification, Controller Details, Controller State." The top right corner shows the time as 02:42 PM on Thursday.

2021

2022 b. Set Controller Scans as follows:

2023 i. Navigate to Local Settings &gt; Queries &gt; Controller (Figure 2-66)

2024 ii. Enable the following options:

2025 1) All Controller Queries

2026 2) Periodic Snapshots

2027 3) Controller Discovery

2028 4) Controller Status Query

2029 5) Controller Details Query

2030 6) Backplane Query

2031 **Figure 2-66 Tenable.OT Controller Scans**

Query Type	Frequency	Action
All Controller Queries	Every 4 days at 9:00 PM	<a href="#">Edit</a> <a href="#">Run now</a>
Periodic Snapshots	Every 4 days at 9:00 PM	<a href="#">Edit</a> <a href="#">Run now</a>
Policy Triggered Snapshots		
Controllers Discovery	Every 1 hour	<a href="#">Edit</a> <a href="#">Run now</a>
Controller State Query	Every 15 Minutes	<a href="#">Edit</a> <a href="#">Run now</a>
Diagnostic Buffer Query	Every 4 days at 9:00 PM	<a href="#">Edit</a> <a href="#">Run now</a>
Controller Details Query	Every 1 hour	<a href="#">Edit</a> <a href="#">Run now</a>
Backplane Query	Every 1 hour	<a href="#">Edit</a> <a href="#">Run now</a>

2032

- 2033 c. Set Network Scans as follows:
- 2034 i. Navigate to Local Settings > Queries > Network (Figure 2-67)
- 2035 ii. Enable the following options:
- 2036     1) All Network Queries
- 2037     2) DNS Query
- 2038     3) ARP Query
- 2039     4) NetBIOS Query

2040 **Figure 2-67 Tenable.OT Network Scan Settings**

The screenshot shows the Tenable.OT interface with the 'Network' tab selected in the sidebar. The main area displays a list of network queries:

- All Network Queries**: Enabled.
- Port Mapping**: Disabled. Details: Mapping Range: Periodic mapping rate: 1 ports mapped per second; On-demand mapping rate: 1 ports mapped per second. Actions: Edit, Run now.
- SNMP Query**: Enabled. Details: Frequency: Every 1 hour; SNMP V2 Community Strings: public, private; SNMP V3 Usernames: --. Actions: Edit, Run now.
- DNS Query**: Enabled.
- ARP Query**: Enabled.
- NetBIOS**: Enabled. Details: Frequency: Every 1 hour. Actions: Edit, Run now.
- Active Asset Tracking**: Enabled. Details: Frequency: Every 5 minutes. Actions: Edit.
- WMI Query**: Enabled. Details: WMI Username:; WMI Frequency: Every 1 day at 12:00 PM. Actions: Edit, Run now.
- USB Connections Query**: Enabled. Details: USB Frequency: Every 1 day at 12:00 PM. Actions: Edit, Run now.
- Ripple20 Vulnerabilities Scan**: Enabled. Actions: Edit, Run now.

Version 3.8.17 | Expires: Dec 9, 2021

2041

2042 4. Create Group Object as follows:

2043 a. Set DMZ Group Object

2044 i. Navigate to Groups &gt; Asset Groups

2045 ii. Click Create Asset Group to initiate the Wizard process.

2046 1) Select **IP Range** for the Asset Group Type (Figure 2-68) and Click **Next**.2047 2) Enter the asset name in Name, the starting IP address in Start IP, and the  
2048 ending IP Address in End IP (Figure 2-69) and Click **Create**.2049 **Figure 2-68 Tenable.OT Create Asset Group Type**

The screenshot shows the 'Create Asset Group' wizard with the title 'Create Asset Group'. A progress bar at the top indicates 'Group Type' is selected. Below the progress bar are three options:

- Asset Selection** (highlighted in red)
- IP Range**
- IP List**

At the bottom are 'Cancel' and 'Next >' buttons.

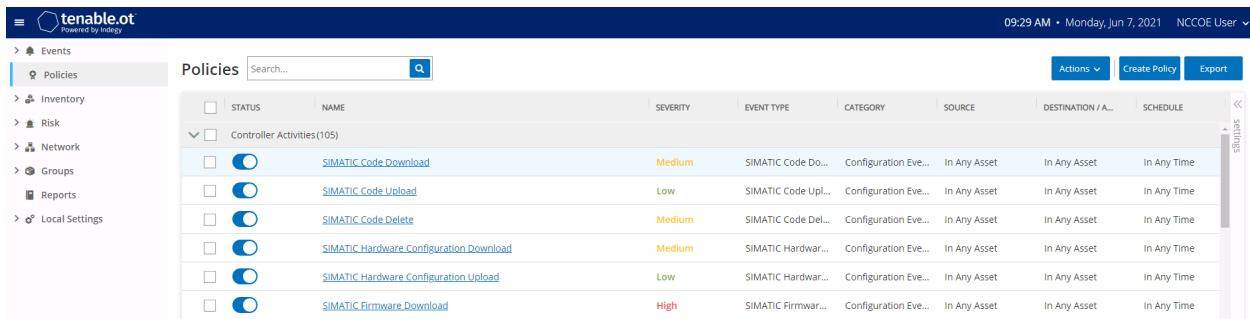
2050 Figure 2-69 Tenable.OT Create Asset Group Definition

The screenshot shows a 'Create Asset Group' dialog box. At the top, there are two tabs: 'Group Type' (selected) and 'Group Definition'. Below the tabs, there are three input fields: 'NAME \*' (containing 'DMZ Zone'), 'START IP \*' (containing '10.100.1.0'), and 'END IP \*' (containing '10.100.1.254'). At the bottom of the dialog box are three buttons: '< Back', 'Cancel', and 'Create'.

2051

- 2052 5. Create Policy to Detect External RDP Traffic:
- 2053 a. In the left side navigation, click **Policies**.
- 2054 b. Click **Create Policy** in the upper right corner of the page (Figure 2-70), then follow these  
2055 steps:
- 2056 i. For the Event Type (Figure 2-71), select as a **Network Events > RDP Connection**  
2057 **(Authenticated)** and click **Next**.
- 2058 ii. For the Policy Definition (Figure 2-72), specify the following parameters and click  
2059 **Next**:
- 2060     1) Policy Name: Enter "External RDP Communications"
- 2061     2) Source Group: Select "In" from the first drop-down, and "DMZ" from the  
2062       second drop-down.
- 2063     3) Destination Group: Select "In" from the first drop-down and select "In Any  
2064       Asset" from the second drop-down.
- 2065     4) Schedule Group: Select "In" from the first drop-down, and "In Any Time"  
2066       from the second drop-down.
- 2067 iii. For the Policy Action (Figure 2-73), select **Medium** Sensitivity and click **Create**.

2068 Figure 2-70 Tenable.OT Policy Settings

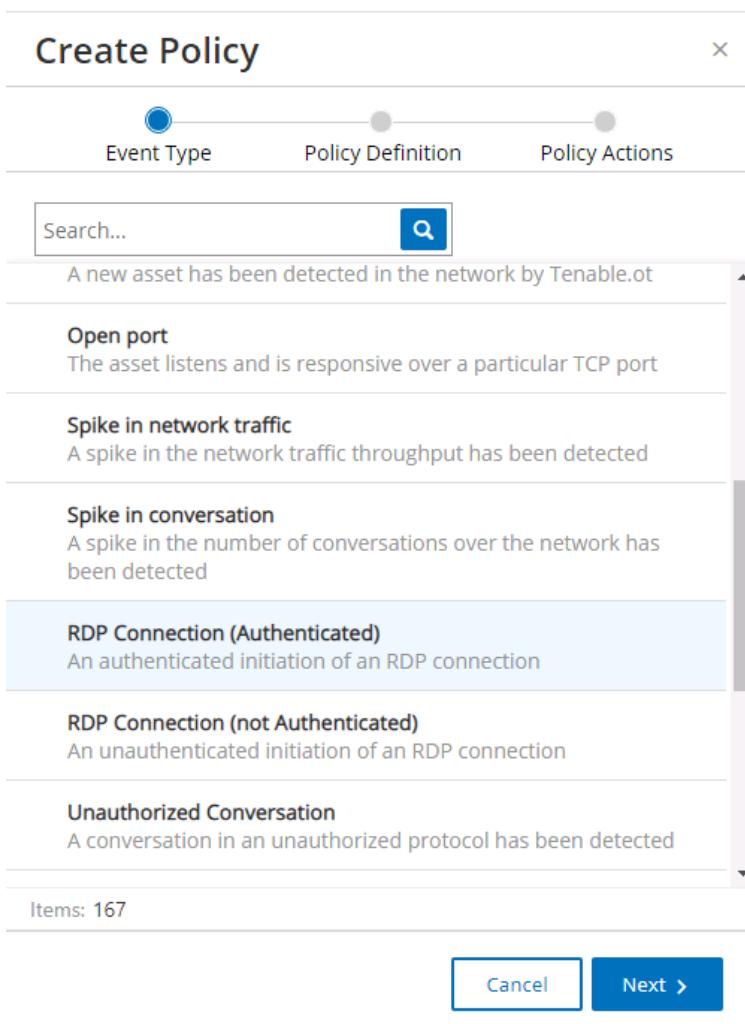


The screenshot shows the Tenable.OT web interface under the 'Policies' tab. The left sidebar includes links for Events, Policies (selected), Inventory, Risk, Network, Groups, Reports, and Local Settings. The main content area displays a table titled 'Controller Activities (105)' with columns for STATUS, NAME, SEVERITY, EVENT TYPE, CATEGORY, SOURCE, DESTINATION / A..., and SCHEDULE. Six policies are listed:

NAME	SEVERITY	EVENT TYPE	CATEGORY	SOURCE	DESTINATION / A...	SCHEDULE
SIMATIC Code Download	Medium	SIMATIC Code Do...	Configuration Eve...	In Any Asset	In Any Asset	In Any Time
SIMATIC Code Upload	Low	SIMATIC Code Up...	Configuration Eve...	In Any Asset	In Any Asset	In Any Time
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 Asset	In Any Asset	In Any Time

2069

2070 Figure 2-71 Tenable.OT Create Policy – Event Type Options



The screenshot shows the 'Create Policy' dialog with three tabs: Event Type (selected), Policy Definition, and Policy Actions. Below the tabs is a search bar with a magnifying glass icon.

**Event Type**

A new asset has been detected in the network by Tenable.ot

- Open port**  
The asset listens and is responsive over a particular TCP port
- Spike in network traffic**  
A spike in the network traffic throughput has been detected
- Spike in conversation**  
A spike in the number of conversations over the network has been detected
- RDP Connection (Authenticated)**  
An authenticated initiation of an RDP connection
- RDP Connection (not Authenticated)**  
An unauthenticated initiation of an RDP connection
- Unauthorized Conversation**  
A conversation in an unauthorized protocol has been detected

Items: 167

Cancel Next >

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

**Create Policy**

Event Type      Policy Definition      Policy Actions

POLICY NAME \*

SOURCE GROUP \*

In      DMZ      + Or      + And

DESTINATION \*

In      Any Asset      + Or      + And

SCHEDULE GROUP \*

In      Any Time

< Back      Cancel      Next >

This screenshot shows the 'Create Policy' interface in Tenable.OT. The top navigation bar has three tabs: 'Event Type' (selected), 'Policy Definition' (highlighted in blue), and 'Policy Actions'. The main area is titled 'Create Policy'. It contains four sections: 'POLICY NAME \*' with the value 'External RDP Communications'; 'SOURCE GROUP \*' with 'In' selected and 'DMZ' as the source; 'DESTINATION \*' with 'Any Asset' selected; and 'SCHEDULE GROUP \*' with 'Any Time' selected. At the bottom are buttons for '< Back', 'Cancel', and 'Next >'.

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

**Create Policy**

Event Type    Policy Definition    Policy Actions

RDP Connection (Authenticated)

SEVERITY \*

High    Medium    Low    None

SYSLOG

Syslog servers are not configured

EMAIL GROUP

SMTP servers are not configured

ADDITIONAL ACTIONS

Disable after first hit

< Back    Cancel    Create

2073 **2.10 VMware Carbon Black App Control**

2074 VMware Carbon Black App Control is an endpoint protection tool that provides multiple file integrity  
 2075 and application features, including application allow/deny listing and file modification or deletion  
 2076 protection. Carbon Black was used for Builds 1 and 4 as the application allowlisting (AAL) and file  
 2077 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 Engineering Workstation	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 Engineering Workstation	Dell Precision T5610	Windows 10	8	16GB	465GB	CRS Supervisory 192.168.0.20
CRS OSIsoft Pi Server	Hyper-V VM	Windows Server 2016 Standard	4	16GB	80GB/171GB	CRS Supervisory 192.168.0.21

2084 **2.10.2 Installation**

2085 Prepare the Carbon Black App Control Server (fka CB\_Protection) in accordance with the CB Protection  
 2086 Operating Environment Requirements v8.1.6 document that is provided for installation. This document,  
 2087 and all Carbon Black documentation, can be found on the website <https://community.carbonblack.com>.

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

- 2089        a. Created nccoeCarbon domain user account on LAN AD to be used for installation and  
2090              administration of CB App Control Server and add this user to the local administrators'  
2091              group on the server.
- 2092        b. Install SQL Server Express 2017 according to the CB Protection SQL Server Configuration  
2093              v8.1.4 document.
- 2094        c. Install the CB App Control Server according to the CB Protection Server Install Guide  
2095              v8.1.6 document.

### 2096     [2.10.3 Configuration](#)

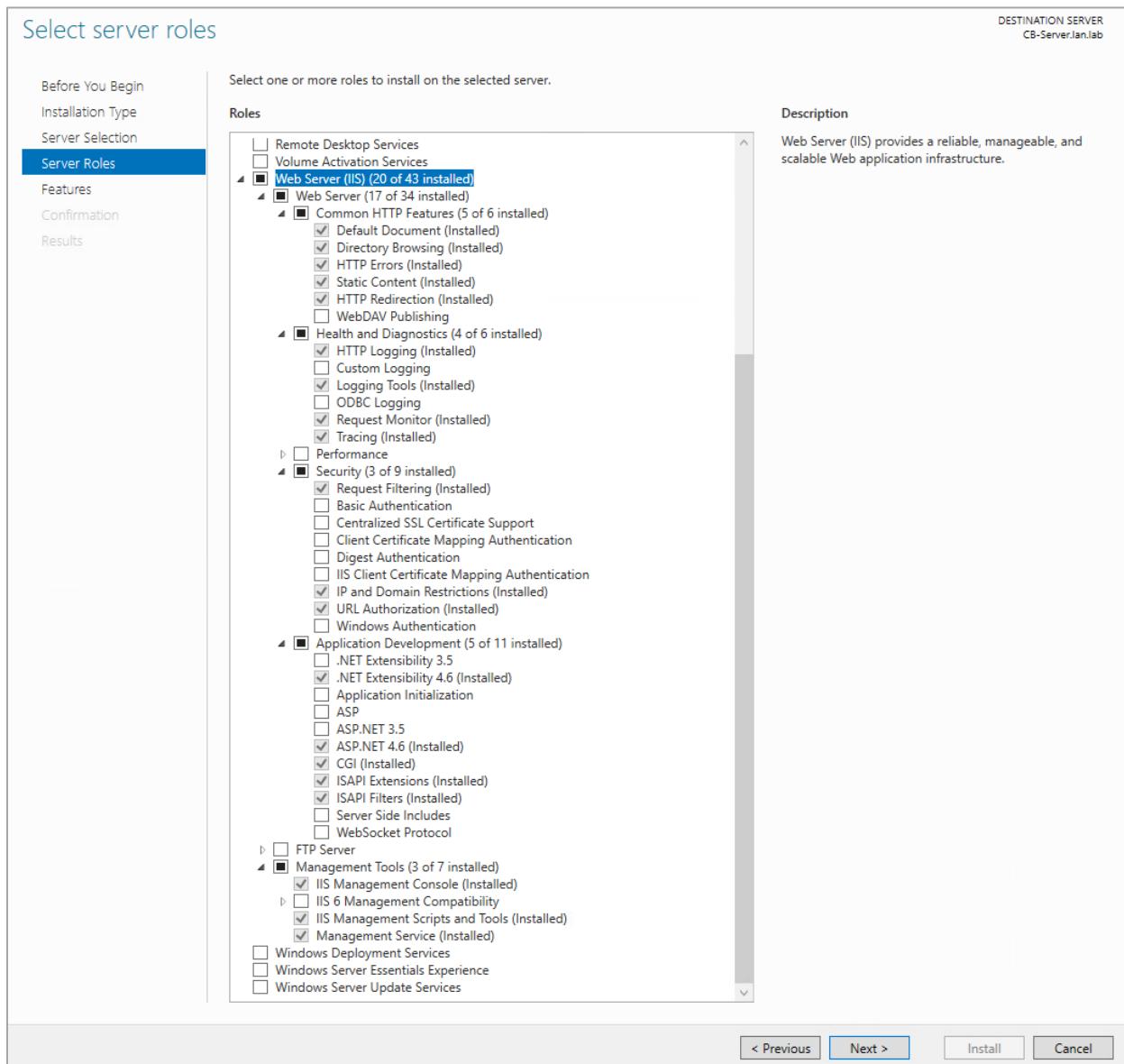
2097     Follow these steps to configure Windows Server 2016:

- 2098        1. On the Carbon Black App Control Server, configure Windows Server 2016:
- 2099              a. Based on Carbon Black documentation (Figure 2-74), Windows Server 2016 will need to  
2100              have the following features for the Internet Information Services (IIS) role enabled for  
2101              Carbon Black to work (Figure 2-75).

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

<b>Carbon Black.</b>								
<b>CB Protection Web Server Platform: Support Server</b>								
<b>Common Requirements ①</b>		<b>Restrictions ②</b>						
In the IIS Roles Manager, verify the following configuration:		Beginning with v8.0.0, the console relies on the CB Protection API. An incorrectly configured IIS server can prevent console access.						
<ul style="list-style-type: none"> <li>• Common HTTP Features:           <ul style="list-style-type: none"> <li>- Static Content</li> <li>- Default Document</li> <li>- HTTP Errors</li> <li>- HTTP Redirection</li> </ul> </li> <li>• Application development:           <ul style="list-style-type: none"> <li>- ASP.NET (version 4.5)</li> <li>- .NET Extensibility (version 4.5)</li> <li>- CGI</li> <li>- ISAPI Extensions</li> <li>- ISAPI Filters</li> </ul> </li> <li>• Health &amp; Diagnostics:           <ul style="list-style-type: none"> <li>- HTTP Logging</li> <li>- Logging Tools</li> <li>- Request Monitor</li> <li>- Tracing</li> </ul> </li> <li>• Security:           <ul style="list-style-type: none"> <li>- URL Authorization</li> <li>- Request Filtering</li> <li>- IP and Domain Restrictions</li> </ul> </li> <li>• Performance: None</li> <li>• Management Tools:           <ul style="list-style-type: none"> <li>- IIS Management Console</li> <li>- IIS Management Scripts and Tools</li> <li>- Management Service</li> </ul> </li> <li>• FTP Publishing Service: None</li> </ul>								
		<ul style="list-style-type: none"> <li>• To confirm API functionality, go to <b>System Configuration &gt; Advanced Options</b> in your current console and check the "API Access Enabled" box. If a green dot appears next to the checkbox, then you can assume that IIS is configured correctly. Otherwise, make sure you meet the following restrictions:</li> <li>• Site Bindings: The CB Protection API will not connect to localhost if the console web application is bound to a specific IP address instead of "*". Make sure that "*" is added to the list of bindings.</li> <li>• IP Address and Domain Restrictions: If you must limit console access to specific IP addresses, be sure that the IPv6 localhost address is added to the list.</li> <li>• Application Pools: CB Protection must be run within the DefaultAppPool application pool. Using a different app pool results in the CB Protection server not having the appropriate credentials to access the SQL Server database.</li> <li>• Authentication: You must disable Basic Authentication and Windows Authentication so that the CB Protection Server handles authentication. Otherwise, users will not be able to log into the CB Protection Server.</li> </ul>						
Version	Part Of OS	Current Version	Supported Architecture	Supported Level	Additional Notes/Requirements			
IIS 8.5	Windows 2012 Server R2 only		x64		<p>① ② Common Requirements and Restrictions are listed in the table above</p> <p>Additional requirements: Private memory for IIS should be increased to 800 MB</p>			
IIS 10	Windows 2016 Server		X64		<p>① ② Common Requirements and Restrictions are listed in the table above</p> <p>Additional requirements: Private memory for IIS should be increased to 800 MB</p>			

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



- 2104 2. Manually update the Windows Server firewall configuration to allow inbound port 41002 traffic from CB App Control clients/agents.
- 2105 3. Configure Policy in the Carbon Black Console using these steps:
- 2106 a. In the CB App Control Console, go to **Rules > Policies**.
- 2107 b. Create a new policy with the desired enforcement level. In this case, a high enforcement level was chosen to actively block execution of unapproved or banned executables (Figure 2-76).
- 2108  
2109  
2110

2111 Figure 2-76 Carbon Black Policy Edit

The screenshot shows the Carbon Black Protection interface. The left sidebar is titled 'RULES' and contains sections for Policies, Mappings, Notifiers, Software Rules (Updaters, Rapid Configs, Publishers, Users, Directories, Files, Custom, Memory, Registry), Scripts, Reputation, Event Rules, and Indicator Sets. The main content area is titled 'Edit Policy HighEnfcmt\_NCCOE'. It displays the following details:

- Policy Name:** HighEnfcmt\_NCCOE
- Description:** High Enforcement Block Unapproved or Banned
- Mode:** Control (radio button selected)
- Enforcement Level:** Connected (High (Block Unapproved)) and Disconnected (High (Block Unapproved)) dropdown menus.
- Automatic Policy Assignment For New Computers:** A checkbox is unchecked.
- Set Manual Policy For Existing Computers:** A note states there are currently no computers in this policy.
- Options:** Checkboxes for Allow Upgrades, Track File Changes, Load Agent in Safe Mode, and Suppress Logo In Notifier are present; Allow Upgrades and Track File Changes are checked.
- Total Computers:** 0
- Connected Computers:** 0

Below these settings is a table titled 'Device Control Settings' with columns for Name, Status, and Notifiers. It lists three rules:

Name	Status	Notifiers
Block writes to unapproved removable devices	Active	<default>. Block writes to unapproved removable
Block writes to banned removable devices	Active	<default>. Block writes to banned removable devi
Report reads from unapproved removable devices	Report Only	<none>

Buttons at the bottom include Advanced, File Rules, Custom Rules, Memory Rules, Registry Rules, Publisher Rules, Rapid Configs, Computers, and Device Control Settings.

2112

2113

4. Enable AD Integration Features as follows:

2114

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

2115

2116

2117

2118 Figure 2-77 Carbon Black App Control System Configuration

The screenshot shows the Carbon Black Protection web interface. The left sidebar is titled 'ADMINISTRATION' and includes sections for 'Login Accounts' (Users, User Roles, User Role Mappings), 'System Configuration' (General, Events, Security, Advanced Options, Mail, Licensing, External Analytics, Connectors, SAML Login), 'System Health', and 'Update Agent/Rule Versions'. The main content area has tabs at the top: General, Events, Security, Advanced Options, Mail, Licensing, External Analytics, Connectors, and SAML Login. The 'General' tab is selected. It displays 'General Settings' and 'Server Status' sections. Under 'Server Status', the following information is shown:

Cb Protection Version:	8.1.10.3
Server Address:	CB-Server.lan.lab
Server Port:	41002
Server Timezone:	Automatic
Database Schema Version:	8.1.10.3
Database Address:	\SQLEXPRESS
Database Auth.Type:	NT
Database Size:	463.06 MB
Free Local Disk Space:	480.1 GB / 499.5 GB
CL Version:	1835

Below this is the 'Active Directory / LDAP integration' section, which includes fields for AD-Based Logins (Enabled), AD Security Domain (lan.lab), AD-Based Policy (Enabled), Windows 2000 DCs (checkbox), and a 'Test AD Connectivity' button with a success message. At the bottom is the 'Agent Management' section.

2119

2120 5. Add users from AD and assign policies:

2121 a. Add "Test Users" OU from the AD to policy mapping settings and assign the "High-  
2122 Enfcmt\_NCCOE" policy (Figure 2-78).2123 This OU includes the "nccoeUser" and "nccoeAdmin" user accounts created for the test  
2124 scenarios. This policy will be automatically applied to these users logged in on any com-  
2125 puter that is running the CB Protection Agent. The "HighEnfcmt\_NCCOE" policy is set to  
2126 High Enforcement level, which will actively block all unapproved or banned files, applica-  
2127 tions, or devices.

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

The screenshot shows the Carbon Black Protection web interface. The left sidebar has a 'RULES' section with 'Policies', 'Mappings' (which is selected), 'Notifiers', and various software rule categories like Updaters, Rapid Configs, Publishers, Users, Directories, Files, Custom, Memory, Registry, and Scripts. The main content area is titled 'Active Directory Policy Mappings'. It shows a table with two rows:

Object	Relationship	Match	Action	Policy
<input checked="" type="checkbox"/> if User	is in OU	Test Users <a href="#">i</a>	move to	HighEnfcomt_NCCOE
<input checked="" type="checkbox"/>	[all others]		apply policy from	Default Policy

At the bottom of the page, the URL is https://cb-server.lan.lab/dashboard.php?dbid=HOMEPAGE.

2129

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

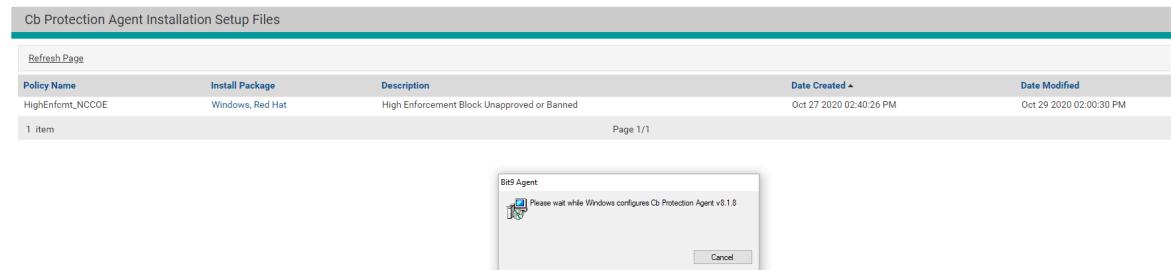
2131 (The process outlined below uses the CRS Engineering Workstation as an example, but the process  
2132 was the same for all the agent computers.). Follow these steps:

- 2133 a. Open the browser on the CRS Engineering Workstation and enter the URL to download  
2134 the agent installer: <https://CB-Server.lan.lab/hostpkg>. This URL is on the Carbon Black  
2135 server itself and is accessed on the local network. CB-Server.lan.lab is the full host name  
2136 we gave this server during installation.
  - 2137 i. If the host cannot access CB-Server.lan.lab, update the environment DNS Server  
2138 by mapping the IP address, 10.100.0.52, to CB-Server.lan.lab or add the mapping  
2139 to the local host file.
- 2140 b. Download the Windows CB App Control Agent installer from the CB App Control Server  
2141 and install on the CRS Engineering Workstation (Figure 2-79).

**2142 Figure 2-79 Carbon Black Agent Download**

Installing the Cb Protection Agent software is simple:

1. Click the installation setup file for the policy assigned to you by your network administrator.
2. Download the installation setup file to a convenient location on your hard-drive.
3. From the download directory, double-click the newly downloaded file to install Cb Protection Agent.



**2143**

- 2144 c. Check the CB App Control Console to verify communication and initialization of the new  
2145 CRS Engineering Workstation agent computer on the CB App Control Server (Figure  
2146 2-80).**

**2147 Figure 2-80 Carbon Black App Control Computers**

The screenshot shows the "Computers" page in the CB Protection console. The left sidebar has sections for ASSETS (Computers, Files, Applications, Devices, Certificates) and FILES (File Catalog, Files on Computers, Application Catalog, Applications on Computers). The main area displays a table of connected computers. One computer, "LAN\POLARIS", is listed with the following details:

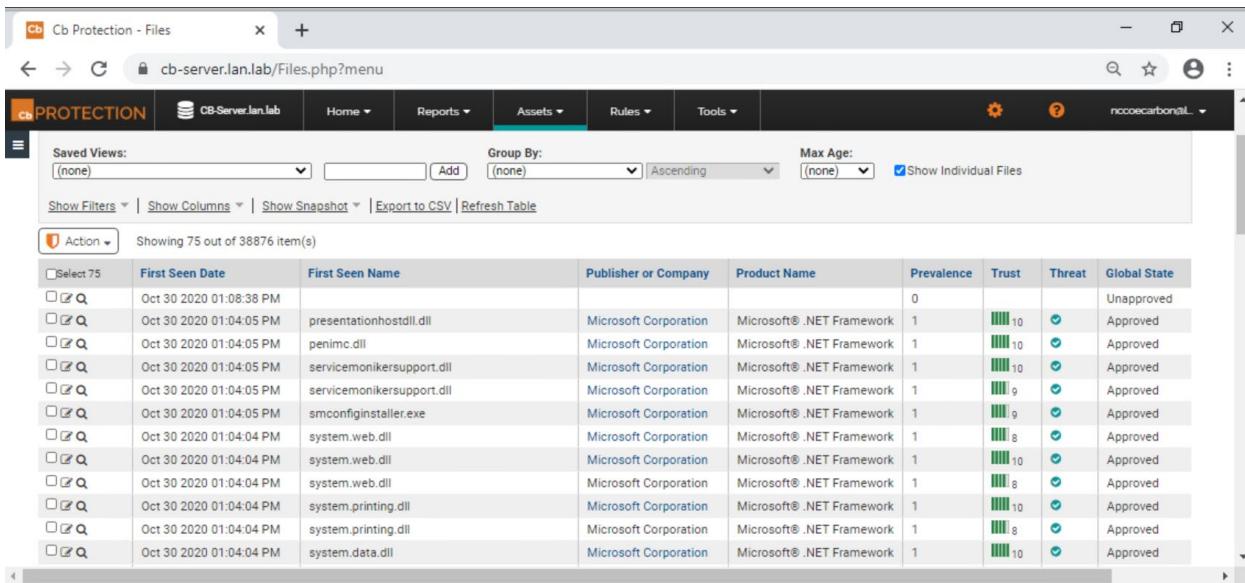
Action	Computer Name	Connected	Policy Status	Upgrade Status	Connected Enforcement	Disconnected Enforcement	IP Address	Policy
<input type="checkbox"/>	LAN\POLARIS	●	Up to date	Up to date	High (Block Unapproved)	High (Block Unapproved)	10.100.0.20	-HighEnfmcmt_NCCOE-

Below the table, it says "1 item" and "Page 1/1". On the right, there are dropdowns for "Days Disconnected" and "rows per page" set to 25.

**2148**

- 2149 d. Approve all new trusted files and publishers that were added from the CRS Engineering  
2150 Workstation to the catalog on the CB App Control Server.  
2151 e. This image (Figure 2-81) shows the Cb Protection - Files page of the CB App Control Con-  
2152 sole.**

2153 Figure 2-81 Carbon Black App Control File Catalog



The screenshot shows a web-based application interface for Carbon Black Protection. The title bar reads "Cb Protection - Files". The main content area is titled "PROTECTION" and shows a table of file catalog entries. The columns include "First Seen Date", "First Seen Name", "Publisher or Company", "Product Name", "Prevalence", "Trust", "Threat", and "Global State". The table lists various Microsoft .NET Framework files from October 30, 2020, with prevalence ranging from 0 to 10 and trust levels mostly at 10. The "Global State" column indicates some files are "Unapproved" while others are "Approved".

Action	Showing 75 out of 38876 item(s)							
	First Seen Date	First Seen Name	Publisher or Company	Product Name	Prevalence	Trust	Threat	Global State
<input type="checkbox"/>	Oct 30 2020 01:08:38 PM				0			Unapproved
<input type="checkbox"/>	Oct 30 2020 01:04:05 PM	presentationhost.dll	Microsoft Corporation	Microsoft® .NET Framework	1	10	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:05 PM	penimc.dll	Microsoft Corporation	Microsoft® .NET Framework	1	10	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:05 PM	servicemonikersupport.dll	Microsoft Corporation	Microsoft® .NET Framework	1	10	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:05 PM	servicemonikersupport.dll	Microsoft Corporation	Microsoft® .NET Framework	1	9	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:05 PM	smconfiginstaller.exe	Microsoft Corporation	Microsoft® .NET Framework	1	9	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:04 PM	system.web.dll	Microsoft Corporation	Microsoft® .NET Framework	1	8	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:04 PM	system.web.dll	Microsoft Corporation	Microsoft® .NET Framework	1	10	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:04 PM	system.web.dll	Microsoft Corporation	Microsoft® .NET Framework	1	8	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:04 PM	system.printing.dll	Microsoft Corporation	Microsoft® .NET Framework	1	10	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:04 PM	system.printing.dll	Microsoft Corporation	Microsoft® .NET Framework	1	8	✓	Approved
<input type="checkbox"/>	Oct 30 2020 01:04:04 PM	system.data.dll	Microsoft Corporation	Microsoft® .NET Framework	1	10	✓	Approved

2154

## 2.11 Windows Software Restriction Policy (SRP)

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

### 2.11.1 Host and Network Configuration

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

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 (Secondary) 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.

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

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 [Figure B-3](#). 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 Supervisory LAN 192.168.0.20
CRS Local Historian	Hyper-V VM	Windows 2016	4x vCPU	16 GB	80 GB, 171 GB	CRS Supervisory LAN 192.168.0.21

2173 

## 2.11.2 Installation

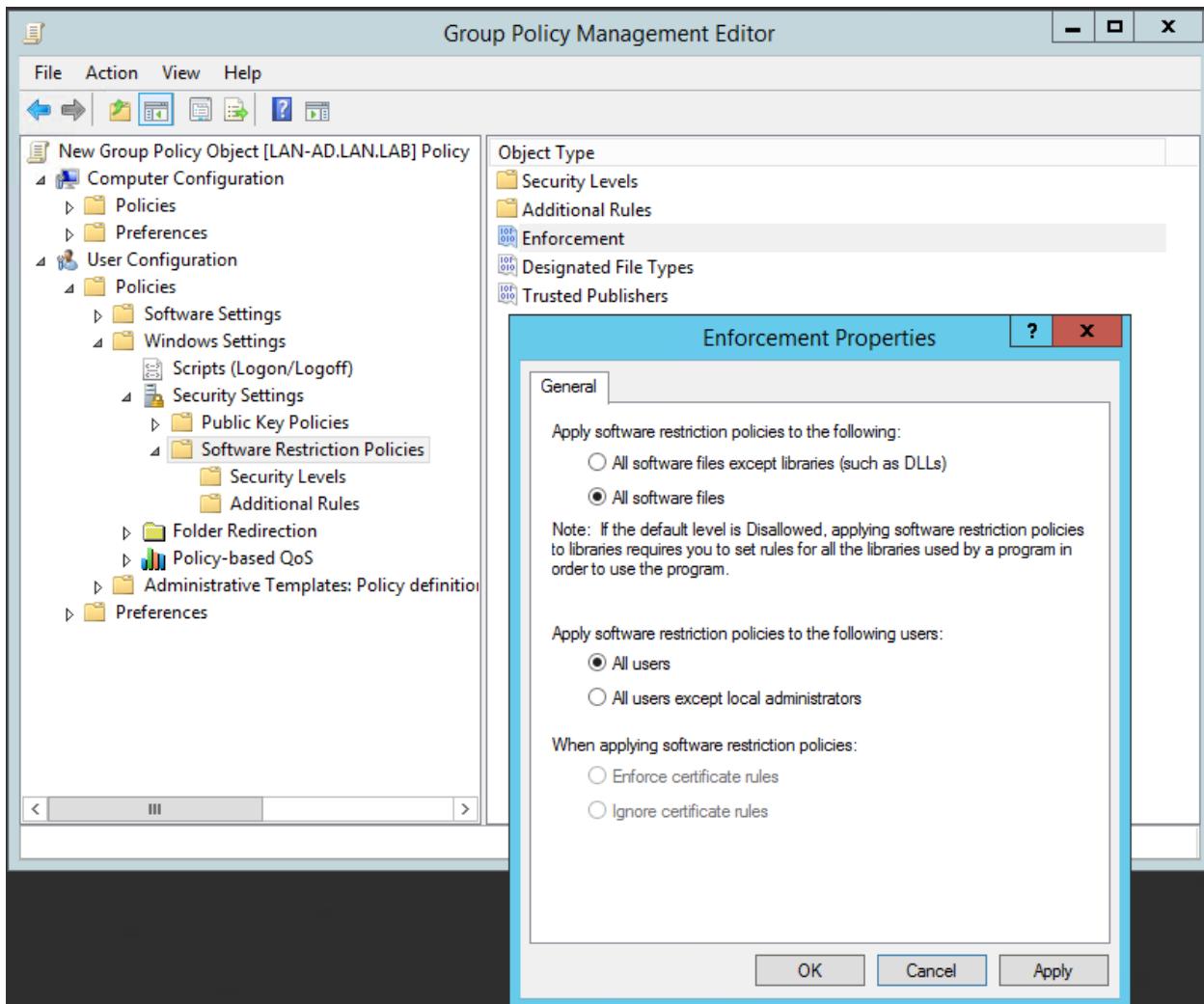
2174 Windows SRP is a feature of the Windows operating system and therefore did not require any specific  
2175 installation for use in the project.2176 

## 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     1. Set up AD with a “Test User” OU and add the NCCOE User (nccoeUser) and Admin (nccoeAdmin)  
2182       accounts for this project to the OU.
- 2183     2. To allow the NCCOE Admin account to be included as a local administrator within the  
2184       environment, modify the Default Domain GPO to add Administrators to Restricted Group and  
2185       include the NCCOE Admin account.
- 2186     3. To support applying GPOs as local settings to non-domain computers, download LGPO.zip from  
2187       Microsoft Security Compliance Toolkit 1.0 available at <https://www.microsoft.com/en-us/download/details.aspx?id=55319>.
- 2189     4. Review the National Security Agency (NSA) Guidance for Application Whitelisting using Software  
2190       Restriction Policies and Guidelines for Application Whitelisting ICSs available at  
2191       <https://apps.nsa.gov/iaarchive/library/reports/application-whitelisting-using-srp.cfm> and  
2192       <https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/guidelines-for-application-whitelisting-industrial-control-systems.cfm> respectively.
- 2194     5. 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.

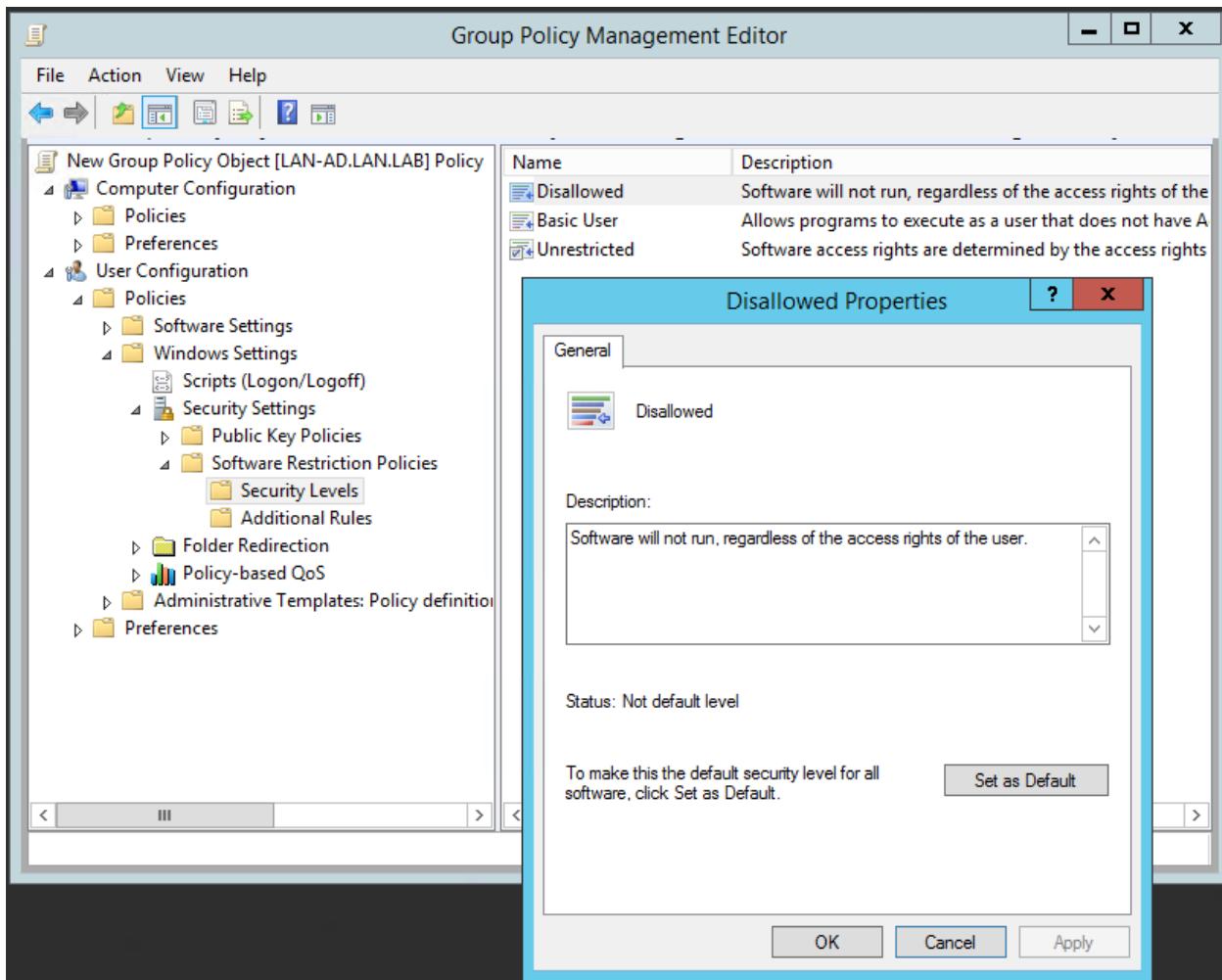
2198 Figure 2-82 Setting Enforcement Properties



2199

- 2200        b. In the Group Policy Management Editor, in the Security Levels folder:
- 2201           i. Double-click the Disallowed security level to open the Disallowed Properties window.
- 2202           ii. Click the Set as Default radio button (Figure 2-83) to configure SRP in allowlist mode. After completing this step, only programs in the paths specified by the environment variables SYSTEMROOT (typically C:\Windows), PROGRAMFILES (C:\Program Files), and PROGRAMFILES(x86) (C:\Program Files (x86)) are permitted to execute. These path rules are automatically added when the "Disallowed" security level is set as the default.

2209 Figure 2-83 Setting Security Level Default



2210

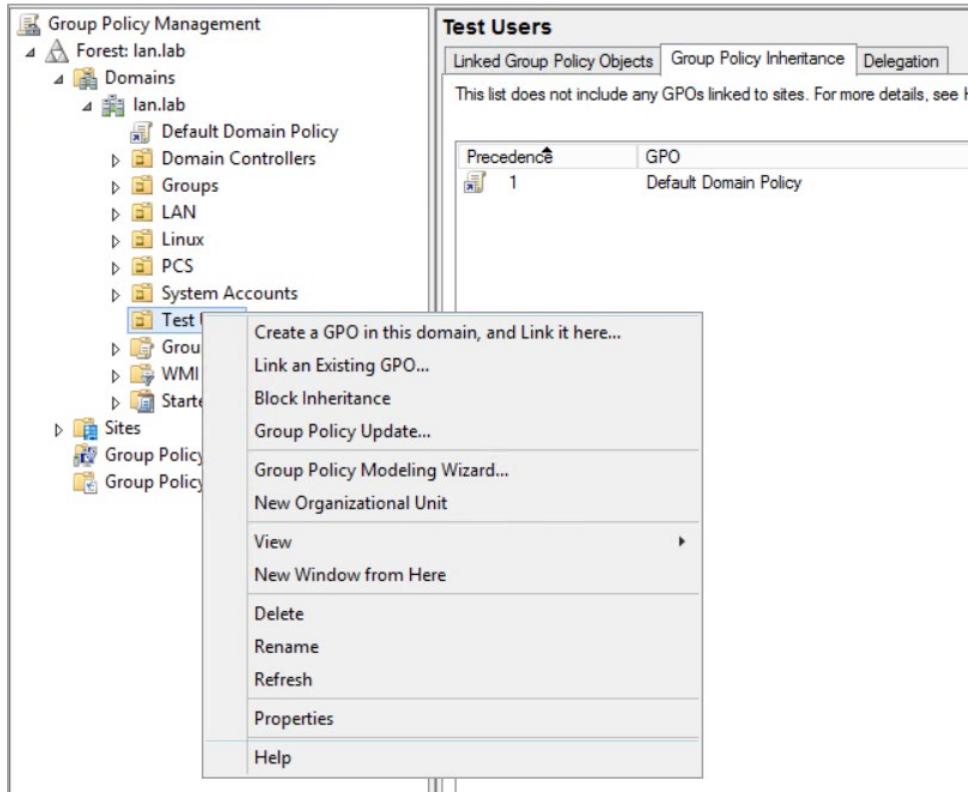
- 2211       c. Customize the Allowlist Rules to enhance security by disallowing specific subfolders in  
2212           the default allowed paths and to support organization application requirements.  
2213           i. Click the **Additional Rules** folder and apply the rules shown in Figure 2-84. This  
2214           figure combines the NSA recommended path settings in addition to lab applica-  
2215           tion requirements and for disabling installers and other executable content as in-  
2216           dicated in the comments. *Organizations should audit their environments to deter-*  
2217           *mine the appropriate rules to define within the policy.*

2218 Figure 2-84 Additional Rules Defined for Lab Environment

Name	Type	Security Level	Description
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Path	Unrestricted	Default System Root Allow Rule
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Debug	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\PCHEALTH\ERRORREP	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Registration	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\catroot2	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\com\dmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\Fx1Tmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\spool\drivers\c...	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32\spool\PRINTERS	Path	Disallowed	Deny execution per NSA Guidance
%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%\System32\spool\SERVERS	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\com\dmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\Fx1Tmp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\SysWOW64\Tasks	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Tasks	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\Temp	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\tracing	Path	Disallowed	Deny execution per NSA Guidance
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)%	Path	Unrestricted	Allow 32-bit Program Files on 64 bit systems.
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Path	Unrestricted	Default Program Files Directory Allow Rule
%USERPROFILE%\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Path	Unrestricted	Temp rule for Workstations Allow OneDrive
%USERPROFILE%\Forescout Console 8.2.1	Path	Unrestricted	Temporary Rule to Allow Forescout Console
*.lnk	Path	Unrestricted	Allow Links to executables
*.msi	Path	Disallowed	Prevent installers from executing
\%USERDNSDOMAIN%\Sysvol\	Path	Unrestricted	Allow Domain Login Scripts
C:\TwinCAT	Path	Unrestricted	Added to support CRS PLC Programming
E:\Program Files	Path	Unrestricted	Approved alternate Program Files Location
E:\Program Files (x86)	Path	Unrestricted	Approved alternate 32-bit Program Files location
runas.exe	Path	Disallowed	Deny execution per NSA Guidance

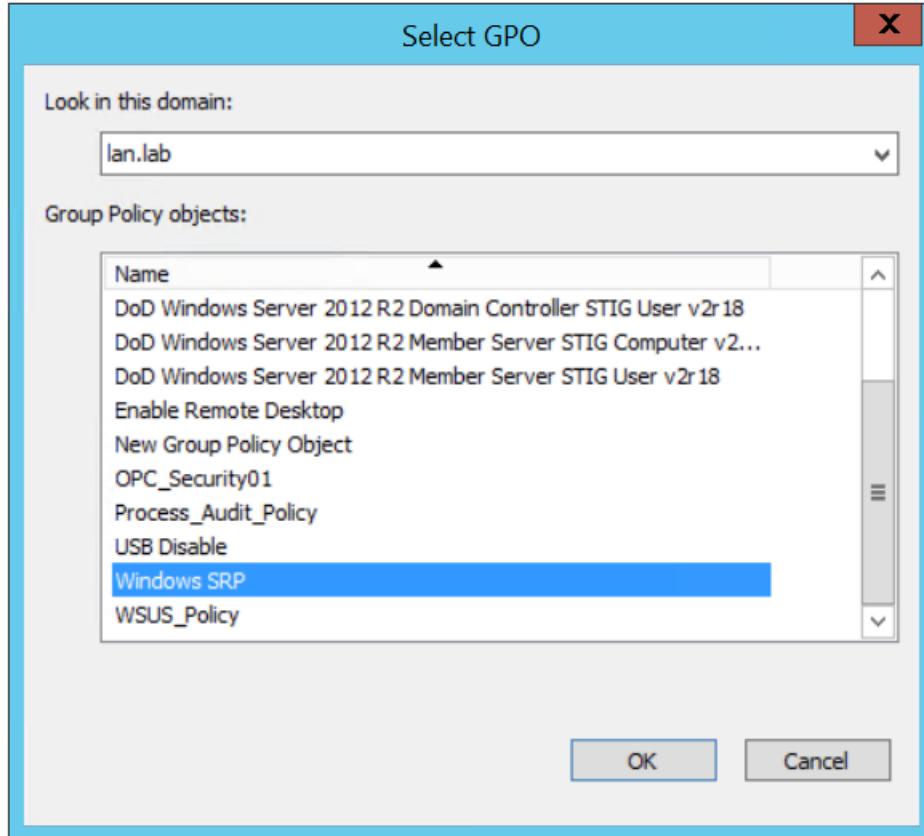
- 2219        6. Link the GPO to the Test User OU:  
2220            a. In the Group Policy Management tool, right click the “Test User” OU and select **Link an Existing GPO** from the pop-up menu (Figure 2-85).  
2221

2222 **Figure 2-85 Menu Options for Accessing the Link an Existing GPO Option**



- 2223        b. In the dialog box, select the Windows SRP GPO Object from the list and click OK (Figure  
2224              2-86).

2225        Figure 2-86 Dialog Box for Selecting GPO to Link



- 2226
- 2227        (Optional) Install GPO as the local policy on non-domain systems; for systems that are not joined  
2228              to the domain, the nccoeUser and nccoeAdmin accounts are created as local user and  
2229              administrator accounts, respectively. Additionally, the Windows SRP GPO is manually applied to  
2230              the local 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-click on the Windows SRP GPO object.
- 2233
- 2234              ii. Select the **Back Up...** option from the pop-up menu.
- 2235
- 2236              iii. In the dialog box, choose a destination location such as *C:\Backup GPO Folder* or  
some other convenient location to place the files and click **Back Up**.
- 2237
- 2238              d. Copy the LGPO.exe along with the files created in the previous step to the non-domain  
computer system.
- 2239
- 2240              e. Login as an administrator on the non-domain computer and navigate to the **{GUID}\Domain\sysvol\GPO\User** folder, which should contain the **registry.pol** file for the GPO.

2241 f. Execute the following commands to apply the settings to the local nccoeUser and  
2242 nccoeAdmin accounts:

2243 **lgpo.exe /u:nccoeUser registry.pol**

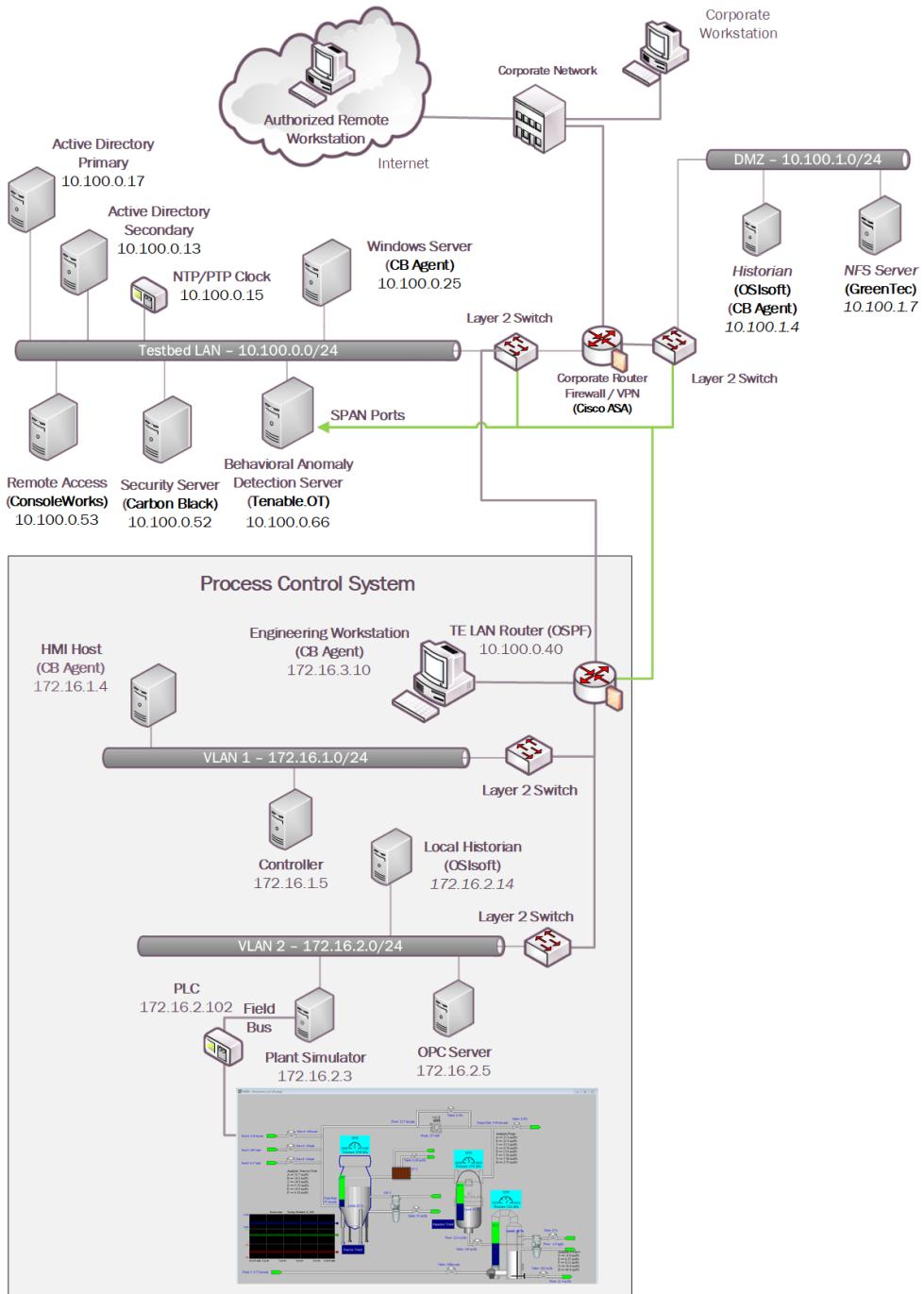
2244 **lgpo.exe /u:nccoeAdmin registry.pol**

	<b>Appendix A List of Acronyms</b>
2245	AAL Application Allowlisting
2246	AD Active Directory
2247	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	IoT 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	OT Operational Technology

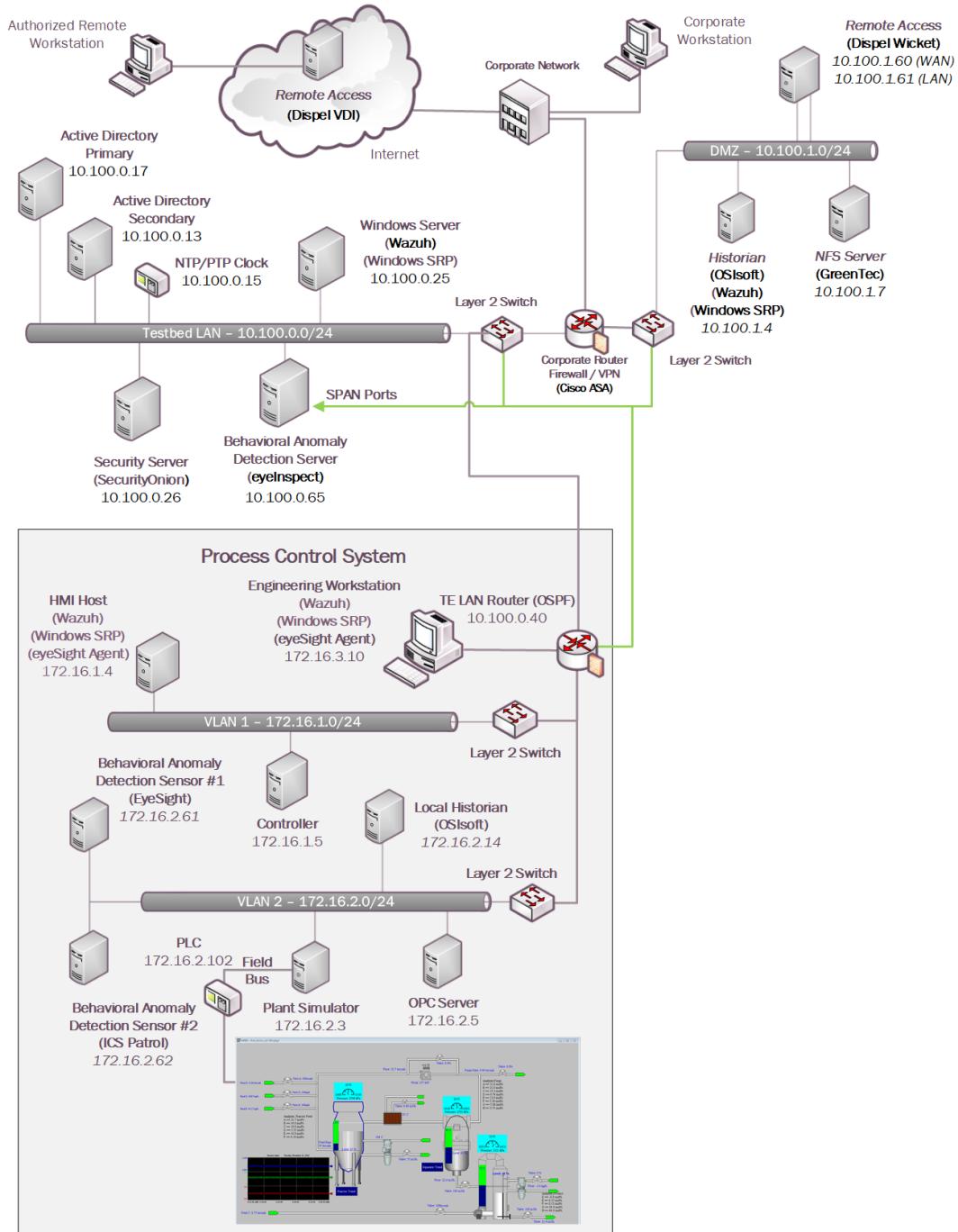
2273	OU	Organizational Unit
2274	PCS	Process Control System
2275	PI	Process Information
2276	PLC	Programmable Logic Controller
2277	RDP	Remote Desktop Protocol
2278	SP	Special Publication
2279	SPAN	Switch Port Analyzer
2280	VDI	Virtual Desktop Interface
2281	VLAN	Virtual Local Area Network
2282	VM	Virtual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

## 2284 Appendix B Build Architectures Diagrams

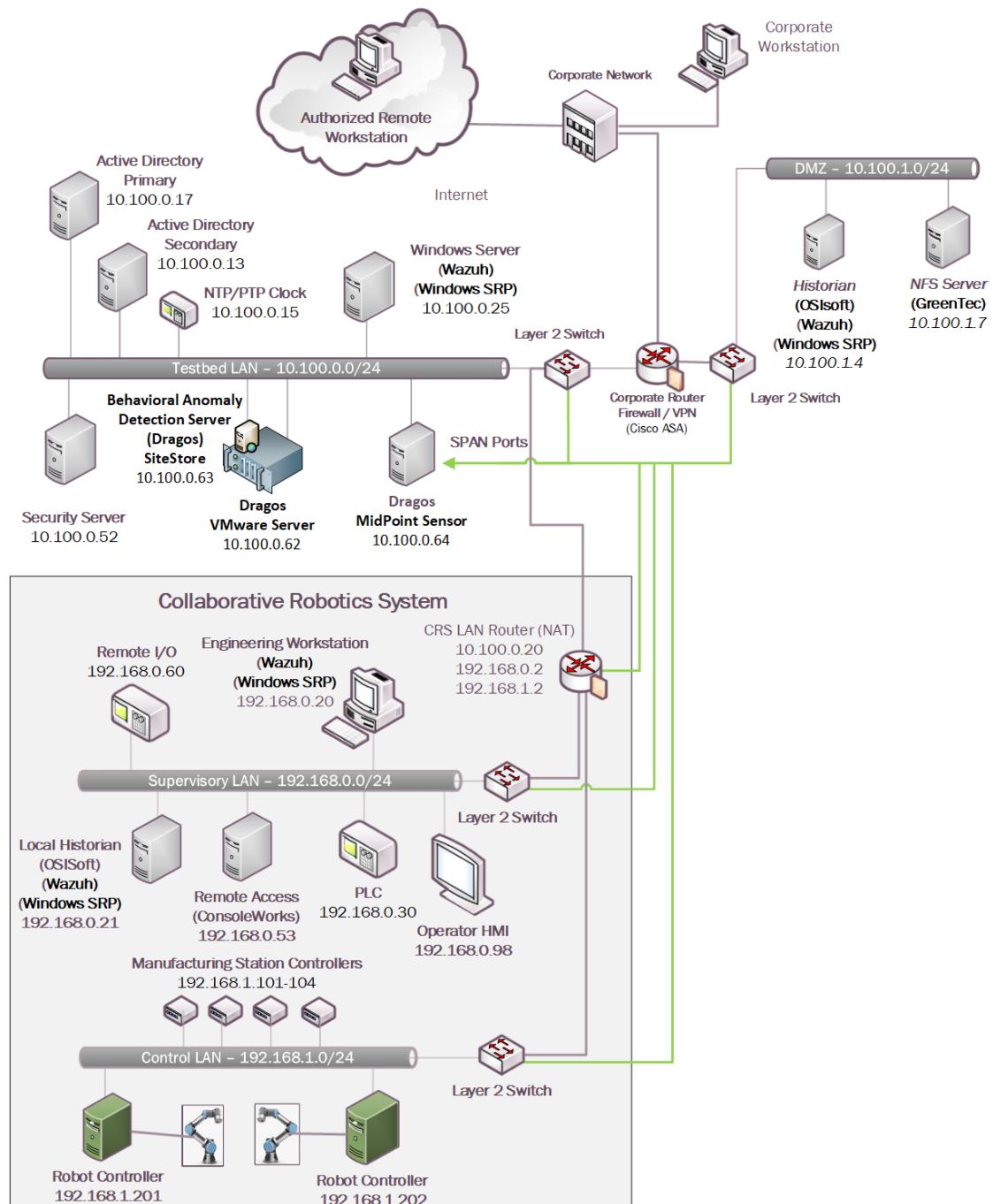
2285 Figure B-1 Build 1 Architecture Diagram



2286 Figure B-2 Build 2 Architecture Diagram



2287 Figure B-3 Build 3 Architecture Diagram



2288 Figure B-4 Build 4 Architecture Diagram

