

**NISTIR 8219**

# **Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection**

James McCarthy  
Michael Powell  
Keith Stouffer  
CheeYee Tang  
Timothy Zimmerman  
William Barker  
Titilayo Ogunyale  
Devin Wynne  
Johnathan Wiltberger

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

**NISTIR 8219**

# Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

James McCarthy  
Michael Powell  
*National Cybersecurity Center of Excellence  
Information Technology Laboratory*

Keith Stouffer  
CheeYee Tang  
Timothy Zimmerman  
*Intelligent Systems Division  
Engineering Laboratory*

William Barker  
*Dakota Consulting  
Silver Spring, MD*

Titilayo Ogunyale  
Devin Wynne  
Johnathan Wiltberger  
*The MITRE Corporation  
McLean, VA*

November 2018



U.S. Department of Commerce  
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology  
*Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology*

1 **Abstract**

2 Industrial control systems (ICS) are used in many industries to monitor and control physical  
3 processes. As ICS continue to adopt commercially available information technology (IT) to  
4 promote corporate business systems' connectivity and remote access capabilities, ICS  
5 become more vulnerable to cybersecurity threats. The National Institute of Standards and  
6 Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE), in  
7 conjunction with NIST's Engineering Laboratory (EL), has demonstrated a set of behavioral  
8 anomaly detection (BAD) capabilities to support cybersecurity in manufacturing  
9 organizations. The use of these capabilities enables manufacturers to detect anomalous  
10 conditions in their operating environments to mitigate malware attacks and other threats to  
11 the integrity of critical operational data. NIST's NCCoE and EL have mapped these  
12 demonstrated capabilities to the Cybersecurity Framework and have documented how this set  
13 of standards-based controls can support many of the security requirements of manufacturers.  
14 This report documents the use of BAD capabilities in two distinct, but related, demonstration  
15 environments: a robotics-based manufacturing system and a process control system that  
16 resembles what is being used by chemical manufacturing industries.

17 **Audience**

18 This report is intended for individuals or entities that are interested in understanding BAD  
19 technologies and their application to ICS environments. Additionally, this report is intended  
20 for those who are interested in understanding how to implement BAD tools in ICS and other  
21 operational technology environments.

22 **Keywords**

23 *BAD; behavioral anomaly detection; cybersecurity; Cybersecurity Framework; ICS;*  
24 *industrial control systems; manufacturing; process control*

25 **Acknowledgments**

26 NIST and the NCCoE wish to thank Omer Schneider, Phil Neray, and Joe DiPietro of  
27 CyberX; Paul J. Geraci, Andrew Duke, and Mark McCoy of OSIsoft; Dennis Murphy, Jason  
28 Sharp, and Daniel Trivellato of SecurityMatters; and Erlend A. Engum, Jishnu Nair, Nina  
29 Hesby Tvedt, and Siv Hilde Houmb of Secure-NOK for their contributions to this document.

30

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

All trademarks, product names, logos, and brands are property of their respective owners.

31 **Executive Summary**

32 NIST's NCCoE, with NIST's EL and NCCoE collaborators, offers information regarding the  
33 use of BAD capabilities to support cybersecurity in ICS for manufacturing. This National  
34 Institute of Standards and Technology Interagency Report (NISTIR) was developed in  
35 response to feedback from members of the manufacturing sector concerning the need for  
36 cybersecurity guidance.

37 Cybersecurity attacks directed at manufacturing infrastructure can be detrimental to both  
38 human life and property. BAD mechanisms support a multifaceted approach to detecting  
39 cybersecurity attacks against ICS devices on which manufacturing processes depend, in order  
40 to permit the mitigation of those attacks.

41 The NCCoE and EL deployed commercially available hardware and software provided by  
42 industry, in response to a NIST notice in the Federal Register, in order to demonstrate BAD  
43 capabilities in an established laboratory infrastructure. We mapped security characteristics of  
44 the demonstrated capabilities to the *Framework for Improving Critical Infrastructure*  
45 *Cybersecurity* [1] based on NISTIR 8183, the *Cybersecurity Framework Manufacturing*  
46 *Profile* [2]. The mapping can be used as a reference in applying specific security controls  
47 found in prominent industry standards and guidance.

48 Introducing anomalous data into a manufacturing process can disrupt operations, whether  
49 deliberately or inadvertently. The goal of this NISTIR is to provide practical approaches for  
50 manufacturers to use in their efforts to strengthen the cybersecurity of their manufacturing  
51 processes. This NISTIR demonstrates how BAD tools can be used as a key security  
52 component in sustaining business operations, particularly those based on ICS. The examples  
53 provided in this NISTIR illustrate how detecting anomalous conditions can improve the  
54 reliability of ICS, in addition to providing specific cybersecurity benefits.

|    |   |           |
|----|---|-----------|
| 55 | <b>Table of Contents</b>  |           |
| 56 | <b>1. Introduction</b>  | <b>1</b>  |
| 57 | 1.1. Background   | 1         |
| 58 | 1.2. Purpose and Scope  | 1         |
| 59 | 1.3. Challenges   | 2         |
| 60 | 1.4. Approach to Addressing Challenges                                    | 2         |
| 61 | 1.5. Benefits   | 3         |
| 62 | <b>2. Cybersecurity Framework and NIST Manufacturing Profile</b>          | <b>3</b>  |
| 63 | <b>3. Demonstration Environment Architecture</b>                          | <b>6</b>  |
| 64 | 3.1. Collaborative Robotic System   | 7         |
| 65 | 3.1.1. CRS Network Architecture   | 8         |
| 66 | 3.2. Process Control System   | 9         |
| 67 | 3.2.1. PCS Network Architecture   | 11        |
| 68 | 3.3. Behavioral Anomaly Detection Capabilities Demonstrated               | 12        |
| 69 | 3.3.1. SecurityMatters SilentDefense                                      | 12        |
| 70 | 3.3.2. Secure-NOK SNOK  | 12        |
| 71 | 3.3.3. CyberX   | 13        |
| 72 | 3.3.4. OSIsoft PI Data Archive  | 13        |
| 73 | 3.4. Behavioral Anomaly Detection Methods and Security Functions          | 13        |
| 74 | 3.5. Typographic Conventions  | 14        |
| 75 | <b>4. Demonstration Scenarios and Findings</b>                            | <b>14</b> |
| 76 | 4.1. Network-Based Behavioral Anomaly Detection                           | 15        |
| 77 | 4.2. Agent-Based Behavioral Anomaly Detection                             | 15        |
| 78 | 4.3. Historian-Based and Sensor-Based Behavioral Anomaly Detection        | 15        |
| 79 | 4.4. Demonstration Results and Findings                                   | 16        |
| 80 | <b>5. Conclusion</b>  | <b>16</b> |
| 81 | <b>Appendix A. SecurityMatters SilentDefense Supplemental Information</b> | <b>17</b> |
| 82 | A.1. Build Architecture   | 17        |
| 83 | A.2. Installation and Configuration                                       | 18        |
| 84 | A.2.1. Hardware   | 18        |
| 85 | A.2.2. Operating System   | 18        |
| 86 | A.2.3. Configure Sniffing Ports   | 19        |
| 87 | A.2.4. Configure the Management Port Internet Protocol Address            | 19        |
| 88 | A.2.5. Configure the SPAN Ports on Layer 3 Network Switches               | 20        |

89        A.2.6. Log into SilentDefense ..... 20

90    A.3. Anomaly Scenarios..... 20

91        A.3.1. Unencrypted Passwords Are Used to Access a Networking Device..... 21

92        A.3.2. Transmission Control Protocol Connection Requests Are Received from

93        the Internet ..... 21

94        A.3.3. Data Exfiltration Between ICS Devices via Server Message Block ..... 22

95        A.3.4. Data Exfiltration to the Internet via File Transfer Protocol ..... 23

96        A.3.5. Unauthorized Device Is Connected to the Network ..... 24

97        A.3.6. Loss of Communications with Modbus TCP Device ..... 25

98        A.3.7. Brute-Force Password Attack Against an ICS Device ..... 26

99        A.3.8. Invalid Credentials for Remote Access ..... 27

100       A.3.9. Unauthorized ICS Device Firmware Update..... 28

101       A.3.10. Unauthorized HMI Logic Modification ..... 29

102       A.3.11. ICS Device Receives Diagnostic Modbus TCP Function Codes ..... 30

103       A.3.12. ICS Device Receives Undefined Modbus TCP Function Codes ..... 31

104       A.3.13. ICS Device Receives Malformed Modbus TCP Traffic ..... 32

105       A.3.14. Illegal Memory Addresses of ICS Device Are Accessed..... 33

106       A.3.15. ICS Device Scanning Is Performed on the Network..... 34

107    **Appendix B. Secure-NOK SNOK Supplemental Information..... 36**

108       B.1. Build Architecture ..... 36

109       B.2. Installation and Configuration..... 37

110        B.2.1. Hardware ..... 37

111        B.2.2. Windows XP / Windows 7 / Windows Server 2012 Installation ..... 37

112        B.2.3. Ubuntu 12 / Ubuntu 14 Installation..... 38

113        B.2.4. SNOK Detector Configuration..... 39

114       B.3. Anomaly Scenarios..... 40

115        B.3.1. Web Browser Is Used to Access the Internet ..... 40

116        B.3.2. Data Exfiltration to the Internet via HTTP..... 41

117        B.3.3. European Institute for Computer Antivirus Research Virus Test File Is Detected

118        on Host..... 41

119        B.3.4. Host Scanning Is Performed on the Network ..... 41

120        B.3.5. Port Scanning Is Performed on the Network..... 43

121        B.3.6. Unauthorized Installation of Software ..... 44

122        B.3.7. Unauthorized Programmable Logic Controller Firmware Update ..... 44

123        B.3.8. Unauthorized PLC Logic Download..... 45

|     |   |           |
|-----|---|-----------|
| 124 | B.3.9. Unauthorized PLC Logic Modification.....                                       | 45        |
| 125 | B.3.10. Unauthorized Connection Is Established Between ICS Devices .....              | 46        |
| 126 | B.3.11. Host-Based Firewall Is Disabled.....  | 46        |
| 127 | B.3.12. Host-Based Anti-Virus Software Is Disabled .....                              | 47        |
| 128 | B.3.13. Host Central Processing Unit Load Is Increased.....                           | 47        |
| 129 | B.3.14. Unauthorized Detachment of Keyboard to Host .....                             | 47        |
| 130 | B.3.15. Unauthorized Insertion of USB Storage Device .....                            | 48        |
| 131 | <b>Appendix C. CyberX Supplemental Information.....</b>                               | <b>49</b> |
| 132 | C.1. Build Architecture .....   | 49        |
| 133 | C.2. Installation and Configuration.....  | 50        |
| 134 | C.2.1. Configuration Guide.....   | 51        |
| 135 | C.2.2. Configuration of Forwarding Rules .....  | 51        |
| 136 | C.2.3. Enabling Self-Learning Analytics .....   | 51        |
| 137 | C.3. Anomaly Scenarios.....   | 52        |
| 138 | C.3.1. Unencrypted Hypertext Transfer Protocol Credentials Are Detected on            |           |
| 139 | the Network .....   | 53        |
| 140 | C.3.2. Unauthorized Secure Shell Session Is Established with an Internet-Based Server |           |
| 141 | 54  |           |
| 142 | C.3.3. Data Exfiltration to the Internet via DNS Tunneling .....                      | 54        |
| 143 | C.3.4. Data Exfiltration to the Internet via Secure Copy Protocol.....                | 55        |
| 144 | C.3.5. European Institute for Computer Antivirus Research Virus Test File Is Detected |           |
| 145 | on the Network .....  | 56        |
| 146 | C.3.6. Unauthorized Device Is Connected to the Network.....                           | 57        |
| 147 | C.3.7. Denial-of-Service Attack Is Executed Against the ICS Local Area Network ....   | 58        |
| 148 | C.3.8. Data Exfiltration Between ICS Devices via User Datagram Protocol .....         | 58        |
| 149 | C.3.9. Invalid Credentials Are Used to Access a Networking Device.....                | 59        |
| 150 | C.3.10. Brute-Force Password Attack Against a Networking Device .....                 | 60        |
| 151 | C.3.11. Unauthorized PLC Logic Download.....  | 61        |
| 152 | C.3.12. Unauthorized PLC Logic Update – CRS .....                                     | 62        |
| 153 | C.3.13. Unauthorized PLC Logic Update – PCS.....                                      | 63        |
| 154 | C.3.14. Undefined Modbus Transmission Control Protocol Function Codes Are             |           |
| 155 | Transmitted to the PLC.....   | 64        |
| 156 | C.3.15. Unauthorized Ethernet/IP Scan of the Network .....                            | 65        |
| 157 | <b>Appendix D. OSIsoft Process Information Supplemental Information .....</b>         | <b>67</b> |
| 158 | D.1. Build Architecture .....   | 67        |

|     |   |           |
|-----|---|-----------|
| 159 | D.2. Installation and Configuration.....  | 67        |
| 160 | D.2.1. PI AF Installation .....   | 68        |
| 161 | D.2.2. PI Data Archive Installation .....   | 68        |
| 162 | D.2.3. PI System Process Explorer Installation .....                              | 69        |
| 163 | D.2.4. PI Vision Installation.....  | 69        |
| 164 | D.2.5. PI System Modbus Ethernet Interface Installation.....                      | 70        |
| 165 | D.2.6. PI System Points and Assets Configuration .....                            | 70        |
| 166 | D.2.7. PLC Asset Template Analysis Functions .....                                | 72        |
| 167 | D.2.8. Machining Station Asset Template Analysis Functions.....                   | 73        |
| 168 | D.2.9. Viewing and Acknowledging Alerts .....                                     | 75        |
| 169 | D.3. Anomaly Scenarios.....   | 75        |
| 170 | D.3.1. Frequency Increase of Trouble Calls from a Machining Station .....         | 76        |
| 171 | D.3.2. Machining Station Shuts Down During Normal Workcell Operations.....        | 76        |
| 172 | D.3.3. Inspection Station Rejects All Parts Leaving the Workcell .....            | 76        |
| 173 | D.3.4. Machining Station Door Sensor Fails .....                                  | 77        |
| 174 | D.3.5. Abnormal Process Variable Data Is Transmitted to the PLC.....              | 77        |
| 175 | D.3.6. Abnormal Process Variable Data Is Transmitted to a Machining Station ..... | 77        |
| 176 | D.3.7. Robots Fail to Send Required Sensor Data to a Machining Station.....       | 78        |
| 177 | D.3.8. Workcell Temperature Increases Above a Specified Threshold .....           | 78        |
| 178 | <b>Appendix E. Acronyms and Abbreviations .....</b>                               | <b>79</b> |
| 179 | <b>Appendix F. References .....</b>   | <b>82</b> |

180 **List of Tables**

|     |  |    |
|-----|--|----|
| 181 | Table 2-1 Mapping of Cybersecurity Framework Functions Addressed by BAD Capabilities |    |
| 182 | to the Manufacturing Profile.....  | 5  |
| 183 | Table 3-1 BAD Methods and Security Functions.....                                    | 13 |
| 184 | Table 3-2 Typographic Conventions .....  | 14 |

185 **List of Figures**

|     |   |    |
|-----|---|----|
| 186 | Figure 3-1 BAD High-Level Architecture.....                                     | 7  |
| 187 | Figure 3-2 Robotic Assembly Enclave Network .....                               | 8  |
| 188 | Figure 3-3 PCS Network Architecture.....  | 9  |
| 189 | Figure 3-4 TE Process Control Model.....  | 10 |
| 190 | Figure A-1 SPAN Port Connections to the SilentDefense Appliance in the PCS      | 17 |
| 191 | Figure A-2 SPAN Port Connections to the SilentDefense Appliance in the CRS..... | 18 |
| 192 |   |    |

|     |  |    |
|-----|--|----|
| 193 | Figure B-1 SPAN Port Connections to the SNOK Appliance in the PCS (Including the Hosts       |    |
| 194 | with SNOK Agents).....   | 36 |
| 195 | Figure B-2 SPAN Port Connections to the SNOK Appliance in the CRS (Including the Hosts       |    |
| 196 | with SNOK Agents).....   | 37 |
| 197 | Figure C-1 SPAN Port Connections to the CyberX Appliance in the PCS                          | 50 |
| 198 | Figure C-2 SPAN Port Connections to the CyberX Appliance in the CRS.....                     | 50 |
| 199 | Figure C-3 CyberX Network Reconfiguration Program on the Appliance .....                     | 51 |
| 200 | Figure C-4 Example Screenshot with All Five Self-Learning Analytics Enabled .....            | 52 |
| 201 | Figure C-5 Event Log (Timeline View) of Real-Time Alerts in the CyberX Console.....          | 53 |
| 202 | Figure D-1 Server Role Features to Be Selected During PI AF Installation                     | 68 |
| 203 | Figure D-2 Data Directories to Be Selected During PI Data Archive Installation .....         | 69 |
| 204 | Figure D-3 Configuration Options in the PI Point Builder for Tags Utilizing the ModbusE      |    |
| 205 | Interface .....  | 71 |
| 206 | Figure D-4 Example Configuration Settings for the Tag PLC-ExperimentMode .....               | 71 |
| 207 | Figure D-5 PI System Explorer View Showing the Configured Assets (Elements), the             |    |
| 208 | Resulting Hierarchical Structure of Assets, and Live Attributes Received from Station 1 .... | 72 |
| 209 | Figure D-6 PI System Explorer Interface Showing an Example of Alerts Displayed to the        |    |
| 210 | Operator for Acknowledgment, as Used During Anomaly Scenario Execution .....                 | 75 |

211 **1. Introduction**

212 The goal of this National Institute of Standards and Technology Interagency Report  
213 (NISTIR) is to show practical approaches that manufacturers can use to strengthen  
214 cybersecurity in their manufacturing processes. Behavioral anomaly detection (BAD) tools  
215 can provide a key security component for sustaining business operations, particularly those  
216 based on industrial control systems (ICS). Because introducing anomalous data into a  
217 manufacturing process can disrupt operations, whether deliberately or inadvertently, the  
218 examples provided in this NISTIR demonstrate how detecting anomalous conditions can  
219 improve the reliability of manufacturing and other ICS, in addition to providing the  
220 demonstrated cybersecurity benefits.

221 **1.1. Background**

222 As stated in the National Institute of Standards and Technology (NIST) Special Publication  
223 (SP) 800-82 [3], ICS are vital to the operation of the United States' critical infrastructures,  
224 which are often highly interconnected and mutually dependent systems. While federal  
225 agencies also operate many ICS, approximately 90 percent of the nation's critical  
226 infrastructures are privately owned and operated. As ICS increasingly adopt information  
227 technology (IT) to promote corporate business systems' connectivity and remote access  
228 capabilities by using industry-standard computers, operating systems (OSs), and network  
229 protocols, the accompanying integration provides significantly less isolation for ICS from the  
230 outside world. While security controls have been designed to deal with security issues in  
231 typical IT systems, special precautions must be taken when introducing these same  
232 approaches in ICS environments. In some cases, new security techniques tailored to the  
233 specific ICS environment are needed. NIST recognizes this concern and is working with  
234 industry to solve these challenges through the development of reference designs and the  
235 practical application of cybersecurity technologies. BAD is one tool for improving ICS  
236 security.

237 NIST's National Cybersecurity Center of Excellence (NCCoE), in conjunction with NIST's  
238 Engineering Lab (EL) and NCCoE industry collaborators, has demonstrated a set of BAD  
239 capabilities to support cybersecurity in manufacturing organizations. The use of these  
240 capabilities enables manufacturers to detect anomalous conditions in their operating  
241 environments to mitigate malware attacks and other threats to the integrity of critical  
242 operational data. NIST's NCCoE and EL have mapped these demonstrated capabilities to the  
243 NIST Cybersecurity Framework [1] and have documented how this set of standards-based  
244 controls can support many of the security requirements of manufacturers. This NISTIR  
245 documents the use of BAD capabilities in two distinct, but related, demonstration  
246 environments: a collaborative robotics-based manufacturing system and a process control  
247 system (PCS) that resembles what is being used by chemical manufacturing industries.

248 **1.2. Purpose and Scope**

249 The scope of this NISTIR is a single cybersecurity capability. The security characteristics of  
250 different BAD approaches were mapped to the Cybersecurity Framework. The mapping  
251 points manufacturers to specific security controls found in prominent cybersecurity  
252 standards.

253 **1.3. Challenges**

254 Cybersecurity is essential to the safe and reliable operation of modern industrial processes.  
255 Threats to ICS can come from numerous sources, including hostile governments, criminal  
256 groups, disgruntled employees, other malicious individuals, unanticipated consequences of  
257 component interactions, accidents, and natural disasters. The Cybersecurity Framework [1]  
258 addresses identifying threats and potential vulnerabilities; preventing and detecting events;  
259 and responding to, and recovering from, incidents. It is not possible to prevent all cyber  
260 events. It may not even be possible to identify all threats for which ICS need to be prepared.  
261 It is certainly necessary to detect incidents before the response to, or recovery from, the  
262 incidents can be undertaken. Therefore, the detection of cyber incidents is an essential  
263 element for cybersecurity.

264 Many incident-detection tools involve monitoring system behaviors for out-of-specification  
265 settings or readings or for predefined threat signatures (information elements previously  
266 identified as being associated with threats or vulnerability characteristics). However, as  
267 previously mentioned, not all threats and vulnerabilities are known beforehand (e.g., zero-  
268 day attacks); therefore, not all threats and vulnerabilities can be included among signatures  
269 for which monitoring is undertaken. BAD involves the continuous monitoring of systems for  
270 unusual events or trends. The monitor looks for evidence of compromise, rather than for the  
271 attack itself.

272 The challenge addressed by this project is to demonstrate example implementations of BAD  
273 capabilities that manufacturers can adopt to achieve their cybersecurity goals. Specifically,  
274 this project responds to a need within the manufacturing community to improve the ability to  
275 detect anomalous behavior in real or near-real time. Early detection of potential cybersecurity  
276 incidents is key to helping reduce the impact of these incidents for ICS.

277 **1.4. Approach to Addressing Challenges**

278 The NCCoE developed and demonstrated a set of example approaches for detecting  
279 anomalous conditions within manufacturers' ICS environments. These examples include  
280 recommendations that are practical for businesses to implement to strengthen cybersecurity  
281 in their manufacturing processes, with an additional potential for detecting anomalous  
282 conditions not related to security, such as equipment malfunctioning.

283 The NCCoE examples provide the following capabilities:

- 284 • models of BAD capabilities that manufacturers can adopt to achieve their security  
285 goals for mitigating the risks posed by threats to cybersecurity
- 286 • nonintrusive techniques to analyze industrial network communications, allowing the  
287 existing ICS infrastructure to flow through the network without interruption or a  
288 performance impact
- 289 • establishment of one or more baselines, and notification when specific changes or  
290 anomalies occur in the environment over time
- 291 • identification of new devices on the ICS network and of assets that have disappeared  
292 from the network

- 293 • detection of unauthorized configuration changes and of the transfer of files in the
- 294 network
- 295 • increased visibility into network operation and real-time alerting

296 The NCCoE used commercially available products provided by industry collaborators to  
297 address this cybersecurity challenge. These products were provided under Cooperative  
298 Research and Development Agreements. This NISTIR does not endorse any products and  
299 does not guarantee compliance with any regulatory initiatives. An organization’s information  
300 security experts should identify the products that will best integrate with their existing tools,  
301 processes, and system infrastructure. Organizations can adopt one of the demonstrated  
302 approaches or another one that adheres to the suggested guidelines. This NISTIR can also be  
303 used as a starting point for implementing BAD.

### 304 **1.5. Benefits**

305 This NISTIR is intended to help organizations accomplish their goals by using anomaly  
306 detection tools for the following purposes:

- 307 • detect cyber incidents in time to permit effective response and recovery
- 308 • expand visibility and monitoring capabilities within manufacturing control systems,  
309 networks, and devices
- 310 • reduce opportunities for disruptive cyber incidents by providing real-time monitoring  
311 and anomaly-detection alerts
- 312 • support the oversight of resources (e.g., IT, personnel, data)
- 313 • enable faster incident-response times, fewer incidents, and shorter downtimes

## 314 **2. Cybersecurity Framework and NIST Manufacturing Profile**

315 The *Framework for Improving Critical Infrastructure Cybersecurity* [1] is a voluntary  
316 risk-based assemblage of industry standards and best practices designed to help organizations  
317 manage cybersecurity risks. The Cybersecurity Framework, created through collaboration  
318 between government and the private sector, uses a common language to address and manage  
319 cybersecurity risk in a cost-effective way, based on business needs, without imposing  
320 additional regulatory requirements. The *Cybersecurity Framework Manufacturing Profile* [2]  
321 defines specific cybersecurity activities and outcomes for the protection of the manufacturing  
322 system and its components, facility, and environment. By using the profile, the manufacturer  
323 can align cybersecurity activities with business requirements, risk tolerances, and resources.  
324 The profile provides a manufacturing sector-specific approach to cybersecurity from  
325 standards, guidelines, and industry best practices.

326 Table 2-1 maps functions addressed by BAD capabilities to NIST Cybersecurity Framework  
327 functions as presented in the profile. In Table 2-1, the references to the requirements are  
328 American National Standards Institute / International Society of Automation Standard 62443-  
329 2-1 (*Security for Industrial Automation and Control Systems: Establishing an Industrial  
330 Automation and Control Systems Security Program*) [4], American National Standards  
331 Institute / International Society of Automation Standard 62443-2-3 (*Security for Industrial  
332 Automation and Control Systems – Part 2-3: Patch Management in the IACS Environment*)

333 [5], and NIST SP 800-53 (*Security and Privacy Controls for Federal Information Systems*  
334 *and Organizations*) [6].

335  
336

**Table 2-1 Mapping of Cybersecurity Framework Functions Addressed by BAD Capabilities to the Manufacturing Profile**

| Function  | Category                            | Subcategory    | Manufacturing Profile  | Reference   |
|---|-------------------------------------|----------------|--|---|
| <b>Detect</b>   | <b>Anomalies and Events (DE.AE)</b> | <b>DE.AE-2</b> | <b>Low</b>   | 62443-2-1:2009<br>4.3.4.5.6,<br>62443-2-3:2015<br>SR 2.8, 2.9 |
|   |                                     |                | Review and analyze detected events within the manufacturing system to understand attack targets and methods  | <a href="#">AU-6</a><br><a href="#">IR-4</a>                  |
|   |                                     |                | <b>Moderate and High</b>   |   |
|   |                                     |                | Employ automated mechanisms, where feasible, to review and analyze detected events within the manufacturing system   | <a href="#">AU-6(1)</a><br><a href="#">IR-4(1)</a>            |
|   |                                     | <b>DE.AE-3</b> | <b>Low and Moderate</b>  | 62443-3-3:2013<br>SR 6.1                                      |
|   |                                     |                | Ensure that event data is compiled and correlated across the manufacturing system by using various sources, such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports                                | <a href="#">IR-5</a>  |
|   |                                     |                | <b>High</b>  |   |
|   |                                     |                | Integrate the analysis of events, where feasible, with the analysis of vulnerability scanning information, performance data, manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity | <a href="#">AU-6(5)(6)</a><br><a href="#">AU-12(1)</a>        |
|   |                                     | <b>DE.AE-4</b> | <b>Low</b>   |   |
|   |                                     |                | Determine the negative impacts, resulting from detected events, to manufacturing operations, assets, and individuals, and correlate the impacts with the risk assessment outcomes  | <a href="#">RA-3</a>  |
|   |                                     |                | <b>Moderate</b>  |   |
|   |                                     |                | Employ automated mechanisms to support impact analysis   | <a href="#">IR-4(1)</a><br><a href="#">SI-4(2)</a>            |
| <b>High</b>   |                                     |                |  |   |
| Correlate detected event information and responses to achieve perspective on the event's impact across the organization | <a href="#">IR-4(4)</a>             |                |  |   |

337

338 **3. Demonstration Environment Architecture**

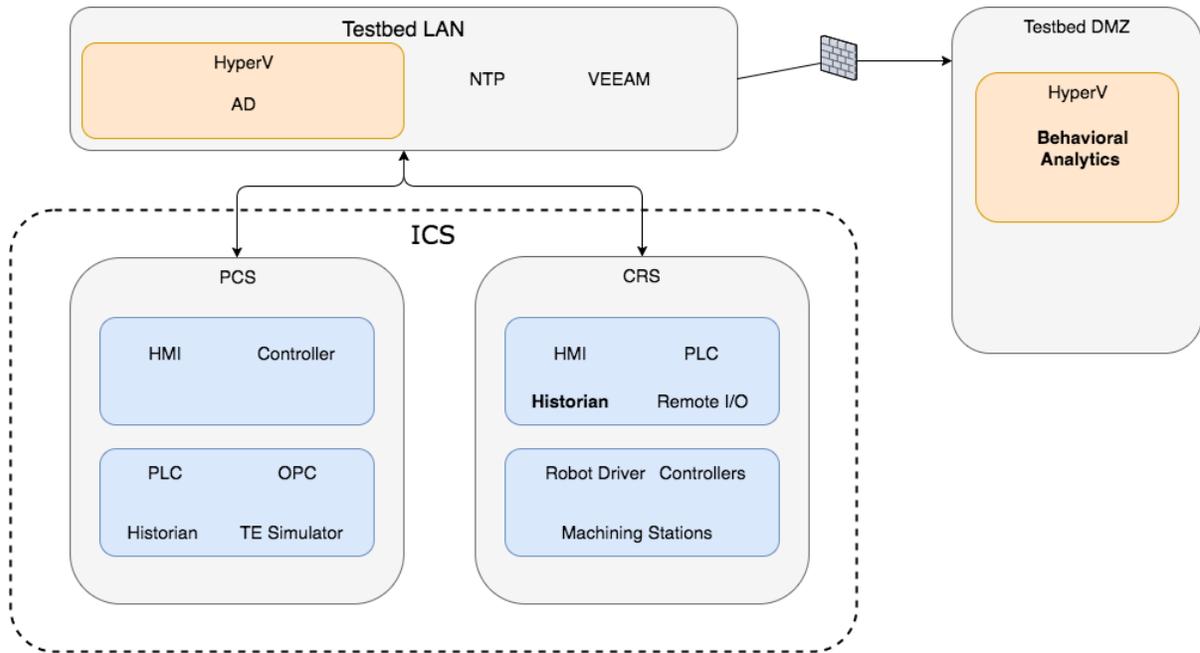
339 The Cybersecurity for Smart Manufacturing Systems (CSMS) demonstration environment  
340 emulates real-world manufacturing processes and their ICS by using software simulators and  
341 commercial off-the-shelf hardware in a laboratory environment [7]. The CSMS environment  
342 was designed to measure the performance impact on ICS that is induced by cybersecurity  
343 technologies. The PCS and the collaborative robotic system (CRS) are the two systems used  
344 for the demonstration of BAD capabilities. The PCS and CRS demonstration enclaves are  
345 described in Sections 3.1 and 3.2.

346 Figure 3-1 depicts a high-level architecture for the BAD demonstration environment. The  
347 capabilities that are introduced in the demonstration environment are bolded in Figure 3-1  
348 and address the Cybersecurity Framework functions and subcategories listed in Table 2-1.

349 The local area network (LAN), a firewalled-off cybersecurity tool environment  
350 (demilitarized zone [DMZ]), and two ICS environments make up the existing architecture of  
351 the CSMS demonstration environment. The LAN consists of a hypervisor for virtualization, a  
352 network time protocol (NTP) server for time synchronization, a server for backup and  
353 storage, and a virtualized Active Directory server for domain services. Within the  
354 demonstration environment's DMZ, there is a hypervisor that allows cybersecurity tools to  
355 be deployed within an isolated environment.

356 Within this architecture, the BAD capability is introduced in two areas that use four  
357 collaborator products. Two BAD systems are installed within the demonstration  
358 environment's DMZ. One of these BAD systems is agent-based and is installed at multiple  
359 endpoints within the CRS and the PCS, while data is aggregated at the demonstration  
360 environment's DMZ. The other BAD system is implemented as an additional capability to  
361 the historian within the CRS only. This build consisted of performing and introducing the  
362 BAD capability into the CRS and PCS environments, one product at a time. In other words,  
363 only one product was installed and performing BAD at any given time. Each collaborator's  
364 product installation was scheduled to run in sequence to ensure complete autonomy from  
365 each product in the build.

366 **Figure 3-1 BAD High-Level Architecture**



367

368 **3.1. Collaborative Robotic System**

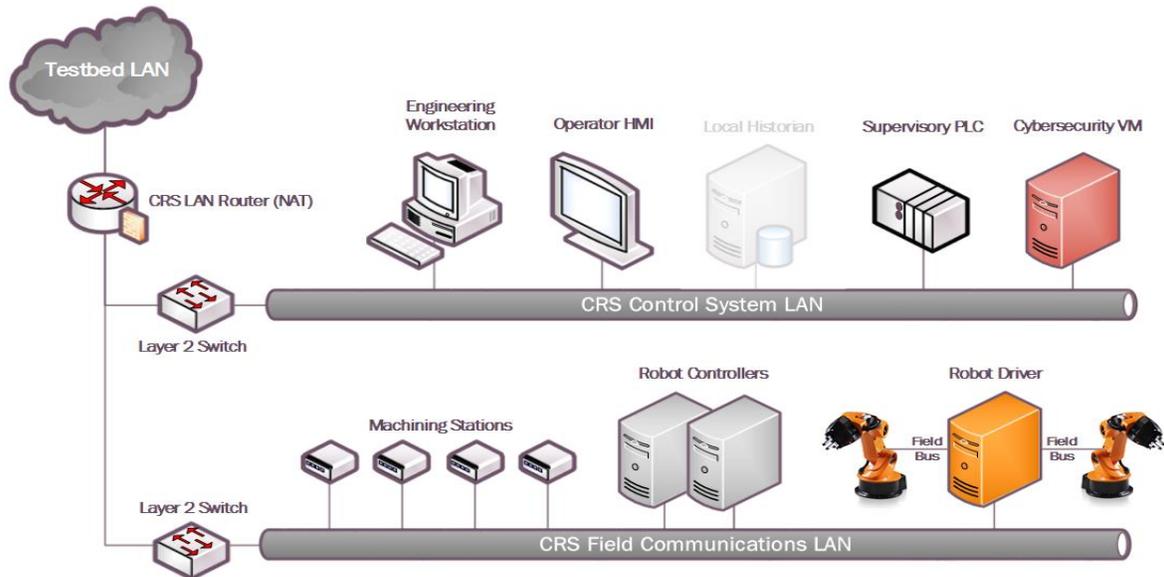
369 The CRS enclave of the environment is composed of two robotic arms that emulate a  
370 material-handling application known as “machine tending” [8]. Robotic machine tending  
371 uses robots to interact with the machinery, performing operations that a human operator  
372 would normally perform (e.g., loading and unloading parts, opening and closing machine  
373 doors, activating operator control-panel buttons). The robots operate in concert according to a  
374 material-handling procedure that changes dynamically based on feedback from the simulated  
375 machining operations. An architecture of the robotic enclave network is shown in Figure 3-2.

376 The robot controllers can operate in one of two modes: deployed or virtualized. In the  
377 deployed mode, each robot is controlled on a dedicated Dell PowerEdge R420 server running  
378 the robot operating system (ROS) on top of Ubuntu Linux. In the virtualized mode, each  
379 robot is controlled by virtualized servers within a hypervisor running on a Dell PowerEdge  
380 620 server. The deployed mode supports experiments with a pseudo-ideal configuration. The  
381 virtualized mode supports experiments with a resource-restricted configuration and can  
382 maintain independent demonstration environments.

383 The pseudo-ideal configuration provides the robot controller software with computational  
384 resources that are well beyond the minimum requirements for unimpeded operations.  
385 Operating in this manner is reserved for experiments that do not require server performance  
386 impacts to be measured (e.g., network-specific experiments). The resource-restricted  
387 configuration allows the researchers to restrict the available resources to the robot controller  
388 software and underlying OS (e.g., memory allocation, available hard-disk space, hard-disk  
389 access rates, number of central processing unit [CPU] cores).

390 The hypervisor also allows software-based cybersecurity tools to be deployed within an  
391 isolated environment, and allows for the ability to restore the enclave environment to a  
392 known-good state, reducing the chances of cross-contamination by residual software modules  
393 or services remaining within a virtual machine (VM) post-experiment. Software-based  
394 cybersecurity tools are installed on VMs dedicated to specific experiments within the  
395 hypervisor and are archived. This allows any tool to be recalled for any experiment that  
396 requires its execution.

397 **Figure 3-2 Robotic Assembly Enclave Network**



398

### 399 **3.1.1. CRS Network Architecture**

400 In addition to the two industrial robots, the enclave includes a supervisory programmable  
401 logic controller (PLC), a human-machine interface (HMI), several servers for executing  
402 required computational resources and applications, a cybersecurity virtual machine  
403 (CybersecVM), and an engineering workstation.

404 The CRS enclave LAN is constructed as a hierarchal architecture. For the BAD  
405 implementation, the reconfigurable design of the enclave enabled the implementation of  
406 network segmentation and security perimeters. The local network traffic (CRS LAN) is  
407 managed by a Siemens RUGGEDCOM RX1510, and the high-level environment traffic  
408 (environment LAN) and its connection to the “corporate network” are managed by a Cisco  
409 ASA 5512-X.

410 The CRS LAN has numerous machines that directly operate and support the operation of the  
411 enclave. The robot controllers or driver servers execute the operational code and  
412 communicate directly with the robots to direct their actions. The supervisory PLC  
413 communicates the status of the machining stations and operator controls to the robot  
414 controllers, and of part tracking for manufacturing performance measurements. The operator  
415 HMI also communicates with the PLC to display manufacturing process information and  
416 performance measurements to the operator. The engineering workstation hosts the  
417 programming environment and debugging tools that are used to modify the robot code and to

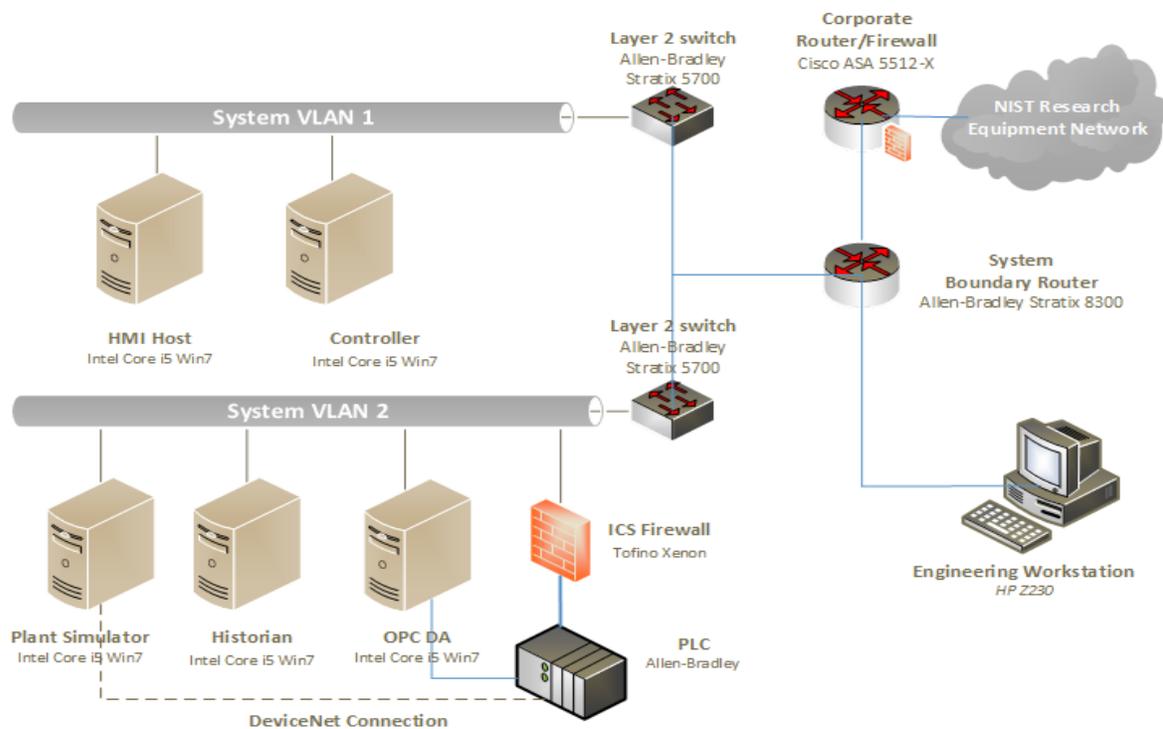
418 give terminal-level access to other machines within the enclave. The HyperV server provides  
419 server virtualization to the enclave, allowing researchers to create servers on demand, as  
420 required by specific software tools or packages.

### 421 3.2. Process Control System

422 The PCS enclave emulates an industrial continuous manufacturing system, a manufacturing  
423 process to produce or process materials continuously, where the materials are continuously  
424 moving, going through chemical reactions, or undergoing mechanical or thermal treatment.  
425 Continuous manufacturing usually implies a 24/7 (24 hours a day, seven days a week)  
426 operation with infrequent maintenance shutdowns and is contrasted with batch  
427 manufacturing. Examples of continuous manufacturing systems are chemical production, oil  
428 refining, natural-gas processing, and wastewater treatment [9]. An architecture of the PCS  
429 network is depicted in Figure 3-3.

430 **Figure 3-3 PCS Network Architecture**

## Process Control System Network Diagram



431

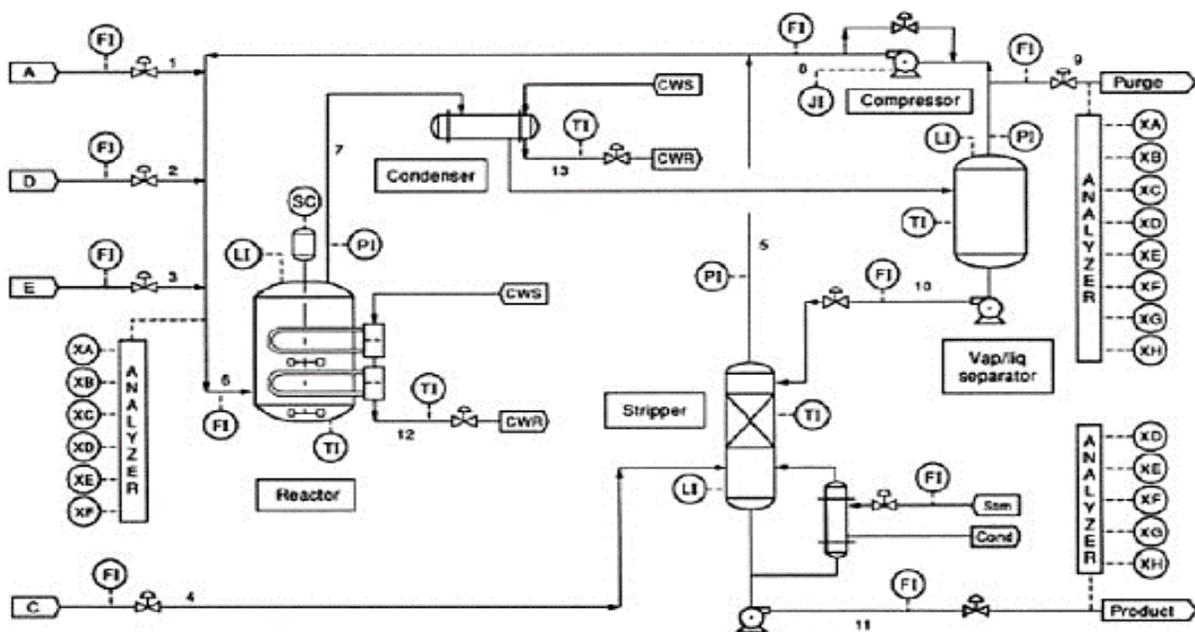
432 The PCS includes a software simulator to emulate the Tennessee Eastman (TE) chemical  
433 reaction process. The TE problem, presented by Downs and Vogel [10], is a well-known  
434 process-control problem in continuous chemical manufacturing. The TE control problem was  
435 chosen as the continuous process model for several reasons. First, the TE model is a  
436 well-known plant model that is used in control-systems research, and the dynamics of the  
437 plant process are well understood. Second, the process must be controlled; otherwise,  
438 perturbations will drive the system into an unstable state. The inherent unstable open-loop

439 operation of the TE process model presents a real-world scenario in which a cybersecurity  
 440 attack could represent a real risk to human safety, environmental safety, and economic  
 441 viability. Third, the process is complex, nonlinear, and has many degrees of freedom by  
 442 which to control and perturb the dynamics of the process. Finally, numerous simulations of  
 443 the TE process have been developed with readily available reusable code. We chose the  
 444 University of Washington Simulink controller design by Ricker [11]. The Ricker Simulink  
 445 model was chosen for its multiloop control architecture, making distributed control  
 446 architectures viable. It accurately matches the Downs and Vogel model, and the control code  
 447 is easily separable from the plant code.

448 The TE process model is illustrated in Figure 3-4. Downs and Vogel did not reveal the actual  
 449 substances used in the process; instead, they used generic identifiers for each substance. The  
 450 process produces two products (G and H) from four reactants (A, C, D, and E). The process  
 451 is defined as irreversible and exothermic, and the reaction rates of the four reactants are a  
 452 function of the reactor temperature. The process is broken down into five major operations: a  
 453 reactor, a product condenser, a vapor-liquid separator, a product stripper, and a recycle  
 454 compressor. The PCS is housed in a 19-inch rack system. The model has 12 actuators for  
 455 control and 41 sensors for monitoring. The process description is summarized below.

456 As previously mentioned, the reaction rates of the reactants are a function of the reactor  
 457 temperature. The gaseous reactants are combined in the reactor to form liquid products. The  
 458 reactor temperature is then cooled by using an internal cooling bundle. The reactor product  
 459 passes through the condenser to the separator. The vapor-liquid separator then separates  
 460 unreacted gases from the liquid products. The unreacted gases are sent back to the reactor  
 461 by the recycle compressor. The remaining reactants are removed in a stripping column. Finally,  
 462 the two end products are sent downstream for further refining and separation.

463 **Figure 3-4 TE Process Control Model**



464

### 465 3.2.1. PCS Network Architecture

466 The PCS includes a software simulator to emulate the TE chemical reaction process. The  
467 simulator is written in C code and is executed on a computer running Windows 7. In  
468 addition, the system includes a PLC, a software controller implemented in MATLAB, an  
469 HMI, an object linking and embedding for process control (OPC) data access (DA) server, a  
470 data historian, an engineering workstation, and several virtual LAN switches and network  
471 routers.

472 The PCS network is segmented from the demonstration network via a boundary router. The  
473 router is using a dynamic routing protocol, Open Shortest Path First, to communicate with  
474 the main demonstration environment router. All network traffic needs to go through the  
475 boundary router to access the main demonstration network. There are two virtual network  
476 segments in the system. Each network is managed by an Ethernet switch. The HMI and the  
477 controller are in Virtual Local Area Network (VLAN)-1, while the plant simulator, data  
478 historian, OPC DA server, and PLC are in VLAN-2. VLAN-1 simulates a central  
479 control-room environment in which the HMI and the controllers are virtually located in the  
480 same network segment. VLAN-2 simulates the process operation environment, which  
481 typically consists of the operating plant, PLCs, OPC DA server, and data historian. These  
482 network switches and routers are highly reconfigurable and therefore allow the system to  
483 implement various network topologies for demonstration.

484 A Tofino Xenon security appliance, a firewall specially designed for ICS application, is  
485 installed to protect the PLC. The firewall rules are configured to allow only certain network  
486 nodes and specific protocols to access the PLC, and to deny all other traffic. All of the  
487 computer nodes in the system have the Windows firewall enabled. Rules are configured to  
488 allow computer access to only traffic specific to their applications. For example, the firewall  
489 of the OPC DA server computer allows only a restricted range of remote procedure call and  
490 Distributed Component Object Model (DCOM) ports for the OPC clients to access, and it  
491 restricts the source Internet Protocol (IP) address of the OPC clients.

492 The plant simulator is implemented in C code, which was based on the Fortran code  
493 originally developed by Downs and Vogel. The plant simulator requires a controller to  
494 provide a control loop in order to operate continuously. A decentralized controller  
495 implemented in Simulink, developed by Ricker, is used as the process controller. The Ricker  
496 implementation accurately matches the plant simulator, and the controller is a separate  
497 software process that runs on a separate computer from the plant simulator. To provide  
498 communication between the plant simulator and the controller, a hardware PLC with an  
499 industrial network protocol capability is used. The industrial network protocol is used to  
500 communicate between the plant simulator and the PLC. The plant simulator sends its sensor  
501 information to the controller, and the controller algorithm uses the sensor inputs to compute  
502 the desired values of the actuators and then sends those values back to the plant simulator.

503 In the plant simulator computer, a multinode DeviceNet card was installed. DeviceNet is a  
504 common industrial protocol that is used in the automation industry to exchange data between  
505 control devices. The multinode card allows a single hardware device to emulate multiple  
506 virtual DeviceNet nodes. In this case, each sensor and actuator point are dedicated nodes.  
507 Therefore, 53 virtual nodes (41 for sensors and 12 for actuators) were configured in the

508 system. A software interface was developed to send and receive sensor and actuator values  
509 between the plant simulator and the PLC, through DeviceNet. An OPC DA server is running  
510 on a Windows 7 computer, acting as the main data gateway for the PLC. The PLC  
511 communicates to the OPC DA server to update and retrieve all of the sensor and actuator  
512 information, respectively. This sensor and actuator information is also known as a “tag” in  
513 PLC terminology. The controller has a MATLAB Simulink interface that directly  
514 communicates with the OPC DA server.

515 An HMI and a data historian are implemented in the system. The HMI provides a graphical  
516 user interface (GUI) to present information to an operator or user about the state of the  
517 process. The data historian serves as the main database to record all of the process sensor and  
518 actuator information. Both the HMI and the data historian have built-in interfaces to establish  
519 connections to the OPC DA server to access all of the process information. An engineering  
520 workstation is used in the system for engineering support, such as PLC development and  
521 control, HMI development and deployment, and data-historian data retrieval.

522 All systems in the PCS are synchronized with the NTP server environment. A network  
523 packet analyzer tool is installed in all of the computers in the system to capture and analyze  
524 network packets. Other specialized software tools are also used to monitor the system. For  
525 example, an OPC data analyzer is used to monitor OPC data exchange, and DeviceNet  
526 logging is used to log DeviceNet-level traffic.

### 527 **3.3. Behavioral Anomaly Detection Capabilities Demonstrated**

528 The BAD capability was demonstrated by installing single products into each environment.  
529 Only one product was installed and performing BAD at any given time. The BAD capability  
530 is achieved by three different detection methods: network-based, agent-based, and  
531 historian/sensor-based. CyberX and SecurityMatters SilentDefense demonstrated  
532 network-based detection. Secure-NOK’s SNOK Detector demonstrates agent-based  
533 detection. The OSIsoft Process Information (PI) System’s PI Data Archive (historian)  
534 demonstrates sensor-based detection from historian data.

#### 535 **3.3.1. SecurityMatters SilentDefense**

536 SecurityMatters SilentDefense utilizes sensors to passively sniff traffic at the Layer 3 peer-  
537 to-peer switches to monitor critical networks for anomalies. The SilentDefense product also  
538 uses a command center to manage and collect data from all sensors at an enterprise site. The  
539 installation and configuration procedures undertaken for the SecurityMatters SilentDefense  
540 product are provided in Appendix A.

#### 541 **3.3.2. Secure-NOK SNOK**

542 Secure-NOK’s SNOK is a cybersecurity monitoring and detection system tailored for  
543 industrial networks and control systems. SNOK utilizes nonintrusive endpoint monitoring  
544 agents and passive network monitoring from Layer 2 and Layer 3 switches. The SNOK  
545 network intrusion detection system (IDS) comes preinstalled on an appliance, and endpoint  
546 monitoring agents are integrated into the asset owner’s environment. The installation and  
547 configuration procedures undertaken for the Secure-NOK SNOK appliance are provided in  
548 Appendix B.

549 **3.3.3. CyberX**

550 The CyberX platform delivers continuous operational technology (OT) threat monitoring and  
 551 asset discovery, combining a deep understanding of industrial protocols, devices, and  
 552 applications with OT-specific behavioral analytics, threat intelligence, risk and vulnerability  
 553 management, and automated threat modeling. The platform is delivered as a preconfigured  
 554 appliance, including the IP address, subnet mask, default gateway, and Domain Name  
 555 System (DNS) servers utilized in the build environment. The installation and configuration  
 556 procedures undertaken for the CyberX appliance are provided in Appendix C.

557 **3.3.4. OSIsoft PI Data Archive**

558 The OSIsoft PI System’s PI Data Archive is a component of the PI System that retrieves,  
 559 archives, and enables high-performance data storage and rapid retrieval by using minimal  
 560 disk space. The installation and configuration procedures undertaken for OSIsoft’s PI System  
 561 software are provided in Appendix D.

562 **3.4. Behavioral Anomaly Detection Methods and Security Functions**

563 Table 3-1 identifies methods used in this project and provides a mapping between the method  
 564 type, the function performed, and the security control(s) provided. Refer to Table 2-1 for an  
 565 explanation of the Cybersecurity Framework subcategory codes.

566 **Table 3-1 BAD Methods and Security Functions**

| Type                   | Function   | CSF Subcategories  |
|------------------------|--|--|
| Network-based          | Identifies, monitors, and reports anomalous ICS traffic that might indicate a potential intrusion. Collects ICS network traffic via passive (agentless) monitoring. The system uses deep packet inspection to dissect traffic from both serial and Ethernet control network equipment.   | DE.AE-1,<br>DE.AE-2,<br>DE.AE-5,<br>DE.CM-1,<br>DE.CM-4,<br>DE.CM-7,<br>DE.DP-4  |
| Historian/sensor-based | Gathers raw data, records process data, and creates calculations. Provides monitoring and performance alerts of the process historian. The historian accesses historical data and consolidates it with current, real-time data. It allows for investigating intermittent issues, troubleshooting equipment failures, comparing current versus past production performance, and measuring new-plant startups against existing facilities. | Does not support a NIST Cybersecurity Framework subcategory in and of itself. It provides the data to be monitored by the ICS behavior monitor (next item).<br><br>Related subcategories:<br>DE.AE-5,<br>DE.CM-1 |

| Type        | Function   | CSF Subcategories   |
|-------------|--|---|
| Agent-based | Identifies, monitors, and reports anomalous ICS traffic that might indicate a potential intrusion. Uses nonintrusive software agents to monitor the ICS network that requires no updating. The network IDS passively collects data from the ICS / Supervisory Control and Data Acquisition (SCADA) network via Switch Port Analyzer (SPAN)/mirroring ports. The nonintrusive host-monitoring agents collect data from within endpoints. The agents send event information to the detector, which looks for early warnings of cybersecurity attacks, and alerts on the anomalies detected by using a web interface. | DE.AE-1,<br>DE.AE-2,<br>DE.AE-5,<br>DE.CM-1,<br>DE.CM-4,<br>DE.CM-7,<br>DE.DP-4 |

567

### 568 3.5. Typographic Conventions

569 Table 3-2 presents the typographic conventions used in this NISTIR's descriptions of  
570 scenarios and demonstration findings.

#### 571 Table 3-2 Typographic Conventions

| Typeface/Symbol           | Meaning   | Example   |
|---------------------------|---|---|
| <i>Italics</i>            | file names and path names; references to documents that are not hyperlinks; new terms; and placeholders | For detailed definitions of terms, see the <i>CSRC Glossary</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                   | Mkdi r  |
| <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 Uniform Resource Locator (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> . |

## 572 4. Demonstration Scenarios and Findings

573 With both the robotic and process-control infrastructures available for immediate use, the  
574 implementation of the BAD capabilities consisted of installing and integrating a single tool  
575 with the existing infrastructures. The BAD products are installed within the demonstration  
576 environment's DMZ of the existing infrastructure.

577 **4.1. Network-Based Behavioral Anomaly Detection**

578 Network-based anomaly detection requires the aggregation of all network traffic into a single  
579 collection point. Multiple appliances can also be used with centralized management to collect  
580 network traffic data from different zones and sites. Network traffic is examined and  
581 compared with a preexisting baseline, which is assumed to be normal at the time that it is  
582 captured. Should the network traffic show deviations from this baseline or show any other  
583 types of behavior considered suspicious or unauthorized, an alert will be generated based on  
584 preconfigured parameters.

585 During network-based anomaly detection, network traffic from the CRS and PCS LAN  
586 networks is aggregated at the demonstration environment's DMZ via SPAN ports. At the  
587 demonstration environment's DMZ, the traffic is inspected by the CyberX and SilentDefense  
588 platforms. Once a baseline of network traffic is established as normal, this aggregation of  
589 traffic can show deviations from the baseline, triggering an alert based on preconfigured  
590 parameters. Parameters can be configured to trigger alerts relating to network-traffic  
591 deviations, user-behavior deviations, volumetric deviations, and protocol deviations.

592 **4.2. Agent-Based Behavioral Anomaly Detection**

593 Agent-based anomaly detection combines some of the features of network-based anomaly  
594 detection with the nonintrusive monitoring of endpoints. Agent-based anomaly detection uses  
595 distributed software agents installed onto or close to devices, such as servers, HMIs, network  
596 switches, and controllers. Agents collect and preprocess device information, such as the use  
597 of removable media; logged-in users; ingress/egress traffic; device configurations; process  
598 and program details; and device parameters, such as memory, disk, and processor utilization.  
599 The collected information is sent securely to a detection engine. The detection engine alerts  
600 on deviations from preconfigured security policies and preexisting baselines. The preexisting  
601 baselines are reviewed and accepted as normal at the time that they are captured.

602 During agent-based anomaly detection, the behavior of Windows 7 devices in the PCS  
603 network, and of Ubuntu Linux devices in the CRS network, was monitored. The host agent  
604 information and network traffic are inspected by the Secure-NOK SNOK Detector. Once a  
605 baseline of the device configuration and behaviors is established as normal, deviations will  
606 trigger alerts.

607 **4.3. Historian-Based and Sensor-Based Behavioral Anomaly Detection**

608 Operational historian/sensor-based anomaly detection relies on the collection of sensor data  
609 into ICS network components, such as operational historians. Because historians are  
610 constantly being fed real-time operational data, which has already been configured within  
611 operational bounds, or set points, any deviations from these thresholds will produce an alert  
612 that can be captured. Typically, this would be considered an operational anomaly. OSIsoft's  
613 PI Data Archive performs historian/sensor-based detection.

#### 614 **4.4. Demonstration Results and Findings**

615 The demonstration effort examined 16 classes of BAD. These 16 classes for which  
616 anomalous events were successfully detected include the detection of the following items:

- 617 • plaintext passwords
- 618 • user authentication failures
- 619 • new network devices
- 620 • abnormal network traffic between devices
- 621 • internet connectivity
- 622 • data exfiltration
- 623 • unauthorized software installations
- 624 • PLC firmware modifications
- 625 • unauthorized PLC logic modifications
- 626 • file transfers between devices
- 627 • abnormal ICS protocol communications
- 628 • malware
- 629 • denial of service (DoS)
- 630 • abnormal manufacturing system operations
- 631 • port scans/probes
- 632 • environmental changes

633 Each of the demonstration events addressed threats that would not normally be detected by  
634 current security tools that involve monitoring system behaviors for predefined out-of-  
635 specification settings or readings or that involve threat signatures (information elements  
636 previously identified as being associated with threats or vulnerability characteristics, such as  
637 with an IDS or an intrusion protection system). Network-based, agent-based, and  
638 historian/sensor-based detection capabilities were examined. Each product that was  
639 demonstrated performed as expected.

640 As indicated in Section 4.1, individual products were examined in different scenarios, and  
641 not all types of detection events were examined in each scenario. As a result, no comparison  
642 of product detection capabilities can usefully be made or is appropriate to this NISTIR.

643 The installation, configuration, anomaly scenarios, and results for each tool are described in  
644 the appendixes of this document.

#### 645 **5. Conclusion**

646 The goal of this project was to demonstrate BAD techniques that businesses can implement  
647 and use to strengthen the cybersecurity of their manufacturing processes. The BAD project  
648 demonstrated three different detection methods: network-based, agent-based, and operational  
649 historian/sensor-based. We have shown that BAD techniques can serve as a key security  
650 component in sustaining ICS operations. This NISTIR illustrates the use of the different  
651 BAD capabilities, to provide a better understanding of what each of the techniques offers and  
652 how to apply each of these techniques in different ICS network environments.

653 **Appendix A. SecurityMatters SilentDefense Supplemental Information**

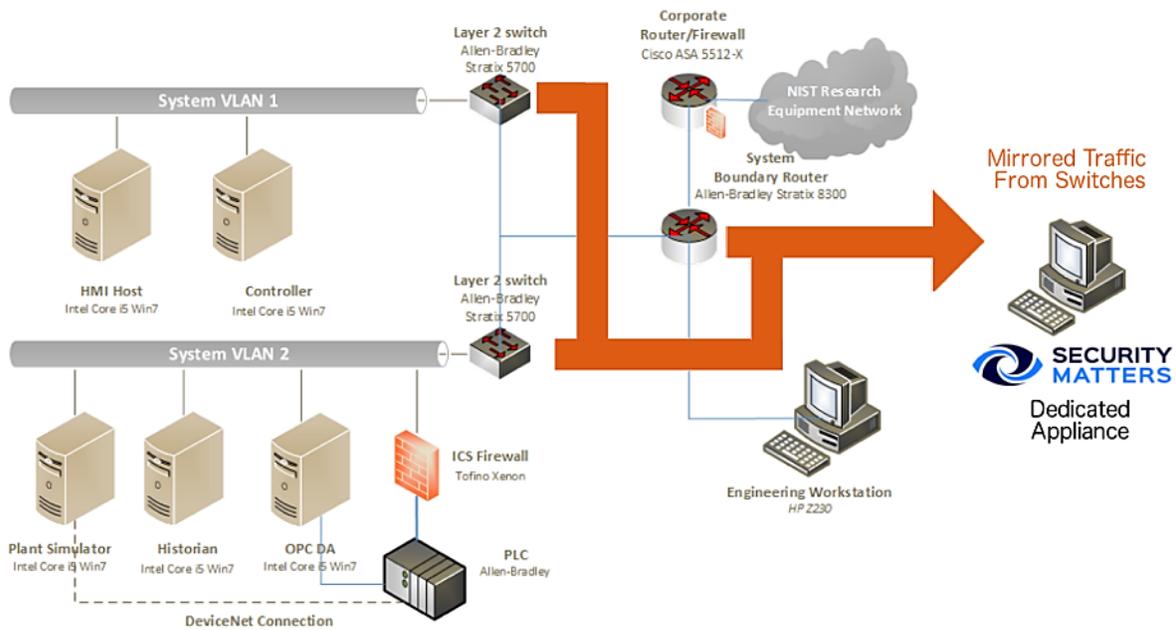
654 SecurityMatters SilentDefense utilizes sensors to passively sniff traffic at the Layer 3 peer-  
655 to-peer switches to monitor critical networks for anomalies. The SilentDefense product also  
656 uses a command center to manage and collect data from all network-based sensors within a  
657 manufacturing system.

658 **A.1. Build Architecture**

659 The SilentDefense dedicated appliance was physically installed in the measurement rack of  
660 the Cybersecurity for Smart Manufacturing Systems (CSMS) environment. Three existing  
661 Switch Port Analyzer (SPAN) ports from each system (collaborative robotic system [CRS]  
662 and process control system [PCS]) were connected to dedicated network interfaces on the  
663 appliance, for a total of six SPAN ports. The SPAN port connections to the appliance, within  
664 the PCS and CRS networks, are shown in Figure A-1 and Figure A-2, respectively.

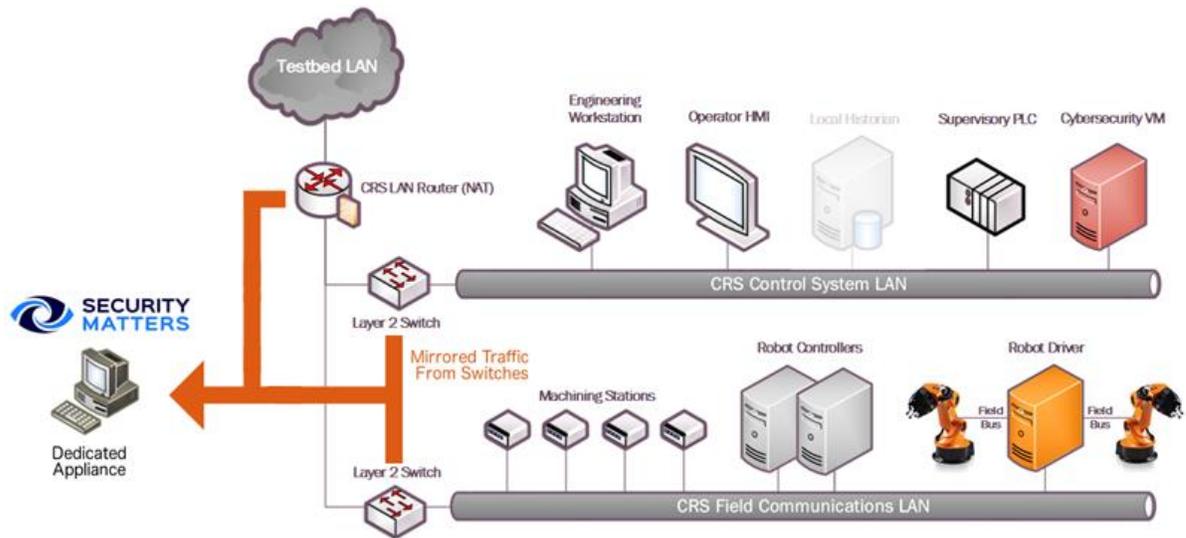
665 The appliance network connection was connected to the demilitarized zone (DMZ) network  
666 located in the test bed’s measurement rack, to isolate the appliance’s network traffic from the  
667 rest of the network. Engineering laptops were used to interface with the SilentDefense  
668 graphical user interface (GUI) via network connections to the DMZ. More information  
669 regarding the specific configuration of the test-bed network can be found in Section 3.

670 **Figure A-1 SPAN Port Connections to the SilentDefense Appliance in the PCS**



671

672 **Figure A-2 SPAN Port Connections to the SilentDefense Appliance in the CRS**



673

## 674 **A.2. Installation and Configuration**

675 Physical hardware and software were provided by SecurityMatters for this demonstration.  
676 After the hardware appliance was received, it was installed into the CSMS test bed. Soon  
677 after the initial installation, engineers from SecurityMatters arrived on site to complete the  
678 installation and configuration of the tool. The following subsections describe the steps taken  
679 to install and configure the appliance.

### 680 **A.2.1. Hardware**

681 The SilentDefense appliance was installed as a bundle (with the sensor and the command  
682 center on the same hardware). Typically, these functions are separated in production  
683 installations; however, because this was a lab system, the bundle was sufficient for the  
684 demonstration environment. The bundled hardware was a Dell R630 1U Rackmount Server  
685 with the following specifications:

- 686 • central processing unit (CPU): Intel Xeon E5-2620, 2.4 gigahertz, 5-megabyte (M)  
687 cache, 6C/12T (6 cores and 12 threads)
- 688 • random-access memory: 32 gigabytes (GB), registered dual in-line memory module,  
689 2,400 megatransfers per second
- 690 • hard drive: 800 GB, solid-state drive
- 691 • redundant array of independent disks controller: PERC H730, 1 GB cache
- 692 • sniffing network interface card (NIC): Intel i350 Quad Port Peripheral Component  
693 Interconnect Express Card

### 694 **A.2.2. Operating System**

695 SilentDefense 3.11.1 uses the Ubuntu 16.04.3 Long-Term Support (LTS) Server operating  
696 system (OS), which is modified with two scripts. First, there is a SecurityMatters OS update  
697 script to update libraries to the latest versions and to install some new libraries necessary for  
698 SilentDefense operation. The OS is then modified with a main-configuration script, which

699 hardens the OS by performing operations, such as disabling users, setting iptables, and  
700 setting the update repository addresses to local hard-drive folders (so that, automatic updates  
701 are not from the internet). The steps for modifying the OS are as follows:

- 702 1. Install the Ubuntu 16.04.3 LTS Server OS.
- 703 2. Run the SilentDefense OS by using the following command:

```
704 sudo ./update_os_16.04.3_to_29.11.2017.run
```

- 705 3. Reboot the system by using the following command:

```
706 sudo reboot now
```

- 707 4. Run the SilentDefense main-configuration script by using the following command:

```
708 sudo ./main_configuration_29.11.2017.run
```

### 709 **A.2.3. Configure Sniffing Ports**

710 The Intel i350 card has four sniffing ports to configure. This configuration is done through  
711 the SilentDefense `sdconfig` utility:

- 712 1. Run the SilentDefense configuration utility by using the following command:

```
713 sudo sdconfig
```

- 714 2. Choose the option **Configure New Monitoring Interface**.
- 715 3. Select the four Intel i350 NIC interfaces by using the space bar on your keyboard.
- 716 4. Click **OK**.
- 717 5. Choose the option **Exit this configuration Utility**.

### 718 **A.2.4. Configure the Management Port Internet Protocol Address**

719 The SilentDefense system has a management port that is used to connect to the sensors and  
720 for the SilentDefense administrators and analysts to access the system GUI. This  
721 configuration is done through the SilentDefense `sdconfig` utility:

- 722 1. Run the SilentDefense configuration utility by using the following command:

```
723 sudo sdconfig
```

- 724 2. Choose the option **Remove management interface configuration**.
- 725 3. Choose the option **Configure management interface**.
- 726 4. Type in the following information:
  - 727 a. **IP address** (Internet Protocol address)

- 728           **b. subnet mask**
- 729           **c. gateway**
- 730           **d. Domain Name System server(s)**

731           5. Press **OK**.

### 732   **A.2.5. Configure the SPAN Ports on Layer 3 Network Switches**

733   The SilentDefense passive monitoring system uses SPAN ports to intercept and analyze  
734   network packets. The process to configure a SPAN port varies among different makes and  
735   models of networking hardware. For SPAN port configuration information, consult the  
736   current configuration manual or user guide for the specific networking hardware.

### 737   **A.2.6. Log into SilentDefense**

738   The SilentDefense GUI has a default username and password of `admin`. Upon the first login,  
739   you are required to change the password to something more secure. The SilentDefense  
740   software will not allow the new username and password to be the same.

- 741           1. Browse to the SilentDefense GUI from a web browser, using the following Uniform  
742           Resource Locator (URL):

```
743           https://<mgmt_ip_address>
```

- 744           2. Type the username `admin` and the password `admin` in the login fields, and then click  
745           **Sign in**.
- 746           3. A new window pops up, requiring you to change the password. Type in a new  
747           password that meets the following requirements:
  - 748               a. Contains eight characters minimum
  - 749               b. Does not contain the account name
  - 750               c. Contains at least three character groups (e.g., uppercase, lowercase, number,  
751               special)
- 752           4. Click **Apply**.
- 753           5. The dashboard now appears, and you can begin to use SilentDefense.

### 754   **A.3. Anomaly Scenarios**

755   The network-based anomaly detection method was demonstrated for the scenarios detailed in  
756   the following subsections. Each scenario includes a description of the anomaly, a detailed  
757   description of how each demonstration event was conducted in the CSMS environment, and  
758   the observed results.

759 For the sake of brevity, only a subset of the alerts observed during each anomaly scenario is  
 760 shown. However, each anomaly scenario includes a screenshot of the alerts summary (or  
 761 aggregated summary) observed after the anomaly scenario had completed.

### 762 A.3.1. Unencrypted Passwords Are Used to Access a Networking Device

763 Unencrypted or plaintext passwords transmitted over a network are a vulnerability for  
 764 industrial control system (ICS) networks. If packets containing these credentials are  
 765 intercepted, then the passwords can be easily unmasked and can be used to obtain  
 766 unauthorized access to devices or services that use those credentials. This vulnerability can  
 767 be amplified if multiple devices utilize the same credentials.

768 This anomaly was executed on the PCS. The network switches and router provide a Telnet  
 769 service for remote management. This protocol transmits user credentials as plaintext. A  
 770 Telnet connection was opened between the engineering workstation and Virtual Local Area  
 771 Network (VLAN)-1 by using the open-source PuTTY [12] client.

| Alert ID         | 3270  |
|------------------|---|
| Timestamp        | Dec 7, 2017 14:50:04  |
| Sensor name      | Local   |
| Detection engine | Industrial threat library (ITL)   |
| ID and name      | !l_sec_p_telnet - Use of insecure protocol (TELNET)   |
| Description      | Insecure protocol: the use of TELNET has been blacklisted in the Industrial Threat Library because TELNET is considered insecure (all data is exchanged in clear). Consider using SSH instead |
| Severity         | High  |
| Source MAC       | 40:A8:F0:3D:48:AE (HewlettP)  |
| Destination MAC  | E4:90:69:3B:C2:C0 (Rockwell)  |
| Source IP        | 172.16.3.10 (fgs-47631ehh.lan.lab)  |
| Destination IP   | 172.16.1.3  |
| Source port      | 50204   |
| Destination port | 23  |
| L2 proto         | Ethernet  |
| L3 proto         | IP  |
| L4 proto         | TCP   |
| L7 proto         | TELNET  |
| Status           | Not analyzed  |
| Labels           |   |

| IP address         | 172.16.3.10 (Private IP)   |
|--------------------|--|
| Host name          | fgs-47631ehh.lan.lab   |
| MAC addresses      | E4:90:69:3B:C2:C4 (Rockwell)<br>40:A8:F0:3D:48:AE (HewlettP)<br>E4:90:69:3B:C2:C5 (Rockwell)   |
| Role               | Master   |
| Other roles        | Windows workstation, Terminal client   |
| Vendor/model       | Rockwell   |
| OS version         | Windows 7 or Windows Server 2008 R2  |
| Client protocol(s) | DCOM (TCP 135, 49158, 49187, 49188)<br>DNS (UDP 53, 5355)<br>ETHIP (TCP 44818)<br>HTTP (TCP 80, 8530)<br>Kerberos (TCP 88)<br>LDAP (TCP 389)<br>LDAP (UDP 389)<br>NTP (UDP 123)<br>NetBIOS (UDP 137)<br>NoData (TCP 56224, 56614, 58847)<br>NotAKnownOne (TCP 1332, 3060, 3389)<br>NotAKnownOne (UDP 3702)<br>RDP (TCP 3389)<br>SMB (TCP 445)<br>SMB (UDP 138)<br>SSDP (UDP 1900)<br>SSH (TCP 22)<br>SSL (TCP 443, 3389)<br>Syslog (UDP 514) |

| Alert ID | Timestamp            | Description               | Sensor | Engine  | Severity     | Source IP          | Destination IP | Source Port | Destination Port | Protocol | Service      |
|----------|----------------------|---------------------------|--------|---------|--------------|--------------------|----------------|-------------|------------------|----------|--------------|
| 3270     | Dec 7, 2017 14:50:04 | Destination host not...   | Local  | Com...  | 8 - TCP c... | 172.16.3.10 (fg... | 172.16.1.3     | 50204       | 23 (TCP)         | TELNET   | Not analyzed |
| 3270     | Dec 7, 2017 14:50:04 | Use of insecure protoc... | Local  | Indu... | -            | 172.16.3.10 (fg... | 172.16.1.3     | 50204       | 23 (TCP)         | TELNET   | Not analyzed |

772

773

### 774 A.3.2. Transmission Control Protocol Connection Requests Are Received from 775 the Internet

776 When attempting to form a connection by using the transmission control protocol (TCP), a  
 777 connection request first must be sent to the server. If a TCP connection request is received  
 778 from the internet (i.e., it has a public Internet Protocol [IP] address), then this can indicate a  
 779 network misconfiguration, a device misconfiguration, or an unidentified internet connection  
 780 within the lower levels of the ICS network.

781 This anomaly was executed on the CRS. The packet manipulation tool Scapy [13] was used  
 782 with Python [14] to create a TCP SYN packet with a public IP as the source address  
 783 (129.6.1.10) and with the programmable logic controller (PLC) IP as the destination address,  
 784 and was injected into the CRS local area network (LAN).

The screenshot shows the SilentDefense™ interface with the following sections:

- Summary:** Alert ID 67467, Timestamp Jan 3, 2018 13:39:12, Sensor name Local, Detection engine Industrial threat library (ITL), ID and name ITL\_sec\_breach\_public\_ip\_attempt - Communication between public and private networks was attempted. Description: A host with a public IP address has attempted to communicate with a host that has a private IP address or vice versa. Public IP addresses are typically used by devices that can be accessed over the Internet and are not expected to communicate with private networks. Please verify that this is a legitimate communication. Severity: Medium.
- Source host info:** IP address 129.6.1.10 (Public IP), MAC addresses 00:15:5D:04:58:2B (Microsoft), Role Unknown, Client protocols FailedConnection (TCP 80), Purdue level 4 - Site business network, Criticality L.
- Destination host info:** IP address 192.168.0.30 (Private IP), MAC addresses 00:01:05:17:D8:08 (Beckhoff), Role PLC, Other roles Master, Slave, File server, Web server, Time server, Vendor/model Beckhoff, Client protocols MODBUS/TCP (TCP 502), NTP (UDP 123), NetBIOS (UDP 137), NetBIOS (TCP 139), NetBIOS (UDP 137), NoData (TCP 2217, 4116, 10924, 46204, 54411, 54981, 59328).
- Monitored networks:** Table with columns Name, Address, VLAN IDs. Row: RoboticsControlLAN, 192.168.0.0/24, any.

785

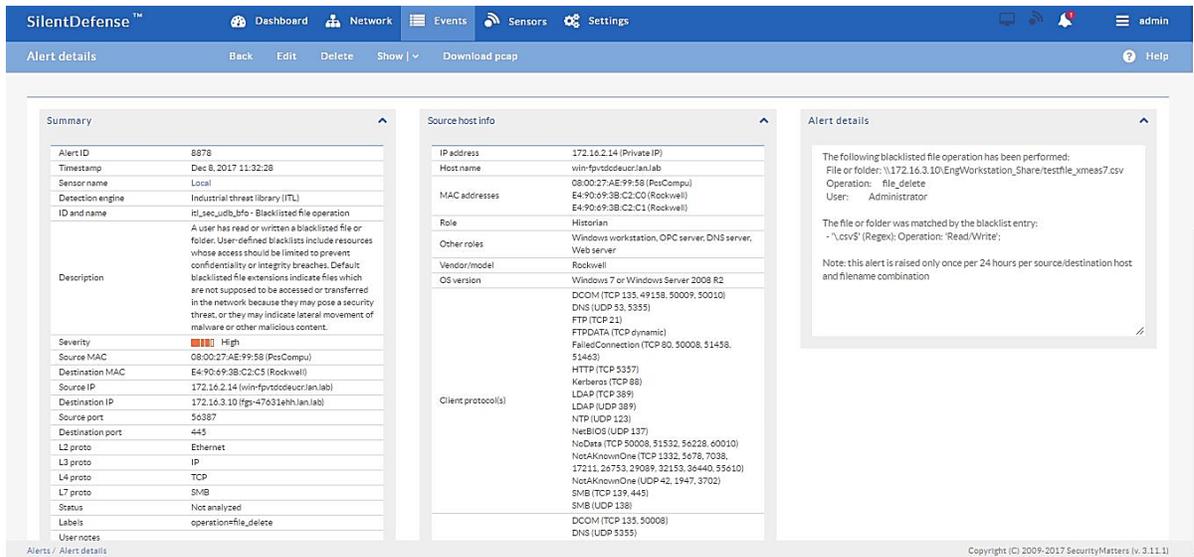
| Timestamp            | Event name(s)          | Sensor | Engine   | Profile | Status       | Severity | Source IP  | Destination IP     | Dest. Port |
|----------------------|------------------------|--------|----------|---------|--------------|----------|------------|--------------------|------------|
| Jan 3, 2018 13:40:05 | Communication betwe... | Local  | Indus... | -       | Not analyzed | M        | 129.6.1.10 | 192.168.0.30 (p... | 80 (TCP)   |
| Jan 3, 2018 13:39:12 | Communication betwe... | Local  | Indus... | -       | Analyzed     | M        | 129.6.1.10 | 192.168.0.30 (p... | 80 (TCP)   |
| Jan 3, 2018 13:38:45 | Communication betwe... | Local  | Indus... | -       | Analyzed     | M        | 129.6.1.10 | 192.168.0.30 (p... | 80 (TCP)   |

786

### 787 A.3.3. Data Exfiltration Between ICS Devices via Server Message Block

788 Vulnerable devices within an ICS network can be used as a pivot to bring higher-value  
 789 targets within reach to exfiltrate data (e.g., using a vulnerable Internet of Things device to  
 790 pivot and leverage attacks against a PLC on the same network). Monitoring for abnormal  
 791 communication patterns between ICS devices can help detect these types of attacks,  
 792 especially if the affected devices do not communicate during normal operations.

793 This anomaly was executed on the PCS. An unauthorized Windows File Share (using the  
 794 Server Message Block protocol) was configured between the human-machine interface  
 795 (HMI) server and the engineering workstation. Three types of files were transferred over the  
 796 share: a comma-separated values (CSV) file, a Microsoft Excel workbook (XLSX) file, and  
 797 an Adobe Portable Document File (PDF).



798

|                          |                      |                               |       |           |               |              |        |                       |                        |           |     |
|--------------------------|----------------------|-------------------------------|-------|-----------|---------------|--------------|--------|-----------------------|------------------------|-----------|-----|
| <input type="checkbox"/> | Dec 8, 2017 11:32:28 | Blacklisted file operation    | Local | Indust... | -             | Not analyzed | High   | 172.16.2.14 (win-f... | 172.16.3.10 (figs-4... | 445 (TCP) | SMB |
| <input type="checkbox"/> | Dec 8, 2017 11:32:28 | Blacklisted file operation    | Local | Indust... | -             | Not analyzed | High   | 172.16.2.14 (win-f... | 172.16.3.10 (figs-4... | 445 (TCP) | SMB |
| <input type="checkbox"/> | Dec 8, 2017 11:32:15 | Application protocol not ...  | Local | Comm...   | 8 - TCP co... | Not analyzed | Medium | 172.16.2.14 (win-f... | 172.16.3.10 (figs-4... | 445 (TCP) | SMB |
| <input type="checkbox"/> | Dec 8, 2017 11:32:15 | Successful login using bla... | Local | Indust... | -             | Not analyzed | High   | 172.16.2.14 (win-f... | 172.16.3.10 (figs-4... | 445 (TCP) | SMB |

799

### 800 A.3.4. Data Exfiltration to the Internet via File Transfer Protocol

801 Attacks against ICS, with the goal of information gathering, must (at some point) attempt to  
 802 exfiltrate the data from the ICS network, likely utilizing the internet as a transport  
 803 mechanism. Monitoring for ICS devices communicating over the internet can help detect  
 804 data exfiltration events, especially if the affected device does not normally communicate over  
 805 the internet. Depending on the protocol used for exfiltration, the file contents and/or data  
 806 being exfiltrated may be ascertainable (e.g., file names, file types, data transferred using the  
 807 File Transfer Protocol [FTP]), providing insight into the impact of the anomaly.

808 This anomaly was executed on the PCS. An FTP server was installed and configured on a  
 809 server with an internally routed public IP address (129.6.1.2). The FileZilla FTP client [15]  
 810 was installed on the historian server and was used to transfer three types of files to the  
 811 simulated “internet-based” FTP server: a CSV file, an XLSX file, and an Adobe PDF.

The screenshot displays a security alert interface with three main panels:

- Summary:**
  - Alert ID: 8859
  - Timestamp: Dec 8, 2017 11:16:36
  - Sensor name: Local
  - Detection engine: Industrial threat library (ITL)
  - ID and name: Itl\_sec\_usb\_bfo - Blacklisted file operation
  - Description: A user has read or written a blacklisted file or folder. User-defined blacklists include resources whose access should be limited to prevent confidentiality or integrity breaches. Default blacklisted file extensions indicate files which are not supposed to be accessed or transferred in the network because they may pose a security threat, or they may indicate lateral movement of malware or other malicious content.
  - Severity: High
  - Source MAC: 08:00:27:AE:99:58 (PcsCompu)
  - Destination MAC: E4:90:a9:3b:c2:c0 (Rockwell)
  - Source IP: 172.16.2.14 (win-fpvtdoeur/lan/lab)
  - Destination IP: 129.6.1.2
  - Source port: 56302
  - Destination port: 21
  - L2 proto: Ethernet
  - L3 proto: IP
  - L4 proto: TCP
  - L7 proto: FTP
  - Status: Not analyzed
  - Labels: operation=file\_create
  - User notes:
- Source host info:**
  - IP address: 172.16.2.14 (Private IP)
  - Host name: win-fpvtdoeur/lan/lab
  - MAC addresses: 08:00:27:AE:99:58 (PcsCompu), E4:90:a9:3b:c2:c0 (Rockwell), E4:90:a9:3b:c2:c1 (Rockwell)
  - Role: Historian
  - Other roles: Windows workstation, OPC server, DNS server, Web server
  - Vendor/model: Rockwell
  - OS version: Windows 7 or Windows Server 2008 R2
  - Client protocol(s): DCOM (TCP 135, 49138, 50009, 50010), DNS (UDP 53, 5355), FTP (TCP 21), FTPDATA (TCP dynamic), PalladConnection (TCP 80, 50008, 51458, 51463), HTTP (TCP 5557), Kerberos (TCP 88), LDAP (TCP 389), LDAP (UDP 389), NTP (UDP 123), NetBIOS (UDP 137), NoData (TCP 50008, 51532, 56228, 60010), NotAKnownOne (TCP 1332, 5678, 7038, 17211, 20753, 29089, 32153, 39440, 35610), NotAKnownOne (UDP 42, 4947, 3702), SMB (TCP 139, 445), SMB (UDP 138), DCOM (TCP 135, 50008), DNS (UDP 5355)
- Alert details:**
  - The following blacklisted file operation has been performed: File or folder: testfile\_xmeas7.csv
  - Operation: file\_create
  - User: lctsec
  - The file or folder was matched by the blacklist entry: '\\.\csv\$' (Regex). Operation: 'Read/Write'
  - Note: this alert is raised only once per 24 hours per source/destination host and filename combination

812

|                          |                      |                               |       |             |                |              |      |   |                         |           |             |              |
|--------------------------|----------------------|-------------------------------|-------|-------------|----------------|--------------|------|---|-------------------------|-----------|-------------|--------------|
| <input type="checkbox"/> | Dec 8, 2017 11:16:37 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 13161 (TCP) | FTPDATA      |
| <input type="checkbox"/> | Dec 8, 2017 11:16:37 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 13161 (TCP) | FTPDATA      |
| <input type="checkbox"/> | Dec 8, 2017 11:16:37 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 7038 (TCP)  | NotAKnownOne |
| <input type="checkbox"/> | Dec 8, 2017 11:16:37 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 7038 (TCP)  | NotAKnownOne |
| <input type="checkbox"/> | Dec 8, 2017 11:16:36 | Blacklisted file operation    | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |
| <input type="checkbox"/> | Dec 8, 2017 11:16:36 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 36440 (TCP) | NotAKnownOne |
| <input type="checkbox"/> | Dec 8, 2017 11:16:36 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 36440 (TCP) | NotAKnownOne |
| <input type="checkbox"/> | Dec 8, 2017 11:16:35 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |
| <input type="checkbox"/> | Dec 8, 2017 11:16:35 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |
| <input type="checkbox"/> | Dec 8, 2017 11:16:35 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |
| <input type="checkbox"/> | Dec 8, 2017 11:16:35 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 29089 (TCP) | NotAKnownOne |
| <input type="checkbox"/> | Dec 8, 2017 11:16:35 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 29089 (TCP) | NotAKnownOne |
| <input type="checkbox"/> | Dec 8, 2017 11:16:30 | Blacklisted file operation    | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |
| <input type="checkbox"/> | Dec 8, 2017 11:16:15 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 37193 (TCP) | FTPDATA      |
| <input type="checkbox"/> | Dec 8, 2017 11:16:15 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 37193 (TCP) | FTPDATA      |
| <input type="checkbox"/> | Dec 8, 2017 11:16:08 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 25658 (TCP) | FTPDATA      |
| <input type="checkbox"/> | Dec 8, 2017 11:16:08 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 25658 (TCP) | FTPDATA      |
| <input type="checkbox"/> | Dec 8, 2017 11:16:08 | Blacklisted communication     | Local | Commu...    | 8 - TCP com... | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |
| <input type="checkbox"/> | Dec 8, 2017 11:16:08 | Communication between publ... | Local | Industri... | -              | Not analyzed | High | H | 172.16.2.14 (win-fpv... | 129.6.1.2 | 21 (TCP)    | FTP          |

813

### 814 A.3.5. Unauthorized Device Is Connected to the Network

815 It is important to identify all devices on the ICS network, for a complete risk analysis and for  
 816 minimizing potential attack vectors. The detection of unauthorized devices attached to the  
 817 ICS network may indicate anomalous activity. These unauthorized devices are important to  
 818 find and remove, especially because the purpose of an unauthorized device is unknown and  
 819 may be malicious.

820 This anomaly was executed on the CRS. The engineering laptop (Windows 7 OS) was  
 821 removed from the network during the baseline phase of the tool configuration and was later  
 822 connected to the CRS LAN to execute the anomaly. After the initial connection, background  
 823 traffic was automatically generated onto the network by the laptop.

824

The screenshot displays a network security dashboard with the following sections:

- Summary:** Alert ID 13407, Timestamp Dec 12, 2017 09:36:56, Sensor name Local, Detection engine Communication patterns (LAN CP), Profile 9 - UDP communications, Severity Medium, Source MAC 34:E6:D7:22:C3:ED (Dell), Destination MAC FF:FF:FF:FF:FF:FF (Broadcast), Source IP 192.168.0.147 (knuckles.local), Destination IP 255.255.255.255, Source port 12309, Destination port 12307, L2 proto Ethernet, L3 proto IP, L4 proto UDP, L7 proto NotAKnownOne, Status Not analyzed.
- Source host info:** IP address 192.168.0.147 (Private IP), Host name knuckles.local, MAC addresses 34:E6:D7:22:C3:ED (Dell), Role Unknown, Client protocols DNS (UDP 5353, 5355), NetBIOS (UDP 137), NotAKnownOne (UDP 12307), SMB (UDP 138), Purdue level 4 - Site business network, Criticality L, Known vulnerabilities 0, Related alerts 16 (Show), First seen Dec 12, 2017 09:23:47, Last seen Dec 12, 2017 09:49:21.
- Destination host info:** IP address 255.255.255.255 (Broadcast, Private IP), MAC addresses FF:FF:FF:FF:FF:FF (Broadcast), Role Broadcast, Server protocols DHCP (UDP 67), DNS (UDP 53), ETHIP (UDP 44818), NotAKnownOne (UDP 1947, 12307), Purdue level 4 - Site business network, Criticality N/A, Known vulnerabilities 0, Related alerts 17 (Show), First seen Dec 4, 2017 04:28:15, Last seen Dec 12, 2017 09:50:14.
- Alert Details:** ID and name lin\_cp\_cmw\_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, Triggering rule/default action alert.
- Monitored networks:** Table with columns Name, Address, VLAN IDs. Row: RoboticsControlLAN, 192.168.0.0/24, any.

825

| Timestamp             | Event name(s)           | Sensor | Engine | Profile      | Status       | Severity | Source IP           | Destination IP  | Dest. Port  | L7 Proto     |
|-----------------------|-------------------------|--------|--------|--------------|--------------|----------|---------------------|-----------------|-------------|--------------|
| Dec 12, 2017 09:37:06 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 192.168.0.255   | 137 (UDP)   | NetBIOS      |
| Dec 12, 2017 09:36:56 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 192.168.0.255   | 138 (UDP)   | SMB          |
| Dec 12, 2017 09:36:56 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 255.255.255.255 | 12307 (UDP) | NotAKnownOne |
| Dec 12, 2017 09:24:11 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 192.168.0.255   | 138 (UDP)   | SMB          |
| Dec 12, 2017 09:23:58 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 224.0.0.251     | 5353 (UDP)  | DNS          |
| Dec 12, 2017 09:23:56 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 192.168.0.255   | 137 (UDP)   | NetBIOS      |
| Dec 12, 2017 09:23:52 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 255.255.255.255 | 12307 (UDP) | NotAKnownOne |
| Dec 12, 2017 09:23:47 | Communication patter... | Local  | Com... | 9 - UDP c... | Not analyzed | Medium   | 192.168.0.147 (...) | 224.0.0.252     | 5355 (UDP)  | DNS          |

826

### A.3.6. Loss of Communications with Modbus TCP Device

827

ICS devices must exhibit high availability to support manufacturing operations. This quality becomes more important as the speed of manufacturing operations increases (i.e., short cycle times). If an ICS device hosting a network service becomes unavailable during manufacturing operations, then this may be a sign of anomalous activity and should be investigated. Loss of communications with a device or service may be caused by a multitude of anomalies, including device restarts, software faults, high network utilization, and an increased processing load on the device.

828

829

830

831

832

833

834 This anomaly was executed on the CRS. A firewall rule was added to the Linux iptables  
 835 (Linux kernel firewall) on Machining Station 1 to block all incoming packets on Modbus  
 836 TCP Port 502. The firewall replied with a TCP reset for each incoming packet or connection  
 837 request, to make it appear as if the Modbus server had terminated and the TCP socket was  
 838 closed.

839

| Timestamp             | Event name(s)            | Sensor | Engine   | Profile | Status       | Severity | Source IP           | Destination IP      | Dest. Port | L7 Proto  |
|-----------------------|--------------------------|--------|----------|---------|--------------|----------|---------------------|---------------------|------------|-----------|
| Dec 11, 2017 11:26:01 | MODBUS/TCP device ...    | Local  | Indus... | -       | Not analyzed | High (H) | -                   | 192.168.1.101 (...) | -          | MODBUSTCP |
| Dec 11, 2017 11:26:00 | Device with many fail... | Local  | Indus... | -       | Not analyzed | Low (L)  | 192.168.0.98 (h...) | 192.168.1.101 (...) | 502 (TCP)  | -         |

840

### 841 A.3.7. Brute-Force Password Attack Against an ICS Device

842 Authentication systems that are not rate-restricted may be vulnerable to password-guessing  
 843 attacks, especially if the default credentials of the device have not been changed. Compiled  
 844 lists containing default user credentials are freely available on the internet, as are lists of  
 845 commonly used usernames and passwords. Given enough time, an attacker may be able to  
 846 access vulnerable systems by using a brute-force password attack.

847 This anomaly was executed on the CRS. The software Nmap [16] was used to generate the  
 848 brute-force password attack by using the script `http-brute`. The attack was pointed at an  
 849 Apache [17] Hypertext Transfer Protocol (HTTP) server on Machining Station 4, containing  
 850 a directory that was protected by HTTP basic authentication. The HTTP server was not  
 851 configured to limit the number of authentication attempts.

**Summary**

|                  |   |
|------------------|---|
| Alert ID         | 10585   |
| Timestamp        | Dec 11, 2017 13:12:40   |
| Sensor name      | Local   |
| Detection engine | Industrial threat library (ITL)   |
| ID and name      | ITL_sec_uId_bred_fall - Login attempt using blacklisted credentials   |
| Description      | A user has attempted to login to a system using blacklisted credentials. The login failed but it may be an indication of an attacker trying to use default device credentials to gain access to the system. |
| Severity         | High  |
| Source MAC       | 00:15:5D:04:5B:2B (Microsoft)   |
| Destination MAC  | 94:BB:C5:0E:E1:9F (Ruggedco)  |
| Source IP        | 192.168.0.10  |
| Destination IP   | 192.168.1.104 (station4.lan.lab)  |
| Source port      | 44436   |
| Destination port | 80  |
| L2 proto         | Ethernet  |
| L3 proto         | IP  |
| L4 proto         | TCP   |
| L7 proto         | HTTP  |
| Status           | Not analyzed  |
| Labels           |   |
| User notes       |   |

**Source host info**

|                       |  |
|-----------------------|--|
| IP address            | 192.168.0.10 (Private IP)  |
| MAC addresses         | 00:15:5D:04:5B:2B (Microsoft)<br>94:BB:C5:0E:E1:9F (Ruggedco)  |
| Role                  | Unknown  |
| Client protocol(s)    | DNS (UDP 5353)<br>FailedConnection (TCP 20.21.22.443, 502, 1020, 1021, 1022, 1023, 1024)<br>HTTP (TCP 80, 5120)<br>SSDP (UDP 1900) |
| Server protocol(s)    | SSH (TCP 22)   |
| Purdue level          | 4 - Site business network  |
| Criticality           | L  |
| Known vulnerabilities | 0  |
| Related alerts        | 53 (Show)  |
| First seen            | Dec 4, 2017 04:40:29   |
| Last seen             | Dec 11, 2017 13:15:15  |

**Alert details**

Login attempt using blacklisted credentials:  
Username: root  
Password: root

Comment:  
The credentials listed above are known default credentials for (at least) the following device(s):  
'Adcon Telemetry addVANTAGE Pro 6.1.6.5'  
'Metrobility NetBeacon Element Management Software'  
'Moxa Cellular Micro RTU Controller (ioLogik W53xx, ioLogik, IA240/241 Embedded computer'

This is a default blacklist entry

**Monitored networks**

| Name                | Address        | VLAN IDs |
|---------------------|----------------|----------|
| RoboticsFieldBusLAN | 192.168.1.0/24 | any      |
| RoboticsControlLAN  | 192.168.0.0/24 | any      |

852

Filters applied: Today's alerts, By status: Robotics

| n. of alert details | Event name                                     | Severity | Event-specific info | Protocol    | Source IPs   | Destination IPs                  | Destination Sensor - Engine - Profile ports | Min value                    | Max value | First event  | Last event   |
|---------------------|--|----------|---------------------|-------------|--------------|----------------------------------|---|------------------------------|-----------|--------------|--------------|
| 15                  | Communication pattern not whitelisted          | M        |                     | IP/TCP/HTTP | 192.168.0.10 | 192.168.1.104 (station4.lan.lab) | 80  | 1 - Local - Communica...     |           | Dec 11, 2017 | Dec 11, 2017 |
| 11                  | Login attempt using blacklisted credentials    | H        |                     | IP/TCP/HTTP | 192.168.0.10 | 192.168.1.104 (station4.lan.lab) | 80  | 1 - Local - Industrial th... |           | Dec 11, 2017 | Dec 11, 2017 |
| 1                   | Successful login using blacklisted credentials | H        |                     | IP/TCP/HTTP | 192.168.0.10 | 192.168.1.104 (station4.lan.lab) | 80  | 1 - Local - Industrial th... |           | Dec 11, 2017 | Dec 11, 2017 |

853

### 854 A.3.8. Invalid Credentials for Remote Access

855 While it can be expected that some users will accidentally enter invalid credentials on a daily  
 856 basis, it is important to monitor these events for trends of anomalies. Large quantities of  
 857 invalid-credential usage may indicate a password-guessing attack. These credentials may also  
 858 be used to authenticate connections between ICS devices. With the increasing use of remote  
 859 access for ICS devices, it is important to monitor these services for attempts made by  
 860 attackers to gain unauthorized access.

861 This anomaly was executed on the PCS. A remote desktop session was initialized from the  
 862 engineering workstation to the HMI server and required authentication with the Microsoft  
 863 Active Directory service. Invalid credentials were submitted for authentication.

**Summary**

|                                     |                                    |
|-------------------------------------|------------------------------------|
| Alert ID                            | 10571                              |
| Timestamp                           | Dec 11, 2017 13:07:14              |
| Sensor name                         | Local                              |
| Detection engine                    | Communication patterns (LAN CP)    |
| Profile                             | 8 - TCP communications             |
| Severity                            | Medium                             |
| Source MAC                          | F8:B1:56:BA:09:A8 (Dell)           |
| Destination MAC                     | 94:B8:C5:0E:E1:9F (Ruggedco)       |
| Source IP                           | 192.168.0.20 (polaris)             |
| Destination IP                      | 192.168.1.101 (beaglebone-2.local) |
| Source port                         | 50661                              |
| Destination port                    | 80                                 |
| L2 proto                            | Ethernet                           |
| L3 proto                            | IP                                 |
| L4 proto                            | TCP                                |
| L7 proto                            | HTTP                               |
| TCP stream opened in hot start mode | false                              |
| Status                              | Not analyzed                       |
| Labels                              |                                    |
| User notes                          |                                    |

**Monitored networks**

| Name                | Address        | VLAN IDs |
|---------------------|----------------|----------|
| RoboticsFieldBusLAN | 192.168.1.0/24 | any      |
| RoboticsControlLAN  | 192.168.0.0/24 | any      |

**Source host info**

|                    |   |
|--------------------|---|
| IP address         | 192.168.0.20 (Private IP)   |
| Host name          | polaris   |
| MAC addresses      | F8:B1:56:BA:09:A8 (Dell)<br>94:B8:C5:0E:E1:9F (Ruggedco)  |
| Role               | Web server  |
| Client protocol(s) | DNS (TCP 53)<br>DNS (UDP 53, 5353)<br>FTP (TCP 21)<br>FailedConnection (TCP 80, 5000, 34050, 42299, 45300, 45956, 48605, 50000, 51627, 52203, 56117)<br>HTTP (TCP dynamic)<br>Kerberos (TCP 88)<br>LDAP (TCP 389, 3268)<br>LDAP (UDP 389)<br>NFS (TCP 920)<br>NFS (UDP 944)<br>NTP (UDP 123)<br>NoData (TCP 35387, 43010, 46460, 47486)<br>NotAKnownOne (TCP 22, 389, 464, 3268, 9999, 33569, 42998, 47647, 52730, 53282, 55912, 60779, 60917)<br>NotAKnownOne (UDP 686, 861, 910, 918, 928, 9999, 44444, 44445, 44446)<br>SMB (TCP 445)<br>SMB (UDP 138)<br>SSH (TCP 22)<br>SSL (TCP 443)<br>Syslog (UDP 514)<br>HTTP (TCP 11311)<br>NoData (TCP 32793, 34119, 34121)<br>NotAKnownOne (TCP 5000, 50000)<br>NotAKnownOne (UDP 33443, 33444, 33445, 33446, 33447, 33448, 33449, 33450, 33451, 59798)<br>SunRPC (TCP 111, 2049)<br>SunRPC (UDP 111) |
| Server protocol(s) |   |

**Alert Details**

|                                |   |
|--------------------------------|---|
| ID and name                    | lan_cp_pnw - Application protocol not whitelisted   |
| Description                    | Application protocol not whitelisted: the application protocol used in the communication is not whitelisted for this host combination |
| Triggering rule/default action | alert   |

864

| Nr. of agr. details ▾ | Event type ID       | Event severity | L7 Protocol | Source IP              | Destination IP                     | Sensor       | First seen            | Last seen             |
|-----------------------|---------------------|----------------|-------------|------------------------|------------------------------------|--------------|-----------------------|-----------------------|
| 3                     | authentication_fail | Medium         | HTTP        | 192.168.0.20 (polaris) | 192.168.1.101 (beaglebone-2.local) | Local (id=1) | Dec 11, 2017 13:07:00 | Dec 11, 2017 13:07:00 |

865

### 866 A.3.9. Unauthorized ICS Device Firmware Update

867 Many ICS devices provide services to remotely update firmware over the network. These  
 868 network services can also provide a mechanism for attackers to replace valid firmware with  
 869 malicious firmware if the device is not protected.

870 This anomaly was executed on the PCS. The Allen-Bradley PLC implemented in the PCS  
 871 contains an Ethernet module (1756-EN2T) that allows its firmware to be upgraded and  
 872 downgraded over Ethernet/IP. The firmware was upgraded or downgraded using the  
 873 ControlFLASH firmware upgrade tool.

SilentDefense™ Dashboard Network Events Sensors Settings admin

Alert details Back Edit Delete Show | Download pcap Help

**Summary**

Alert ID: 11390  
 Timestamp: Dec 11, 2017 16:11:28  
 Sensor name: Local  
 Detection engine: Industrial threat library (ITL)  
 ID and name: RI\_Op\_260p\_eThip\_firmware\_update - ETHIP firmware update command  
 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.  
 Severity: High  
 Source MAC: 40:A8:F0:3D:48:A6 (HewlettP)  
 Destination MAC: E4:90:69:3B:C2:C0 (Rockwell)  
 Source IP: 172.16.3.10 (figs-47631ehh.lan.lab)  
 Destination IP: 172.16.2.102 (pic\_tesim)  
 Source port: 54521  
 Destination port: 44818  
 L2 proto: Ethernet  
 L3 proto: IP  
 L4 proto: TCP  
 L7 proto: ETHIP  
 Status: Not analyzed  
 Labels: command=Firmware\_update, dtr\_route=Module\_3  
 User notes:

**Monitored networks**

| Name                      | Address       | VLAN IDs |
|---------------------------|---------------|----------|
| ProcessControlVLAN2       | 172.16.2.0/24 | any      |
| ProcessControlEngineering | 172.16.3.0/24 | any      |

**Source host info**

IP address: 172.16.3.10 (Private IP)  
 Host name: figs-47631ehh.lan.lab  
 MAC addresses: E4:90:69:3B:C2:C4 (Rockwell), 40:A8:F0:3D:48:A6 (HewlettP), E4:90:69:3B:C2:C5 (Rockwell), E4:90:69:3B:C2:C1 (Rockwell)  
 Role: Master  
 Other roles: Windows workstation, Terminal client  
 Vendor/model: Rockwell  
 OS version: Windows 7 or Windows Server 2008 R2  
 Client protocol(s): DCOM (TCP 135, 49158, 49187, 49188), DNS (UDP 53, 5355), ETHIP (TCP 44818), ETHIP (UDP 44818), FTP (TCP 21), FTPOJATA (TCP 57921, 64849), HTTP (TCP 80, 8530), Kerberos (TCP 88), LDAP (TCP 389), LDAP (UDP 389), NTP (UDP 123), NetBIOS (UDP 137), NoData (TCP 56224, 56614, 58847), NotAKnownOne (TCP 1332, 3060, 3389, 15787, 60472), NotAKnownOne (UDP 3702), RDP (TCP 3389), SMB (TCP 445), SMB (UDP 138), SSDP (UDP 1900), SSH (TCP 22), SSL (TCP 443, 3389), Syslog (UDP 514), TELNET (TCP 23), DCOM (TCP 135, 49197), FailedConnection (TCP 80, 139, 49194, 49250, 49329, 57980, 58099), NetBIOS (UDP 137), NoData (TCP 49390, 49201, 49205, 58099), SMB (TCP 445)  
 Server protocol(s):  
 Purdue level: 2 - Supervisory control

**Alert details**

Command: Firmware update  
 Destination route: Module 3

874

|                          |                       |                              |       |           |               |              |        |                        |                       |             |       |      |
|--------------------------|-----------------------|------------------------------|-------|-----------|---------------|--------------|--------|------------------------|-----------------------|-------------|-------|------|
| <input type="checkbox"/> | Dec 11, 2017 16:12:03 | ETHIP controller reset co... | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:03 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:01 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:01 | Message type not whitelis... | Local | Comm...   | 8 - TCP co... | Not analyzed | Medium | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | Exit |
| <input type="checkbox"/> | Dec 11, 2017 16:12:01 | Message type not whitelis... | Local | Comm...   | 8 - TCP co... | Not analyzed | Medium | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | Exit |
| <input type="checkbox"/> | Dec 11, 2017 16:12:00 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:00 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:00 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:00 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:12:00 | Message type not whitelis... | Local | Comm...   | 8 - TCP co... | Not analyzed | Medium | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:11:28 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |
| <input type="checkbox"/> | Dec 11, 2017 16:11:28 | ETHIP firmware update c...   | Local | Indust... | -             | Not analyzed | High   | 172.16.3.10 (figs-4... | 172.16.2.102 (pic_... | 44818 (TCP) | ETHIP | -    |

875

### 876 A.3.10. Unauthorized HMI Logic Modification

877 Many ICS devices provide services to remotely update control logic over the network. These  
 878 network services can also provide a mechanism for attackers to replace valid control logic  
 879 with malicious logic if the device is not protected. This is especially important for HMIs, as  
 880 they are typically used by operators to monitor and manipulate the manufacturing process in  
 881 a safe and controlled manner.

882 This anomaly was executed on the CRS. The database implemented on the CRS Red Lion  
 883 HMI (Model G310) was modified and uploaded to the HMI by using the Red Lion Crimson  
 884 3.0 software. The Modbus TCP registers in the modified database differed slightly from  
 885 those in the original database.

886

| n. of agr. details | Event name  | Severity | Event-specific info                    | Protocol         | Source IPs                     | Destination IPs                     | Destination Sensor - Engine - Profile | Min value                | Max value | First event | Last event   |              |
|--------------------|---|----------|--|------------------|--------------------------------|-------------------------------------|---------------------------------------|--------------------------|-----------|-------------|--------------|--------------|
| 15                 | Numeric field value outside whitelisted enumeration | Medium   | /upstream/read_input_registers/star... | IP/TCP/Modbus... | 192.168.0.98 (hmi.lan.lab)     | 192.168.0.30 (pic-robotics.lan.lab) | 502                                   | 1 - Local - Protocol     | 32771     | 32771       | Dec 12, 2017 | Dec 12, 2017 |
| 15                 | Length field value outside whitelisted range        | Medium   | /upstream/read_discrete_inputs/qua...  | IP/TCP/Modbus... | 192.168.0.98 (hmi.lan.lab)     | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol     | 2         | 2           | Dec 12, 2017 | Dec 12, 2017 |
| 15                 | Numeric field value outside whitelisted enumeration | Medium   | /upstream/read_discrete_inputs/sta...  | IP/TCP/Modbus... | 192.168.0.98 (hmi.lan.lab)     | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol     | 4         | 4           | Dec 12, 2017 | Dec 12, 2017 |
| 1                  | Numeric field value outside whitelisted enumeration | Medium   | /upstream/read_holding_registers/s...  | IP/TCP/Modbus... | 192.168.0.98 (hmi.lan.lab)     | 192.168.0.30 (pic-robotics.lan.lab) | 502                                   | 1 - Local - Protocol     | 0         | 0           | Dec 12, 2017 | Dec 12, 2017 |
| 1                  | Source host not whitelisted                         | Medium   |  | IP/TCP/NotAkn... | 192.168.0.147 (knuckles.local) | 192.168.0.98 (hmi.lan.lab)          | 789                                   | 1 - Local - Communica... |           |             | Dec 12, 2017 | Dec 12, 2017 |
| 1                  | Message type not whitelisted                        | Medium   | Read Holding Registers Exception (1... | IP/TCP/Modbus... | 192.168.0.98 (hmi.lan.lab)     | 192.168.0.30 (pic-robotics.lan.lab) | 502                                   | 1 - Local - Communica... |           |             | Dec 12, 2017 | Dec 12, 2017 |

887

### 888 A.3.11. ICS Device Receives Diagnostic Modbus TCP Function Codes

889 Certain ICS network protocols enable diagnostic access to ICS devices. While this type of  
 890 functionality enables remote maintenance and diagnostics to authorized personnel, it may  
 891 also be leveraged by aggressors to compromise ICS devices.

892 This anomaly was executed on the CRS. Python [14] was used to create a Modbus TCP  
 893 message with the diagnostic function code value of 43 (0x2B), known as encapsulated  
 894 interface transfer. The message was generated by the cybersecurity virtual machine  
 895 (CybersecVM) and was transmitted to the PLC Modbus server.

896

| Timestamp             | Event name(s)             | Sensor | Engine  | Profile      | Status       | Severity | Source IP    | Destination IP     | Dest. Port | L7 Proto  |
|-----------------------|---------------------------|--------|---------|--------------|--------------|----------|--------------|--------------------|------------|-----------|
| Dec 11, 2017 13:40:28 | Communication patter...   | Local  | Com...  | 8 - TCP c... | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |
| Dec 11, 2017 13:40:27 | Numeric field value ou... | Local  | Prot... | 10 - MB-t... | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |

897

### 898 A.3.12. ICS Device Receives Undefined Modbus TCP Function Codes

899 Communications that do not conform to the defined specifications of the industrial protocol  
 900 may cause an ICS device to act in an undefined or unsafe manner. Depending on the  
 901 manufacturing process and the ICS device, the nonconforming communications may or may  
 902 not be impactful, but investigation into the cause is warranted.

903 This anomaly was executed on the CRS. Python [14] was used to create a Modbus TCP  
 904 message with the undefined function code value of 49 (0x31). The message was generated  
 905 by the CybersecVM and was transmitted to the PLC Modbus server.

906

| Timestamp             | Event name(s)             | Sensor | Engine  | Profile      | Status       | Severity | Source IP    | Destination IP     | Dest. Port | L7 Proto  |
|-----------------------|---------------------------|--------|---------|--------------|--------------|----------|--------------|--------------------|------------|-----------|
| Dec 11, 2017 13:37:02 | Communication patter...   | Local  | Com...  | 8 - TCP c... | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |
| Dec 11, 2017 13:37:02 | Numeric field value ou... | Local  | Prot... | 10 - MB-t... | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |

907

### 908 A.3.13. ICS Device Receives Malformed Modbus TCP Traffic

909 Communications that do not conform to the defined specifications of the industrial protocol  
 910 may cause an ICS device to act in an undefined or unsafe manner. Depending on the  
 911 manufacturing process and the ICS device, the nonconforming communications may or may  
 912 not be impactful, but investigation into the cause is warranted.

913 This anomaly was executed on the CRS. Python [14] was used to create a malformed  
 914 Modbus TCP message. The message was generated by the CybersecVM and was transmitted  
 915 to the PLC Modbus server.

The screenshot displays the SilentDefense™ interface with the following sections:

- Summary:** Alert ID 10833, Timestamp Dec 11, 2017 14:31:02, Sensor name Local, Detection engine Malformed packet, Severity Medium, Source MAC 00:15:5D:04:5B:2B (Microsoft), Destination MAC 00:01:05:17:DB:08 (Beckhoff), Source IP 192.168.0.10, Destination IP 192.168.0.30 (plc-robotics.lan.lab), Source port 56396, Destination port 502, L2 proto Ethernet, L3 proto IP, L4 proto TCP, L7 proto MODBUSTCP, TCP stream opened in hot start mode false, Status Not analyzed, Labels uid=222.
- Source host info:** IP address 192.168.0.10 (Private IP), MAC addresses 00:15:5D:04:5B:2B (Microsoft) and 94:B8:C5:0E:E1:9F (Ruggedco), Role Master, Client protocol(s) DNS (UDP 5353), FailedConnection (TCP 20, 21, 22, 443, 1020, 1021, 1022, 1023, 1024), HTTP (TCP 80, 5120), MODBUSTCP (TCP 502), SSDP (UDP 1900), Server protocol(s) SSH (TCP 22), Purdue level 2 - Supervisory control, Criticality H, Known vulnerabilities 0, Related alerts 60 (Show), First seen Dec 4, 2017 04:40:29, Last seen Dec 11, 2017 14:31:02.
- Destination host info:** IP address 192.168.0.30 (Private IP), MAC addresses 00:01:05:17:DB:08 (Beckhoff) and 94:B8:C5:0E:E1:9F (Ruggedco), Role PLC, Other roles Master, Slave, File server, Web server, Vendor/model Beckhoff, Client protocol(s) MODBUSTCP (TCP 502), NTP (UDP 123), SSDP (UDP 1900).
- Alert details:** Details from parsed request/response: 0, ID and name pars\_ops\_trunc\_pdu - Truncated application protocol message, Description Malformed application protocol message: the application message PDU is truncated or incomplete, Direction Upstream, Field path /upstream.
- Alert data:** Upstream data: 1B, 0000 53.
- Monitored networks:** Table with columns Name, Address, VLAN IDs. Entry: RoboticsControlLAN, 192.168.0.0/24, any.

916

| Timestamp             | Event name(s)             | Sensor | Engine  | Profile      | Status       | Severity | Source IP    | Destination IP     | Dest. Port | L7 Proto  |
|-----------------------|---------------------------|--------|---------|--------------|--------------|----------|--------------|--------------------|------------|-----------|
| Dec 11, 2017 14:31:02 | Truncated application ... | Local  | Malf... | -            | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |
| Dec 11, 2017 14:31:02 | Communication patter...   | Local  | Com...  | 8 - TCP c... | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |
| Dec 11, 2017 14:31:01 | Numeric field value ou... | Local  | Prot... | 10 - MB-t... | Not analyzed | Medium   | 192.168.0.10 | 192.168.0.30 (p... | 502 (TCP)  | MODBUSTCP |

917

### 918 A.3.14. Illegal Memory Addresses of ICS Device Are Accessed

919 Some industrial protocols (like Modbus) require relative addressing to access ICS device  
 920 registers. Attackers may attempt to modify illegal memory locations of ICS devices by using  
 921 these types of industrial protocols or may attempt to cause the ICS device to act in an  
 922 undefined or unsafe manner by modifying data located in a protected memory location.

923 This anomaly was executed on the CRS. The HMI database was modified to access an illegal  
 924 register on the PLC Modbus TCP server when the anomaly was activated. The valid Modbus  
 925 address range for the PLC registers is 0x8000 to 0x80FF.

926

| Timestamp             | Event name(s)             | Sensor | Engine  | Profile      | Status       | Severity | Source IP    | Destination IP     | Dest. Port | L7 Proto   |
|-----------------------|---------------------------|--------|---------|--------------|--------------|----------|--------------|--------------------|------------|------------|
| Dec 11, 2017 14:34:58 | Message type not whit...  | Local  | Com...  | 8 - TCP c... | Not analyzed | Medium   | 192.168.0.98 | 192.168.0.30 (p... | 502 (TCP)  | MODBUS TCP |
| Dec 11, 2017 14:34:58 | Numeric field value ou... | Local  | Prot... | 10 - MB-t... | Not analyzed | Medium   | 192.168.0.98 | 192.168.0.30 (p... | 502 (TCP)  | MODBUS TCP |

927

### 928 A.3.15. ICS Device Scanning Is Performed on the Network

929 During the reconnaissance phase, an attacker may attempt to locate vulnerable devices in an  
 930 ICS network and will likely probe for ICS-specific services (e.g., Modbus TCP). Once a  
 931 vulnerable service is discovered, an attacker may attempt to exploit that service.

932 This anomaly was executed on the CRS. The software Nmap [16] was used to generate the  
 933 Modbus device scan by using the script `modbus-discover` [18]. The attack was directed at  
 934 two ICS devices: the PLC and Machining Station 4.

SilentDefense™ Dashboard Network Events Sensors Settings timzim

Alert details Back Edit Delete Trim Show | Download pcap Help

#### Summary

|                                     |                                     |
|-------------------------------------|-------------------------------------|
| Alert ID                            | 10909                               |
| Timestamp                           | Dec 11, 2017 14:38:08               |
| Sensor name                         | Local                               |
| Detection engine                    | Protocol fields (DPBI)              |
| Profile                             | 10 - MB-to-0-30                     |
| Severity                            | Medium                              |
| Source MAC                          | 00:15:5D:04:5B:2B (Microsoft)       |
| Destination MAC                     | 00:01:05:17:DB:08 (Beckhoff)        |
| Source IP                           | 192.168.0.10                        |
| Destination IP                      | 192.168.0.30 (plc-robotics.lan.lab) |
| Source port                         | 56410                               |
| Destination port                    | 502                                 |
| L2 proto                            | Ethernet                            |
| L3 proto                            | IP                                  |
| L4 proto                            | TCP                                 |
| L7 proto                            | MODBUSTCP                           |
| TCP stream opened in hot start mode | false                               |
| Status                              | Not analyzed                        |
| Labels                              | uid=2                               |
| User notes                          |                                     |

#### Monitored networks

| Name               | Address        | VLAN IDs |
|--------------------|----------------|----------|
| RoboticsControlLAN | 192.168.0.0/24 | any      |

#### Source host info

|                       |   |
|-----------------------|---|
| IP address            | 192.168.0.10 (Private IP)   |
| MAC addresses         | 00:15:5D:04:5B:2B (Microsoft)<br>94:B8:C5:0E:E1:9F (Ruggedco)   |
| Role                  | Master  |
| Client protocol(s)    | DNS (UDP 5353)<br>FailedConnection (TCP 20, 21, 22, 443, 1020, 1021, 1022, 1023, 1024)<br>HTTP (TCP 80, 5120)<br>MODBUSTCP (TCP 502)<br>SSDP (UDP 1900) |
| Server protocol(s)    | SSH (TCP 22)  |
| Purdue level          | 2 - Supervisory control   |
| Criticality           | H   |
| Known vulnerabilities | 0   |
| Related alerts        | 86 (Show)   |
| First seen            | Dec 4, 2017 04:40:29  |
| Last seen             | Dec 11, 2017 14:38:17   |

#### Destination host info

|                    |  |
|--------------------|--|
| IP address         | 192.168.0.30 (Private IP)  |
| MAC addresses      | 00:01:05:17:DB:08 (Beckhoff)<br>94:B8:C5:0E:E1:9F (Ruggedco)                                     |
| Role               | PLC  |
| Other roles        | Master, Slave, File server, Web server   |
| Vendor/model       | Beckhoff   |
| Client protocol(s) | MODBUSTCP (TCP 502)<br>NTP (UDP 123)<br>SSDP (UDP 1900)<br>FTP (TCP 21)<br>FTPDATA (TCP dynamic) |

#### Alert details

Details from parsed request/response: 0

| ID and name   | Description  | Direction | Field path             | Field value | Field model                        |
|---|--|-----------|------------------------|-------------|------------------------------------|
| dpbi_uv_num_set - Numeric field value outside whitelisted enumeration | Unusual numeric field value: the value of a numeric field is not in the enumeration (set of values allowed by the field model) | Upstream  | /upstream/header/rc    | 17 (0x11)   | [[2, 6], 15] - samples: 33,572,816 |
| dpbi_uv_num_set - Numeric field value outside whitelisted enumeration | Unusual numeric field value: the value of a numeric field is not in the enumeration (set of values allowed by the field model) | Upstream  | /upstream/header/uid   | 2 (0x02)    | [[0, 1]] - samples: 33,572,816     |
| dpbi_uf_fw - Field not whitelisted                                    | Field not whitelisted: an application protocol field used in the communication is not allowed by the protocol model            | Upstream  | /upstream/report_slave |             |                                    |

935

| n. of aggr. details | Event name  | Severity | Event-specific info | Protocol                              | Source IPs   | Destination IPs                     | Destination Sensor - Engine - Profile | Min value                   | Max value | First event  | Last event   |              |
|---------------------|---|----------|---------------------|---------------------------------------|--------------|-------------------------------------|---------------------------------------|-----------------------------|-----------|--------------|--------------|--------------|
| 14                  | Communication pattern not whitelisted               | Medium   | M                   | IP/TCP/MODBU...                       | 192.168.0.10 | 3 destination IPs                   | 502                                   | 1 - Local - Communica...    |           | Dec 11, 2017 | Dec 11, 2017 |              |
| 10                  | Numeric field value outside whitelisted enumeration | Medium   | M                   | /upstream/header/rc                   | 192.168.0.10 | 192.168.0.30 (plc-robotics.lan.lab) | 502                                   | 1 - Local - Protocol fie... | 17        | 17           | Dec 11, 2017 | Dec 11, 2017 |
| 10                  | Field not whitelisted                               | Medium   | M                   | /upstream/report_slave                | 192.168.0.10 | 192.168.0.30 (plc-robotics.lan.lab) | 502                                   | 1 - Local - Protocol fie... |           |              | Dec 11, 2017 | Dec 11, 2017 |
| 9                   | Numeric field value outside whitelisted enumeration | Medium   | M                   | /upstream/header/uid                  | 192.168.0.10 | 192.168.0.30 (plc-robotics.lan.lab) | 502                                   | 1 - Local - Protocol fie... | 2         | 10           | Dec 11, 2017 | Dec 11, 2017 |
| 2                   | Length field value outside whitelisted range        | Medium   | M                   | /upstream/header/len                  | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... | 2         | 5            | Dec 11, 2017 | Dec 11, 2017 |
| 2                   | Numeric field value outside whitelisted enumeration | Medium   | M                   | /downstream/header/rc                 | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... | 43        | 145          | Dec 11, 2017 | Dec 11, 2017 |
| 2                   | Numeric field value outside whitelisted enumeration | Medium   | M                   | /upstream/header/rc                   | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... | 17        | 43           | Dec 11, 2017 | Dec 11, 2017 |
| 1                   | Field not whitelisted                               | Medium   | M                   | /downstream/encapsulated_interfac...  | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... |           |              | Dec 11, 2017 | Dec 11, 2017 |
| 1                   | Field not whitelisted                               | Medium   | M                   | /downstream/report_slave_exception    | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... |           |              | Dec 11, 2017 | Dec 11, 2017 |
| 1                   | Field not whitelisted                               | Medium   | M                   | /upstream/encapsulated_interface_t... | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... |           |              | Dec 11, 2017 | Dec 11, 2017 |
| 1                   | Field not whitelisted                               | Medium   | M                   | /upstream/report_slave                | 192.168.0.10 | 192.168.1.104 (station4.lan.lab)    | 502                                   | 1 - Local - Protocol fie... |           |              | Dec 11, 2017 | Dec 11, 2017 |

936

937 **Appendix B. Secure-NOK SNOK Supplemental Information**

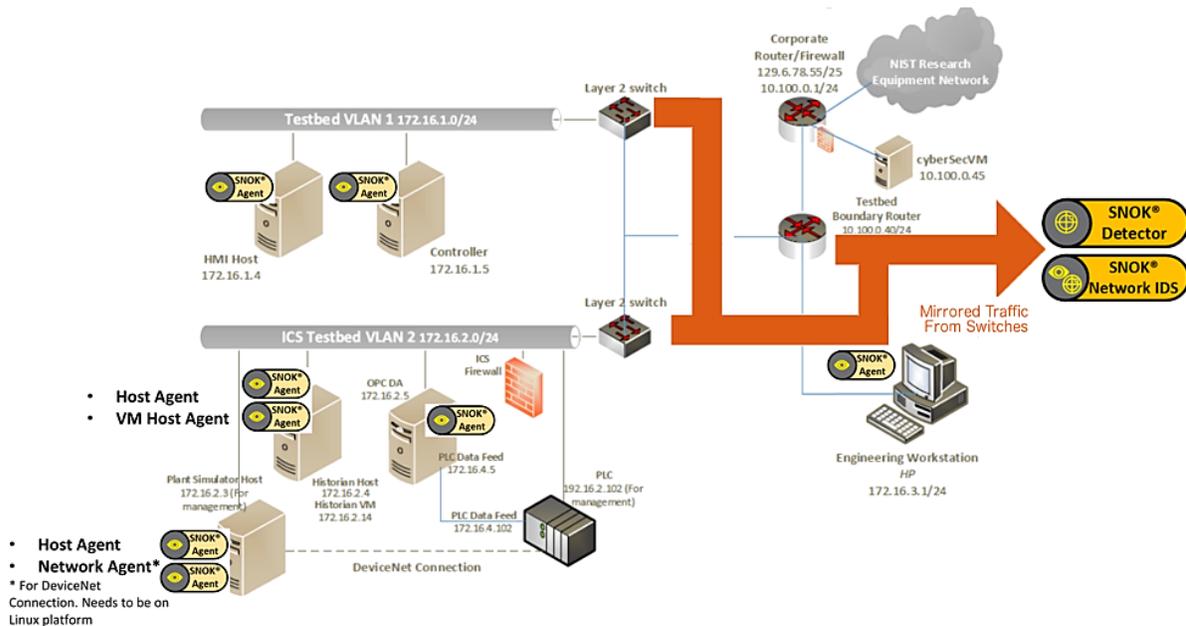
938 Secure-NOK SNOK is a cybersecurity monitoring and detection system tailored for  
939 industrial networks and control systems. In the installation, the SNOK network intrusion  
940 detection system (IDS) comes preinstalled on an appliance that is integrated into the asset  
941 owner’s environment.

942 **B.1. Build Architecture**

943 Two SNOK dedicated appliances were physically installed in the measurement rack of the  
944 Cybersecurity for Smart Manufacturing Systems (CSMS) environment. One appliance was  
945 dedicated to the process control system (PCS), and the other appliance was dedicated to the  
946 collaborative robotic system (CRS). Three existing Switch Port Analyzer (SPAN) ports from  
947 each system (PCS and CRS) were connected to a VERSAstream packet broker (VS-1208BT-  
948 S) to aggregate the mirrored traffic from the PCS and the CRS into two respective streams,  
949 for a total of six SPAN ports. The appliance connections within the PCS and CRS networks  
950 are shown in Figure B-1 and Figure B-2, respectively.

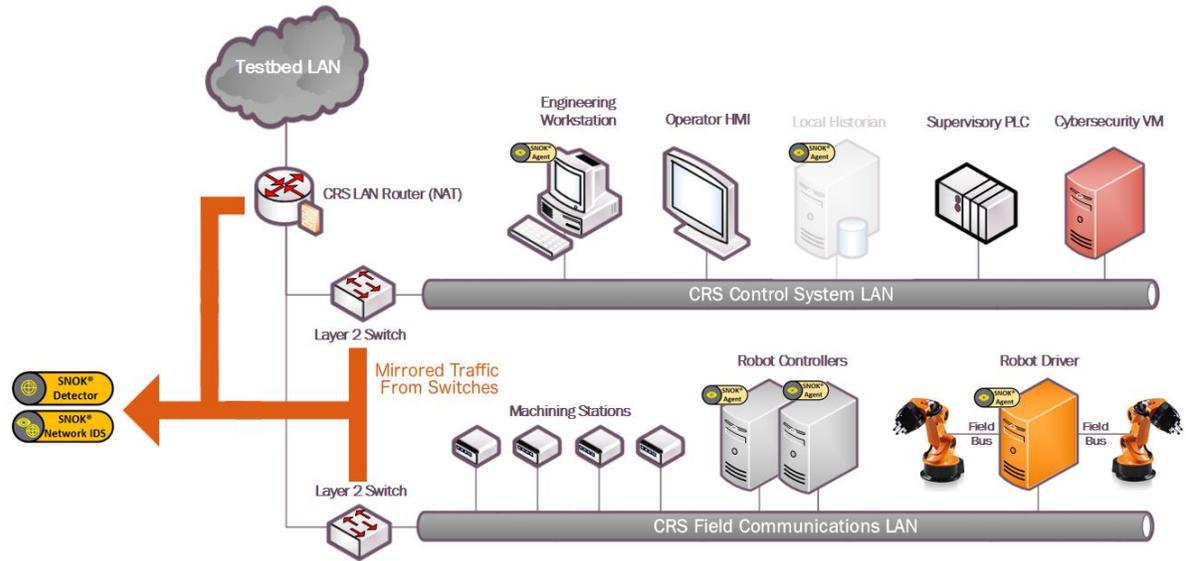
951 The PCS appliance network was connected to the demilitarized zone (DMZ) network located  
952 in the test bed’s measurement rack, to isolate the appliance’s network traffic from the rest of  
953 the network traffic. The engineering laptop was used to interface with the SNOK graphical  
954 user interface (GUI) via physical connections to the DMZ. The CRS appliance network was  
955 connected to the industrial control system (ICS) local area network (LAN), and the SNOK  
956 GUI was accessed via the engineering workstation. More information regarding the specific  
957 configuration of the test-bed network can be found in Section 3.

958 **Figure B-1 SPAN Port Connections to the SNOK Appliance in the PCS (Including the Hosts**  
959 **with SNOK Agents)**



960

961 **Figure B-2 SPAN Port Connections to the SNOK Appliance in the CRS (Including the Hosts**  
 962 **with SNOK Agents)**



963

964 **B.2. Installation and Configuration**

965 Physical hardware appliances and software were provided by Secure-NOK for this  
 966 demonstration. After the hardware appliances were received, they were installed into the  
 967 CSMS test bed. Soon after the initial installation, engineers from Secure-NOK arrived on site  
 968 to complete the installation and configuration of the tool. The following subsections describe  
 969 the steps taken to install and configure the appliances.

970 **B.2.1. Hardware**

971 The hardware used included two Siemens SIMATIC industrial personal computers (IPCs)  
 972 executing the SNOK services: a SIMATIC IPC227E for the PCS and a SIMATIC IPC427E  
 973 for the CRS. A VERSAstream packet broker (VS-1208BT-S) was used to aggregate the  
 974 mirrored traffic from the PCS and the CRS into two respective streams, one for each IPC.

975 **B.2.2. Windows XP / Windows 7 / Windows Server 2012 Installation**

976 The steps in this section describe the installation of SNOK Agents on endpoints with  
 977 Microsoft Windows operating systems (OSs).

- 978 1. Launch *SNOKAgentSetup.exe* from the Windows Agent folder in the installation  
 979 pack.
- 980 2. Click **Next>**.
- 981 3. Select both components, and then click **Next>**.
- 982 4. Input the username and password for administrative privileges, and then click **Install**.

- 983 5. Modify the configuration file located at *<installation directory>\SNOK-*  
984 *agent\bin\snokagentconfig.txt* to include the following information:
- 985 a. **idAgent**: a unique identifier (ID) that will not be used by any other agent that  
986 reports to the same SNOK Detector
  - 987 b. **detectorIP**: the Internet Protocol (IP) address of the SNOK Detector to which  
988 the agent will report
  - 989 c. **licenseKey**: the license key provided for the SNOK Detector

#### 990 **B.2.2.1. Start SNOK Agent Manually**

991 If the installation did not include selecting **Automatically start agent**, then follow the steps  
992 below to manually start the agent:

- 993 1. Open the command prompt.
- 994 2. Change the directory to *<installation directory>\bin\* by using the following  
995 command:

```
996 > cd C:\SNOK\bin\
```

- 997 3. Run the agent by using the following command and then pressing the **Enter** key:

```
998 > SNOKAgent.exe
```

#### 999 **B.2.2.2. Stop SNOK Agent Manually**

- 1000 1. Open the **Task Manager**.
- 1001 2. Open the **Processes** tab.
- 1002 3. Select the process name **SNOKAgent.exe**.
- 1003 4. Click the **End Task** button.

#### 1004 **B.2.3. Ubuntu 12 / Ubuntu 14 Installation**

- 1005 1. Copy the file *snoknetmonagent\_<version>.deb* into the */home* directory of the IPC.
- 1006 2. Add the Debian Wheezy universe to the apt sources file by using the following  
1007 command:

```
1008 > sudo echo "deb http://httpredir.debian.org/debian wheezy  
1009 main" >> /etc/apt/sources.list
```

- 1010 3. Install the libpcap-dev package by using the following command:

```
1011 > sudo apt-get install libpcap-dev
```

1012 4. Install the SNOK Agent from the Debian software package file by using the  
1013 following command:

```
1014 > sudo dpkg -I ~/snoknetmonagent_<version>.deb
```

1015 5. Modify the configuration file *snok-netmonconfig.txt* located in the directory  
1016 */etc/default/* to include the following information:

1017 a. **idAgent**: a unique ID that will not be used by any other agent that reports to  
1018 the same SNOK Detector

1019 b. **detectorIP**: the IP address of the SNOK Detector to which the agent will  
1020 report

1021 c. **licenseKey**: the license key provided for the SNOK Detector

## 1022 B.2.4. SNOK Detector Configuration

1023 The SNOK Detector comes installed as part of a preconfigured appliance, requiring final  
1024 configuration before integration into the asset owner's environment. The following  
1025 configuration must be completed on the appliance before installation:

1026 1. Obtain a license key from Secure-NOK. The media access control (MAC) address of  
1027 the network interface is needed to generate the license. On the appliance, execute the  
1028 following command to obtain the address, which will be the hexadecimal number  
1029 after `HWaddr`, in the format of `xx:xx:xx:xx:xx:xx`:

```
1030 sudo ifconfig eth0
```

1031 2. Copy the license key file *snoklicense.key* to the directory */home/snok/*.

1032 3. Start the configuration software by using the following command:

```
1033 > sudo /usr/share/snok/snok-config.sh
```

1034 4. Ensure that *1 (VMs Installation) SNOK Detector with local Visualizer* is highlighted,  
1035 and then press the **Enter** key.

1036 5. On the Database VM IP page, enter the IP address of the preconfigured appliance,  
1037 and then press the **Enter** key.

1038 6. On the Detector mode page, ensure the messages received are not forwarded  
1039 (isolated) and is selected, and then press the **Enter** key.

1040 7. On the Date-Time Synchronization page, select **1 Enter IP for Simple Network**  
1041 **Time Protocol Server** (Network Time Protocol [NTP] / Simple Network Time  
1042 Protocol [SNTP] server available), and then press the **Enter** key.

1043 8. On the NTP/SNTP IP page, type the IP address of the NTP server, and then press the  
1044 **Enter** key. The lab NTP server (10.100.0.15) was used for the build environment.

- 1045 9. On the External Event Reporting page, select any reporting methods, and then press  
 1046 the **Enter** key. The build configuration did not require any external reporting  
 1047 (e.g., syslog, email), so the *option 3 Go to next step* was selected.
- 1048 10. When prompted, enter the database password to enable the automated configuration.
- 1049 11. Start the snok-box service by using the following command:

```
> sudo service snok-box start
```

- 1051 12. Start the snok-dumper service by using the following command:

```
> sudo service snok-dumper start
```

1053 **B.3. Anomaly Scenarios**

1054 The agent-based anomaly detection method was demonstrated for the scenarios detailed in  
 1055 the following subsections. Each scenario includes a description of the anomaly, a detailed  
 1056 description of how each demonstration event was conducted in the CSMS environment, and  
 1057 the observed results.

1058 For the sake of brevity, only a subset of the alerts observed during the demonstration is  
 1059 shown. However, each anomaly scenario includes a screenshot of the alerts summary  
 1060 observed after the anomaly scenario had completed.

1061 **B.3.1. Web Browser Is Used to Access the Internet**

1062 The detection of unauthorized internet traffic on ICS networks is important for mitigating  
 1063 risk to the manufacturing system. Internet-accessible network connections introduce a  
 1064 gateway for malware into the ICS network, as well as a gateway for sensitive manufacturing  
 1065 system data to be exfiltrated out of the ICS network.

1066 This anomaly was executed on the CRS. A Hypertext Transfer Protocol (HTTP) server was  
 1067 installed and configured on a server with an internally routed public IP address (129.6.1.2).  
 1068 The Firefox web browser was used to connect to a web page, from the engineering  
 1069 workstation to the internet-based HTTP server.

|   |                                   |   |                           |   |   |              |
|---|-----------------------------------|---|---------------------------|---|---|--------------|
| Installed Base Mismatch   |                                   | Installed Base Mismatch : Unknown Process detected<br>Process Name: firefox-esr |                           |   |   |              |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 |                                   | 02/16/2018 13:12:02   | Unexpected new connection | A new IP address has been detected in the network | Source IP: 129.6.1.2<br>Destination IP: 192.168.0.20<br>Source MAC Address: 94:b8:c5:0e:e1:9f<br>Destination MAC Address: f8:b1:56:ba:09:a8 |              |
| 129.6.1.2<br>94:b8:c5:0e:e1:9f  | 192.168.0.20<br>f8:b1:56:ba:09:a8 | HTTP  |                           | 02/16/2018<br>13:11:59                            | 02/16/2018<br>13:13:01  | 0.15<br>0.98 |

1070

1071

1072

1073 **B.3.2. Data Exfiltration to the Internet via HTTP**

1074 Attacks against ICS, with the goal of information gathering, must (at some point) attempt to  
 1075 exfiltrate sensitive or proprietary data from the ICS network, potentially utilizing the internet  
 1076 as a transport mechanism. Monitoring for ICS devices communicating to other devices over  
 1077 the internet can help detect data exfiltration events, especially if the affected device does not  
 1078 normally communicate over the internet.

1079 This anomaly was executed on the CRS. An HTTP server and the PHP (Hypertext  
 1080 Preprocessor) server-side scripting language [19] were installed and configured on a server  
 1081 with an internally routed public IP address (129.6.1.2). A PHP web page was created to  
 1082 enable file uploads over HTTP. The web page was accessed by the Firefox web browser on  
 1083 the engineering workstation, and the sensitive file *ControlsSchematic.dwg*, an AutoCAD  
 1084 drawing file, was selected and uploaded to the server.

1085

|   |                     |                           |   |   |  |
|---|---------------------|---------------------------|---|---|--|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/16/2018 13:07:52 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 129.6.1.2<br>Destination IP: 192.168.0.20<br>Source MAC Address: 94:b8:c5:0e:e1:9f<br>Destination MAC Address: f8:b1:56:ba:09:a8 | Authorized by:<br><b>admin</b><br>Timestamp:<br>02/16/2018<br>13:12:00<br>Message: |
|---|---------------------|---------------------------|---|---|--|

1086

|   |                     |                         |  |                           |
|---|---------------------|-------------------------|--|---------------------------|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Engineering WS | 02/16/2018 13:10:23 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: wget | <a href="#">Authorize</a> |
|---|---------------------|-------------------------|--|---------------------------|

1087

| Source IP<br>Source MAC           | Destination<br>Destination MAC | Protocol Type | Start<br>Timestamp     | End<br>Timestamp       | Packets/second | kBits/second |
|-----------------------------------|--------------------------------|---------------|------------------------|------------------------|----------------|--------------|
| 192.168.0.20<br>f8:b1:56:ba:09:a8 | 129.6.1.2<br>94:b8:c5:0e:e1:9f | HTTP          | 02/16/2018<br>13:23:27 | 02/16/2018<br>13:24:30 | 0.17           | 0.08         |

1088 **B.3.3. European Institute for Computer Antivirus Research Virus Test File Is**  
 1089 **Detected on Host**

1090 Computer viruses and malware are serious threats to the ICS. They can undermine the ICS  
 1091 security, confidentiality, and stability, and can even sabotage the ICS. Providing the ability to  
 1092 detect viruses and malware in the ICS network is important.

1093 This anomaly was executed on the PCS. Before the CyberX platform tool was installed, a  
 1094 European Institute for Computer Antivirus Research (EICAR) test file was created and stored  
 1095 on the engineering workstation.

1096

| Host   | Timestamp           | Type                      | Description   |
|--|---------------------|---------------------------|---|
| NIST EL<br>Process Control<br>All Segments<br>Engineering WS | 02/21/2018 12:47:00 | Security Policy Violation | Security Policy Violation : Anti-Virus Event : Anti-Virus Disabled<br>Network Segment Security Policy Violation |

1097 **B.3.4. Host Scanning Is Performed on the Network**

1098 During the reconnaissance phase, an attacker may attempt to locate vulnerable devices on an  
 1099 ICS network. A host scan is one method to discover hosts or devices in the network. Once a  
 1100 host or device is discovered and identified, an attacker may attempt to exploit the host or  
 1101 device.

1102 This anomaly was executed on the PCS. The software Nmap [16] was used to perform a host  
 1103 discovery scan of the ICS network on the subnet 172.16.2.0/24. The scan originated from  
 1104 the cybersecurity virtual machine (CybersecVM), logically located in the test-bed LAN.

|  |                     |                           |   |  |  |
|--|---------------------|---------------------------|---|--|--|
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.80<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorized by:<br><b>admin</b><br>Timestamp:<br>02/21/2018<br>13:06:25<br>Message: |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.82<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorized by:<br><b>admin</b><br>Timestamp:<br>02/21/2018<br>13:06:15<br>Message: |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.84<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorized by:<br><b>admin</b><br>Timestamp:<br>02/21/2018<br>13:06:21<br>Message: |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.97<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.91<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.86<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.93<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorized by:<br><b>admin</b><br>Timestamp:<br>02/21/2018<br>13:06:18<br>Message: |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.88<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.95<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.9<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1  | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.99<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.85<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.8<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1  | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.81<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorized by:<br><b>admin</b><br>Timestamp:<br>02/21/2018<br>13:06:12<br>Message: |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.83<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.90<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.98<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.92<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:05:15 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.2.87<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize  |

1105

1106 **B.3.5. Port Scanning Is Performed on the Network**

1107 During the reconnaissance phase, an attacker may attempt to locate vulnerable services in an  
 1108 ICS network, likely probing for any open network ports to determine if a specific network  
 1109 service is available (e.g., Modbus). Once a vulnerable service is discovered, an attacker may  
 1110 attempt to exploit that service.

1111 This anomaly was executed on the CRS. The software Nmap [16] was used to perform a  
 1112 network scan for devices with the Modbus service enabled (Port 502). The scan originated  
 1113 from the CybersecVM, logically hosted on the historian located in the test-bed LAN.

1114

|  |                     |                         |  |           |
|--|---------------------|-------------------------|--|-----------|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Historian | 02/20/2018 13:43:42 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: nmap | Authorize |
|--|---------------------|-------------------------|--|-----------|

1115

| NetMonAgent   | Timestamp           | Type                      | Description                                       | Connection Details  | Authorization |
|---|---------------------|---------------------------|---|---|---------------|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/20/2018 13:44:29 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 192.168.0.10<br>Destination IP: 192.168.0.30<br>Source MAC Address: 00:15:5d:02:0a:0e<br>Destination MAC Address: 00:01:05:17:db:08  | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/20/2018 13:44:29 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 192.168.0.10<br>Destination IP: 192.168.0.60<br>Source MAC Address: 00:15:5d:02:0a:0e<br>Destination MAC Address: 00:30:de:00:c4:3c  | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/20/2018 13:44:29 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 192.168.0.10<br>Destination IP: 192.168.1.104<br>Source MAC Address: 00:15:5d:02:0a:0e<br>Destination MAC Address: 94:b8:c5:0e:a1:9f | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/20/2018 13:44:29 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 192.168.0.10<br>Destination IP: 192.168.1.104<br>Source MAC Address: 94:b8:c5:0e:a1:9f<br>Destination MAC Address: b0:d5:cc:f4:26:ec | Authorize     |

1116

|  |                     |                           |   |   |           |
|--|---------------------|---------------------------|---|---|-----------|
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:33:00 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.1.5<br>Source MAC Address: e4:90:69:3b:c2:c4<br>Destination MAC Address: 0c:c4:7a:31:3e:d7 | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:33:00 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.1.4<br>Source MAC Address: e4:90:69:3b:c2:c4<br>Destination MAC Address: 0c:c4:7a:31:44:47 | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:33:00 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.1.4<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/21/2018 13:33:00 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 10.100.0.28<br>Destination IP: 172.16.1.5<br>Source MAC Address: 00:15:5d:02:0a:08<br>Destination MAC Address: e4:90:69:3b:c2:c1 | Authorize |

1117

| Source IP<br>Source MAC           | Destination<br>Destination MAC     | Protocol Type | Start<br>Timestamp     | End<br>Timestamp       | Packets/second | kBits/second |
|-----------------------------------|------------------------------------|---------------|------------------------|------------------------|----------------|--------------|
| 192.168.0.10<br>00:15:5d:02:0a:0e | 192.168.0.30<br>00:01:05:17:db:08  | Modbus/TCP    | 02/20/2018<br>13:43:24 | 02/20/2018<br>13:44:27 | 0.49           | 0.00         |
| 192.168.0.10<br>00:15:5d:02:0a:0e | 192.168.0.60<br>00:30:de:00:c4:3c  | Modbus/TCP    | 02/20/2018<br>13:43:24 | 02/20/2018<br>13:44:27 | 0.15           | 0.00         |
| 192.168.0.10<br>00:15:5d:02:0a:0e | 192.168.1.104<br>94:b8:c5:0e:a1:9f | Modbus/TCP    | 02/20/2018<br>13:43:24 | 02/20/2018<br>13:44:27 | 0.76           | 0.01         |
| 192.168.0.10<br>94:b8:c5:0e:a1:9f | 192.168.1.104<br>b0:d5:cc:f4:26:ec | Modbus/TCP    | 02/20/2018<br>13:43:24 | 02/20/2018<br>13:44:27 | 0.38           | 0.00         |

1118 **B.3.6. Unauthorized Installation of Software**

1119 Many Linux distributions provide an automated method to download and install packages.  
 1120 Often, these packages originate from third parties and may not be validated against the ICS  
 1121 environments. Attackers may install unvalidated, or even malicious, packages to the ICS. The  
 1122 ability to detect unauthorized downloads and unauthorized installations of software is  
 1123 important.

1124 This anomaly was executed on the CRS. The Advanced Package Tool (apt-get) was used to  
 1125 install a small package with minimal dependencies (md5deep). The installation was  
 1126 performed on the engineering workstation via the command line.

1127

| Host  | Timestamp           | Type                    | Description  | Authorization |
|---|---------------------|-------------------------|--|---------------|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Robotic Driver | 02/20/2018 11:12:35 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: python           | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Robotic Driver | 02/20/2018 11:12:33 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: /bin/dbus-daemon | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Robotic Driver | 02/20/2018 11:12:05 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: [dpkg]           | Authorize     |

1128

| NetMonAgent   | Timestamp           | Type                      | Description                                       | Connection Details   | Authorization |
|---|---------------------|---------------------------|---|--|---------------|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/20/2018 11:13:12 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 192.168.1.5<br>Destination IP: 91.189.94.25<br>Source MAC Address: a0:ce:c8:1fbd:99<br>Destination MAC Address: 94:b8:c5:0e:e1:9f | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>NetworkAgent 1 | 02/20/2018 11:12:09 | Unexpected new connection | A new IP address has been detected in the network | Source IP: 192.168.1.5<br>Destination IP: 91.189.91.23<br>Source MAC Address: a0:ce:c8:1fbd:99<br>Destination MAC Address: 94:b8:c5:0e:e1:9f | Authorize     |

1129

| Source IP<br>Source MAC         | Destination<br>Destination MAC    | Protocol Type | Start<br>Timestamp     | End<br>Timestamp       | Packets/second | kBits/second |
|---------------------------------|-----------------------------------|---------------|------------------------|------------------------|----------------|--------------|
| 192.168.1.5<br>a0:ce:c8:1fbd:99 | 91.189.94.25<br>94:b8:c5:0e:e1:9f | HTTP          | 02/20/2018<br>11:12:05 | 02/20/2018<br>11:13:08 | 0.03           | 0.00         |

1130 **B.3.7. Unauthorized Programmable Logic Controller Firmware Update**

1131 Many ICS devices provide services to remotely update firmware over the network. These  
 1132 network services can also provide a mechanism for attackers to replace valid firmware with  
 1133 malicious firmware if the device is not protected.

1134 This anomaly was executed on the PCS. The Allen-Bradley programmable logic controller  
 1135 (PLC) implemented in the PCS contains an Ethernet module (1756-EN2T) that allows its  
 1136 firmware to be upgraded and downgraded over Ethernet/IP. The firmware was upgraded or  
 1137 downgraded using the ControlFLASH firmware upgrade tool.

1138

| Host  | Timestamp           | Type                    | Description  | Authorization |
|---|---------------------|-------------------------|--|---------------|
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Robotic Driver | 02/20/2018 11:12:35 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: python           | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Robotic Driver | 02/20/2018 11:12:33 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: /bin/dbus-daemon | Authorize     |
| NIST EL<br>Collaborative Robots Sys<br>All segments<br>Robotic Driver | 02/20/2018 11:12:05 | Installed Base Mismatch | Installed Base Mismatch : Unknown Process detected<br>Process Name: [dpkg]           | Authorize     |

1139

| Source IP<br>Source MAC          | Destination<br>Destination MAC    | Protocol Type | Start<br>Timestamp     | End<br>Timestamp       | Packets/second | kBits/second |
|----------------------------------|-----------------------------------|---------------|------------------------|------------------------|----------------|--------------|
| 192.168.1.5<br>a0:ce:c8:1f:bd:99 | 91.189.94.25<br>94:b8:c5:0e:e1:9f | HTTP          | 02/20/2018<br>11:12:05 | 02/20/2018<br>11:13:08 | 0.03           | 0.00         |

### 1140 B.3.8. Unauthorized PLC Logic Download

1141 Many PLCs enable remote access for uploading and downloading control logic to and from  
 1142 the controller. This service provides great convenience, but also provides a mechanism for  
 1143 attackers to remotely access the control logic and proprietary manufacturing information if  
 1144 the PLC is not protected.

1145 This anomaly was executed on the PCS. The Allen-Bradley software Studio 5000 was used  
 1146 to download the logic from the PCS PLC to the engineering workstation. Physical access to  
 1147 the PLC was required in order to change the operation mode from RUN to REMOTE RUN.

1148

|  |                     |  |   |   |           |
|--|---------------------|--|---|---|-----------|
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:24:41 | Abnormal communication pattern on a specific protocol between IP addresses | The communication between two IP addresses on a specific protocol is high in both number of packets and traffic bandwidth usage | Source IP: 172.16.2.102<br>Destination IP: 172.16.3.10<br>Source MAC Address: 00:1d:5c:c9:6d:42<br>Destination MAC Address: e4:90:69:3b:c2:c5<br>Protocol: CIP<br>[ 41(kbps) > 0(kbps) ]<br>[ 157(pps) > 0(pps) ] | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:24:41 | Abnormal communication pattern on a specific protocol between IP addresses | The communication between two IP addresses on a specific protocol is low in traffic bandwidth usage                             | Source IP: 172.16.2.4<br>Destination IP: 172.16.3.10<br>Source MAC Address: 0c:c4:7a:31:44:bd<br>Destination MAC Address: e4:90:69:3b:c2:c5<br>Protocol: TCP<br>[ 0(kbps) < 1(kbps) ]                             | Authorize |

### 1149 B.3.9. Unauthorized PLC Logic Modification

1150 As previously mentioned, many PLCs enable remote access for uploading and downloading  
 1151 control logic to and from the controller. This service provides great convenience, but also  
 1152 provides a mechanism for attackers to replace valid control logic with malicious logic if the  
 1153 device is not protected.

1154 This anomaly was executed on the PCS. The Allen-Bradley software Studio 5000 was used  
 1155 to upload new logic from the engineering workstation to the PCS PLC. Physical access to the  
 1156 PLC was required in order to change the operation mode from RUN to REMOTE RUN.

|  |                     |  |   |  |           |
|--|---------------------|--|---|--|-----------|
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:27:49 | Abnormal communication pattern on a specific protocol between IP addresses | The communication between two IP addresses on a specific protocol is high in both number of packets and traffic bandwidth usage | Source IP: 172.16.3.10<br>Destination IP: 172.16.2.102<br>Source MAC Address: 40:a8:f0:3d:48:a6<br>Destination MAC Address: e4:90:69:3b:c2:c0<br>Protocol: CIP<br>[ 50(kbps) > 0(kbps) ]<br>[ 19(pps) > 0(pps) ] | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:27:49 | Abnormal communication pattern on a specific protocol between IP addresses | The communication between two IP addresses on a specific protocol is high in both number of packets and traffic bandwidth usage | Source IP: 172.16.3.10<br>Destination IP: 172.16.2.102<br>Source MAC Address: e4:90:69:3b:c2:c5<br>Destination MAC Address: 00:1d:9c:c9:6d:42<br>Protocol: CIP<br>[ 99(kbps) > 0(kbps) ]<br>[ 37(pps) > 0(pps) ] | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:27:49 | Abnormal communication pattern between IP addresses                        | The communication between two IP addresses is high in terms of both packet and traffic bandwidth usage                          | Source IP: 172.16.2.102<br>Destination IP: 172.16.3.10<br>Source MAC Address: 00:1d:9c:c9:6d:42<br>Destination MAC Address: e4:90:69:3b:c2:c5<br>[ 37(kbps) > 0(kbps) ]<br>[ 125(pps) > 0(pps) ]                 | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:27:49 | Abnormal communication pattern between IP addresses                        | The communication between two IP addresses is high in terms of both packet and traffic bandwidth usage                          | Source IP: 172.16.3.10<br>Destination IP: 172.16.2.102<br>Source MAC Address: 40:a8:f0:3d:48:a6<br>Destination MAC Address: e4:90:69:3b:c2:c0<br>[ 50(kbps) > 0(kbps) ]<br>[ 19(pps) > 0(pps) ]                  | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:27:49 | Abnormal communication pattern between IP addresses                        | The communication between two IP addresses is high in terms of both packet and traffic bandwidth usage                          | Source IP: 172.16.3.10<br>Destination IP: 172.16.2.102<br>Source MAC Address: e4:90:69:3b:c2:c5<br>Destination MAC Address: 00:1d:9c:c9:6d:42<br>[ 99(kbps) > 0(kbps) ]<br>[ 37(pps) > 0(pps) ]                  | Authorize |

1157

### 1158 B.3.10. Unauthorized Connection Is Established Between ICS Devices

1159 An unauthorized connection between two ICS devices may indicate anomalous activity and  
1160 is important to discover, especially when the devices do not normally communicate.

1161 The anomaly was executed on the PCS. An unauthorized remote desktop session was  
1162 initialized from the human-machine interface (HMI) server to the object linking and  
1163 embedding for process control (OPC) server. Valid credentials were used to complete the  
1164 connection.

|  |                     |  |  |  |           |
|--|---------------------|--|--|--|-----------|
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:45:34 | Abnormal communication pattern on a specific protocol between IP addresses | The communication between two IP addresses on a specific protocol is high in traffic bandwidth usage | Source IP: 172.16.2.5<br>Destination IP: 172.16.1.4<br>Source MAC Address: 0c:c4:7a:32:b3:01<br>Destination MAC Address: e4:90:69:3b:c2:c5<br>Protocol: TCP<br>[ 116(kbps) > 109(kbps) ] | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>PCS NetMon | 02/22/2018 16:45:34 | Abnormal communication pattern on a specific protocol between IP addresses | The communication between two IP addresses on a specific protocol is high in traffic bandwidth usage | Source IP: 172.16.2.5<br>Destination IP: 172.16.1.4<br>Source MAC Address: e4:90:69:3b:c2:c4<br>Destination MAC Address: 0c:c4:7a:31:44:47<br>Protocol: TCP<br>[ 77(kbps) > 73(kbps) ]   | Authorize |

1165

### 1166 B.3.11. Host-Based Firewall Is Disabled

1167 The host-based firewall is an important part of the overall network security strategy.  
1168 Attackers may attempt to disable the firewall to gain access to the host. Any change in the  
1169 operating state of the host-based firewall may indicate malicious activity.

1170 This anomaly was executed on the PCS. The engineering workstation utilized the Microsoft  
1171 Windows 7 OS, which included the Windows Firewall component. The Windows Firewall  
1172 was manually disabled and enabled to generate the anomaly.

|              |                |                     |                           |   |
|--------------|----------------|---------------------|---------------------------|---|
| All Segments | Engineering WS | 02/23/2018 15:41:47 | Windows firewall status   | Windows firewall enabled                  |
| All Segments | Engineering WS | 02/23/2018 15:41:45 | Windows firewall status   | Windows firewall enabled                  |
| All Segments | Engineering WS | 02/23/2018 15:41:45 | Security Policy Violation | Network Segment Security Policy Violation |

1173

1174 **B.3.12. Host-Based Anti-Virus Software Is Disabled**

1175 The anti-virus software is an important part of the overall ICS security strategy. Attackers  
 1176 may attempt to disable the anti-virus software to download malwares to the host. Any change  
 1177 in the operating state of the anti-virus software may indicate malicious activity.

1178 This anomaly was executed on the PCS. Symantec Endpoint Protection anti-virus software  
 1179 was installed and operational on the engineering workstation. The software was manually  
 1180 disabled and enabled to generate the anomaly.

|              |                |                     |                           |   |
|--------------|----------------|---------------------|---------------------------|---|
| All Segments | Engineering WS | 02/23/2018 15:43:07 | Antivirus status          | AntiVirus protection disabled             |
| All Segments | Engineering WS | 02/23/2018 15:43:07 | Security Policy Violation | Network Segment Security Policy Violation |

1181

1182 **B.3.13. Host Central Processing Unit Load Is Increased**

1183 Most hosts in the ICS environment are running a predefined set of tasks or schedules. The  
 1184 system load of each host usually closely follows a routine or pattern. Any change or  
 1185 deviation from the routine could indicate malicious activity or abnormal or fault behavior of  
 1186 the ICS.

1187 This anomaly was executed on the PCS. The software Prime95 [20] was installed on the  
 1188 engineering workstation to generate the anomaly. The Prime95 torture test option “Blend”  
 1189 was used to execute a search for large prime numbers, resulting in a central processing unit  
 1190 utilization increase that was continuously greater than 95 percent.

| NetworkSegment      | Host   | Timestamp (Detector) | Type   | Description                          |
|---------------------|--|----------------------|--|--------------------------------------|
| Any<br>All Segments | All Segments:HMI Host<br>All Segments:Controller<br>All Segments:Historian VM<br>All Segments:OPC DA Server<br>All Segments:Engineering WS | From<br>To           | Any Agent started<br>Detector started<br>USB event<br>CPU load | Free text search                     |
| All Segments        | Engineering WS   | 02/27/2018 11:41:16  | CPU load   | CPU usage normal<br>CPU Load: 32%    |
| All Segments        | Engineering WS   | 02/27/2018 11:38:44  | CPU load   | CPU usage increased<br>CPU Load: 99% |
| All Segments        | Engineering WS   | 02/27/2018 11:27:39  | CPU load   | CPU usage normal<br>CPU Load: 31%    |

1191

1192 **B.3.14. Unauthorized Detachment of Keyboard to Host**

1193 While access to unused Universal Serial Bus (USB) ports can be denied through numerous  
 1194 physical means, the potential may still exist for an attacker to simply remove an attached  
 1195 USB device to gain access to a USB port. Detection of the disconnection of an input device  
 1196 may indicate malicious activity.

1197 This anomaly was executed on the PCS. A USB keyboard attached to the engineering  
 1198 workstation was temporarily disconnected from the USB port.

|  |                     |                           |   |           |
|--|---------------------|---------------------------|---|-----------|
| NIST EL<br>Process Control<br>All Segments<br>Engineering WS | 02/27/2018 11:47:18 | Security Policy Violation | Security Policy Violation : USB Event : Device Inserted<br>Site Security Policy Violation<br>(Device class: Device) | Authorize |
| NIST EL<br>Process Control<br>All Segments<br>Engineering WS | 02/27/2018 11:47:10 | Security Policy Violation | Security Policy Violation : USB Event : Device Removed<br>Site Security Policy Violation<br>(Device class: Device)  | Authorize |

1199

1200 **B.3.15. Unauthorized Insertion of USB Storage Device**

1201 Portable USB storage devices could be a threat to the ICS. An unauthorized USB device may  
1202 contain malware. Once inserted into a host, the malware can potentially gain control of the  
1203 host and infect other hosts in the ICS network.

1204 This anomaly was executed on the PCS. A USB storage device (flash drive) was temporarily  
1205 connected to the engineering workstation.

| Host   | Timestamp           | Type                      | Description   | Authorization |
|--|---------------------|---------------------------|---|---------------|
| NIST EL<br>Process Control<br>All Segments<br>Engineering WS | 02/27/2018 11:19:01 | Security Policy Violation | Security Policy Violation : USB Event : Device Inserted<br>Site Security Policy Violation<br>(Device class: Device) | Authorize     |
| NIST EL<br>Process Control<br>All Segments<br>Engineering WS | 02/27/2018 11:18:56 | Security Policy Violation | Security Policy Violation : USB Event : Device Removed<br>Site Security Policy Violation<br>(Device class: Device)  | Authorize     |

1206

1207 **Appendix C. CyberX Supplemental Information**

1208 The CyberX platform delivers continuous operational technology (OT) threat monitoring and  
1209 asset discovery, combining a deep understanding of industrial protocols, devices, and  
1210 applications with OT-specific behavioral analytics, threat intelligence, risk and vulnerability  
1211 management, and automated threat modeling. The platform is delivered as a preconfigured  
1212 appliance, including the Internet Protocol (IP) address, subnet mask, default gateway, and  
1213 Domain Name System (DNS) servers utilized in the build environment.

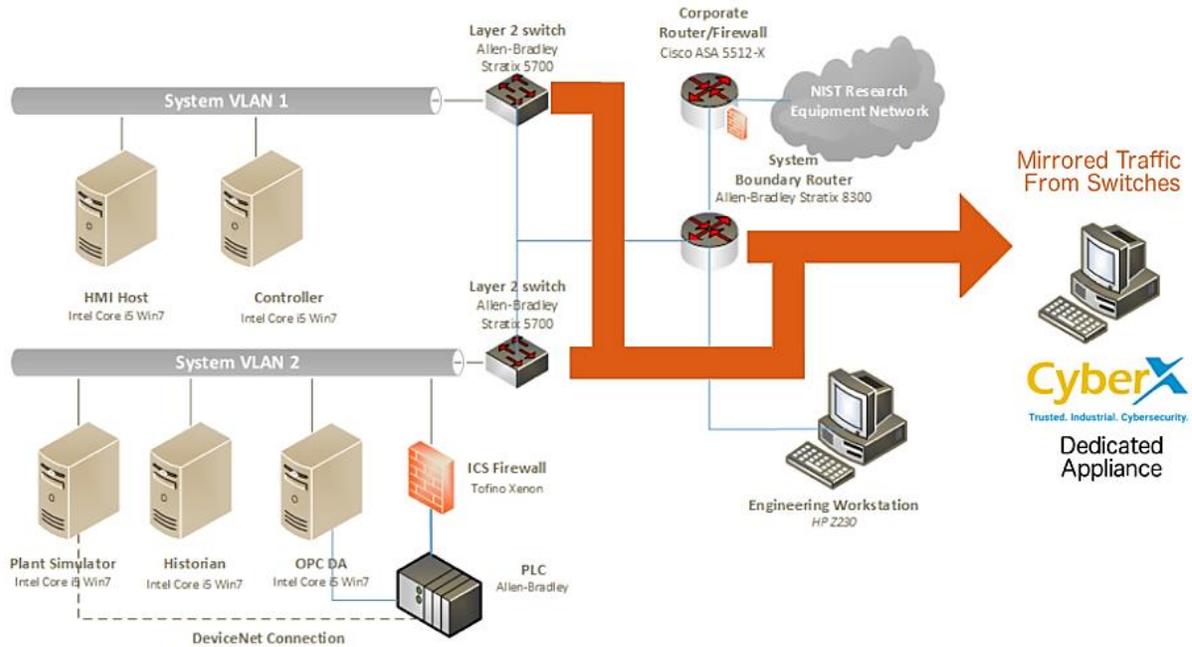
1214 **C.1. Build Architecture**

1215 The CyberX appliance was physically installed in the measurement rack of the Cybersecurity  
1216 for Smart Manufacturing Systems (CSMS) environment. Three existing Switch Port  
1217 Analyzer (SPAN) ports from each system (collaborative robotic system [CRS] and process  
1218 control system [PCS]) were connected to dedicated network interfaces on the appliance, for a  
1219 total of six SPAN ports. The SPAN port connections to the appliance, within the PCS and  
1220 CRS networks, are shown in Figure C-1 and Figure C-2, respectively.

1221 Enterprises typically deploy multiple CyberX appliances across various geographically  
1222 distributed sites, along with a central manager that is used to aggregate asset, vulnerability,  
1223 and threat information from each CyberX appliance, and to manage software updates and  
1224 configurations for each individual appliance.

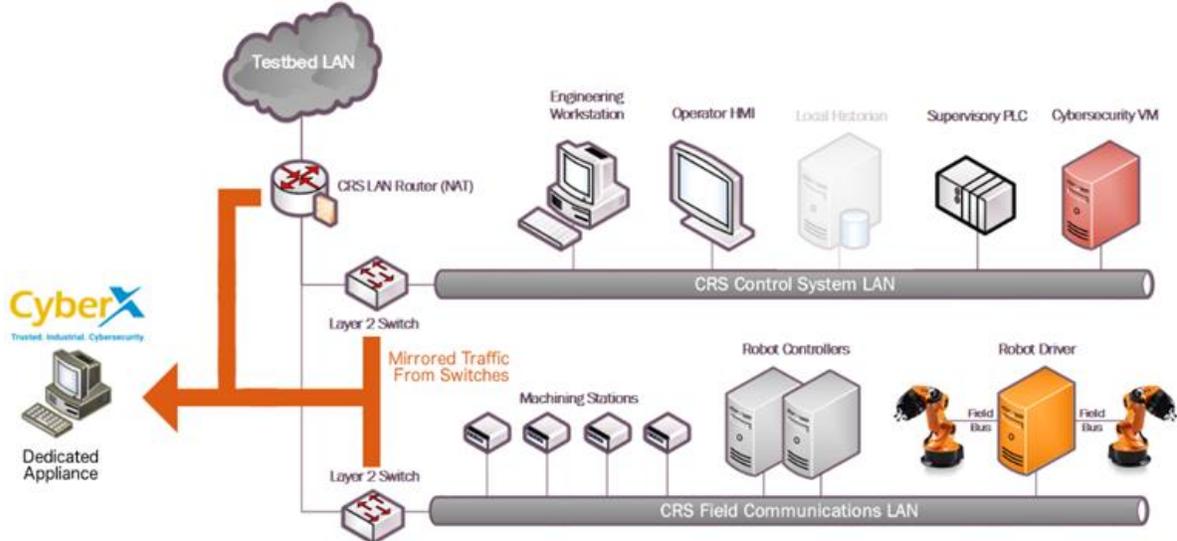
1225 The appliance network was connected to the demilitarized zone (DMZ) network located in  
1226 the test bed's measurement rack, to isolate the appliance's network traffic from the rest of the  
1227 network traffic. Engineering laptops were used to interface with the CyberX console  
1228 graphical user interface (GUI) via physical connections to the DMZ. More information  
1229 regarding the specific configuration of the test-bed network can be found in Section 3.

1230 **Figure C-1 SPAN Port Connections to the CyberX Appliance in the PCS**



1231

1232 **Figure C-2 SPAN Port Connections to the CyberX Appliance in the CRS**



1233

1234 **C.2. Installation and Configuration**

1235 Physical hardware and software were provided by CyberX for this demonstration. After the  
 1236 hardware appliance was received, it was installed into the CSMS test bed. Soon after the  
 1237 initial installation, engineers from CyberX arrived on site to complete the installation and  
 1238 configuration of the product. The following subsections describe the steps taken to install and  
 1239 configure the appliance.

1240 **C.2.1. Configuration Guide**

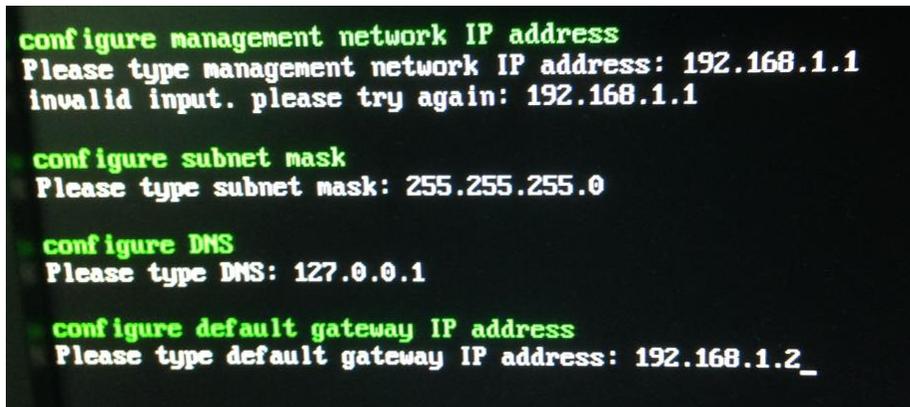
1241 The CyberX appliance was received preconfigured for the build environment, with the proper  
1242 IP address, subnet mask, default gateway, and DNS server. If reconfiguration is needed, then  
1243 access the server via the command line and type the following command:

1244 

```
> cyberx-xsense-network-reconfigure
```

1245 This will open a dialog for the configuration, similar to the dialog shown in Figure C-3.

1246 **Figure C-3 CyberX Network Reconfiguration Program on the Appliance**



```
configure management network IP address
Please type management network IP address: 192.168.1.1
invalid input. please try again: 192.168.1.1

configure subnet mask
Please type subnet mask: 255.255.255.0

configure DNS
Please type DNS: 127.0.0.1

configure default gateway IP address
Please type default gateway IP address: 192.168.1.2_
```

1247

1248 **C.2.2. Configuration of Forwarding Rules**

1249 The CyberX platform is typically combined with an existing security information and event  
1250 management (SIEM) system. The following steps describe the process to forward data from  
1251 CyberX to the SIEM:

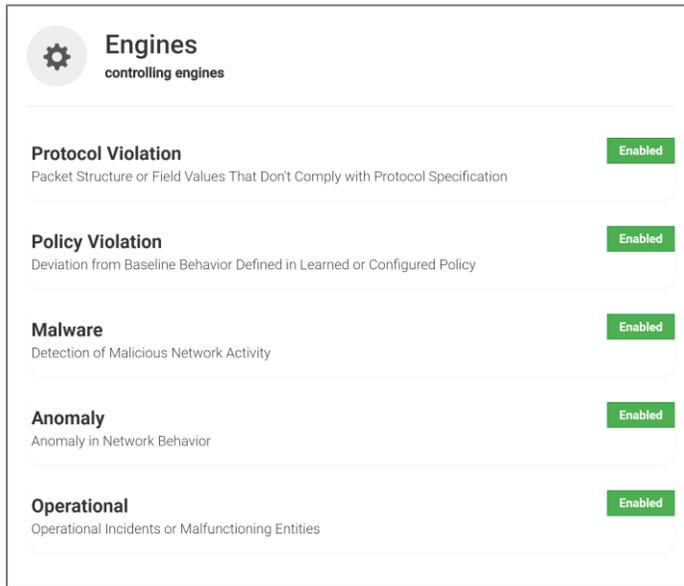
- 1252 1. Select **Forwarding** from the navigation menu on the CyberX console.
- 1253 2. Select **Create Forwarding Rule**.
- 1254 3. Complete the required information for the Forwarding Rule, and then select **Submit**.

1255 **C.2.3. Enabling Self-Learning Analytics**

1256 The CyberX platform has five different self-learning analytics engines that are used to detect  
1257 various types of behavioral anomalies within the network. The following steps describe the  
1258 process to enable individual analytics engines:

- 1259 1. Select **System Settings** from the navigation menu on the CyberX console.
- 1260 2. Click the **Enabled/Disabled** button next to each engine to enable or disable the  
1261 engine. If an engine is enabled, then the button will indicate **Enabled** and will be  
1262 illuminated with a green background color. An example with all five engines enabled  
1263 is shown in Figure C-4.

1264 **Figure C-4 Example Screenshot with All Five Self-Learning Analytics Enabled**



1265

### 1266 **C.3. Anomaly Scenarios**

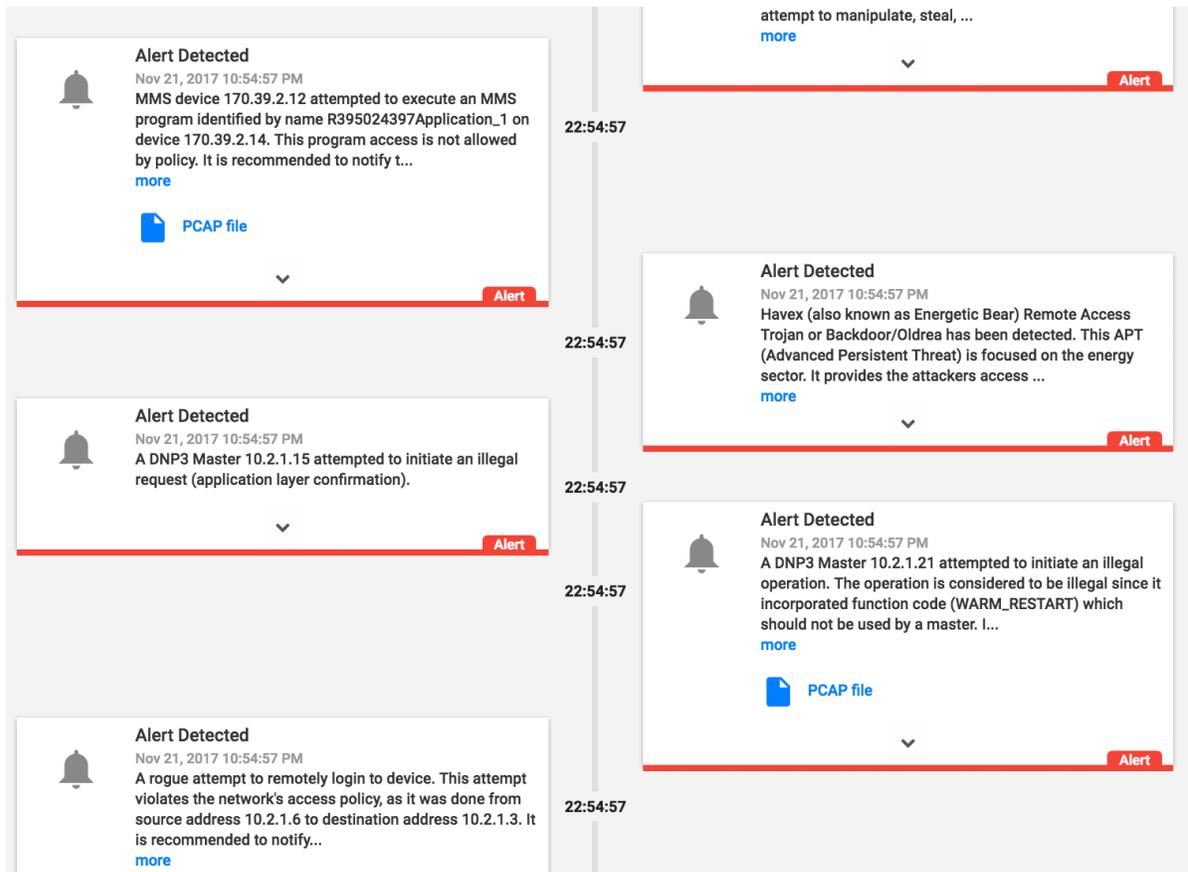
1267 The network-based anomaly detection method was demonstrated for the scenarios detailed in  
1268 the following subsections. Each scenario includes a description of the anomaly, a detailed  
1269 description of how each demonstration event was conducted in the CSMS environment, and  
1270 the observed results.

1271 For the sake of brevity, only a subset of the alerts observed during the demonstration is  
1272 shown. However, each anomaly scenario includes a screenshot of the alerts summary  
1273 observed after the anomaly scenario had completed.

1274 Alerts can be observed in the Alerts dashboard, grouped by the severity and type of alert, as  
1275 well as in the Event Log (timeline view). The Event Log view is shown in the screenshot in  
1276 Figure C-5.

1277

**Figure C-5 Event Log (Timeline View) of Real-Time Alerts in the CyberX Console**

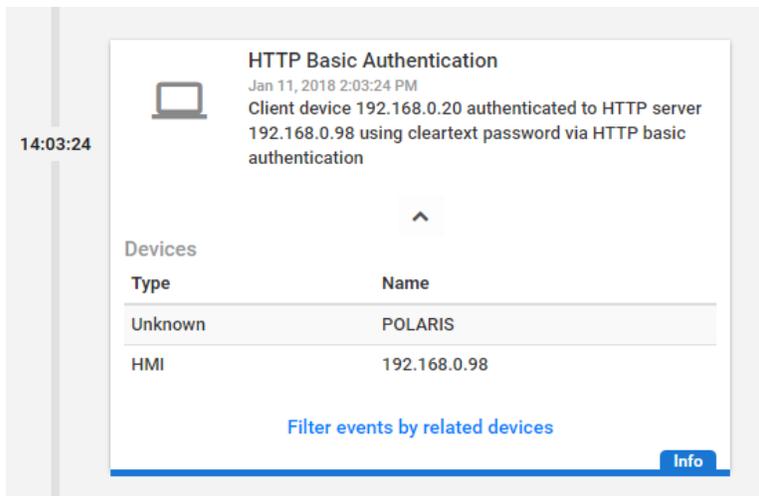


1278

1279 **C.3.1. Unencrypted Hypertext Transfer Protocol Credentials Are Detected on**  
1280 **the Network**

1281 Unencrypted or plaintext credentials transmitted over a network are a vulnerability for  
1282 industrial control systems (ICS) networks. If packets containing these credentials are  
1283 intercepted, then the credentials can be easily unmasked and can be used to obtain  
1284 unauthorized access to devices or services that use those credentials. This vulnerability can  
1285 be amplified if multiple devices utilize the same credentials.

1286 This anomaly was executed on the CRS. An Apache [17] Hypertext Transfer Protocol  
1287 (HTTP) server was configured on Machining Station 1 and contained a directory that was  
1288 protected by HTTP basic authentication. The web pages hosted in the protected directory  
1289 enabled an operator to remotely view machine status information. The connection was  
1290 initiated from the Firefox browser on the engineering workstation.

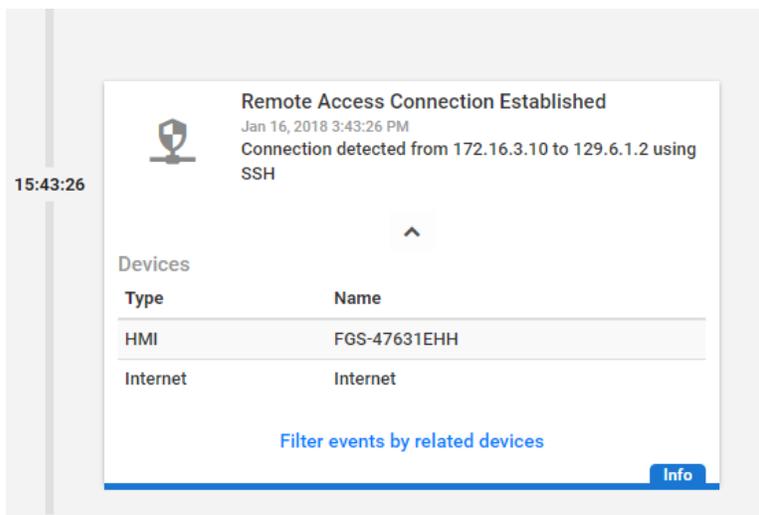


1291

### 1292 C.3.2. Unauthorized Secure Shell Session Is Established with an Internet-Based Server

1293 A Secure Shell (SSH) session is an encrypted and secure connection for remotely sending  
 1294 commands over a network. However, unauthorized SSH sessions with internet-based servers  
 1295 could indicate malicious activity. Attackers can use an SSH session to gain access to the ICS  
 1296 device and network.

1297 This anomaly was executed on the PCS. The OpenSSH [21] suite was installed and  
 1298 configured on a server with an internally routed public IP address (129.6.1.2). The  
 1299 open-source SSH client `PuTTY` [12] was used to establish a connection with the SSH service  
 1300 from the engineering workstation to the internet-based server.



1301

### 1302 C.3.3. Data Exfiltration to the Internet via DNS Tunneling

1303 Attacks against ICS, with the goal of information gathering, must (at some point) attempt to  
 1304 exfiltrate sensitive or proprietary data from the ICS network, potentially utilizing the internet  
 1305 as a transport mechanism. Monitoring for ICS devices communicating to other devices over  
 1306 the internet can help detect data exfiltration events, especially if the affected device does not  
 1307 normally communicate over the internet.

1308 This anomaly was executed on the CRS. A script was written in Python [14] to exfiltrate the  
1309 file contents via DNS tunneling. The DNS request functionality was enabled by the Linux  
1310 command-line tool `nslookup`. A DNS Type A was record was added to the test-bed DNS  
1311 server, mapping the `*.nist.gov` domain to our local internet-based server IP address  
1312 (129.6.1.2).

1313 To exfiltrate the file, the Python script would first read 30 bytes from the file  
1314 `measurements.cmm`, convert the bytes into a hexadecimal representation encoded as an  
1315 American Standard Code for Information Interchange string, and concatenate the string as a  
1316 subdomain with the Uniform Resource Identifier (URI) `.nist.gov`. The resulting URI is  
1317 sent to the `nslookup` tool, which subsequently transmitted the DNS request. This process  
1318 repeated until the complete file contents were exfiltrated.

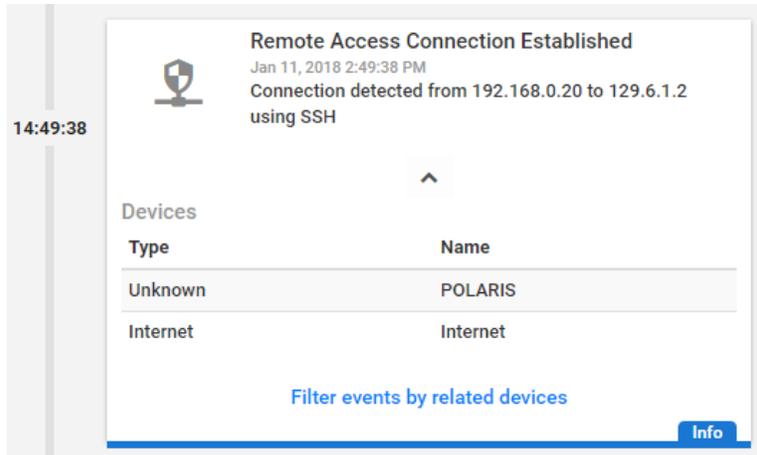
The screenshot displays a security alert interface. At the top, a bell icon is next to the heading "Alert Detected" and the timestamp "Jan 18, 2018 11:19:20 AM". The main text of the alert reads: "DNS client 192.168.0.20 sent a name query of type A to resolve name 202020302e30303036c39020c390202031393520c3900a.nist.gov which is not allowed by policy. It is recommended to notify the security off...". Below this text is a blue "more" link and a "PCAP file" download button. A "Related Alerts" section shows a "POLICY VIOLATION" titled "Unauthorized DNS Name Query | 4 minutes ago" with a truncated description. A "Devices" table lists two entries: "Domain Controller" (LAN-AD) and "Unknown" (POLARIS). A "Filter events by related devices" link is at the bottom. A red "Alert" button is visible in the bottom right corner of the alert card.

1319

### 1320 C.3.4. Data Exfiltration to the Internet via Secure Copy Protocol

1321 As previously mentioned, attacks against ICS, with the goal of information gathering, must  
1322 (at some point) attempt to exfiltrate the data from the ICS network, potentially utilizing the  
1323 internet as a transport mechanism. Monitoring for ICS devices communicating to other  
1324 devices over the internet can help detect data exfiltration events, especially if the affected  
1325 device does not normally communicate over the internet. Depending on the protocol used for  
1326 exfiltration, the file contents and/or data being exfiltrated may be ascertainable (e.g., specific  
1327 file types transferred using the File Transfer Protocol [FTP] protocol), providing insight into  
1328 the impact of the event.

1329 This anomaly was executed on the CRS. The OpenSSH [21] suite was installed and  
1330 configured on a server with an internally routed public IP address (129.6.1.2). The secure  
1331 copy protocol was then used to transfer a sensitive file over SSH from the engineering  
1332 workstation to the internet.

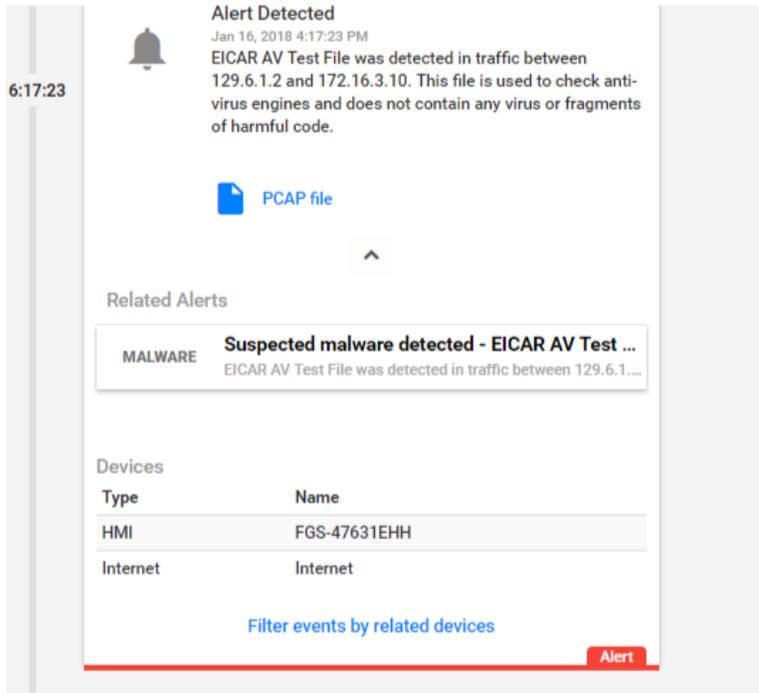


1333

1334 **C.3.5. European Institute for Computer Antivirus Research Virus Test File Is**  
1335 **Detected on the Network**

1336 Malware and computer viruses are serious threats to ICS. Malware can undermine ICS  
1337 security, confidentiality, and stability, with the potential to sabotage the ICS. Providing the  
1338 ability to detect the presence of viruses and malware in the ICS network is important for  
1339 minimizing risk to the manufacturing system.

1340 This anomaly was executed on the PCS. The European Institute for Computer Antivirus  
1341 Research (EICAR) virus test file was transferred from the human-machine interface (HMI)  
1342 server to the object linking and embedding for process control (OPC) server by using  
1343 Windows File Sharing (Server Message Block protocol).

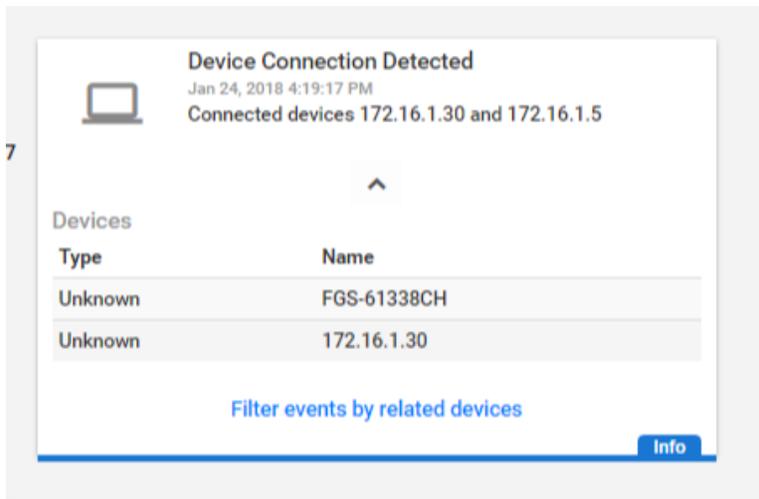


1344

1345 **C.3.6. Unauthorized Device Is Connected to the Network**

1346 It is important to identify all devices on the ICS network, for a complete risk analysis and for  
 1347 minimizing potential attack vectors. The detection of unauthorized devices attached to the  
 1348 ICS network may indicate anomalous activity. These unauthorized devices are important to  
 1349 find and remove, especially because the purpose of an unauthorized device is unknown and  
 1350 may be malicious.

1351 This anomaly was executed on the PCS. The engineering laptop (Windows 7 operating  
 1352 system) was removed from the network during the baseline analysis phase of the product and  
 1353 was later connected to Virtual Local Area Network (VLAN)-2 to execute the anomaly. After  
 1354 the initial connection, background traffic was automatically generated onto the network by  
 1355 the laptop.



1356

1357 **C.3.7. Denial-of-Service Attack Is Executed Against the ICS Local Area Network**

1358 Disruptive attacks, like a denial of service (DoS), are a serious threat to ICS, especially ICS  
1359 that rely heavily on networks to communicate. An attacker can launch a DoS attack on ICS  
1360 and disrupt normal operations, with potentially debilitating effects to the system. The ability  
1361 to detect such attacks is important to protect the manufacturing system.

1362 This anomaly was executed on the PCS. The Linux **ping** command-line tool was used to  
1363 transmit a flood of Internet Control Message Protocol (ICMP) packets to the OPC server.  
1364 The anomaly utilizes **ping**'s `flood` flag to inundate the OPC server with ICMP packets.  
1365 Each ICMP packet requires fragmentation, due to its large size (3,000 bytes), configured  
1366 using the packet-size flag.



## Alert Report

ID: 1206

Anomaly | 01/17/2018 11:01:12

### ICMP Flooding

An abnormal quantity of ICMP traffic was detected in the network which could be the result of an ICMP flooding attack. Number of ICMP packets detected was: 65.

1367

1368 **C.3.8. Data Exfiltration Between ICS Devices via User Datagram Protocol**

1369 An unauthorized file transfer between two ICS devices could indicate anomalous activity and  
1370 is important to identify, especially when the devices do not normally communicate or when  
1371 the exchange of files is unauthorized.

1372 This anomaly was executed on the CRS. A tape archive file was transmitted from the  
1373 cybersecurity virtual machine (CybersecVM) to the engineering workstation by using the  
1374 Linux utility netcat and User Datagram Protocol (UDP) sockets. UDP Port 9999 was used for  
1375 the transfer.

12:55:28

**Alert Detected**  
 Jan 18, 2018 12:55:28 PM  
 A service not allowed by policy has been detected. Client: 192.168.0.20, Server: 129.6.1.2

 [PCAP file](#)

^

**Related Alerts**

**POLICY VIOLATION** **Service Mapping** | 2 minutes ago  
 A service not allowed by policy has been detected. Client: 1...

**Devices**

| Type     | Name     |
|----------|----------|
| Unknown  | POLARIS  |
| Internet | Internet |

[Filter events by related devices](#)

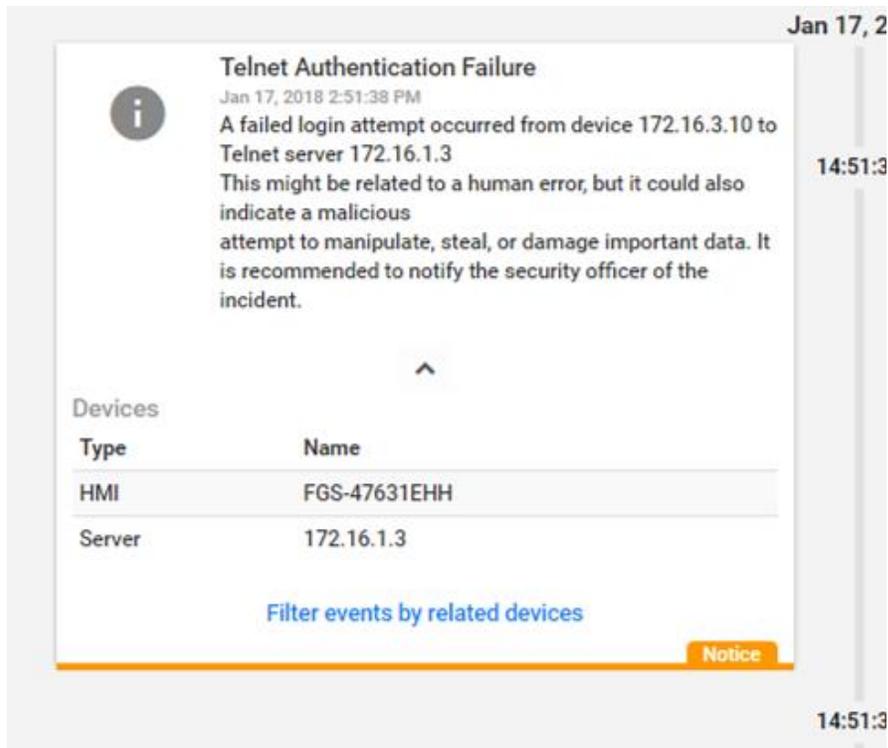
Alert

1376

1377 **C.3.9. Invalid Credentials Are Used to Access a Networking Device**

1378 Authentication systems that are not rate-restricted may be vulnerable to password-guessing  
 1379 attacks, especially if the default credentials of the device have not been changed. Compiled  
 1380 lists containing default user credentials are freely available on the internet, as are lists of  
 1381 commonly used usernames and passwords. Given enough time, an attacker may be able to  
 1382 access vulnerable systems by using a brute-force password attack.

1383 This anomaly was executed on the PCS. The Allen-Bradley software Studio 5000 was used  
 1384 to download the logic from the PCS programmable logic controller (PLC) to the engineering  
 1385 workstation. Physical access to the PLC was required in order to change the operation mode  
 1386 from RUN to REMOTE RUN.



1387

### 1388 C.3.10. Brute-Force Password Attack Against a Networking Device

1389 As previously mentioned, authentication systems that are not rate-restricted may be  
1390 vulnerable to password-guessing attacks, especially if the default credentials of the device  
1391 have not been changed. Compiled lists containing default user credentials are freely available  
1392 on the internet, as are lists of commonly used usernames and passwords. Given enough time,  
1393 an attacker may be able to access vulnerable systems by using a brute-force password attack.

1394 This anomaly was executed on the PCS. The software Nmap [16] was used to generate the  
1395 brute-force password attack by using the script `telnet-brute`. The attack was pointed at  
1396 the PCS router, which has a Telnet service for remote configuration and is protected by a  
1397 password. The service was not configured to limit the number of authentication attempts.

**Alert Detected**  
 Jan 17, 2018 3:22:43 PM  
 Device 10.100.0.28 attempted to authenticate with Server 172.16.1.3 on port 23 using different default credentials more frequently than expected.  
 This could represent suspicious behavior.  
 It is recommended to notify the security officer about the incident.

PCAP file

**Related Alerts**

**ANOMALY Password Guessing Attempt Detected | just now**  
 Device 10.100.0.28 attempted to authenticate with Server 1...

**Devices**

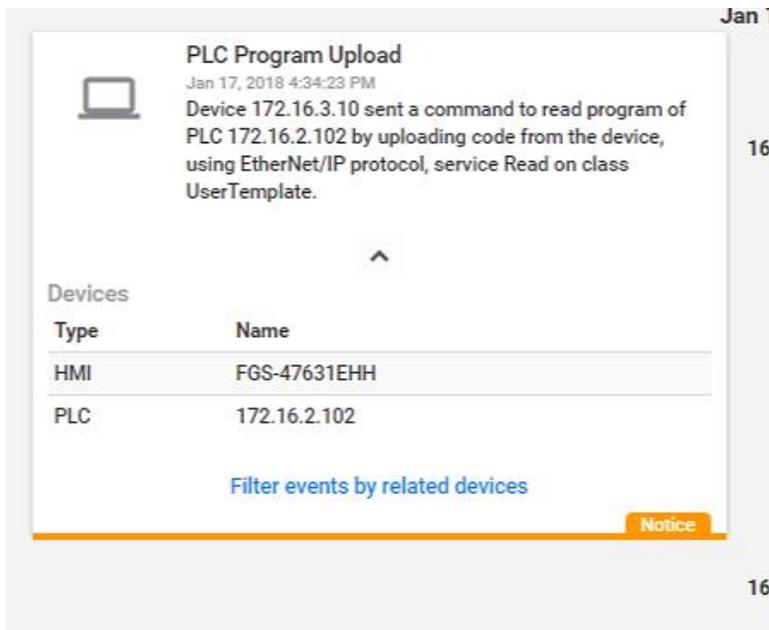
| Type   | Name        |
|--------|-------------|
| Server | 10.100.0.28 |
| Server | 172.16.1.3  |

1398

1399 **C.3.11. Unauthorized PLC Logic Download**

1400 Many ICS devices provide services to remotely update control logic over the network. These  
 1401 network services can also provide a mechanism for attackers to replace valid control logic  
 1402 with malicious logic if the device is not protected.

1403 This anomaly was executed on the PCS. The Allen-Bradley software Studio 5000 was used  
 1404 to download the logic from the PCS PLC to the engineering workstation. Physical access to  
 1405 the PLC was required in order to change the operation mode from RUN to REMOTE RUN.



1406

### 1407 **C.3.12. Unauthorized PLC Logic Update – CRS**

1408 Many ICS devices provide services to remotely update control logic over the network. These  
1409 network services can also provide a mechanism for attackers to replace valid control logic  
1410 with malicious logic if the device is not protected.

1411 This anomaly was executed on the CRS. The TwinCAT eXtended Automation Engineering  
1412 (XAE) software from Beckhoff was used to deploy new logic to the CRS PLC. The  
1413 deployment was performed by using the engineering laptop while the PLC was in the  
1414 ONLINE mode. The unauthorized logic was functionally compatible with the authorized  
1415 logic that it replaced, with minor modifications.

14:28:59

**Alert Detected**  
 Jan 16, 2018 2:28:59 PM  
 PLC 192.168.0.30 was programmed from device 192.168.0.147 using protocol AMS, which is not defined as a Programming Device.  
 This is not allowed by policy.  
 It is recommended to notify the security offi...  
[more](#)

^

**Related Alerts**

**POLICY VIOLATION** **Unauthorized PLC Programming | 1 minute ago**  
 PLC 192.168.0.30 was programmed from device 192.168.0...

**Devices**

| Type                | Name          |
|---------------------|---------------|
| Engineering Station | 192.168.0.30  |
| PLC                 | 192.168.0.147 |

[Filter events by related devices](#)

Alert

1416

1417 **C.3.13. Unauthorized PLC Logic Update – PCS**

1418 As previously mentioned, many ICS devices provide services to remotely update control  
 1419 logic over the network. These network services can also provide a mechanism for attackers to  
 1420 replace valid control logic with malicious software if the device is not protected.

1421 This anomaly was executed on the PCS. The Allen-Bradley software Studio 5000 was used  
 1422 to upload new logic from the engineering workstation to the PCS PLC. Physical access to the  
 1423 PLC was required in order to change the operation mode from RUN to REMOTE RUN.

1424

The screenshot displays an alert titled "Alert Detected" with a bell icon. The timestamp is "Jan 17, 2018 4:36:33 PM". The main text reads: "PLC 172.16.2.102 was programmed from device 172.16.3.10 using protocol ETHERNET/IP, which is not defined as a Programming Device. This is not allowed by policy. It is recommended to notify the securit...". A "more" link is present. Below the text is a "PCAP file" icon. Underneath is a "Related Alerts" section with a table entry: "POLICY VIOLATION Unauthorized PLC Programming | 4 minutes ago PLC 172.16.2.102 was programmed from device 172.16.3.1...". At the bottom is a "Devices" table with columns "Type" and "Name".

| Type | Name         |
|------|--------------|
| HMI  | FGS-47631EHH |
| PLC  | 172.16.2.102 |

1425

1426 **C.3.14. Undefined Modbus Transmission Control Protocol Function Codes Are Transmitted to the PLC**

1427 Communications that do not conform to the defined specifications of the industrial protocol  
 1428 may cause an ICS device to act in an undefined or unsafe manner. Depending on the  
 1429 manufacturing process and the ICS device, the nonconforming communications may or may  
 1430 not be impactful, but investigation into the cause is warranted.

1431 This anomaly was executed on the CRS. Python [14] was used to create a Modbus  
 1432 Transmission Control Protocol (TCP) message with the undefined function code value of 49  
 1433 (0x31). The message was generated by the CybersecVM and was transmitted to the PLC  
 1434 Modbus server.

ID: 1512

## Unpermitted Usage of Modbus Function Code

Policy Violation | Jan 18, 2018 1:48:18 PM ( 2 minutes ago )

MODBUS device 192.168.0.10 attempted to initiate a Request (function code 49) which is not allowed by policy. It is recommended to notify the security officer of the incident.



### Mitigation

- Consult a relevant Control Systems Engineer to validate this infraction.

### Notifications

- PCAP file exists.
- If valid, CyberX platform can learn this behavior for future use, at 'Operations'.

1435

### 1436 C.3.15. Unauthorized Ethernet/IP Scan of the Network

1437 During the reconnaissance phase, an attacker may attempt to locate vulnerable services in an  
1438 ICS network and will likely include probing for ICS-specific services (e.g., Ethernet/IP).  
1439 Once a vulnerable service, host, or device is discovered, an attacker may attempt to exploit  
1440 that entity.

1441 This anomaly was executed on the PCS. The software Nmap [16] was used to perform a port  
1442 scan (Ports 1 through 1024) against two hosts: the HMI and the plant controller. The scan  
1443 originated from the CybersecVM, logically located in the test-bed local area network (LAN).

1444 This anomaly was executed on the PCS. The software Nmap [16] was used to perform an  
1445 Ethernet/IP device scan by using the script `enip-info`. The scan was pointed at the PCS  
1446 subnet `172.16.2.100/28` and was executed by the CybersecVM in the test-bed LAN.



**Alert Detected**

Jan 19, 2018 10:18:00 AM

**Address scan detected.**

Scanning address: 10.100.0.28

Scanned subnet: 172.16.0.0/16

Scanned addresses: 172.16.2.1, 172.16.2.10, 172.16.2.28, 172.16.2.37, 172.16.2.54...

It is recommended to notify the ...

[more](#)

10:18

 [PCAP file](#)



**Related Alerts**

**ANOMALY** **Address Scan Detected** | 2 minutes ago

Address scan detected. Scanning address: 10.100.0.28 Sca...

**Devices**

| Type   | Name        |
|--------|-------------|
| Server | 10.100.0.28 |

[Filter events by related devices](#)

Alert

1447

1448 **Appendix D. OSIsoft Process Information Supplemental Information**

1449 The OSIsoft Process Information (PI) System is a suite of software applications for  
1450 capturing, analyzing, and storing real-time data for industrial processes. Although the PI  
1451 System is typically utilized as a process historian, the PI System is also utilized to collect,  
1452 store, and manage data in real time. Interface nodes retrieve data from disparate sources to  
1453 the PI Server, where the PI Data Archive resides. Data is stored in the Data Archive and is  
1454 accessible in the assets defined in the Asset Framework (AF). Data is then typically accessed,  
1455 either directly from the Data Archive or from the AF Server, by using tools in the PI  
1456 visualization suite. Typically, most PI System users consume data by accessing the AF  
1457 Server, rather than directly accessing the Data Archive. This build demonstrates how PI can  
1458 be leveraged to monitor for specific behavioral anomalies of the process that may be caused  
1459 by cybersecurity incidents, and to alert operators and cybersecurity personnel of the  
1460 anomalies.

1461 **D.1. Build Architecture**

1462 The PI System was installed in a virtual environment (HyperV) that already existed within  
1463 the collaborative robotic system (CRS). The virtual machine (VM) for the PI System used  
1464 Windows Server 2008 R2 as the operating system, with four virtual central-processing-unit  
1465 cores and 16 gigabytes (GB) of random-access memory. The VM was networked directly  
1466 into the existing network topology of the CRS with a dedicated Internet Protocol (IP) address  
1467 (192.168.0.21).

1468 **D.2. Installation and Configuration**

1469 Compared with the other three installations, the PI System was installed locally on existing  
1470 virtualization hardware. Remote assistance and troubleshooting were provided by OSIsoft for  
1471 the installation and configuration of the system within the CRS.

1472 Six components were installed in the VM:

- 1473 • PI AF
- 1474 • PI Data Archive
- 1475 • PI Process Explorer
- 1476 • PI Vision
- 1477 • PI Modbus Ethernet Interface
- 1478 • Structured Query Language Server 2012

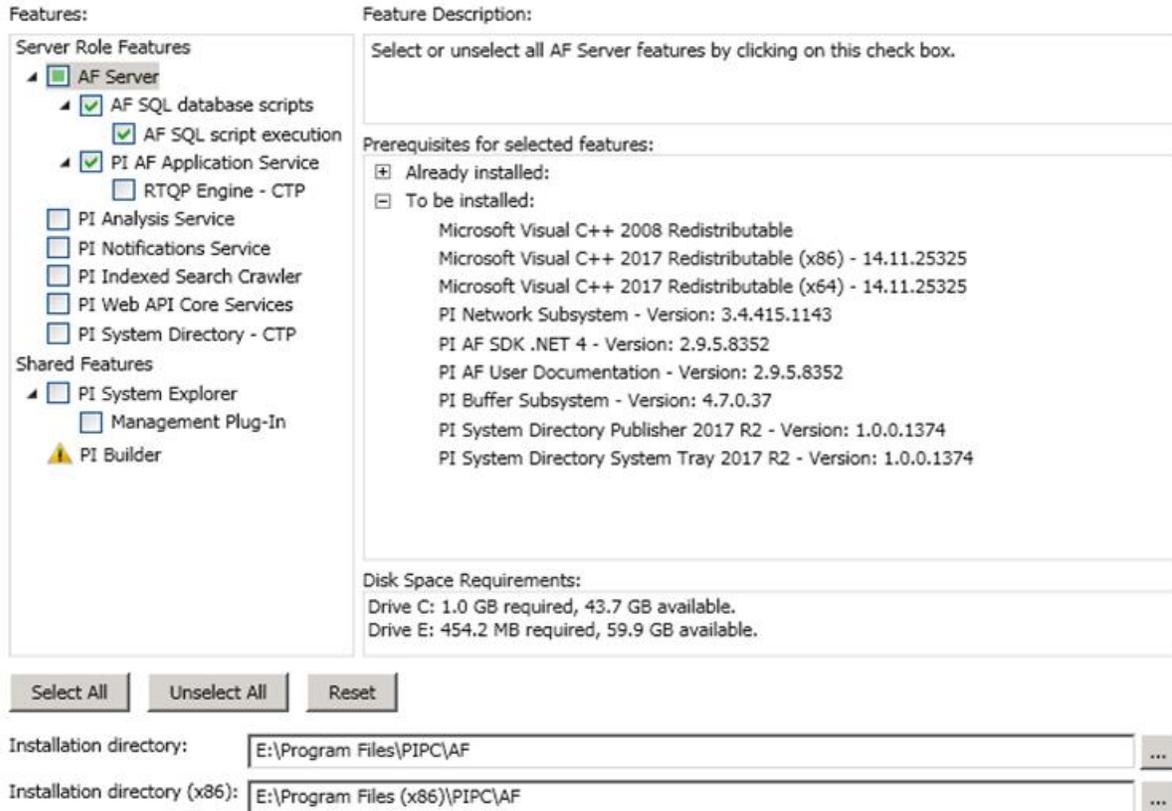
1479 Four additional hard-drive partitions (virtual) were created to support the PI System  
1480 installation:

- 1481 • PI Server (E:): 60 GB
- 1482 • archives (F:): 60 GB
- 1483 • queues (G:): 30 GB
- 1484 • backups (H:): 21 GB

1485 **D.2.1. PI AF Installation**

- 1486 1. Run *PI-AF-Services\_2017-R2-Update-1\_Demo.exe* to launch the installer.
- 1487 2. Select the **Server Role Features** shown in Figure D-1. Ensure that the **Installation**
- 1488 **Directory** is set to the corresponding drive letter labeled as *PI Server*. Click **Next**.

1489 **Figure D-1 Server Role Features to Be Selected During PI AF Installation**



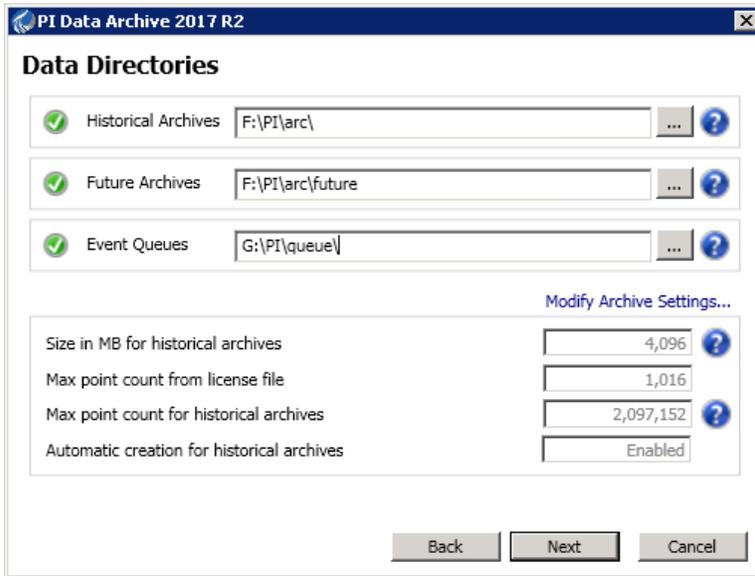
- 1490
- 1491 3. Keep the default settings. Click **Next**.
- 1492 4. Set the **Directory Name** to *<Configure Later>*. Click **Next**.
- 1493 5. Leave the **Service Account** as default. Click **Next**.
- 1494 6. Upon completed installation, reboot the server.

1495 **D.2.2. PI Data Archive Installation**

- 1496 1. Run the *PI-Data-Archive\_2017\_R2A\_Demo\_.exe* file.
- 1497 2. When prompted for the **License File**, browse to the location of the *pilicense.dat* file
- 1498 from OSIsoft. Click **Next**.
- 1499 3. Specify a name for the **Default Asset server**, or leave it as the default host name.
- 1500 Click **Next**.

- 1501 4. Select the **Installation Directory** for the Data Archive. Click **Next**.
- 1502 5. Set the remaining directories as shown in Figure D-2, corresponding to the correct
- 1503 drive letters. Click Next.
- 1504 6. Click **Next**, and verify that the service status shows as **Running**. Click **Next** to finish
- 1505 the installation and to reboot the server.

1506 **Figure D-2 Data Directories to Be Selected During PI Data Archive Installation**



1507

### 1508 **D.2.3. PI System Process Explorer Installation**

- 1509 1. Run the *PIProcessBook\_2015\_R2\_SP1\_06-Jun-2018.exe* file to start the installation.
- 1510 2. A screen titled OSISOFT Setup Progress will begin, installing the different required
- 1511 components.
- 1512 3. A dialog box will appear once the installation is complete.

### 1513 **D.2.4. PI Vision Installation**

- 1514 1. Run the *PI-Vision\_2017-R2-Update-1-90-Day-Trial\_.exe* file to start the installation.
- 1515 2. Select the **Operating Configuration Store**. In this build, the Asset Server was called
- 1516 PI-ROBOTICS. Click **Connect**, and then click **Next**.
- 1517 3. Verify that the **PI Web API port is 443**. Click **Next**.
- 1518 4. On the Submit URL page, do not change the automatically generated **Indexed**
- 1519 **Search Crawler Submit URL**. In this build, the automatically generated Uniform
- 1520 Resource Locator (URL) was *https://pi-robotics.lan.lab/piwebapi/*. Click **Next**.
- 1521 5. Review the changes. Click **Next**.

- 1522 6. When the installation has completed, review the Confirmation page for errors. If no  
1523 errors are found, then click **Finish**.
- 1524 7. The installer will continue installing additional components. Click **Continue** when  
1525 prompted to install Windows features.
- 1526 8. If prompted, leave the default installation directories. Click **Next**.
- 1527 9. Once the installation finishes, click **Finish**.

#### 1528 **D.2.5. PI System Modbus Ethernet Interface Installation**

- 1529 1. Run the *ModbusE\_ReadWrite\_4.2.2.31\_DEMO.exe* file to start the installation.
- 1530 2. Keep all default settings, and complete the installation.
- 1531 3. Open PI Interface Configuration Utility, and select the interface **PIModbusE1**.
- 1532 4. Configure the **Display Name**. In this build, the default name was kept.
- 1533 5. Select the option **Service** in the left navigation panel.
- 1534 6. Select the **Startup Type** option **Auto**, click **Create**, and then click **Apply**.
- 1535 7. Click the Start Service (▶) button on the top navigation bar.
- 1536 8. If the service is running properly, then the label **Running** will appear on the status bar  
1537 at the bottom of the dialog.

#### 1538 **D.2.6. PI System Points and Assets Configuration**

1539 PI System points utilizing the ModbusE interface were manually created using the PI System  
1540 Management Tools (SMT) software. Modbus device addresses, register names, and register  
1541 addresses were known prior to configuring the points.

- 1542 1. Launch the PI SMT by navigating to **Start > All Programs > PI System > PI**  
1543 **System Management Tools**.
- 1544 2. Select **Points > Points Builder** from the left navigation pane.
- 1545 3. Create a new tag, and enter the required attributes (shown in Figure D-3). An example  
1546 of the configuration for the Point PLC-ExperimentMode is shown in Figure D-4.
- 1547 4. Click **Save**.

1548  
1549

**Figure D-3 Configuration Options in the PI Point Builder for Tags Utilizing the ModbusE Interface**

| Point Builder Tab | Field          | Setting  |
|-------------------|----------------|--|
| <b>General</b>    | Name           | ModbusETest  |
|                   | Point source   | MODBUSE  |
|                   | Point type     | Int32  |
| <b>Classic</b>    | Location 1     | 1 (or whatever was used in the Interface ID field in PI ICU)   |
|                   | Location 2     | (Node ID). Example: 1  |
|                   | Location 3     | (Data Type * 100 + Function Code). Example: 103 (which is 1 (for Int16) * 100 + 3 (for holding registry)). Refer the interface manual for a full list of data types and function codes |
|                   | Location 4     | 1 (Scan class Frequency)   |
|                   | Location 5     | (offset from 40000 for holding registry). Example: 52 Represents 40052 register  |
|                   | Instrument tag | IP address or hostname of the Ethernet communications node. Must match with the IP Addr./Hostname entered  |

1550

1551

**Figure D-4 Example Configuration Settings for the Tag PLC-ExperimentMode**

The screenshot shows the 'Classic' configuration tab in the PI Point Builder. It contains the following fields and values:

- Location1: 1
- Location2: 0
- Location3: 103
- Location4: 1
- Location5: 32778
- Conversion Factor: 1
- Filter Code: 0
- Square Root Code: 0
- Total Code: 0
- UserInt1: 0
- UserInt2: 0
- UserReal1: 0
- UserReal2: 0
- Instrument Tag: 192.168.0.30

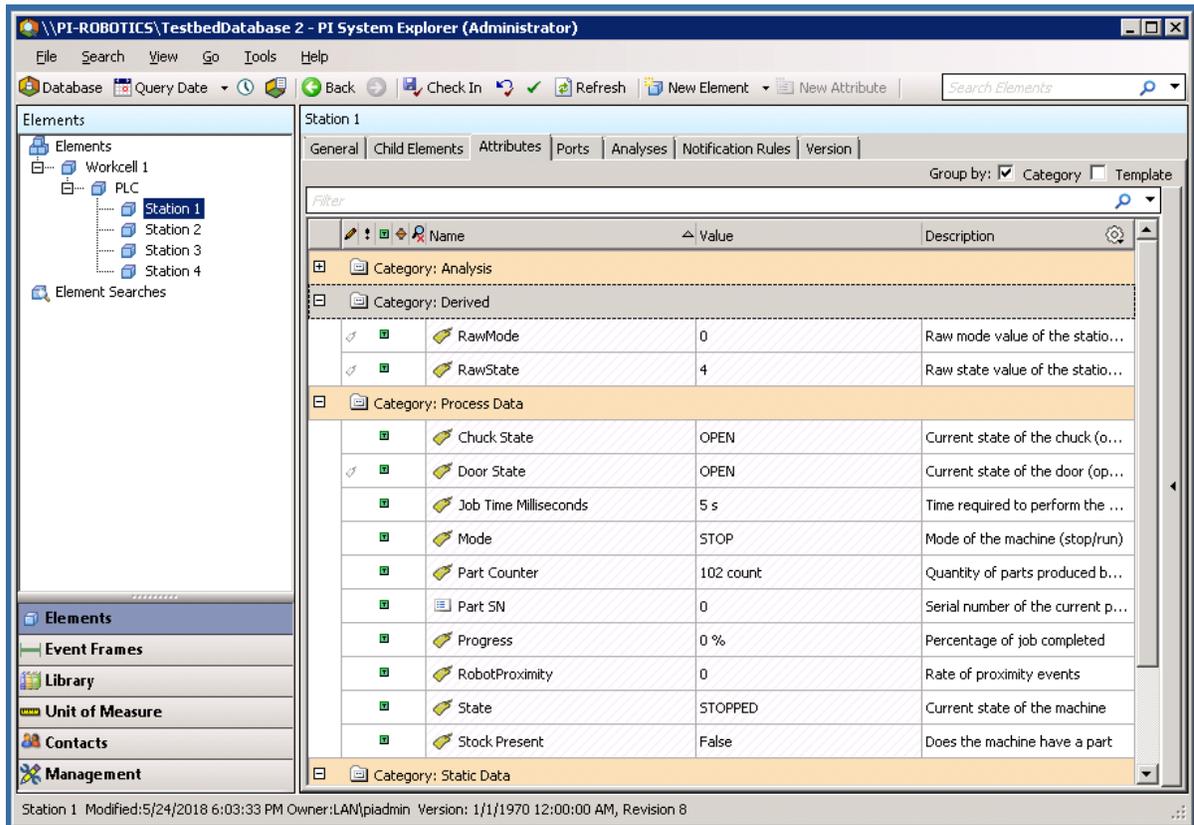
1552

1553 In Figure D-4, the fields **Location1** through **Location5** have different uses, depending on the  
 1554 interface used, and are described in detail in Figure D-3. The **Instrument Tag** field describes  
 1555 the IP address of the Modbus Transmission Control Protocol (TCP) server that the ModbusE  
 1556 interface needs to poll.

1557 The PI System AF and System Explorer were used to define a hierarchical structure for the  
 1558 PI System points, to display tag values for each asset, and to provide an interface for viewing  
 1559 and acknowledging alerts. Because of the relatively simple interactions among elements of  
 1560 the CRS, the structure created in the AF contained the supervisory programmable logic  
 1561 controller (PLC) as the top-level element, and Station 1 through Station 4 as child elements.

1562 Asset templates were created for the PLC and four machining stations to automatically link  
 1563 to the proper PI System points based on the asset. The final configuration of assets is shown  
 1564 in Figure D-5, showing the hierarchical structure of **Workcell 1 > PLC > Station 1**. Also  
 1565 shown in this figure are the **Attributes** for Station 1, as received from the PI System points.

1566 **Figure D-5 PI System Explorer View Showing the Configured Assets (Elements), the Resulting**  
 1567 **Hierarchical Structure of Assets, and Live Attributes Received from Station 1**



1568  
 1569 For both the PLC and machining-station asset templates, analysis functions were created to  
 1570 generate alerts for the operator when identified anomalous events are detected. The  
 1571 anomalous events to be detected are the anomalies described in Section D.3. The analysis  
 1572 functions are described in Sections D.2.7 and D.2.8. Respective event-frame generators for  
 1573 each analysis function were created to generate the actual alerts.

1574 **D.2.7. PLC Asset Template Analysis Functions**

1575 The analysis functions provided in the following subsections were created to generate alerts  
 1576 in the PLC asset template when their respective anomalous events are detected. For the sake  
 1577 of brevity, the event-frame generation code is not shown. In general, the typical event-frame  
 1578 generator contains logic to activate the event frame when the analysis function result is `TRUE`,  
 1579 and to stop the event frame after the analysis function result is `FALSE` or after a related  
 1580 element variable changes to a value indicating that the failure or fault has been resolved.

1581 **D.2.7.1. High Workcell Temperature**

1582 If the simulated workcell temperature increases above the value of 29.0 degrees Celsius, then  
1583 generate an alert by using the following command:

```
1584 R261 := if ('WorkcellTemperature'>= 29.0) then 1 else 0;
```

1585 **D.2.7.2. Inspection Failure**

1586 If the inspection station reports a failed inspection count greater than or equal to three, then  
1587 generate an alert by using the following command:

```
1588 Alarm := If('FailedInspectionCounter' >= 3) Then 1 Else 0;
```

1589 **D.2.7.3. Station Out-of-Sync**

1590 If any of the machining stations is not in the RUN mode while the workcell is in the RUN  
1591 state, then generate an alert by using the following commands:

```
1592 S1State := '.\Elements[@Name=Station 1]|State';  
1593 S2State := '.\Elements[@Name=Station 2]|State';  
1594 S3State := '.\Elements[@Name=Station 3]|State';  
1595 S4State := '.\Elements[@Name=Station 4]|State';  
1596  
1597 WCState := If(TimeEq('WorkcellState', '*-5s', '*', "RUN")>=5)  
1598 Then "RUN" Else "Starting";  
1599 StationModes := if (S1State = "STOPPED" Or S2State = "STOPPED"  
1600 OR  
1601 S3State = "STOPPED" Or S4State = "STOPPED")  
1602 Then 1 Else 0;  
1603 Alarm := if (StationModes = 1 And WCState = "RUN") Then 1 Else  
1604 0;
```

1605 **D.2.8. Machining Station Asset Template Analysis Functions**

1606 The analysis functions provided in the following subsections were created to generate alerts  
1607 in the machining station asset template when their respective anomalous events are detected.  
1608 For the sake of brevity, the event-frame generation code is not shown. As previously  
1609 mentioned, in general, the typical event-frame generator contains logic to activate the event  
1610 frame when the analysis function result is TRUE, and to stop the event frame after the analysis  
1611 function result is FALSE or after a related element variable changes to a value indicating that  
1612 the failure or fault has been resolved.

1613 **D.2.8.1. High Trouble Call Count**

1614 Two analysis functions were created for this alert. First, determine if the machining station is  
1615 in the TROUBLE state by using the following command:

```
1616 Trouble := if ('State' = "TROUBLE" AND ((PrevVal('State','*-  
1617 1s') = "TROUBLE") = False)) THEN "TROUBLE" ELSE NoOutput();
```

1618 If the machining station has entered the TROUBLE state, then count this event. If the number  
1619 of times that the machining station has entered the TROUBLE state in the previous  
1620 10 minutes is greater than or equal to five, then generate an alert by using the following  
1621 command:

```
1622 TroubleCount := If (EventCount('Alarm-TroubleCounterEvent','*-  
1623 10m','*') >= 5) Then 1 Else 0;  
1624 Variable1 := 'State';
```

1625 **D.2.8.2. Robot Proximity Fault**

1626 If the machining station is in the RUN mode and a robot proximity message has not been  
1627 received within the previous two minutes, then generate an alert by using the following  
1628 command:

```
1629 Alarm := If (('Mode' = "RUN") And (PrevVal('Mode','*-2m') =  
1630 "RUN") And (TagMax(';RobotProximity','*-2m','*') = 0)) then 1  
1631 else 0;
```

1632 **D.2.8.3. Station Door Fault**

1633 If the machining station is in the ACTIVE state and the door is not closed, then generate an  
1634 alert by using the following command:

```
1635 Door_Open_Alarm := if (TimeEq('State','*-2s','*', "ACTIVE")>=2  
1636 And TimeEq('Door State','*-2s','*', "CLOSED")<1) Then 1 ELSE 0;  
1637 Variable1 := TimeEq('Door State','*-2s','*', "CLOSED");
```

1638 **D.2.8.4. Station Mode Error**

1639 If the register value for the machining station mode (as written by the PLC) is not within the  
1640 valid range of values (0 to 1), then generate an alert by using the following command:

```
1641 Alarm := If('RawMode' < 0 OR 'RawMode' > 1) Then 1 Else 0;
```

1642 **D.2.8.5. Station State Error**

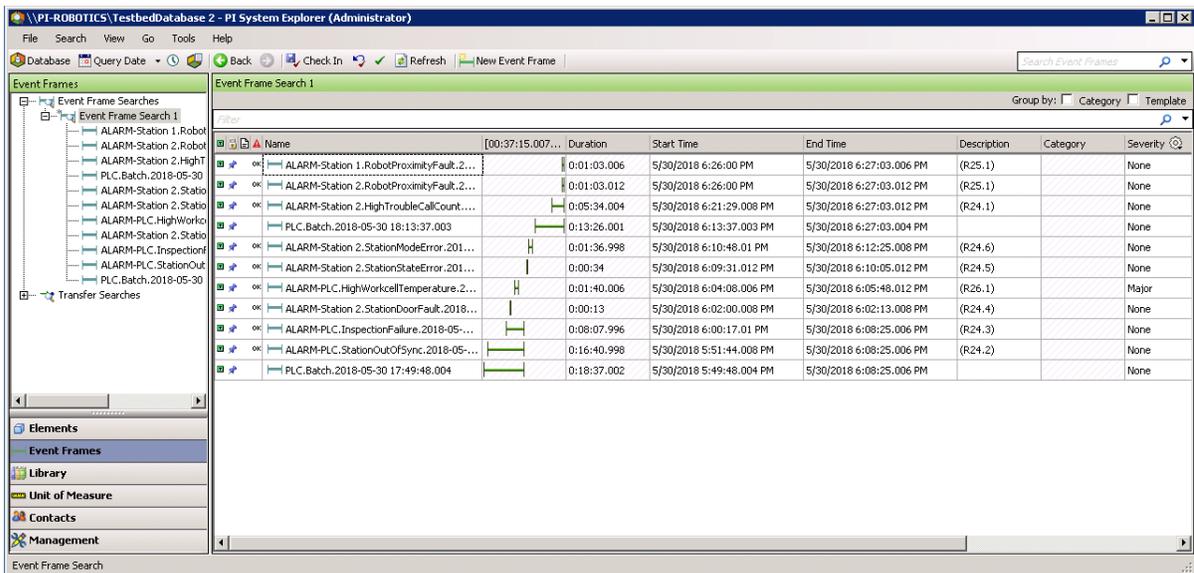
1643 If the register value for the machining station state (as reported by the machining station) is  
1644 not within the valid range of values (0 to 5), then generate an alert by using the following  
1645 command:

```
1646 Alarm := If('RawState' < 0 OR 'RawState' > 5) Then 1 Else 0;
```

1647 **D.2.9. Viewing and Acknowledging Alerts**

1648 The PI System Explorer was used to view and acknowledge alerts (event frames) generated  
1649 by the analyses templates. An example of the alerts is shown in Figure D-6, showing all of  
1650 the alerts generated by the anomalies during the execution of the anomaly scenarios.

1651 **Figure D-6 PI System Explorer Interface Showing an Example of Alerts Displayed to the**  
1652 **Operator for Acknowledgment, as Used During Anomaly Scenario Execution**



1653

1654 **D.3. Anomaly Scenarios**

1655 The historian/sensor-based anomaly detection method was demonstrated for the scenarios  
1656 detailed in the following subsections. Each scenario includes a description of the anomaly, a  
1657 detailed description of how each demonstration event was conducted in the Cybersecurity for  
1658 Smart Manufacturing Systems environment, and the observed results.

1659 The anomalies listed below demonstrate the fusion of cybersecurity and manufacturing  
1660 activities into a cohesive operation for detecting operational/maintenance issues and for  
1661 potentially identifying issues caused by cybersecurity incidents. In-depth knowledge of the  
1662 manufacturing system enables engineers to design PI System analysis functions to monitor  
1663 and alert when anomalous events occur, and to track trends of anomalies over extended  
1664 periods of time. With proper communication between operators and cybersecurity personnel,  
1665 anomalous manufacturing process events can be analyzed to determine if they could have  
1666 been caused by a cybersecurity incident and could have been mitigated.

1667 **D.3.1. Frequency Increase of Trouble Calls from a Machining Station**

1668 Trouble calls are automatically generated by a machining station when it detects an anomaly  
 1669 during manufacturing operations (e.g., broken tooling, coolant failure).

1670 This anomaly was executed on the CRS. The machining station logic for Station 2 contained  
 1671 a register that enabled trouble calls to be initiated on demand, generating the anomaly. This  
 1672 register was set using a menu option on the human-machine interface (HMI). When enabled,  
 1673 the machining station would enter the TROUBLE state after each part was placed in the  
 1674 machine, and would be automatically cleared after eight seconds had elapsed.

1675

| Name                                    | Duration    | Start Time               |
|---|-------------|--------------------------|
| ALARM-Station 2.HighTroubleCallCount... | 0:02:21.415 | 5/30/2018 6:21:29.008 PM |
| PLC.Batch.2018-05-30 18:13:37.003       | 0:10:13.423 | 5/30/2018 6:13:37.003 PM |

1676 **D.3.2. Machining Station Shuts Down During Normal Workcell Operations**

1677 The workcell requires that all four machining stations are operational and in the RUN mode  
 1678 while the workcell is in the RUN state.

1679 This anomaly was executed on the CRS. The machining station logic for Station 2 contained  
 1680 a register that enabled a “forced shutdown” to be initiated, generating the anomaly. This  
 1681 register was set using a menu option on the HMI. When enabled, the machining station  
 1682 would enter the STOP mode while the rest of the workcell machines were operational.

1683

| Name                                   | Duration    | Start Time               |
|--|-------------|--------------------------|
| ALARM-PLC.StationOutOfSync.2018-05-... | 0:00:45.531 | 5/30/2018 5:51:44.008 PM |
| PLC.Batch.2018-05-30 17:49:48.004      | 0:02:41.536 | 5/30/2018 5:49:48.004 PM |

1684 **D.3.3. Inspection Station Rejects All Parts Leaving the Workcell**

1685 The quantity of good and bad parts exiting the inspection station is counted by the  
 1686 supervisory PLC. An increase in the number of rejected parts indicates that the workcell  
 1687 should be inspected by an operator to determine the cause.

1688 This anomaly was executed on the CRS. The station logic for Station 4 contained a register  
 1689 that enabled the “inspection failure of all parts” anomaly. This register was set using a menu  
 1690 option on the HMI. When enabled, the inspection station would report a failed result for  
 1691 every inspection performed until the anomaly was disabled.

1692

| Name                                    | Duration    | Start Time              |
|---|-------------|-------------------------|
| ALARM-PLC.InspectionFailure.2018-05-... | 0:00:43.048 | 5/30/2018 6:00:17.01 PM |

1693 **D.3.4. Machining Station Door Sensor Fails**

1694 The unsafe condition that this sensor failure can cause warrants investigation by an operator.  
1695 Substantial damage can occur to both the machining station and robots if this sensor failure is  
1696 not detected. This anomaly could be a goal for an attacker who has the intent to cause  
1697 production disruption or financial loss through equipment damage.

1698 This anomaly was executed on the CRS. The machining station has a simulated door that  
1699 must open and close to allow the robot to have access into the machine for placing raw  
1700 material and removing finished parts. The machining station logic for Station 2 contained a  
1701 register that enabled the door-sensor failure anomaly. This register was set using a menu  
1702 option on the HMI. When enabled, the failure of this sensor caused the machining station to  
1703 report that the door was always “OPEN.”

1704

| Name                                     | Duration    | Start Time               |
|--|-------------|--------------------------|
| ALARM-Station 2.StationDoorFault.2018... | 0:00:10.492 | 5/30/2018 6:02:00.008 PM |

1705 **D.3.5. Abnormal Process Variable Data Is Transmitted to the PLC**

1706 Two-way communication occurs between the supervisory PLC and the machining station  
1707 during normal operations. If a process variable trends outside the known operational range,  
1708 then this anomaly should be reported.

1709 This anomaly was executed on the CRS. Each machining station contains a Modbus TCP  
1710 server for communicating operational information to, and receiving commands from, the  
1711 supervisory PLC. The machining station logic for Station 2 contained a register that enabled  
1712 specific operational information to be corrupted before it was transmitted to the PLC. This  
1713 register was set using a menu option on the HMI.

1714

| Name                                     | Duration    | Start Time               |
|--|-------------|--------------------------|
| ALARM-Station 2.StationStateError.201... | 0:00:36.826 | 5/30/2018 6:09:31.012 PM |

1715 **D.3.6. Abnormal Process Variable Data Is Transmitted to a Machining Station**

1716 As previously mentioned, two-way communication occurs between the supervisory PLC and  
1717 the machining station during normal operations. If a process variable trends outside the  
1718 known operational range, then this anomaly should be reported.

1719 This anomaly was executed on the CRS. The supervisory PLC contains a Modbus TCP client  
1720 for communicating commands to, and receiving operational information from, the machining  
1721 stations. The supervisory PLC contained a register that enabled specific commands to be  
1722 corrupted before they were transmitted to the machining stations. This register was set using  
1723 a menu option on the HMI.

1724

| Name                                    | Duration    | Start Time              |
|---|-------------|-------------------------|
| ALARM-Station 2.StationModeError.201... | 0:00:42.732 | 5/30/2018 6:10:48.01 PM |

1725 **D.3.7. Robots Fail to Send Required Sensor Data to a Machining Station**

1726 As previously mentioned, the unsafe condition that this sensor failure can cause warrants  
1727 investigation by an operator. Substantial damage can occur to both the machining station and  
1728 robots if this sensor failure is not detected. This anomaly could be a goal for an attacker who  
1729 intends to cause production disruption or financial loss through equipment damage.

1730 This anomaly was executed on the CRS. The machining station has a simulated door that  
1731 must open and close to allow the robot access into the machine for placing raw material and  
1732 removing finished parts. The two robots report their locations (via Modbus TCP) to the  
1733 machining stations so that they do not attempt to close the door while the robot is still  
1734 operating within the machine. Robot Controller 1 contains a configuration option to disable  
1735 this reporting, resulting in Stations 1 and 2 not receiving robot location information. This  
1736 configuration option was used to generate the anomaly.

| Name                                     | [00:36:12.995... | Duration    | Start Time           |
|--|------------------|-------------|----------------------|
| ALARM-Station 1.RobotProximityFault.2... |                  | 0:00:31.083 | 5/30/2018 6:26:00 PM |
| ALARM-Station 2.RobotProximityFault.2... |                  | 0:00:31.086 | 5/30/2018 6:26:00 PM |

1737

1738 **D.3.8. Workcell Temperature Increases Above a Specified Threshold**

1739 Process variables that impact the output quality of the workcell must be monitored for  
1740 deviation from expected values. The temperature of the workcell increases during normal  
1741 operations and must be properly cooled to maintain quality; therefore, the workcell  
1742 temperature is monitored.

1743 This anomaly was executed on the CRS. The workcell contained a simulated temperature  
1744 sensor, which was used to “monitor” the temperature within the workcell. The temperature  
1745 was then displayed to the operator, on the HMI. The workcell temperature would increase to  
1746 an expected value while the workcell was operational and would decrease to room  
1747 temperature when the system was shut down. During anomalous conditions, the temperature  
1748 would increase beyond a threshold, causing all parts produced during that period to be  
1749 scrapped.

1750 The temperature sensor was simulated by the PLC. The anomalous temperature increase was  
1751 enabled by a register within the PLC and was set using a menu option on the HMI.

| Name                                   | [00:14:21.001... | Duration    | Start Time               |
|--|------------------|-------------|--------------------------|
| ALARM-PLC.HighWorkcellTemperature.2... |                  | 0:00:33.602 | 5/30/2018 6:04:08.006 PM |

1752

1753 **Appendix E. Acronyms and Abbreviations**

|                   |  |
|-------------------|--|
| <b>24/7</b>       | 24 Hours a Day, Seven Days a Week                  |
| <b>AF</b>         | Asset Framework                                    |
| <b>BAD</b>        | Behavioral Anomaly Detection                       |
| <b>CPU</b>        | Central Processing Unit                            |
| <b>CRS</b>        | Collaborative Robotic System                       |
| <b>CSMS</b>       | Cybersecurity for Smart Manufacturing Systems      |
| <b>CSV</b>        | Comma-Separated Values                             |
| <b>CybersecVM</b> | Cybersecurity Virtual Machine                      |
| <b>DA</b>         | Data Access  |
| <b>DCOM</b>       | Distributed Component Object Model                 |
| <b>DMZ</b>        | Demilitarized Zone                                 |
| <b>DNS</b>        | Domain Name System                                 |
| <b>DoS</b>        | Denial of Service                                  |
| <b>EICAR</b>      | European Institute for Computer Antivirus Research |
| <b>EL</b>         | Engineering Laboratory                             |
| <b>FTP</b>        | File Transfer Protocol                             |
| <b>GB</b>         | Gigabyte(s)  |
| <b>GUI</b>        | Graphical User Interface                           |
| <b>HMI</b>        | Human-Machine Interface                            |
| <b>HTTP</b>       | Hypertext Transfer Protocol                        |
| <b>ICMP</b>       | Internet Control Message Protocol                  |
| <b>ICS</b>        | Industrial Control System                          |
| <b>ID</b>         | Identifier   |
| <b>IDS</b>        | Intrusion Detection System                         |
| <b>IP</b>         | Internet Protocol                                  |
| <b>IPC</b>        | Industrial Personal Computer                       |
| <b>IT</b>         | Information Technology                             |
| <b>LAN</b>        | Local Area Network                                 |

|               |   |
|---------------|---|
| <b>LTS</b>    | Long-Term Support   |
| <b>M</b>      | Megabyte(s)   |
| <b>MAC</b>    | Media Access Control  |
| <b>NCCoE</b>  | National Cybersecurity Center of Excellence                       |
| <b>NIC</b>    | Network Interface Card  |
| <b>NIST</b>   | National Institute of Standards and Technology                    |
| <b>NISTIR</b> | National Institute of Standards and Technology Interagency Report |
| <b>NTP</b>    | Network Time Protocol   |
| <b>OPC</b>    | Object Linking and Embedding for Process Control                  |
| <b>OS</b>     | Operating System  |
| <b>OT</b>     | Operational Technology  |
| <b>PCS</b>    | Process Control System  |
| <b>PDF</b>    | Portable Document File  |
| <b>PHP</b>    | Hypertext Preprocessor  |
| <b>PI</b>     | Process Information   |
| <b>PLC</b>    | Programmable Logic Controller                                     |
| <b>ROS</b>    | Robot Operating System  |
| <b>SCADA</b>  | Supervisory Control and Data Acquisition                          |
| <b>SIEM</b>   | Security Information and Event Management                         |
| <b>SMT</b>    | System Management Tools   |
| <b>SNTP</b>   | Simple Network Time Protocol                                      |
| <b>SP</b>     | Special Publication   |
| <b>SPAN</b>   | Switch Port Analyzer  |
| <b>SSH</b>    | Secure Shell  |
| <b>TCP</b>    | Transmission Control Protocol                                     |
| <b>TE</b>     | Tennessee Eastman   |
| <b>UDP</b>    | User Datagram Protocol  |
| <b>URI</b>    | Uniform Resource Identifier                                       |
| <b>URL</b>    | Uniform Resource Locator  |

|             |                                 |
|-------------|---------------------------------|
| <b>USB</b>  | Universal Serial Bus            |
| <b>VLAN</b> | Virtual Local Area Network      |
| <b>VM</b>   | Virtual Machine                 |
| <b>XAE</b>  | eXtended Automation Engineering |
| <b>XLSX</b> | Microsoft Excel Workbook File   |

1754 **Appendix F. References**

- 1755 [1] “Framework for improving critical infrastructure cybersecurity,” NIST, Gaithersburg,  
1756 MD, Apr. 16, 2018 [Online]. Available:  
1757 [https://www.nist.gov/publications/framework-improving-critical-infrastructure-](https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11)  
1758 [cybersecurity-version-11](https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11).
- 1759 [2] K. Stouffer et al., “Cybersecurity framework manufacturing profile,” NIST,  
1760 Gaithersburg, MD, NISTIR 8183, 2017 [Online]. Available:  
1761 <https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile>.
- 1762 [3] K. Stouffer et al., “Guide to industrial control systems (ICS) security,” NIST,  
1763 Gaithersburg, MD, SP 800-82 Revision 2, May 2015 [Online]. Available:  
1764 <https://www.nist.gov/publications/guide-industrial-control-systems-ics-security>.
- 1765 [4] *Security for Industrial Automation and Control Systems: Establishing an Industrial*  
1766 *Automation and Control Systems Security Program*, ANSI/ISA Standard 62443-2-1,  
1767 2009.
- 1768 [5] *Security for Industrial Automation and Control Systems – Part 2-3: Patch*  
1769 *Management in the IACS Environment*, ANSI/ISA Standard 62443-2-3, 2015.
- 1770 [6] Joint Task Force Transformation Initiative, “Security and privacy controls for federal  
1771 information systems and organizations,” NIST, Gaithersburg, MD, SP 800-53  
1772 Revision 4, Apr. 2013.
- 1773 [7] R. Candell, T. Zimmerman, and K. Stouffer, “An industrial control system  
1774 cybersecurity performance testbed,” NIST, Gaithersburg, MD, NISTIR 8089, Nov.  
1775 2015 [Online]. Available: [https://www.nist.gov/publications/industrial-control-](https://www.nist.gov/publications/industrial-control-system-cybersecurity-performance-testbed)  
1776 [system-cybersecurity-performance-testbed](https://www.nist.gov/publications/industrial-control-system-cybersecurity-performance-testbed).
- 1777 [8] T. Zimmerman, “Metrics and key performance indicators for robotic cybersecurity  
1778 performance analysis,” NIST, Gaithersburg, MD, NISTIR 8177, Apr. 2017 [Online].  
1779 Available: [https://www.nist.gov/publications/metrics-and-key-performance-](https://www.nist.gov/publications/metrics-and-key-performance-indicators-robotic-cybersecurity-performance-analysis)  
1780 [indicators-robotic-cybersecurity-performance-analysis](https://www.nist.gov/publications/metrics-and-key-performance-indicators-robotic-cybersecurity-performance-analysis).
- 1781 [9] C. Tang, “Key performance indicators for process control system cybersecurity  
1782 performance analysis,” NIST, Gaithersburg, MD, NISTIR 8188, Aug. 2017 [Online].  
1783 Available: [https://www.nist.gov/publications/key-performance-indicators-process-](https://www.nist.gov/publications/key-performance-indicators-process-control-system-cybersecurity-performance-analysis)  
1784 [control-system-cybersecurity-performance-analysis](https://www.nist.gov/publications/key-performance-indicators-process-control-system-cybersecurity-performance-analysis).
- 1785 [10] J. J. Downs and E. F. Vogel, “A plant-wide industrial process control problem,”  
1786 *Comput. Chem. Eng.*, vol. 17, no. 3, pp. 245-255, 1993.
- 1787 [11] N. L. Ricker. (2015, Jan. 23). *Tennessee Eastman challenge archive* [Online].  
1788 Available: <https://depts.washington.edu/control/LARRY/TE/download.html>.
- 1789 [12] S. Tatham. (1999). *Download PuTTY* [Online]. Available: <https://www.putty.org/>.
- 1790 [13] P. Biondi. (2008). *Scapy* [Online]. Available: <https://scapy.net/>.

- 1791 [14] G. van Rossum. (1990). *Python* [Online]. Available: <https://www.python.org/>.
- 1792 [15] T. Kosse. (2001). *FileZilla* [Online]. Available: <https://filezilla-project.org/>.
- 1793 [16] G. Lyon. (1997). *Nmap.org* [Online]. Available: <https://nmap.org/>.
- 1794 [17] R. McCool. (1995). *Apache HTTP server project* [Online]. Available:  
1795 <https://httpd.apache.org/>.
- 1796 [18] A. Rudakov. (n.d.). *File modbus-discover* [Online]. Available:  
1797 <https://nmap.org/nsedoc/scripts/modbus-discover.html>.
- 1798 [19] PHP Group. (2001). *PHP: Hypertext preprocessor* [Online]. Available:  
1799 <http://www.php.net/>.
- 1800 [20] G. Woltman. (1996). *Free Mersenne prime search software: Prime95 version 29.4*  
1801 *build 7* [Online]. Available: <https://www.mersenne.org/download/>.
- 1802 [21] Wikimedia Foundation, Inc. (1999). *OpenSSH* [Online]. Available:  
1803 <https://en.wikipedia.org/wiki/OpenSSH>.