

# NIST SPECIAL PUBLICATION 1800-41

---

## Responding to and Recovering from a Cyber Attack: Cybersecurity for the Manufacturing Sector

---

**Michael Powell**

**Michael Pease**

**Keith Stouffer**

Information Technology  
Laboratory  
National Institute of  
Standards and Technology

**Toby Maysey**

**Chris Peloquin**

**Bob Stea**

**Kangmin Zheng**

The MITRE Corporation

**Geoff Sweet**

AWS (Amazon Web Services)

**Brian Butler**

Cisco

**Josh Carlson**

**Chris Manrique**

Dragos

**Chris Bihary**

**Jason Drewniak**

Garland Technology

**Nathan Boeger**

**Brad Fischer**

Inductive Automation

**Kim Gajewski**

**Sri Goutisetti**

**Chris Sistrunk**

Google Cloud (including Mandiant)

**Stephen Petruzzo**

**Billy John Stewart**

GreenTec-USA, LLC

**Ahmik Hindman**

Rockwell Automation

**John Crawford**

**Allen Cantrell**

**Dallas Levine**

Siemens

**Ray Erlinger**

**Bill Johnson**

**Pam Johnson**

**Clyde Poole**

TDI Technologies

**Chris Jensen**

**Joshua Moll**

Tenable

May 2026

INITIAL PUBLIC DRAFT

This publication is available free of charge from <https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack>

1 **DISCLAIMER**

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

8 **NOTE TO REVIEWERS**

9 This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions,  
10 and success stories will improve subsequent versions of this guide.

11 You can view the project description, the web version, or the feedback portal from the [Manufacturing  
12 Response and Recovery project page](#).

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

14 Public comment period: May 21, 2026 – July 8, 2026

15 All comments are subject to release under the Freedom of Information Act.

16 NIST is particularly interested in your feedback on the following questions:

- 17 1. How well do the practices in this guide relate to existing practices leveraged by your  
18 organization? Are there significant gaps between the sets of practices that this guide should  
19 address?
- 20 2. How do you expect this guide to influence your future practices and processes?
- 21 3. How do you envision using this guide? What changes would you like to see to increase/improve  
22 that use?
- 23 4. What suggestions do you have on changing the format of the provided information?

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

## 30 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 46 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 56 **ABSTRACT**

57 Industrial Control Systems (ICS) that operate manufacturing environments play a critical role in the  
58 supply chain. Manufacturing organizations rely on control systems to monitor and control physical  
59 processes that produce goods for public consumption. These same systems are facing an increasing  
60 number of cyber incidents, posing a real threat to safety and production, and impacting the economic  
61 performance of manufacturing organizations. Though defense-in-depth security architecture helps  
62 mitigate cyber risks, it cannot eliminate all cyber risks; therefore, manufacturing organizations should  
63 also have a plan to recover and restore operations should a cyber incident impact operations. This  
64 practice guide showcases various cyber attack scenarios developed with industry collaborators to

65 produce a methodology that enables the adoption and implementation of response and recovery  
 66 measures in manufacturing environments to strengthen operational resilience.

67 **KEYWORDS**

68 *cybersecurity; incident investigation; incident response; industrial control systems; manufacturing;*  
 69 *operational technology; recovery; response; restoration.*

70 **ACKNOWLEDGMENTS**

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

Name	Organization
Cherilyn Pascoe	NIST
Timothy Zimmerman*	NIST
Theresa Suloway	MITRE
John Hoyt*	MITRE
Lynette Wilcox*	MITRE
Stephanie Saravia*	MITRE
Aslam Sherule*	MITRE
Philip Fenimore*	MITRE
Ethan Cheung	MITRE
Kyle Hussey*	TDi Technologies
Kyle McMillan	Siemens
Peter Romness*	Cisco

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

73 **DOCUMENT CONVENTIONS**

74 The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publica-  
 75 tion and from which no deviation is permitted. The terms “should” and “should not” indicate that

76 among several possibilities, one is recommended as particularly suitable without mentioning or exclud-  
77 ing others, or that a certain course of action is preferred but not necessarily required, or that (in the  
78 negative form) a certain possibility or course of action is discouraged but not prohibited. The terms  
79 “may” and “need not” indicate a course of action permissible within the limits of the publication. The  
80 terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

## 81 **CALL FOR PATENT CLAIMS**

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

88 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in  
89 written or electronic form, either:

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

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

- 95 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;  
96 or
- 97 2. without compensation and under reasonable terms and conditions that are demonstrably free  
98 of any unfair discrimination.

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

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

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

107 **Contents**

108 **Executive Summary ..... 1**

109 **1 Introduction..... 1**

110 1.1 Scope .....1

111 1.2 Audience .....2

112 1.3 How to Use This Guide.....2

113 **2 Project Overview ..... 3**

114 2.1 Project Approach & Assumptions .....3

115 2.2 Response and Recovery Challenges .....4

116 2.3 Project Collaborators .....5

117 2.4 Build Architecture & Collaborator.....6

118 2.4.1 Product Control Mappings.....7

119 2.4.2 Build Components.....9

120 2.4.3 Build Details .....12

121 2.5 Assumptions .....15

122 2.5.1 Attack Assumptions .....16

123 2.5.2 Preparation Assumptions .....16

124 2.5.3 General Project Assumptions .....16

125 **3 Functional Demonstrations ..... 17**

126 3.1 Demonstration Methodology .....17

127 3.2 Demonstration Use Cases .....17

128 3.2.1 Scenario A: Compromise Human Machine Interface (HMI) or Operator Console .....17

129 3.2.2 Scenario A: Response Execution .....19

130 3.2.3 Scenario A: Recovery Execution.....24

131 3.2.4 Scenario B: Data Exfiltration .....25

132 3.2.5 Scenario B: Response Execution .....27

133 3.2.6 Scenario B: Recovery Execution.....32

134 3.2.7 Scenario C: Unauthorized Command Message.....33

135 3.2.8 Scenario C: Response Execution .....35

136 3.2.9 Scenario C: Recovery Execution .....40

137 **4 General Findings ..... 41**

138 **Appendix A List of Acronyms..... 43**

139	<b>Appendix B</b>	<b>References</b>	<b>45</b>
140	<b>Appendix C</b>	<b>Build Implementation Instructions</b>	<b>46</b>
141	C.1	Scenario A: Technical Details - Preparation	46
142	C.1.1	Creating a Splunk Dashboard to detect USB Activity	46
143	C.1.2	Backup the Rockwell PanelView™ HMI	58
144	C.1.3	ForceField Zero Trust Storage	62
145	C.1.4	FactoryTalk® Logs in Windows Event Viewer	66
146	C.2	Scenario A: Technical Details – Response	71
147	C.2.1	Dragos Case Creation	71
148	C.2.2	Disconnect WAN from Cisco ISA Firewall	72
149	C.2.3	Isolation of HMI	73
150	C.2.4	Inductive Automation, Data Historian	74
151	C.2.5	Rockwell FactoryTalk® Transfer Utility	75
152	C.2.6	Rockwell Automation FactoryTalk® AssetCentre, Log Review	76
153	C.2.7	Update Dragos Case	76
154	C.2.8	Remove Virtual Machine from Network	77
155	C.2.9	Taking Snapshots of VMs	79
156	C.2.10	Remove Physical Device from the Network	82
157	C.2.11	Antivirus Scan	84
158	C.2.12	Search for Malicious File	84
159	C.2.13	Script for Finding Malicious File	85
160	C.3	Scenario A: Technical Details – Recovery	88
161	C.3.1	Downloading Backups from Authoritative Source	88
162	C.3.2	Restore the HMI	89
163	C.3.3	Close Dragos Ticket	89
164	C.4	Scenario B: Technical Details – Preparation	91
165	C.4.1	Configuring Garland to Enable Multiple Detections	91
166	C.4.2	Creating Graphic Interface in ConsoleWorks	92
167	C.4.3	Creating a Redundant Ignition Instance in AWS	93
168	C.4.4	Creating a Baseline in Dragos	97
169	C.4.5	Creating a Baseline Policy in Tenable	98
170	C.4.6	Creating a Splunk Dashboard for SQL protocol Activity	101
171	C.5	Scenario B: Technical Details – Response	111
172	C.5.1	Detection using Splunk Dashboard	111

173 C.5.2 Analyzing Tenable Alert ..... 113

174 C.5.3 Analyzing Dragos Deviation Alert ..... 113

175 C.5.4 Dragos Case Management ..... 114

176 C.5.5 Isolate ICS DMZ using ISA3000..... 115

177 C.5.6 Disconnect JumpHost VM from Network ..... 118

178 C.5.7 Take Snapshot of JumpHost VM ..... 118

179 C.5.8 Isolate Local Database and Historian Gateway..... 119

180 C.5.9 Validate Redundant AWS Cloud Historian ..... 124

181 C.5.10 Detecting Large Data Transfer in Dragos ..... 125

182 C.5.11 Detecting Policy Deviation in Tenable ..... 132

183 C.5.12 Browsing Packet Captures from Tenable..... 134

184 C.5.13 Reviewing ConsoleWorks User Session ..... 145

185 C.5.14 Disable Compromised Accounts ..... 148

186 C.6 Scenario B: Technical Details – Recovery ..... 150

187 C.7 Scenario C: Technical Details – Preparation ..... 151

188 C.7.1 Creating Siemens Traffic Detection Policy in Tenable ..... 151

189 C.7.2 Creating Splunk dashboard for unauthorized Siemens traffic..... 152

190 C.8 Scenario C: Technical Details – Response ..... 154

191 C.8.1 View Tags in Data Historian ..... 154

192 C.8.2 Managing Dragos Tickets..... 154

193 C.8.3 Isolate ICS Network using SIBERprotect ..... 159

194 C.8.4 Viewing policy violations in Tenable..... 160

195 C.8.5 TIA Portal Diagnostics ..... 161

196 C.8.6 Windows Task Manager..... 162

197 C.8.7 Review ConsoleWorks Sessions for User Activity ..... 162

198 C.9 Scenario C: Technical Details – Recovery ..... 165

199 C.9.1 TIA Portal Reinstall ..... 165

200 C.9.2 Download PLC Backup Program File from ForceField..... 166

201 C.9.3 Add Password and Restore from Backup with TIA Portal..... 167

202 **List of Figures**

203 **Figure 2-1: Discrete manufacturing without security tools ..... 7**

204 **Figure 2-2: Build architecture with security tools ..... 9**

205 **Figure 2-3: Zoomed in top right portion of the build architecture ..... 10**

206 **Figure 2-4: Zoomed in top left portion of the build architecture ..... 10**

207 **Figure 2-5: Zoomed in middle right portion of the build architecture ..... 11**

208 **Figure 2-6: Zoomed in middle left portion of the build architecture ..... 11**

209 **Figure 2-7: Zoomed in bottom right portion of the build architecture..... 12**

210 **Figure 2-8: Zoomed in bottom left portion of the build architecture..... 12**

211 **Figure 3-1: 8428 identification, Scenario A ..... 19**

212 **Figure 3-2: 8428 event handling, Scenario A..... 20**

213 **Figure 3-3: 8428 analysis and response, Scenario A ..... 21**

214 **Figure 3-4: 8428 end of incident, Scenario A..... 24**

215 **Figure 3-5: 8428 identification, Scenario B ..... 27**

216 **Figure 3-6: 8428 event handling, Scenario B ..... 28**

217 **Figure 3-7: 8428 analysis and response, Scenario B ..... 29**

218 **Figure 3-8: 8428 end of incident, Scenario B..... 32**

219 **Figure 3-9: 8428 DFIR Identification, Scenario C ..... 35**

220 **Figure 3-10: 8428 Event Handling, Scenario C..... 37**

221 **Figure 3-11: 8428 Analysis and Response, Scenario C ..... 38**

222 **Figure 3-12: 8428 End of Incident, Scenario C..... 40**

223 **Figure 4-1: Path to Windows Applications and Service Logs in Event Viewer ..... 47**

224 **Figure 4-2: Path to DriverFrameworks-UserMode Operational logs in Event Viewer..... 47**

225 **Figure 4-3: Opening the Driver Frameworks Operational logs properties..... 48**

226 **Figure 4-4: The properties used for the Driver Frameworks logs in Scenario A..... 49**

227 **Figure 4-5: The location of the “inputs.conf” file for the Splunk Universal Forwarder ..... 50**

228 **Figure 4-6: The “inputs.conf” file opened in Notepad++ to add Operational logs to the ingest ..... 51**

229 **Figure 4-7: Restarting the Splunk Forwarder service..... 51**

230 **Figure 4-8: The “Create New Dashboard” button on the top-right of the Splunk web interface ..... 52**

231 **Figure 4-9: The menu for creating a new dashboard in Splunk..... 53**

232 **Figure 4-10: The “Add Panel” button highlighted in a newly created Splunk dashboard ..... 53**

233 **Figure 4-11: Creating a new “Statistics Table” in a Splunk dashboard, search string included ..... 54**

234 **Figure 4-12: A newly created panel in the Splunk dashboard..... 54**

235 **Figure 4-13: Changing the title of a panel in the Splunk dashboard..... 54**

236 Figure 4-14: Saving the Splunk dashboard once all panels are created..... 56

237 Figure 4-15: Final “Removable Storage Connections” dashboard in Splunk..... 57

238 Figure 4-16: Final “Removable Storage Connections” dashboard in Splunk..... 57

239 Figure 4-17: Final “Removable Storage Connections” dashboard in Splunk..... 58

240 Figure 4-18: Showing the “Schedules” button in FactoryTalk® AssetCentre ..... 59

241 Figure 4-19: The “Schedules” view in AssetCentre ..... 59

242 Figure 4-20: Location of the “Working Folders” without the “.mer” file present ..... 60

243 Figure 4-21: Location of the stored “.mer” project file in AssetCentre ..... 60

244 Figure 4-22: Right-clicking on the Supervisory HMI asset and selecting “Get”  
 245 to pull the “.mer” file ..... 61

246 Figure 4-23: The default “Get” options in AssetCentre ..... 61

247 Figure 4-24: “.mer” file now located in the “Working Folders” directory after  
 248 using the “Get” tool ..... 62

249 Figure 4-25: The default view after logging into the web interface for ForceField ..... 62

250 Figure 4-26: The default view when selecting the “Upload” option in ForceField..... 63

251 Figure 4-27: Selecting a file to upload to ForceField..... 64

252 Figure 4-28: After selected, the files to upload will show here in ForceField ..... 64

253 Figure 4-29: Showing that the files were successfully backed up in ForceField..... 64

254 Figure 4-30: The default view after logging into the web interface for ForceField ..... 65

255 Figure 4-31: A list of uploaded files residing in ForceField..... 65

256 Figure 4-32: The FactoryTalk® Diagnostics logs residing in Event Viewer ..... 66

257 Figure 4-33: The FactoryTalk® Diagnostics logs residing in Event Viewer ..... 67

258 Figure 4-34: The location of the “inputs.conf” file to edit ..... 68

259 Figure 4-35: The “inputs.conf” file opened in Notepad++ to add FactoryTalk®  
 260 logs to the ingest ..... 69

261 Figure 4-36: Restarting the Splunk Forwarder service..... 70

262 Figure 4-37: Searching for the newly ingested FactoryTalk® Diagnostic logs ..... 70

263 Figure 4-38: Login screen for the web interface of Dragos ..... 71

264 Figure 4-39: Creating a new case in the Dragos web interface ..... 72

265 Figure 4-40: Newly created case listed in Dragos ..... 72

266 Figure 4-41: Unplugging the Ethernet cable from the WAN port..... 73

267 Figure 4-42: Network diagram showing where the Supervisor HMI is  
 268 plugged into the Siemens switch..... 73

269 **Figure 4-43: Data historian showcasing the tags indicating system start and stops** ..... 74

270 **Figure 4-44: Selecting the file to upload using Rockwell’s Transfer Utility**..... 75

271 **Figure 4-45: Comparing files using Rockwell’s Transfer Utility** ..... 76

272 **Figure 4-46: Blue line indicating the malicious file name and date of occurrence**..... 76

273 **Figure 4-47: Audit log showing which users logged in recently** ..... 76

274 **Figure 4-48: Updating a Dragos ticket with a new comment**..... 77

275 **Figure 4-49: Highlighting the Edit Settings button for a virtual machine (VM) in vCenter** ..... 78

276 **Figure 4-50: Highlighting where to turn off network adapters for VMs in Edit Settings**..... 78

277 **Figure 4-51: Network settings for a VM turned off in Edit Settings** ..... 79

278 **Figure 4-52: The Take Snapshot button on a VM’s settings page**..... 80

279 **Figure 4-53: The Take Snapshot button in the Actions context menu**..... 80

280 **Figure 4-54: Entering details for the snapshot to be created**..... 81

281 **Figure 4-55: Snapshot progress in vCenter** ..... 81

282 **Figure 4-56: Snapshots in the VM’s settings in vCenter**..... 82

283 **Figure 4-57: Windows Settings window, searching for “Ethernet settings”** ..... 82

284 **Figure 4-58: Highlighting “Change adapter options” in Ethernet settings**..... 83

285 **Figure 4-59: Disabling the unwanted Ethernet adapter in Network Settings on Windows**..... 83

286 **Figure 4-60: Performing a “Full scan” in the “Virus & threat protection” tab of**  
 287 **Windows Security** ..... 84

288 **Figure 4-61: Searching for a malicious “.mer” configuration file in Windows** ..... 85

289 **Figure 4-62: Custom script for searching the entire C:\ drive for a specific file**..... 85

290 **Figure 4-63: Output of running the custom script, showing all files with that specific name** ..... 86

291 **Figure 4-64: Custom script to search through a computer to find a file based**  
 292 **on a cryptographic hash**..... 86

293 **Figure 4-65: Taking a cryptographic hash of the suspected malicious file to find any variants**..... 87

294 **Figure 4-66: Inputting the hash of the file users want to search for** ..... 87

295 **Figure 4-67: Script output, showing the files that match the hash in the script** ..... 87

296 **Figure 4-68: Stored files in ForceField, with the file wanted for the scenario highlighted**..... 88

297 **Figure 4-69: Showing the button in Dragos to resolve an incident for a case** ..... 90

298 **Figure 4-70: Confirming the change in the status of the case in Dragos** ..... 90

299 **Figure 4-71: Highlighting the new state of the case in Dragos**..... 90

300 **Figure 4-72: Garland hardware configuration**..... 91

301 **Figure 4-73: Garland software configuration** ..... 92

302 **Figure 4-74: ConsoleWorks configured to provide remote access** ..... 93

303 **Figure 4-75: Ignition historian redundancy architecture using Tag Splitter**..... 94

304 **Figure 4-76: Ignition Edge Tag Provider is enabled** ..... 94

305 **Figure 4-77: Ignition outgoing connections configuration** ..... 95

306 **Figure 4-78: Ignition incoming connections configuration** ..... 95

307 **Figure 4-79: Tag Splitter history settings** ..... 96

308 **Figure 4-80: Ignition display for real-time operational data** ..... 97

309 **Figure 4-81: Ignition dashboard for historical data** ..... 97

310 **Figure 4-82: Creating a new Dragos baseline rule** ..... 98

311 **Figure 4-83: Create a custom criteria for the new rule**..... 98

312 **Figure 4-84: Unauthorized Conversation policy creation in Tenable** ..... 99

313 **Figure 4-85: Unauthorized Conversation policy creation in Tenable** ..... 100

314 **Figure 4-86: A Dragos log showing no dissected fields** ..... 101

315 **Figure 4-87: Where to find the “Extract Fields” option for this specific log entry** ..... 102

316 **Figure 4-88: Choosing “Regular Expression” as the field extraction method** ..... 103

317 **Figure 4-89: The top bar of the field extractor, click next to go to the next step** ..... 103

318 **Figure 4-90: Selecting the first custom line to extract as a field, labeled “Date”** ..... 103

319 **Figure 4-91: Selecting second custom line to extract as a field, labeled “Host\_IP”** ..... 104

320 **Figure 4-92: Potential error when selecting too many fields** ..... 104

321 **Figure 4-93: Location of directory to create custom applications in Splunk**..... 105

322 **Figure 4-94: The directory of the custom app, two additional folders created for it**..... 105

323 **Figure 4-95: Location of main “limits.conf” file to edit for the custom application**..... 105

324 **Figure 4-96: Location of “default.meta” file for the custom application**..... 106

325 **Figure 4-97: Default values of the “limits.conf” file** ..... 106

326 **Figure 4-98: New values for the Regex variable, fixing the previous error**..... 106

327 **Figure 4-99: Chosen values for “default.meta” file** ..... 107

328 **Figure 4-100: Same extracted fields as before, no more error after increasing**

329 **Regex limit values** ..... 107

330 **Figure 4-101: The Regex generated based on the previous field selection portion** ..... 107

331 **Figure 4-102: Saving the new Regex created for this field extraction** ..... 108

332 **Figure 4-103: Dragos log now properly dissecting fields due to the Field Extractor tool** ..... 109

333 Figure 4-104: Tenable logs properly dissected and ready for use in a dashboard ..... 110

334 Figure 4-105: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs ..... 111

335 Figure 4-106: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs ..... 112

336 Figure 4-107: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs ..... 112

337 Figure 4-108: An alert generated in Tenable for a Historian Violation of Access policy ..... 113

338 Figure 4-109: Dragos PostgreSQL Historian Baseline Deviation ..... 114

339 Figure 4-110: Creating a new case within Dragos ..... 115

340 Figure 4-111: Cisco firewall configuration ..... 116

341 Figure 4-112: Permit rule for AWS gateway and hosts ..... 117

342 Figure 4-113: Block rule for the ICS network ..... 118

343 Figure 4-114: Select the local historian database server in vCenter ..... 119

344 Figure 4-115: Locate Edit settings for local historian database host in vCenter ..... 120

345 Figure 4-116: Locate “Edit Settings” for local historian database host in vCenter ..... 121

346 Figure 4-117: VM Network adapter settings, currently turned on ..... 122

347 Figure 4-118: VM Network adapter settings, currently turned off ..... 123

348 Figure 4-119: No historian data was shown from the local gateway dashboard ..... 124

349 Figure 4-120: AWS Gateway Ignition historian dashboard ..... 125

350 Figure 4-121: List of notifications in Dragos ..... 125

351 Figure 4-122: Expanding Dragos notification to find additional information ..... 126

352 Figure 4-123: Suspicious large file transfer added to Dragos ticket ..... 127

353 Figure 4-124: Looking for the logs surrounding the time of the event in Kibana ..... 128

354 Figure 4-125: Filter to look for larger amounts of bytes ..... 129

355 Figure 4-126: Seeing a large number of bytes around the time of the notification ..... 130

356 Figure 4-127: Expanded the log to view its contents ..... 131

357 Figure 4-128: Larger amounts of data found ..... 131

358 Figure 4-129: Expanded the log to view its contents ..... 132

359 Figure 4-130: Historian Violation of Access policy definition ..... 133

360 Figure 4-131: Historian Violation of Access policy being triggered ..... 133

361 Figure 4-132: Full Network Summary page in Tenable ..... 134

362 Figure 4-133: Where to find the Network Summary tab ..... 135

363 Figure 4-134: The center portion, showing the latest traffic in gigabytes (GB) on the network ..... 135

364 **Figure 4-135: Shows the most traffic by GBs based on protocol..... 136**

365 **Figure 4-136: The Packet Captures tab, highlighted areas are the**

366 **PCAPs used in the scenario ..... 137**

367 **Figure 4-137: Four downloaded PCAPs from Tenable ..... 138**

368 **Figure 4-138: Choosing the option to merge multiple PCAPs together in Wireshark ..... 138**

369 **Figure 4-139: Selecting the four downloaded PCAPs from Tenable to merge ..... 139**

370 **Figure 4-140: Selecting the option to view network conversations in Wireshark ..... 140**

371 **Figure 4-141: List of all conversations between multiple IP addresses ..... 140**

372 **Figure 4-142: Applying a filter in Wireshark based on conversations ..... 141**

373 **Figure 4-143: Follow TCP Stream in Wireshark ..... 142**

374 **Figure 4-144: A single TCP Stream for a set of packets..... 143**

375 **Figure 4-145: Following another TCP Stream ..... 143**

376 **Figure 4-146: A new TCP Stream showing a different PostgreSQL database being targeted ..... 144**

377 **Figure 4-147: Some key phrases found in TCP Stream to use for further investigation ..... 145**

378 **Figure 4-148: Selecting the JumpBox VM in the graphical view in ConsoleWorks..... 146**

379 **Figure 4-149: Selecting the appropriate desktop session for the jsmith user..... 146**

380 **Figure 4-150: The jsmith user logging into pgAdmin ..... 147**

381 **Figure 4-151: The jsmith user selecting “Backup” for the target database ..... 147**

382 **Figure 4-152: The jsmith user successfully backing up the IGN\_Hist database..... 148**

383 **Figure 4-153: Disabling the jsmith user account in Active Directory..... 149**

384 **Figure 4-154: Changing the jsmith user’s password in ConsoleWorks ..... 150**

385 **Figure 4-155: Changing the jsmith user’s password in ConsoleWorks ..... 150**

386 **Figure 4-156: Tenable policy to track unauthorized S7 traffic ..... 151**

387 **Figure 4-157: Tenable policy to track unauthorized S7+ traffic ..... 152**

388 **Figure 4-158: Splunk dashboard tracking unauthorized S7 and S7+ traffic ..... 152**

389 **Figure 4-159: Splunk dashboard tracking unauthorized S7 and S7+ traffic ..... 153**

390 **Figure 4-160: Splunk dashboard tracking unauthorized S7 and S7+ traffic ..... 153**

391 **Figure 4-161: Enabling specific tags (PRG\_LCH and PRG\_UCH) in the data historian..... 154**

392 **Figure 4-162: Creating a new ticket in Dragos..... 155**

393 **Figure 4-163: Adding a justification for the ticket ..... 155**

394 **Figure 4-164: Updating the Dragos ticket to include the operator locking**

395 **down the ICS network..... 156**

396 **Figure 4-165: Changing the Dragos ticket priority to 5** ..... 157

397 **Figure 4-166: Converting the Dragos ticket to an incident** ..... 157

398 **Figure 4-167: Adding information about the jsmith user to Dragos ticket** ..... 158

399 **Figure 4-168: Adding additional details to the Dragos ticket about the jsmith user** ..... 159

400 **Figure 4-169: SIBERprotect HMI indicates threat detected** ..... 160

401 **Figure 4-170: Operator lockdown (segment) selection** ..... 160

402 **Figure 4-171: All recent logs from the unauthorized S7+ traffic policy in Tenable** ..... 161

403 **Figure 4-172: Tenable alert showing the engineering workstation**  
 404 **accessing PLC via S7+ connection** ..... 161

405 **Figure 4-173: Error when opening the TIA Portal showing the user**  
 406 **who was still logged into the system**..... 162

407 **Figure 4-174: Task Manager in Windows showing the jsmith user was disconnected** ..... 162

408 **Figure 4-175: Show the user’s last login** ..... 163

409 **Figure 4-176: Viewing the latest desktop recording of users**..... 163

410 **Figure 4-177: Watching a recording of the jsmith user logging into the TIA Portal** ..... 164

411 **Figure 4-178: Recording of the jsmith user accessing PLC Tags**..... 164

412 **Figure 4-179: TIA Portal install navigation menu** ..... 165

413 **Figure 4-180: TIA Portal install settings** ..... 166

414 **Figure 4-181: ForceField web interface**..... 167

415 **Figure 4-182: Selecting the latest known-good backup for the Conveyor program**..... 167

416 **Figure 4-183: Adding a password to Siemens PLC**..... 168

417 **Figure 4-184: Compile PLC program**..... 169

418 **Figure 4-185: Download configuration to PLC**..... 170

419 **List of Tables**

420 **Table 1: List of collaborators, their products, and their functions within the build architecture**..... 5

421 **Table 2: Products used, their capabilities, and the associated CSF 2.0 mappings** ..... 7

## 422 Executive Summary

423 Manufacturing systems play a critical role in the supply chain and are essential to the nation's economic  
424 security. Manufacturing organizations rely on Industrial Control Systems (ICS) to monitor and control  
425 physical processes to improve business agility and operational efficiencies. These same systems are  
426 facing an increasing number of cyber incidents from destructive malware, malicious insider activity,  
427 hardware failures, or unintended human error. Potential outages can be significant in scope and  
428 downtime, and may result in a loss of production, affecting safety controls for personnel, or the loss of  
429 millions of dollars to the organization. While defense-in-depth security architecture can help mitigate  
430 these risks, it cannot guarantee the elimination of cyber incidents. Therefore, manufacturing  
431 organizations should have a plan in place to maintain a resilient infrastructure in the event of cyber  
432 incidents that impact operations. To help with these challenges, this practice guide was developed using  
433 the *NIST Cybersecurity Framework (CSF) 2.0* [\[1\]](#) as the basis for a response and recovery effort. The CSF  
434 defines standardized outcomes upon which organizations can base response and recovery objectives.

435 For organizations without established cybersecurity controls, establishing and implementing response  
436 and recovery procedures can be a daunting task. In addition, guidelines and frameworks alone can be  
437 difficult to follow without practical applications. In response, the National Institute of Standards and  
438 Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) worked with stakeholders and  
439 industry collaborators specializing in response and recovery to demonstrate the practical application of  
440 cybersecurity technologies in a discrete-based manufacturing system that emulates a typical  
441 manufacturing environment. The effort resulted in this Practice Guide, providing three functional  
442 scenarios that demonstrate implementation of response and recovery procedures using commercially  
443 available technologies. The aim is to illustrate effective execution of response and recovery  
444 fundamentals, as well as highlight the benefits that result from the deployment of technologies that  
445 improve operational resilience.

446 Key takeaways from the development of this Practice Guide are as follows:

- 447 • Planning and preparation are critical in responding to and recovering from cyber incidents, since  
448 risks still exist despite efforts to implement defense-in-depth protections against known threats.
- 449 • Logging and visibility across assets and the supporting ecosystem improve investigation,  
450 diagnostics, and protection, and shorten the time between detection and containment.
- 451 • Robust monitoring goes beyond simple event logging and should include behavioral analysis and  
452 ongoing coordination between the OT engineering and the Security Operations Center (SOC)  
453 team.
- 454 • Human factors, such as employee training on the stages of response and recovery,  
455 communicating between IT and ICS administrators, and working with OT product vendors, will  
456 allow for effective plan implementation in addition to technical solutions.

## 457 1 Introduction

458 This publication provides practical information to organizations with ICS environments seeking to apply  
459 CSF objectives related to response and recovery, utilizing a range of improved capabilities (such as  
460 detection, analysis, and network architecture improvements) with the goal of establishing operational  
461 resiliency. The NCCoE-led consortium of project collaborators developed reference architectures,  
462 identified scenarios (system compromise, data exfiltration, and unauthorized command messaging), and  
463 investigated approaches and capabilities in conducting effective response and recovery. In conjunction  
464 with the CSF, this practice guide also draws upon the publication *NISTIR 8428, Digital Forensics and  
465 Incident Response (DFIR) Framework for Operational Technology (OT)* [2], which was also developed to  
466 assist organizations by providing response and recovery workflows. In addition, this guide references  
467 response steps from *NIST SP 800-61r3, Incident Response Recommendations and Considerations for  
468 Cybersecurity Risk Management: A CSF 2.0 Community Profile* [3] to support the core objectives of the  
469 CSF.

470 While the project consortium decided to utilize workflows from the DFIR, with additional reference to  
471 800-61r3, we note that organizations using this publication should establish their own workflow and  
472 planning practices specifically tailored for their own environments. Also note that the reference  
473 architectures were intentionally designed with a modular "building block" approach, based on distinct  
474 capabilities, which will allow organizations to deploy the design in whole or in part over time within their  
475 own ICS environments based on operational needs, limitations, or risk priorities. For example, Scenario C  
476 demonstrates handling and response (in this case, network isolation) using Siemens components; while  
477 your manufacturing environment may use different equipment, it can still benefit from taking a similar  
478 approach and workflow in implementing network isolation.

### 479 1.1 Scope

480 This project covers the activities in conducting response and recovery of an ICS environment following  
481 the detection of a cyber incident and provides guidance on how manufacturers can increase operational  
482 resiliency by integrating supporting technologies and capabilities (such as detection) into their  
483 architectures. The guidance provided is illustrated with step-by-step examples showing the workflows  
484 and tasks needed to satisfactorily resolve cyber events.

485 The document focuses on the Respond (RS) and Recover (RC) core functions of the CSF. *NISTIR 8428* and  
486 *NIST SP 800-61r3* are used as supporting documents for the cyber incident scenarios. These stages  
487 included areas such as:

- 488 • Detection, reporting, and analysis of events
- 489 • Collection and review of logs and monitoring information
- 490 • Handling, response, eradication, and recovery from incidents

491 Designed with collaborators, the above-mentioned activities are supported by capabilities that are  
492 exercised in the demonstration scenarios in this guide, including but not limited to:

- 493 • Establishing case documentation for incidents

- 494 • Monitoring and analysis of network traffic, trends, and configuration changes
- 495 • Utilizing security information and event management
- 496 • Performing access management
- 497 • Enabling recovery from known good backups and configurations through the use of immutable  
498 storage
- 499 • Maintaining resilient infrastructure through cloud, data historians, and networking architecture

500 For this project, note that ICS refers to control systems such as PLCs that combine control components  
501 (e.g., robot arm, sensors) to achieve the goals of a manufacturing organization. Also note that this  
502 document does not focus on traditional business IT environments. Given the real-time and deterministic  
503 nature of ICS systems, there are specific considerations for addressing cyber threats beyond what is  
504 normally addressed in IT environments. Also, although OT and IT environments are becoming  
505 increasingly interconnected, there may be differences between them with regard to response and  
506 recovery methodologies.

507 This practice guide focuses on:

- 508 • Reducing downtime for operations
- 509 • Leveraging tools for faster response and recovery
- 510 • Enabling logging capabilities with a sample of ICS tools
- 511 • Conducting data aggregation and forensic analysis techniques
- 512 • Exploring different containment options within an ICS environment

## 513 1.2 Audience

514 The information in this guide is intended for those responsible for ICS systems within their organizations.  
515 It will also assist program management, individuals tasked with making business decisions, security  
516 officers, and those engaging in general cybersecurity of the ICS environment. This includes but is not  
517 limited to:

- 518 • Asset owners and stakeholders
- 519 • Technology providers and integrators of ICS systems
- 520 • Critical Infrastructure operators
- 521 • Public and private utility providers
- 522 • State and Local government regulators

## 523 1.3 How to Use This Guide

524 This document is organized as follows:

- 525 • Section 1 (this section) provides an overview of the project, its scope, and intended audience.
- 526 • Section 2 outlines the approach of the project by providing the reference architectures, control  
527 mappings, and associated vendor products, and assumptions made in the scenarios.

- 528 • Section 3 provides the detailed stages of each scenario, showing how the stages of response and  
529 recovery were conducted.
- 530 • Section 4 highlights lessons learned and summarizes the general findings from the scenarios.
- 531 • Appendix A is a list of acronyms
- 532 • Appendix B includes the references
- 533 • Appendix C outlines the step-by-step instructions used to implement each stage of the scenarios  
534 (Note: Appendix C will be made available as a separate online resource).

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

- 536 • Business decision-makers, including chief information security and technology officers, can use  
537 the Executive Summary, Introduction, and Project Overview to understand the motivation for  
538 this guide, the cybersecurity challenge being addressed, an approach to solving this challenge,  
539 and how the solution could benefit their organization.
- 540 • Program Managers for technology, security, and privacy who are concerned with identifying  
541 technologies to enhance cyber incident response and recovery can use the Project Overview and  
542 General Findings. Those sections describe what is built, why, and key takeaways.
- 543 • ICS cybersecurity and IT professionals who want to prepare for incident response and recovery  
544 in a manufacturing environment can make use of Functional Demonstrations and Build  
545 Implementation Instructions. These sections present how response and recovery capabilities can  
546 be used in response to cyber attacks. Regular testing of response and recovery plans is advised  
547 for any manufacturing organization. This practice guide can also be used in the design of  
548 tabletop exercises.

549 In addition, the NCCoE OT project team will also provide further guidance to supplement this practice  
550 guide, to be provided at <https://www.nccoe.nist.gov/manufacturing>. The resources will include an OT  
551 Security Series and White Papers covering various related topics.

## 552 **2 Project Overview**

553 The Manufacturing project at the National Institute of Standards and Technology (NIST) is a  
554 collaborative, standards-driven initiative implemented by the National Cybersecurity Center of  
555 Excellence (NCCoE) to demonstrate how to operationalize the Cybersecurity Framework core functions  
556 (e.g., Detect, Respond, Recover) to help manufacturing organizations quickly, safely, and effectively  
557 recover from a cyber incident. Eleven collaborators have engaged with the NCCoE throughout project  
558 development to provide technology solutions, integrate those solutions into the NCCoE lab  
559 infrastructure, and design scenarios that highlight how processes and tools can be leveraged to improve  
560 response and recovery efforts in a manufacturing environment. This document provides a detailed  
561 description of how the collaborator products meet the capabilities outlined in the scope to enhance  
562 response and recovery in operational environments.

### 563 **2.1 Project Approach & Assumptions**

564 Working with the CRADA partners, the NCCoE team approached this project by developing three cyber  
565 incident scenarios focusing on real-world use cases. These scenarios were developed to demonstrate  
566 the implementation of response and recovery procedures using commercially available technologies. All

567 three scenarios simulate a malicious incident, one involving an unknowing participant with a USB device  
568 and the others involving active threats in the ICS environment. Each scenario simulates various cyber  
569 threats that can shut down operations. Each scenario will use cybersecurity capabilities (e.g., case  
570 management, analysis, containment, eradication, recovery, and resilient architecture) to apply the core  
571 functions from the CSF. The aim is to illustrate effective execution of detection, response, and recovery,  
572 as well as highlight the benefits that result from the deployment of technologies that improve  
573 operational resilience.

574 The practice guide assumes that an Incident Response Plan (IRP) has been developed by the  
575 organization, that the IRP includes a workflow similar to *NISTIR 8428* [2], and the Incident Response  
576 Team (IRT) follows their IRP throughout the response and recovery effort. As each scenario is executed  
577 in the NCCoE lab, the IRT's progression through response and recovery is captured in this guide. Section  
578 3 follows the process of responding and recovering through the scenarios, while Appendix C details the  
579 technical implementation of response and recovery tools used to accelerate response and recovery  
580 time.

## 581 2.2 Response and Recovery Challenges

582 ICS systems and networks are facing an increasing number of cyber incidents, which present a significant  
583 threat to safety, production, and financial stability. Organizations that rely on these systems are  
584 required to constantly develop mature cybersecurity capabilities to meet these challenges. However,  
585 to the extent that cybersecurity demands are prioritized, a manufacturer may struggle to keep up with  
586 the pace of changes and requirements needed to maintain a secure posture.

587 Establishing effective **response** activities in OT environments requires capabilities such as rapid  
588 identification of threats and incidents, coordination across subsystems and differing vendor equipment,  
589 and visibility into networks and operational components. However, many ICS systems have  
590 correspondingly limited logging and telemetry into legacy assets, constraints on managing third-party  
591 vendor subsystems, the use of a wide range of hardware and associated network protocols, and  
592 inconsistent approaches to coordinating information across business units and operations. Unless  
593 addressed, these conditions create a challenging environment to accomplish response objectives.

594 Similarly, a mature **recovery** program involves robust backup (software) and spares (hardware)  
595 strategies, ongoing employee training and awareness, established methods such as playbooks for types  
596 of incidents, and trusted / known-good configurations and files. Despite this, many manufacturing  
597 organizations may not prioritize these practices in their environments, possibly due to tight production  
598 schedules, downtime management, supply chain issues with a wide variety of ICS components,  
599 dependencies on specialized vendor equipment, and gaps in training and awareness. With these  
600 conditions, recovery practices may remain ineffective and lead to longer outages.

601 In addition, ICS systems are also becoming more integrated with IT in their supporting ecosystem,  
602 creating new sets of challenges. Historically, ICS and their networks were isolated from business systems  
603 and IT networks. Isolation allowed for a limited attack surface; therefore, systems were designed for  
604 enhanced reliability with limited consideration for cyber incidents. As IT and ICS networks become more  
605 integrated, this increases the likelihood of an attack, and cybersecurity controls implemented in ICS  
606 environments have not kept pace with modern threats. The cyber risk mitigations used in IT networks  
607 (e.g., intrusion prevention systems (IPS)) are often not suitable for ICS networks because of the real-time

608 and deterministic nature of ICS (e.g., an IPS accidentally stopping safety control functions). Due to IT and  
 609 OT convergence, the need for plans to respond and recover from a potential cyber attack is more  
 610 apparent, as the challenges lead to an increasing likelihood of a cyber incident.

## 611 2.3 Project Collaborators

612 The NIST project team would like to acknowledge the CRADA consortium that helped us realize the  
 613 Manufacturing Response & Recovery project. A Federal Register Notice invited technology providers to  
 614 join this project by providing their products and/or expertise to develop example solutions. Eleven  
 615 collaborators have engaged with the NCCoE throughout project development to provide technology  
 616 solutions, integrate those solutions into the NCCoE lab infrastructure, and design scenarios that  
 617 highlight how processes and tools can be leveraged to improve response and recovery efforts in a  
 618 manufacturing environment. The following table is a high-level overview of our CRADA partners, their  
 619 products, and their functions in the build architecture:

620 **Table 1: List of collaborators, their products, and their functions within the build architecture**

Collaborator	Product	Function
AWS (Amazon Web Services)	AWS Infrastructure as a Service (IaaS)	Cloud infrastructure for redundant data historian
Cisco	1) Splunk 9.2.2 2) Industrial Security Appliance (ISA) 3000	Splunk for the Security Information and Event Management (SIEM) system ISA 3000 for the networking infrastructure
Dragos	1) Dragos Platform: SiteStore Version 2.5.4 2) Dragos Sensor Version 12.18.15 3) KP Plus 10.0.2-9.63.0	Asset inventory, baseline deviation detection, and case management
Garland Technology	High Density SPAN/TAP Aggregator INT1G10CSASP	Enables SPAN network traffic to Dragos and Tenable
Inductive Automation	Ignition V8.1.36	Data historian
Google Cloud (including Mandiant)	Engineering Services	Ensure the standards-based solutions for responding to and recovering from a cyber attack align with their practical experience
GreenTec-USA, LLC	ForceField 1.9	Immutable storage solution for backups

Collaborator	Product	Function
Rockwell Automation	1) FactoryTalk® AssetCentre Change Management 2) FactoryTalk® AssetCentre Inventory Agent 3) FactoryTalk® AssetCentre Disaster Recovery	Management of ICS backups and disaster recovery
Siemens	1) SIBERprotect 2) SCALANCE 3) TIA Portal	SIBERprotect for syslog ingestion; displays information to security HMI  SCALANCE for isolating ICS environment, securing communications
TDi Technologies	ConsoleWorks 5.6	Remote access and records desktop sessions
Tenable	Tenable OT Security Version 3.17.40	Configuration management and baseline deviation detection

## 621 2.4 Build Architecture & Collaborator

622 Figure 2-1 shows the high-level build architecture located in NCCoE's Manufacturing Lab in Rockville,  
 623 MD. Collaborator tools were integrated with this base unit to demonstrate response and recovery  
 624 capabilities.

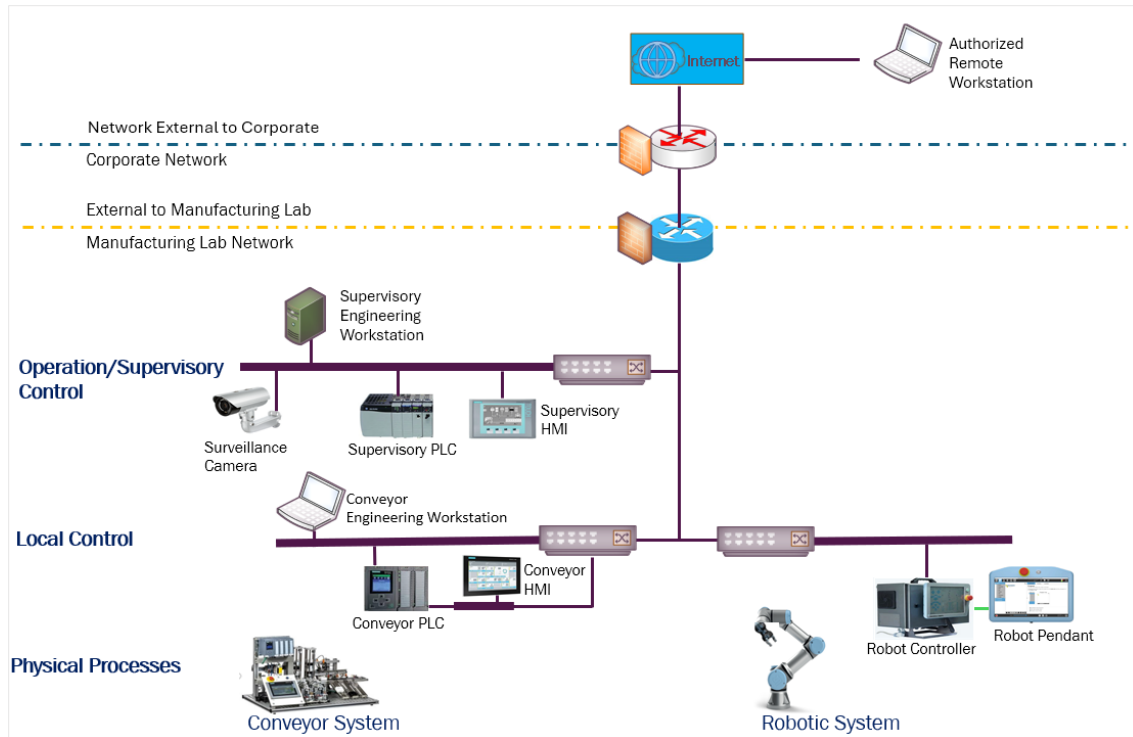


Figure 2-1: Discrete manufacturing without security tools

625

626 The demonstration unit consists of a conveyor system for sorting and transporting unfinished objects, a  
 627 robotic system for assembling blocks, and a storage unit for storing finished products. These systems are  
 628 controlled and operated by a controller, PLCs, and HMIs. A supervisory system enables communication  
 629 between the two main systems. Laptops and virtual machines are used, along with engineering software  
 630 and networking equipment, to interface with the discrete manufacturing system.

### 631 2.4.1 Product Control Mappings

632 Table 1-1 lists the capabilities demonstrated in this project, the mapping of the capabilities to the NIST  
 633 *Cybersecurity Framework 2.0* [1], and the specific vendor’s products that relate to those capabilities and  
 634 mappings. The product implementation details will later be mapped to *NIST SP 800-61r3* and *NISTIR*  
 635 *8428* in the *Demonstration Use Cases* section.

636 Table 2: Products used, their capabilities, and the associated CSF 2.0 mappings

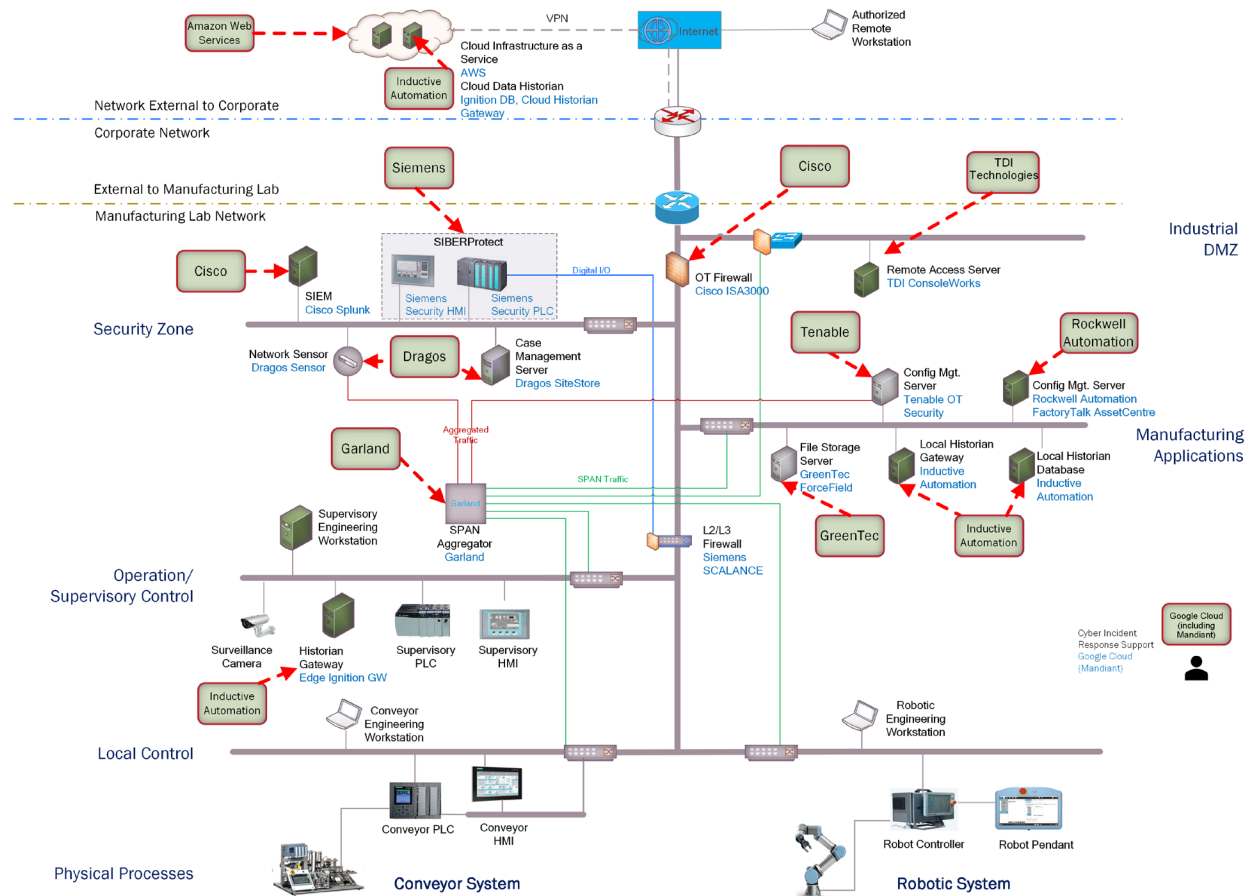
Project Capability	NIST Cybersecurity Framework Subcategories Mapping	Vendor	Product(s)
Case Management	RS.MA	Dragos	Dragos Platform: SiteStore Version 2.5.4 Dragos Sensor Version 12.18.15 KP Plus 10.0.2-9.63.0

Project Capability	NIST Cybersecurity Framework Subcategories Mapping	Vendor	Product(s)
<b>Analysis</b>	RS.AN PR.PS-01 PR.PS-04 DE.CM-01	Dragos	Dragos Platform: SiteStore Version 2.5.4 Dragos Sensor Version 12.18.15 KP Plus 10.0.2-9.63.0
		Google Cloud (including Mandiant)	Engineering Services
		Inductive Automation	Ignition V8.1.36
		Rockwell Automation	FactoryTalk® AssetCentre Change Management FactoryTalk® AssetCentre Inventory Agent
		Cisco	Splunk 9.2.2
		TDi Technologies	ConsoleWorks 5.6
		Tenable	Tenable OT Security Version 3.17.40
<b>Containment</b>	RS.MI-01	Cisco	Industrial Security Appliance (ISA) 3000
		Siemens	SIBERprotect
<b>Eradication</b>	RS.MI-02	TDi Technologies	ConsoleWorks 5.6
<b>Recovery</b>	PR.DS-11	GreenTec USA	ForceField 1.9
	RC.RP-03 RC.RP-05	Rockwell Automation	FactoryTalk® AssetCentre Disaster Recovery
<b>Resilient Infrastructure</b>	PR.IR-03	Amazon Web Services (AWS)	AWS Infrastructure as a Service (IaaS)
	DE.CM-01	Garland Technology	High Density SPAN/TAP Aggregator INT1G10CSASP

637 **2.4.2 Build Components**

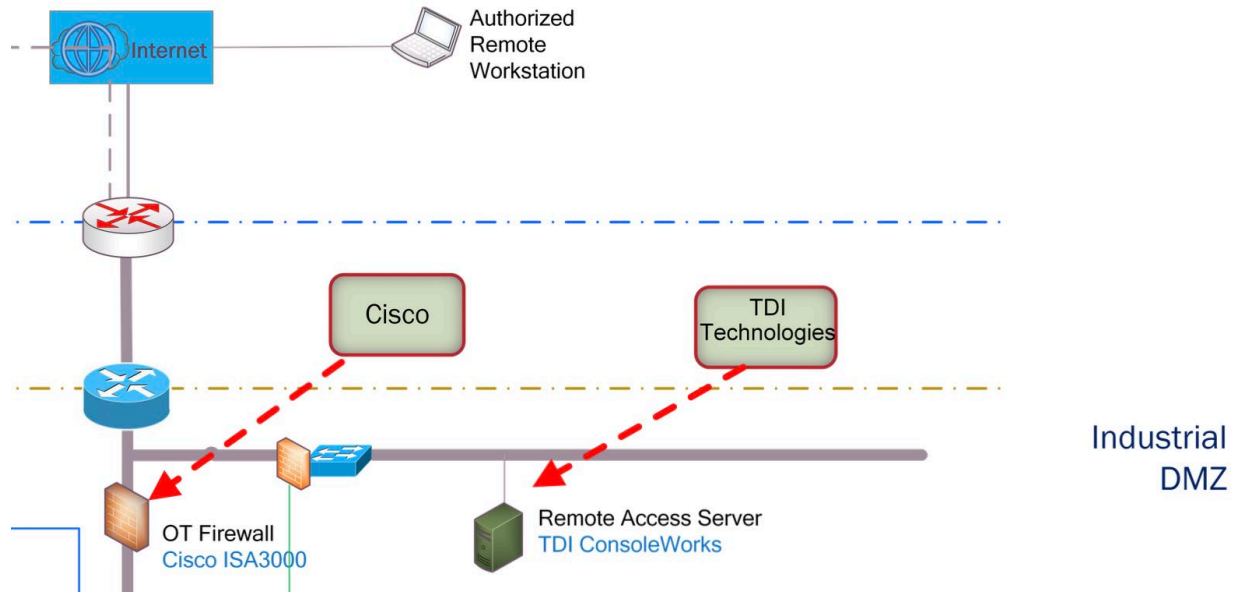
638 The following set of figures illustrates a high-level diagram of how the collaborators were integrated into  
 639 the ICS environment to enhance response and recovery for manufacturing. The three scenarios were  
 640 designed to include as many collaborators as feasible based on the narrative and execution details  
 641 defined in [Section 3](#).

642 *Note: Figures 2-3 to 2-8 are zoomed-in portions of the entire diagram for visual clarity.*

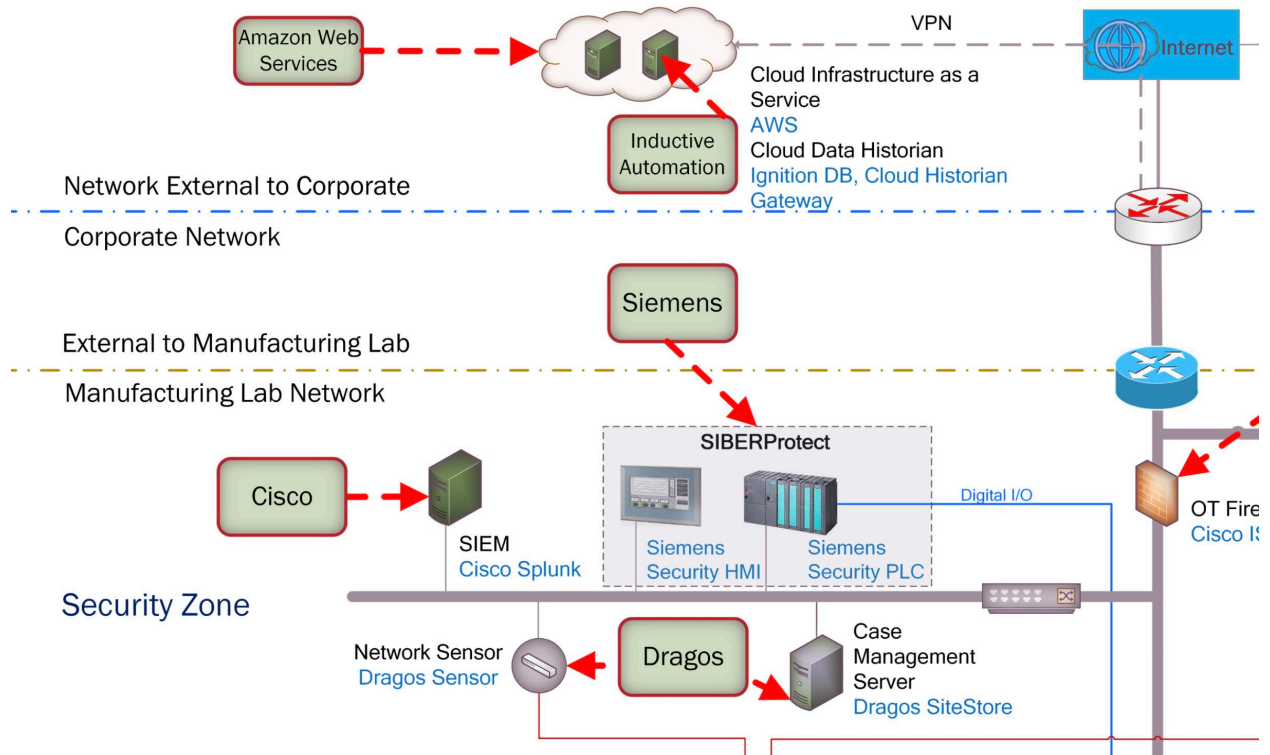


643 **Figure 2-2: Build architecture with security tools**

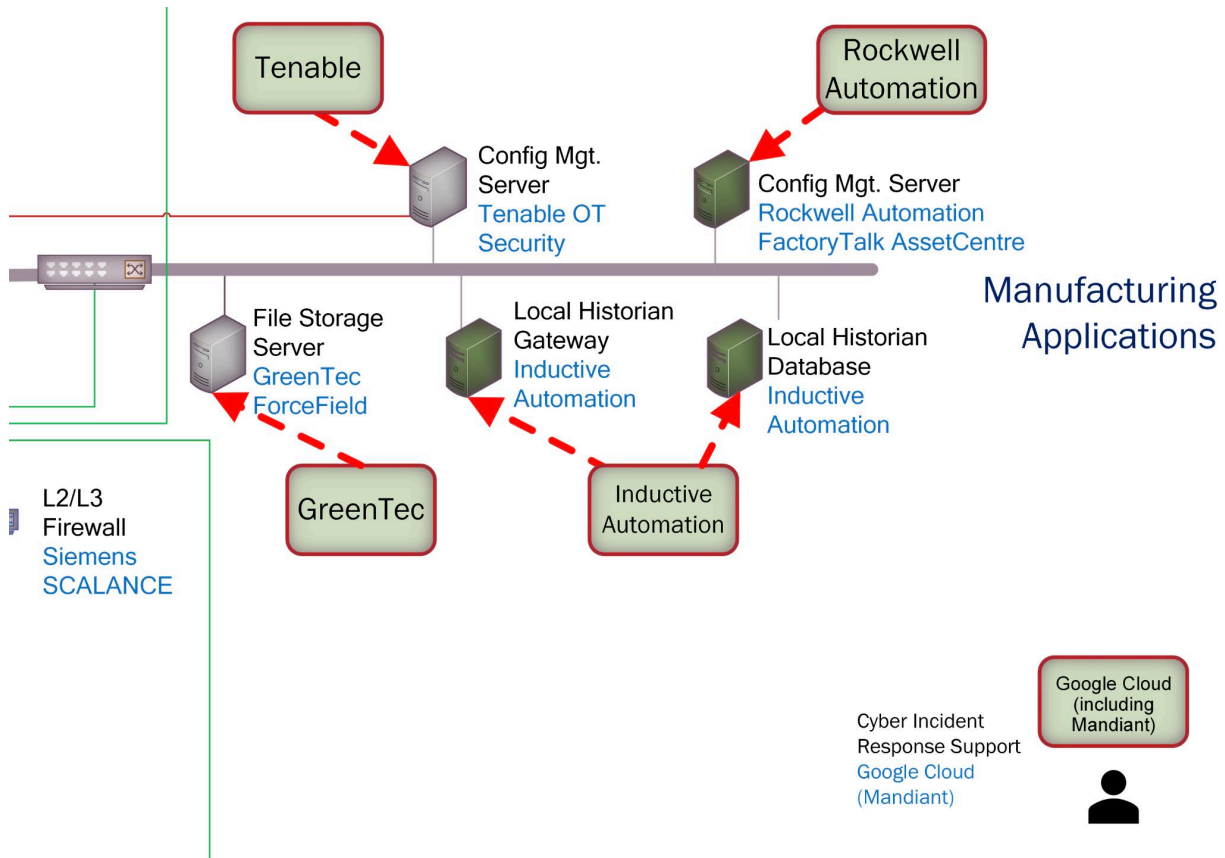
644 *Note: Red borders and arrows in the figures indicate collaborator-provided solutions.*



645 **Figure 2-3: Zoomed in top right portion of the build architecture**

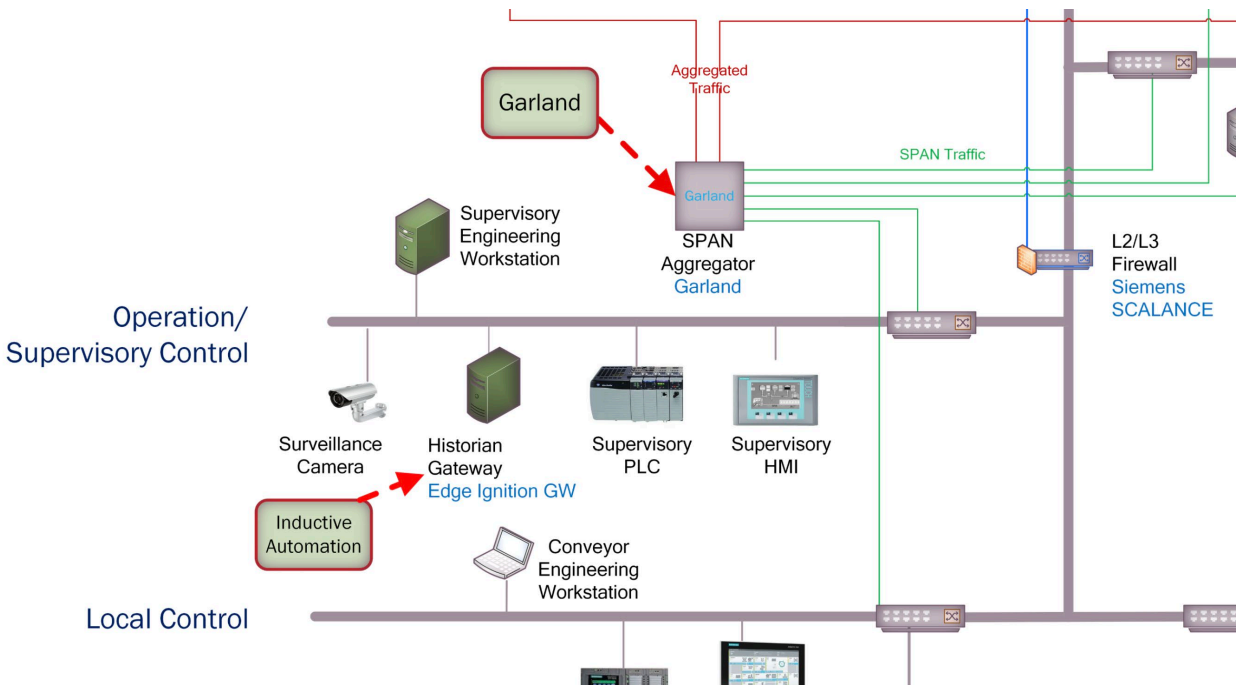


646 **Figure 2-4: Zoomed in top left portion of the build architecture**



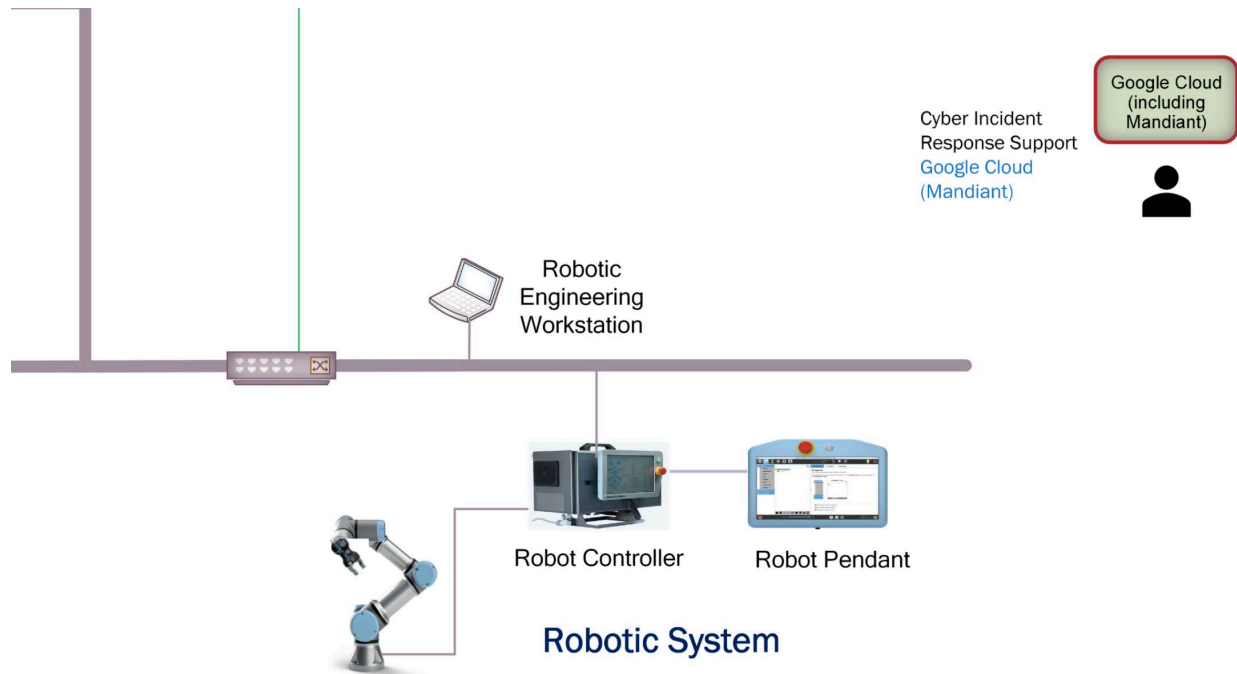
647

Figure 2-5: Zoomed in middle right portion of the build architecture



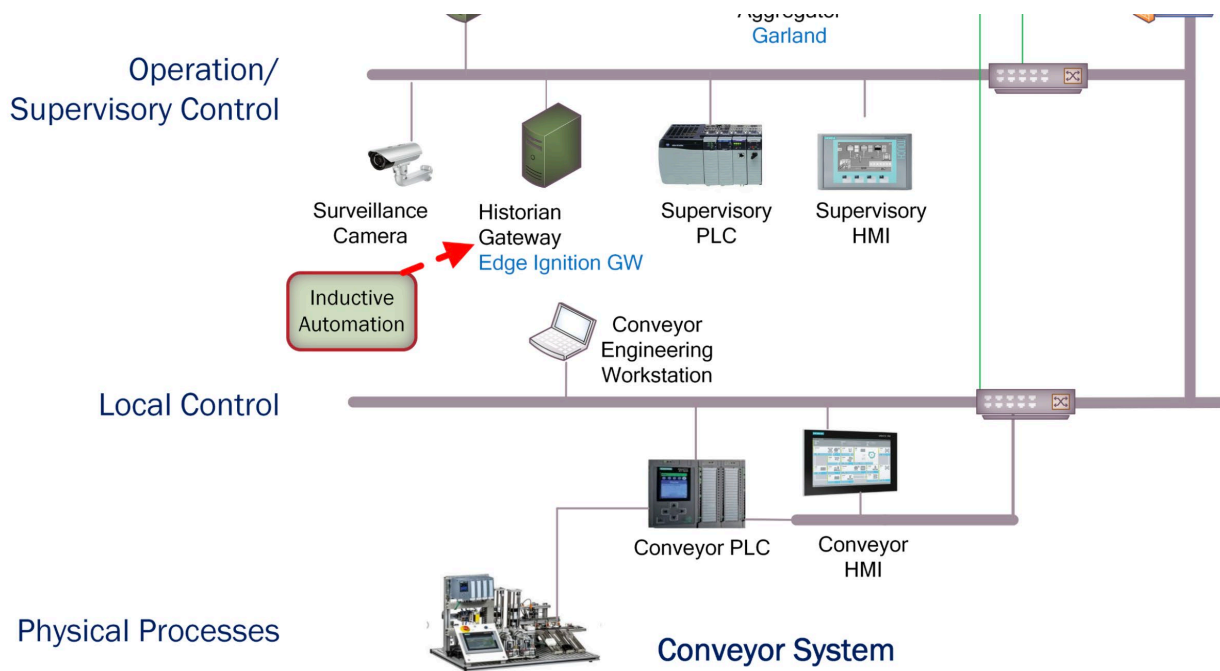
648

Figure 2-6: Zoomed in middle left portion of the build architecture



649

Figure 2-7: Zoomed in bottom right portion of the build architecture



650

Figure 2-8: Zoomed in bottom left portion of the build architecture

651 **2.4.3 Build Details**

652 This section details the features and configurations of the collaborator tools that were selected for  
 653 demonstration in this project.

### 654 *2.4.3.1 Garland Technology*

#### 655 **High-Density SPAN/TAP Aggregator INT1G10CSASP**

656 The build architecture includes two detection platforms for the purpose of case management and  
657 configuration management. To deliver mirrored network traffic from all switches to two different  
658 platforms, an aggregator was needed. Garland provided their SPAN Aggregator to ingest SPAN traffic  
659 from multiple switches and output two connections: one to Dragos and one to Tenable. The Garland  
660 product was an enabling infrastructure component supporting detection technologies.

661 The High-Density SPAN Aggregator with (8) Copper Inputs is integrated into the ICS network, collecting  
662 mirrored network traffic from the following networks:

- 663 • Local control for conveyor and robotic systems
- 664 • Operation/Supervisory control
- 665 • Manufacturing applications
- 666 • Security zone
- 667 • Industrial DMZ

668 Aggregated signals are copied to two security solutions:

- 669 • Dragos Platform Sensor
- 670 • Tenable OT Security Server

### 671 *2.4.3.2 Dragos*

#### 672 **Dragos Platform:**

673 **SiteStore Version 2.5.4**

674 **Dragos Sensor Version 12.18.15**

675 **KP Plus 10.0.2-9.63.0**

676 A Dragos sensor and SiteStore support cyber incident case management for enabling cross-functional  
677 collaboration and reporting. The sensor is installed in the Security Zone and receives mirrored network  
678 traffic from the Garland Aggregator and passes information to the Dragos SiteStore. Collectively, these  
679 tools passively monitor network traffic, create a list of assets, and analyze the traffic for threats. Once  
680 the Dragos platform identifies an asset, incident cases can be created and tracked against it.

### 681 *2.4.3.3 Tenable*

#### 682 **Tenable OT Security Version 3.17.40**

683 Tenable OT Security provides the ability to detect and alert on changes to network traffic. The Tenable  
684 OT server ingests network traffic from the Garland Aggregator, creates an asset inventory, monitors  
685 network traffic, and alerts on various networking anomalies. This tool was configured to send an alert to  
686 the Siemens SIBERprotect solution via syslog once Tenable detected an adversarial connection to a PLC.

#### 687 *2.4.3.4 Amazon Web Services*

##### 688 **AWS Infrastructure as a Service**

689 AWS's cloud infrastructure enables off-premise redundancy of the Inductive Automation Ignition data  
690 historian. Data historians are large databases and user interfaces that allow someone to view historical  
691 trends for maintenance, operational improvements, and investigations. Redundancy is desirable for  
692 many critical systems in an operational environment, including the data historian. In this architecture,  
693 the Ignition data historian software is configured on the AWS infrastructure to serve as a backup for the  
694 on-premise data historian.

#### 695 *2.4.3.5 Inductive Automation*

##### 696 **Ignition V8.1.36**

697 The Ignition Tag Historian Module is used to receive, store, and display historical tag data from the robot  
698 controller, conveyor PLC, and supervisory PLC. A redundant data historian architecture is implemented  
699 using an Edge server installed in the Operation/Supervisory Control network to collect real-time ICS  
700 data. This data is sent to a Local Gateway and a Cloud Gateway. Redundant databases are also used to  
701 store historical tag data.

702 A dashboard showing the operational and historical tag information is created and displayed using a  
703 web browser. During normal operation, users access the dashboard through the Local Gateway. If the  
704 Local Gateway is not available, the dashboard on the Cloud Gateway is used to avoid disruption.

#### 705 *2.4.3.6 Siemens*

##### 706 **TIA Portal**

##### 707 **S7-1500 CPU and CP Module**

##### 708 **SCALANCE 2C**

709 Siemens SIBERprotect technology is used to enable isolation of the Conveyor, Robot, and Supervisory  
710 systems from the Manufacturing Applications and Security Zones. Syslog alerts are configured within the  
711 Dragos and Tenable platforms based on high-risk detections and are forwarded to the Siemens Security  
712 PLC for visualization on the Security HMI. When the Security HMI displays an alert, operators can choose  
713 to either acknowledge the notification or initiate network isolation by selecting the appropriate action  
714 button. If network isolation is selected, the Siemens Security PLC sends a digital signal to the SCALANCE,  
715 which responds by segmenting the protected network from external connections, effectively acting as a  
716 firewall.

#### 717 *2.4.3.7 Rockwell Automation*

##### 718 **FactoryTalk® AssetCentre Change Management**

##### 719 **FactoryTalk® AssetCentre Disaster Recovery**

##### 720 **FactoryTalk® AssetCentre Inventory Agent**

721 FactoryTalk® AssetCentre manages asset backup and recovery for this project. It collects and manages  
722 configuration files, program backups, and other relevant data related to automation equipment. It  
723 creates logs of changes to the equipment, which are used for forensics, and can be configured to alert in  
724 a SIEM. These backup files are used to support the restoration of assets after an incident.

#### 725 *2.4.3.8 Cisco*

##### 726 **ISA3000**

##### 727 **Splunk 9.2.2**

728 Cisco contributed two technologies for this project for network segmentation and cyber incident  
729 response. The Cisco ISA 3000, a ruggedized industrial security appliance, is deployed in the NCCoE  
730 Manufacturing Lab to segment the industrial network from the DMZ. It is used to isolate the corporate  
731 network from the industrial network during cyber incidents to protect either network from the other.

732 Splunk is used as the SIEM for this project. Syslog data is configured on each of the workstations,  
733 detection platforms, and configuration software to be sent to Cisco Splunk for data aggregation and  
734 display, enabling Security Operation Center (SOC) personnel to respond to cyber incidents.

#### 735 *2.4.3.9 GreenTec*

##### 736 **ForceField 1.9**

737 GreenTec ForceField is a suite of zero-trust storage technologies for data protection and integrity by  
738 preventing unauthorized deletion, modification, or sabotage of data. Backup files for this project are  
739 stored in the ForceField immutable storage device. This storage solution ensures the integrity of backup  
740 files.

#### 741 *2.4.3.10 TDi Technologies*

##### 742 **ConsoleWorks 5.6**

743 TDi ConsoleWorks is a remote access solution that is configured to capture the actions of users remotely  
744 accessing the industrial environment. Video recordings are viewed after an incident occurs to track who  
745 logged in when and what actions they took while on the network.

#### 746 *2.4.3.11 Google Cloud (including Mandiant)*

##### 747 **Incident Response Expertise**

748 With recognized experience in dynamic cyber defense, threat intelligence, and incident response  
749 services, Mandiant participates in the NCCoE team to ensure the standards-based solutions for  
750 responding to and recovering from a cyber-attack align with their practical experience.

## 751 **2.5 Assumptions**

752 A comprehensive security architecture should be designed to detect cyber incidents prior to impact,  
753 including detection of initial access, discovery, and lateral movement. However, a thorough defense  
754 should also be prepared to restore and recover if an adversary goes undetected and operations are  
755 impacted. This guide focuses on the hopefully rare event of an adversary causing an impact. This section  
756 organizes the project assumptions into three key areas:

- 757     ▪ Attack Assumptions – defines the nature of the attacks demonstrated in this project.
- 758     ▪ Preparation Assumptions – describes prerequisite planning, organizational readiness, and  
759       framework alignment expected prior to incident response.

- 760       ▪ General Project Assumptions – describes the laboratory environment’s representativeness and  
761       assumed existing cybersecurity functions.

### 762 2.5.1 Attack Assumptions

763 The scenarios demonstrate simulated attacks. No product vulnerabilities were exploited during the  
764 execution of this project. The attack is discovered after an impact has occurred or immediately prior to  
765 the impact occurring. Assume that the simulated adversary has gained initial access, performed  
766 discovery, and moved laterally as needed to set up each scenario.

### 767 2.5.2 Preparation Assumptions

768 An incident response plan has been developed for the manufacturing organization, and that incident  
769 response plan includes a workflow similar to the one found in NISTIR 8428, *Digital Forensics and Incident*  
770 *Response (DFIR) Framework for Operational Technology (OT)* [2]. This incident response plan was  
771 developed by a team including individuals with operational expertise who know the functionality of the  
772 manufacturing factory; engineers and maintenance personnel who know the systems and networks that  
773 operate the factory; and IT personnel who know the enterprise information systems and networks. The  
774 impact analysis was done prior to a cyber incident, and the response was pre-approved by the system  
775 owner. NIST SP 800-61r3, *Incident Response Recommendations and Considerations for Cybersecurity Risk*  
776 *Management: A CSF 2.0 Community Profile* can help with developing a program to prepare for incident  
777 response [3].

778 Changes to the network and devices may occur as part of incident response. The process for emergency  
779 changes should be documented during planning, prior to incident response execution. During incident  
780 response, change management procedures are enacted, but they are not demonstrated in this  
781 publication.

782 A recovery plan was developed in alignment with the NIST CSF 2.0 and NIST SP 800-184, *Guide for*  
783 *Cybersecurity Event Recovery* [4]. This recovery plan is being referenced throughout incident response  
784 and recovery.

### 785 2.5.3 General Project Assumptions

786 The laboratory infrastructure used for this project has a relatively small number of robotic and  
787 manufacturing process nodes, which are representative of a larger manufacturing facility. The  
788 effectiveness of the example solutions is independent of the scale of the manufacturing environment.

789 This practice guide does not cover every CSF core function. In particular, the project assumes that  
790 organizations will already have an established cybersecurity program and have addressed the Govern,  
791 Identify, Detect, and Protect core functions of the CSF. While this guide does include the Detect  
792 function, the focus will be on the Respond and Recover functions.

## 793 3 Functional Demonstrations

### 794 3.1 Demonstration Methodology

795 Since effective incident response relies on procedures, communication, and analysis in addition to  
796 technical tooling, each demonstration outlines and includes the discussions, plans, procedures, and tools  
797 employed during an incident response following the workflow provided in *NISTIR 8428*. Execution details  
798 for each scenario are included in this section. Some execution details reference tools, plans, and  
799 procedures which may be found in other sections and documents. Each scenario is broken into two  
800 subsections: Response Execution and Recovery Execution.

801 The workflow found in *NISTIR 8428* has been adapted for each scenario executed in this practice guide,  
802 illustrating the path taken during scenario execution. Since each scenario follows a narrative, not every  
803 item in the workflow will be used for all demonstrations. Therefore, items in the workflow that are  
804 grayed out were not explicitly performed during scenario execution. Colored boxes represent steps that  
805 were taken during response and recovery, accompanied by an associated narrative or screenshots.

806 Mappings to standards are included in parentheses at the end of the relevant steps. Incident Response  
807 Recommendations and Considerations for Cybersecurity Risk Management, NIST Special Publication  
808 800-61r3, is referenced as *800-61*. Digital Forensics and Incident Response (DFIR) Framework for  
809 Operational Technology (OT) is referenced as *8428*.

### 810 3.2 Demonstration Use Cases

#### 811 3.2.1 Scenario A: Compromise Human Machine Interface (HMI) or Operator 812 Console

813 *Note: Scenario A in this practice guide was developed from Scenario 3 of the [project description](#).*

##### 814 3.2.1.1 Narrative

815 Background:

816 In a hypothetical factory, USB drives are used to transfer files to engineering workstations for HMI code  
817 updates.

818 Simulated Attack:

819 A malicious individual created malicious code and brought an infected USB into the factory. An  
820 authorized operator, unaware of the infection, transferred these compromised files to the engineering  
821 workstation, resulting in an HMI code update that subsequently infects the supervisory HMI and causes  
822 a loss of view event.

823 MITRE ATT&CK® References:

824 [Loss of View, Technique T0829 - ICS | MITRE ATT&CK®](#)

825 *3.2.1.2 Capabilities & Tools Demonstrated*

- 826       ▪ Incident Response Plan (8428 - Workflow)
- 827       ▪ Logging Configuration (Rockwell Automation – FactoryTalk® AssetCentre; Windows Event
- 828       Viewer)
- 829       ▪ SIEM Configuration and Utilization (Cisco – Splunk)
- 830       ▪ Network Isolation (Cisco – ISA)
- 831       ▪ Disaster Recovery and Change Management (Rockwell Automation – FactoryTalk® AssetCentre)
- 832       ▪ Backup Storage (GreenTec)
- 833       ▪ Case Management (Dragos)
- 834       ▪ Data Historian (Inductive Automation - Ignition)

835 *3.2.1.3 Targeted Devices*

- 836       ▪ Supervisory Engineering Workstation (Virtual Machine)
- 837       ▪ Supervisory HMI (Physical Machine)
- 838       ▪ MFG-Laptop1 Engineering Workstation (Physical Machine)

839 *3.2.1.4 Keywords*

- 840       ▪ USB

841 *3.2.1.5 Routine Preparation Steps*

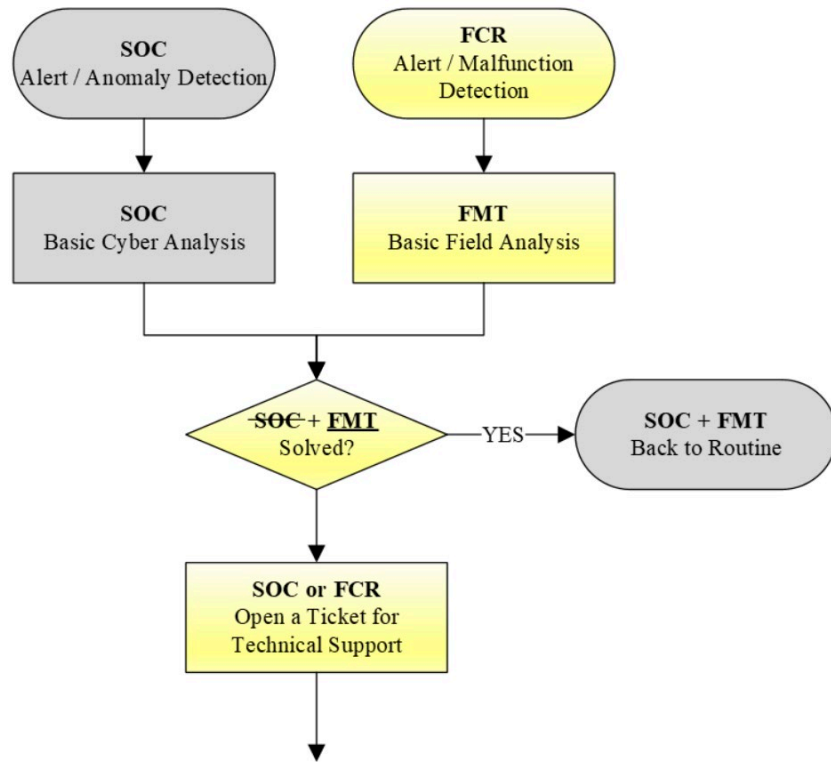
842 To enable detection, response, and recovery, the factory routinely configures and monitors logging

843 capabilities. Key preparation steps that enabled response and recovery for Scenario A are found in

844 [Scenario A: Technical Details - Preparation](#).

## 845 3.2.2 Scenario A: Response Execution

## 846 3.2.2.1 Initial Identification and Reporting



847 Figure 3-1: 8428 identification, Scenario A

848 **Alert/Malfunction Detection:** The operator observes an adversarial message on the Supervisory HMI  
849 screen while making operator rounds. (8428: B.2 FCR)

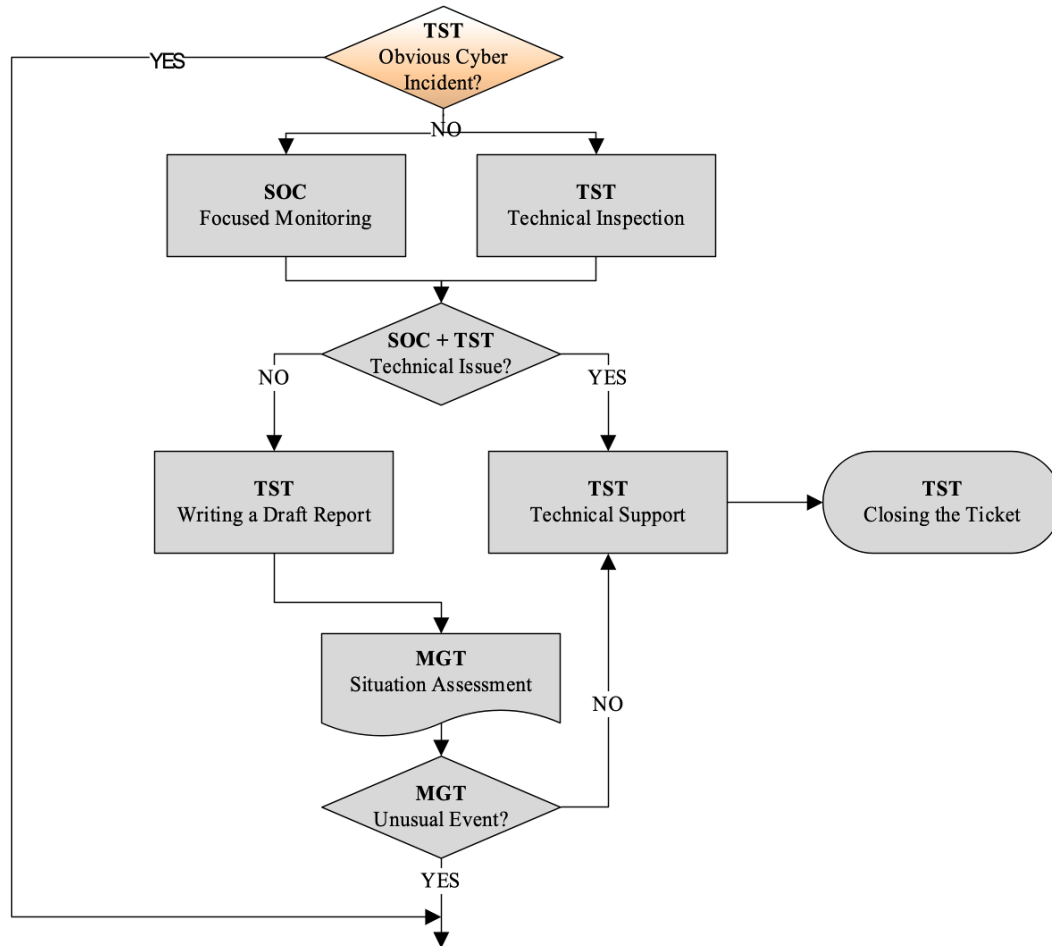
850 **Basic Field Analysis:** The adversarial message indicates a cyber problem.

851 **Operational State:** The manufacturing line can still operate automatically while the HMI screen displays  
852 malicious code. The operator can no longer start or stop the process from the Supervisory HMI.

853 **Communication:** The operator calls the cyber reporting hotline, based on their training and knowledge  
854 of the incident response plan, to report malicious code on the HMI screen. (800-61: PR.AT)

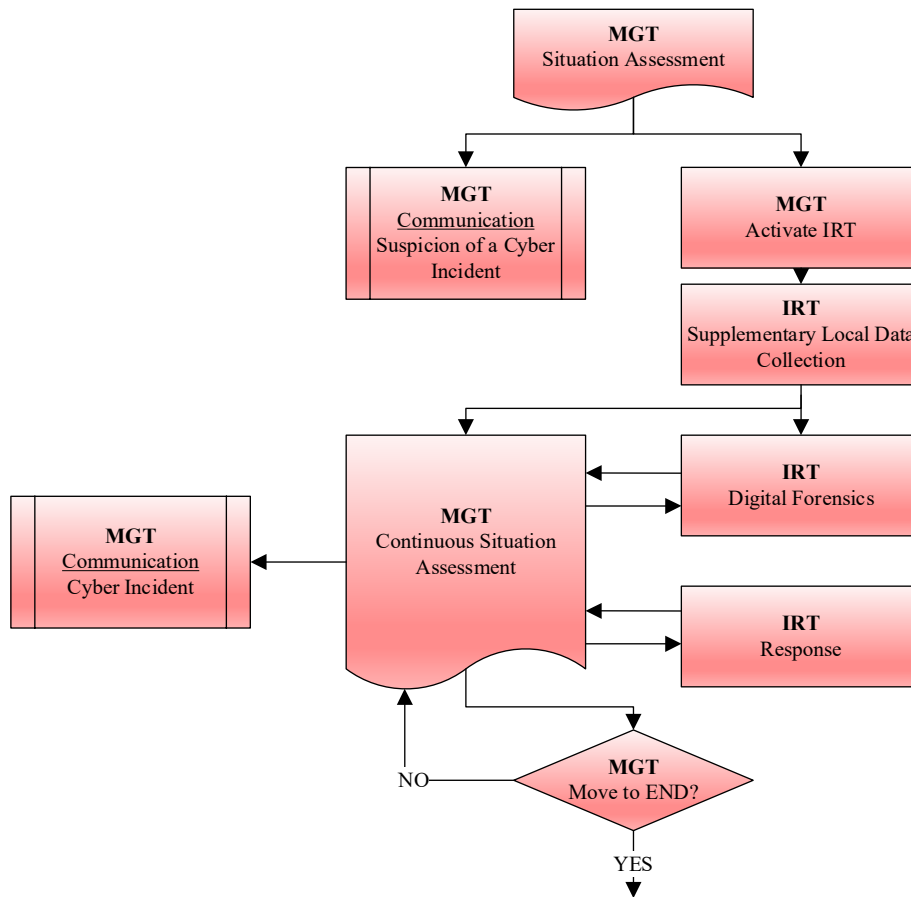
855 **Communication (Open a Ticket for Technical Support):** The SOC is made aware of the cyber incident. To  
856 facilitate the coordination to deal with the incident, the Dragos Platform is used to create a case ticket  
857 [Dragos Case Creation] and to assign the responsible personnel to take care of the incident, set the  
858 incident priority, and enter a brief description about the incident for incident recording and tracking.  
859 (8428: B.6 SOC; 800-61: DE.AE-06, R3)

860 **3.2.2.2 Technical Event Handling**



861 **Figure 3-2: 8428 event handling, Scenario A**

862 **Obvious Cyber Incident:** Since the message on the HMI screen is an obvious cyber attack, the technical  
 863 event handling section can be skipped. In this case, the technical support team (TST) immediately  
 864 gathers a situation assessment to save time and determines to move forward with the next phase, Cyber  
 865 Incident Analysis and Response. (8428: C.1 TST)

866 **3.2.2.3 Cyber Incident Analysis and Response**867 **Figure 3-3: 8428 analysis and response, Scenario A**

868 **Situation Assessment:** The engineer refers to the IRP and arranges a meeting with Engineering,  
 869 Operations, and IT management. The engineer prepares documentation, including all asset inventory  
 870 and network diagrams, to bring to the meeting. The discussion includes the following topics guided by  
 871 the IRP: (8428: D.1 MGT)

- 872 a. Incident Identification: The current situation is agreed upon as a Loss of View event. (800-61:  
 873 DE.AE-04)
- 874 b. Risk Assessment: The current situation is assessed to be of moderate severity. (800-61: DE.AE-  
 875 04, R1)
- 876 c. Operational Response: The IRP indicates that a Loss of View event with Moderate impact  
 877 authorizes the operator to shut down the affected unit for the duration of the investigation. The  
 878 Operations team discusses the event and determines that shutting down the unit is the best  
 879 course of action. (800-61: ID.IM-04)

880 **Operational State:** The operator performs a manual shutdown using a safe shutdown procedure. (800-  
 881 61: RS.MI-01, R1)

882 *Note: "Shut down" means the manufacturing process is put into a safe state (e.g., conveyor stops*  
 883 *moving) and all computing equipment remains powered. The HMI is not powered off.*

884 **Activate IRT:** Operations management decides to declare a cyber incident and activate the IRT. Using  
885 the IRP to assign roles and responsibilities, the Incident Commander is the Operations Manager, the  
886 Operations Section Chief is the IT Manager, and the Operations Section team members are the SOC  
887 Analyst, Operator, and Engineer. A Public Information Officer and Safety Officer are brought onto the  
888 team. (8428: D.2 MGT; 800-61: DE.AE-08, R1)

889 *Note: The IRP was developed using FEMA's NIMS ICS 207 form [5] to determine roles consistent with*  
890 *federal incident response guidance.*

891 **Communication:** The IRP communication plan is referenced. The team discusses wanting to disclose  
892 internally that the unit is down due to an unplanned outage and that a team is investigating the issue. A  
893 Public Information Officer is responsible for communicating directly with CISA and local law  
894 enforcement to inform them of the cyber incident. The team references their IRP for the internal email  
895 distribution list, CISA contact information, and local law enforcement. The Public Information Officer  
896 prepares an email for the Operations Manager to send to all factory employees, informing them of the  
897 incident. (8428: D.7 & D.8 MGT; 800-61: GV.OC-03, R1)

898 *Note: This guide does not cover specific communication details to concentrate on technical responses*  
899 *rather than business requirements and reporting obligations. Please be aware of and prepare to fulfill*  
900 *reporting requirements.*

901 **Response:**

902 Containment: (8428: D.6 IRT; 800-61: RS.MI-01, R1)

903 a. In accordance with IRP, the operator isolates the ICS network from the IT network by  
904 physically disconnecting the WAN Ethernet cable from the Cisco ISA firewall [[Disconnect](#)  
905 [WAN from Cisco ISA Firewall](#)].

906 *Note: During the development of the IRP, the team discusses and documents which*  
907 *incident types and severities should result in which containment actions. A risk*  
908 *assessment should be done at the time of IRP development to understand the business*  
909 *consequences of disconnecting the ICS network from the IT network.*

910 b. The engineer uses the network drawing to identify the point of disconnection. The engi-  
911 neer disconnects the workcell from the network. This involves unplugging the Supervi-  
912 sory HMI, Rockwell Automation PanelView™ Plus 7, from the network switch [[Isolation](#)  
913 [of HMI](#)].

914 **Supplemental Local Data Collection / Digital Forensics:**

915 Analysis: (8428: D.4 & D.5 IRT; 800-61: DE.AE-02, R1 & R3)

916 a. The SOC Analyst reviews Splunk data to determine if any non-standard behaviors  
917 occurred. The Splunk dashboard indicates a USB was inserted just prior to the HMI  
918 compromise. Analyst determines to investigate further [[Creating a Splunk Dashboard to](#)  
919 [detect USB Activity](#)].

920 b. The engineer checks the data historian to verify if any operational changes occurred  
921 around the time of the HMI incident [[Inductive Automation, Data Historian](#)]. No  
922 operational abnormalities found.

- 923 c. The engineer logs into the Supervisory Workstation, Rockwell ME Transfer Utility, to  
 924 determine which files have recently been sent to the HMI [[Rockwell FactoryTalk®](#)  
 925 [Transfer Utility](#)].
- 926 d. The engineer logs into Rockwell Automation’s FactoryTalk® AssetCentre and finds logs  
 927 showing which FactoryTalk® Machine Engine Runtime (.MER) configuration files were  
 928 loaded onto the HMI [[Rockwell Automation FactoryTalk® AssetCentre, Log Review](#)].

929 *Note: Analysis is possible because logs were configured prior to the incident. (8428: D.4 & D.5 IRT)*

930 **Continuous Situation Assessment:** (8428: D.7 MGT & IRT; 800-61: DE.AE-03)

- 931 Communications: Incident response team discusses findings with Incident Commander and  
 932 Safety Officer present. They conclude that a USB was inserted just prior to the incident on MFG-  
 933 Laptop1. They identify the file as NCCoE\_Monf\_Lab.mer. They determine the next steps to be:
- 934 a. Isolate machines directly involved in the attack
  - 935 b. Scan the network with updated signatures
  - 936 c. Scan the network for the malicious file

937 The Safety Officer does not foresee any safety impacts from these containment steps and  
 938 acknowledges that the IRT is OK to proceed.

939 Case Management: Based on the assessment result, the Dragos case ticket for this incident is  
 940 updated to record the investigation findings in the Justification field [[Update Dragos Case](#)]. (800-  
 941 61: DE.AE-06, R1 & R2)

942 **Response:** (8428: D.6 IRT)

943 Containment: (800-61: RS.MI-01, R1)

- 944 a. Isolate Supervisory Engineering Workstation VM [[Remove Virtual Machine from Network](#)].  
 945 Snapshots are taken to preserve evidence [[Taking Snapshots of VMs](#)].
- 946 b. Isolate MFG-Laptop1 [[Remove Physical Device from the Network](#)].
- 947 c. Explicitly deny these workstations from accessing the network using access control on the  
 948 networking devices (e.g., add MAC address to deny list on firewalls).

949 Eradication: (800-61: RS.MI-02, N1, R1, R2)

- 950 a. Scan engineering workstations with updated signatures [[Antivirus Scan](#)].
- 951 b. Scan engineering workstations for additional indicators of compromise. Since the malicious file  
 952 name is known, machines on the network are scanned for the malicious file. Some of the team  
 953 members perform manual searches for the known malicious file [[Search for Malicious File](#)] while  
 954 another team member develops a script to speed up the file search [[Script for Finding Malicious](#)  
 955 [File](#)].
- 956 c. Send Supervisory Engineering Workstation and MFG-Laptop1 to the forensic team for further  
 957 analysis.

958 **Operational State:** The unit remains shut down while the investigation is ongoing.

959 **Communication:** IRT reconvenes to discuss the current status. At this point in the process, the two  
 960 impacted machines are isolated for forensic analysis, the unit is shut down, and all other workstations

961 and servers on the network appear to be clean. The HMI hardware is disconnected from the network.  
 962 Management declares the incident response is over and directs the team to begin recovery efforts.  
 963 (8428: D.9 MGT)

964 **3.2.3 Scenario A: Recovery Execution**

**3.2.3.1 End of Cyber Incident**

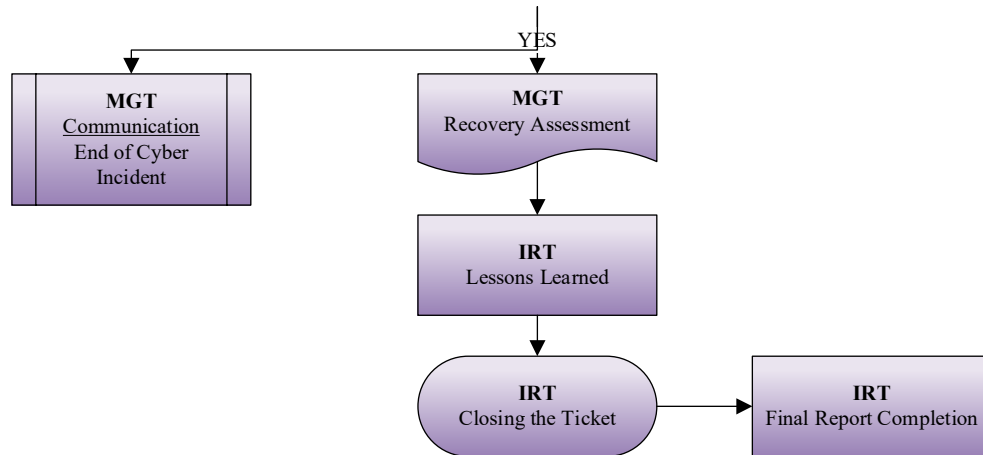


Figure 3-4: 8428 end of incident, Scenario A

965  
 966 **End of Cyber Incident:** The Incident Commander decides it is time to end the cyber incident. (8428: E.1  
 967 MGT)

968 **Recovery Assessment:** The management team determines how to return to production by gathering  
 969 Operations, Maintenance, and Engineering staff to discuss the recovery process. The team determines  
 970 that the adversary has been removed from the network based on a lack of deviations from baseline  
 971 network traffic; the only programming modifications were to the HMI, and no unexpected logons are  
 972 seen on the workstations and servers. The team determines that Operations can recover and restart  
 973 operations. While forensic analysis is ongoing, the team decides to restart operations while remaining  
 974 isolated from the Enterprise via disconnection from the Cisco ISA firewall. (8428: E.2 MGT; 800-61:  
 975 RC.CO, N1, RC.RP-01, R2)

976 **Spare Parts:** They review the spare parts list and determine that a spare PanelView™ Plus is  
 977 available. The new HMI hardware replaces the compromised HMI. (800-61: RC, N2)

978 *Note: This is a risk-based decision per facility. The facility may choose to clean the existing HMI by*  
 979 *resetting to factory default and/or removing corrupt files.*

980 **Backups:** Backups were taken of the HMI per the backup procedure, leveraging AssetCentre  
 981 [\[Backup the Rockwell PanelView™ HMI\]](#) and GreenTec [\[ForceField Zero Trust Storage\]](#)  
 982 technologies. The backup is validated using Rockwell Automation’s AssetCentre and Transfer  
 983 Utility software.

984 The HMI code is transferred using the guidance found in NIST SP 1334, *Reducing the*  
 985 *Cybersecurity Risks of Portable Storage Media in OT Environments* [6]. The HMI code is restored

986 using these backups [[Downloading Backups from Authoritative Source](#)][[Restore the HMI](#)]. (800-  
987 61: RC.RP-03)

988 **Operational State:** Maintenance staff performs standard equipment tests to begin the restart of the  
989 unit. Operators print operational procedures related to the restart. Operators restart the unit. SOC  
990 analysts, engineers, operators, and maintenance are all-hands available to observe the restart until the  
991 Incident Chief determines the return to steady state is acceptable. (800-61: RC.RP-04, R1, R2, R3)

992 **Communication:** Forensics team reports that MFG-Laptop1 and Supervisory Engineering Workstation  
993 have been reimaged and are ready for reuse. The Incident Chief directs the engineer to reconnect  
994 workstations and the operator to reconnect the firewall. (8428: D.5 IRT, E.2 MGT; 800-61: RC.RP-05, R1)

995 Recovery: The operator plugs in the firewall connection to the WAN. The engineer reconnects  
996 workstations to the ICS network, and HMI to the process control switch (800-61: RC.RP-05, R2)

997 **Communication:** Public Information Officer sends an email to the internal email distribution list to  
998 inform factory personnel that the incident has been cleared and operations may resume as normal.  
999 (8428: E.1 MGT; 800-61: RC.CO-03, R1)

1000 **Lessons Learned:** AssetCentre is integrated into Windows Event Viewer so that diagnostics uncovered  
1001 by Rockwell Automation's AssetCentre can easily be integrated into a SIEM for centralized monitoring.  
1002 This information was not integrated into the SIEM at the time of the incident, but the response would  
1003 have been faster if diagnostic monitoring existed in a centralized location. Instructions for integrating  
1004 AssetCentre event codes into Splunk are provided in [[FactoryTalk® Logs in Windows Event Viewer](#)]. It  
1005 would be beneficial to work with vendors, such as Rockwell Automation, to ensure that these tools are  
1006 being implemented in the most secure manner possible. (8428: E.3 IRT; 800-61: ID.IM-03, N3)

1007 **Communication (Closing the Ticket and Final Report Completion):** IRT combines their evidence, up-  
1008 dates the report in Dragos SiteStore, and closes the ticket for this incident [[Close Dragos Ticket](#)]. (8428:  
1009 E.4 IRT; 800-61: DE.AE-06)

### 1010 3.2.4 Scenario B: Data Exfiltration

1011 *Note: Scenario B in this practice guide was developed from Scenario 4 of the [project description](#).*

#### 1012 3.2.4.1 Narrative

1013 A malicious actor stole IT credentials through a phishing campaign. From the corporate network, the  
1014 malicious actor leveraged a misconfigured firewall to pivot into the ICS network. The actor tried the  
1015 same credentials from the IT campaign on the ICS system and was able to gain access to the ICS  
1016 network, including the data historian. The malicious actor exfiltrated a large amount of historian data to  
1017 an external server through the misconfigured firewall.

1018 ATT&CK References:

1019 [Theft of Operational Information, Technique T0882 - ICS | MITRE ATT&CK®](#)

#### 1020 3.2.4.2 Capabilities & Tools Demonstrated

1021 

- Incident Response Plan (8428 - Workflow)

- 1022       ▪ Remote Access Management (TDi Technologies - ConsoleWorks)
- 1023       ▪ Detection Configuration (Tenable – Tenable OT Security)
- 1024       ▪ Detection Configuration (Dragos – SiteStore)
- 1025       ▪ Case Management (Dragos – SiteStore)
- 1026       ▪ SIEM Configuration and Utilization (Cisco – Splunk)
- 1027       ▪ Network Isolation (Cisco – ISA3000)
- 1028       ▪ Data Historian (Inductive Automation - Ignition)
- 1029       ▪ Redundant Cloud Infrastructure (AWS – IaaS)

1030    *3.2.4.3 Targeted Devices*

- 1031       ▪ Corporate Laptop (Physical Machine)
- 1032       ▪ Management Console (Virtual Machine)
- 1033       ▪ Local Historian Database Server (Virtual Machine)

1034    *3.2.4.4 Keywords*

- 1035       ▪ Network Traffic Monitoring
- 1036       ▪ Data Exfiltration

1037    *3.2.4.5 Routine Preparation Steps*

1038    To enable detection, response, and recovery, the factory routinely configures and monitors logging  
1039    capabilities. Key preparation steps that enabled response and recovery for Scenario B are found in  
1040    [Scenario B: Technical Details - Preparation](#).

## 1041 3.2.5 Scenario B: Response Execution

## 1042 3.2.5.1 Initial Identification and Reporting

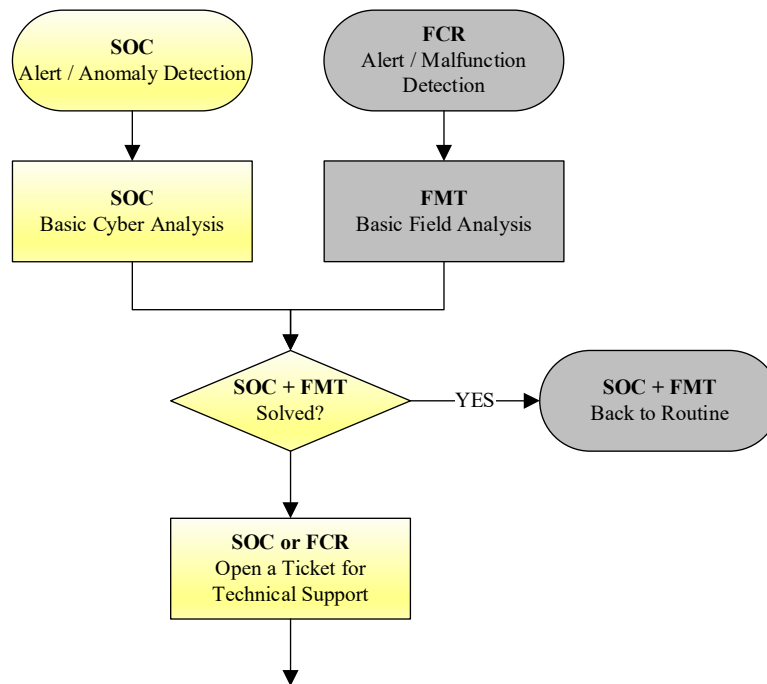


Figure 3-5: 8428 identification, Scenario B

1043 **Alert / Anomaly Detection:** The SOC identifies unauthorized PostgreSQL communication using Splunk  
 1044 [[Detection using Splunk Dashboard](#)]. (8428: B.1 SOC)

1045 **Communication:** The SOC analyst calls the operator to see if there has been any impact on operations.  
 1046 There has not been. The analyst then calls the engineer to work together on analyzing the alerts  
 1047 identified in Splunk, which are being sent from Dragos and Tenable platforms.

1048 **Basic Cyber Analysis:** The SOC analyst and engineer log into Dragos and Tenable and observe a large  
 1049 quantity of data leaving the Industrial DMZ going to an unknown IP outside of the corporate network.  
 1050 [[Analyzing Tenable Alert](#)][[Analyzing Dragos Deviation Alert](#)]. These alerts were enabled by configuring  
 1051 the Garland to duplicate SPAN information to both Tenable and Dragos [[Configuring Garland to Enable](#)  
 1052 [Multiple Detections](#)]. (8428: B.4 SOC)

1053 **Operational State:** Manufacturing has not been impacted. Operations continue as normal.

1054 **Open a Ticket for Technical Support:** To facilitate the coordination of the incident, the SOC analyst  
 1055 utilizes the Dragos Platform case management feature to open a ticket, assign responsibility, set priority,  
 1056 and enter a brief description about the incident for recording and incident tracking [[Dragos Case](#)  
 1057 [Management](#)]. (8428: B.6 SOC; 800-61: DE.AE-06, R3)

1058

## 3.2.5.2 Technical Event Handling

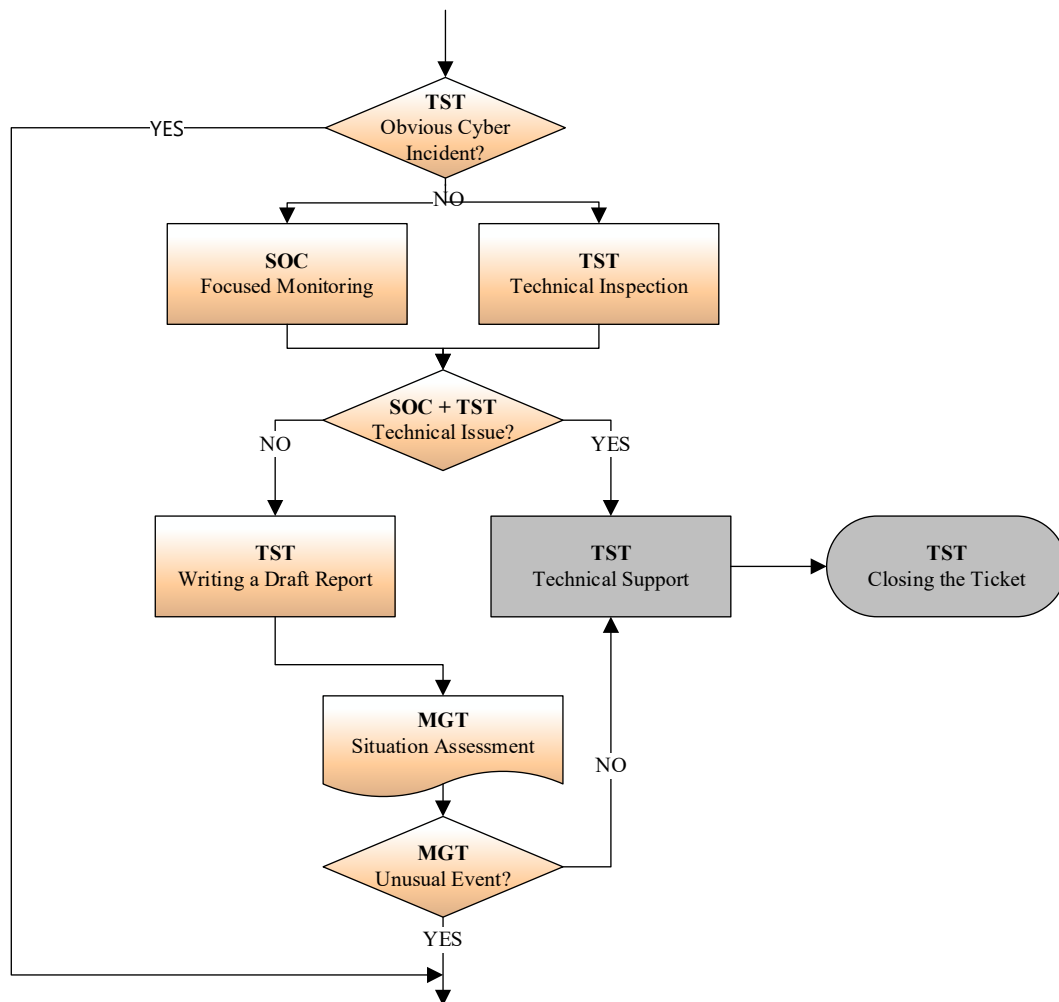


Figure 3-6: 8428 event handling, Scenario B

1059 **Obvious Cyber Incident:** This is not an obvious cyber incident.

1060 **Focused Monitoring / Technical Inspection:** No additional alerts are generated during this time. The  
1061 data historian seems to be functional.

1062 **Technical Issue?:** It does not appear to be a technical malfunction.

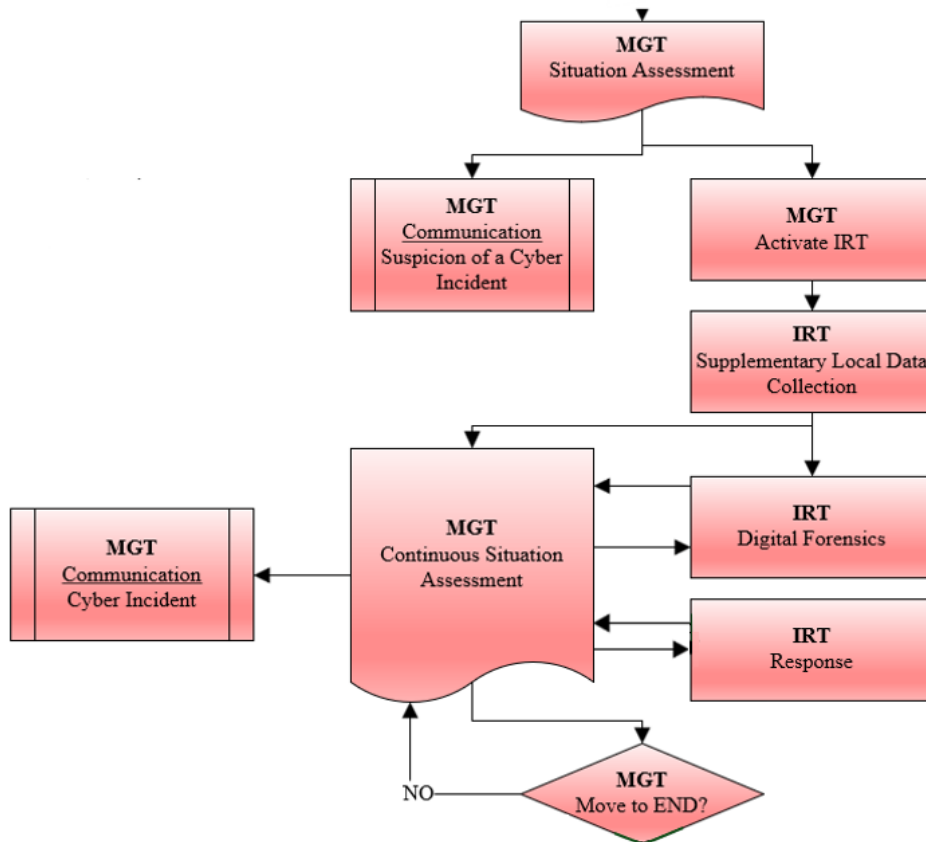
1063 **Writing a Draft Report:** The engineer sets a meeting on the calendar for the operations manager, SOC  
1064 analyst, and engineer to discuss the alert.

1065 **Situation Assessment:** The team meets to discuss current findings. The manager suggests contacting  
1066 anyone with admin access to the database to question if they made any changes to the database  
1067 recently, or had a need for exporting historian information outside of the ICS network. The team is not  
1068 ready to declare a cyber incident, as normal business tasks could have caused these alerts.

1069 **Communication:** The engineer contacts each of the database administrators to discuss their recent  
 1070 database activities. None are aware of this unusual network traffic.

1071 **Unusual Event?:** Management receives feedback that there's no known business reason for the export  
 1072 of data. This is an unusual event that requires further investigation.

### 1073 3.2.5.3 Cyber Incident Analysis and Response



1074 **Figure 3-7: 8428 analysis and response, Scenario B**

#### 1075 **Situation Assessment:**

1076 The engineer refers to the IRP and prepares essential documentation, including asset inventory and  
 1077 network drawings. A meeting is arranged for Engineering, Operations, and IT management. The  
 1078 discussion includes the following topics guided by the IRP: (8428: D.1 MGT)

- 1079 a. **Incident Identification:** The situation is considered a data exfiltration event, known as Theft of  
 1080 Operational Information. (800-61: R.DS-01)
- 1081 b. **Risk Assessment:** The current situation is assessed to be of low severity, since there is no  
 1082 operational impact. There could be a financial impact depending on the adversarial use of that  
 1083 information. More details need to be gathered to determine the scope of impact. (800-61:  
 1084 DE.AE-04, R1)

1085 c. Operational Response: IRT determines to isolate the IT and ICS networks. Operations  
 1086 management determines to continue with manufacturing operations while maintaining  
 1087 communications with the IRT. (800-61: ID.IM-04)

1088 **Activate IRT**: Operations management declares a cyber incident and activates the IRT. The IRP was  
 1089 developed using NIMS ICS 207 [5] to determine roles consistent with federal incident response  
 1090 guidance. Incident response roles and responsibilities are assigned to individuals or teams based on the  
 1091 IRP. In this incident, the Incident Commander is the Operations manager, the Operations Section Chief is  
 1092 the IT manager, and the Operations Section team members were the SOC analyst, operator, and  
 1093 engineer. A Public Information Officer is brought onto the team for managing communications, and a  
 1094 Safety Officer is designated to remain vigilant of any potential impacts to safety. (8428: D.2 MGT; 800-  
 1095 61: DE.AE-08, R1)

1096  
 1097 **Communication**: A Public Information Officer is responsible for communicating directly with CISA and  
 1098 local law enforcement to inform them of the cyber incident. The team referenced their IRP for internal  
 1099 email distribution list, CISA contact information, and local law enforcement. (8428: D.3, D.7 & D.8 MGT;  
 1100 800-61: GV.OC-03, R1)

1101 *Note: Many details of communication are not listed in this guide to focus on technical response rather*  
 1102 *than reporting requirements. Please be aware of and prepare to meet reporting requirements.*

1103 **Response:**

1104 Containment: (8428: D.6 IRT; 800-61: RS.MI-01, R1)

- 1105 a. The engineer logs into Cisco ISA3000 to create rules to allow AWS outbound and rules to  
 1106 deny all other unnecessary outbound traffic [[Isolate ICS DMZ using ISA3000](#)].
- 1107 b. The engineer disconnects the JumpHost VM from the network [[Disconnect JumpHost](#)  
 1108 [VM from Network](#)] and takes a snapshot for forensic analysis [[Take Snapshot of](#)  
 1109 [JumpHost VM](#)].
- 1110 c. The engineer disconnects the local database and local historian servers from the net-  
 1111 work [[Isolate Local Database and Historian Gateway](#)].
- 1112 i. Take a snapshot of both servers for forensic analysis.
- 1113 ii. The historian administrator validates that the cloud instance of the historian is  
 1114 still operational [[Validate Redundant AWS Cloud Historian](#)].
- 1115 iii. Communication: The historian administrator emails their operations and engi-  
 1116 neering colleagues, notifying them of the outage.

1117 **Operational State**: Manufacturing process remains operational. The AWS instance of the data historian  
 1118 is still functional.

1119 **Supplemental Local Data Collection / Digital Forensics:**

1120 Analysis: (8428: D.4 & D.5 IRT; 800-61: DE.AE-02, R1 & R3) The IRT collected and reviewed  
1121 access logs, system logs, network traffic logs, firewall logs, and any indicators of compromise to  
1122 determine the extent of the attack. The reviews on the log and alert data from Splunk, Tenable,  
1123 and Dragos indicate non-standard behaviors occurred.

- 1124 a. Splunk dashboard indicates multiple baseline notifications showing unauthorized  
1125 PostgreSQL protocol being used between the Historian database and the workstation  
1126 utilized to exfiltrate the data.
- 1127 b. Dragos detects and records a baseline alert for an unauthorized database connection.  
1128 On the Dragos notification, Dragos shows a large quantity of data transferring from the  
1129 local historian database to the JumpHostVM [[Detecting Large Data Transfer in Dragos](#)].
- 1130 c. Tenable receives a baseline violation alert for an unauthorized use of the PostgreSQL  
1131 protocol between a JumpHostVM and a data historian database, indicating a  
1132 conversation using the unauthorized protocol [[Detecting Policy Deviation in Tenable](#)].
- 1133 d. The two sources confirm suspicious activity at the same time. In order to understand  
1134 more details of the event, Tenable's Network Packet Captures feature is used to read  
1135 the packets associated with the event. PCAP is opened using a network analysis tool to  
1136 parse the details of the packet. Within those packet details, the jsmith account is  
1137 identified [[Browsing Packet Captures From Tenable](#)].

1138 **Continuous Situation Assessment:** (8428: D.7 MGT & IRT; 800-61: DE.AE-03)

1139 Communication: Incident response team discusses the findings. They conclude that the jsmith  
1140 account was used for the attack. They want to investigate further and assign tasks to be  
1141 performed in parallel.

- 1142 a. Review logs in ConsoleWorks to understand the extent of the attack.
- 1143 b. Disable and/or delete the jsmith account to prevent further attacks.
- 1144 c. Speak with the owner of the jsmith account to understand if these actions were inten-  
1145 tional, accidental, or an incident of stolen credentials.

1146 Case Management: Based on the initial analysis, the Dragos case ticket for this incident is  
1147 updated to record the investigation findings in the Justification field [[Dragos Case Management](#)].  
1148 (800-61: DE.AE-06, R1 & R2)

1149 **Operational State:** Unit remains operational while the investigation is ongoing.

1150 **Digital Forensics:**

- 1151 a. Because the jsmith user account was identified using Tenable, the IRT now logs into  
1152 TDI's ConsoleWorks to view recordings of user activity associated with that account. The  
1153 session recordings indicate database login and data exfiltration [[Reviewing Console-  
1154 Works User Session](#)].

- 1155           b. IRT investigates the extent of compromise. IRT views other logins to the database ma-  
 1156           chine. It appears that only jsmith’s account was involved in the incident. The jsmith ac-  
 1157           count only logged into the local historian database and the JumpHostVM. There is no  
 1158           indication of additional accesses from that account within the past three weeks. It ap-  
 1159           pears that only the Historian has been impacted, with the historian data being trans-  
 1160           ferred to an external device.
- 1161           c. The system administrator disables the jsmith account from the Active Directory [[Disable](#)  
 1162           [Compromised Accounts](#)].
- 1163           d. Communications: The operations manager calls the owner of the jsmith account again.  
 1164           The manager discloses that the IRT knows the jsmith account was used in the incident. J  
 1165           Smith is able to prove to the operations manager that they have not logged into the da-  
 1166           tabase for a long time. They only logged into the database to configure it many months  
 1167           ago and have not logged in since. The manager and employee discussed possible scenar-  
 1168           ios and discover that J Smith uses the same credentials for their IT login as they do with  
 1169           their ICS login. They also have unnecessary access to administrative accounts when they  
 1170           should only have engineering access for most situations.

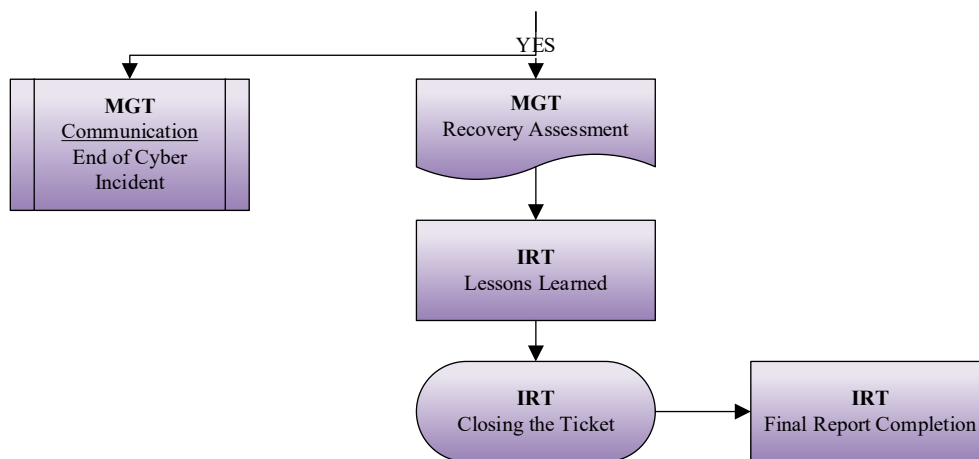
1171 *Note: Technical analysis is possible because appropriate logs were configured prior to the incident.*

1172 **Continuous Situation Assessment:** IRT discusses the findings. They conclude that the adversary  
 1173 leveraged stolen credentials. IRT believes they’ve captured all the necessary forensic data and that the  
 1174 adversary has been eradicated. (8428: D.7 MGT & IRT; 800-61: DE.AE-03)

1175 **Move to End?:** Operations Manager decides to move to recovery.

### 1176 3.2.6 Scenario B: Recovery Execution

#### 1177 3.2.6.1 End of Cyber Incident



1178 **Figure 3-8: 8428 end of incident, Scenario B**

1179 **End of Cyber Incident:** The Incident Commander decides it is time to end the cyber incident. (8428: E.1  
 1180 MGT)

1181 **Communication: The** Public Information Officer works with local law enforcement to understand the  
1182 impact of the stolen data.

1183 *Note: Further communication occurs but is outside of the scope of this document.*

1184 **Recovery Assessment:** Since there is no interruption on the production operation during this incident,  
1185 there is only a minimal recovery needed.

1186 Recovery:

1187 a) Create a new jsmith\_2 account in Active Directory and ConsoleWorks.

1188 b) Create a new VM for local historian database. Recreate the database configuration  
1189 from the backup using the new account and password.

1190 c) Verify local historian is getting live data.

1191 d) Update firewalls to re-enable remote access, and to block all PostgreSQL traffic from  
1192 leaving the ICS network.

1193 **Operational State:** Manufacturing operations are not impacted and are continuously running.

1194 **Lessons Learned:** The IRT reconvened to discuss what could have been done better to improve  
1195 response, recovery, detection, and protection to prevent the incident from recurring and respond more  
1196 efficiently in the future. They determined the following as follow-up actions:

1197 a) Enable MFA for remote access in ConsoleWorks.

1198 b) Regularly communicate between IT and ICS network administrators to ensure the two firewalls  
1199 of the DMZ work together to block unnecessary traffic.

1200 c) Train employees to use different passwords on different accounts, and implement strong pass-  
1201 word practices to prevent compromise of multiple accounts if one is breached.

1202 **Communication (Closing the Ticket and Final Report Completion):** Update the ticket within Dragos, and  
1203 close out the investigation.

### 1204 3.2.7 Scenario C: Unauthorized Command Message

1205 *Note: Scenario C in this practice guide was developed from Scenario 2 of the [project description](#).*

#### 1206 3.2.7.1 Narrative

1207 Background:

1208 A hypothetical factory is fully staffed from 9 pm–5 am, operating as a “lights-out” facility between 5 am–  
1209 9 pm. There are three products currently being made in this hypothetical factory, which an operator  
1210 selects from the Conveyor HMI. These are Widget A (black-black cube), Widget B (black-white cube), and  
1211 Widget C (black-aluminum cube). The operator intends to produce additional Widget As during lights-  
1212 out operation, so they preload the feeder with Widget A components and select Widget A using the  
1213 Conveyor HMI.

1214 The engineering workstation is also capable of modifying the Conveyor PLC's parameters; however, the  
1215 engineering workstation is not typically used for this purpose. The engineering workstation maintains a  
1216 persistent connection and access to the ICS network for troubleshooting and occasional logic changes to  
1217 the PLC and HMI.

1218 Simulated Attack:

1219 A malicious actor leveraged stolen credentials to access the engineering workstation. From the  
1220 engineering workstation, the adversary modified the parameters of the Conveyor PLC to make Widget B  
1221 or Widget C each day while the factory is not staffed. This caused an interruption to production since the  
1222 feeder was preloaded with Widget A components. When the malicious actor selected Widget B, the  
1223 Widget A components were rejected, causing a mess on the factory floor and a loss of production. There  
1224 is no modification of the program file because the malicious actor was living off the land to modify these  
1225 parameters. The actor used existing software installed on the engineering workstation to log into the  
1226 PLC and manipulate the value of the Widget selection parameter, which is a valid value within the PLC's  
1227 program. No modification of the PLC programming logic was necessary to create this attack.

1228 ATT&CK References:

1229 [Remote Services, Technique T0886 - ICS | MITRE ATT&CK®](#)

1230 [Unauthorized Message: Command Message, Sub-technique T1692.001 | MITRE ATT&CK®](#)

1231 [Manipulation of Control, Technique T0831 - ICS | MITRE ATT&CK®](#)

### 1232 *3.2.7.2 Capabilities & Tools Demonstrated*

- 1233     ▪ Incident Response Plan (8428 - Workflow)
- 1234     ▪ Detection Configuration (Tenable – Tenable OT Security)
- 1235     ▪ SIEM (Cisco - Splunk)
- 1236     ▪ Network Isolation (Siemens - SIBERprotect)
- 1237     ▪ Analysis (Siemens – TIA Portal)
- 1238     ▪ Data Historian (Inductive Automation - Ignition)
- 1239     ▪ Backup Management (Rockwell Automation – FactoryTalk® AssetCentre)
- 1240     ▪ Backup Storage (GreenTec - ForceField)
- 1241     ▪ Case Management (Dragos - SiteStore)
- 1242     ▪ Remote Access Monitoring (TDi Technologies – ConsoleWorks)

### 1243 *3.2.7.3 Targeted Devices*

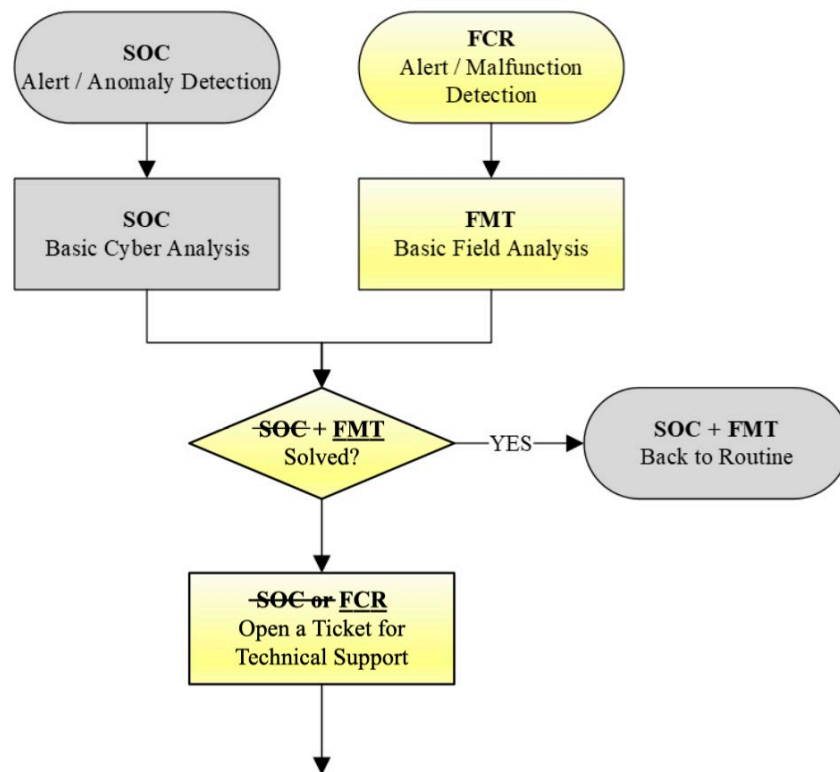
- 1244     ▪ Engineering Workstation (Physical Machine)
- 1245     ▪ Conveyor System (PLC)
- 1246     ▪ Remote access server (Virtual Machine)

1247 **3.2.7.4 Keywords**

- 1248     ▪ Unauthorized command message
- 1249     ▪ PLC
- 1250     ▪ Manipulation of control

1251 **3.2.7.5 Routine Preparation Steps**

1252 To enable detection, response, and recovery, the factory routinely configures and monitors logging  
 1253 capabilities. Key preparation steps that enabled response and recovery for Scenario C are found in  
 1254 [Scenario C: Technical Details – Preparation](#).

1255 **3.2.8 Scenario C: Response Execution**1256 **3.2.8.1 Initial Identification and Reporting**1257 **Figure 3-9: 8428 DFIR Identification, Scenario C**

1258 **Alert/Malfunction Detection:** The operator arrives at the factory and observes a pile of components on  
 1259 the floor. Only a few Widget As were produced during lights-out operation. (8428: B.2 FCR)

1260 **Basic Field Analysis:** The operator cleans the mess and checks the Conveyor HMI. The Conveyor HMI  
 1261 indicates Widget B is selected for production, even though the operator prepared Widget A components  
 1262 as feed into the Conveyor the previous day, and the operator thought they selected Widget A on the  
 1263 HMI the previous day.

1264 **Operational State:** The operator resets the feedstock to the Conveyor and selects Widget A on the HMI.  
1265 Operator restarts operation.

1266 **Communication:** The operator reports to management that a mistake was made, and production was  
1267 lost the day before. The operator begins discussing with colleagues whether anyone had touched the  
1268 HMI.

1269 *Next day*

1270 **Alert/Malfunction Detection:** The operator arrives at the factory and observes a pile of components on  
1271 the floor. Only a few Widget As were produced during lights-out operation. (8428: B.2 FCR)

1272 **Basic Field Analysis:** The operator cleans the mess and checks the Conveyor HMI. The Conveyor HMI  
1273 indicates Widget B is selected for production, even though the operator prepared Widget A components  
1274 as feed into the Conveyor the previous day, and the operator thought they selected Widget A on the  
1275 HMI the previous day.

1276 **Operational State:** The operator resets the feedstock to the Conveyor and selects Widget A on the HMI.  
1277 The operator restarts the operation.

1278 **Communication:** The operator reports a repeat incident to management. The operator contacts physical  
1279 security to review camera footage.

1280 **Basic Field Analysis:** The camera footage indicates the operator stood at the Conveyor HMI at 4:45 am,  
1281 touching the screen. Camera footage does not indicate any additional manipulation of the HMI.

1282 **Communication:** The operator is (falsely) written up for making repeated mistakes that lead to loss of  
1283 production.

1284 *Next day*

1285 **Alert/Malfunction Detection:** A different operator arrives at the factory and observes a pile of  
1286 components on the floor. Only a few Widget As were produced during lights-out operation. (8428: B.2  
1287 FCR)

1288 **Basic Field Analysis:** The operator cleans the mess and checks the Conveyor HMI. The Conveyor HMI  
1289 indicates Widget C is selected for production, even though the operator prepared Widget A components  
1290 as feed into the Conveyor the previous day, and the operator thought they selected Widget A on the  
1291 HMI the previous day.

1292 **Operational State:** The operator resets the feedstock to the Conveyor and selects Widget A on the HMI.  
1293 The operator restarts the operation.

1294 **Communication:** The operator reports a repeat incident to management. Incident is treated as a  
1295 reliability problem.

1296 **Basic Field Analysis:** The engineer logs into the Siemens TIA Portal to review logic. The engineer  
1297 determines that the parameter can only be changed from the engineering workstation or the HMI. The  
1298 engineer adds an indication of Widget selection to the data historian [[View Tags in Data Historian](#)].

1299 The engineer sees that the PRG\_LCH tag has been modified during the off-shift over the past few days.

1300 *Next day*

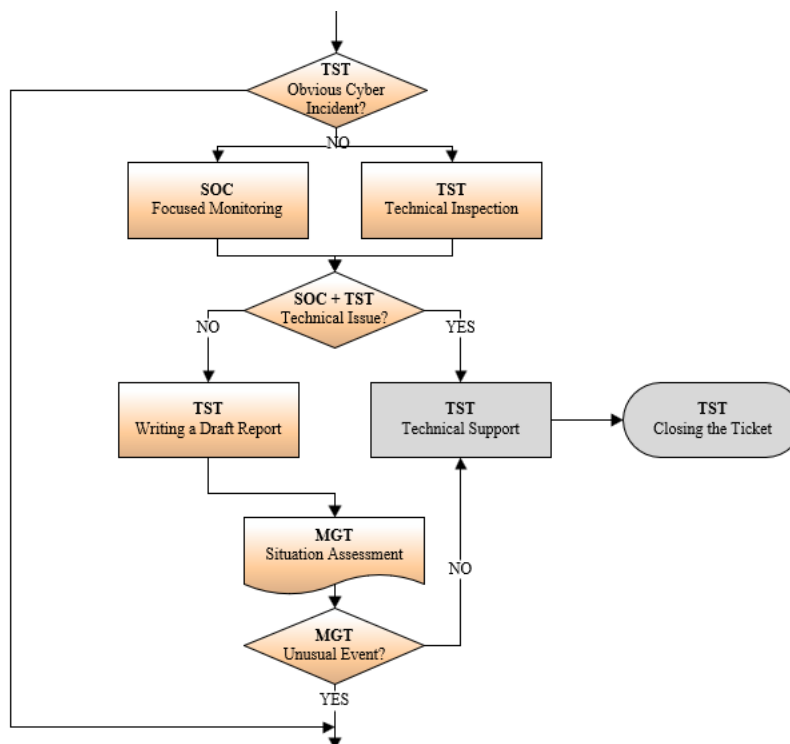
1301 **Alert/Malfunction Detection:** The original operator arrives at the factory and observes a pile of  
 1302 components on the floor. Only a few Widget As were produced during lights-out operation. (8428: B.2  
 1303 FCR)

1304 **Communication:** The engineer calls SOC to review for alerts.

1305 **Alert / Anomaly Detection:** Nothing obviously suspicious is found in the Splunk alerts.

1306 **Communication (Open a Ticket for Technical Support):** The SOC opens a ticket within Dragos [[Managing](#)  
 1307 [Dragos Tickets](#)].

1308 **3.2.8.2 Technical Event Handling**



1309 **Figure 3-10: 8428 Event Handling, Scenario C**

1310 **Obvious Cyber Incident:** No. The cause of this incident has not yet been determined.

1311 **Focused Monitoring:** The engineer creates a new alert in Tenable to be sent to the Siemens  
 1312 SIBERprotect and Security HMI to detect any connection to the Conveyor PLC [[Creating Siemens Traffic](#)  
 1313 [Detection Policy in Tenable](#)]. This alert identifies any unauthorized communication going to the Siemens  
 1314 Conveyor PLC, and it enables isolation through the SIBERprotect Security HMI.

1315 The SOC analyst creates a dashboard to monitor any unexpected Siemens network traffic based on the  
 1316 configured Tenable alerts. This enables both operations and cybersecurity personnel to monitor the  
 1317 situation [[Creating a Splunk dashboard for unauthorized Siemens traffic](#)].

1318 **Communication:** Management determines that an engineer and an operator will work through the  
 1319 lights-out off-shift to detect the cause of the problem.

1320 *Next day*

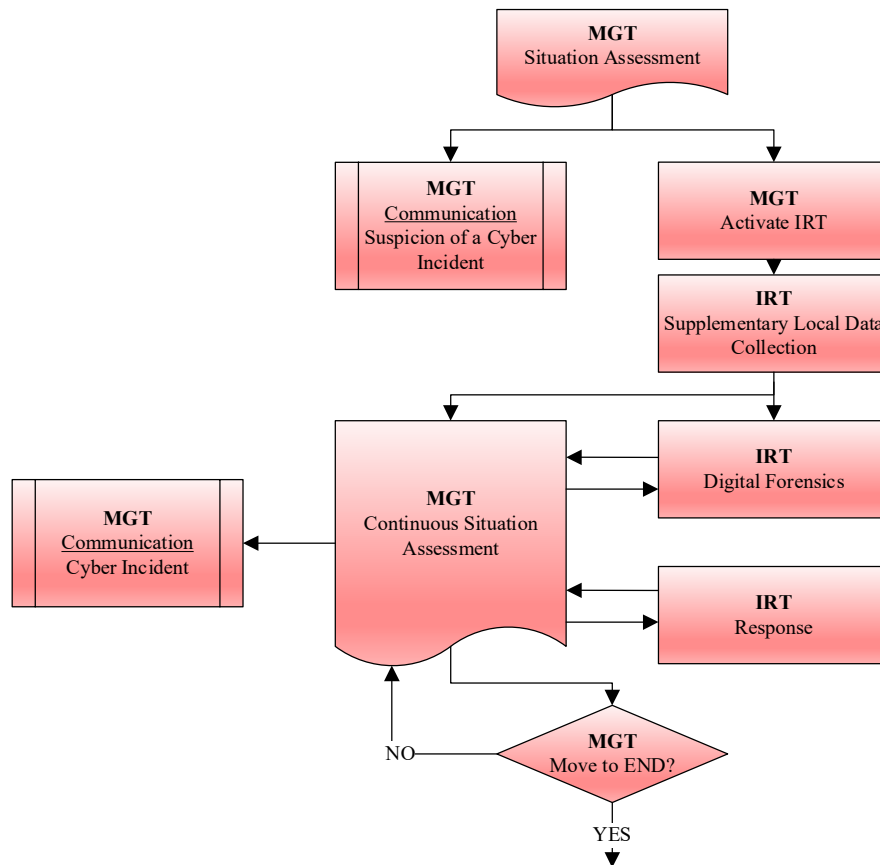
1321 **Alert/Malfunction Detection:** The Security HMI triggers an alarm indicating that something is  
 1322 connecting to the Conveyor PLC.

1323 **Response:** The operator acknowledges the alarm and isolates the Conveyor, Robot, and Supervisory  
 1324 systems from the rest of the ICS network [[Isolate ICS Network using SIBERprotect](#)].

1325 **Operational Status:** Manufacturing operations can continue through local access to Conveyor, Robot,  
 1326 and Supervisory HMIs.

1327 **Writing a Draft Report:** The SOC updates the ticket with information about the isolation actions taken  
 1328 through SIBERprotect [[Managing Dragos Tickets](#)].

1329 **3.2.8.3 Cyber Incident Analysis and Response**



1330 **Figure 3-11: 8428 Analysis and Response, Scenario C**

1331 **Situation Assessment / Activate IRT:** Management meets with the operator, engineer, and SOC analyst  
 1332 to discuss the situation. Management determines that this is a cyber incident. Management calls the IRT  
 1333 to take action.

1334 **Situation Assessment:** The engineer refers to the Incident Response Plan (IRP) and prepares essential  
1335 documentation, including asset inventory and network drawing. A meeting is arranged for Engineering,  
1336 Operations, and IT management. The discussion includes the following topics guided by the IRP: (8428:  
1337 D.1 MGT)

1338 Incident Identification: The current situation is considered a Manipulation of Control. (800-61: DE.AE-04)

1339 Risk Assessment: The current situation is assessed to be of Moderate severity. (800-61: DE.AE-04, R1)

1340 Operational Response: The incident response plan indicates that a Manipulation of Control event with  
1341 Moderate impact means that the Operator is authorized to shut down the affected unit for the duration  
1342 of the investigation. The Operations team discusses the event and determines that a unit shutdown is  
1343 not necessary. They continue to operate locally while isolated from the Manufacturing Application Zone,  
1344 Security Zone, and Enterprise networks. (800-61: ID.IM-04)

1345 **Operational State:** Manufacturing operations continue using local HMIs.

1346 **Supplemental Local Data Collection:** The engineer logs into Siemens TIA Portal to troubleshoot soon  
1347 after the Conveyor parameters were modified. Engineer discovers an error message indicating the  
1348 account jsmith was recently logged into TIA Portal and did not shut down properly [[TIA Portal](#)  
1349 [Diagnostics](#)].

1350 The engineer opens the Task Manager to see who is logged into MFG-Laptop1. The Task Manager  
1351 indicates that the jsmith user is in a disconnected state, but is still showing the session is available in  
1352 Task Manager [[Windows Task Manager](#)].

1353 **Digital Forensics:** The engineer works with IT management to hand over the physical laptop for  
1354 additional forensics.

1355 **Continuous Situation Assessment:** The team discusses the new findings. The jsmith account was logged  
1356 into the Engineering Workstation during an off-shift at the time of the Widget change. Jsmith is a  
1357 legitimate employee account, but the account owner was not assigned to work in the off-shift during  
1358 this investigation. The team determines that more data should be gathered.

1359 **Digital Forensics:** SOC analyst opens TDi Technologies' ConsoleWorks to review jsmith's session. The  
1360 SOC analyst reviews historical footage while also analyzing the data historian. Modifications of the  
1361 Conveyor PLC parameters found in the jsmith sessions align with the data historian indications of  
1362 parameter modification [[Review ConsoleWorks Sessions for User Activity](#)].

1363 **Continuous Situation Assessment:** The IRT determines to take action to disable the jsmith account and  
1364 to meet with the account owner at the beginning of the next shift to perform an investigative interview.

1365 **Response:** (8428: D.6 IRT)

1366 Analysis: The account owner of jsmith either maliciously modified production or their account was  
1367 compromised. The interview will determine account usage.

1368 Containment: (800-61: RS.MI-01, R1)

1369 Disable the jsmith account from Active Directory.

1370 Change the password of the jsmith account in ConsoleWorks.

1371 [Refer to Scenario B screenshots, [Disable Compromised Accounts](#)]

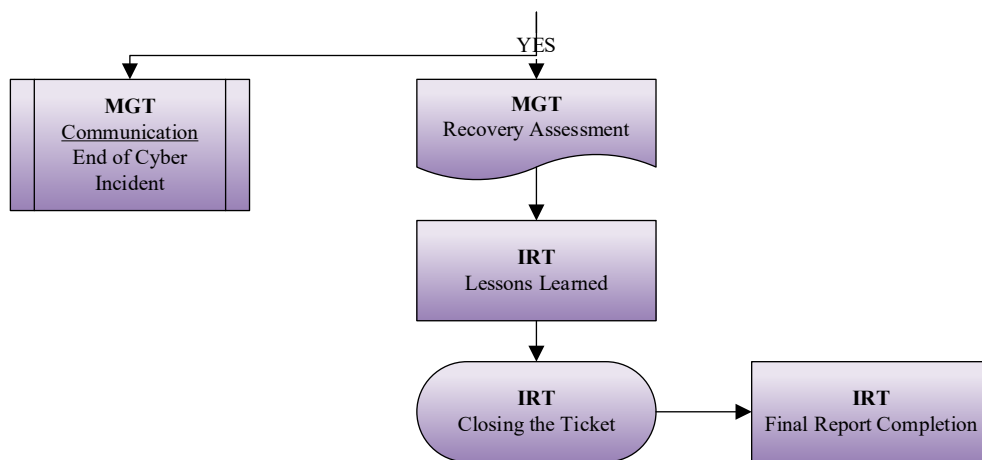
1372 **Communication:** Management met with the account owner of jsmith. They denied logging in during the  
 1373 off-shift. Management believes the account owner and determines that the jsmith account will need to  
 1374 be re-enabled with additional security measures after the investigation concludes.

1375 **Communication: Case Management:** The Dragos ticket is updated with the latest findings from the  
 1376 investigation [[Managing Dragos Tickets](#)].

1377 **Continuous Situation Assessment:** The team discusses that they believe the adversary is now out of the  
 1378 system. The team believes that initial access was caused by the account owner of jsmith using the same  
 1379 password on work systems as his personal email account. The employee later confirms that they were  
 1380 previously notified about their personal email account being compromised.

### 1381 3.2.9 Scenario C: Recovery Execution

#### 1382 3.2.9.1 End of Cyber Incident



1383 **Figure 3-12: 8428 End of Incident, Scenario C**

1384 **End of Cyber Incident:** The Incident Commander decides it is time to end the cyber incident. (8428: E.1  
 1385 MGT)

1386 **Recovery Assessment:** The team still needs to verify that the program on the Conveyor was not  
 1387 modified, but the laptop with the Siemens TIA Portal software installed is now in the hands of the  
 1388 forensics team. The engineer works with Siemens to transfer the license to a new engineering  
 1389 workstation [[TIA Portal Reinstall](#)] so that operational recovery can continue while the forensics team is  
 1390 doing their analysis.

1391 **Recovery:** The team identifies recovery actions that need to be taken. Some of these can be done while  
 1392 manufacturing is ongoing, and some of them require a manufacturing outage.

1393 Reinstall engineering software on the newly commissioned engineering workstation. Verify with the  
1394 vendor to ensure compatibility between the operating system and the engineering software. Use  
1395 Automation License Manager to transfer the license.

1396 Perform a factory reset on the PLC.

1397 Reinstall the PLC program from the known-good file saved in ForceField. [[Download PLC Backup](#)  
1398 [Program File from ForceField](#)]

1399 Validate the checksum between the current and previous versions of the PLC code to ensure the  
1400 authenticity of the code.

1401 User Security HMI to reset SCALANCE firewall. This re-enables communication between the Robot,  
1402 Conveyor, and Supervisory systems and the rest of the ICS network.

1403 **Operational State:** Operations and engineering work together to determine an optimal time for a ~4-  
1404 hour outage to replace and validate the PLC code. Operations return to normal with one staffed shift  
1405 and one lights-out shift.

1406 **Lessons Learned:** While the recovery team is preparing for the operational outage, the IRT reconvenes  
1407 to discuss what could have been done better to improve response, recovery, detection, and protection  
1408 to prevent the incident from recurring and respond more efficiently in the future. They determined the  
1409 following as follow-up actions:

1410 Enable MFA for remote access on ConsoleWorks

1411 Add a password for connecting to the Conveyor PLC from the engineering workstation using the Siemens  
1412 TIA Portal [[Add Password and Restore from Backup with TIA Portal](#)].

1413 The incident was not caught until after the impact was achieved. The team believes that more focused  
1414 monitoring, including behavioral analysis, would help to detect this event faster in the future. An  
1415 additional IT network engineer and SOC analyst are asked to work with the factory engineer to develop a  
1416 more robust monitoring plan.

1417 **Operational State:** The Operations Manager schedules a maintenance window for tomorrow at noon for  
1418 the engineering and maintenance team to add MFA to ConsoleWorks, add a password to the Conveyor  
1419 PLC, reload the Conveyor program, test that the code is functional, and work on maintenance tasks that  
1420 cannot otherwise be performed during normal operations.

1421 **Communication (Closing the Ticket and Final Report Completion):** Update the ticket within Dragos to  
1422 close out the incident.

## 1423 **4 General Findings**

1424 The Lessons Learned from the Scenarios emphasize the importance of coordination across all the  
1425 components involved in response and recovery. Several specific findings to highlight include:

### 1426 **1. Preparation and planning are critical for the successful implementation of response and recovery.**

1427 The scenarios demonstrate that establishing a predetermined and structured approach to assess  
1428 potential threats to operations was key to ensuring timely and optimal decision-making. Another area of

1429 preparation is taking preventative measures by addressing common threat vectors, such as credential  
1430 reuse and sharing.

1431 **2. Logging and monitoring enable rapid assessment and resolution.** Tuning the tools and configurations  
1432 for your environment to collect and confirm trends and findings increases the ability to identify issues  
1433 and provide next steps with higher degrees of confidence. The lessons learned also confirmed that  
1434 response time can be faster when diagnostic tools native to OT equipment is integrated into an  
1435 organization's overall security information and event management system.

1436 **3. Enabling backups with secure storage will avoid manipulation.** The provision of immutable storage  
1437 to prevent unauthorized alteration of backups ensures that information (such as logging data) gathered  
1438 will not be subject to modification.

1439 **4. Establishing operational context allows for effective decision-making during a response.** Evaluation  
1440 and input from all team members is critical in understanding and reacting to cyber incidents. These  
1441 should include inputs from production and operational teams to ensure safety is maintained and  
1442 disruptions to manufacturing activities are limited.

1443 **5. Improving monitoring methods can improve detection** and should include parameters beyond  
1444 traditional data logging to correlate information from other inputs, such as behavioral analysis. This will  
1445 reduce the time necessary to detect anomalous behavior, conduct investigations, and improve the  
1446 overall resilience of the ICS environment.

1447 Throughout the three Scenarios, overall capabilities that generally stood out as supporting successful  
1448 implementation activities included logging and monitoring, establishing correlations across data inputs,  
1449 and tuning as enabling visibility across the environment, leading to a reduction in the time required  
1450 between the identification and resolution of anomalous behavior. In addition, the use of secure backups  
1451 in each Scenario supported effective and resilient recovery by accomplishing restoration using known-  
1452 good system configurations and files.

## 1453 **Appendix A** List of Acronyms

1454	<b>AD</b>	Active Directory
1455	<b>CRADA</b>	Cooperative Research and Development Agreement
1456	<b>CTL</b>	Communications Technology Laboratory
1457	<b>DFIR</b>	Digital Forensics and Incident Response
1458	<b>DMZ</b>	Demilitarized Zone
1459	<b>DNS</b>	Domain Name System
1460	<b>FCR</b>	Facility Control Room
1461	<b>HMI</b>	Human Machine Interface
1462	<b>IP</b>	Internet Protocol
1463	<b>IRP</b>	Incident Response Plan
1464	<b>IRT</b>	Incident Response Team
1465	<b>ISA</b>	(Cisco) Industrial Security Appliance
1466	<b>IT</b>	Information Technology
1467	<b>ITL</b>	Information Technology Laboratory
1468	<b>MFA</b>	Multifactor Authentication
1469	<b>MGT</b>	Management
1470	<b>NCCoE</b>	National Cybersecurity Center of Excellence
1471	<b>NIC</b>	Network Interface Card
1472	<b>NIST</b>	National Institute of Standards and Technology
1473	<b>NISTIR</b>	National Institute of Standards and Technology Interagency Report
1474	<b>OS</b>	Operating System
1475	<b>OT</b>	Operational Technology
1476	<b>RDP</b>	Remote Desktop Protocol
1477	<b>SIEM</b>	Security Information and Event Management
1478	<b>SP</b>	Special Publication
1479	<b>SOC</b>	Security Operations Center
1480	<b>SSH</b>	Secure Shell
1481	<b>TAP</b>	Test Access Point
1482	<b>TST</b>	Technical Support Team

INITIAL PUBLIC DRAFT

1483	<b>USB</b>	Universal Serial Bus
1484	<b>VM</b>	Virtual Machine
1485	<b>SP</b>	Special Publication

## 1486 Appendix B References

- 1487 [1] National Institute of Standards and Technology (2024), The NIST Cybersecurity Framework (CSF)  
1488 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity  
1489 White Paper (CSWP) NIST CSWP 29. <https://doi.org/10.6028/NIST.CSWP.29>.
- 1490 [2] Salfati, E. and Pease, M. (2022), Digital Forensics and Incident Response (DFIR) Framework for  
1491 Operational Technology (OT), NIST Interagency/Internal Report (NISTIR), National Institute of  
1492 Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.IR.8428>.
- 1493 [3] Nelson A, Rekhi S, Souppaya M, Scarfone K (2025), Incident Response Recommendations and  
1494 Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. (National  
1495 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP  
1496 800-61r3. <https://doi.org/10.6028/NIST.SP.800-61r3>.
- 1497 [4] Bartock M, Cichonski J, Souppaya M, Smith M, Witte G, Scarfone K (2016), Guide for  
1498 Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg,  
1499 MD), NIST Special Publication (SP) NIST SP 800-184. <https://doi.org/10.6028/NIST.SP.800-184>.
- 1500 [5] Federal Emergency Management Agency (FEMA). (n.d.). *Incident Organization Chart (ICS 207)*.  
1501 [https://training.fema.gov/emiweb/is/icsresource/assets/ics%20forms/ics%20form%20207,%20i](https://training.fema.gov/emiweb/is/icsresource/assets/ics%20forms/ics%20form%20207,%20incident%20organization%20chart%20(v3).pdf)  
1502 [ncident%20organization%20chart%20\(v3\).pdf](https://training.fema.gov/emiweb/is/icsresource/assets/ics%20forms/ics%20form%20207,%20incident%20organization%20chart%20(v3).pdf)
- 1503 [6] (2025), Reducing the Cybersecurity Risks of Portable Storage Media in OT Environments.  
1504 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication  
1505 (SP) NIST SP 1334. <https://doi.org/10.6028/NIST.SP.1334>.
- 1506 [7] Security Synapse. (2018), *Monitoring USB Storage Activity with Splunk – Part 1 (Connectivity*  
1507 *events)*. [online], [https://securitysynapse.blogspot.com/2018/11/monitoring-usb-storage-](https://securitysynapse.blogspot.com/2018/11/monitoring-usb-storage-activity-part-1.html)  
1508 [activity-part-1.html](https://securitysynapse.blogspot.com/2018/11/monitoring-usb-storage-activity-part-1.html).
- 1509 [8] Security Synapse. (2018), *Monitoring USB Storage Activity with Splunk – Part II*  
1510 *(Read/Write/Delete/Modify events)*. [online],  
1511 <https://securitysynapse.blogspot.com/2018/11/monitoring-usb-storage-activity-part-2.html>.

## 1512 **Appendix C Build Implementation Instructions**

1513 This appendix contains screenshots and instructions on how the operations and incident response team  
1514 prepares, responds, and recovers.

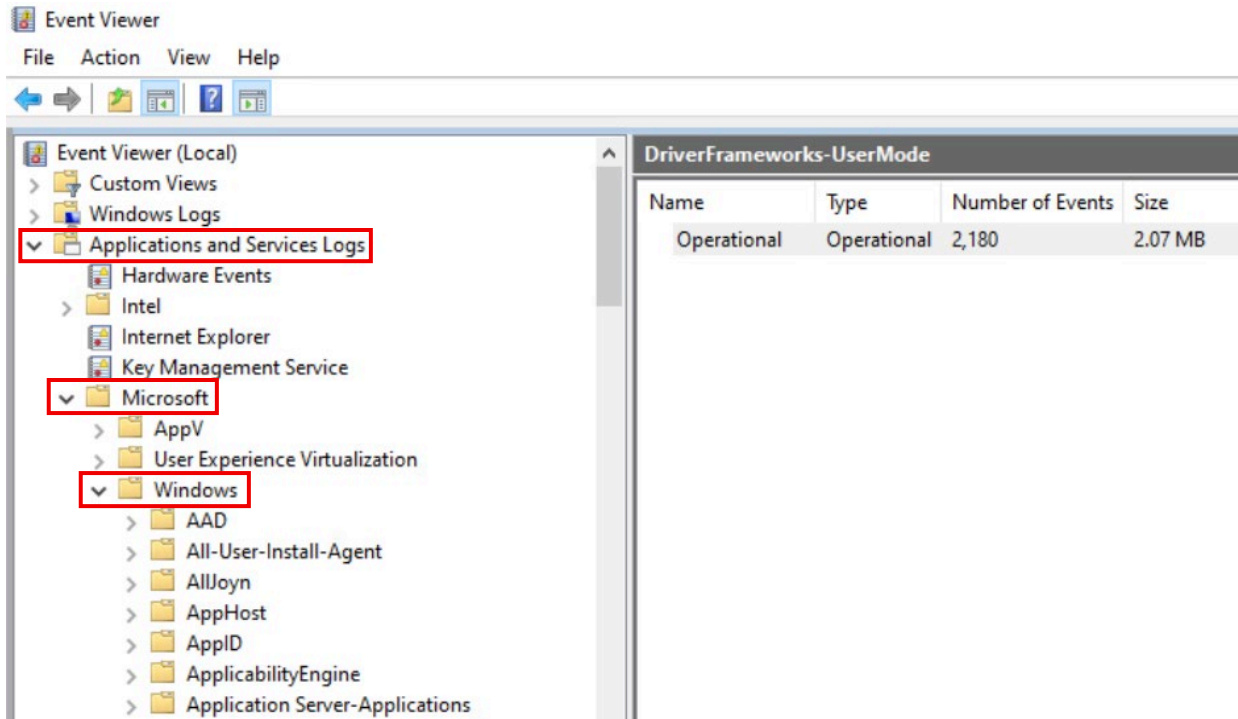
### 1515 **C.1 Scenario A: Technical Details - Preparation**

1516 Before an incident occurs, a manufacturer must prepare for incident response and recovery. The  
1517 following steps were taken as part of a comprehensive cybersecurity program during normal operation,  
1518 which enabled response and recovery during the Scenario A cyber incident.

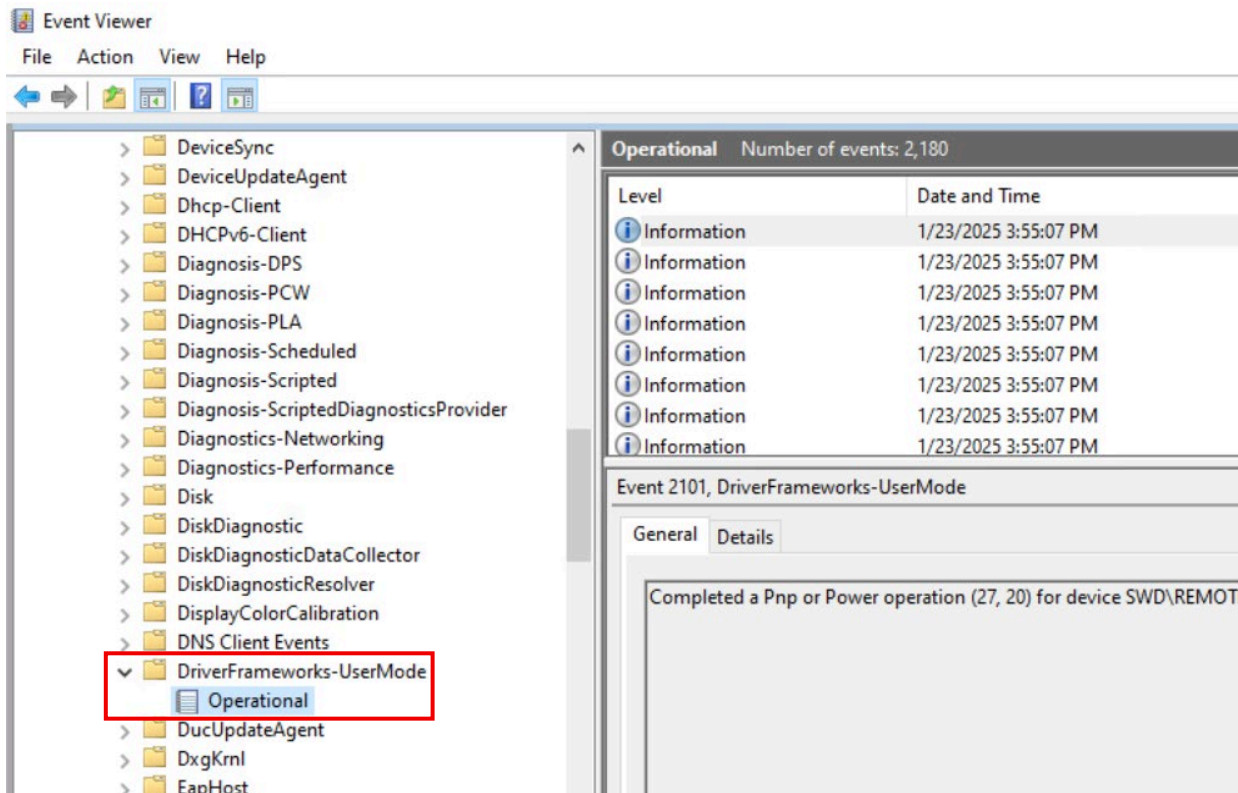
1519 [\[Return to Scenario A\]](#)

#### 1520 **C.1.1 Creating a Splunk Dashboard to detect USB Activity**

1521 During the investigation, the incident response team may want to examine USB activity on the network  
1522 for any malicious behavior. In this scenario, Splunk is used to monitor this activity. First, specific logs are  
1523 enabled on the Windows machines to detect USB activity. To enable these logs, open Windows Event  
1524 Viewer and locate the following log: `Applications and Services Logs\Microsoft\Win-`  
1525 `dows\DriverFrameworks-UserMode\Operational`

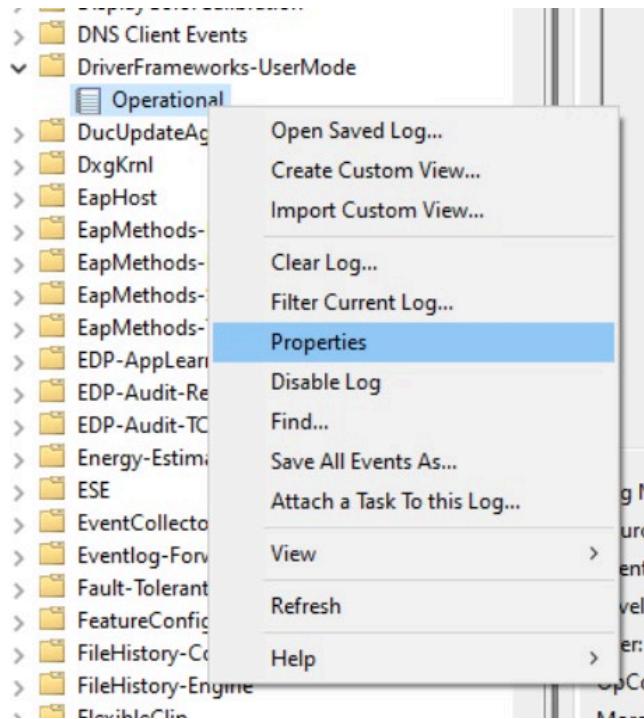


1526 Figure 4-1: Path to Windows Applications and Service Logs in Event Viewer

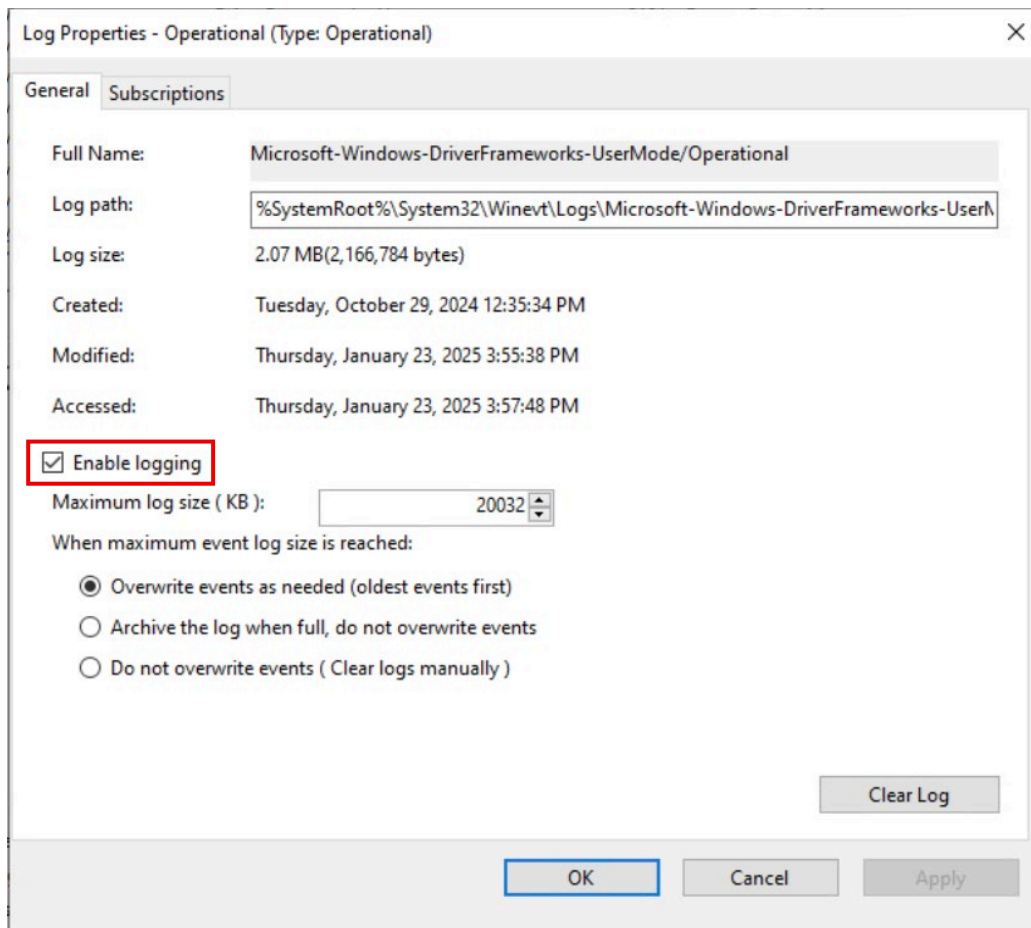


1527 Figure 4-2: Path to DriverFrameworks-UserMode Operational logs in Event Viewer

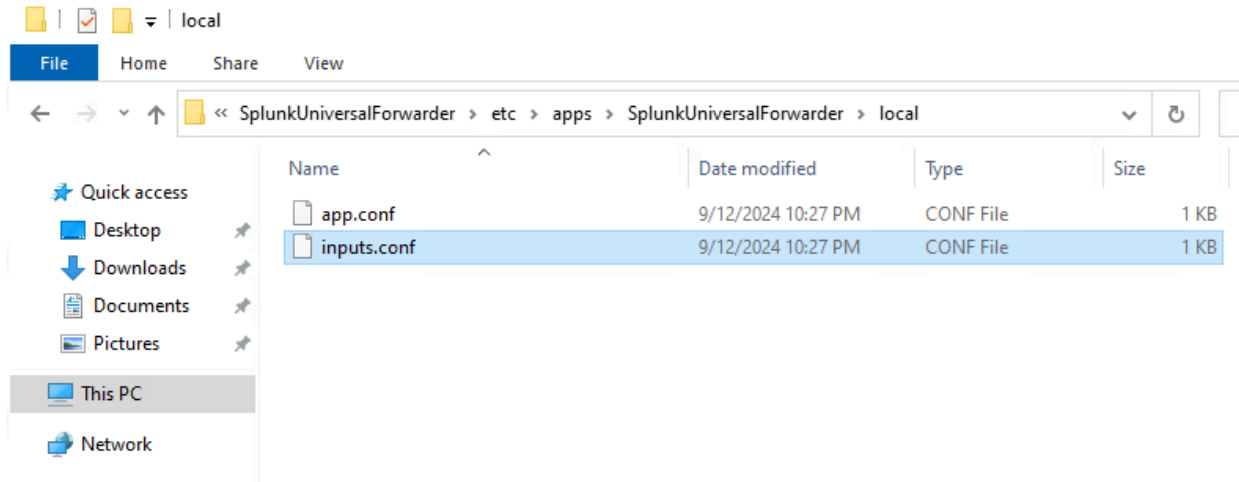
1528 Right-click on `Operational` and choose `Properties`, then check the box labeled `Enable log-`  
1529 `ging`. Select the rest of the settings based on organizational requirements, but for the scenario's pur-  
1530 `pose`, the default log size and `Overwrite events as needed` were selected.



1531 **Figure 4-3: Opening the Driver Frameworks Operational logs properties**



- 1532 **Figure 4-4: The properties used for the Driver Frameworks logs in Scenario A**
- 1533 To transfer these logs into Splunk, edit the `inputs.conf` file located in the Splunk Universal
- 1534 Forwarder directory on the machine. The default path for this file is `C:\Program`
- 1535 `Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local`



1536 **Figure 4-5: The location of the “inputs.conf” file for the Splunk Universal Forwarder**

1537 Using a text editor, add the following lines to this file:

```
1538 [WinEventLog://Microsoft-Windows-DriverFrameworks-UserMode/Operational]  
1539 sourcetype = WinEventLog:DriverFramework-UserMode  
1540 checkpointInterval = 5  
1541 current_only = 0  
1542 disabled = 0  
1543 start_from = oldest
```

1544 See the screenshot below for reference.

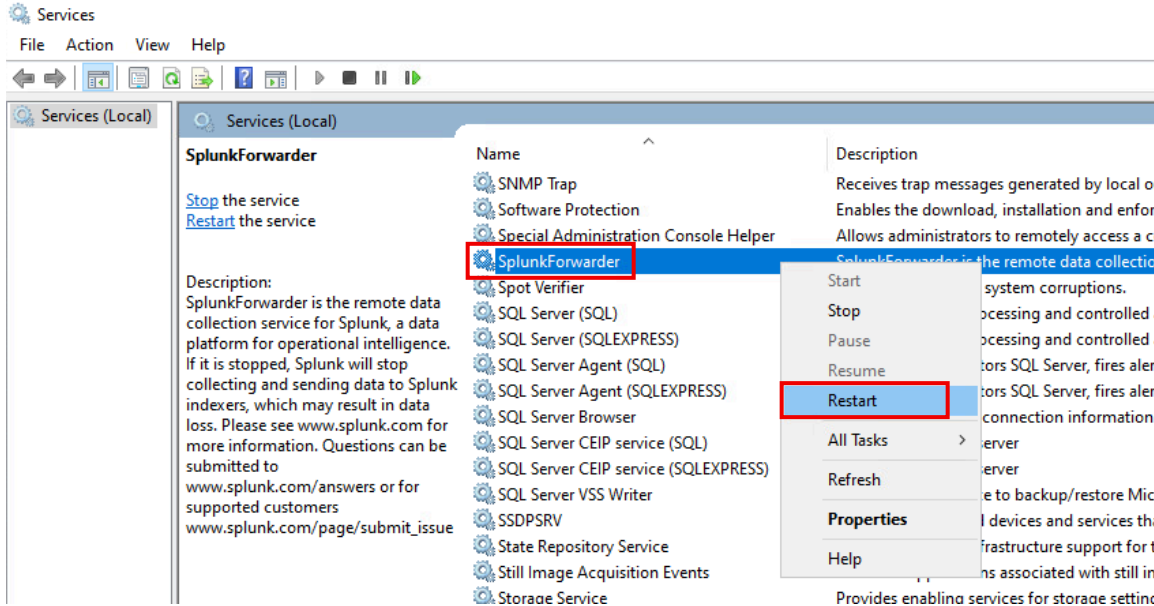
```

19  |
20  | [WinEventLog://ForwardedEvents]
21  |   checkpointInterval = 5
22  |   current_only = 0
23  |   disabled = 0
24  |   start_from = oldest
25  |
26  | [WinEventLog://Microsoft-Windows-DriverFrameworks-UserMode/Operational]
27  |   sourcetype = WinEventLog:DriverFramework-UserMode
28  |   checkpointInterval = 5
29  |   current_only = 0
30  |   disabled = 0
31  |   start_from = oldest
32  |
33  | [perfmon://Free Disk Space]
34  |   counters = Free Megabytes;% Free Space
35  |   instances = _Total
36  |   interval = 3600
37  |   object = LogicalDisk
38  |

```

1545 **Figure 4-6: The “inputs.conf” file opened in Notepad++ to add Operational logs to the ingest**

1546 Restart the SplunkForwarder service:



1547 **Figure 4-7: Restarting the Splunk Forwarder service**

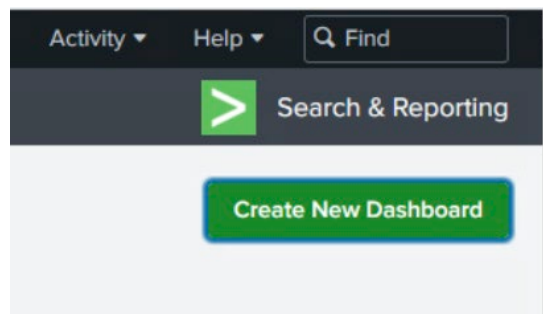
1548 Within these Operational logs, there are a few Event IDs that are useful in identifying USB usage on the  
 1549 host machine:

- 1550 • 2003: tracks when a USB is connected to a computer

- 1551 • 2100 or 2102: tracks when a USB has been disconnected (mainly used 2102 for this scenario)

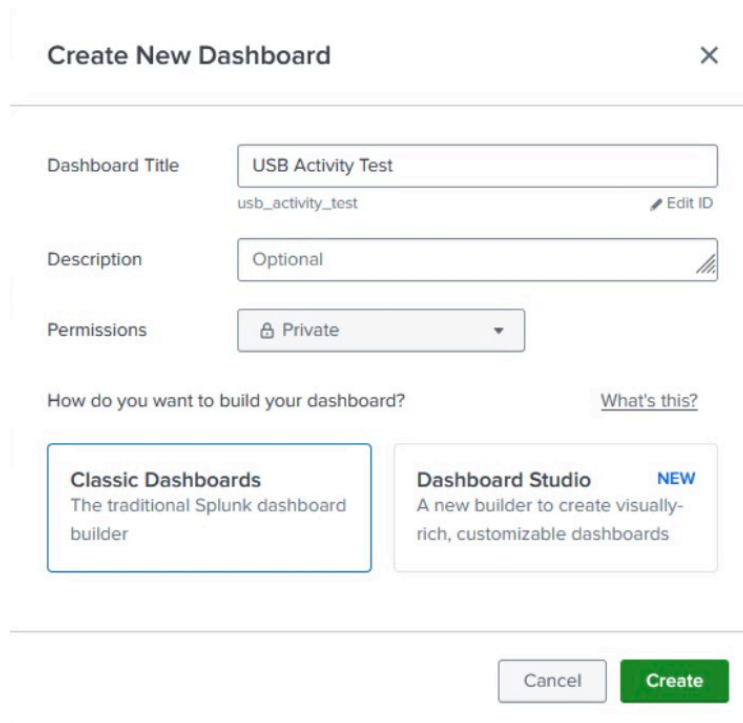
1552 In this scenario, a dashboard was created to track the following:

- 1553 • Number of Connect Events
  - 1554 ○ A simple count of Connect Events
- 1555 • Number of Disconnect Events
  - 1556 ○ A simple count of Disconnect Events
- 1557 • Top Hosts with USB Activity
  - 1558 ○ The top hosts on the network to have any Connect or Disconnect event
- 1559 • Top Removable Storage Vendors
  - 1560 ○ The vendors associated with the USB device (if that information is available)
- 1561 • Top Removable Storage Products
  - 1562 ○ The USB product type (if information is available)
- 1563 • Top Serial Numbers
  - 1564 ○ The serial numbers associated with the USB device (if that information is available)
- 1565 • Events Over Time
  - 1566 ○ A chart showing the Connect and Disconnect events over time
- 1567 • Connection Events (EventCode 2003)
  - 1568 ○ Each individual Connect Event showing all previous information and the date/time the event occurred
  - 1569
- 1570 • Disconnect Events (EventCode 2102)
  - 1571 ○ Each individual Disconnect Event showing all previous information and the date/time the event occurred
  - 1572



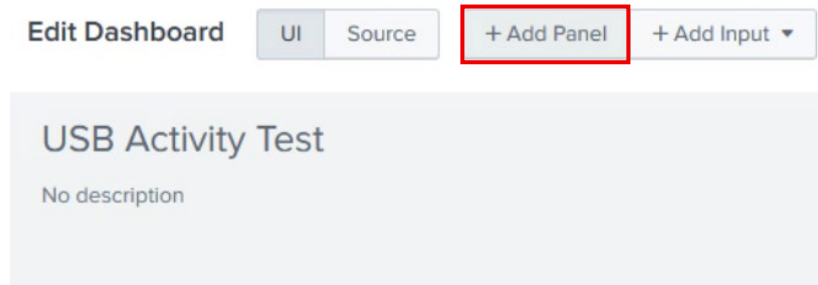
1573 **Figure 4-8: The “Create New Dashboard” button on the top-right of the Splunk web interface**

1574 When creating a new dashboard, Splunk will provide two options: `Classic` or `Studio` dashboard. This  
1575 Practice Guide demonstrates the `Classic` dashboard.



1576 **Figure 4-9: The menu for creating a new dashboard in Splunk**

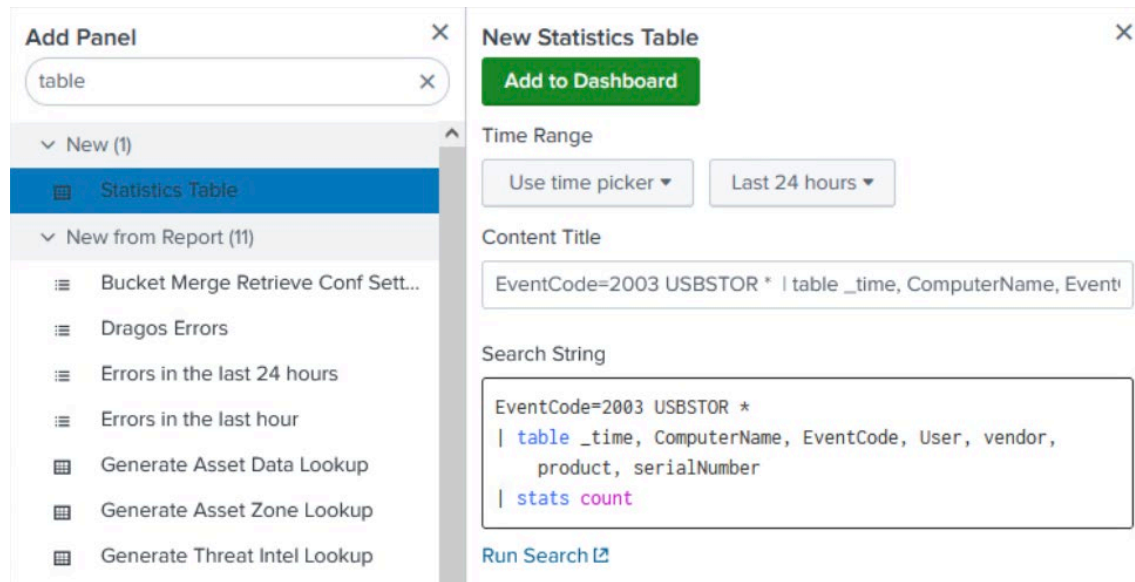
1577 Click the Add Panel button.



1578 **Figure 4-10: The “Add Panel” button highlighted in a newly created Splunk dashboard**

1579 When the new panel appears, click on or search for the `Statistics Table` and enter the following  
 1580 search string into the box, as seen in the screenshot below:

```
1581 EventCode=2003 USBSTOR *
1582 | table _time, ComputerName, EventCode, User, vendor, product, serialNumber
1583 | stats count
```



1584 **Figure 4-11: Creating a new “Statistics Table” in a Splunk dashboard, search string included**

1585 *Note: The same search string is applied to the “Content Title” for clarity when viewing the dashboard; a*  
 1586 *quick reference to visually see how each string is being used.*



1587 **Figure 4-12: A newly created panel in the Splunk dashboard**

1588 In the same edit view, give this panel a name:



1589 **Figure 4-13: Changing the title of a panel in the Splunk dashboard**

1590 Continue creating new panels using the following search strings:

1591           **Number of Disconnect Events:**

1592            EventCode=2102 USBSTOR \*

1593            | transaction maxspan=5s EventCode, ComputerName, serialNumber

1594            | dedup \_time, ComputerName, serialNumber

1595            | table \_time, ComputerName, EventCode, User, vendor, product,

1596            serialNumber

1597            | stats count

1598           **Top Hosts with USB Activity:**

1599            (EventCode=2003 OR EventCode=2102) USBSTOR \*

1600            | transaction maxspan=5s EventCode, ComputerName, serialNumber

1601            | table \_time, ComputerName, EventCode, User, vendor, product,

1602            serialNumber

1603            | top limit=0 ComputerName

1604           **Top Removable Storage Vendors:**

1605            (EventCode=2003 OR EventCode=2102) USBSTOR \*

1606            | dedup serialNumber

1607            | table \_time, ComputerName, EventCode, User, vendor, product,

1608            serialNumber

1609            | top limit=0 vendor

1610           **Top Removable Storage Products:**

1611            (EventCode=2003 OR EventCode=2102) USBSTOR \*

1612            | dedup serialNumber

1613            | table \_time, ComputerName, EventCode, User, vendor, product,

1614            serialNumber

1615            | top limit=0 product

1616           **Top Serial Numbers:**

1617            (EventCode=2003 OR EventCode=2102) USBSTOR \*

1618            | dedup serialNumber

1619            | table \_time, ComputerName, EventCode, User, vendor, product,

1620            serialNumber

1621            | top limit=0 serialNumber

1622           **Events Over Time:**

1623            (EventCode=2003 OR EventCode=2102) USBSTOR \*

1624            | eval action=case(EventCode == 2003, "Connect", EventCode ==

1625            2102, "Connect")

1626            | table \_time, ComputerName, action, EventCode, User, vendor,

1627            product, serialNumber

1628            | eval ActionSerial = action + ":" + serialNumber

1629            | timechart dc(serialNumber) by ActionSerial

1630           **Connection Events (EventCode 2003):**

1631            EventCode=2003 USBSTOR \*

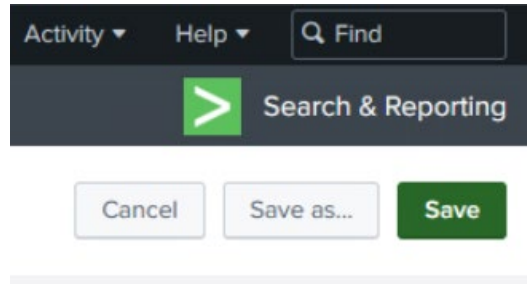
1632            | table \_time, ComputerName, User, vendor, product, serialNumber

1633            | fillnull value="Not Available"

1634           **Disconnect Events (EventCode 2102):**

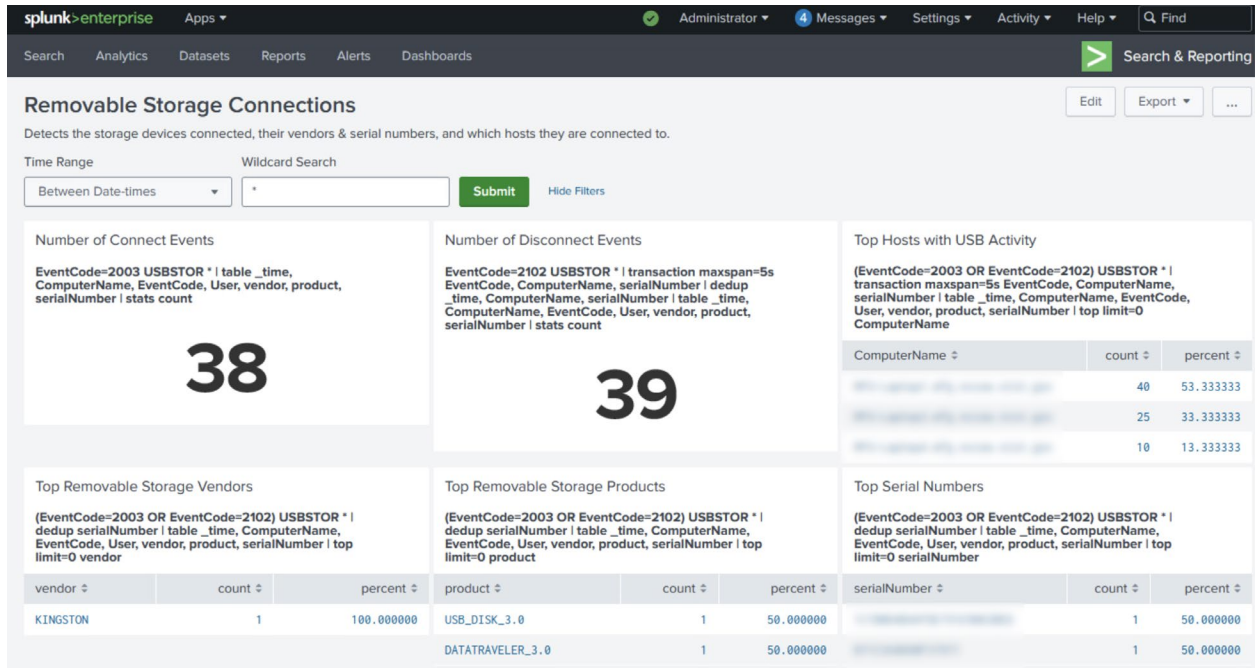
```
1635      EventCode=2102 USBSTOR *
1636      | transaction maxspan=5s EventCode, ComputerName, serialNumber
1637      | dedup _time, ComputerName, serialNumber
1638      | table _time, ComputerName, User, vendor, product, serialNumber
1639      | fillnull value="Not Available"
```

1640 After creating the panels, they can be moved as desired while editing the dashboard. Once satisfied with  
1641 the layout, save the dashboard:



1642 **Figure 4-14: Saving the Splunk dashboard once all panels are created**

1643 This is the dashboard created to capture Removable Storage usage.



1644 **Figure 4-15: Final “Removable Storage Connections” dashboard in Splunk**



1645 **Figure 4-16: Final “Removable Storage Connections” dashboard in Splunk**

Connection Events (EventCode 2003)

EventCode=2003 USBSTOR \* | table \_time, ComputerName, User, vendor, product, serialNumber | fillnull value="Not Available"

_time	ComputerName	User	vendor	product	serialNumber
2025-01-24 12:17:39		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-28 15:20:56		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-28 16:11:33		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-29 14:09:59		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-13 11:07:13		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-13 12:26:17		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-13 13:02:28		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2024-12-17 11:44:39		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2024-10-01 14:02:28		NOT_TRANSLATED	KINGSTON	DATATRAVELER_3.0	
2024-10-01 14:01:57		NOT_TRANSLATED	KINGSTON	DATATRAVELER_3.0	

< Prev 1 2 3 4 Next >

Disconnect Events (EventCode 2102)

EventCode=2102 USBSTOR \* | transaction maxspan=5s EventCode, ComputerName, serialNumber | dedup \_time, ComputerName, serialNumber | table \_time, ComputerName, User, vendor, product, serialNumber | fillnull value="Not Available"

_time	ComputerName	User	vendor	product	serialNumber
2025-01-29 14:57:55		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-28 16:15:42		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-28 16:08:06		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-24 15:23:29		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-13 14:20:17		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-13 12:26:35		NOT_TRANSLATED	Not Available	USB_DISK_3.0	
2025-01-13 11:09:38		NOT_TRANSLATED	Not Available	USB_DISK_3.0	

1646 **Figure 4-17: Final “Removable Storage Connections” dashboard in Splunk**

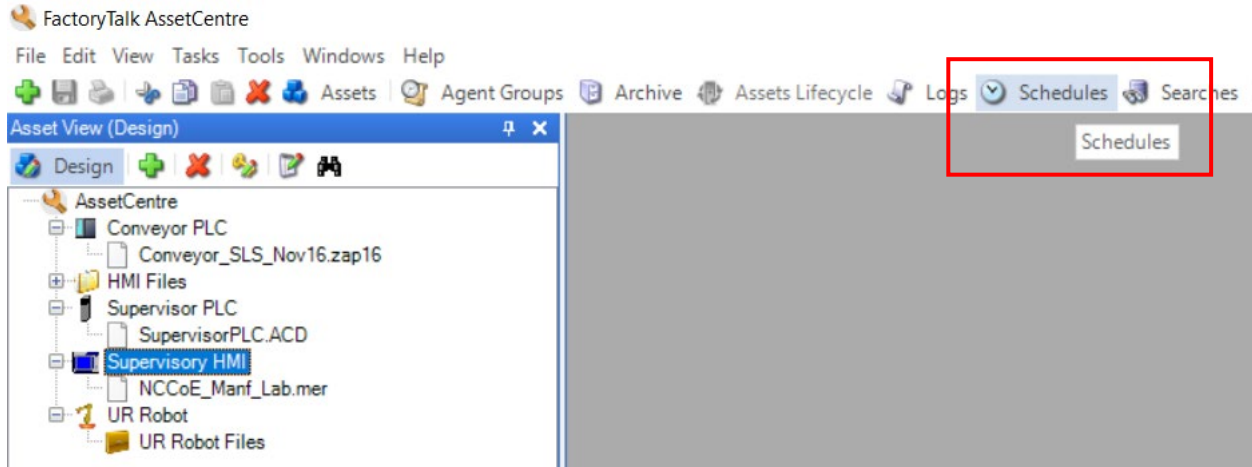
1647 Online resources have been leveraged in the development of these dashboards [7][8].

1648 [\[Return to Scenario A\]](#)

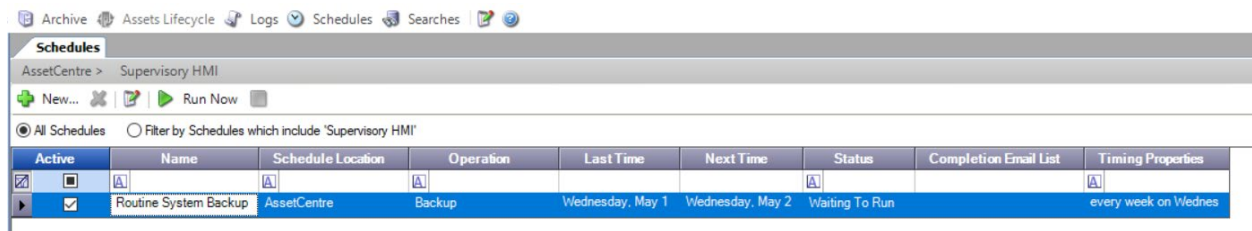
### 1649 C.1.2 Backup the Rockwell PanelView™ HMI

1650 Rockwell Automation offers several different tools and methods for generating backups. The factory  
 1651 engineer took backups using AssetCentre. To configure the backup of the HMI using AssetCentre, design  
 1652 mode must be enabled by signing in as a qualified administrator account and selecting the design  
 1653 button on any AssetCentre Desktop Client. Upon verifying connection to the HMI through FactoryTalk®  
 1654 Linx, an HMI item in design mode is created, both by selecting the HMI through Linx and associating a  
 1655 qualified HMI machine edition runtime file, labeled .mer, with the asset in the creation menu.

1656 Upon creation, the asset can then be added to a schedule by right-clicking on the asset and selecting  
 1657 Schedules or clicking the Schedules icon on the icon bar. The frequency of the Disaster Recovery –  
 1658 Backup and Compare schedule was set to one week, and a timeslot for execution was selected. Upon  
 1659 enabling the backup and verification schedule, AssetCentre will automatically run a check on all assets  
 1660 configured this way in the schedule and will log any discrepancies, attach the compare report to the  
 1661 record, and/or email the report out.

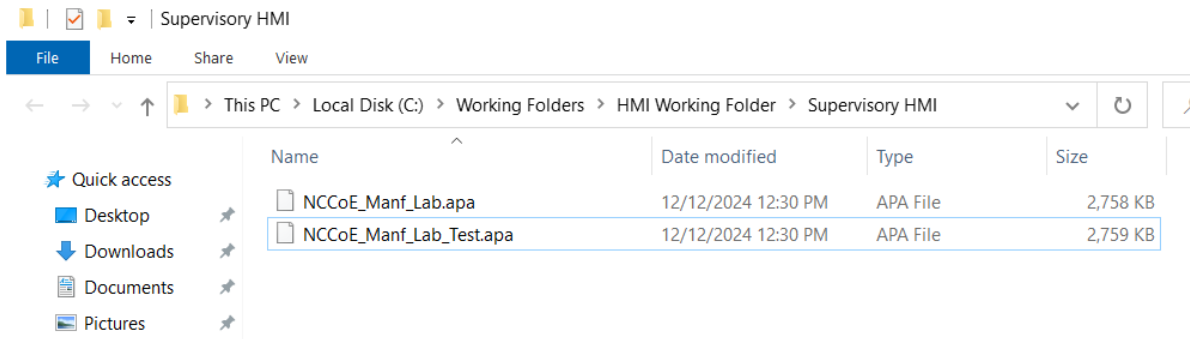


1662 **Figure 4-18: Showing the “Schedules” button in FactoryTalk® AssetCentre**

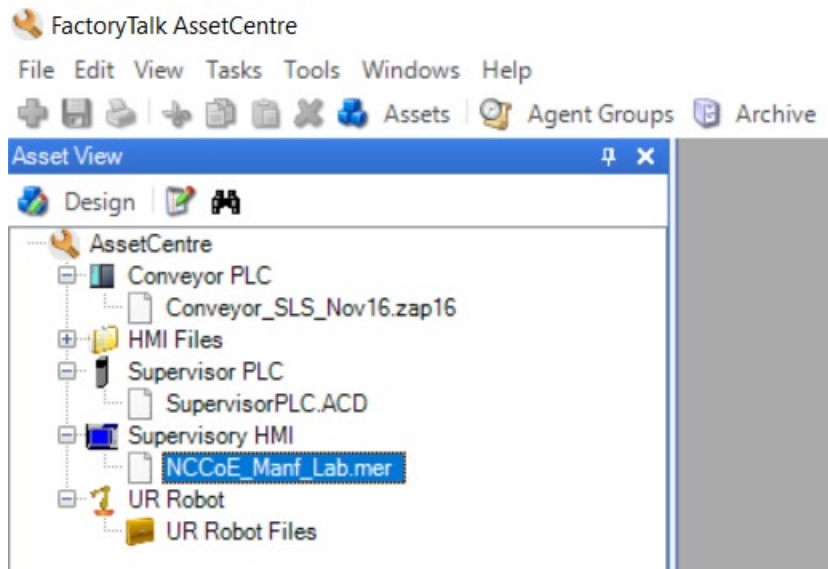


1663 **Figure 4-19: The “Schedules” view in AssetCentre**

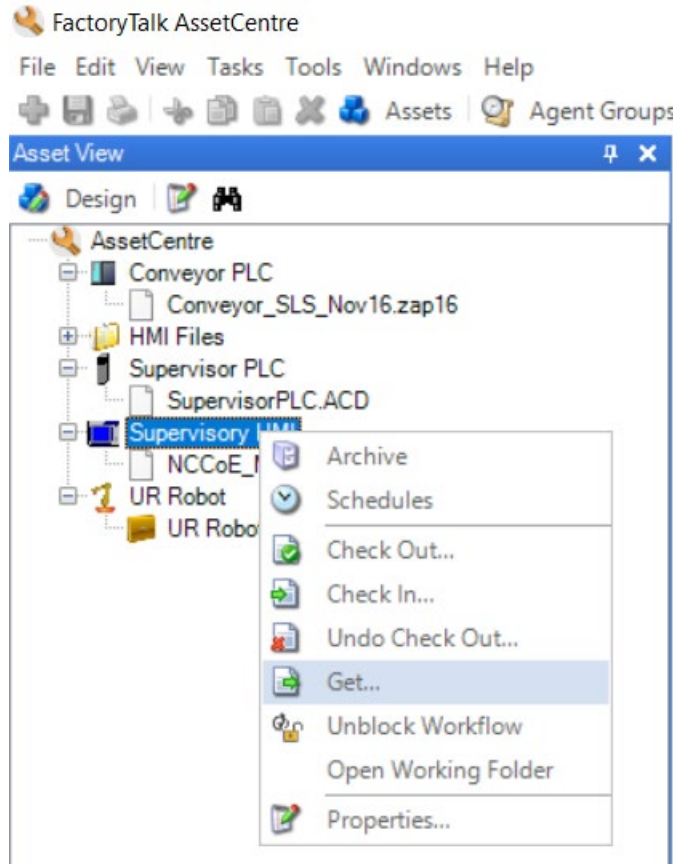
1664 Additionally, the configuration file (.mer) can be retrieved using the “get” feature. In the Asset View,  
 1665 right-click on the Supervisory HMI and click on `get`. This will pull up a menu with optional information.  
 1666 After confirming, the file will be placed into the Working Folder chosen in the `Archive` section:



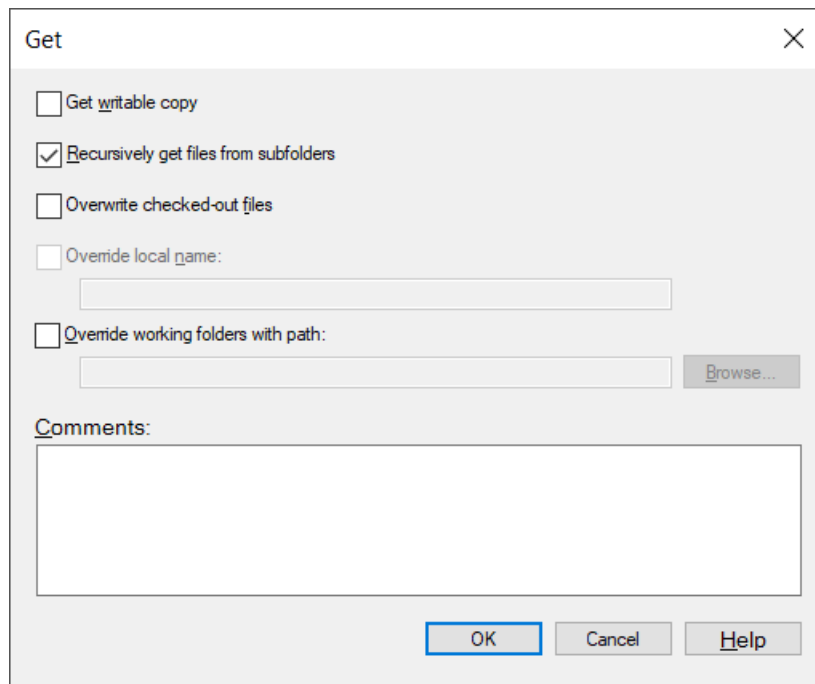
1667 **Figure 4-20: Location of the “Working Folders” without the “.mer” file present**



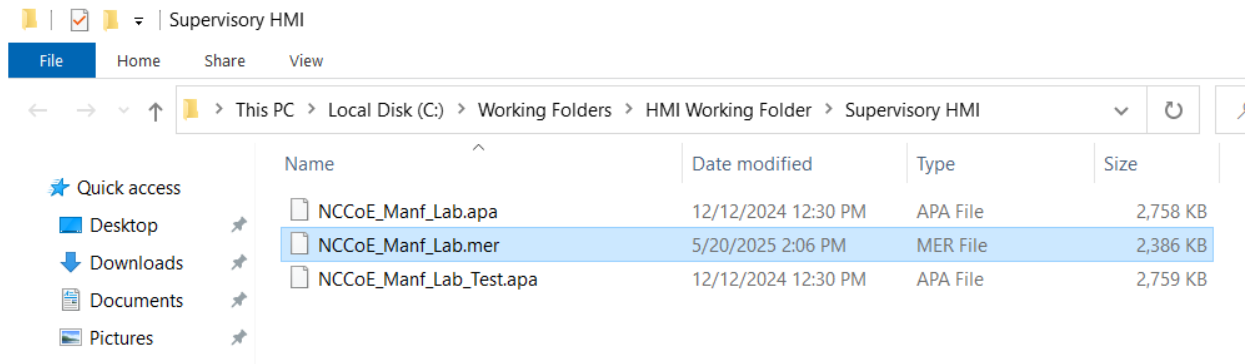
1668 **Figure 4-21: Location of the stored “.mer” project file in AssetCentre**



1669 Figure 4-22: Right-clicking on the Supervisory HMI asset and selecting “Get” to pull the “.mer” file



1670 Figure 4-23: The default “Get” options in AssetCentre



1671 **Figure 4-24: “.mer” file now located in the “Working Folders” directory after using the “Get” tool**

1672 Comparing the first and final screenshot in this set, it can be seen that the .mer configuration file has  
 1673 been uploaded to the Working Folders directory that is created inside AssetCentre. Now this file  
 1674 can safely be backed up. These are the options used to back up the project files in all scenario testing.

1675 [\[Return to Scenario A\]](#)

### 1676 C.1.3 ForceField Zero Trust Storage

1677 The data storage used for every scenario is ForceField Zero Trust Storage by GreenTec. As an immutable  
 1678 storage solution, it enforces write-once, read-many (WORM) behavior to protect backups from  
 1679 tampering or deletion. Access is available through the command line or a GUI-based web server. This  
 1680 section demonstrates the web server option for uploads and downloads.

1681 After logging into the web server, the accessible storage drives configured when establishing the server  
 1682 are viewable. To upload files, click the Upload button on the desired storage device.

#### ForceField Zero Trust Storage™ Running on Host: qnode7

SerialNum	Device	UpLoad
[blurred]	/dev/sdf	Upload
[blurred]	/dev/sdg	Upload
[blurred]	/dev/sdh	Upload
[blurred]	/dev/sdi	Upload

1683 **Figure 4-25: The default view after logging into the web interface for ForceField**

1684 *Note: Links on this web interface will not have visual indicators/feedback, but still work when clicked on.*

1685 When uploading, the screenshot below will appear. If choosing to encrypt the files, enter the  
 1686 information on this page. Select the files desired for upload, and when ready, click the Begin File  
 1687 Upload button at the bottom of the screen.

## ForceField™ File Upload to Zero Trust Storage™ Volume

**\*\*\* PLEASE READ \*\*\***

**\*\*\* WARNING -----> Encrypted Files Require Special CAUTIONS and Requirements.**

**Please Read the Documentation and Understand the Risks of Losing Data Access with Encryption.**

- 1. You MUST SAVE the Generated Associated KEY FILES.**
- 2. You MUST REMEMBER your FILE Userid & FILE Password to Access any data in these files.**
- 3. You MUST REMEMBER the Serial Number or Realm (If specified).**

**Enter Userid & Password ONLY IF FILES ARE TO BE ENCRYPTED.  
Otherwise, MAKE SURE THEY ARE EMPTY.**

**SerialNo:**  **Device:** /dev/sdf (H)

<b>Userid</b>
<input type="text"/>
<b>Password</b>
<input type="text"/>
<b>Confirm</b>
<input type="text"/>
<b>Realm</b>
<input type="text"/>

**SELECT Files to Upload:**

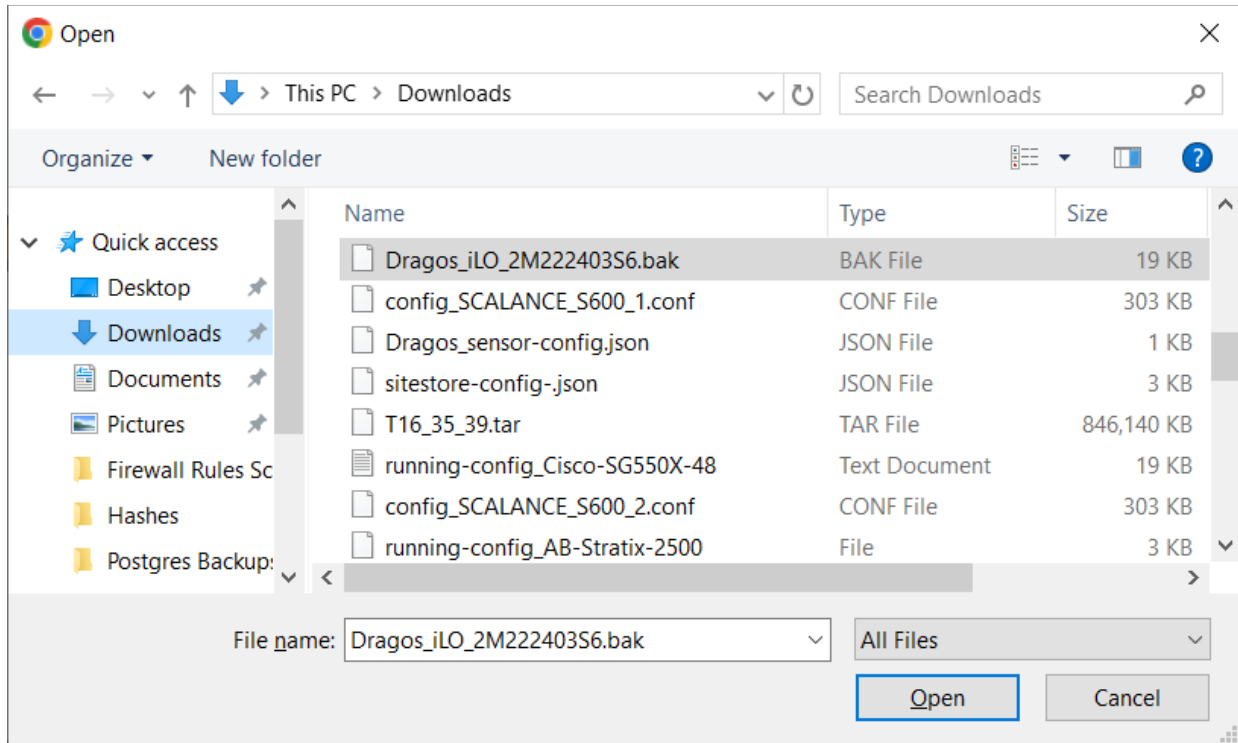
**Multiple files:**  No file chosen

**SUBMIT File Upload:**

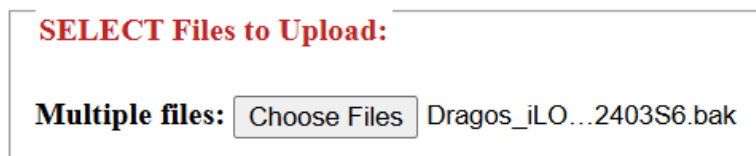
**Click on the button below to begin file uploads**

1688 Figure 4-26: The default view when selecting the “Upload” option in ForceField

1689 The following set of screenshots is an example of choosing a file to upload.



1690 **Figure 4-27: Selecting a file to upload to ForceField**



1691 **Figure 4-28: After selected, the files to upload will show here in ForceField**

```

-----
File Upload Status:
-----
stored as Dragos_iLO_2M222403S6.bak (18756 bytes)

* * *   File Uploads Completed   * * *
    
```

1692 **Figure 4-29: Showing that the files were successfully backed up in ForceField**

1693 After uploading all files, they can be located by clicking on the storage name under SerialNum:

## ForceField Zero Trust Storage™ Running on Host: qnode7

SerialNum	Device	UpLoad
[Blurred]	/dev/sdf	Upload
[Blurred]	/dev/sdg	Upload
[Blurred]	/dev/sdh	Upload
[Blurred]	/dev/sdi	Upload

1694 **Figure 4-30: The default view after logging into the web interface for ForceField**

1695 Once inside the device where the backup was uploaded, search to ensure the file was backed up. If  
 1696 necessary, validate the backup file uploaded properly by downloading the file and comparing the hashes  
 1697 of both files.

Filename	Ext#	Size	Created
NIST_NCCoE_Logo.jpg	1	33.77K	20240129 16:25:00
20240617 [Blurred] running-config.txt	1	18.94K	20240617 12:30:57
20240617 [Blurred] running-config.txt	2	18.94K	20240617 12:32:54
20240617 [Blurred] running-config.txt	3	75.78K	20240617 12:32:58
.._doc_WFSsvr_User_Guide.pdf	1	1.29M	20240711 13:17:41
_opt_greentec_forcefield_doc_ForceField_WFS_Users_Guide.pdf	1	1.11M	20240711 13:18:30
Dragos_sitestore-config-2024-08-15T19_22_11.573Z.json	1	2.13K	20240822 10:10:28
Tenable_2024-08-15T17_12_59.tar.gz	1	267.82M	20240822 10:10:28
running-config_Cisco-SG550X-48_20240815.txt	1	19.10K	20240822 10:17:50
config_SCALANCE-S600_20240815.conf	1	309.77K	20240822 10:17:50
running-config_AB-Stratix-2500_20240815	1	2.35K	20240822 10:17:51
all_databases_backup-20240822.sql	1	8.58M	20240822 15:14:27
Ignition-Edge-Historian_Ignition-backup-edge20240822-1204.gwbk	1	8.53M	20240822 15:16:21
Ignition-Local-Historian-Gateway_Ignition-backup-20240822-0903.gwbk	1	8.73M	20240822 15:16:35
Ignition-Local-Hist-DB_Ignition-backup-20240822-0856.gwbk	1	8.49M	20240822 15:16:49
Dragos_iLO_2M222403S6_20241126_1619.bak	1	18.76K	20241126 17:18:01
config_SCALANCE_S600 (1).conf	1	309.77K	20241126 17:18:02
Dragos_sensor-config-20241126.json	1	575	20241126 17:18:03
sitestore-config-2024-11-26T17_05_52.757Z.json	1	2.13K	20241126 17:18:03
2024-11-26T16_35_39.tar	1	866.45M	20241126 17:18:04
running-config_Cisco-SG550X-48_20241126.txt	1	19.10K	20241126 17:41:29
config_SCALANCE_S600_20241126.conf	1	309.77K	20241126 17:41:30
running-config_AB-Stratix-2500_20241126	1	2.35K	20241126 17:41:31
NCCoE_Manf_Lab.apa	1	2.82M	20241212 12:33:38
NCCoE_Manf_Lab.mer	1	2.44M	20241212 12:33:43
NCCoE_Manf_Lab_Test.apa	1	2.82M	20241212 12:33:48
running-config-AB-Stratix-2500-20250124.txt	1	2.35K	20250124 14:50:31
hash-search-for-mer-files-FINAL.ps1	1	871	20250124 15:36:46
Ignition-DB-Backup-test.sql	1	55.30M	20250429 13:19:50
<span style="border: 1px solid red;">Dragos_iLO_2M222403S6.bak</span>	1	18.76K	20250520 10:34:19

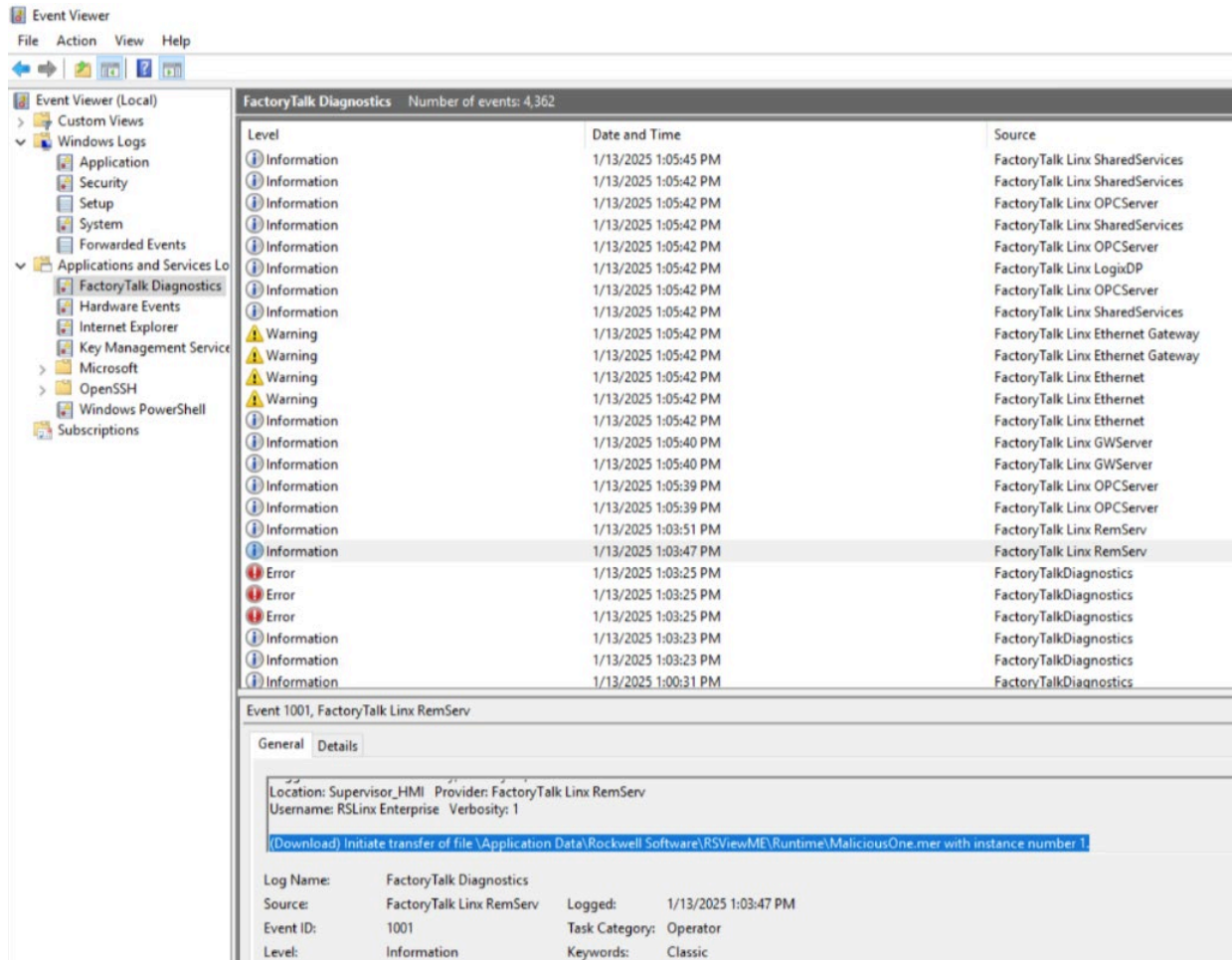
30 File Extents on this Volume

1698 **Figure 4-31: A list of uploaded files residing in ForceField**

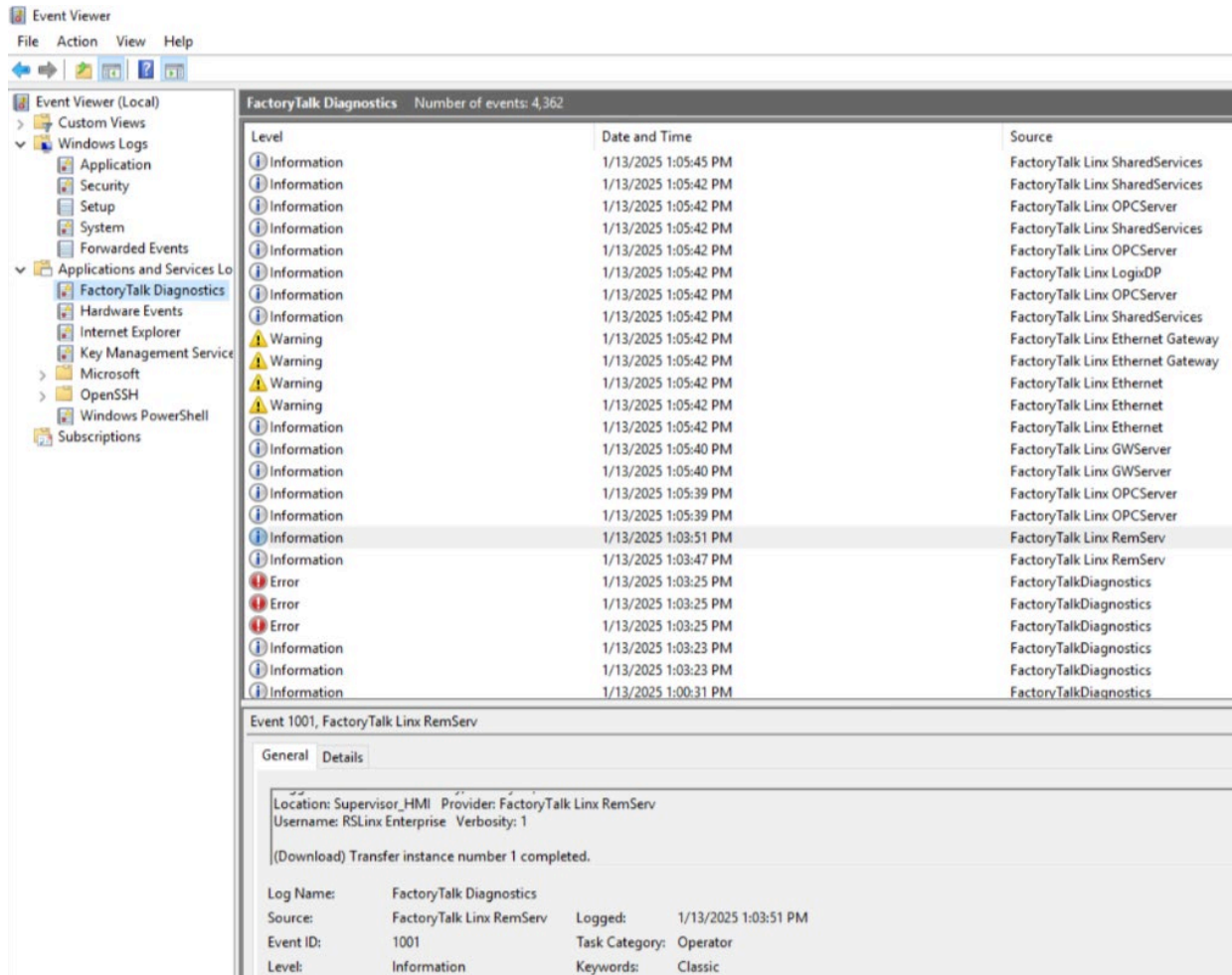
1699 [\[Return to Scenario A\]](#)

1700 **C.1.4 FactoryTalk® Logs in Windows Event Viewer**

1701 FactoryTalk® AssetCentre provides valuable insight into the change of the HMI program. The IRT meets  
 1702 to identify lessons learned at the conclusion of the incident investigation. The IRT discusses that incident  
 1703 response could have been faster if the AssetCentre logs were integrated into the SIEM. This action item  
 1704 is documented in the incident report and scheduled for future implementation.

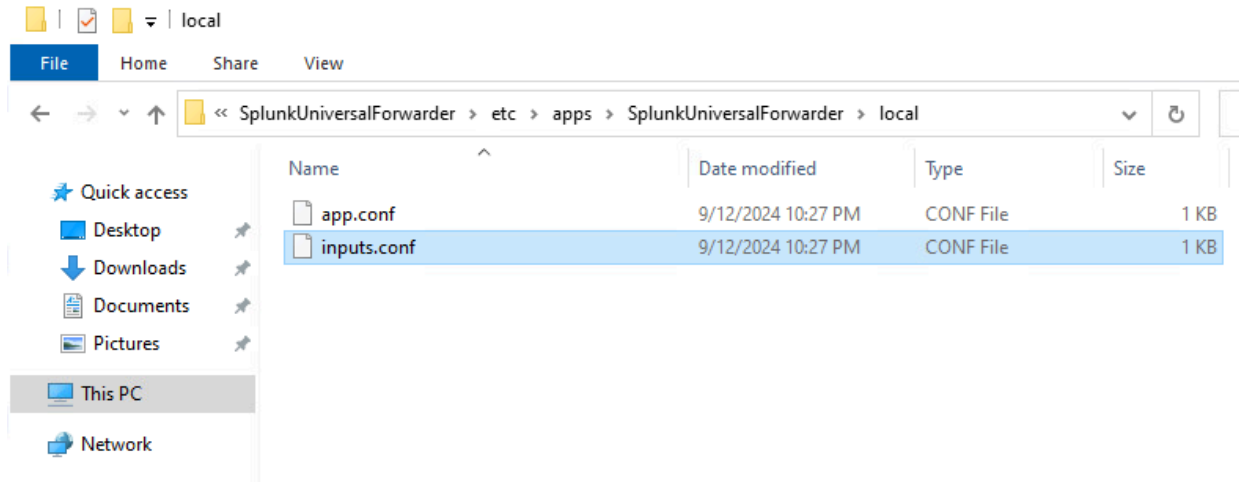


1705 **Figure 4-32: The FactoryTalk® Diagnostics logs residing in Event Viewer**



1706 **Figure 4-33: The FactoryTalk® Diagnostics logs residing in Event Viewer**

1707 To transfer these logs into Splunk, edit the `inputs.conf` file located in the Splunk Universal Forwarder  
 1708 directory on the machine. The default path for this file is `C:\Program Files\SplunkUniversal-`  
 1709 `Forwarder\etc\apps\SplunkUniversalForwarder\local` (see the screenshot below for ref-  
 1710 erence). Step-by-step instructions are included for this process.

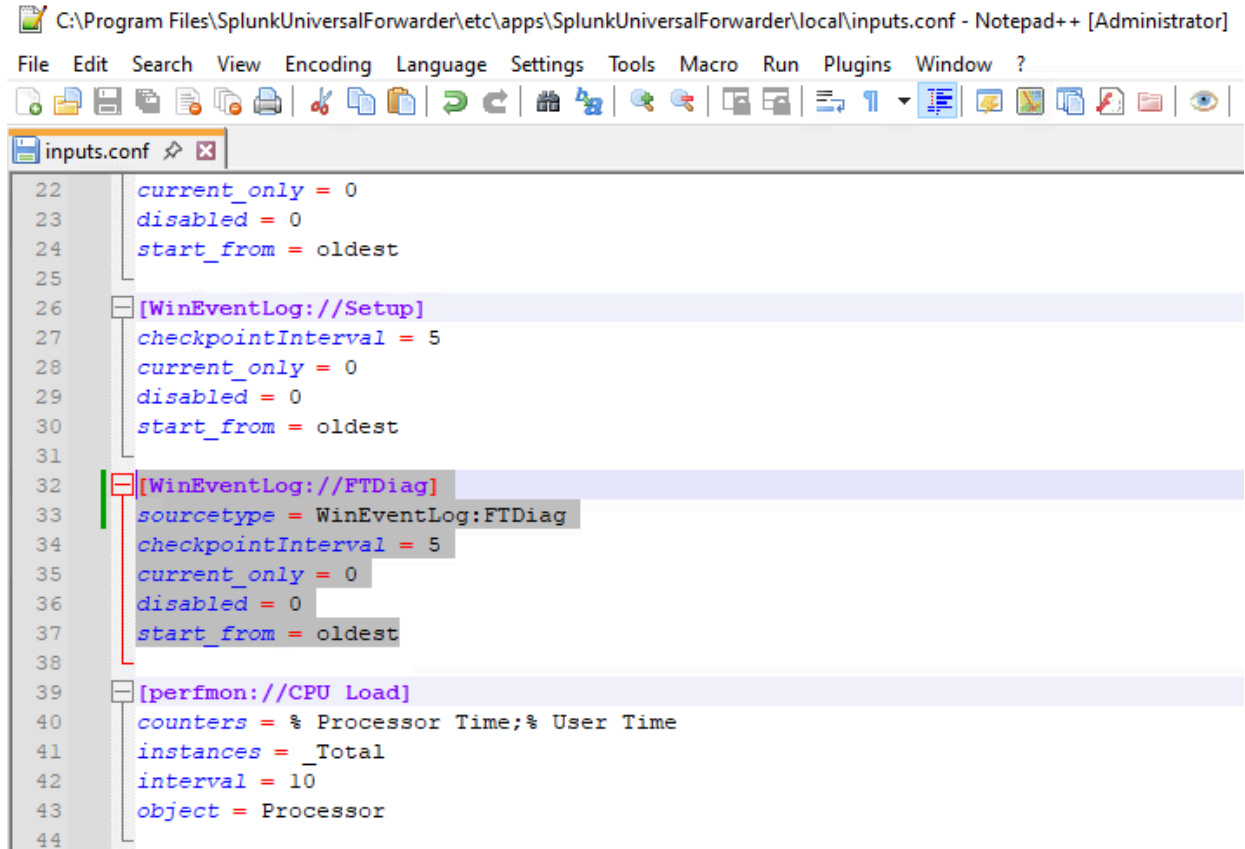


1711 **Figure 4-34: The location of the “inputs.conf” file to edit**

1712 Using a text editor, add the following lines to this file:

```
1713     [WinEventLog://FTDiag]
1714     Sourcetype = WinEventLog:FTDiag
1715     checkpointInterval = 5
1716     current_only = 0
1717     disabled = 0
1718     start_from = oldest
```

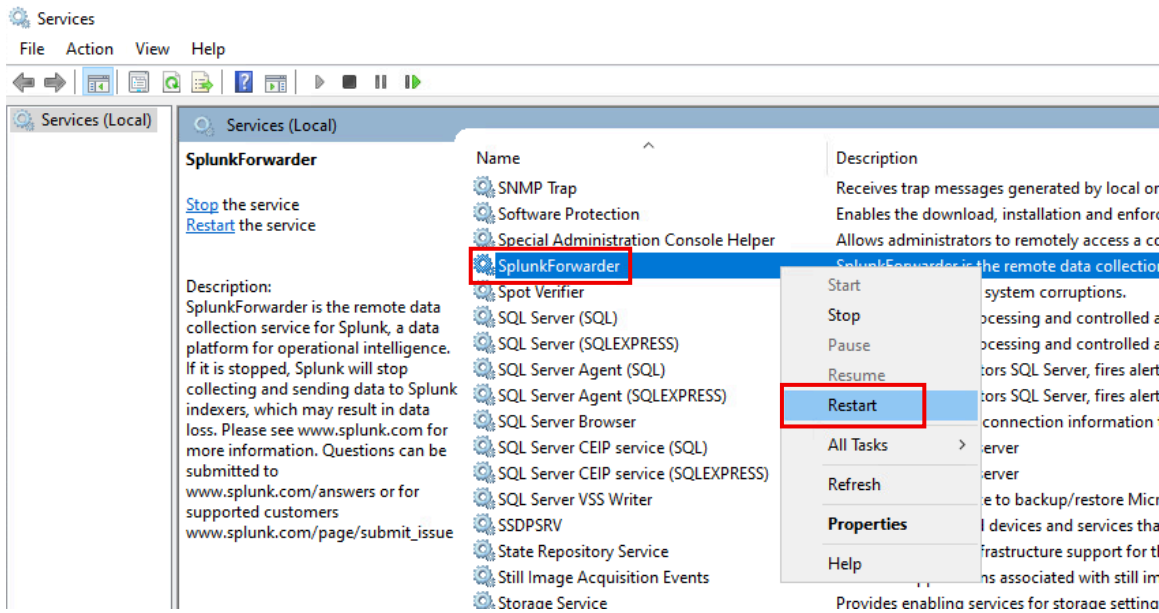
1719 See the screenshot below for reference.



```
22 current_only = 0
23 disabled = 0
24 start_from = oldest
25
26 [WinEventLog://Setup]
27 checkpointInterval = 5
28 current_only = 0
29 disabled = 0
30 start_from = oldest
31
32 [WinEventLog://FTDiag]
33 sourcetype = WinEventLog:FTDiag
34 checkpointInterval = 5
35 current_only = 0
36 disabled = 0
37 start_from = oldest
38
39 [perfmon://CPU Load]
40 counters = % Processor Time;% User Time
41 instances = _Total
42 interval = 10
43 object = Processor
44
```

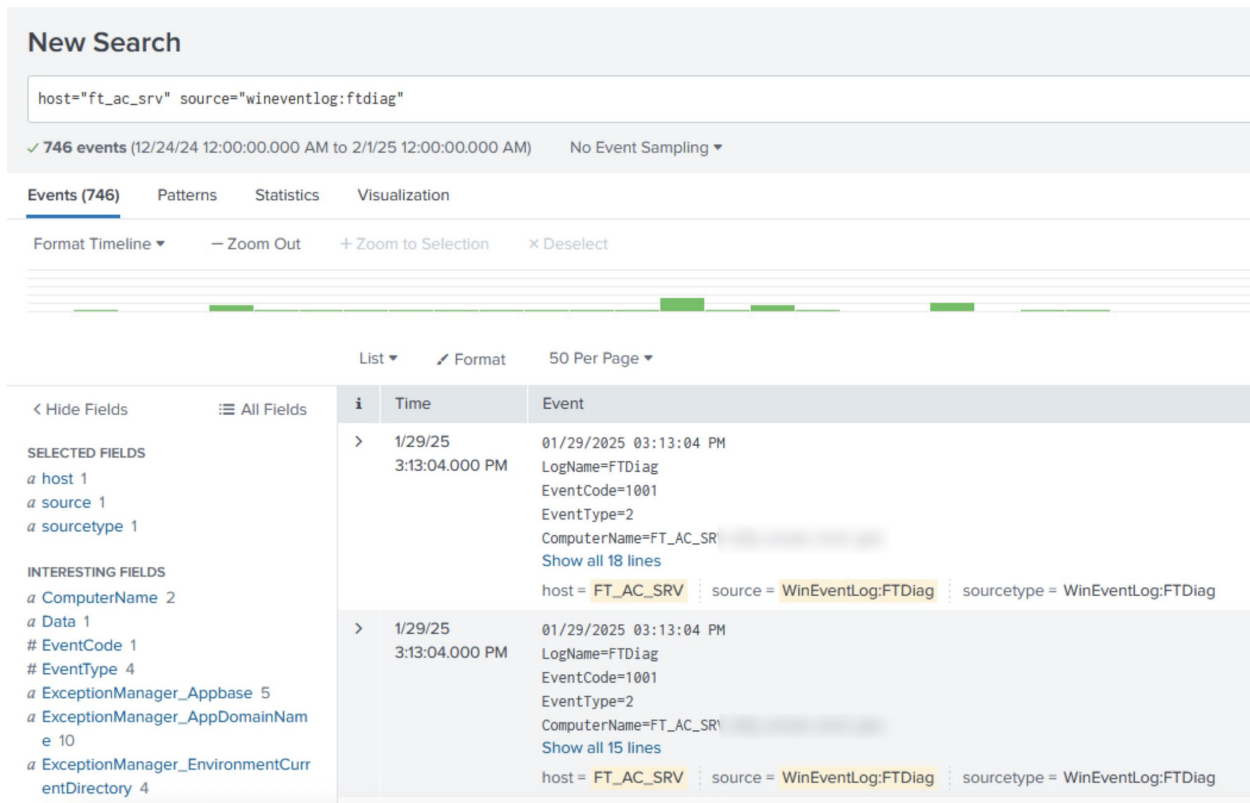
1720 Figure 4-35: The “inputs.conf” file opened in Notepad++ to add FactoryTalk® logs to the ingest

1721 Restart the SplunkForwarder service:



1722 **Figure 4-36: Restarting the Splunk Forwarder service**

1723 Search in Splunk to confirm the FTDiag logs are being forwarded:



1724 **Figure 4-37: Searching for the newly ingested FactoryTalk® Diagnostic logs**

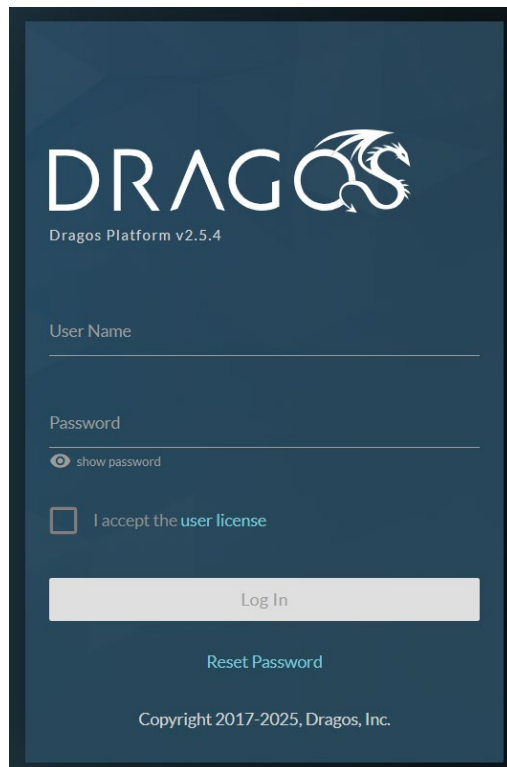
1725 [\[Return to Scenario A\]](#)

1726 **C.2 Scenario A: Technical Details – Response**

1727 **C.2.1 Dragos Case Creation**

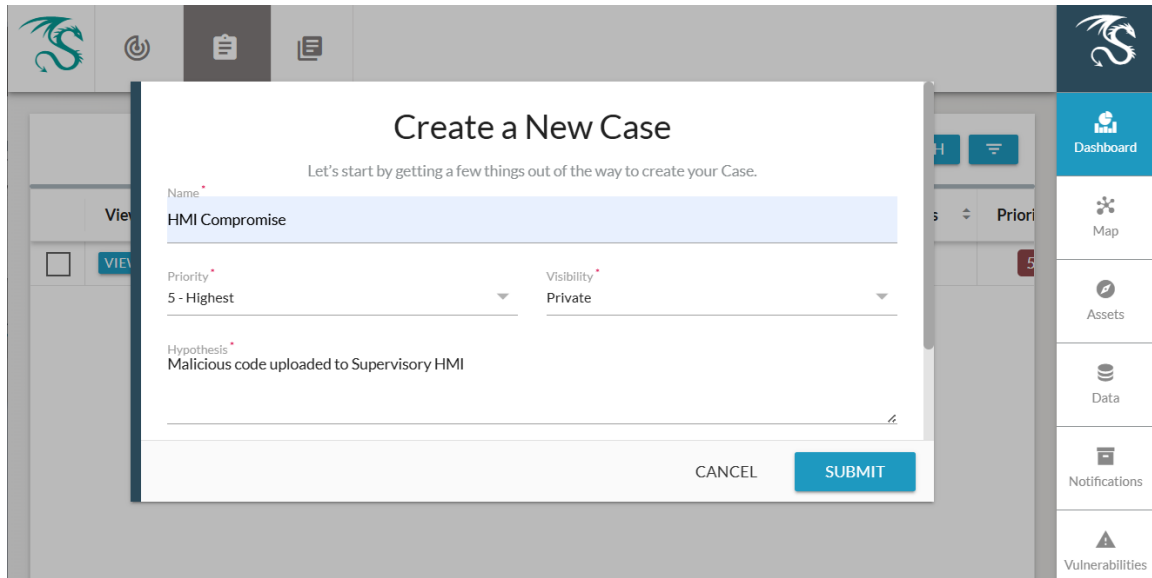
1728 To prioritize, investigate, and respond to cybersecurity alerts in ICS environments, the Dragos SiteStore  
1729 Platform (Version 2.5.4) has a Case Management feature. An incident case is created using the  
1730 management tool with a hypothesis description about the incident, priority setting, and assignment  
1731 notification.

1732 Log in to the Dragos SiteStore web portal using the host URL, username, and password credentials as  
1733 shown below:



1734 **Figure 4-38: Login screen for the web interface of Dragos**

1735 Once logged in, go to the Cases Tab to click the Create a New Case button to open a new case entry  
1736 form. From the entry form, enter the case name, the priority level (0–5, with 5 being highest), visibility  
1737 (public or private), and hypotheses, and then hit the Submit button to create a case.



1738 **Figure 4-39: Creating a new case in the Dragos web interface**

1739 A sample case is generated as shown below:

View	Type	ID	Name	Date	Notifications	Access	Priority	Watchers	Author	State
<input type="checkbox"/> <a href="#">VIEW</a>	Incident	2	HMI Compromise	11/12/24, 11:36 AM EST	0	PRIVATE	5	0	admin	Open

1740 **Figure 4-40: Newly created case listed in Dragos**

1741 [\[Return to Scenario A\]](#)

## 1742 C.2.2 Disconnect WAN from Cisco ISA Firewall

1743 While the ISA3000 has many features that control the flow of network traffic, the IRT determined, based  
 1744 on the risk of the scenario, to isolate physically between the manufacturing lab network and the  
 1745 industrial DMZ. To perform this isolation, the Ethernet cable in the WAN port was disconnected.

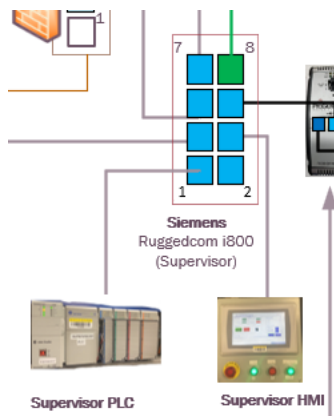


1746 **Figure 4-41: Unplugging the Ethernet cable from the WAN port**

1747 [\[Return to Scenario A\]](#)

### 1748 C.2.3 Isolation of HMI

1749 The compromised HMI should be disconnected from the network. Industrial equipment is sometimes  
1750 physically hardened in the field in a way that network connections are not easily accessible. The  
1751 engineer can use the network drawing to identify the switch that the HMI is connected to, then use the  
1752 inventory to find its physical location. The HMI was connected to a switch inside a rack, which was easier  
1753 to disconnect. Having an available and up-to-date network drawing and inventory allowed for a faster  
1754 isolation.

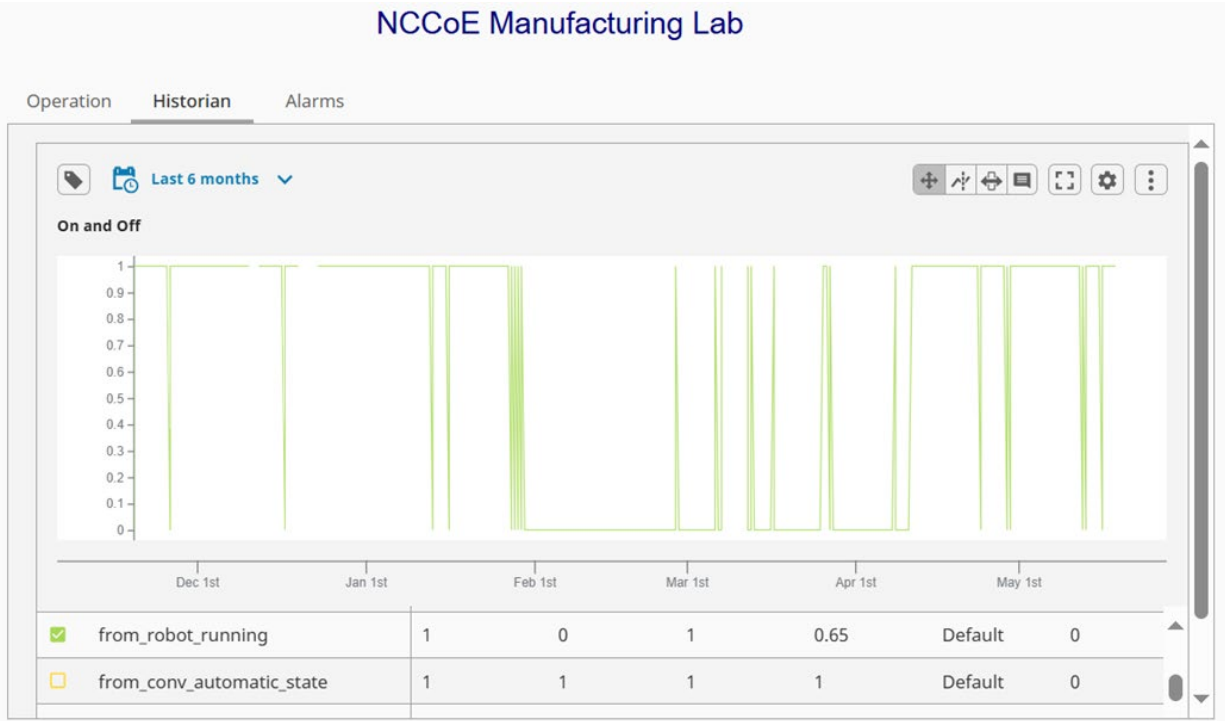


1755 **Figure 4-42: Network diagram showing where the Supervisor HMI is plugged into the Siemens switch**

1756 [\[Return to Scenario A\]](#)

1757 **C.2.4 Inductive Automation, Data Historian**

1758 The following screenshot is the Historian report on the system’s operation during the installation of a  
 1759 malicious file on the supervisor HMI. Even though the system stops, the system signal still shows in  
 1760 running operation.

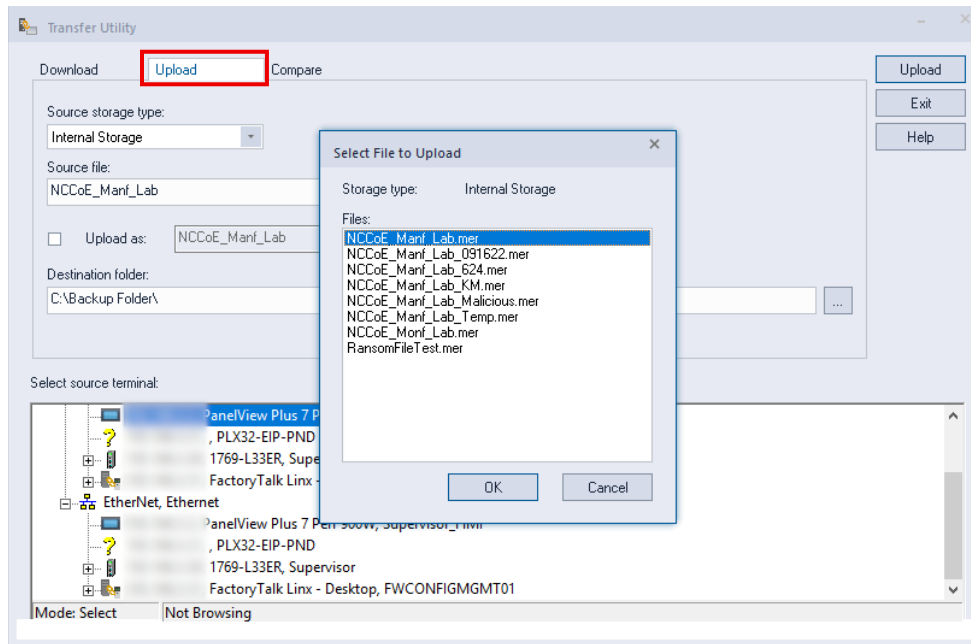


1761 **Figure 4-43: Data historian showcasing the tags indicating system start and stops**

1762 [\[Return to Scenario A\]](#)

1763 **C.2.5 Rockwell FactoryTalk® Transfer Utility**

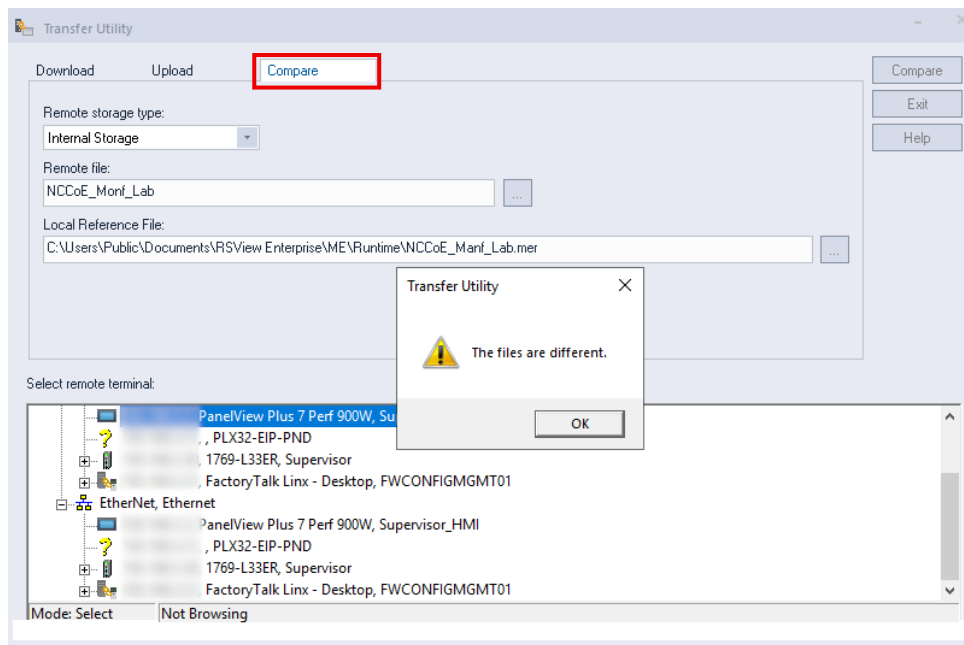
1764 The Upload tab of Rockwell’s Transfer Utility can be used to see which files are stored on the HMI.



1765 **Figure 4-44: Selecting the file to upload using Rockwell’s Transfer Utility**

1766 The “Compare” tab of Rockwell Automation’s Transfer Utility allows the user to determine that the file  
 1767 running on the HMI is different than the desired file found on the Engineering Workstation.

1768 In the following example, the .mer configuration file from backup is compared with the running or  
 1769 “Remote file”:



1770 **Figure 4-45: Comparing files using Rockwell’s Transfer Utility**

1771 [\[Return to Scenario A\]](#)

1772 **C.2.6 Rockwell Automation FactoryTalk® AssetCentre, Log Review**

1773 AssetCentre’s Event and Audit logs show us **who** was moving files, **when** the files were moved, and the  
 1774 **filename** of the malicious file that was transferred. The screenshot below shows the Event log where the  
 1775 malicious file download was initiated:

Logged Time	Occurred Time	Source	Location	Severity	Message
1/24/2025 1:13:31	1/24/2025 2:55:07 P	FactoryTalk Linx	Supervisor_HMI	Warning	Driver AB_ETHIP-1 failed to bind the listening TCP socket( port 10048), socket error = 0x00a8b849
1/24/2025 1:13:31	1/24/2025 2:55:07 P	FactoryTalk Linx	Supervisor_HMI	Information	Driver Ethernet starts to listen to EtherNet/IP TCP port (492262316) from (null)
1/24/2025 1:13:31	1/24/2025 2:55:06 P	FactoryTalk Linx	Supervisor_HMI	Information	Gateway Protocol startup complete. %0
1/24/2025 1:13:31	1/24/2025 2:55:06 P	FactoryTalk Linx	Supervisor_HMI	Information	Gateway Protocol startup in process. %0
1/24/2025 1:13:31	1/24/2025 2:55:04 P	FactoryTalk Linx	Supervisor_HMI	Information	FactoryTalk Linx: Configuration files will be read from folder 'Windows'
1/24/2025 1:13:30	1/24/2025 2:55:00 P	FactoryTalk Linx	Supervisor_HMI	Information	FactoryTalk Linx runtime service is starting.
1/24/2025 1:11:30	1/24/2025 2:52:06 P	FactoryTalk Linx	Supervisor_HMI	Information	(Download) Transfer instance number 1 completed.
1/24/2025 1:11:30	1/24/2025 2:52:02 P	FactoryTalk Diag	Supervisor_HMI	Information	Connection to remote destination computer has been restored.
1/24/2025 1:11:30	1/24/2025 2:52:02 P	FactoryTalk Linx	Supervisor_HMI	Information	(Download) Initiate transfer of file 'Application Data\Rockwell Software\RSViewMERuntime\NCCoE_Monf

1776 **Figure 4-46: Blue line indicating the malicious file name and date of occurrence**

1777 The Audit log can be used to find the user who might have been logged in during this period. It is shown  
 1778 in the following log that there was only one user who had logged in while the malicious transfer  
 1779 occurred:

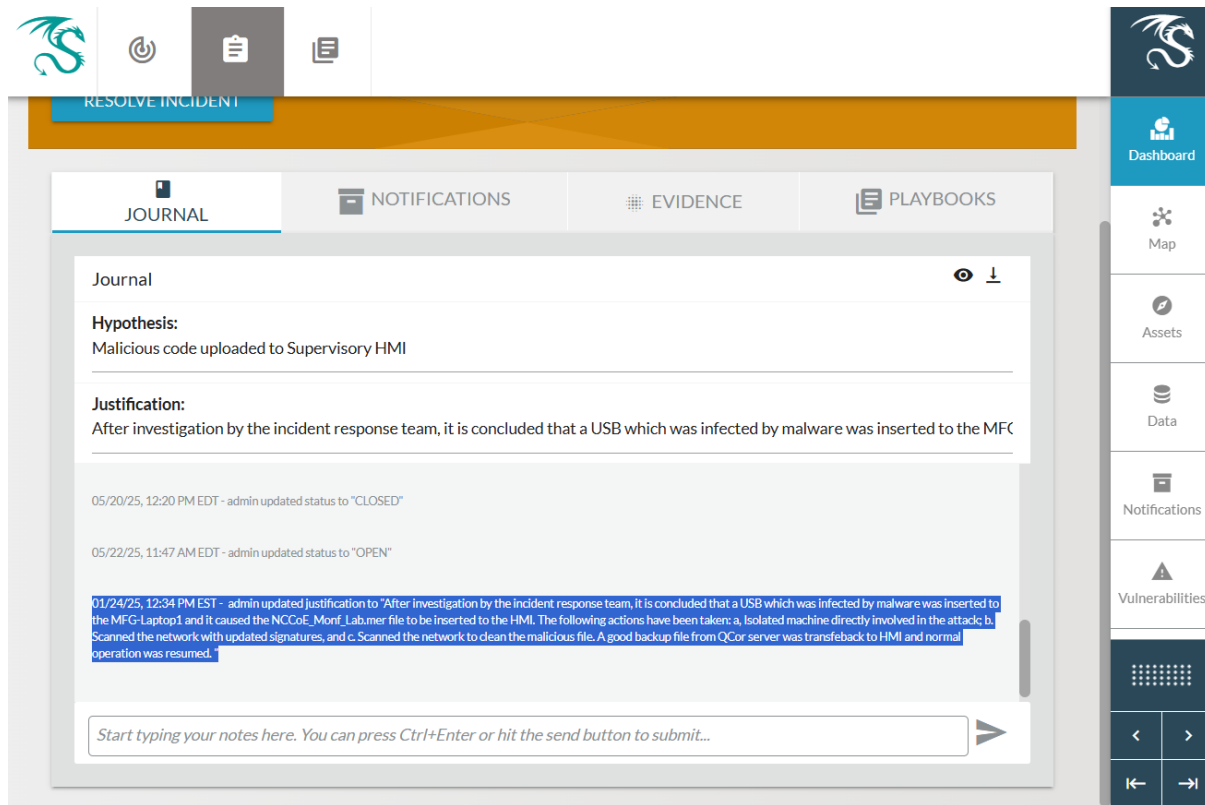
Logged Time	Occurred Time	Source	Location	Resource	Username	Message
1/24/2025 1:13:41	1/24/2025 2:55:21 P	FactoryTalk View	Supervisor_HMI		FactoryTalk Servi	Write 'Friday, January 24, 2025 11:55:21 AM' to 'system\AlarmResetDateAndTimeString'
1/24/2025 1:13:41	1/24/2025 2:55:21 P	FactoryTalk View	Supervisor_HMI		FactoryTalk Servi	Write 'DEFAULT' to 'System\User'.
1/24/2025 11:57:4	1/23/2025 11:04:37	FactoryTalk Secu	SUPERVISOR-SVR	Network	MFG\SSARAVIA [	Successful login of user [MFG\SSARAVIA] on directory [Network]
1/24/2025 11:29:1	1/24/2025 11:29:07	FactoryTalk Secu	MFG-LAPTOP1	Network	Stephanie Saravi	Successful login of user [MFG\SSARAVIA] on directory [Network]

1780 **Figure 4-47: Audit log showing which users logged in recently**

1781 [\[Return to Scenario A\]](#)

1782 **C.2.7 Update Dragos Case**

1783 During the investigation, more evidence can be recorded in the case management. In our case, the  
 1784 following evidence was recorded:

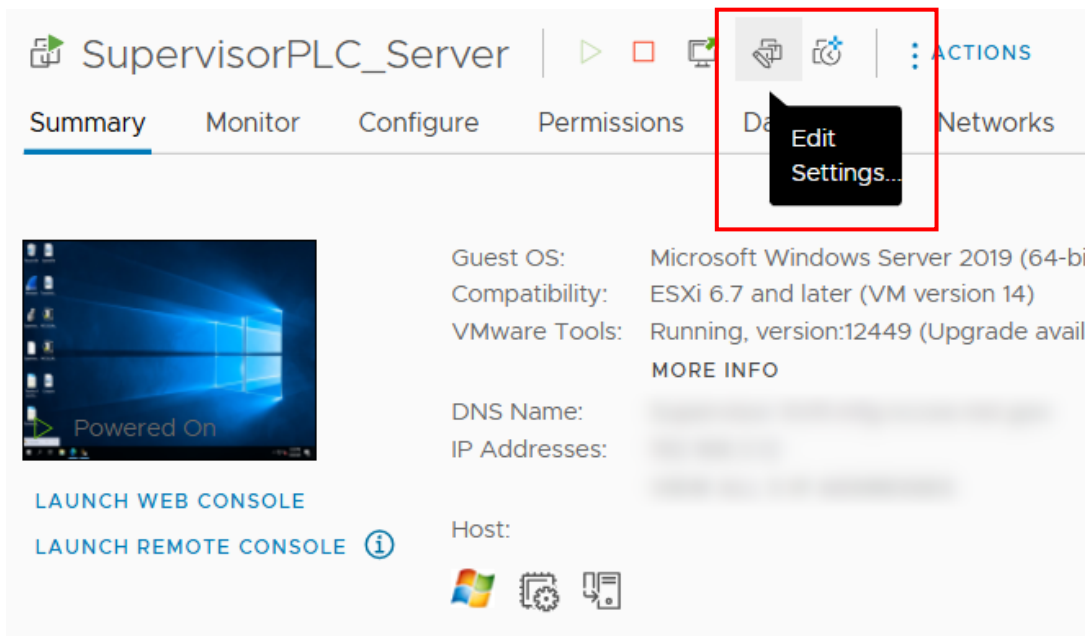


1785 **Figure 4-48: Updating a Dragos ticket with a new comment**

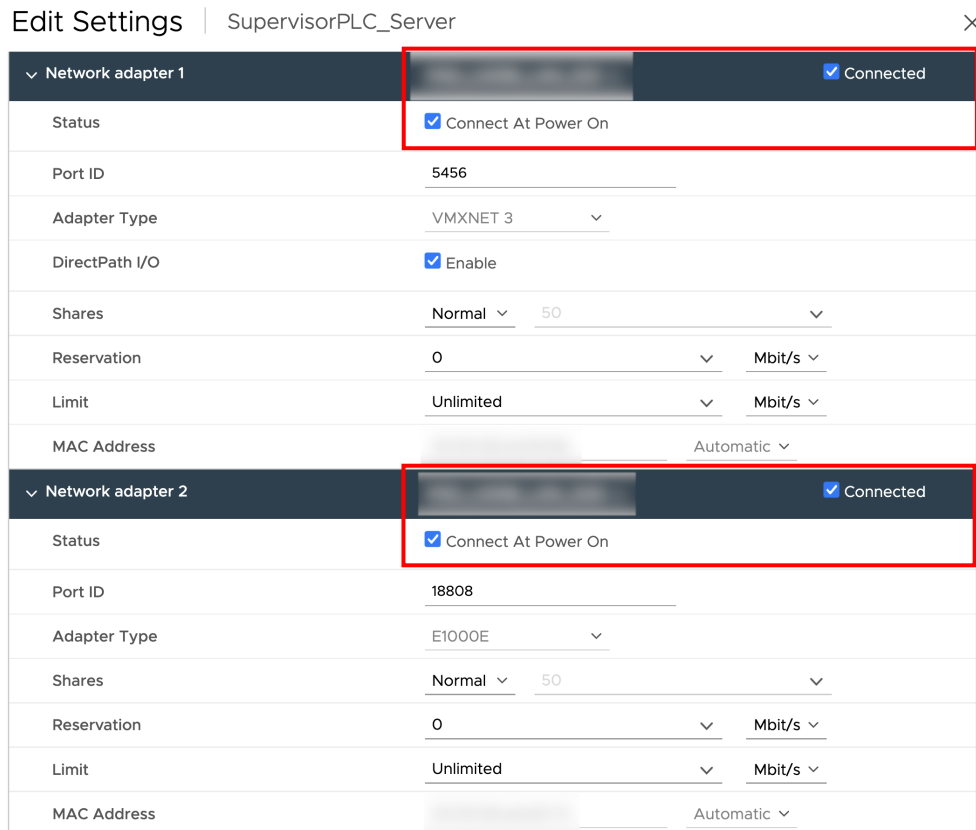
1786 [\[Return to Scenario A\]](#)

## 1787 C.2.8 Remove Virtual Machine from Network

1788 For all scenarios, vSphere was used for the infrastructure of the virtual machines (VMs) (not including  
 1789 AWS). To isolate a virtual machine within a vSphere environment, log into vCenter and find the  
 1790 corresponding VM to remove from the network. The following screenshots provide a step-by-step guide.  
 1791 It starts by demonstrating how to access the VM settings from its `summary` page, then indicates the  
 1792 location of the network settings and the boxes to uncheck. Once these boxes are unchecked, the VM will  
 1793 be disconnected from all networks and will remain disconnected until the virtual NIC is re-enabled:



1794 **Figure 4-49: Highlighting the Edit Settings button for a virtual machine (VM) in vCenter**



1795 **Figure 4-50: Highlighting where to turn off network adapters for VMs in Edit Settings**

Edit Settings | SupervisorPLC\_Server ×

<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Network adapter 1 *</span> <span style="background-color: #ccc; padding: 2px;">[Redacted]</span> <span>Connected</span> </div>	
Status	<input type="checkbox"/> Connect At Power On
Port ID	5456
Adapter Type	VMXNET 3
DirectPath I/O	<input checked="" type="checkbox"/> Enable
Shares	Normal 50
Reservation	0 Mbit/s
Limit	Unlimited Mbit/s
MAC Address	[Redacted] Automatic
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Network adapter 2 *</span> <span style="background-color: #ccc; padding: 2px;">[Redacted]</span> <span>Connected</span> </div>	
Status	<input type="checkbox"/> Connect At Power On
Port ID	18808
Adapter Type	E1000E
Shares	Normal 50
Reservation	0 Mbit/s
Limit	Unlimited Mbit/s
MAC Address	[Redacted] Automatic

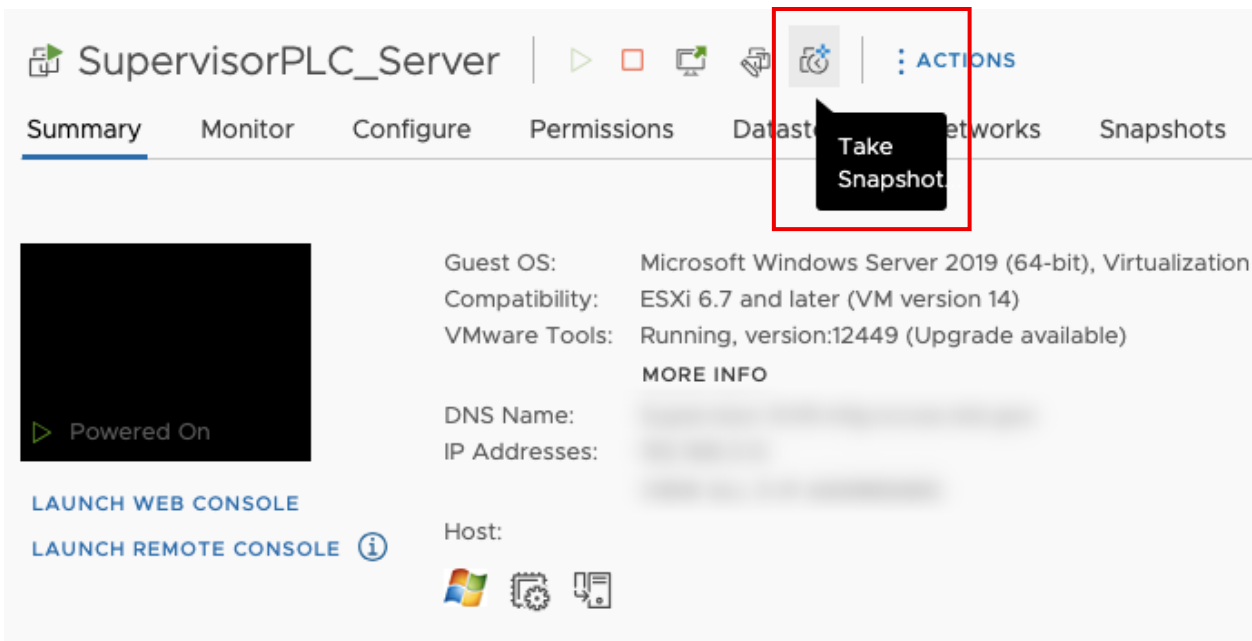
1796 **Figure 4-51: Network settings for a VM turned off in Edit Settings**

1797 [\[Return to Scenario A\]](#)

1798 [\[Return to C.5.6 - Disconnect JumpHost VM from Network\]](#)

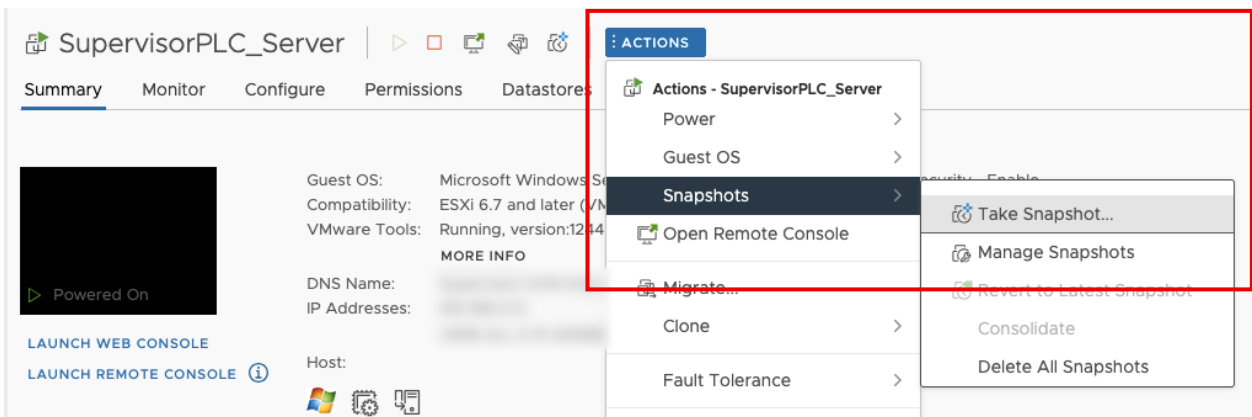
### 1799 C.2.9 Taking Snapshots of VMs

1800 For forensic purposes, the IRT takes a snapshot of the virtual machine. To perform this task, find the  
 1801 Take Snapshot button in the VM's Summary page.



1802 **Figure 4-52: The Take Snapshot button on a VM's settings page**

1803 Users can also click the Actions button and find it in a context menu:



1804 **Figure 4-53: The Take Snapshot button in the Actions context menu**

1805 When taking the snapshot, change the name and add a description. Be sure to include the VM's  
1806 memory:

## Take snapshot ×

Name Compromised\_HMI\_Snapshot

Description 

For forensics purposes, this snapshot was created after the incident (see Dragos case "HMI Compromise")



Include virtual machine's memory

Quiesce guest file system(requires VM tools)

CANCEL
CREATE

1807 **Figure 4-54: Entering details for the snapshot to be created**

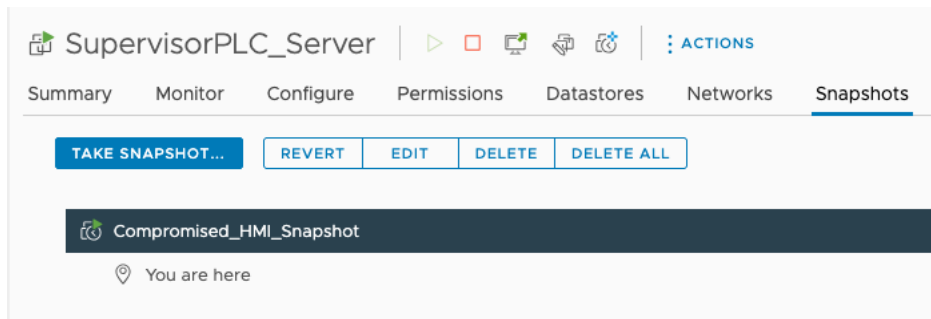
1808 In vCenter's tasks at the bottom of the interface, the progress of the snapshot is shown as a Status:

Recent Tasks		Alarms	
Task Name	Target	Status	
Create virtual machine sn...	 SupervisorPLC_Serv...	<div style="width: 16%; height: 10px; background-color: #0070c0;"></div> 16%	

1809 **Figure 4-55: Snapshot progress in vCenter**

1810 Looking at the VM's settings screen, select the Snapshots tab to find all the current snapshots.

1811 *Note: A snapshot can also be taken from this tab:*



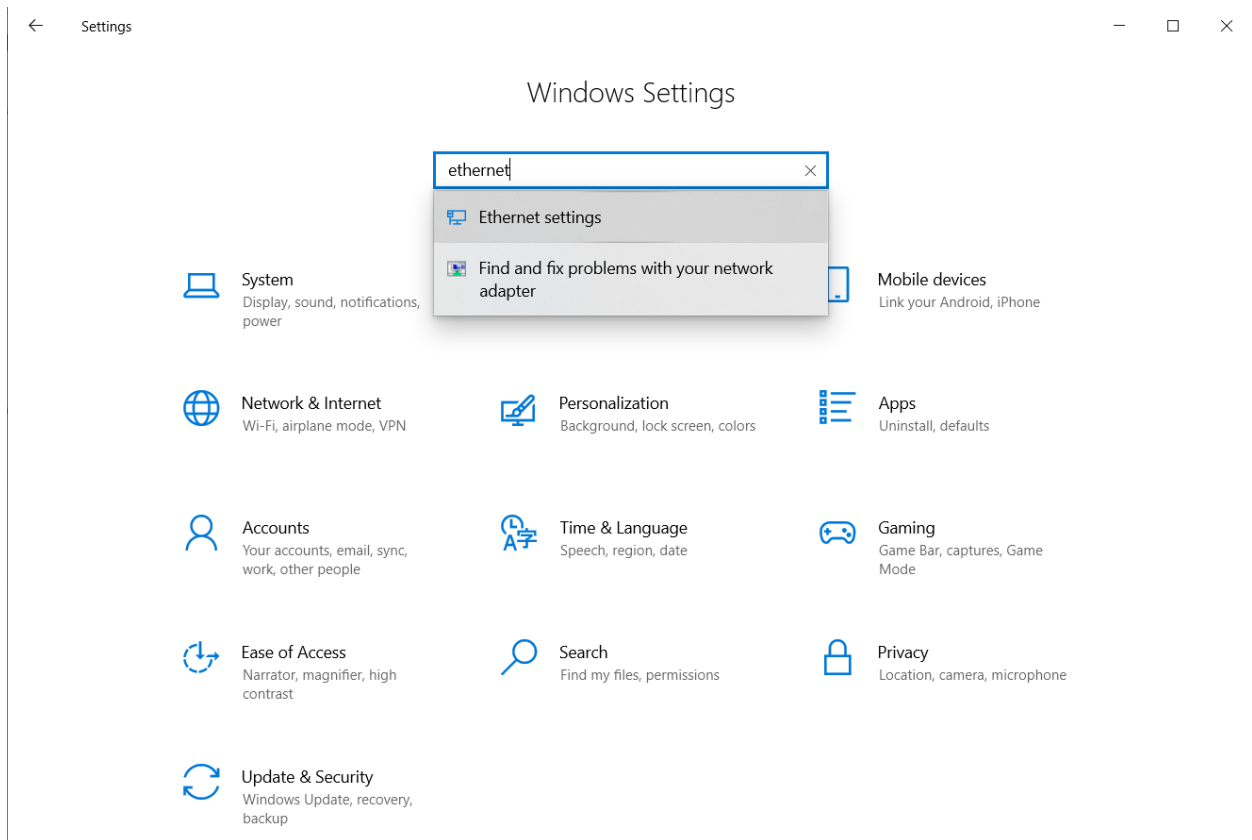
1812 **Figure 4-56: Snapshots in the VM’s settings in vCenter**

1813 [\[Return to Scenario A\]](#)

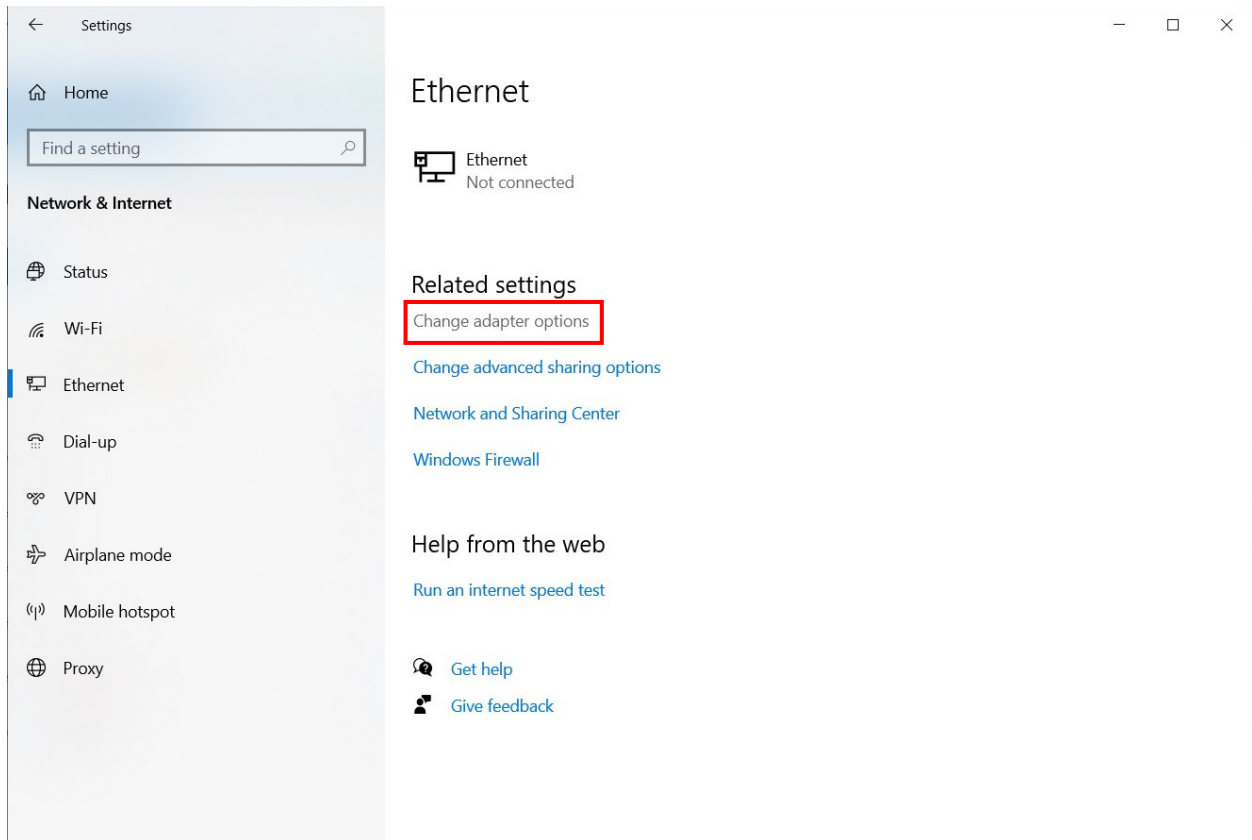
1814 [\[Return to C.5.7 - Take Snapshot of JumpHost VM\]](#)

1815 **C.2.10 Remove Physical Device from the Network**

1816 To disconnect a physical device, such as a laptop, from the network, all network adapters should be  
 1817 disabled. On Windows operating systems, this can be done by going to Ethernet settings, clicking  
 1818 on Change adapter options, and right-clicking each active network connection to select  
 1819 Disable. The following screenshots illustrate how to complete this.

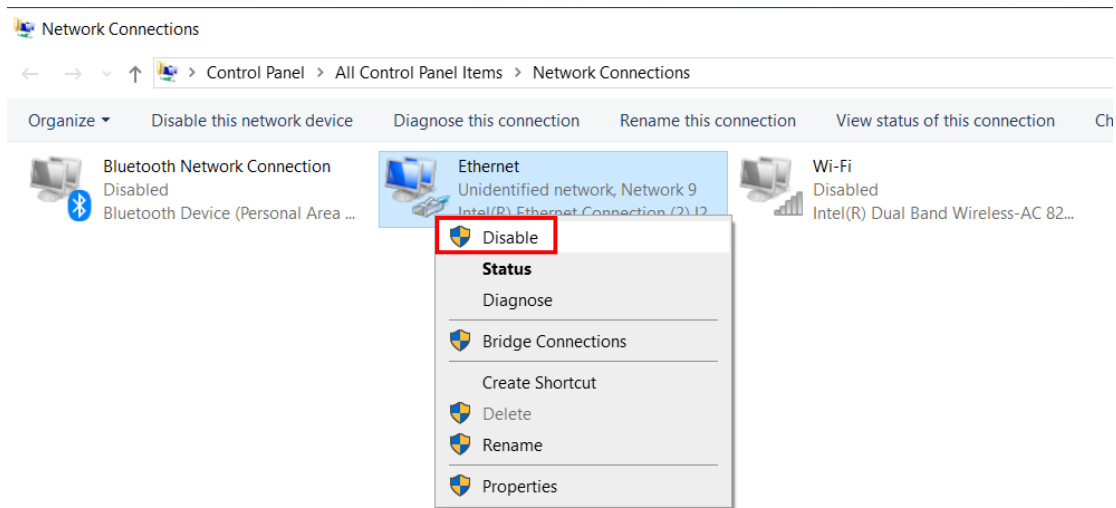


1820 **Figure 4-57: Windows Settings window, searching for “Ethernet settings”**



1821

Figure 4-58: Highlighting “Change adapter options” in Ethernet settings



1822

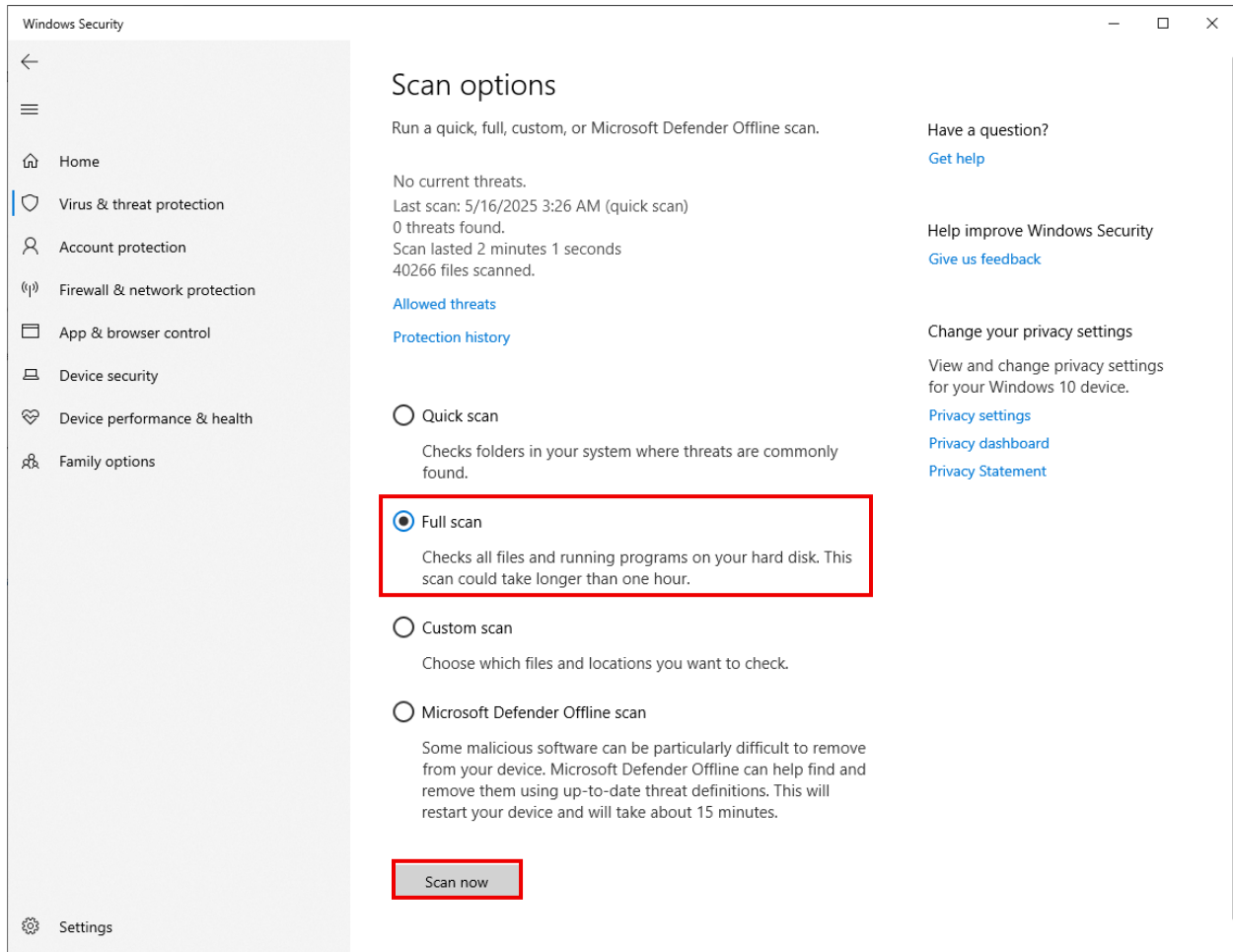
Figure 4-59: Disabling the unwanted Ethernet adapter in Network Settings on Windows

1823

[\[Return to Scenario A\]](#)

1824 **C.2.11 Antivirus Scan**

1825 Run full antivirus scans of all machines on the network. Windows Defender was used on the  
 1826 manufacturing lab workstations.

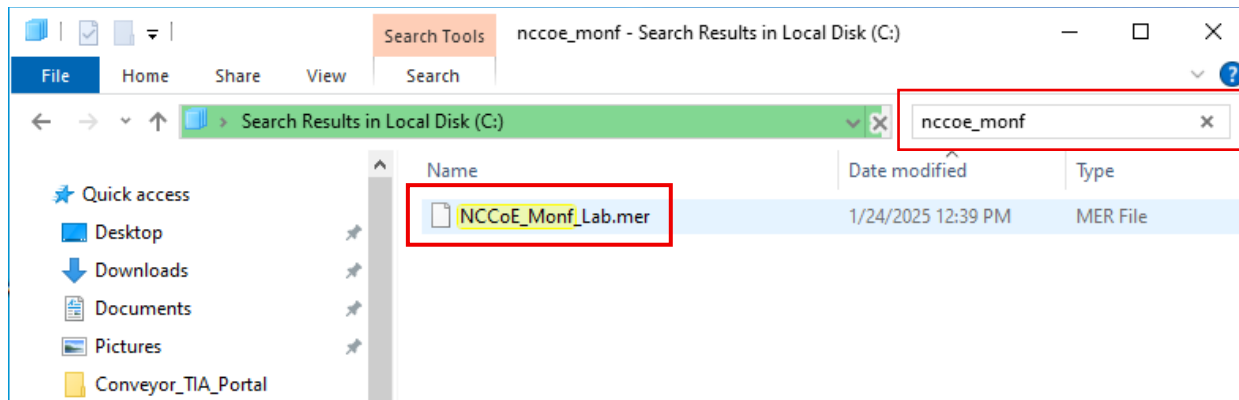


1827 **Figure 4-60: Performing a “Full scan” in the “Virus & threat protection” tab of Windows Security**

1828 [\[Return to Scenario A\]](#)

1829 **C.2.12 Search for Malicious File**

1830 In the absence of tools or scripts, a manual process can be used to search for the malicious file using File  
 1831 Explorer.



1832 **Figure 4-61: Searching for a malicious “.mer” configuration file in Windows**

1833 [\[Return to Scenario A\]](#)

### 1834 C.2.13 Script for Finding Malicious File

1835 Antivirus software may not catch the malicious file if it is not yet known to be malicious. In Scenario A,  
 1836 the user is aware that the HMI was impacted by this file. The next step is to search the network for simi-  
 1837 lar configuration files, such as a .mer file, to see if other machines have been similarly impacted.

1838 To address this, a PowerShell script can be run on IT or engineering workstations to scan all files for a  
 1839 suspicious configuration file. In Scenario A, this script was developed to search for the specific malicious  
 1840 file:

```
<#
Utilizing variables, we can assign specific computers and
file names to search for. In this case, we're searching
for the "Monf" file to see anywhere else this file might be.
#>

$computer = "localhost"
$fileName = "NCCoE_Monf_Lab.mer"

Invoke-Command -ComputerName $computer -ScriptBlock {
    Get-ChildItem -Path C:\ -Recurse -Filter $using:fileName -ErrorAction SilentlyContinue
}
```

1841 **Figure 4-62: Custom script for searching the entire C:\ drive for a specific file**

1842 *Note: To search for every .mer file, change the fileName variable to \*.mer*

1843 Once able, run the script:

```

Select Administrator: Windows PowerShell
PS C:\Manufacturing\Scripts> .\simple-file-search.ps1

Directory: C:\Manufacturing\Supervisory_PLC

Mode                LastWriteTime         Length Name                                           PSComputerName
-----                -
-a----             1/24/2025 12:39 PM      2574852 NCCoE_Monf_Lab.mer                          localhost
PS C:\Manufacturing\Scripts>

```

1844 **Figure 4-63: Output of running the custom script, showing all files with that specific name**

1845 In this scenario, the malicious configuration file has an obvious name. A more thorough method for  
 1846 identifying a malicious file is to manage the integrity of known clean files. This can be achieved by main-  
 1847 taining a list of SHA-256 hashes for all known clean files. In the following set of screenshots, the user  
 1848 confirms the SHA-256 hash of the malicious configuration file and then runs a script that will search for a  
 1849 file based on its file extension and SHA-256 hash.

1850 Here is an example script designed to search for a file using the file hash:

```

$hashOfFileYourLookingfor = "0028A088BBA7F8715B4E657608045D38AF8896B9C25C98BF83A47BDF1170FEDB"

Get-ChildItem -Path C:\ -Filter *.mer -Recurse -ErrorAction SilentlyContinue | ForEach-Object{
    #scoping search to .mer files|

    #get location of files in the folder
    $fullfolderpath = $_.FullName

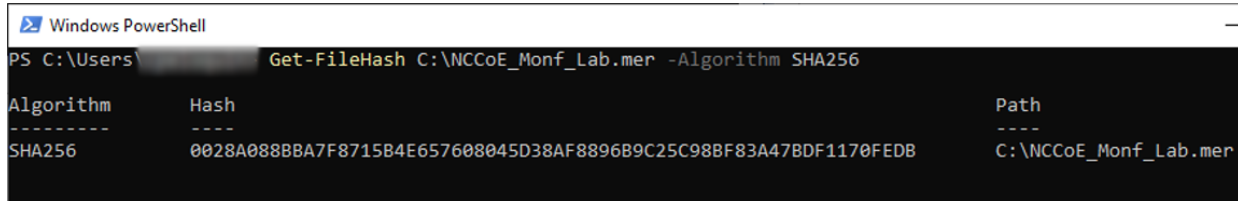
    #get the hash of the file
    $fileHash = Get-FileHash $fullfolderpath |select -expandproperty hash

    #give alert if the file is found
    if($filehash -eq $hashOfFileYourLookingfor){
        Write-Host "File is located at $fullfolderpath"
    }
}

```

1851 **Figure 4-64: Custom script to search through a computer to find a file based on a cryptographic hash**

1852 Prior to running the script, the hash of the malicious file must be collected.



```

Windows PowerShell
PS C:\Users\ > Get-FileHash C:\NCCoE_Monf_Lab.mer -Algorithm SHA256

Algorithm      Hash
-----
SHA256         0028A088BBA7F8715B4E657608045D38AF8896B9C25C98BF83A47BDF1170FEDB
Path
-----
C:\NCCoE_Monf_Lab.mer

```

1853 **Figure 4-65: Taking a cryptographic hash of the suspected malicious file to find any variants**

1854 This hash will then be inserted into the script file by replacing the `$hashOfFileYouAreLookingfor`  
 1855 variable with the SHA256 hash:

```

#hash value you are looking for
$hashOfFileYouAreLookingfor = "0028A088BBA7F8715B4E657608045D38AF8896B9C25C98BF83A47BDF1170FEDB"

Get-ChildItem -Path C:\ -Filter *.mer -Recurse -ErrorAction SilentlyContinue | ForEach-Object{
    #scoping search to .mer files|

    #get location of files in the folder
    $fullfolderpath = $_.FullName

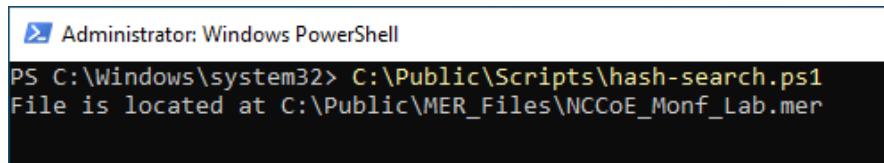
    #get the hash of the file
    $fileHash = Get-FileHash $fullfolderpath |select -expandproperty hash

    #give alert if the file is found
    if($filehash -eq $hashOfFileYouAreLookingfor){
        Write-Host "File is located at $fullfolderpath"
    }
}

```

1856 **Figure 4-66: Inputting the hash of the file users want to search for**

1857 Once able, run the script. If the hashes match, it provides an output of the file location on the system:



```

Administrator: Windows PowerShell
PS C:\Windows\system32> C:\Public\Scripts\hash-search.ps1
File is located at C:\Public\MER_Files\NCCoE_Monf_Lab.mer

```

1858 **Figure 4-67: Script output, showing the files that match the hash in the script**

1859 The scripts provided are a starting point. They can and should be edited to best suit the organization.

1860 [\[Return to Scenario A\]](#)

## 1861 C.3 Scenario A: Technical Details – Recovery

### 1862 C.3.1 Downloading Backups from Authoritative Source

1863 Following the incident, system recovery should be initiated by retrieving backups using the configured  
 1864 backup solution. The solution used in this Practice Guide is ForceField. To perform this recovery,  
 1865 navigate to the Forcefield file structure and click on the file name desired for download from the storage  
 1866 device. To recover from the HMI compromise, the engineer downloads the HMI configuration file:

Filename	Ext#	Size	Created
NIST_NCCoE_Logo.jpg	1	33.77K	20240129 16:25:00
20240617 [redacted] running-config.txt	1	18.94K	20240617 12:30:57
20240617 [redacted] running-config.txt	2	18.94K	20240617 12:32:54
20240617 [redacted] running-config.txt	3	75.78K	20240617 12:32:58
.._doc_WFSsvr_User_Guide.pdf	1	1.29M	20240711 13:17:41
_opt_greentec_forcefield_doc_ForceField_WFS_Users_Guide.pdf	1	1.11M	20240711 13:18:30
Dragos_sitstore-config-2024-08-15T19_22_11.573Z.json	1	2.13K	20240822 10:10:28
Tenable_2024-08-15T17_12_59.tar.gz	1	267.82M	20240822 10:10:28
running-config_Cisco-SG550X-48_20240815.txt	1	19.10K	20240822 10:17:50
config_SCALANCE-S600_20240815.conf	1	309.77K	20240822 10:17:50
running-config_AB-Stratix-2500_20240815	1	2.35K	20240822 10:17:51
all_databases_backup-20240822.sql	1	8.58M	20240822 15:14:27
Ignition-Edge-Historian_Ignition-backup-edge20240822-1204.gwbk	1	8.53M	20240822 15:16:21
Ignition-Local-Historian-Gateway_Ignition-backup-20240822-0903.gwbk	1	8.73M	20240822 15:16:35
Ignition-Local-Hist-DB_Ignition-backup-20240822-0856.gwbk	1	8.49M	20240822 15:16:49
Dragos_iLO_2M222403S6_20241126_1619.bak	1	18.76K	20241126 17:18:01
config_SCALANCE_S600 (1).conf	1	309.77K	20241126 17:18:02
Dragos_sensor-config-20241126.json	1	575	20241126 17:18:03
sitstore-config-2024-11-26T17_05_52.757Z.json	1	2.13K	20241126 17:18:03
2024-11-26T16_35_39.tar	1	866.45M	20241126 17:18:04
running-config_Cisco-SG550X-48_20241126.txt	1	19.10K	20241126 17:41:29
config_SCALANCE_S600_20241126.conf	1	309.77K	20241126 17:41:30
running-config_AB-Stratix-2500_20241126	1	2.35K	20241126 17:41:31
NCCoE_Manf_Lab.apa	1	2.82M	20241212 12:33:38
<b>NCCoE_Manf_Lab.mer</b>	1	2.44M	20241212 12:33:43
NCCoE_Manf_Lab_Test.apa	1	2.82M	20241212 12:33:48
running-config-AB-Stratix-2500-20250124.txt	1	2.35K	20250124 14:50:31
hash-search-for-mer-files-FINAL.ps1	1	871	20250124 15:36:46
Ignition-DB-Backup-test.sql	1	55.30M	20250429 13:19:50
Dragos_iLO_2M222403S6.bak	1	18.76K	20250520 10:34:19
30 File Extents on this Volume			

1867 **Figure 4-68: Stored files in ForceField, with the file wanted for the scenario highlighted**

1868 *NOTE: Links on this site will not have visual indicators/feedback, but still work when clicked on.*

1869 Once clicked, a prompt appears to save the file onto the local machine. Be sure the machine performing  
 1870 the action is a clean workstation. Section C.3.2 will explore the options to restore this configuration file  
 1871 to the HMI.

1872 [\[Return to Scenario A\]](#)

### 1873 C.3.2 Restore the HMI

1874 After determining that the HMI is compromised, the HMI device is disconnected from the network.  
1875 Following this, as production has already ceased, the HMI is removed entirely to achieve isolation on the  
1876 process network. A new HMI is procured, and at this time, the approved file from qualified backup  
1877 sources may be loaded.

1878 If any issues arise, a shutdown may be forced on the HMI by placing a probe on the reset pin, located  
1879 physically on the back of the device, labeled as `default`. This will, on reboot, bring the machine to a  
1880 reset menu. This can be exited with the `no changes` option.

1881 Following this, a reboot menu on the HMI panel will display. For Allen Bradley PanelView™ Plus,  
1882 interrupting normal boot operations is performed by either using the touchscreen to engage the white  
1883 box in the bottom left corner or by connecting a keyboard and pressing F1 to enter the boot menu.

1884 When adding a new file to an HMI via USB, it is recommended to follow NIST SP 1334. There are two  
1885 methods of placing said file on the terminal. If the PanelView™ Plus terminal recognizes the external  
1886 storage device, a transfer can occur by navigating to the external storage source in the terminal and  
1887 initiating a file transfer to internal storage. If this is not possible, the file may be placed in the internal  
1888 storage location by exiting the machine edition terminal to the Windows CE environment, copying the  
1889 file from the external storage drive, and copying the file to the location of internal storage.

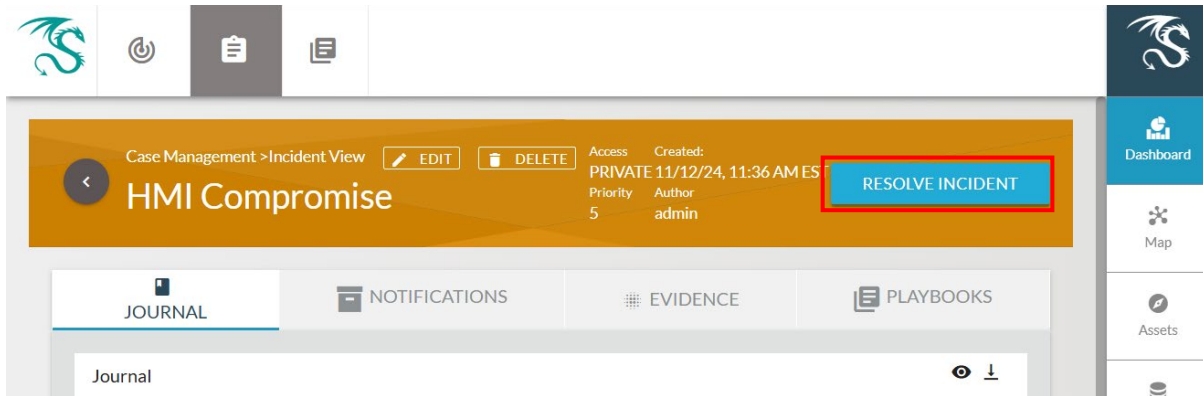
1890 Once the approved file is copied onto the new HMI, the terminal is reloaded, and routine checks are  
1891 performed to ensure all relevant parameters, such as communication, startup preferences, etc., are set.  
1892 The `.mer` configuration file may then be loaded and run on the terminal.

1893 [\[Return to Scenario A\]](#)

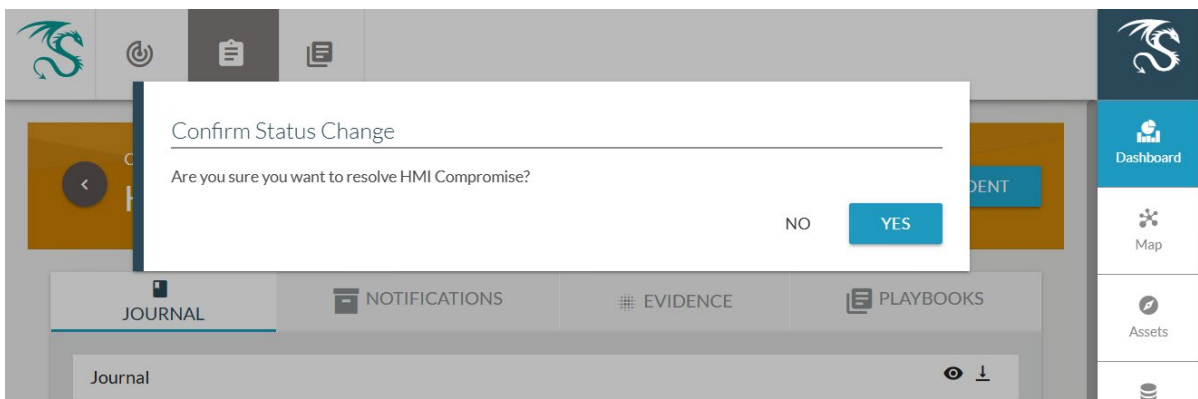
### 1894 C.3.3 Close Dragos Ticket

1895 Once the investigation is finished and the response and recovery have been completed, the case can be  
1896 closed with a proper justification note entered.

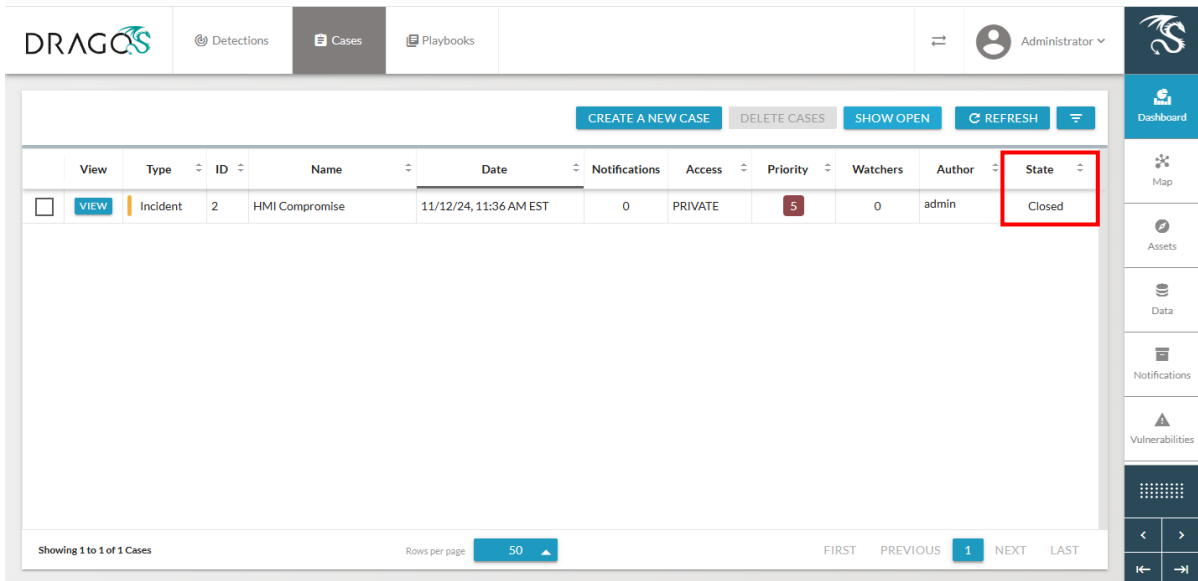
1897 Click the `Resolve Incident` button to close the created case for the incident.



1898 **Figure 4-69: Showing the button in Dragos to resolve an incident for a case**



1899 **Figure 4-70: Confirming the change in the status of the case in Dragos**



1900 **Figure 4-71: Highlighting the new state of the case in Dragos**

1901 [\[Return to Scenario A\]](#)

1902 **C.4 Scenario B: Technical Details – Preparation**

1903 Before an incident occurs, a manufacturer must prepare for incident response and recovery. The  
1904 following steps were taken to prepare for the Scenario B incident.

1905 [\[Return to Scenario B\]](#)

1906 **C.4.1 Configuring Garland to Enable Multiple Detections**

1907 Garland was configured to receive SPAN information from several switches throughout the network and  
1908 send that information to two network sensors, Dragos and Tenable.



1909 **Figure 4-72: Garland hardware configuration**

```

COM5 - PuTTY
Garland Technology INT1G10CSASP (Code Version: 1.1.40)
Power Supply 1: Up
Power Supply 2: Up
Serial Number: ██████████

-----
| Span | Span | Span | Span | Span | Span | Span | Span | Monitoring | |
|Port 1|Port 2|Port 3|Port 4|Port 5|Port 6|Port 7|Port 8|Port 9|Port 10|
|  UP  |  UP  |Down  |Down  |Down  |  UP  |  UP  |  UP  |  UP  |Down  |
| Gbit | Gbit |      |      |      | 100  | 100  | 100  | Gbit |      |
| FULL | FULL |      |      |      | FULL | FULL | FULL | FULL |      |
|      |      |      |      |      |      |      |      |      |      |
-----

Press '0' to return to Main Menu █

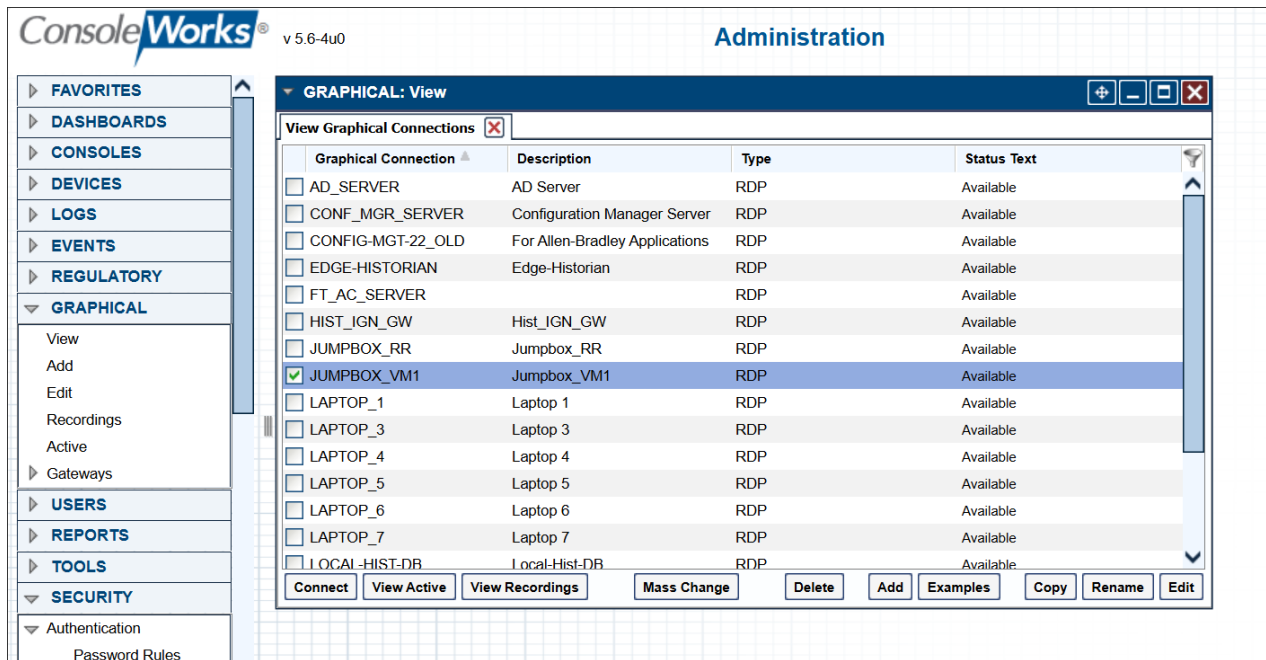
```

1910 **Figure 4-73: Garland software configuration**

1911 [\[Return to Scenario B\]](#)

## 1912 C.4.2 Creating Graphic Interface in ConsoleWorks

1913 The corporate account that's been compromised accesses the OT network through a Jumphost installed  
 1914 in the DMZ between the IT and OT boundary. To protect the assets inside the OT network, all accesses  
 1915 from external networks are required to use the remote access tool's access management interface  
 1916 within ConsoleWorks. Figure 4-74 is the ConsoleWorks Graphic Interface configured for the Jumphost.

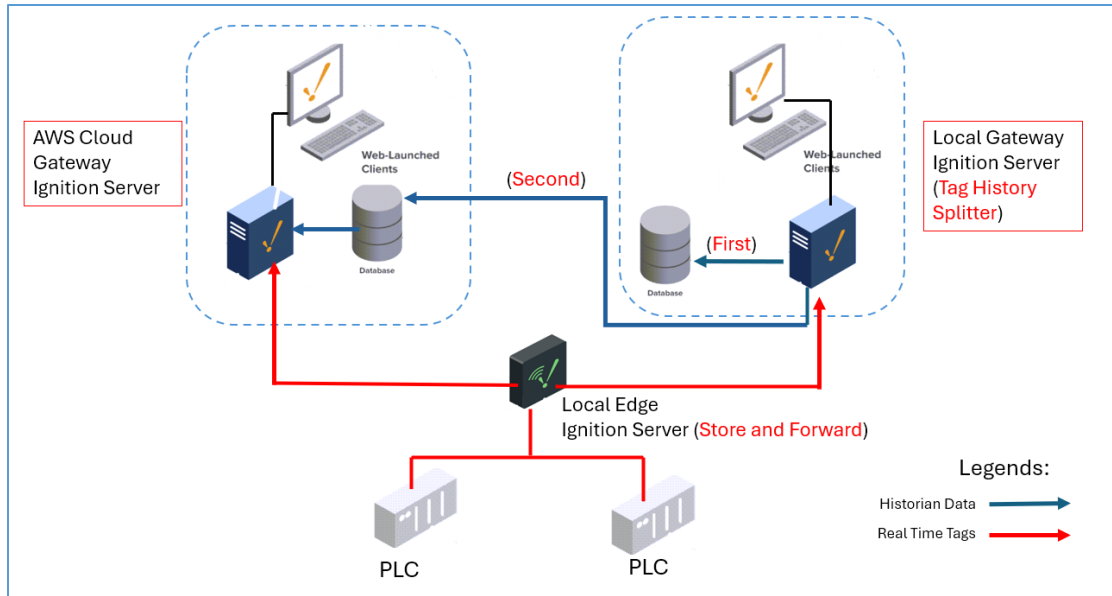


1917 **Figure 4-74: ConsoleWorks configured to provide remote access**

### 1918 C.4.3 Creating a Redundant Ignition Instance in AWS

1919 NCCoE uses the Ignition tag splitter feature to implement redundancy. The Tag History Splitter is useful  
 1920 for automatically creating a backup of operational data. The architecture used in this build that is  
 1921 implementing the tag historian splitter is shown in Figure 4-75. There is one edge Ignition server  
 1922 collecting process data from the controllers, two gateway Ignition servers, and two Database servers.  
 1923 One is called local gateway with a local database for storing historian data sitting in OT DMZ.; the other  
 1924 is called AWS cloud gateway ignition with its own dedicated database also hosted in the cloud server.  
 1925 The Tag History Splitter Provider doesn't store history on its own, but with the proper configuration, the  
 1926 splitter will help to log tag history into multiple databases. The local Edge Ignition server connected to  
 1927 the PLCs is responsible for obtaining the real-time tag data from the PLC. Both the local and cloud  
 1928 Ignition servers are connected directly to the local Edge Ignition server to receive live tag data. The real-  
 1929 time tag data and historian data can be displayed from a web-launched client once the dashboard is  
 1930 built from the Ignition designer.

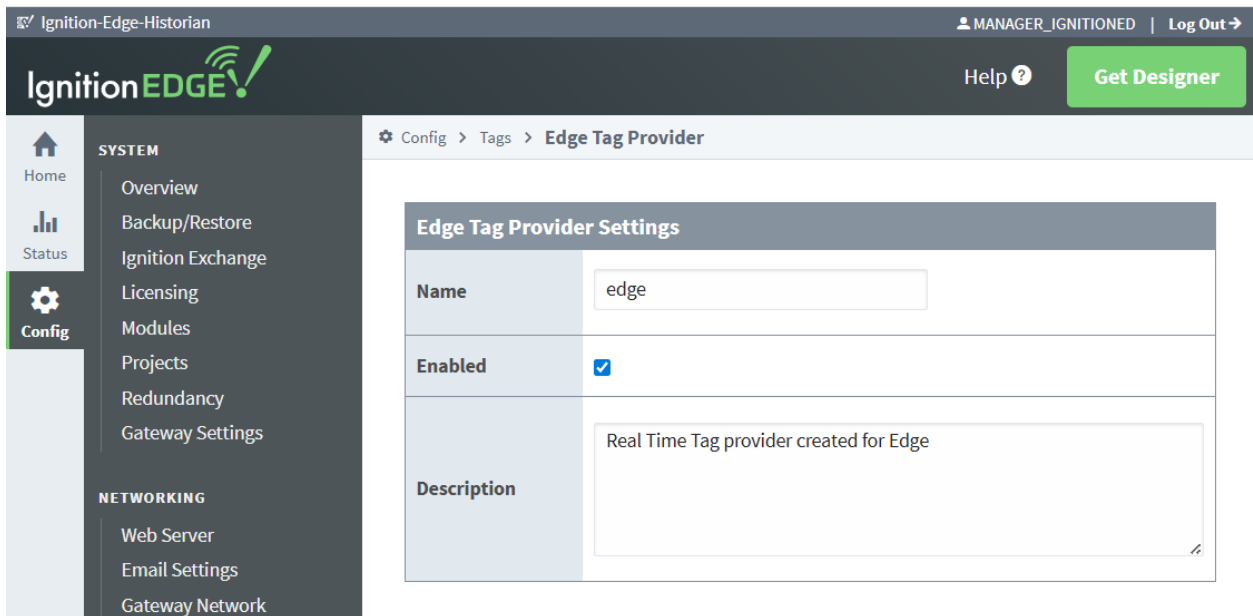
1931 In the event the Local Gateway Server is down, the operational data and the historian data (up to the  
 1932 downtime of the Local Gateway Server) can be viewed in the redundant Web-Launched Client on the  
 1933 cloud.



1934 **Figure 4-75: Ignition historian redundancy architecture using Tag Splitter**

1935 The following procedures are followed to configure the Tag Splitter for Ignition Gateway:

- 1936 • Install Inductive Ignition gateway servers on-premises and in the cloud. Each of the gateway
- 1937 instances is associated with a corresponding PostgreSQL database to store the historian data.
- 1938 • Edge Ignition server is responsible for collecting real-time tag data from the OT devices. The
- 1939 Ignition Edge tag provider can be configured from its web interface. The result setting is shown
- 1940 in the figure below.



1941 **Figure 4-76: Ignition Edge Tag Provider is enabled**

- 1942 • Set the Edge Ignition Server to feed real-time tag data to Ignition gateways. One is called the  
1943 local gateway, and the other is called the cloud gateway, hosted in Amazon AWS. The following  
1944 edge gateway network setting shows that the outgoing connections are pointed to the local  
1945 gateway server and the cloud gateway server to forward real-time tag data.

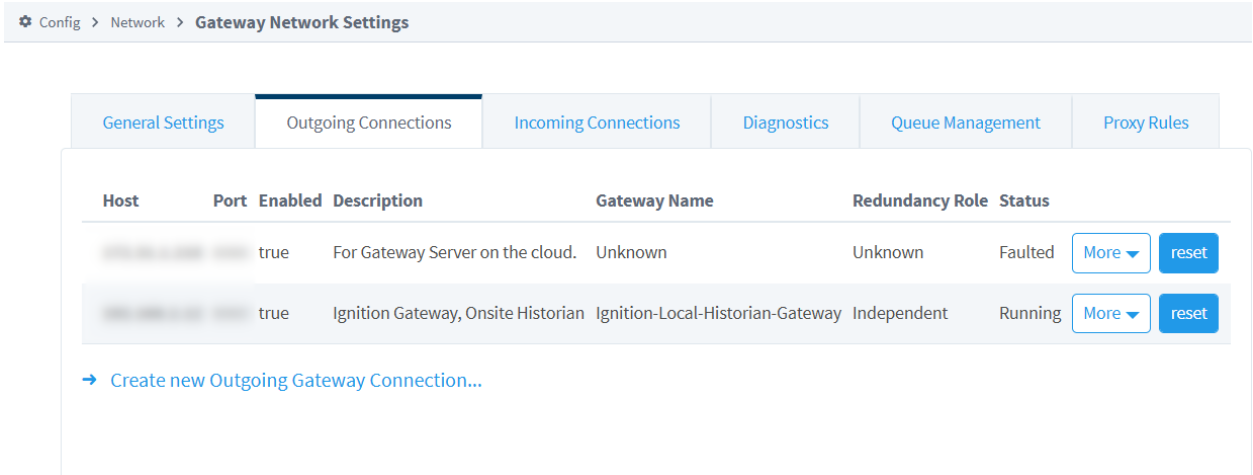


Figure 4-77: Ignition outgoing connections configuration

- 1946 • Set up the local gateway and cloud gateway to receive real-time tag data from the Edge  
1947 Gateway. The gateway network setting for the local gateway is shown below:  
1948

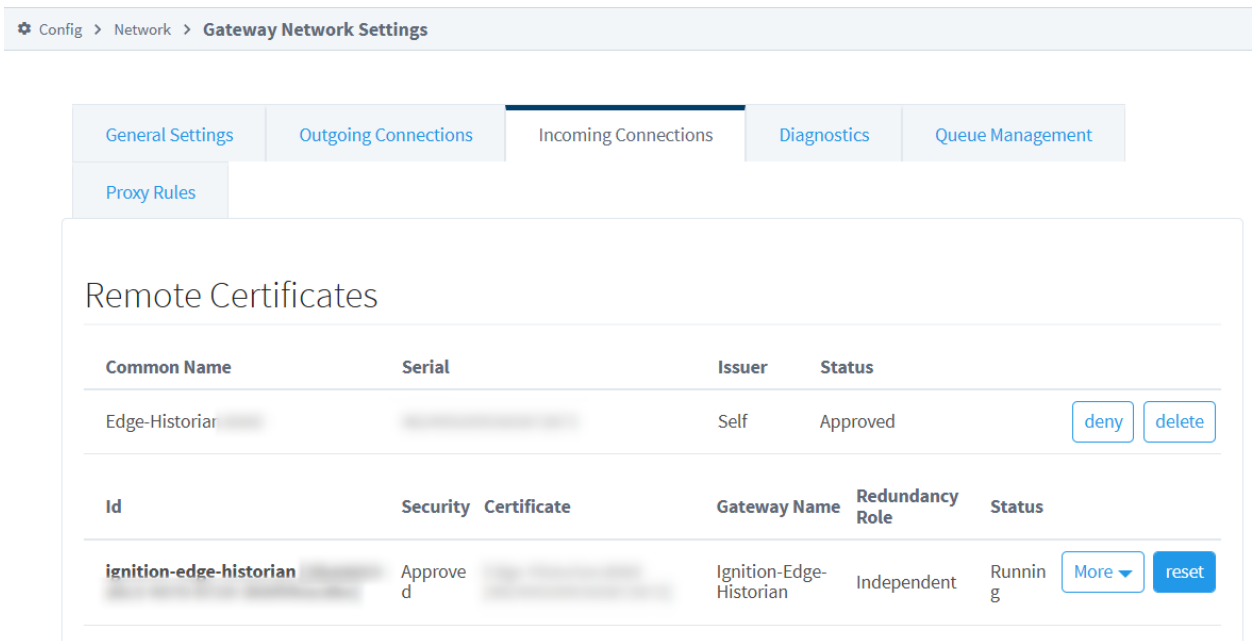


Figure 4-78: Ignition incoming connections configuration

- 1949 • The local gateway Ignition instance is responsible for splitting the tag data for storing in  
1950 different databases. The tag splitting setting is shown below. The Tag Provider called  
1951 TagSplitter is configured to send tag data to two storage locations: IGN\_Hist\_Onsite,  
1952

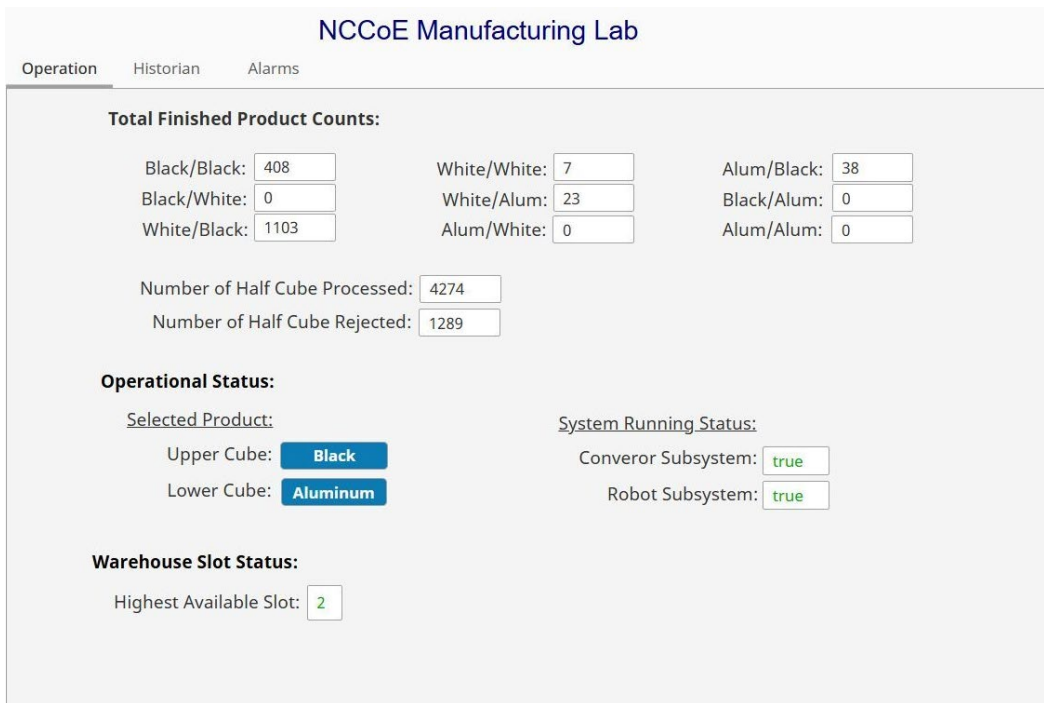
1953 which is the local Ignition database, and IGN\_Hist\_OnCloud, which is the AWS cloud Ignition  
 1954 database.

Config > Tags > History

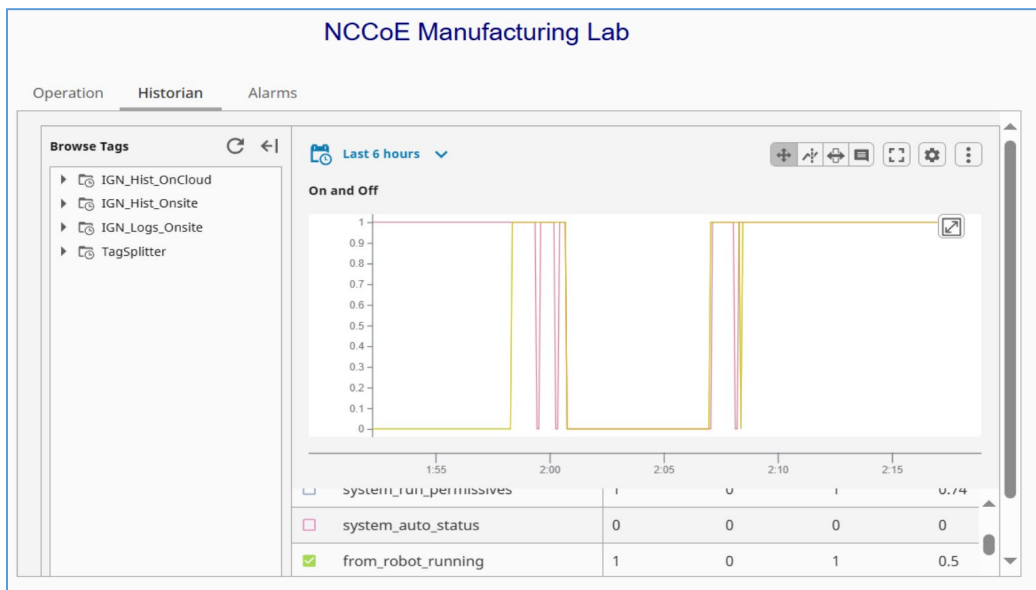
Main	
Provider Name	TagSplitter
Enabled	<input checked="" type="checkbox"/> Enable this tag history provider (default: true)
Description	
Storage	
First Connection	IGN_Hist_Onsite Data is stored to both connections equally. However, all queries execute against the first connection, unless a limit is imposed using the settings below, or the first connection is unavailable.
Second Connection	IGN_Hist_OnCloud

1955 **Figure 4-79: Tag Splitter history settings**

- 1956
- 1957
- 1958
- An Ignition Dashboard is designed to show real-time operation data and historian data. Both the local Ignition Dashboard and the cloud Ignition Dashboard share the same design, and the only difference is that the data are drawn from their associated databases.



1959 **Figure 4-80: Ignition display for real-time operational data**



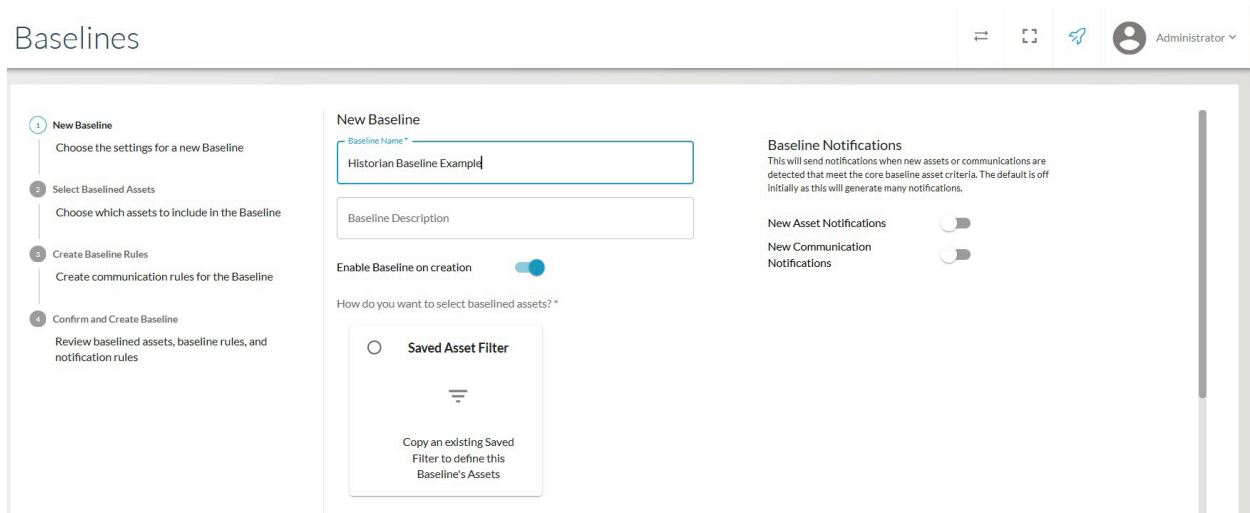
1960 **Figure 4-81: Ignition dashboard for historical data**

1961 [\[Return to Scenario B\]](#)

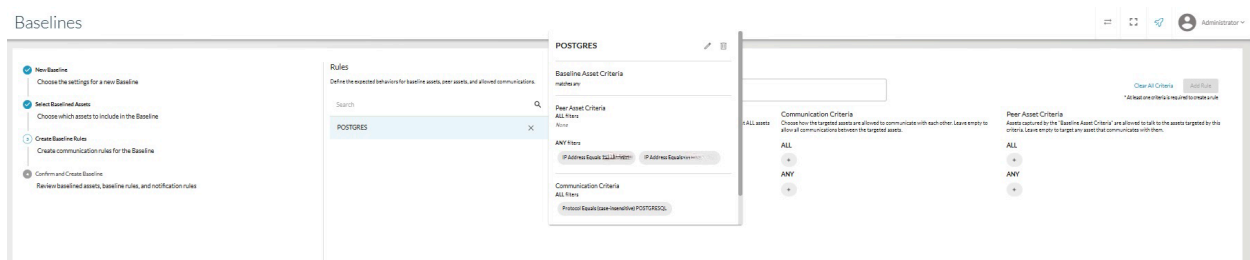
1962 **C.4.4 Creating a Baseline in Dragos**

1963 A new baseline rule is created in Dragos that alerts on any violations of the ruleset. The ruleset is  
 1964 configured to allow PostgreSQL between all devices expected to communicate with the local and cloud  
 1965 historian. Any violation of the baseline rule will generate an alert.

- 1966 The baseline rule is created by navigating to the Baselines section within the Dragos navigation pane.  
 1967 From there, the option Create Baseline is selected. After creating a name for the baseline, as shown in  
 1968 Figure 4-82, scroll down and select Create New Filter. The filter can be customized as shown in Figure  
 1969 4-83 and then saved.



1970 **Figure 4-82: Creating a new Dragos baseline rule**



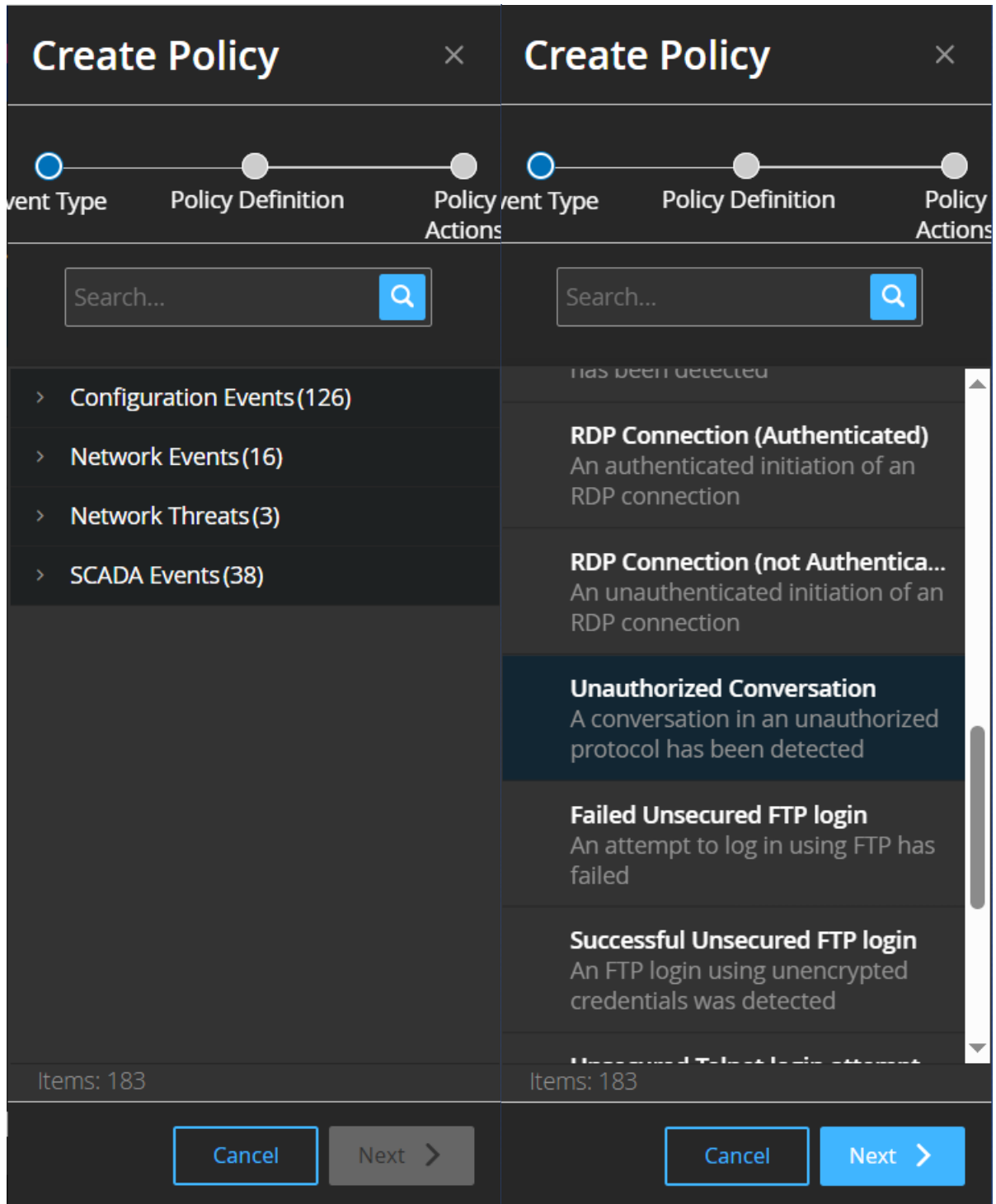
1971 **Figure 4-83: Create a custom criteria for the new rule**

1972 [\[Return to Scenario B\]](#)

### 1973 C.4.5 Creating a Baseline Policy in Tenable

1974 A new baseline policy is created in Tenable OT Security, which alerts on any violations of the ruleset. The  
 1975 ruleset is configured to allow PostgreSQL between all devices expected to communicate with the local  
 1976 and cloud historian. Any violation of the baseline policy will generate an alert.

1977 The baseline policy is created by navigating to the Policies section within the Tenable navigation pane.  
 1978 From there, the option Create Policy is selected. From there, Unauthorized Conversation is selected as  
 1979 shown in Figure 4-84. The rule criteria are entered as shown in Figure 4-85. Figure 4-108 provides a view  
 1980 of the baseline Policy alert within the Tenable OT Security platform.



1981

Figure 4-84: Unauthorized Conversation policy creation in Tenable

**Create Policy** [Close]

Event Type [Checked] Policy Definition [Current] Policy Actions [Unselected]

### Unauthorized Conversation

**POLICY NAME \***  
\*Historian Violation of Access

**SOURCE \***  
In [Dropdown] Select [Button] + Or [Icon] [Trash Icon]  
+ And [Button]

**DESTINATION \***  
In [Dropdown] Select [Button] + Or [Icon] [Trash Icon]  
+ And [Button]

**PROTOCOL \***  
In [Dropdown] Select [Button] [Dropdown]

[Back] [Cancel] [Next]

1982 Figure 4-85: Unauthorized Conversation policy creation in Tenable

1983 [\[Return to Scenario B\]](#)

## 1984 C.4.6 Creating a Splunk Dashboard for SQL protocol Activity

1985 This section discusses the steps of creating a dashboard to track PostgreSQL traffic using logs that are  
1986 coming from both the Tenable and Dragos servers.

1987 Once the detection of a deviation of the baseline has been established within Tenable and Dragos, both  
1988 tools generate notifications that can then be forwarded to Splunk via syslog. Splunk does not natively  
1989 contain a dissector for the logs from Dragos, so users can utilize the Field Extractor tool in Splunk to  
1990 create a custom dissection of the log with the Regular Expression (Regex) option. Users can also  
1991 install the Dragos plugin for Splunk. Logs coming from Tenable were properly dissected already.

### 1992 Dragos

1993 Looking at an initial search for Dragos logs, the dissector does not split the information from this log in a  
1994 way that would be useful for a dashboard:

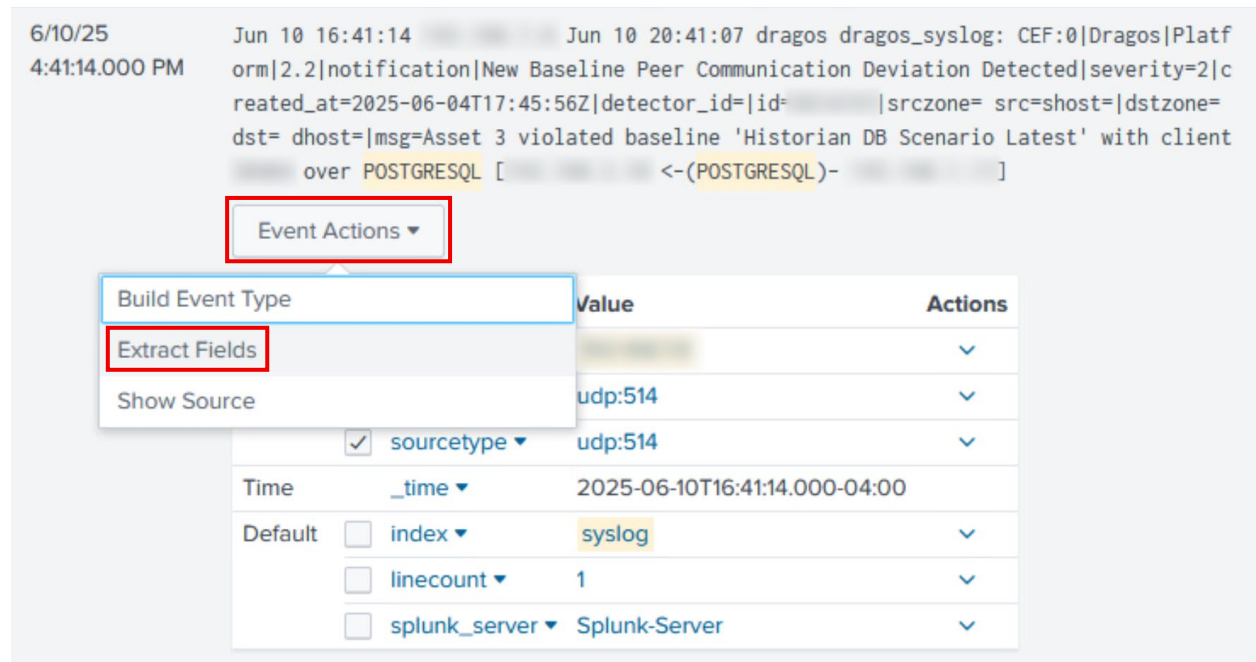
The screenshot shows a Splunk search interface with the following details:

- Search Query: `index="syslog" host= postgresql`
- Time Range: Last 30 days
- Results: 6,366 events (5/25/25 12:00:00.000 AM to 6/24/25 10:03:43.000 AM)
- Event List: 1 event selected
- Event Text: `Jun 10 16:43:14 dragos dragos_syslog: CEF:0|Dragos|Platform|2.2|notification|New Baseline Peer Communication Deviation Detected|severity=2|created_at=2025-06-04T17:45:56Z|detector_id=|id=8|srczone= src=shost=|dstzone= dst= dhost=|msg=Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate' with client over PostgreSQL <-(POSTGRES)-`
- Event Actions:
 

Type	Field	Value	Actions
Selected	host		
	source	udp:514	
	sourcetype	udp:514	
Time	_time	2025-06-10T16:43:14.000-04:00	
Default	index	syslog	
	linecount	1	

1995 **Figure 4-86: A Dragos log showing no dissected fields**

1996 Click on `Event Actions` and then choose the `Extract Fields` option:



1997 **Figure 4-87: Where to find the “Extract Fields” option for this specific log entry**

1998 From here, Splunk provides two options to extract information. The Regex option is chosen for this  
 1999 demonstration. Delimiters are an easier option if the information in the log is specifically set up to do so.  
 2000 For example, the pipe | delimiter can be used, which will search through the log and separate it by the |  
 2001 character. The log chosen in the previous screenshot includes this potential delimiter, but it would  
 2002 include every single line between each pipe | as a Field. The Regex option is chosen to be able to select  
 2003 specific information within the log.

### Select Method

Indicate the method you want to use to extract your field(s). [Learn more](#)  
I prefer to write the regular expression myself >

Source type  
**udp:514**

```
Jun 10 16:41:14 Jun 10 20:41:07 dragos dragos_syslog: CEF:0|Dragos|Platform|2.2|notification|New Baseline Peer Communication  
Deviation Detected|severity=2|created_at=2025-06-04T17:45:56Z|detector_id=id |srczone= src=shost=|dstzone= dst= dhost=|msg=Asset 3  
violated baseline 'Historian DB Scenario Latest' with client over PostgreSQL [ <-(POSTGRESQL)- ]
```



Splunk Enterprise will extract fields using a Regular Expression.

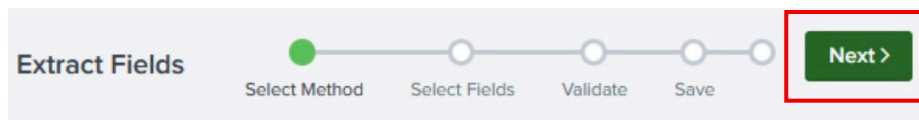
x|y|z

Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

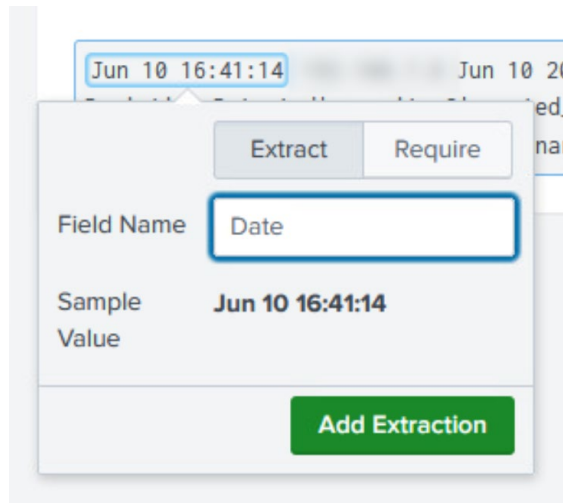
2004 **Figure 4-88: Choosing “Regular Expression” as the field extraction method**

2005 Click **Next** at the top to move to the next section:

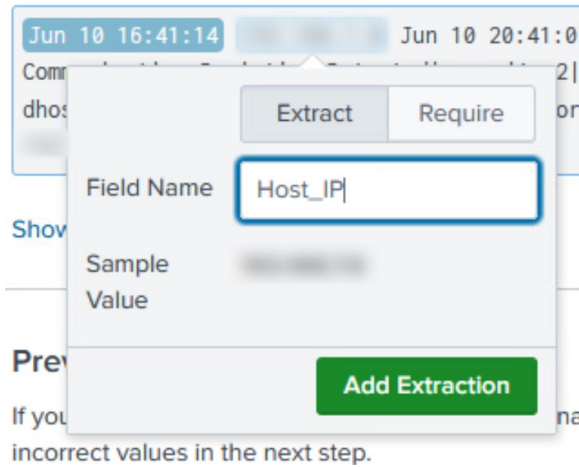


2006 **Figure 4-89: The top bar of the field extractor, click next to go to the next step**

2007 Once in this section, select the portions of the log to be dissected. In the following set of screenshots,  
2008 both the log date and the Dragos server IP address are chosen:



2009 **Figure 4-90: Selecting the first custom line to extract as a field, labeled “Date”**



2010 **Figure 4-91: Selecting second custom line to extract as a field, labeled “Host\_IP”**

2011 Once all the fields are selected, depending on how long the chosen fields are, this error could prevent  
 2012 continuation (highlighted in blue):

```
! Error in 'rex' command: regex="(ms)(P<Date>\w+\s+\d+\s+\d+:\d+:\d+)\s+(?P<Host_IP>[^\s]+)([^\n]*\n)\d+\s+(?P<Type>\w+)[^\n]*\s+(?P<Notification_Type>\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+\s+\w+)[^\n]*\s+(?P<Severity>[^\s]+)\s+(?P<Notification_Creation_Date>[^\s]+)(?P<Notification_ID>\d+)(?P<Baseline>\w+\s+\w+\s+\w+\s+\w+)" with (?P<Client_ID>[a-z]+\s+\d+)\s+\w+\s+\w+\s+(?P<Traffic>+)" has exceeded configured match_limit, consider raising the value in limits.conf
```

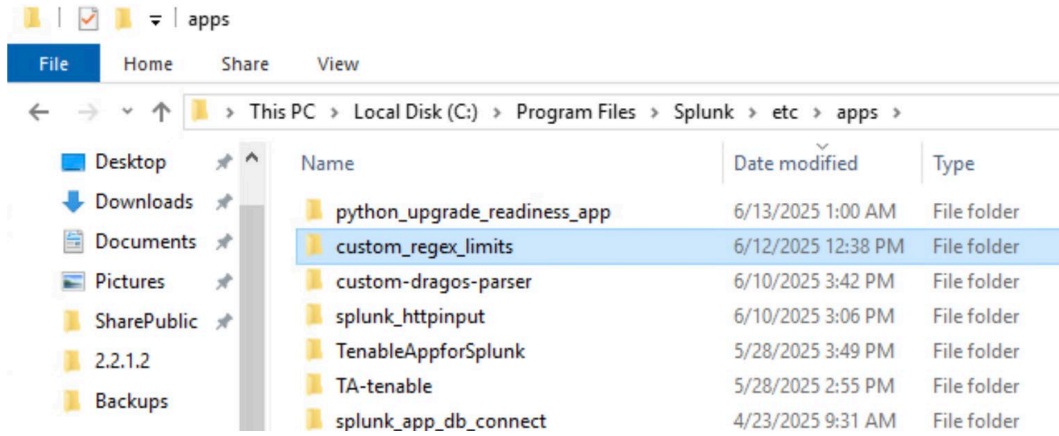
### Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)



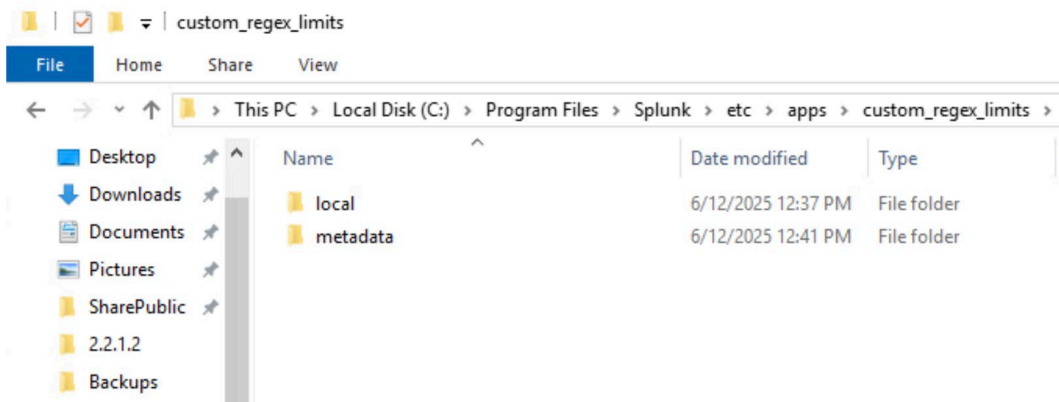
2013 **Figure 4-92: Potential error when selecting too many fields**

2014 The error states “[REGEX] has exceeded configured match\_limit, consider raising the value in  
 2015 limits.conf.” The `limits.conf` file is a system file for Splunk that has default values defined for various  
 2016 variables used in the application. It is best practice to never edit this file, so to fix this, Splunk allows for  
 2017 the creation of custom applications to edit these variables. To create this custom application within  
 2018 Splunk, navigate to the location where Splunk is installed and find the `apps` directory located in the `etc`  
 2019 directory (in this instance: `C:\Program Files\Splunk\etc\apps`). Create a new folder, naming  
 2020 this folder the name of the chosen custom app (in this instance: `custom_regex_limits`):



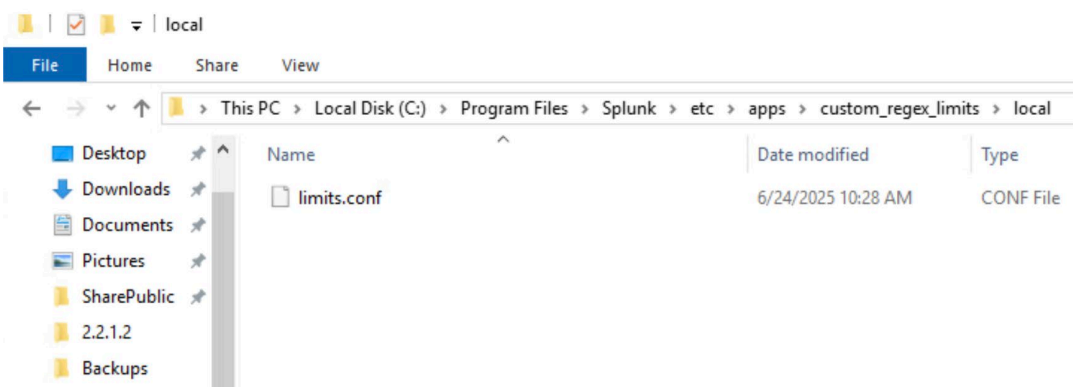
2021 **Figure 4-93: Location of directory to create custom applications in Splunk**

2022 Create two new folders within this new directory, name them `local` and `metadata`:

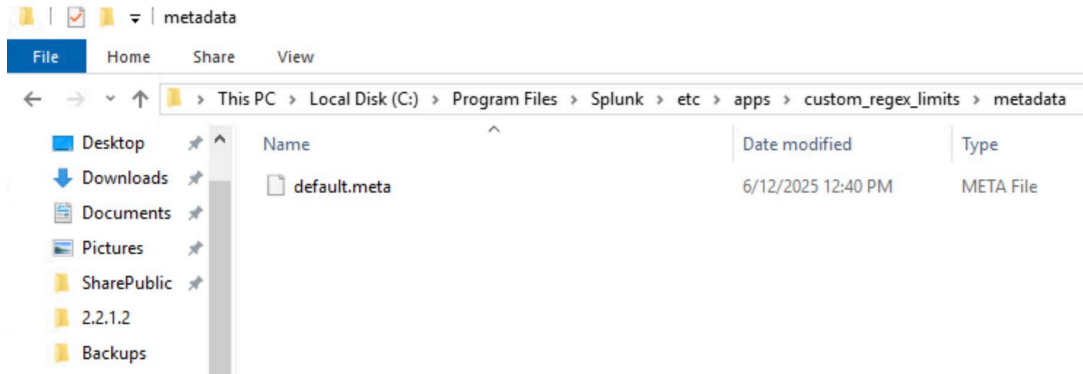


2023 **Figure 4-94: The directory of the custom app, two additional folders created for it**

2024 Within the `local` directory, create the file `limits.conf`, and within the `metadata` directory, create  
 2025 the `default.meta` file:

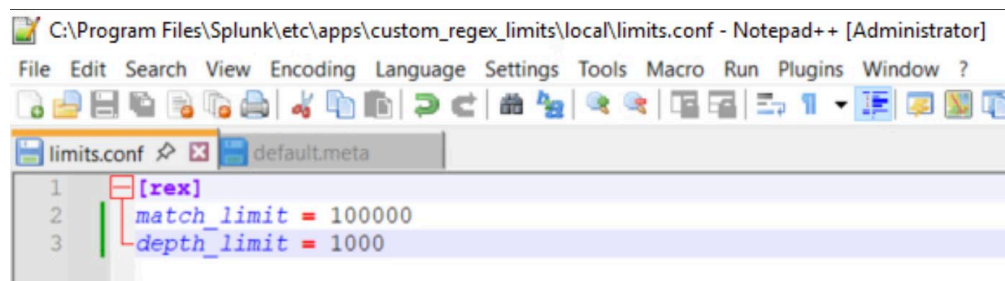


2026 **Figure 4-95: Location of main “limits.conf” file to edit for the custom application**



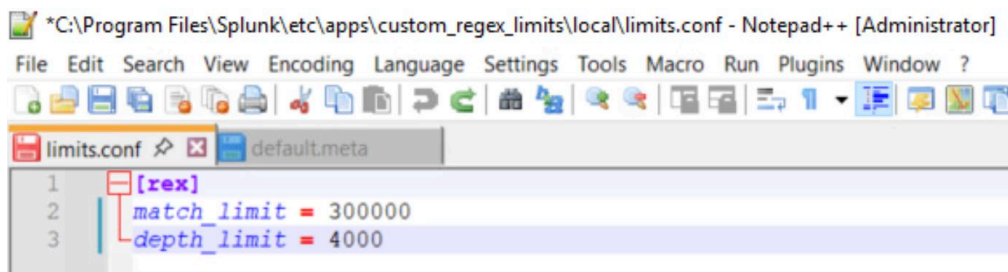
2027 **Figure 4-96: Location of “default.meta” file for the custom application**

2028 The default variable for Regex in the `limits.conf` system file is `rex`. The default values for `rex` are  
 2029 as shown:



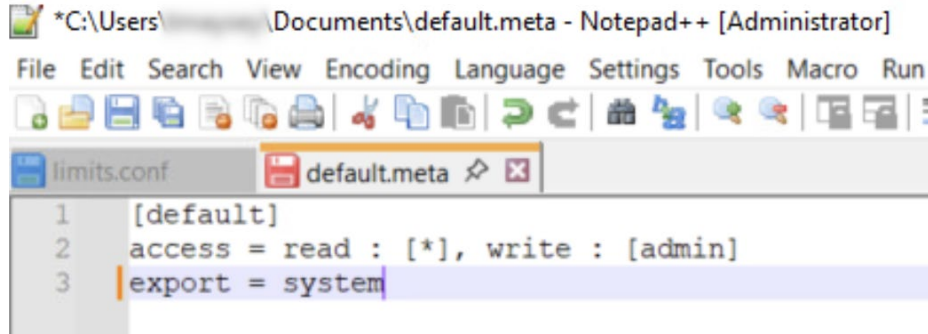
2030 **Figure 4-97: Default values of the “limits.conf” file**

2031 Increase both the `match_limit` and `depth_limit` values to a reasonable value to get the Field  
 2032 Extractor to successfully start the extraction. In this instance, the values that worked are as shown:



2033 **Figure 4-98: New values for the Regex variable, fixing the previous error**

2034 Next, enter the following information into the `default.meta` file. This file defines the metadata for  
 2035 the app, such as the ownership, export settings, and most importantly, the access controls of the app. In  
 2036 the screenshot below, access is set so everyone can read the app, but only admins can create the  
 2037 “views.” The export setting is set to `system`, which means that this custom app will be available to all  
 2038 other apps within Splunk:



2039 **Figure 4-99: Chosen values for “default.meta” file**

2040 Once this is complete, restart the Splunk service.

2041 When re-creating the field extraction, the error is no longer present:



2042 **Figure 4-100: Same extracted fields as before, no more error after increasing Regex limit values**

2043 On the next page, validate the Regex that is produced from this process:

**Validate**

Validate your field extractions and remove values that are incorrectly highlighted in the Events tab. In the field tabs, inspect the extracted values for each field, and optionally click a value to apply it as a search filter to the Events tab event list.



2044 **Figure 4-101: The Regex generated based on the previous field selection portion**

2045 After validated, the next step is to save this so that it can then apply to all logs that match this Regex in

2046 the specified source type:

Extract Fields

< Back

Finish >

## Save

Name the extraction and set permissions.

Extractions Name **EXTRACT-**

Owner **admin**

App **search**

Permissions

Owner

App

All apps

---

Source type **udp:514**

Sample event Jun 10 16:43:14 [redacted] Jun 10 20:43:07 dragos dragos\_syslog: CEF:0|Dragos|Platform|2.2|notification|  
New Baseline Peer Communication Deviation Detected|severity=2|created\_at=2025-06-04T17:45:56Z|  
 detector\_id=id-[redacted]|srczone= src=shost=|dstzone= dst= dhost=msg=Asset 3 violated baseline  
'Historian DB Scenario Latest' with client [redacted] over PostgreSQL [ [redacted] <-(POSTGRESQL)-  
[redacted] ]

Fields **Notification\_Type,Severity,Baseline,Destination\_IP,Protocol,Source\_IP**

Regular Expression `^(?:[^\n]*\.,){4}d+\|w+\|(?P<Notification_Type>[^\|]+)\|severity=(?P<Severity>\d+)[^\n]*"(?P<Baseline>[^\|]+)"[^\n]*\|(?P<Destination_IP>\d+\.\d+\.\d+\.\d+|s+<-\|(?P<Protocol>w+)\|)\|-s+(?P<Source_IP>[^\|]+)`

2047 **Figure 4-102: Saving the new Regex created for this field extraction**

2048 Once this is complete, looking at the same log at the start of this section, the regex will now dissect the  
 2049 log for use in a dashboard:

6/10/25 4:43:14.000 PM Jun 10 16:43:14 Jun 10 20:43:07 dragos dragos\_syslog: CEF:0|Dragos|Platform|2.2|notification|New Baseline Peer Communication Deviation Detected|severity=2|created\_at=2025-06-04T17:45:56Z|detector\_id=|srczone= src=shost=|dstzone=dst= dhost=|msg=Asset 3 violated baseline 'Historian DB Scenario Latest' with client over POSTGRESQL <-(POSTGRESQL)- ]

Event Actions ▾

Type	<input checked="" type="checkbox"/> Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host ▾		▾
	<input checked="" type="checkbox"/> source ▾	udp:514	▾
	<input checked="" type="checkbox"/> sourcetype ▾	udp:514	▾
Event	<input type="checkbox"/> Baseline ▾	Historian DB Scenario Latest	▾
	<input type="checkbox"/> Destination_IP ▾		▾
	<input type="checkbox"/> Notification_Type ▾	New Baseline Peer Communication Deviation Detected	▾
	<input type="checkbox"/> Protocol ▾	POSTGRESQL	▾
	<input type="checkbox"/> Severity ▾	2	▾
	<input type="checkbox"/> Source_IP ▾		▾
	<input type="checkbox"/> created_at ▾	2025-06-04T17:45:56Z	▾
	<input type="checkbox"/> id ▾		▾
	<input type="checkbox"/> msg ▾	Asset	▾
	<input type="checkbox"/> severity ▾	2	▾

2050 **Figure 4-103: Dragos log now properly dissecting fields due to the Field Extractor tool**

2051 This whole process is just one method of dissecting this log. When creating a field extractor using regex,  
 2052 it hinges on the logs being the exact same every time, otherwise it will not dissect the logs the exact  
 2053 same way, if at all. In this instance, this method was useful because all the logs coming from Dragos for  
 2054 the PostgreSQL traffic baseline deviations all appeared in the same format. Dragos also has a plugin with  
 2055 Splunk that was not used for this demonstration.

2056 **Tenable**

2057 Splunk properly dissected the Tenable logs by default. The following screenshot is an example of a log  
 2058 showcasing a trigger of the “Historian Violation of Access” rule that was created in Tenable. Pay  
 2059 attention to the fields to see what has been extracted. An important element to note in the full log is  
 2060 highlighted by the red box:

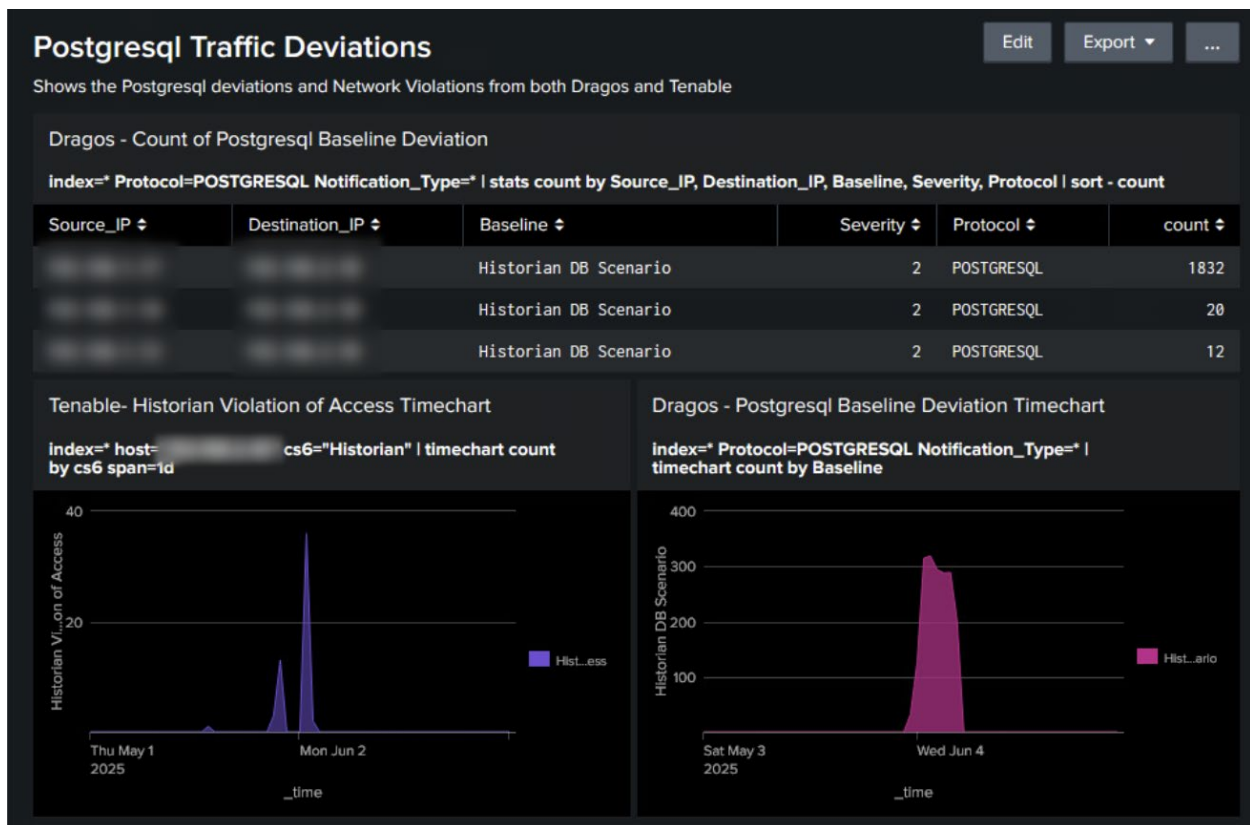
i	Time	Event																																																						
▼	6/3/25 11:43:44.000 AM	Jun 3 11:43:44 [redacted] Jun 3 11:33:47 [redacted] CEF:0 Tenabl e Tenable OT Security 3.17.40 109 Unauthorized Conversation 9 dvchost= Tenable OT Security rt=Jun 3 2025 11:33:47 duser=LOCAL-HIST-DB suser=J UMPHOSTVM1 proto=TCP dst [redacted] src [redacted] dpt=5432 cfp1La bel=cluster_log_id cfp1=259371 externalId=259371 cs6Label=policy_name <b>cs6=Historian Violation of Access</b> cat=NetworkEvents																																																						
<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">Event Actions ▼</div> <table border="1"> <thead> <tr> <th>Type</th> <th><input checked="" type="checkbox"/> Field</th> <th>Value</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td rowspan="3">Selected</td> <td><input checked="" type="checkbox"/> host ▼</td> <td>[redacted]</td> <td>▼</td> </tr> <tr> <td><input checked="" type="checkbox"/> source ▼</td> <td>udp:514</td> <td>▼</td> </tr> <tr> <td><input checked="" type="checkbox"/> sourcetype ▼</td> <td>udp:514</td> <td>▼</td> </tr> <tr> <td rowspan="13">Event</td> <td><input type="checkbox"/> cat ▼</td> <td>NetworkEvents</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> cfp1 ▼</td> <td>259371</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> cfp1Label ▼</td> <td>cluster_log_id</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> cs6 ▼</td> <td>Historian</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> cs6Label ▼</td> <td>policy_name</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> dpt ▼</td> <td>5432</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> dst ▼</td> <td>[redacted]</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> duser ▼</td> <td>LOCAL-HIST-DB</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> dvchost ▼</td> <td>Tenable</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> externalId ▼</td> <td>259371</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> proto ▼</td> <td>TCP</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> rt ▼</td> <td>Jun</td> <td>▼</td> </tr> <tr> <td><input type="checkbox"/> src ▼</td> <td>[redacted]</td> <td>▼</td> </tr> </tbody> </table>			Type	<input checked="" type="checkbox"/> Field	Value	Actions	Selected	<input checked="" type="checkbox"/> host ▼	[redacted]	▼	<input checked="" type="checkbox"/> source ▼	udp:514	▼	<input checked="" type="checkbox"/> sourcetype ▼	udp:514	▼	Event	<input type="checkbox"/> cat ▼	NetworkEvents	▼	<input type="checkbox"/> cfp1 ▼	259371	▼	<input type="checkbox"/> cfp1Label ▼	cluster_log_id	▼	<input type="checkbox"/> cs6 ▼	Historian	▼	<input type="checkbox"/> cs6Label ▼	policy_name	▼	<input type="checkbox"/> dpt ▼	5432	▼	<input type="checkbox"/> dst ▼	[redacted]	▼	<input type="checkbox"/> duser ▼	LOCAL-HIST-DB	▼	<input type="checkbox"/> dvchost ▼	Tenable	▼	<input type="checkbox"/> externalId ▼	259371	▼	<input type="checkbox"/> proto ▼	TCP	▼	<input type="checkbox"/> rt ▼	Jun	▼	<input type="checkbox"/> src ▼	[redacted]	▼
Type	<input checked="" type="checkbox"/> Field	Value	Actions																																																					
Selected	<input checked="" type="checkbox"/> host ▼	[redacted]	▼																																																					
	<input checked="" type="checkbox"/> source ▼	udp:514	▼																																																					
	<input checked="" type="checkbox"/> sourcetype ▼	udp:514	▼																																																					
Event	<input type="checkbox"/> cat ▼	NetworkEvents	▼																																																					
	<input type="checkbox"/> cfp1 ▼	259371	▼																																																					
	<input type="checkbox"/> cfp1Label ▼	cluster_log_id	▼																																																					
	<input type="checkbox"/> cs6 ▼	Historian	▼																																																					
	<input type="checkbox"/> cs6Label ▼	policy_name	▼																																																					
	<input type="checkbox"/> dpt ▼	5432	▼																																																					
	<input type="checkbox"/> dst ▼	[redacted]	▼																																																					
	<input type="checkbox"/> duser ▼	LOCAL-HIST-DB	▼																																																					
	<input type="checkbox"/> dvchost ▼	Tenable	▼																																																					
	<input type="checkbox"/> externalId ▼	259371	▼																																																					
	<input type="checkbox"/> proto ▼	TCP	▼																																																					
	<input type="checkbox"/> rt ▼	Jun	▼																																																					
	<input type="checkbox"/> src ▼	[redacted]	▼																																																					

- 2061 **Figure 4-104: Tenable logs properly dissected and ready for use in a dashboard**
- 2062 As shown above in the red box, the cs6 field represents the policy that is being violated, which shows in
- 2063 the full log as “Historian Violation of Access,” but the field was only able to capture the first word
- 2064 “Historian.” The IRT is able to proceed with this cs6 information, but users should be aware of potential
- 2065 truncation in dashboards. Just like with Dragos, Tenable has an official plugin that is not demonstrated
- 2066 in this Practice Guide.
- 2067 Using the dashboard creation discussed in Scenario A, Appendix C.1.1, a new dashboard is created to
- 2068 track the New Baseline Peer Communication Deviation Detected notification from
- 2069 Dragos, as well as the Historian Violation of Access from Tenable.

## 2070 C.5 Scenario B: Technical Details – Response

### 2071 C.5.1 Detection using Splunk Dashboard

2072 The following dashboard, created in C.4.6, indicates unauthorized PostgreSQL traffic. It tracks the count  
 2073 of PostgreSQL traffic with the source and destination IP addresses, and PostgreSQL traffic in a time chart  
 2074 for both Dragos and Tenable. Both time charts are potentially helpful, quick visuals to see a spike in  
 2075 baseline deviations or policy violations:



2076 **Figure 4-105: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs**

2077 *Note: Observe the search fields used when creating the databases in the screenshot (e.g., "index=\*").*

2078 To provide more in-depth detail, a panel was created in the dashboard to showcase a wide range of  
 2079 information provided by Dragos and Tenable:

Dragos - Baseline Deviation (Full Events)

index=\* Notification\_Type="New Baseline Peer Communication Deviation Detected" | table created\_at, Baseline, host, Source\_IP, Destination\_IP, Severity | sort - created\_at

created_at	Baseline	host	Source_IP	Destination_IP	Severity
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos			2

< Prev 1 2 3 4 5 6 7 8 9 10 Next >

2080 **Figure 4-106: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs**

Tenable - Historian Violation of Access

index=\* host cs6="Historian" | table \_time, cs6, suser, duser, src, dst | rename cs6 as "Policy Name", suser as "Source User", duser as "Destination User", src as "Source IP", dst as "Destination IP" | sort - \_time

_time	Policy Name	Source User	Destination User	Source IP	Destination IP
2025-06-04 13:17:09	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-04 13:11:39	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 18:30:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 18:28:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 16:35:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 16:33:39	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 16:30:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 16:28:24	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 16:27:09	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		
2025-06-03 16:24:39	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB		

< Prev 1 2 3 4 Next >

2081 **Figure 4-107: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs**

2082 Unusual PostgreSQL traffic is being detected by both Dragos and Tenable. Utilizing Splunk dashboards,  
 2083 incident responders can get a quick look into the violations occurring within the traffic. These  
 2084 dashboards can be edited as users see fit. These are just a few examples of how users can set up their  
 2085 dashboards to detect any vital traffic leaving or entering the ICS network.

2086 [\[Return to Scenario B\]](#)

## 2087 C.5.2 Analyzing Tenable Alert

2088 Because the factory's cyber team developed thorough baseline policies in Tenable, the system alerted  
 2089 when an unauthorized conversation occurred between the JumpHostVM and the local historian  
 2090 database. The Historian Violation of Access alert provides details on which machine was accessing the  
 2091 database using what port.

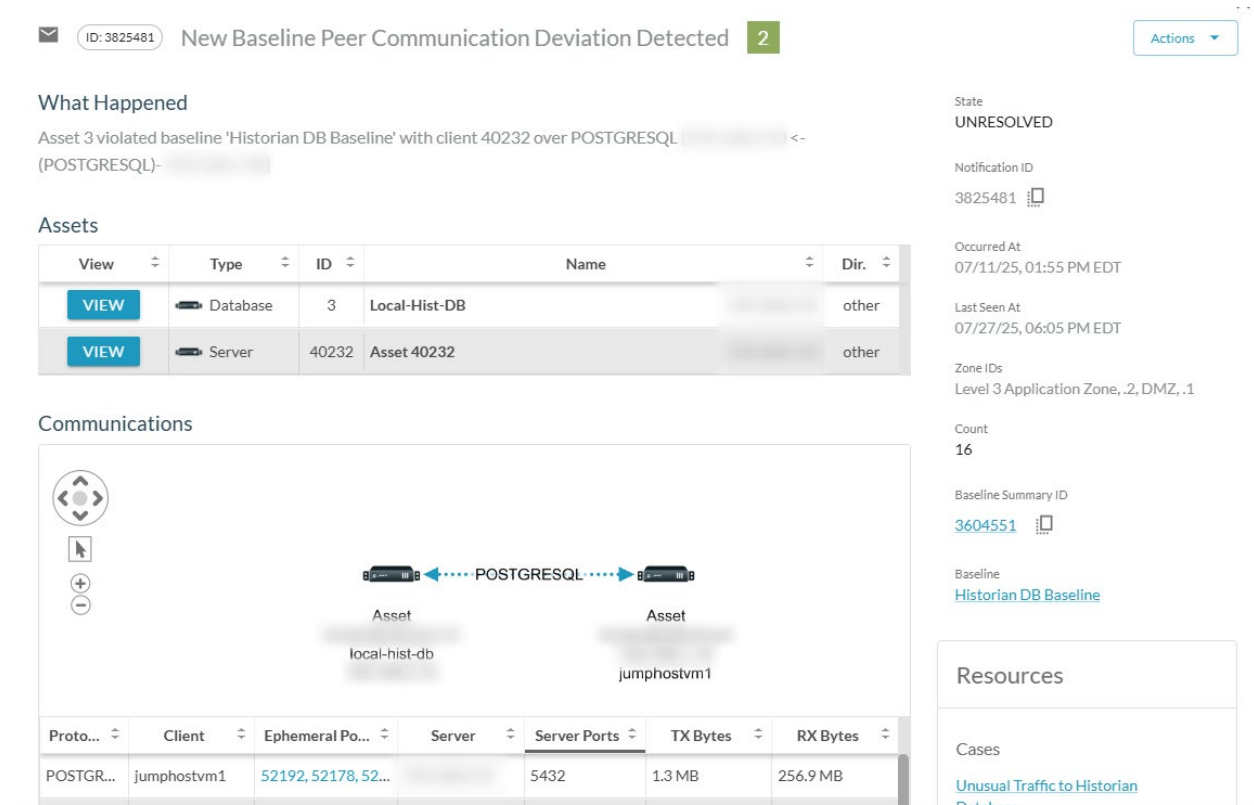
The screenshot shows a Tenable alert interface. At the top, the alert title is 'Historian Violation of Access' with a sub-category 'Unauthorized Conversation'. The status is 'Not resolved' and the severity is 'High'. The event occurred on Jul 11, 2025, at 02:30:23 PM. The event type is 'Unauthorized Co...' and the source asset is 'JUMPHOSTVM1'. The policy name is 'Historian Violation of Acc...'. Below the alert summary, there is a table of triggered events with columns for Status, Log ID, Time, Event Type, Severity, Policy Name, and Source Asset. The table shows one event with Log ID 355775. Below the table, there is a 'Details' section for event 355775, which states 'A conversation in an unauthorized protocol has been detected'. The details include a table with fields: SOURCE NAME (JUMPHOSTVM1), SOURCE IP ADDRESS, DESTINATION NAME (LOCAL-HIST-DB), DESTINATION IP ADDRESS, PROTOCOL (PostgreSQL Database (5432/TCP)), and PORT (5432). To the right of the details table, there are two sections: 'Why is this important?' and 'Suggested Mitigation'. The 'Why is this important?' section explains that conversations in unauthorized protocols may indicate suspicious traffic. The 'Suggested Mitigation' section advises checking if the communication is expected and adjusting policy conditions if necessary.

2092 **Figure 4-108: An alert generated in Tenable for a Historian Violation of Access policy**

2093 [\[Return to Scenario B\]](#)

## 2094 C.5.3 Analyzing Dragos Deviation Alert

2095 A notification appears in Dragos when a new asset communicates with the historian database, based on  
 2096 the Baseline created in section C.4.4. Details about the event can be investigated from the notification,  
 2097 and a case can be created from the notification.



2098 **Figure 4-109: Dragos PostgreSQL Historian Baseline Deviation**

2099 [\[Return to Scenario B\]](#)

2100 **C.5.4 Dragos Case Management**

2101 After the SOC team determined that a data exfiltration incident had occurred, an incident case was  
 2102 created using the Dragos SiteStore Platform (Version 2.4.2) Case Management tool to streamline the  
 2103 incident investigation and support cross-team coordination. Analysts should include their hypothesis  
 2104 description about the incident, priority setting, and assignment notification in the case. During the  
 2105 investigation, the case was updated with further evidence collected from the investigation. Once the  
 2106 investigation is done and response actions are taken, the case can be closed for further record. Below is  
 2107 the screenshot for the case created for the Scenario B incident. Priority 2 was given to the ticket based  
 2108 on initial indications from Dragos and Tenable.

## Create a New Case

Let's start by getting a few things out of the way to create your Case.

Name \*  
Unusual Traffic to Historian Database

Priority \*  
2

Visibility \*  
Public

Justification \*  
Received alert within Splunk that Tenable and Dragos both detected unusual Postgres traffic to the Historian database.

Create as Incident

CANCEL SUBMIT

2109 **Figure 4-110: Creating a new case within Dragos**

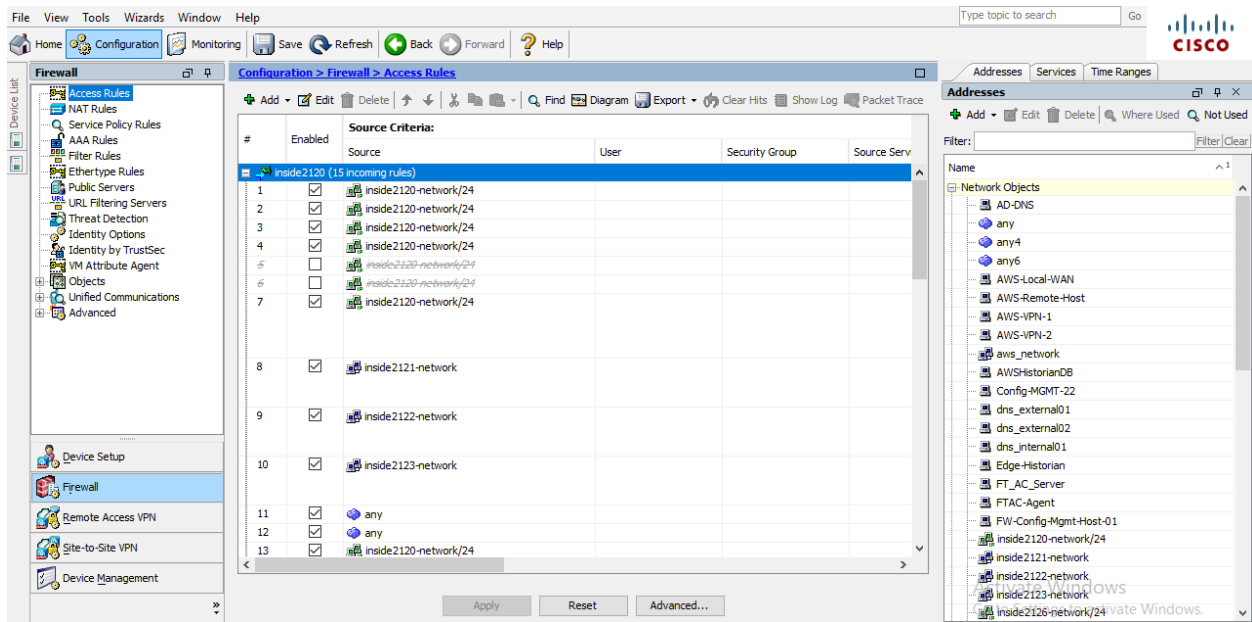
2110 [\[Return to Scenario B - Initial Identification\]](#)

2111 [\[Return to Scenario B - Cyber Incident Analysis and Response\]](#)

### 2112 C.5.5 Isolate ICS DMZ using ISA3000

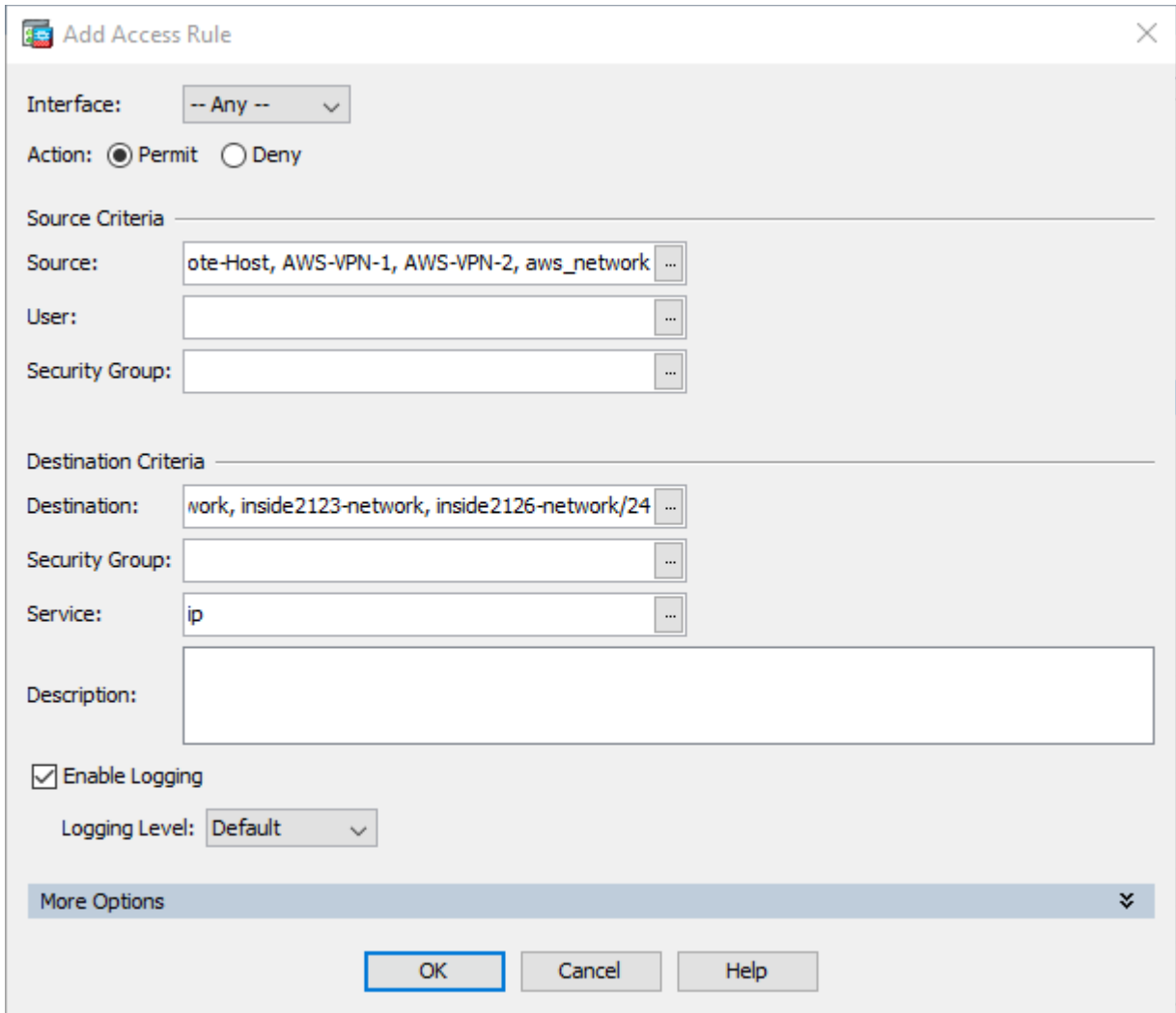
2113 The Incident Response Team updated the Cisco ISA3000 Firewall to limit traffic from the ICS network to  
2114 the corporate network, with the exception of the AWS instance. The following firewall rules were  
2115 applied:

2116 Allow the Edge Gateway server to communicate outbound to the cloud Ignition Gateway; temporarily  
2117 block all other inbound and outbound. Figure 4-111: Cisco Firewall Configuration shows a view into the  
2118 Adaptive Security Device Manager that provides an interface to configure the Cisco IS firewall.



2119 **Figure 4-111: Cisco firewall configuration**

2120 The following Figure 4-112 and [Figure 4-113](#) show the creation of new rules. Rules are created to ensure  
 2121 access is allowed from the ICS network to AWS and from AWS to the ICS network. Also, a block all rule is  
 2122 created to block all external traffic to internal traffic and vice versa. Placing the block rule after the pre-  
 2123 vious allow rule ensures all traffic is blocked, but communication is still allowed to flow over the site-to-  
 2124 site VPN to AWS networks.



2125

Figure 4-112: Permit rule for AWS gateway and hosts

**Add Access Rule**

Interface:

Action:  Permit  Deny

Source Criteria

Source:

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service:

Description:

Enable Logging

Logging Level:

More Options

2126 **Figure 4-113: Block rule for the ICS network**

2127 [\[Return to Scenario B\]](#)

## 2128 C.5.6 Disconnect JumpHost VM from Network

2129 Refer to section [C.2.8](#) in scenario A on how to remove a VM from the network in vSphere. In this step,  
2130 be sure to select the correct VM.

2131 [\[Return to Scenario B\]](#)

## 2132 C.5.7 Take Snapshot of JumpHost VM

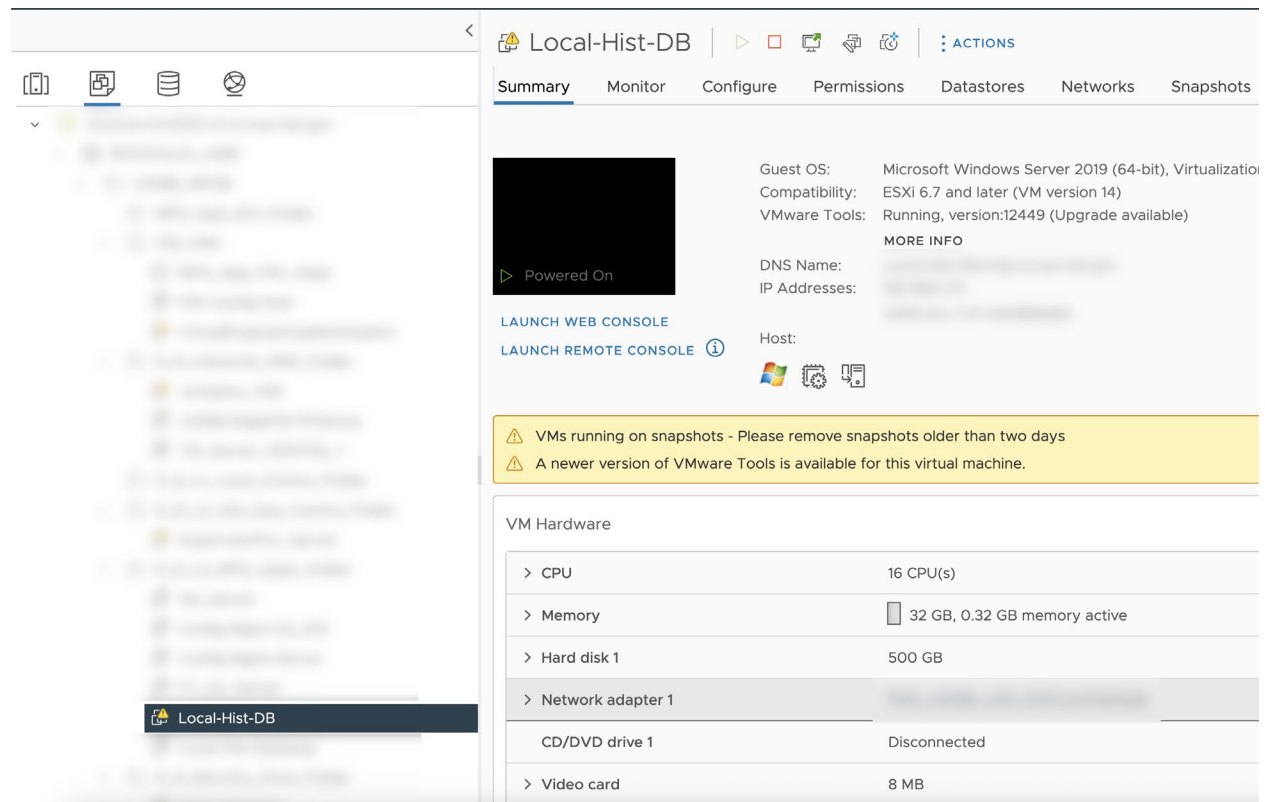
2133 Refer to section [C.2.9](#) in Scenario A on how to take a snapshot of a VM in vSphere. In this step, be sure  
2134 to select the correct VM. A snapshot of the VM is taken for forensics purposes.

2135 [\[Return to Scenario B\]](#)

## 2136 C.5.8 Isolate Local Database and Historian Gateway

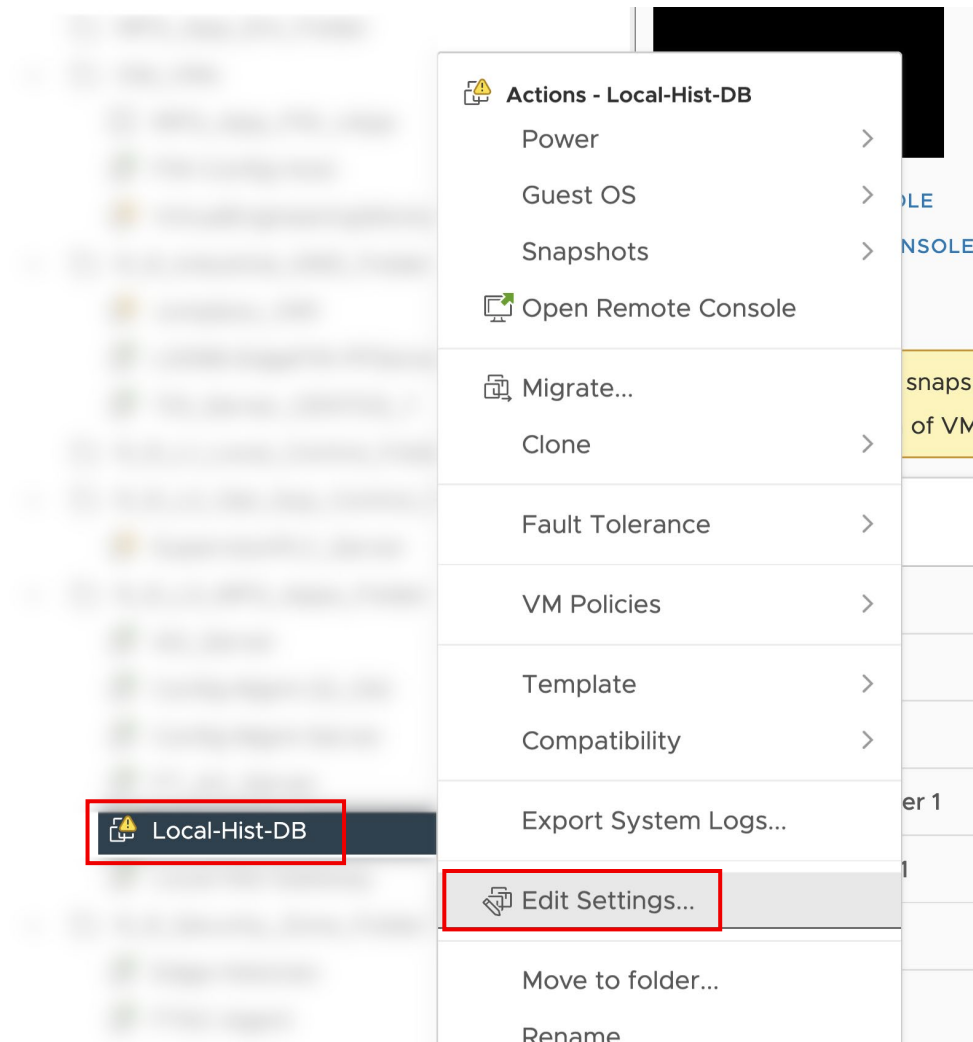
2137 The local historian gateway and database are isolated from the network as part of the containment step  
 2138 of incident response. Since both the local gateway server and the database server are virtual machines,  
 2139 they can be disconnected using the VMware vSphere client. The process to disconnect the Network  
 2140 Connection for a Virtual machine is shown below:

2141 Log in to the VMware vSphere Client. Once logged in, locate the suspect server (Local-Hist-DB) in the  
 2142 vSphere Client.



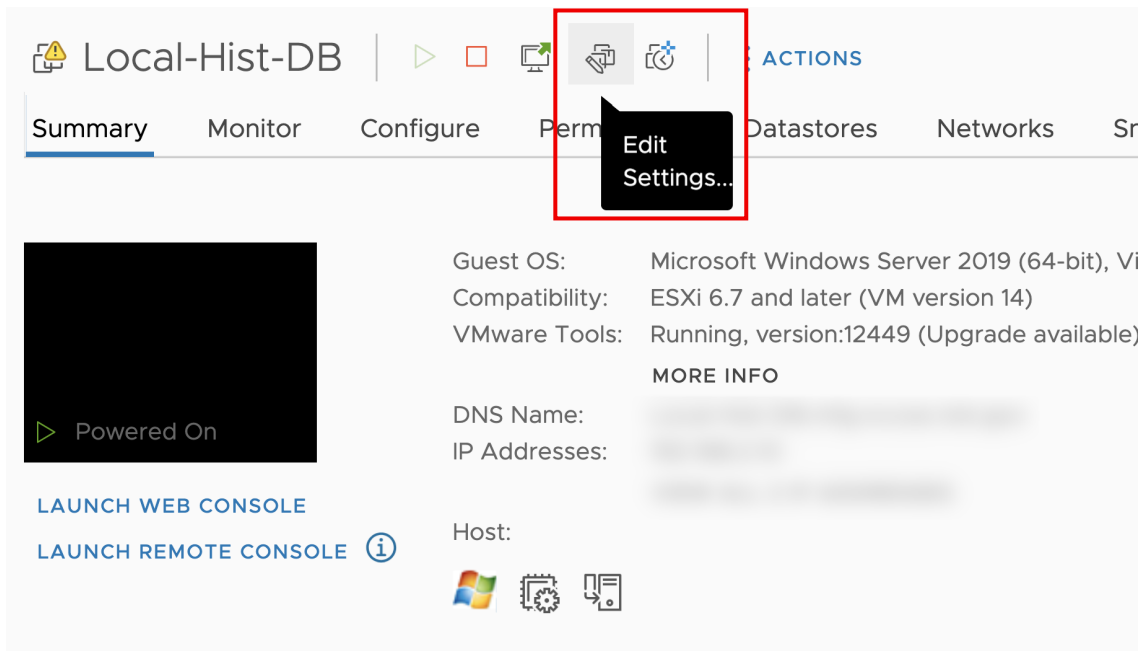
2143 **Figure 4-114: Select the local historian database server in vCenter**

2144 Edit the settings on the VM. There are a few methods: right-click on the selected server and select `Edit`  
 2145 `Settings`, or click on the Edit Settings button on the summary page.



2146

Figure 4-115: Locate Edit settings for local historian database host in vCenter



- 2147 **Figure 4-116: Locate “Edit Settings” for local historian database host in vCenter**
- 2148 Select the Network Adapter and uncheck the Connected and Connect At Power On check
- 2149 boxes.

### Edit Settings | Local-Hist-DB ✕

Virtual Hardware | VM Options ADD NEW DEVICE ▾

> CPU	16 ▾	<span>ⓘ</span>
> Memory	32 ▾	GB ▾
> Hard disk 1	500	GB ▾
> SCSI controller 0	VMware Paravirtual	
▾ Network adapter 1		<input checked="" type="checkbox"/> Connected
Status	<input checked="" type="checkbox"/> Connect At Power On	
Port ID	18218	
Adapter Type	VMXNET 3 ▾	
DirectPath I/O	<input checked="" type="checkbox"/> Enable	
Shares	Normal ▾	50 ▾
Reservation	0 ▾	Mbit/s ▾
Limit	Unlimited ▾	Mbit/s ▾
MAC Address		Automatic ▾
> CD/DVD drive 1	Client Device ▾	<input type="checkbox"/> Connected

2150

Figure 4-117: VM Network adapter settings, currently turned on

Edit Settings | Local-Hist-DB ×

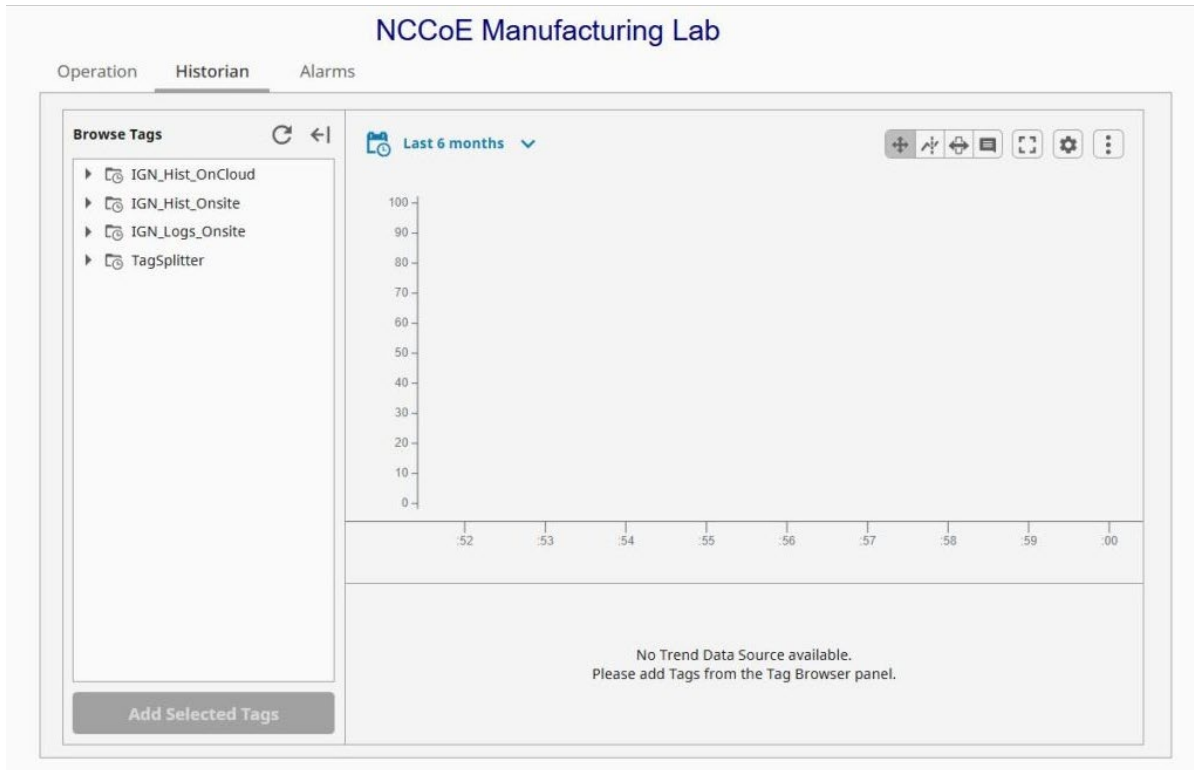
Virtual Hardware | VM Options ADD NEW DEVICE ▾

> CPU	16 ▾	<span style="float: right;">(i)</span>
> Memory	32 ▾	GB ▾
> Hard disk 1	500	GB ▾
> SCSI controller 0	VMware Paravirtual	
▾ Network adapter 1 *	[Blurred] <span style="float: right;">☐ Connected</span>	
Status	<input type="checkbox"/> Connect At Power On	
Port ID	18218	
Adapter Type	VMXNET 3 ▾	
DirectPath I/O	<input checked="" type="checkbox"/> Enable	
Shares	Normal ▾	50 ▾
Reservation	0 ▾	Mbit/s ▾
Limit	Unlimited ▾	Mbit/s ▾
MAC Address	[Blurred]	Automatic ▾
> CD/DVD drive 1	Client Device ▾	<input type="checkbox"/> Connected

2151 **Figure 4-118: VM Network adapter settings, currently turned off**

2152 Click OK. Validate that the database has been disconnected by logging into the local historian gateway.

2153 Verify that the local historian gateway does not show data in the Historian dashboard.



2154 **Figure 4-119: No historian data was shown from the local gateway dashboard**

2155 This same procedure was followed to disconnect the local historian gateway server from the network.

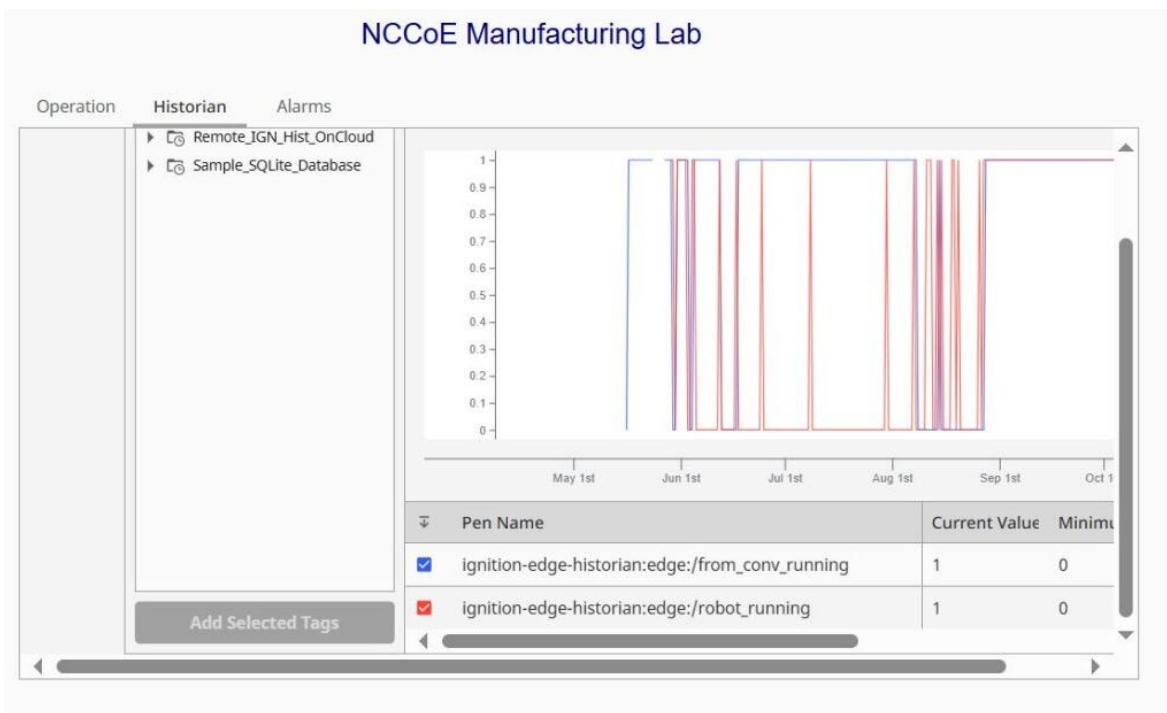
2156 After both the database and the gateway have been disconnected, the local historian is no longer  
 2157 functional. The cloud historian is still operational.

2158 [\[Return to Scenario B\]](#)

### 2159 C.5.9 Validate Redundant AWS Cloud Historian

2160 A cloud database and historian were configured for redundancy. After isolating the local historian, verify  
 2161 that the redundant server installed in the AWS cloud is still functional.

- 2162 - Log in to Ignition historian in the cloud.
- 2163 - Verify live updates on both the Operation and Historian tabs built into the GUI.



2164 **Figure 4-120: AWS Gateway Ignition historian dashboard**

2165 Real-time data is provided from the Edge to the Cloud Ignition Gateway. Historical data is being  
 2166 provided to the cloud database from the tag splitter located in the Local Ignition Gateway. Information  
 2167 seen in the cloud will be real-time, and historical data will be available up to the point in time when the  
 2168 Local Gateway goes offline. Once the Local Ignition Gateway is back online, the missing historical data  
 2169 will automatically be forwarded from the Edge to the Local and Cloud Ignition Gateways.

2170 [\[Return to Scenario B\]](#)

2171 **C.5.10 Detecting Large Data Transfer in Dragos**

2172 After finding the specific notification within Dragos, users can see the amount of data being transferred:

Seve...	ID	Occurred At	Type	Summary	Message
2	3614502	06/04/25, 01:33 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate' with server 28417 over TLS
2	3614501	06/04/25, 01:33 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest' with server 28417 over TLS
2	3614500	06/04/25, 01:33 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate - Duplicate' with server 34132 over HTTP
2	3614499	06/04/25, 01:33 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate' with server 34132 over HTTP
2	3614498	06/04/25, 01:33 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest' with server 34132 over HTTP
2	3614199	06/04/25, 01:11 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate - Duplicate' with client 38484 over PostgreSQL
2	3614198	06/04/25, 01:11 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate' with client 38484 over PostgreSQL
2	3614197	06/04/25, 01:11 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest' with client 38484 over PostgreSQL
2	3614180	06/04/25, 01:09 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate - Duplicate' with server 295 over TLS
2	3614179	06/04/25, 01:09 P...	Baseline	New Baselin...	Asset 3 violated baseline 'Historian DB Scenario Latest - Duplicate' with server 295 over TLS

2173 **Figure 4-121: List of notifications in Dragos**

✉ ID: 3614197 New Baseline Peer Communication Deviation Detected 2

**What Happened**  
 Asset 3 violated baseline 'Historian DB Scenario Latest' with client 38484 over POSTGRESQL [192.168.2.10 <--(POSTGRESQL)- 192.168.1.17]

**Assets**

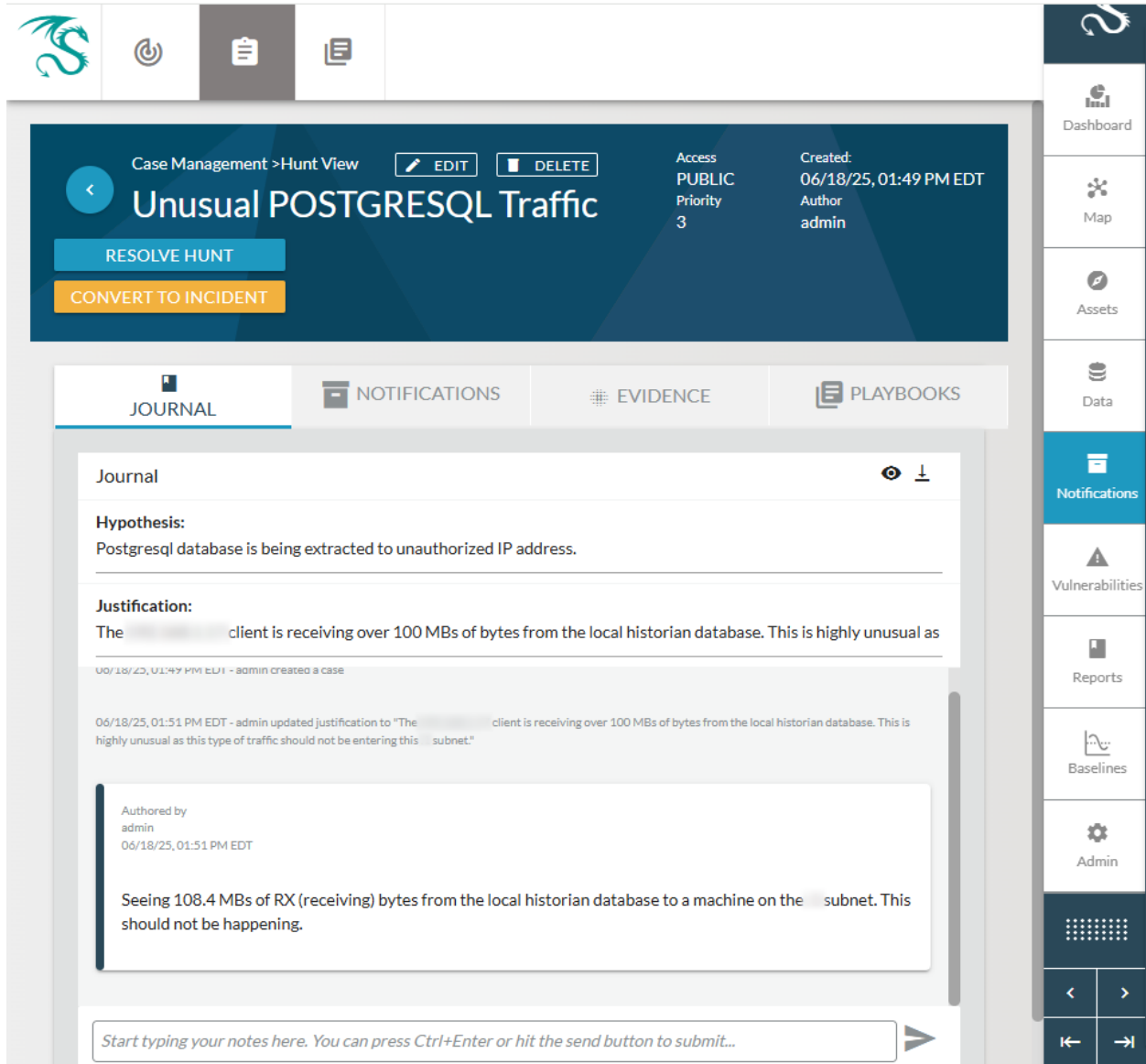
View	Type	ID	Name	Dir.
<a href="#">VIEW</a>	Database	3	Local-Hist-DB	other
<a href="#">VIEW</a>	Server	38484	Asset 38484	other

**Communications**

Proto...	Client	Ephemeral Po...	Server	Server Ports	TX Bytes	RX Bytes
POSTGR...		-		-	509.7 KB	108.4 MB
POSTGR...		-	local-hist-db	-	509.7 KB	108.4 MB

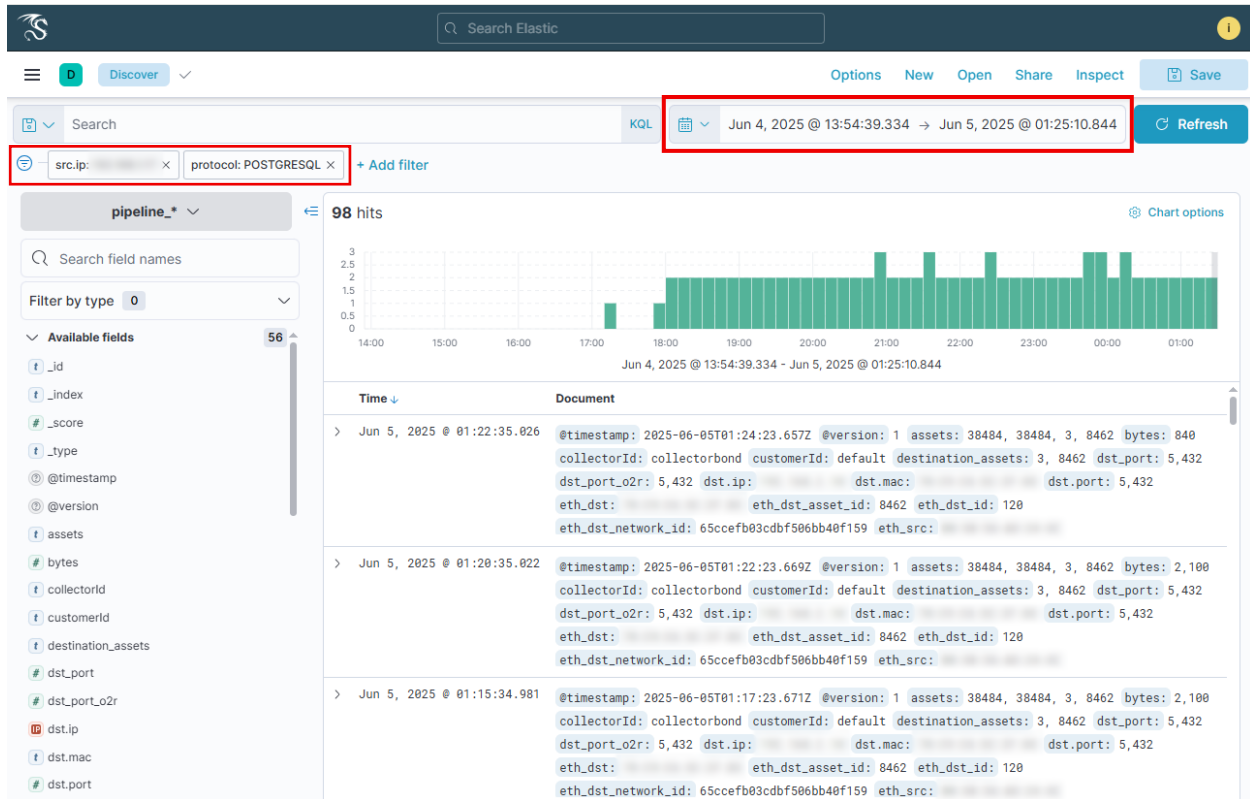
[< PREV](#)

- 2174 **Figure 4-122: Expanding Dragos notification to find additional information**
- 2175 When expanding the notification in Figure 4-123, we can see the number of RX (received) bytes moving
- 2176 between the local historian database and the JumpHostVM1. This information is added to the Dragos
- 2177 ticket:



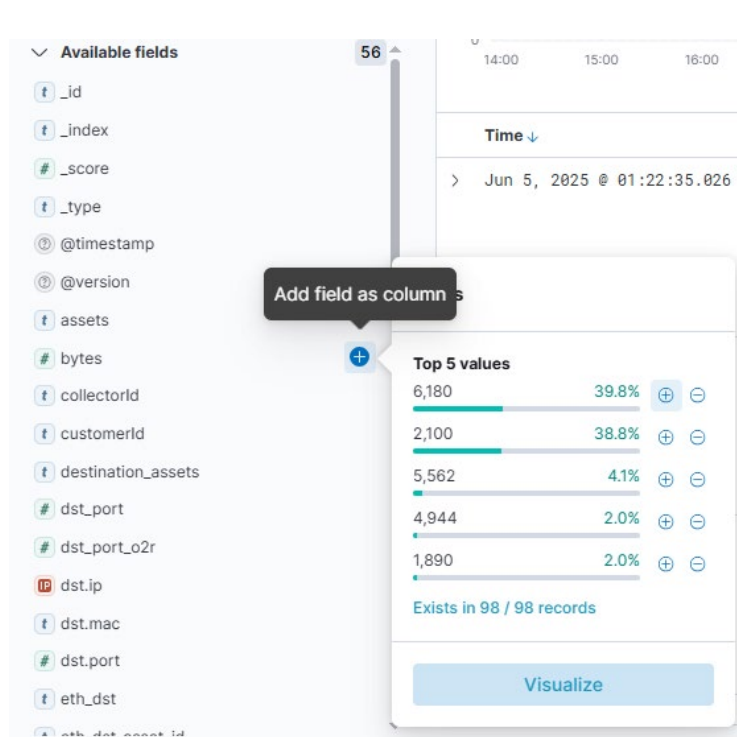
2178 **Figure 4-123: Suspicious large file transfer added to Dragos ticket**

2179 If more evidence is required, incident responders can dive further into Dragos using the built-in Kibana  
 2180 instance. To gather more evidence, this unusual behavior can be tracked even further by shortening the  
 2181 time range to the time of the event found in the notification:



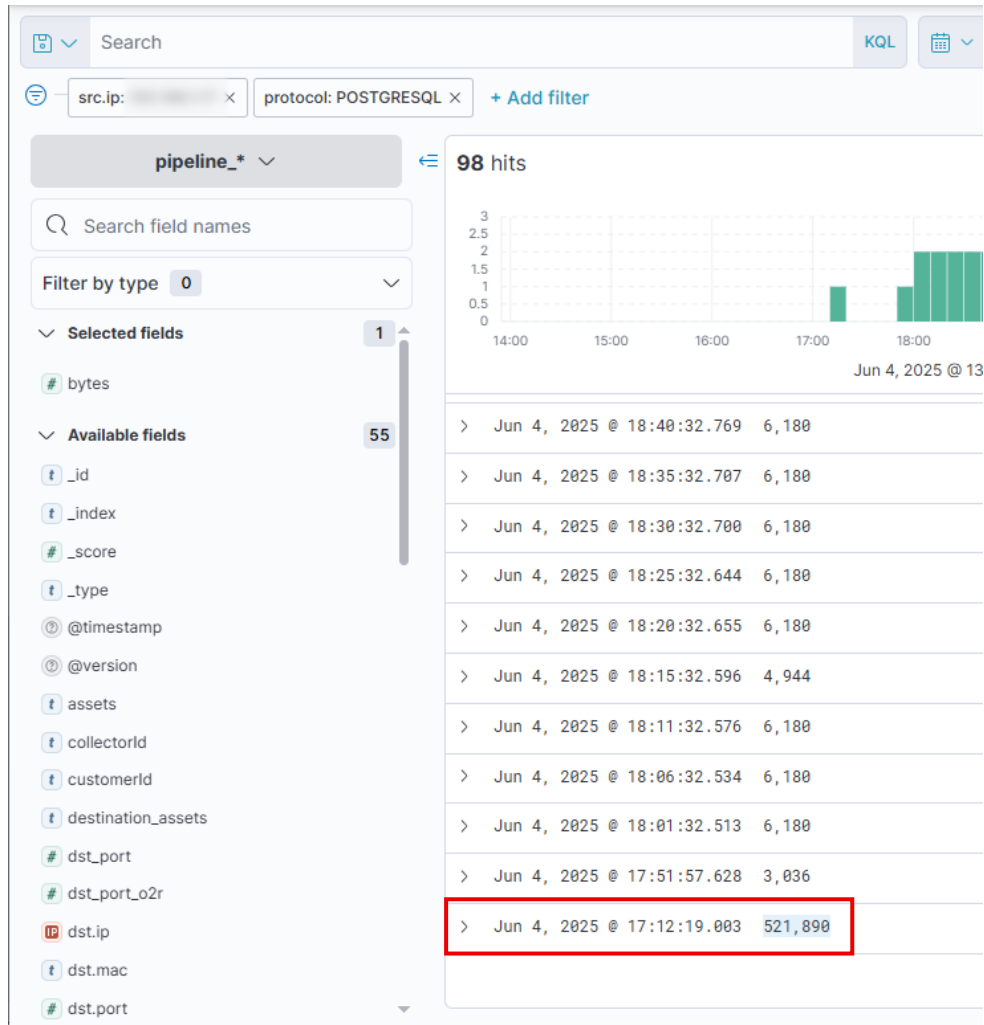
2182 **Figure 4-124: Looking for the logs surrounding the time of the event in Kibana**

2183 Next, filter these entries by sorting by byte size:



2184

Figure 4-125: Filter to look for larger amounts of bytes



2185 **Figure 4-126: Seeing a large number of bytes around the time of the notification**

2186 The red box indicates a single log with 521,890 bytes. Not as large as we’re looking for, so from here we  
 2187 can view additional logs to get closer to what we’re looking for. Start by expanding this log and clicking  
 2188 on the “View surrounding documents” button:

Jun 4, 2025 @ 17:12:19.003 521,890

Expanded document [View surrounding documents](#) View single document

Table JSON

Actions	Field	Value
	<b>_id</b>	f93e9576-18dc-42fd-b2a9-24a8854d102c
	<b>_index</b>	pipeline-000020
	<b>_score</b>	-
	<b>_type</b>	_doc

2189

Figure 4-127: Expanded the log to view its contents

Search Elastic

Discover Surrounding documents

protocol: POSTGRESQL x + Add filter

Documents surrounding #f93e9576-18dc-42fd-b2a9-24a8854d102c

Load 5 newer documents

Time	bytes
> Jun 4, 2025 @ 17:12:19.393	-
> Jun 4, 2025 @ 17:12:19.311	-
> Jun 4, 2025 @ 17:12:19.232	-
> Jun 4, 2025 @ 17:12:19.147	-
> Jun 4, 2025 @ 17:12:19.003	113,674,194
> Jun 4, 2025 @ 17:12:19.003	521,890
> Jun 4, 2025 @ 17:12:18.645	-
> Jun 4, 2025 @ 17:12:18.598	-
> Jun 4, 2025 @ 17:12:18.598	-
> Jun 4, 2025 @ 17:12:18.598	-
> Jun 4, 2025 @ 17:12:18.598	-

2190

Figure 4-128: Larger amounts of data found

Jun 4, 2025 @ 17:12:19.003 113,674,194

Expanded document

Table JSON

Actions	Field	Value
	<b>f</b> _id	92f65138-5411-40c8-b35a-709e25a9efc0
	<b>f</b> _index	pipeline-000020
	<b>#</b> _score	-
	<b>f</b> _type	_doc
	<b>@</b> @timestamp	2025-06-04T17:15:23.727Z
	<b>@</b> @version	1
	<b>f</b> assets	3, 8462, 38484, 38484
	<b>#</b> bytes	113,674,194
	<b>f</b> collectorId	collectorbond
	<b>f</b> customerId	default
	<b>f</b> destination_assets	38484, 38484
	<b>#</b> dst_port	54,167, 54,178, 54,179, 54,204
	<b>#</b> dst_port_r2o	54,167, 54,178, 54,179, 54,204
	<b>ip</b> dst.ip	
	<b>f</b> dst.mac	
	<b>#</b> dst.port	54,167, 54,178, 54,179, 54,204
	<b>f</b> eth_dst	

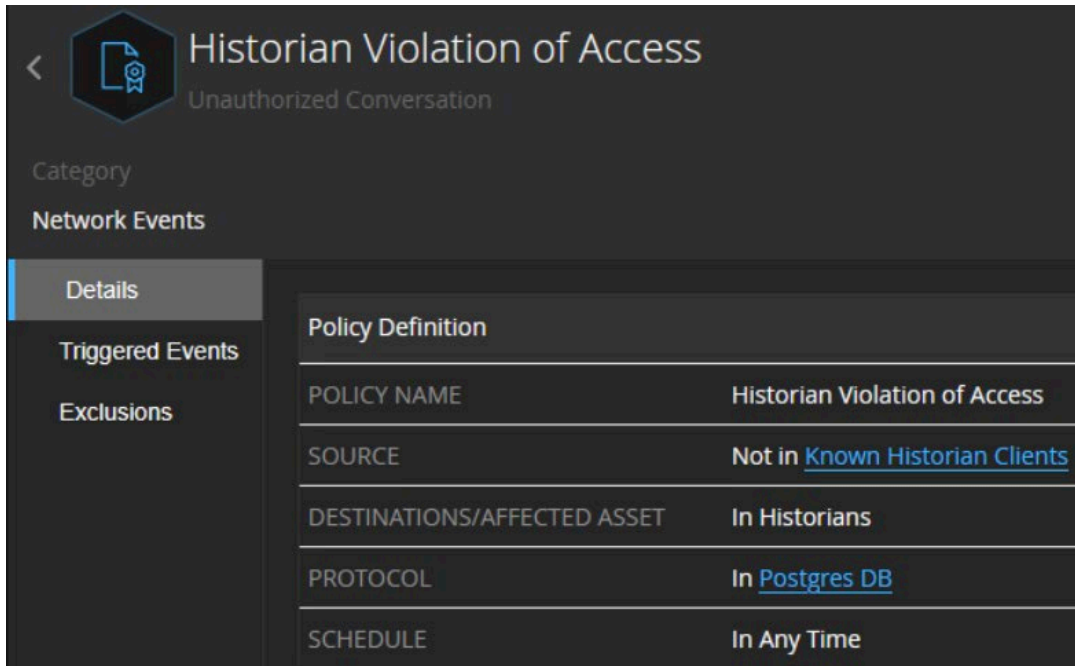
2191 **Figure 4-129: Expanded the log to view its contents**

2192 Incident responders can utilize Dragos tools to narrow down unusual activity found within the OT  
 2193 network, and these are a few methods to do so.

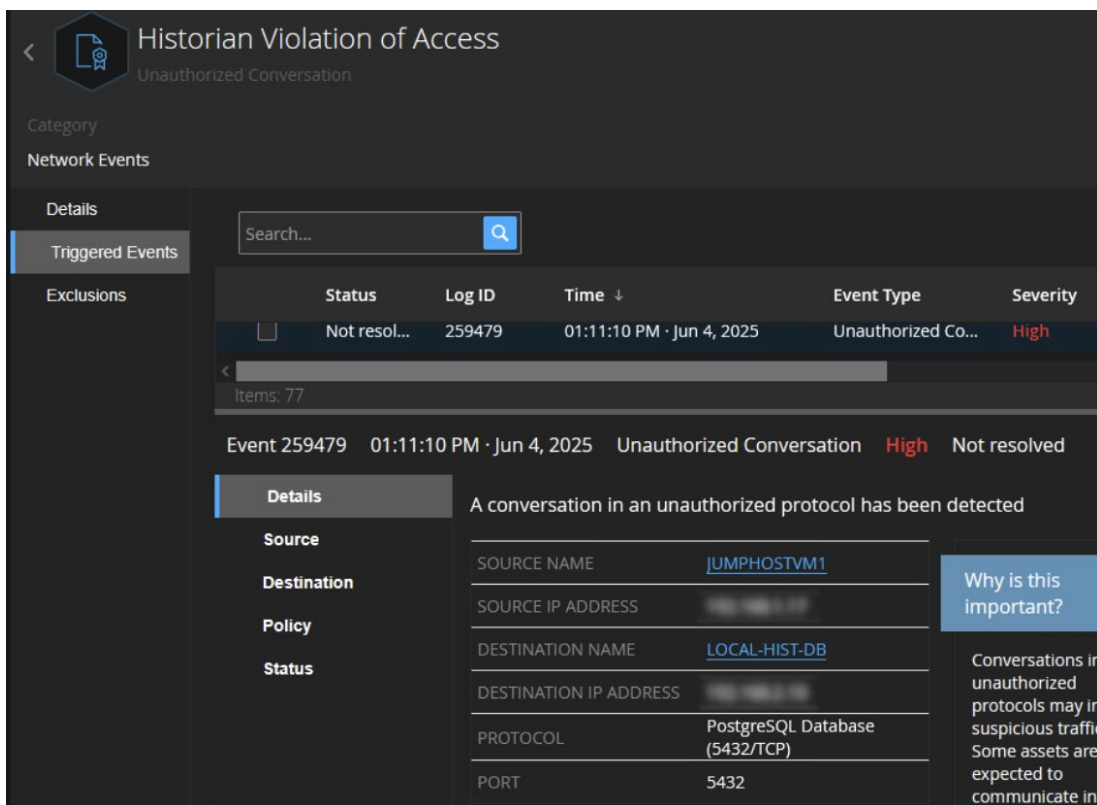
2194 [\[Return to Scenario B\]](#)

2195 **C.5.11 Detecting Policy Deviation in Tenable**

2196 Although Tenable can be configured with policies that can detect unusual traffic, it may need to be  
 2197 trained to differentiate between expected versus anomalous alerts. In this scenario, expected data  
 2198 historian traffic was initially flagged as malicious, so a policy was set up to establish a baseline of normal  
 2199 behavior by detecting and allowing expected PostgreSQL traffic leaving the data historian. The set of  
 2200 screenshots shows the policy itself and the triggered alert:



2201 **Figure 4-130: Historian Violation of Access policy definition**

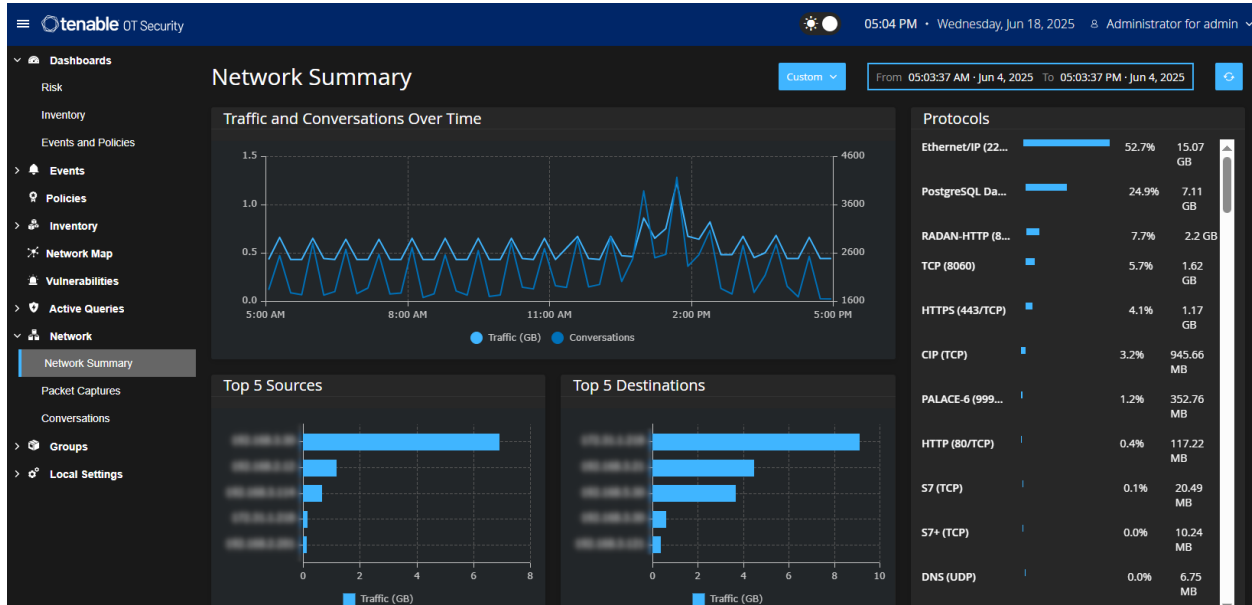


2202 **Figure 4-131: Historian Violation of Access policy being triggered**

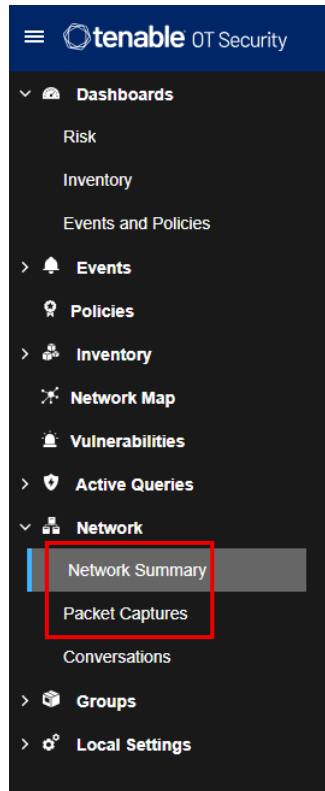
2203 [\[Return to Scenario B\]](#)

2204 **C.5.12 Browsing Packet Captures from Tenable**

2205 With Tenable triggering the alert, along with Dragos, incident responders can use Tenable to pull the  
 2206 network packet captures around the time these violations occurred. Using another tool, Wireshark in  
 2207 this instance, users can attempt to attribute who performed this transfer of data from the data  
 2208 historian. For the scenario, this begins by viewing the Network Summary page under the Network tab on  
 2209 the left-hand side. The following set of screenshots showcases the Network Summary page, starting  
 2210 with the full page, followed by portions of the same screenshot zoomed in for clarity. The time range set  
 2211 for the data shown is the same time frame as the policy violation.

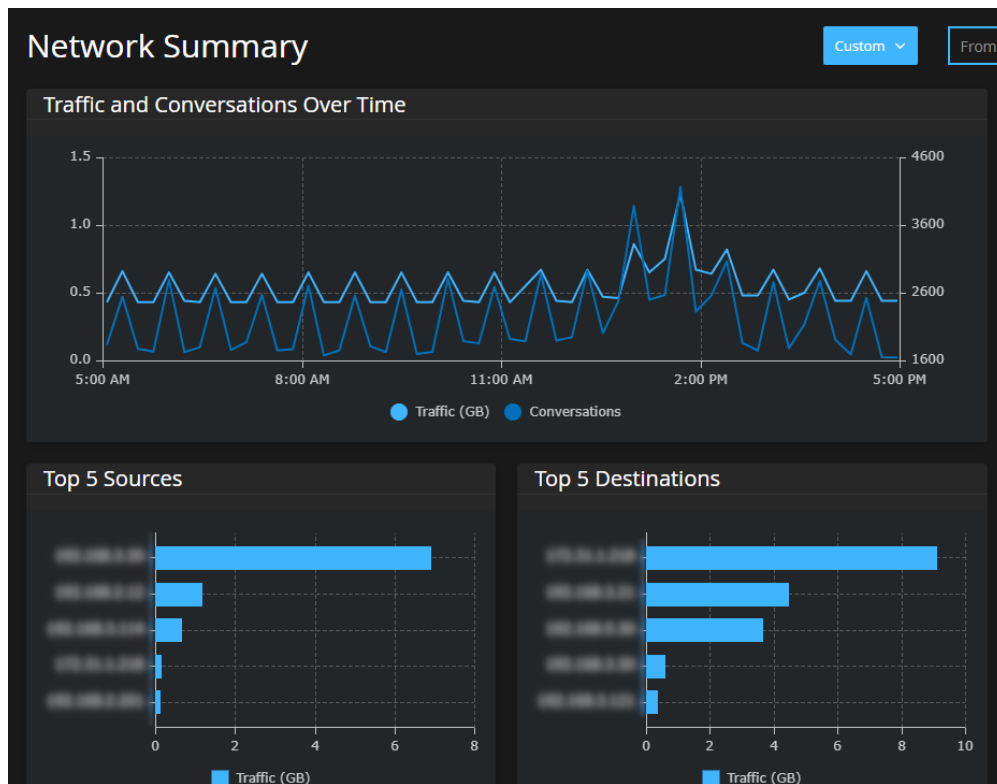


2212 **Figure 4-132: Full Network Summary page in Tenable**



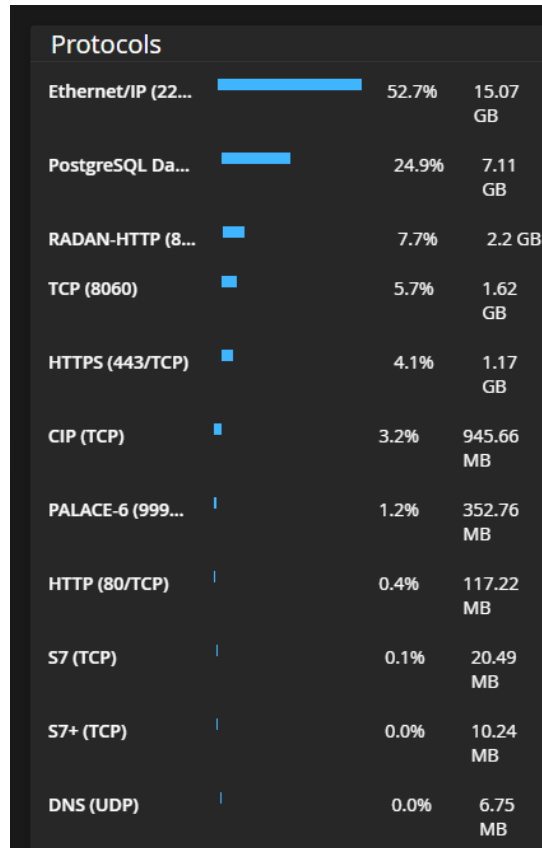
2213

Figure 4-133: Where to find the Network Summary tab



2214

Figure 4-134: The center portion, showing the latest traffic in gigabytes (GB) on the network



2215 **Figure 4-135: Shows the most traffic by GBs based on protocol**

2216 As seen above, PostgreSQL traffic is a little high in the timeframe of the policy violation. Depending on  
 2217 the network, this might not be abnormal, but since this is the main database used for the data historian,  
 2218 it's more evidence of suspicious activity.

2219 At this point, the incident response team wants to investigate further to determine if they can attribute  
 2220 this flow of data to a specific user. They download the packet capture files (PCAPs) from Tenable to view  
 2221 in the program Wireshark.

tenable OT Security 03:24 PM • Wednesday, Jun 18, 2025 & Administrator for admin

**Packet Captures** Search... Oldest capture file: Oct 15, 2024 01:00:09 PM [Download](#) [Close ongoing captures](#)

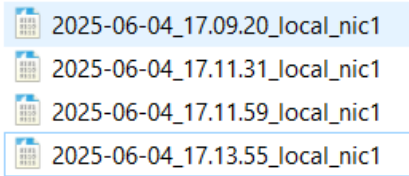
Start Time	End Time	Sensor	File Name
Jun 4, 2025 01:26:37 PM	Jun 4, 2025 01:28:01 PM	local_nic1	2025-06-04_17.26.37_local_nic1.pcap.gz
Jun 4, 2025 01:24:59 PM	Jun 4, 2025 01:26:37 PM	local_nic1	2025-06-04_17.24.59_local_nic1.pcap.gz
Jun 4, 2025 01:23:18 PM	Jun 4, 2025 01:24:59 PM	local_nic1	2025-06-04_17.23.18_local_nic1.pcap.gz
Jun 4, 2025 01:21:42 PM	Jun 4, 2025 01:23:18 PM	local_nic1	2025-06-04_17.21.42_local_nic1.pcap.gz
Jun 4, 2025 01:20:03 PM	Jun 4, 2025 01:21:42 PM	local_nic1	2025-06-04_17.20.03_local_nic1.pcap.gz
Jun 4, 2025 01:18:26 PM	Jun 4, 2025 01:20:04 PM	local_nic1	2025-06-04_17.18.26_local_nic1.pcap.gz
Jun 4, 2025 01:16:52 PM	Jun 4, 2025 01:18:26 PM	local_nic1	2025-06-04_17.16.52_local_nic1.pcap.gz
Jun 4, 2025 01:15:23 PM	Jun 4, 2025 01:16:52 PM	local_nic1	2025-06-04_17.15.23_local_nic1.pcap.gz
Jun 4, 2025 01:13:55 PM	Jun 4, 2025 01:15:23 PM	local_nic1	2025-06-04_17.13.55_local_nic1.pcap.gz
Jun 4, 2025 01:11:59 PM	Jun 4, 2025 01:13:55 PM	local_nic1	2025-06-04_17.11.59_local_nic1.pcap.gz
Jun 4, 2025 01:11:31 PM	Jun 4, 2025 01:11:59 PM	local_nic1	2025-06-04_17.11.31_local_nic1.pcap.gz
Jun 4, 2025 01:09:20 PM	Jun 4, 2025 01:11:31 PM	local_nic1	2025-06-04_17.09.20_local_nic1.pcap.gz
Jun 4, 2025 01:07:24 PM	Jun 4, 2025 01:09:20 PM	local_nic1	2025-06-04_17.07.24_local_nic1.pcap.gz
Jun 4, 2025 01:05:12 PM	Jun 4, 2025 01:07:24 PM	local_nic1	2025-06-04_17.05.12_local_nic1.pcap.gz
Jun 4, 2025 01:02:59 PM	Jun 4, 2025 01:05:12 PM	local_nic1	2025-06-04_17.02.59_local_nic1.pcap.gz
Jun 4, 2025 01:00:47 PM	Jun 4, 2025 01:02:59 PM	local_nic1	2025-06-04_17.00.47_local_nic1.pcap.gz

Version 3.17.40 Expires Jun 28, 2025  
Assets Limit 13400%

2222 **Figure 4-136: The Packet Captures tab, highlighted areas are the PCAPs used in the scenario**

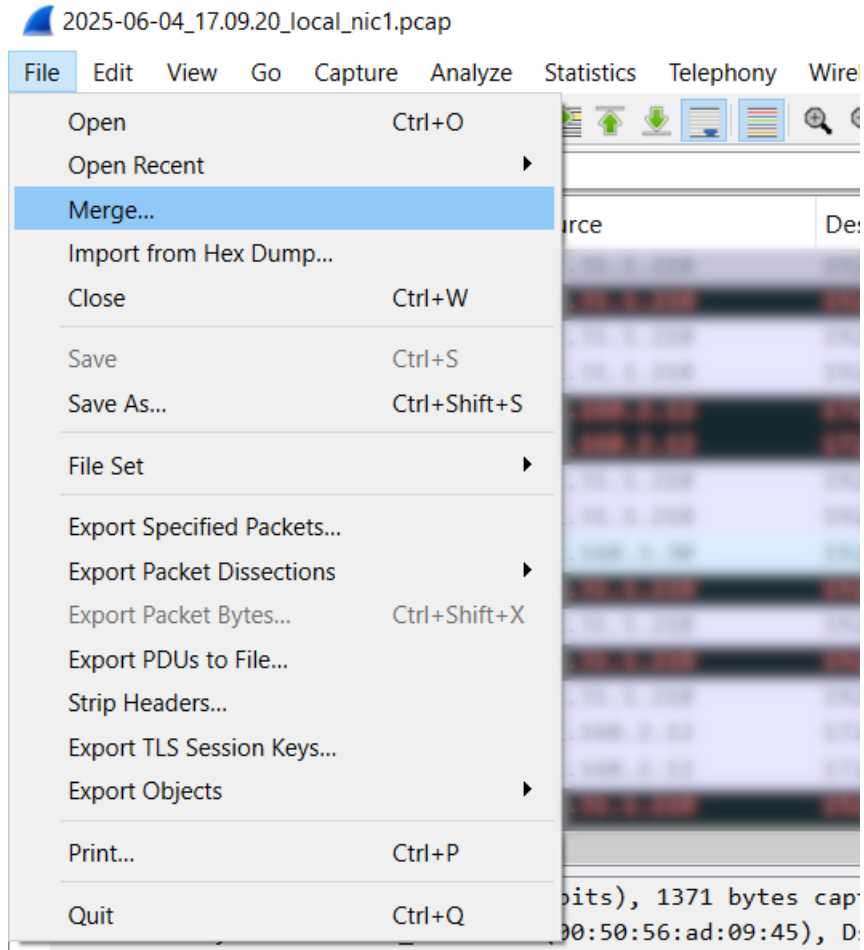
2223 Tenable splits the PCAPs into intervals for logistical reasons, such as keeping the file sizes low since  
 2224 PCAPs can quickly become incredibly high in file size when capturing network traffic. For this reason, the  
 2225 incident response team will download a few PCAPs from around the same time and merge them into a  
 2226 single PCAP. The downloaded PCAPs are highlighted in the red box above.

2227 Open a PCAP in Wireshark, then go to “File” and select “Merge...”:



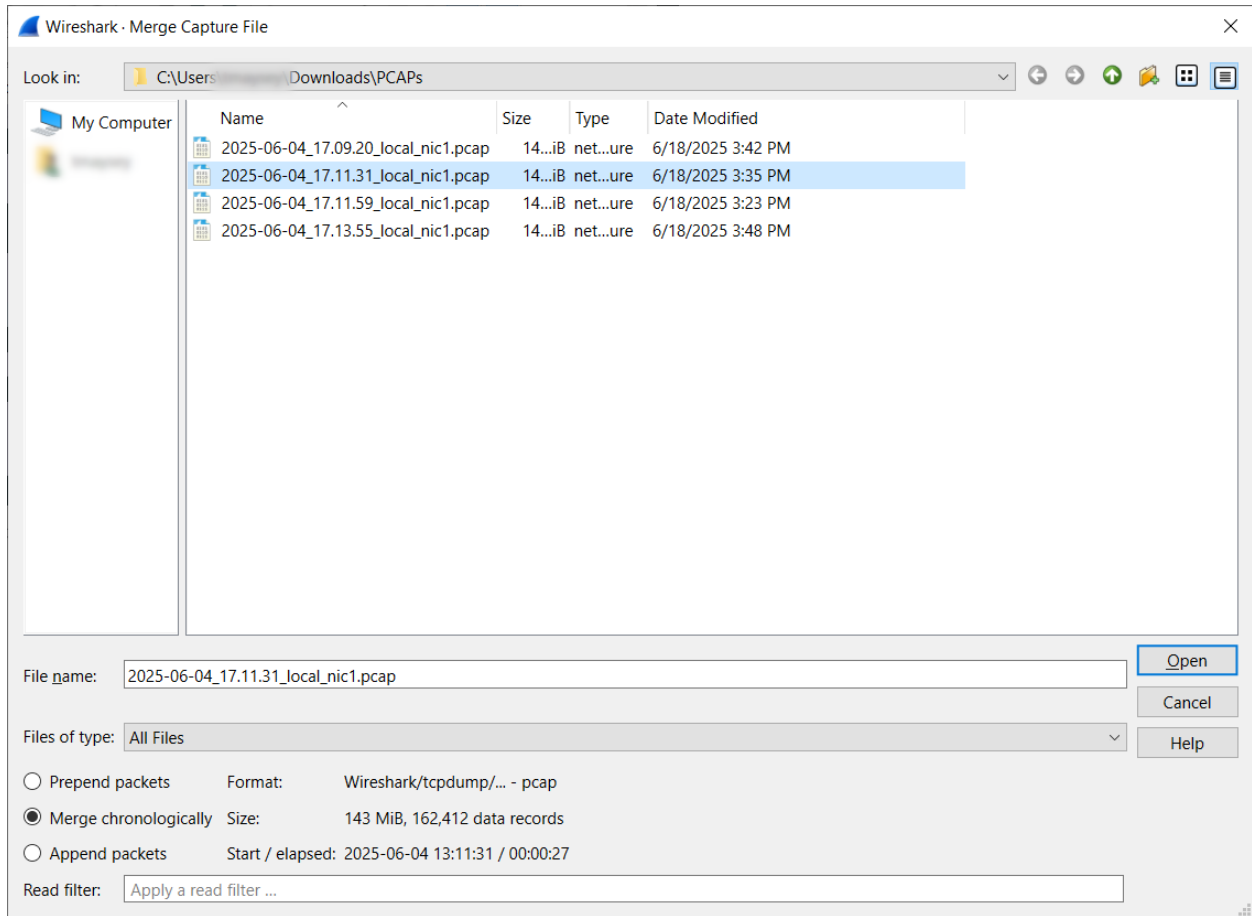
2228

Figure 4-137: Four downloaded PCAPs from Tenable

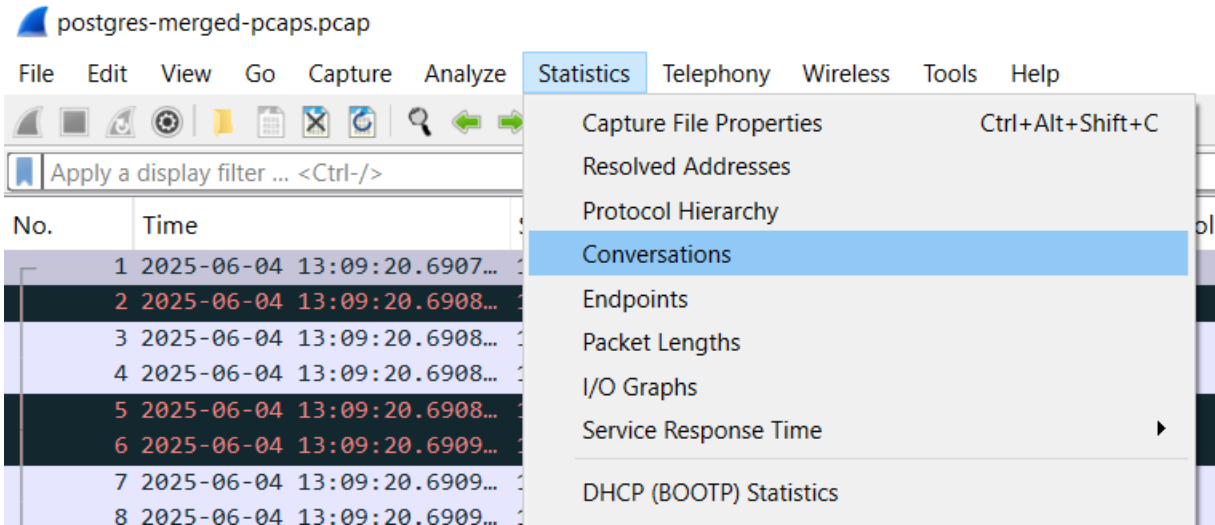


2229

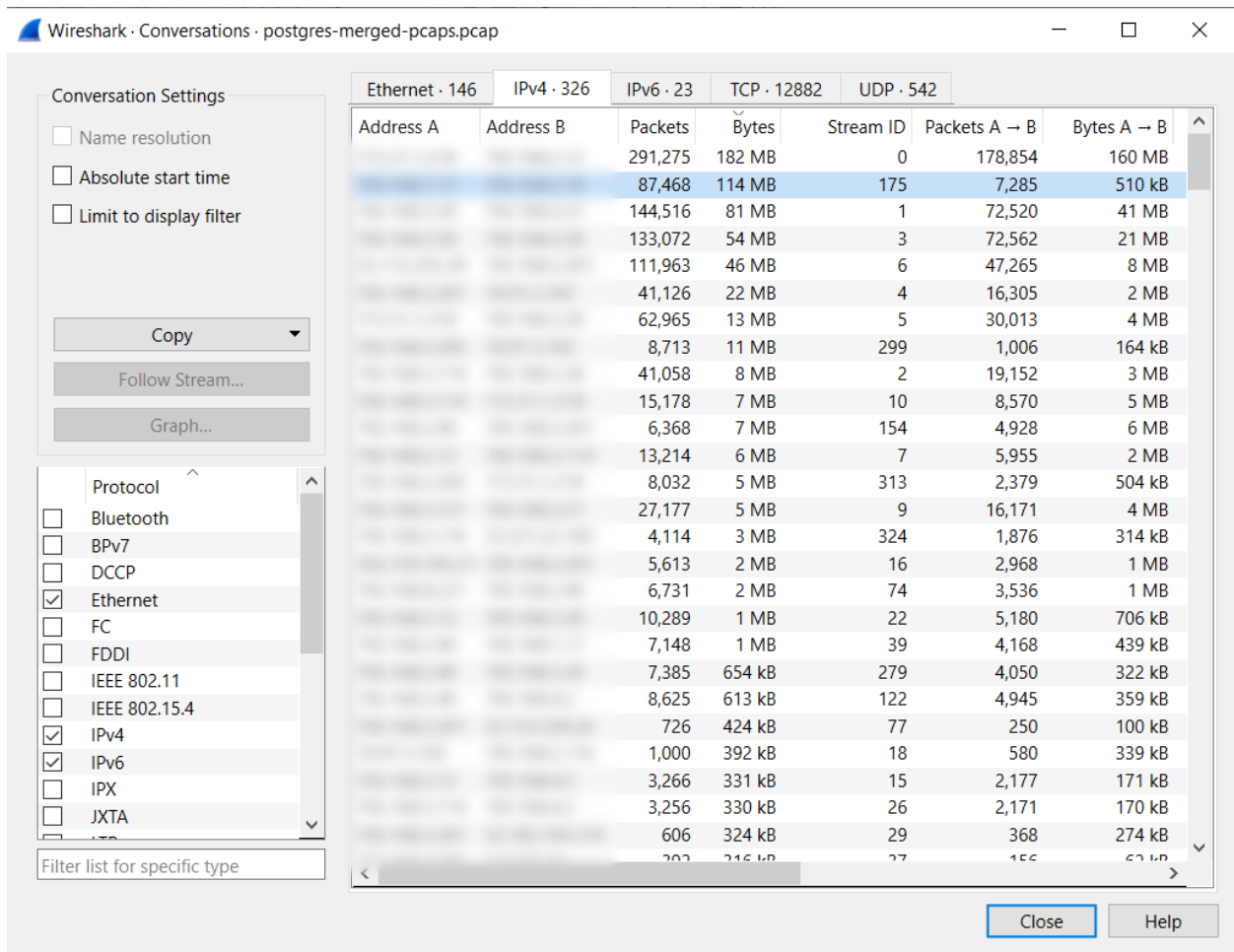
Figure 4-138: Choosing the option to merge multiple PCAPs together in Wireshark



- 2230 **Figure 4-139: Selecting the four downloaded PCAPs from Tenable to merge**
- 2231 Merge each PCAP individually until a fully merged PCAP is formed. From here, the investigation can
- 2232 begin. At the top, go to “Statistics” and then “Conversations”:

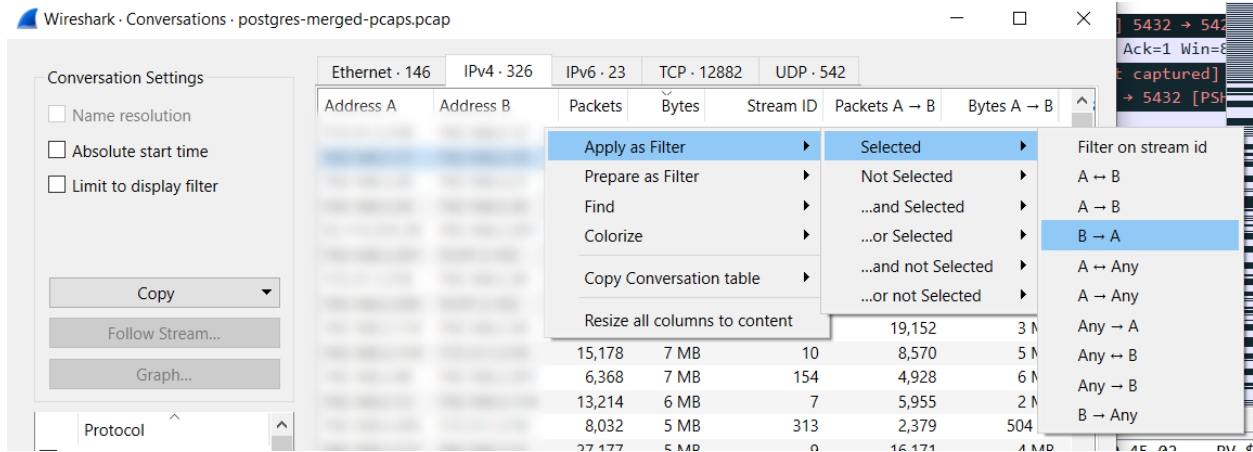


2233 **Figure 4-140: Selecting the option to view network conversations in Wireshark**



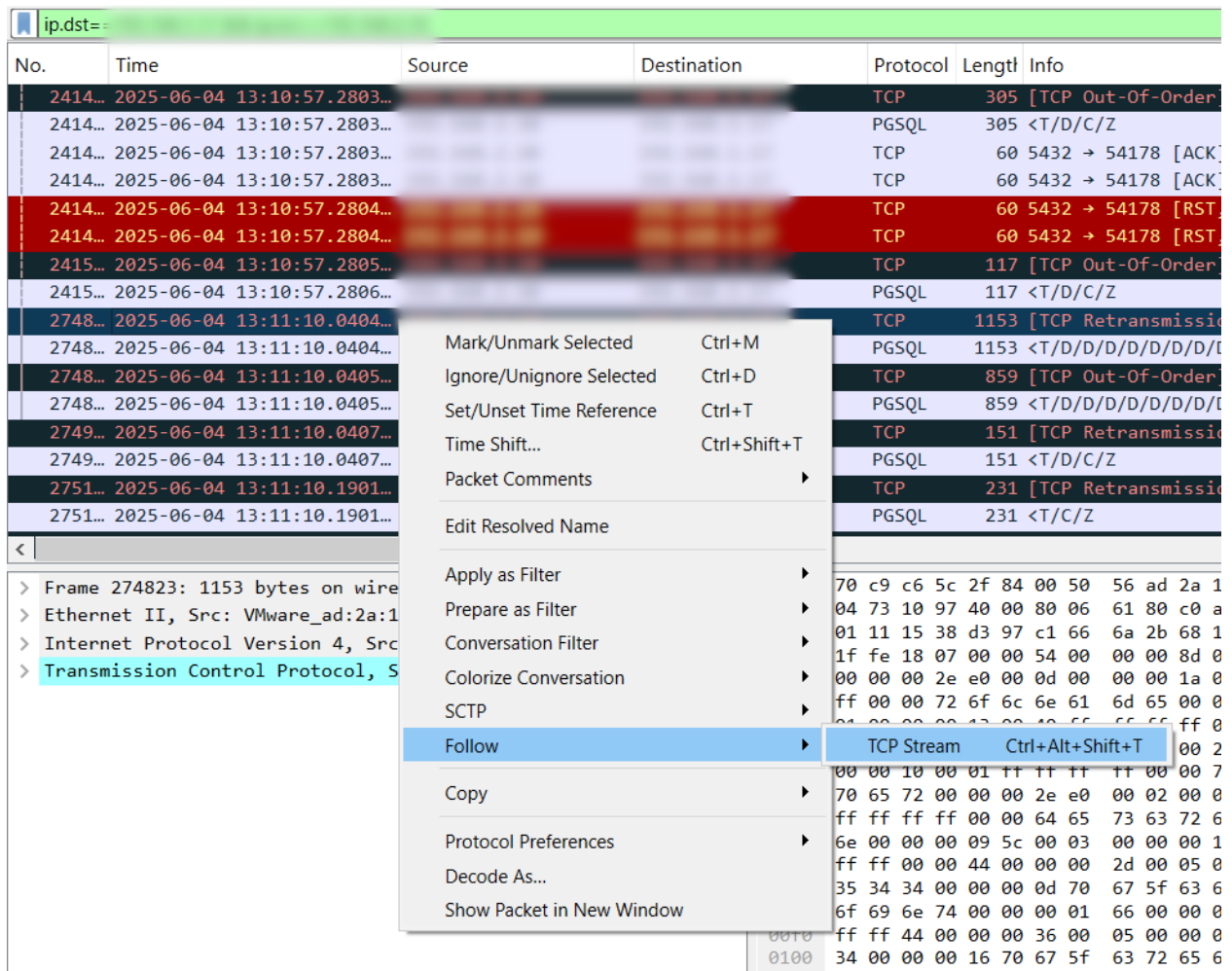
2234 **Figure 4-141: List of all conversations between multiple IP addresses**

2235 The conversations window in Wireshark will show all of the communications between various IP  
 2236 addresses. In the above screenshot, the highlighted line is the IP addresses between the data historian  
 2237 database and the JumpHostVM1. From here, right-click on that line and filter the packets based on this  
 2238 communication:



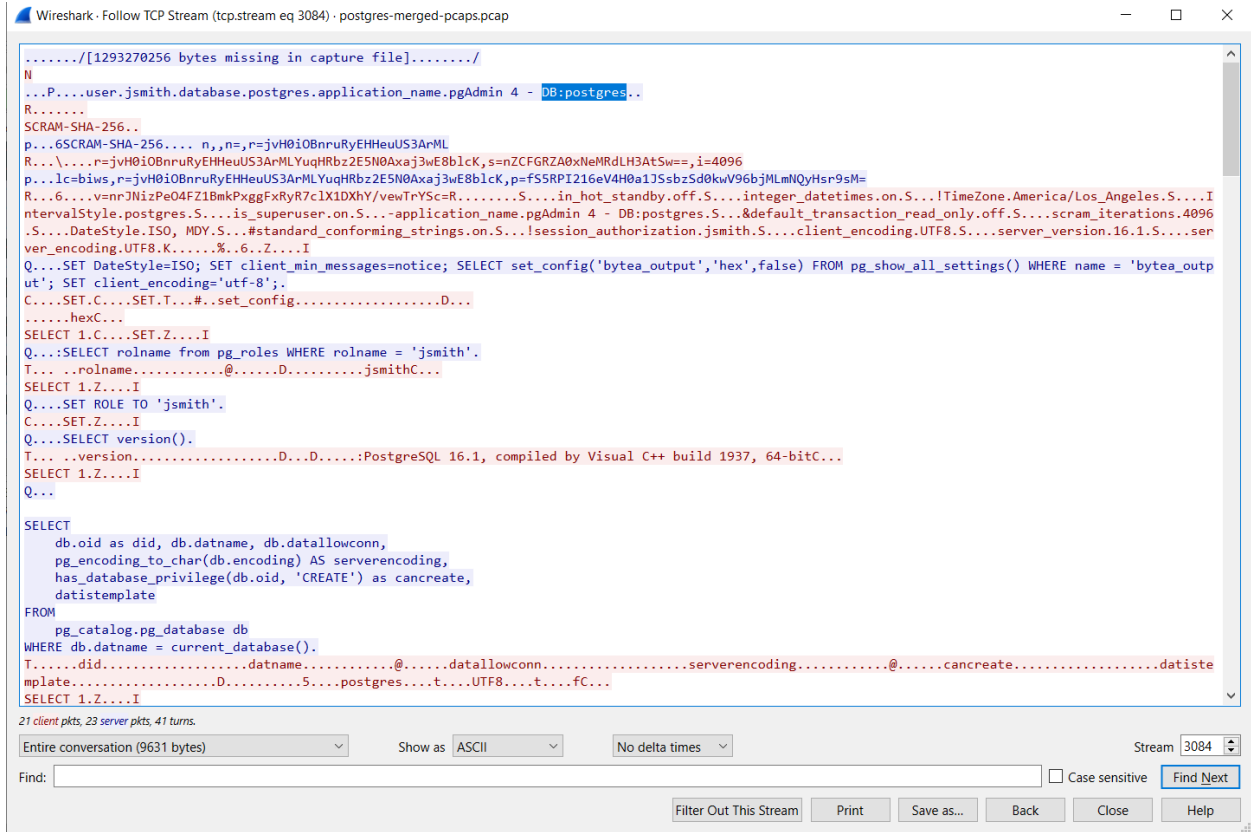
2239 **Figure 4-142: Applying a filter in Wireshark based on conversations**

2240 After the filter has been applied, seek a TCP packet with port 5432, the default for PostgreSQL, and the  
 2241 one we used for all scenarios. Once found, right-click, go to “Follow” and then “TCP Stream”. This will  
 2242 open a new window and display reassembled data of all the packets from that specific TCP connection.  
 2243 The default view is ASCII, so this can give a quick glance at the data involved in this communication. The  
 2244 following set of screenshots will show two separate TCP Streams. The first will highlight the main  
 2245 “postgres” database and the jsmith user seen throughout. For the scenario, this TCP Stream didn’t  
 2246 include full information, so we followed another stream to find more evidence.



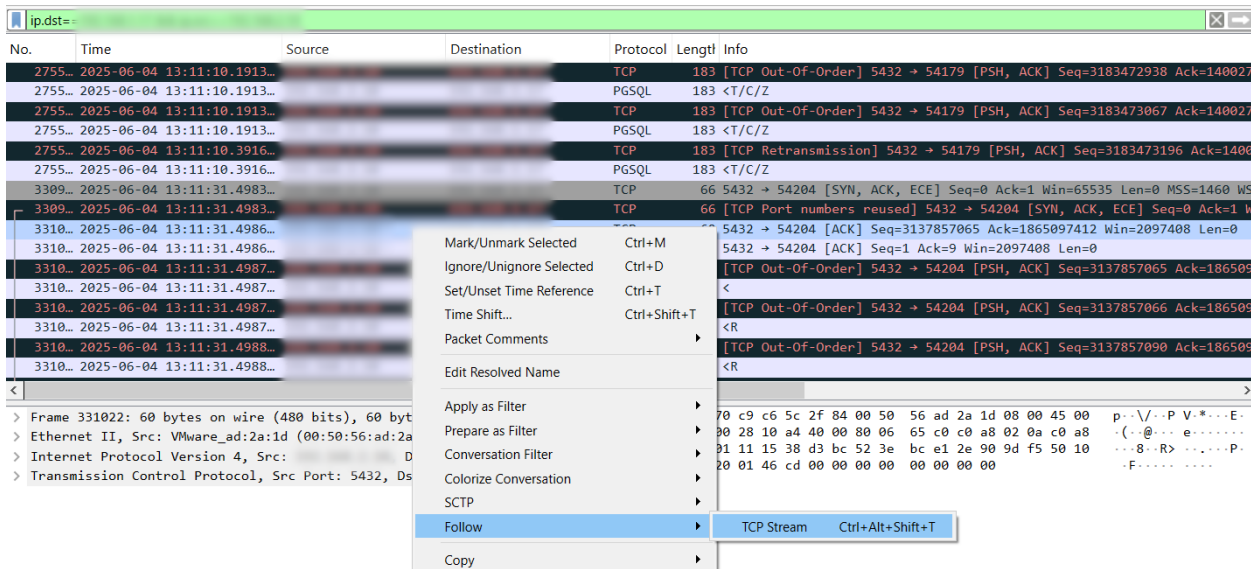
2247

Figure 4-143: Follow TCP Stream in Wireshark



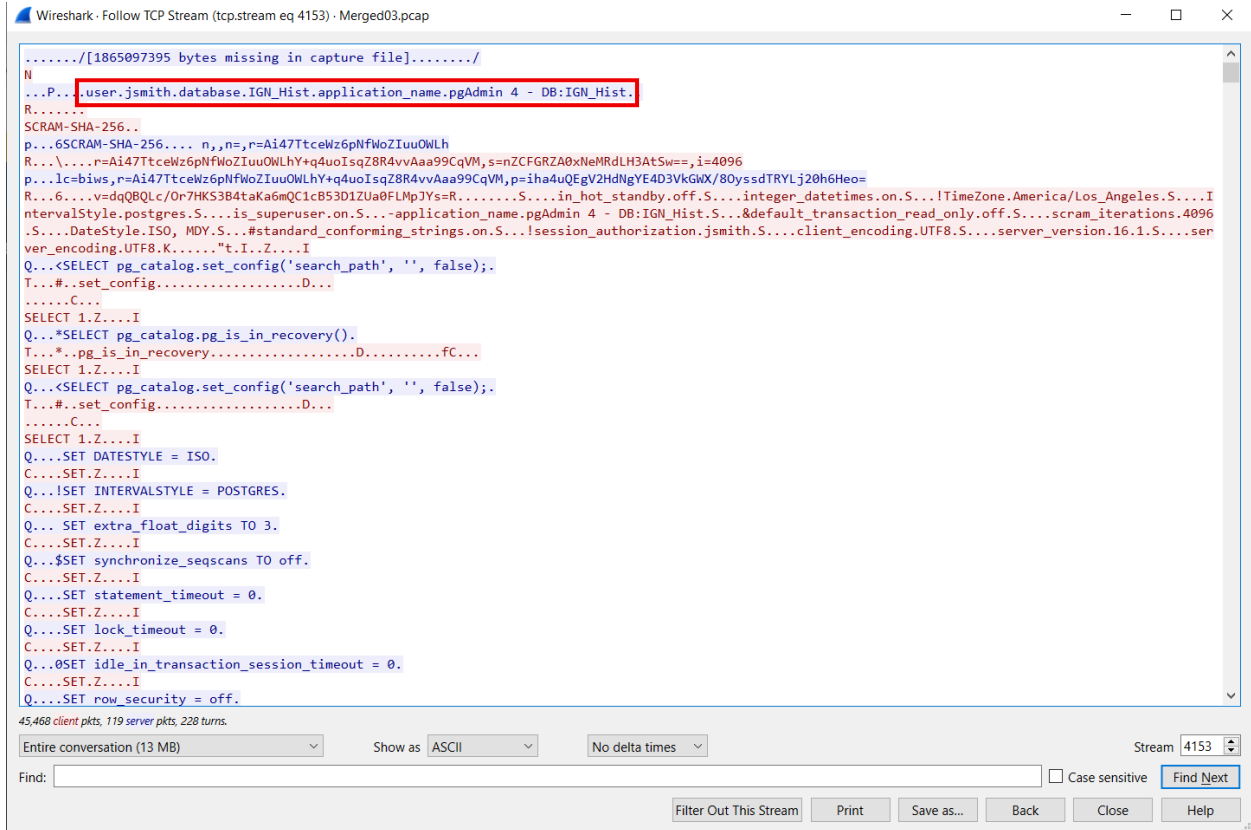
2248

Figure 4-144: A single TCP Stream for a set of packets



2249

Figure 4-145: Following another TCP Stream



2250

Figure 4-146: A new TCP Stream showing a different PostgreSQL database being targeted

```

Q...(SELECT set_config(name, 'view, foreign-table', false) FROM pg_settings WHERE name = 'restrict_nonsystem_relation_kind'.
T...#.set_config.....C...
SELECT 0.Z....I
Q...
BEGIN.
C...
BEGIN.Z....T
Q...?SET TRANSACTION ISOLATION LEVEL REPEATABLE READ, READ ONLY.
C...SET.Z....T
Q...<SELECT oid, rolname FROM pg_catalog.pg_roles ORDER BY 1.
T...6...oid....
.....rolname.....@.....D.....10...postgresD.....3373...
pg_monitorD...&.....3374.....pg_read_all_settingsD...#.....3375.....pg_read_all_statsD...%.....3377.....pg_stat_scan_tablesD...#.....4200.....pg_signal_ba
ckendD.....4544...
pg_checkpointD.....4550.....pg_use_reserved_connectionsD...&.....4569.....pg_read_server_filesD...'.4570.....pg_write_server_filesD...+.....4571.
...pg_execute_server_programD...#.....6171.....pg_database_ownerD...".6181.....pg_read_all_dataD...#.....6182.....pg_write_all_dataD...(.6304...
pg_create_subscriptionD.....16399...IgnitionD...$.32940...MFG\Domain AdminsD.....32941...replicaD.....32942...jsmithC...SELECT 19
.Z....T
Q...SELECT x.tableoid, x.oid, x.extname, n.nspname, x.extrelocatable, x.extversion, x.extconfig, x.extcondition FROM pg_extension x JOIN pg_namespace n ON
n.oid = x.extnamespace.
T.....tableoid.....oid.....extname.....@.....nspname...
7.....@.....extrelocatable.....extversion.....extconfig.....extcondition.....D...D.....3079...
.14965...plpgsql...
pg_catalog....f...1.0.....C...
SELECT 1.Z....T
Q...SELECT classid, objid, refobjid FROM pg_depend WHERE refclassid = 'pg_extension':regclass AND deptype = 'e' ORDER BY 3.
T...S...classid...
0.....objid...
0.....refobjid...
0.....D.....1255...14966...14965D... ..1255...14967...14965D... ..1255...14968...14965D... ..2612...14969...14965C...
SELECT 4.Z....T
Q...SELECT n.tableoid, n.oid, n.nspname, n.nspowner, n.nspacl, acldefault('n', n.nspowner) AS acldefault FROM pg_namespace n.
T.....tableoid...
7.....oid...
7.....nspname...
7.....@.....nspowner...
7.....nspacl...
7.....

```

2251 **Figure 4-147: Some key phrases found in TCP Stream to use for further investigation**

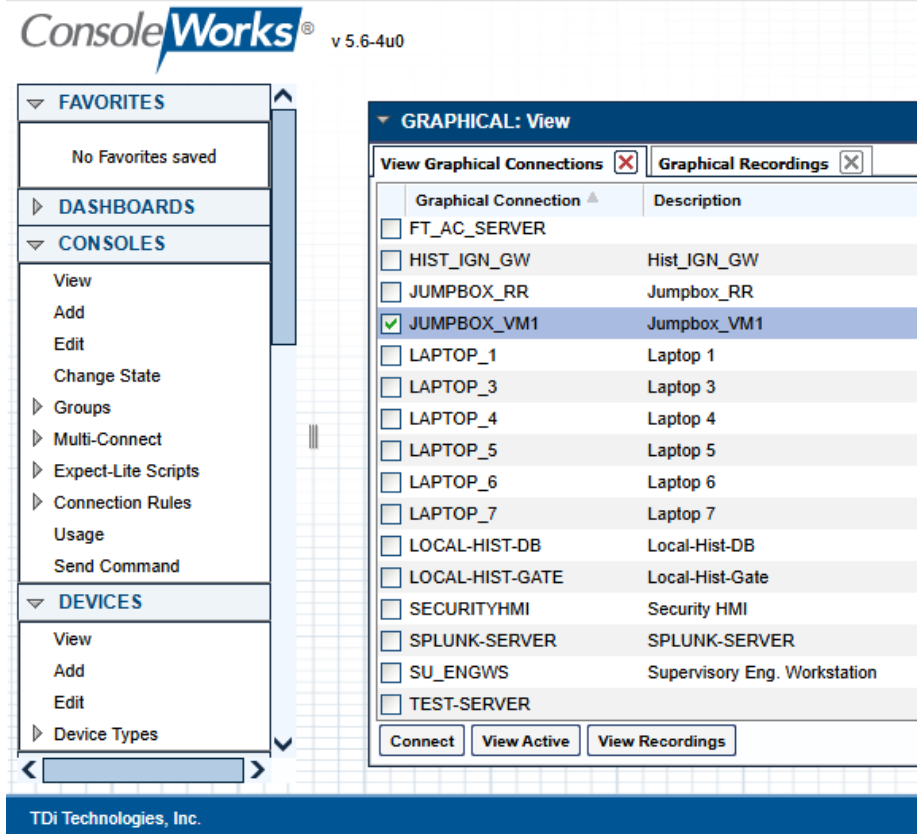
2252 In the second TCP Stream, we see similar items, like the jsmith user being named throughout, but this  
 2253 time we are now seeing the “IGN\_Hist” database, the Domain Admins AD group, and more instances of  
 2254 the jsmith user. For the scenario, it is deemed enough evidence to question the jsmith user.

2255 [\[Return to Scenario B\]](#)

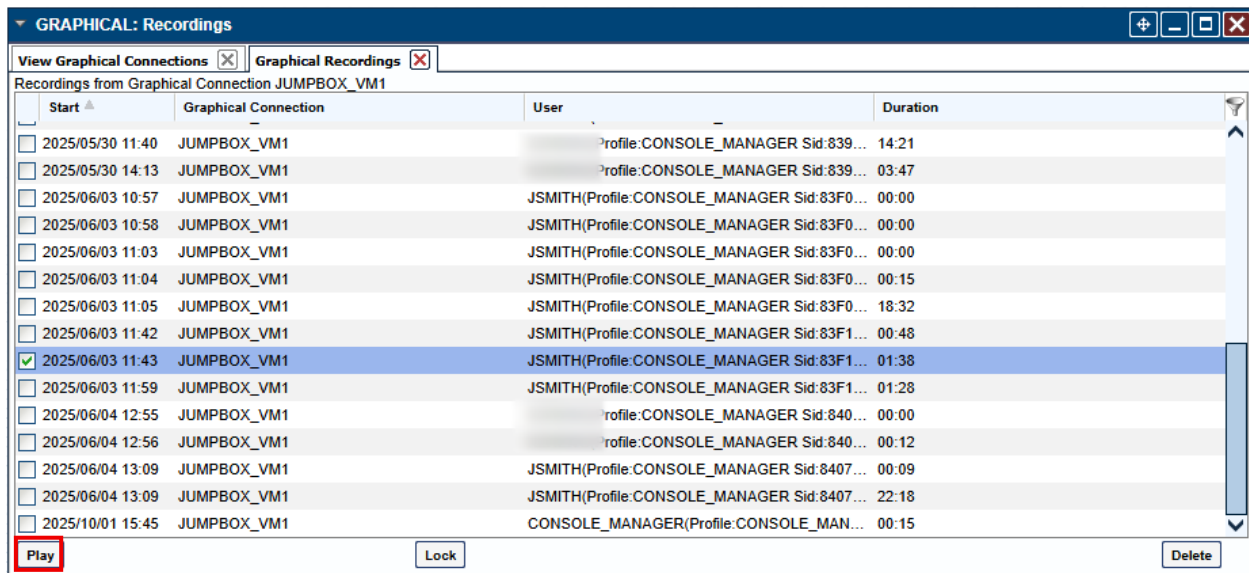
## 2256 C.5.13 Reviewing ConsoleWorks User Session

2257 With evidence pointing towards the jsmith user, the IRT views the desktop session of the jsmith user  
 2258 performing the action of downloading the database using the pgAdmin application. This is performed  
 2259 using the graphical recordings previously set up in section C.4.2. The following setup screenshots will  
 2260 showcase the IRT viewing the session from the jsmith user:

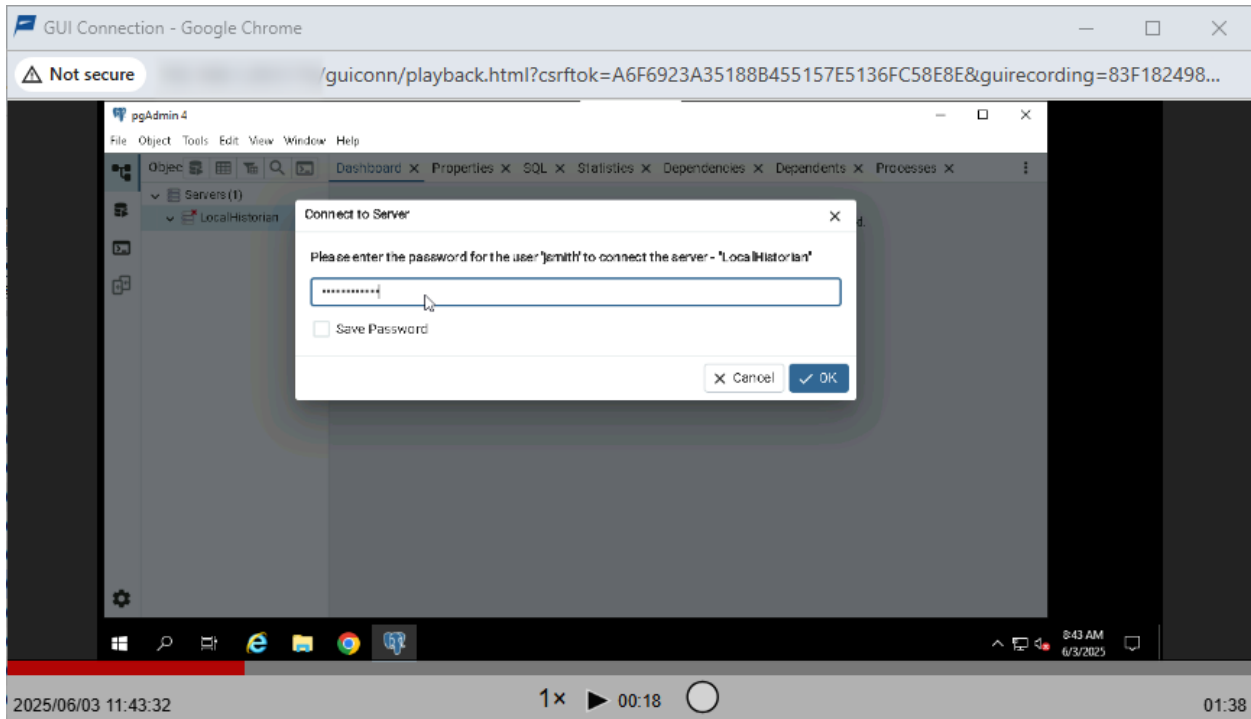
2261 *Note: Not all steps of the backup process in pgAdmin are shown.*



2262 Figure 4-148: Selecting the JumpBox VM in the graphical view in ConsoleWorks

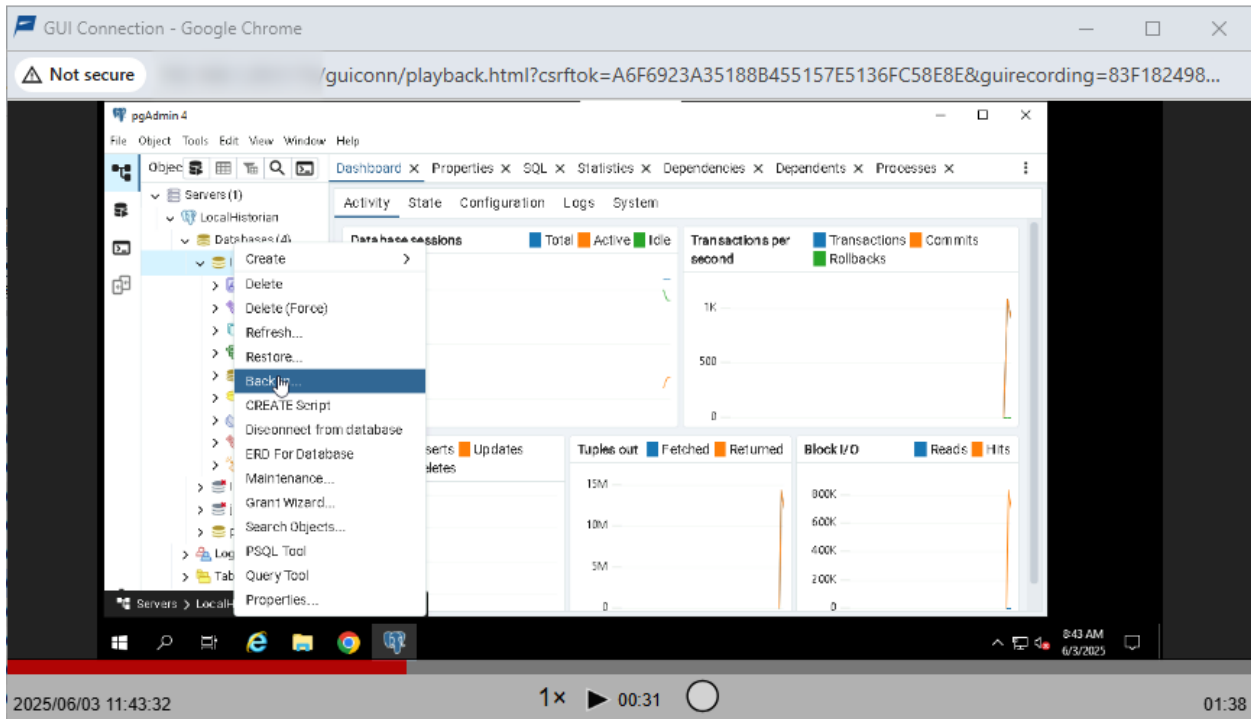


2263 Figure 4-149: Selecting the appropriate desktop session for the jsmith user



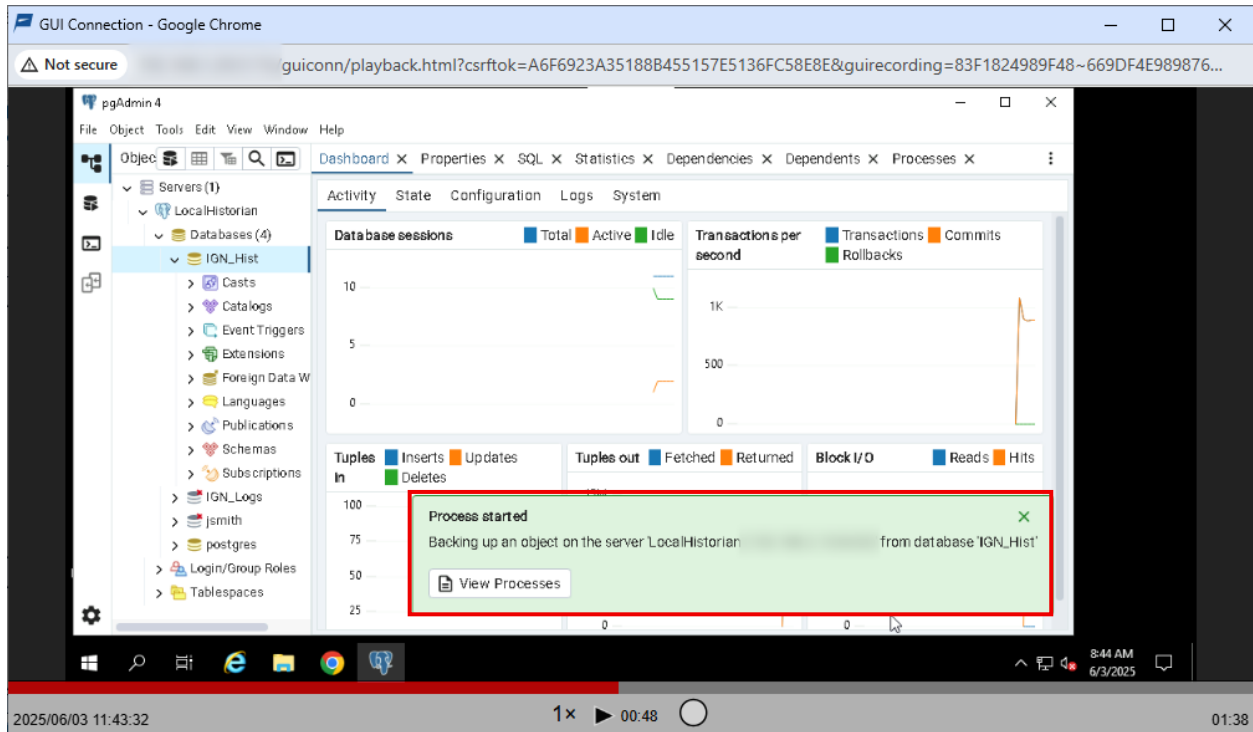
2264

Figure 4-150: The jsmith user logging into pgAdmin



2265

Figure 4-151: The jsmith user selecting “Backup” for the target database



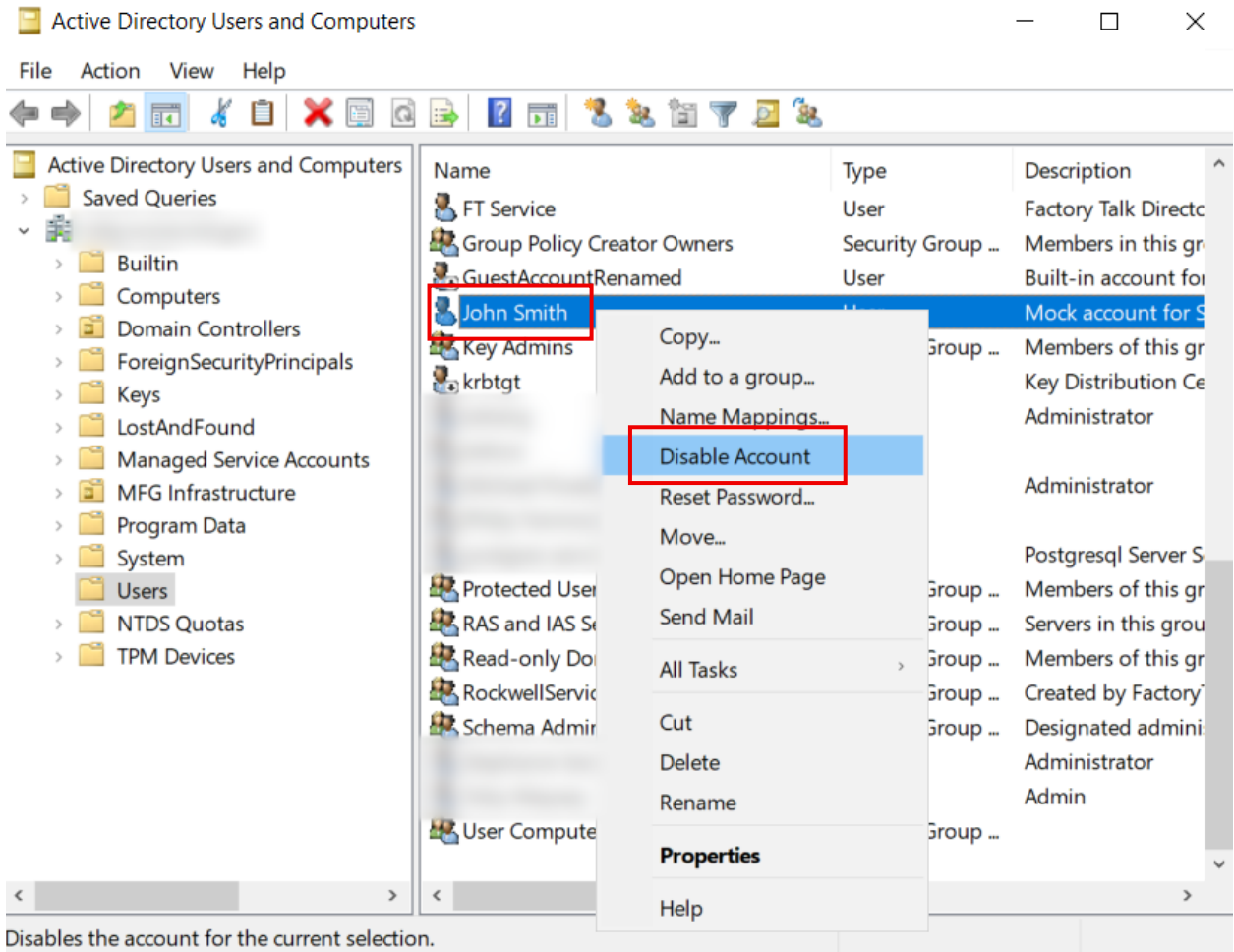
2266 **Figure 4-152: The jsmith user successfully backing up the IGN\_Hist database**

2267 [\[Return to Scenario B\]](#)

## 2268 C.5.14 Disable Compromised Accounts

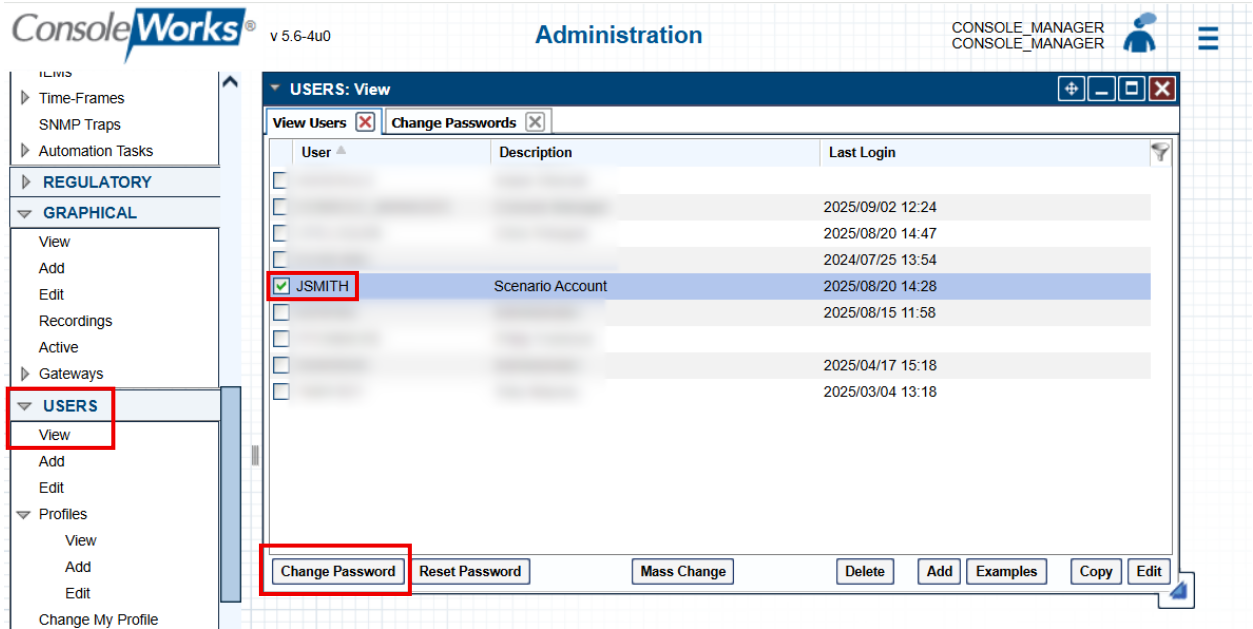
2269 Using Active Directory, corporate IT administrators disabled the remote connection from outside into  
 2270 the corporate asset that is exfiltrating data. The administrator also forced a password change for the  
 2271 compromised ConsoleWorks account. The corporate IT administrator made sure that the compromised  
 2272 account did not have access to the resources running in AWS.

2273 Administrators can disable the user account in Active Directory Users and Computers:

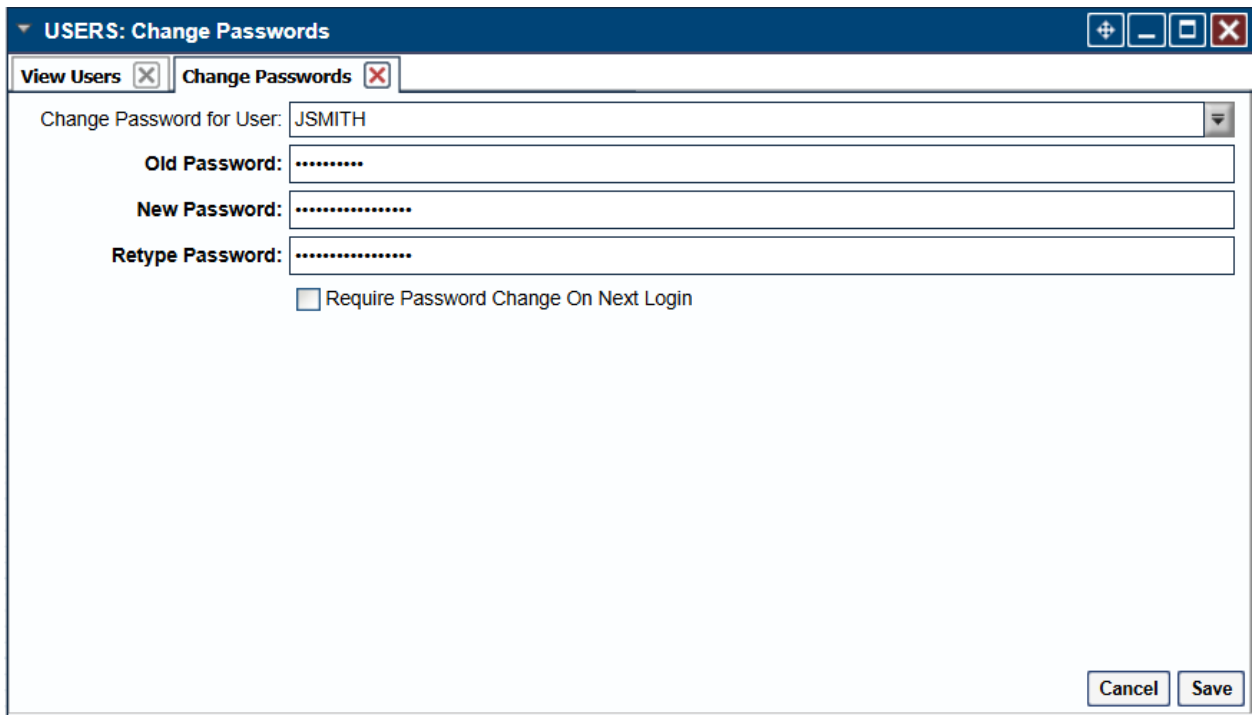


2274 **Figure 4-153: Disabling the jsmith user account in Active Directory**

2275 Within ConsoleWorks, administrators can edit the password of a user by going to the Users tab on the  
 2276 left side of the interface, going to View, and then choosing the user. From there, click the Change  
 2277 Password button on the bottom left, as seen below:



2278 Figure 4-154: Changing the jsmith user’s password in ConsoleWorks



2279 Figure 4-155: Changing the jsmith user’s password in ConsoleWorks

2280 [\[Return to Scenario B\]](#)

2281 [\[Return to Scenario C\]](#)

## 2282 C.6 Scenario B: Technical Details – Recovery

2283 The recovery process was not required for the Scenario B incident.

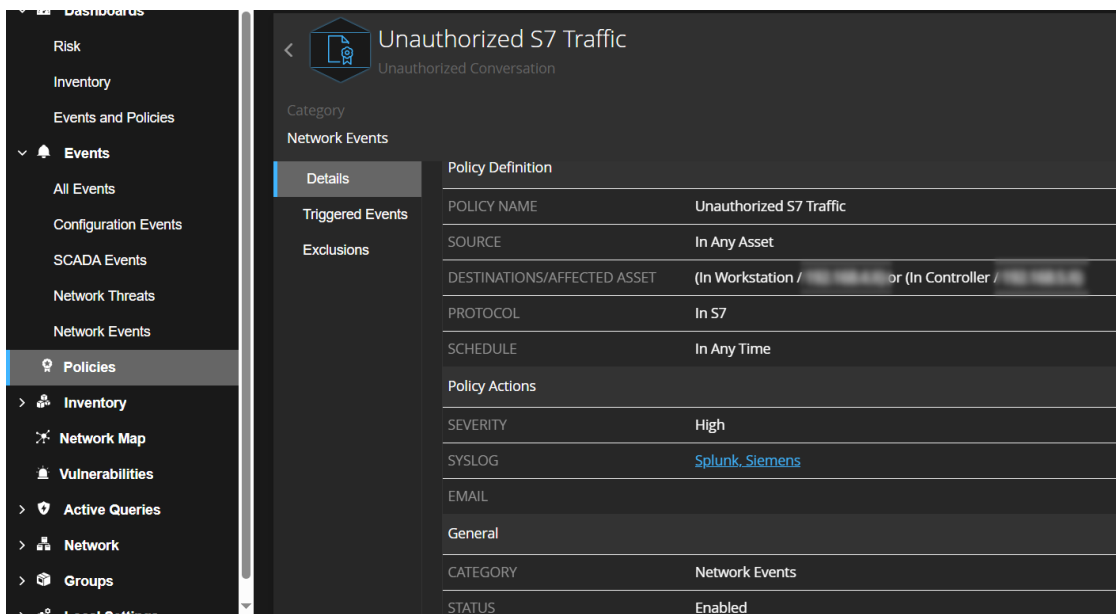
## 2284 C.7 Scenario C: Technical Details – Preparation

2285 Before an incident occurs, a manufacturer must prepare for incident response and recovery. The  
2286 following steps were taken to prepare for the Scenario C incident.

2287 [\[Return to Scenario C\]](#)

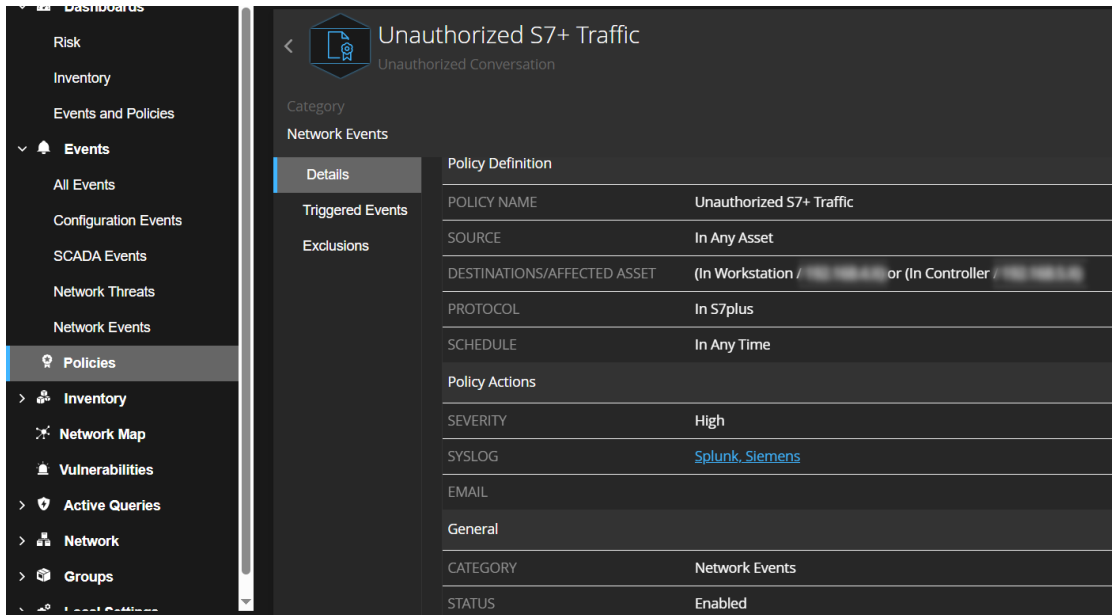
### 2288 C.7.1 Creating Siemens Traffic Detection Policy in Tenable

2289 Using section C.4.5 from Scenario B, follow those steps in creating the policy. The following set of  
2290 screenshots shows the selections made to create a Tenable policy for detecting unauthorized Siemens  
2291 network traffic. Two policies are created to trigger an alert every time they identify unauthorized traffic  
2292 to the Siemens Conveyor PLC:



2293 **Figure 4-156: Tenable policy to track unauthorized S7 traffic**

2294

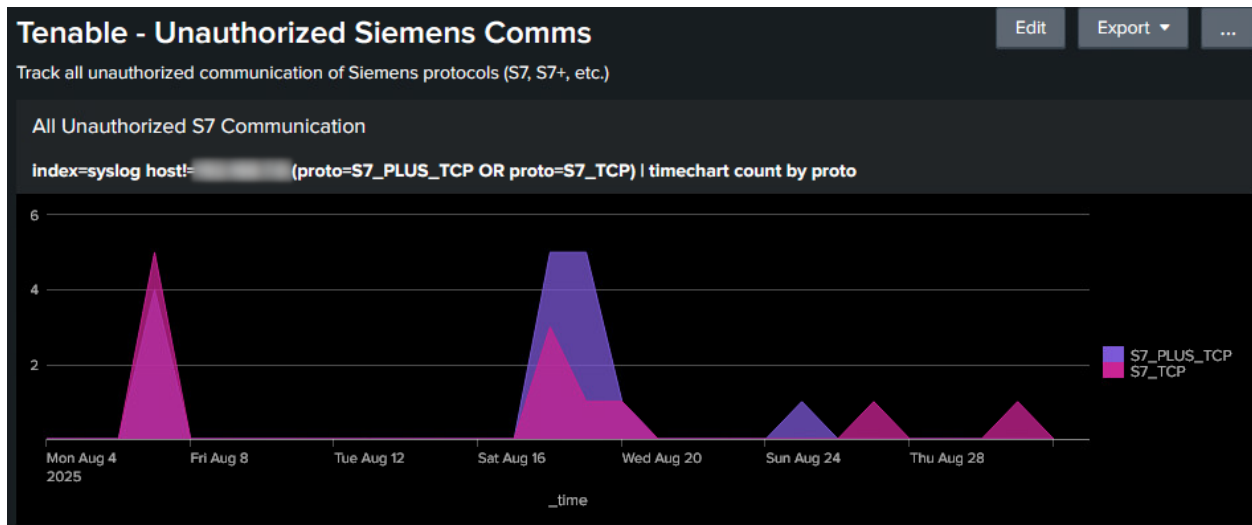


2295 **Figure 4-157: Tenable policy to track unauthorized S7+ traffic**

2296 [\[Return to Scenario C\]](#)

2297 **C.7.2 Creating Splunk dashboard for unauthorized Siemens traffic**

2298 Follow the instructions on C.4.6 on creating the dashboards. The following set of screenshots shows the  
 2299 dashboards created for this Scenario:



2300 **Figure 4-158: Splunk dashboard tracking unauthorized S7 and S7+ traffic**

Full Event Details of S7 Communications

index=syslog host! (proto=S7\_PLUS\_TCP OR proto=S7\_TCP) | table \_time, , suser, duser, proto, dpt, src, dst | rename suser as "Source Host", duser as "Destination Host", proto as "Protocol", dpt as "Destination Port", src as "Source IP", dst as "Destination IP" | sort -\_time

_time	Source Host	Destination Host	Protocol	Destination Port	Source IP	Destination IP
2025-08-31 17:59:53	LOCAL-HIST-GATE	PLC_1	S7_TCP	102		
2025-08-27 16:07:11	LOCAL-HIST-GATE	PLC_1	S7_TCP	102		
2025-08-25 17:11:27	MFG-LAPTOP1	PLC_1	S7_PLUS_TCP	102		
2025-08-20 14:35:00	LOCAL-HIST-GATE	PLC_1	S7_TCP	102		
2025-08-20 14:31:00	MFG-LAPTOP1	PLC_1	S7_PLUS_TCP	102		
2025-08-19 12:27:01	MFG-LAPTOP1	PLC_1	S7_PLUS_TCP	102		
2025-08-19 12:19:46	MFG-LAPTOP1	PLC_1	S7_PLUS_TCP	102		
2025-08-19 12:16:31	MFG-LAPTOP1	PLC_1	S7_PLUS_TCP	102		
2025-08-19 12:13:16	MFG-LAPTOP1	PLC_1	S7_PLUS_TCP	102		
2025-08-19 12:10:01	LOCAL-HIST-GATE	PLC_1	S7_TCP	102		

« Prev 1 2 3 Next »

2301 **Figure 4-159: Splunk dashboard tracking unauthorized S7 and S7+ traffic**

Unauthorized Communication Count by Day			Count of Unauthorized Communication by Source IP	
index=syslog host! (proto=S7_PLUS_TCP OR proto=S7_TCP)   timechart count by proto			index=syslog host! (proto=S7_PLUS_TCP OR proto=S7_TCP)   stats count by src   rename src as "Source IP", count as "Number of Unauthorized S7 Comms"   sort -count	
_time	S7_PLUS_TCP	S7_TCP	Source IP	Number of Unauthorized S7 Comms
2025-08-04	0	0		12
2025-08-05	0	0		11
2025-08-06	0	0		5
2025-08-07	4	5		
2025-08-08	0	0		
2025-08-09	0	0		
2025-08-10	0	0		
2025-08-11	0	0		
2025-08-12	0	0		
2025-08-13	0	0		

« Prev 1 2 3 Next »

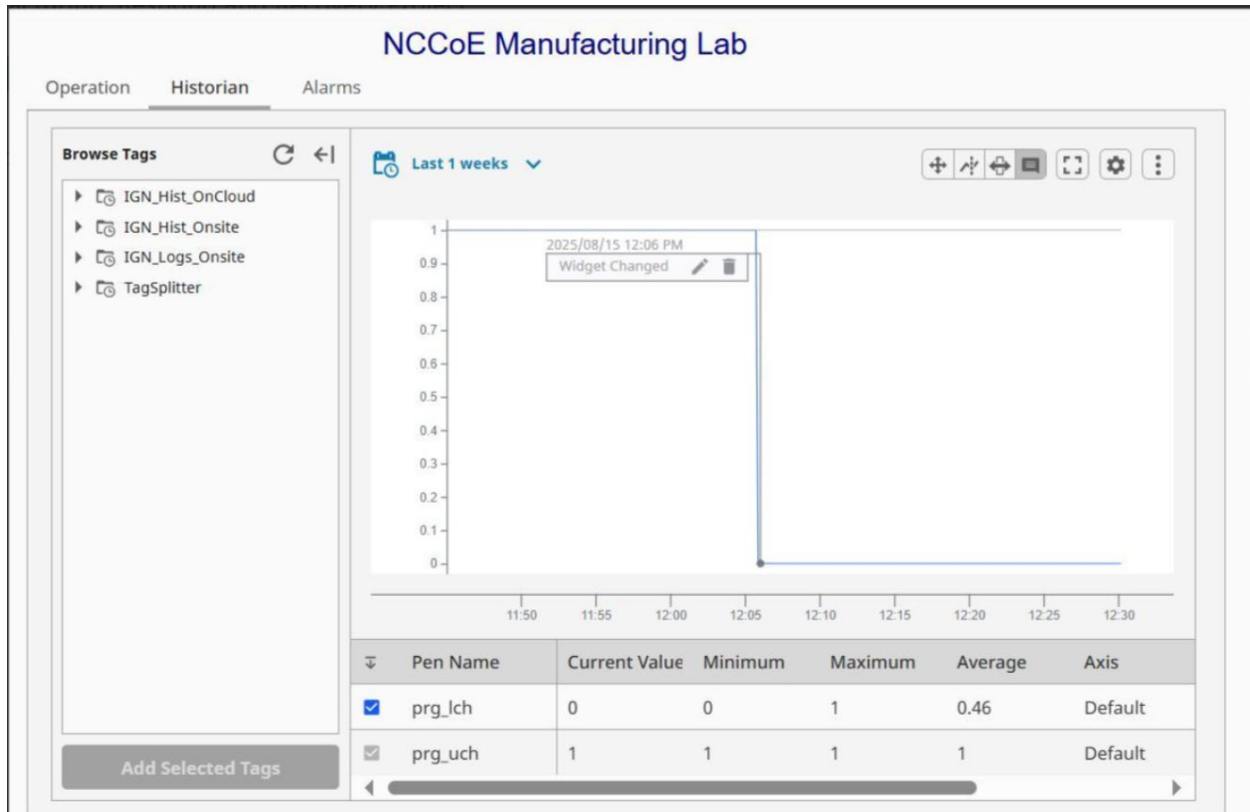
2302 **Figure 4-160: Splunk dashboard tracking unauthorized S7 and S7+ traffic**

2303 [\[Return to Scenario C\]](#)

## 2304 C.8 Scenario C: Technical Details – Response

### 2305 C.8.1 View Tags in Data Historian

2306 Inductive Automation’s Ignition software is used as the data historian. Engineers can use their data  
 2307 Historian of choice to add tags to view when operational changes were made. During the investigation,  
 2308 tags are viewed in the data historian to track when the widgets change from one color to another.



2309 **Figure 4-161: Enabling specific tags (PRG\_LCH and PRG\_UCH) in the data historian**

2310 [\[Return to Scenario C\]](#)

### 2311 C.8.2 Managing Dragos Tickets

2312 Refer to Scenario A sections C.2.1, C.2.7, and C.3.3 on how to create Dragos tickets, add comments, and  
 2313 close tickets. This section will cover multiple steps for the entire investigation of Scenario C.

## Create a New Case

Let's start by getting a few things out of the way to create your Case.

Name \*

Product Widgets Being Rejected During Off-Shift Operation

Priority \*

2

Visibility \*

Public

Hypothesis \*

Someone is changing the widget selection during the off-shift

Create as Incident

CANCEL

SUBMIT

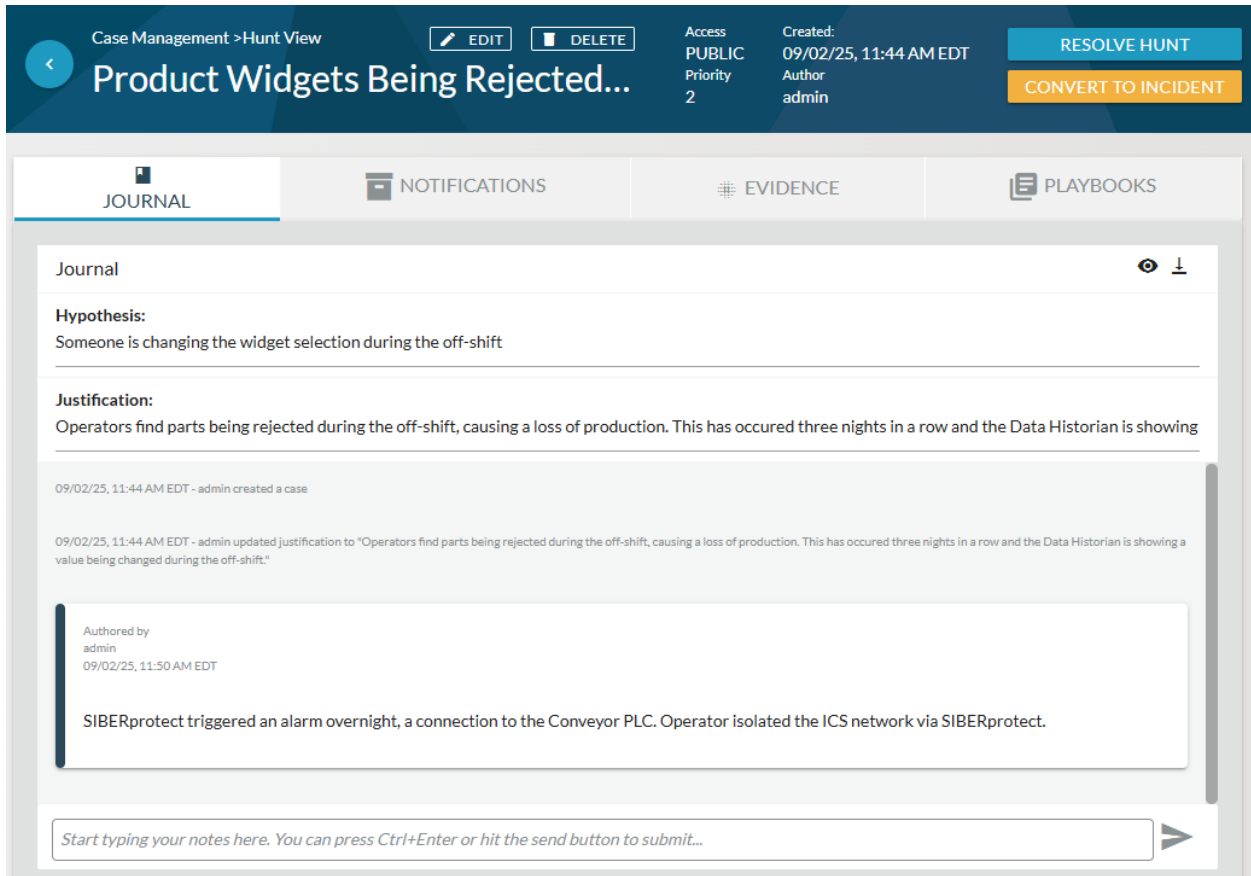
2314

Figure 4-162: Creating a new ticket in Dragos

The screenshot shows the Dragos interface for a case titled "Product Widgets Being Rejected...". The top navigation bar includes "Case Management > Hunt View", "EDIT", and "DELETE" buttons. The case details show "Access PUBLIC", "Priority 2", "Created: 09/02/25, 11:44 AM EDT", and "Author admin". There are "RESOLVE HUNT" and "CONVERT TO INCIDENT" buttons. Below the navigation bar are tabs for "JOURNAL", "NOTIFICATIONS", "EVIDENCE", and "PLAYBOOKS". The "JOURNAL" tab is active, showing a "Hypothesis" section with the text "Someone is changing the widget selection during the off-shift" and a "Justification" section with the text "Operators find parts being rejected during the off-shift, causing a loss of production. This has occurred three nights in a row and the Data Historian is showing". Below the justification are two entries: "09/02/25, 11:44 AM EDT - admin created a case" and "09/02/25, 11:44 AM EDT - admin updated justification to 'Operators find parts being rejected during the off-shift, causing a loss of production. This has occurred three nights in a row and the Data Historian is showing a value being changed during the off-shift.'" At the bottom is a text input field with the placeholder "Start typing your notes here. You can press Ctrl+Enter or hit the send button to submit..." and a send button.

2315

Figure 4-163: Adding a justification for the ticket



2316 **Figure 4-164: Updating the Dragos ticket to include the operator locking down the ICS network**

2317 During the investigation of Scenario C, management upgraded the priority from 2 to 5 and converted  
2318 from hunt status to incident.

## Edit Case

Case Title  
**Product Widgets Being Rejected During Off-Shift Operation**

---

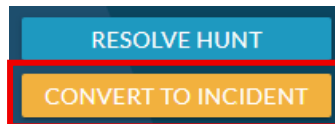
Access  
**Public**

Priority  
0 - Lowest  
1  
2  
3  
4  
**5 - Highest**

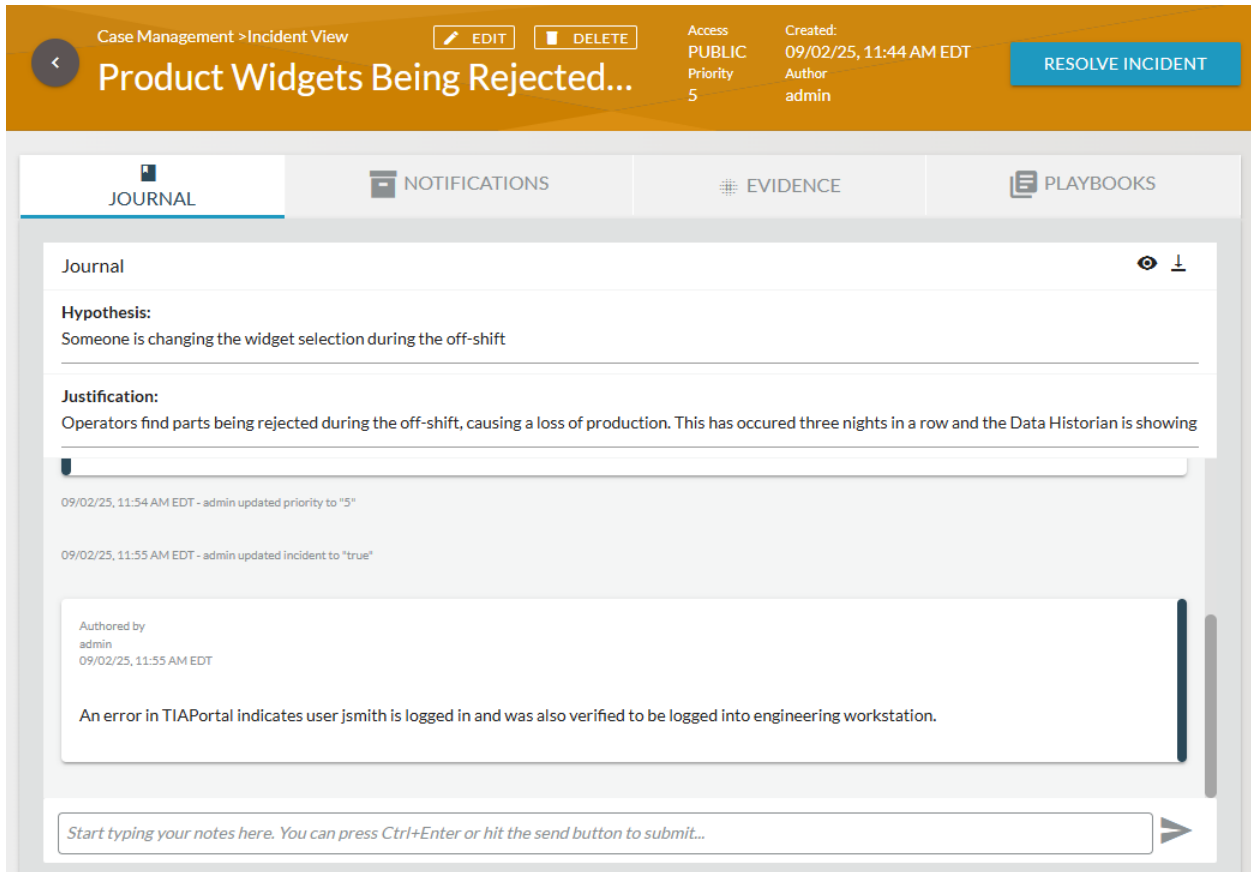
Watchers  
 Admin2       admin       SplunkConnection

CANCEL      **SAVE**

2319      **Figure 4-165: Changing the Dragos ticket priority to 5**



2320      **Figure 4-166: Converting the Dragos ticket to an incident**



2321 **Figure 4-167: Adding information about the jsmith user to Dragos ticket**

2322 The Dragos ticket is updated with the latest findings from the investigation:

Case Management > Incident View

EDIT DELETE

Access: PUBLIC  
Priority: 5

Created: 09/02/25, 11:44 AM EDT  
Author: admin

RESOLVE INCIDENT

JOURNAL NOTIFICATIONS EVIDENCE PLAYBOOKS

Journal

**Hypothesis:**  
Someone is changing the widget selection during the off-shift

**Justification:**  
Operators find parts being rejected during the off-shift, causing a loss of production. This has occurred three nights in a row and the Data Historian is showing

An error in TIAPortal indicates user jsmith is logged in and was also verified to be logged into engineering workstation.

Authored by  
admin  
09/02/25, 12:08 PM EDT

Met with user jsmith who denied logging into the system during the off-shift. Management came to conclusion that jsmith did not log in. The user account will be re-enabled with additional security measures once investigation is concluded.

Start typing your notes here. You can press Ctrl+Enter or hit the send button to submit...

2323 **Figure 4-168: Adding additional details to the Dragos ticket about the jsmith user**

2324 [\[Return to Scenario C - Initial Identification\]](#)

2325 [\[Return to Scenario C - Technical Event Handling\]](#)

2326 [\[Return to Scenario C - Cyber Incident Analysis and Response\]](#)

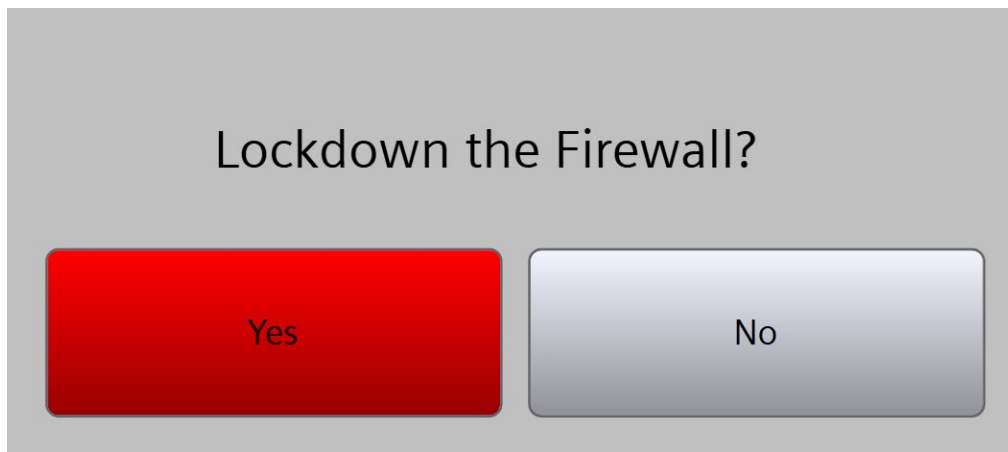
### 2327 C.8.3 Isolate ICS Network using SIBERprotect

2328 Tenable triggers an alert on the SIBERprotect Security HMI. The operator was informed by the engineer  
 2329 and analyst that a new alert may pop-up if a new system connects to the Conveyor PLC. When the alert  
 2330 pops-up on the Security HMI, the operator takes action to segment the physical components and  
 2331 controllers from the rest of the network by pressing a button on the Security HMI.



2332 **Figure 4-169: SIBERprotect HMI indicates threat detected**

2333 The operator selects Yes on the Operator Request to segment the networks.



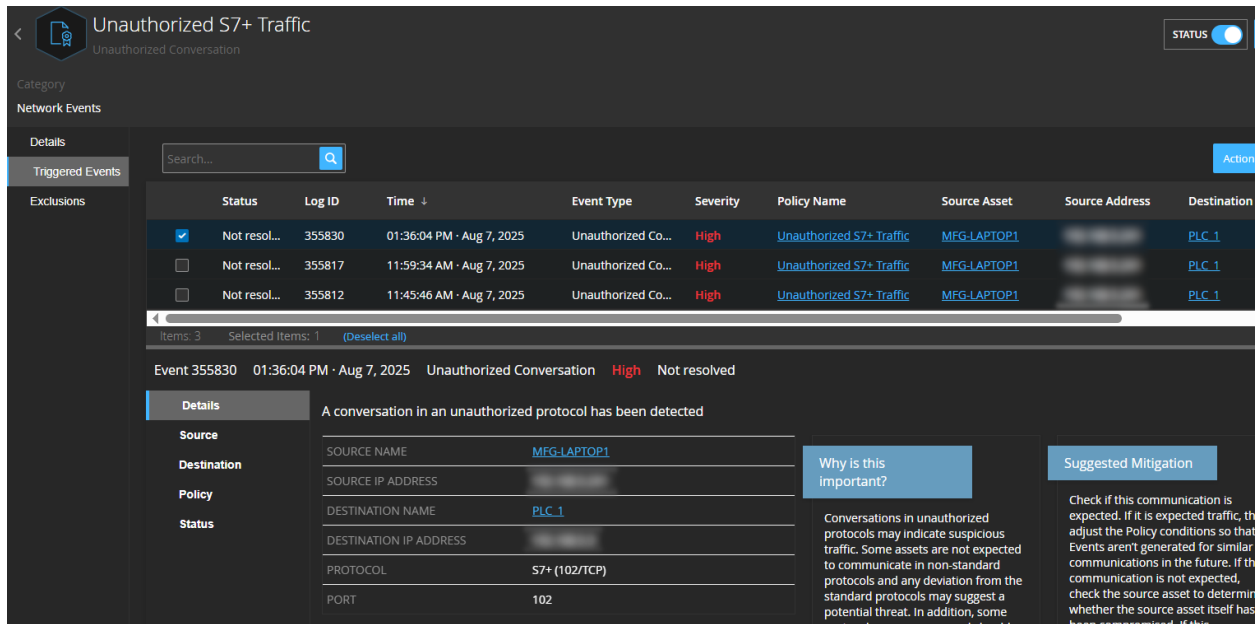
2334 **Figure 4-170: Operator lockdown (segment) selection**

2335 The conveyor and robot are segmented from the rest of the ICS network.

2336 [\[Return to Scenario C\]](#)

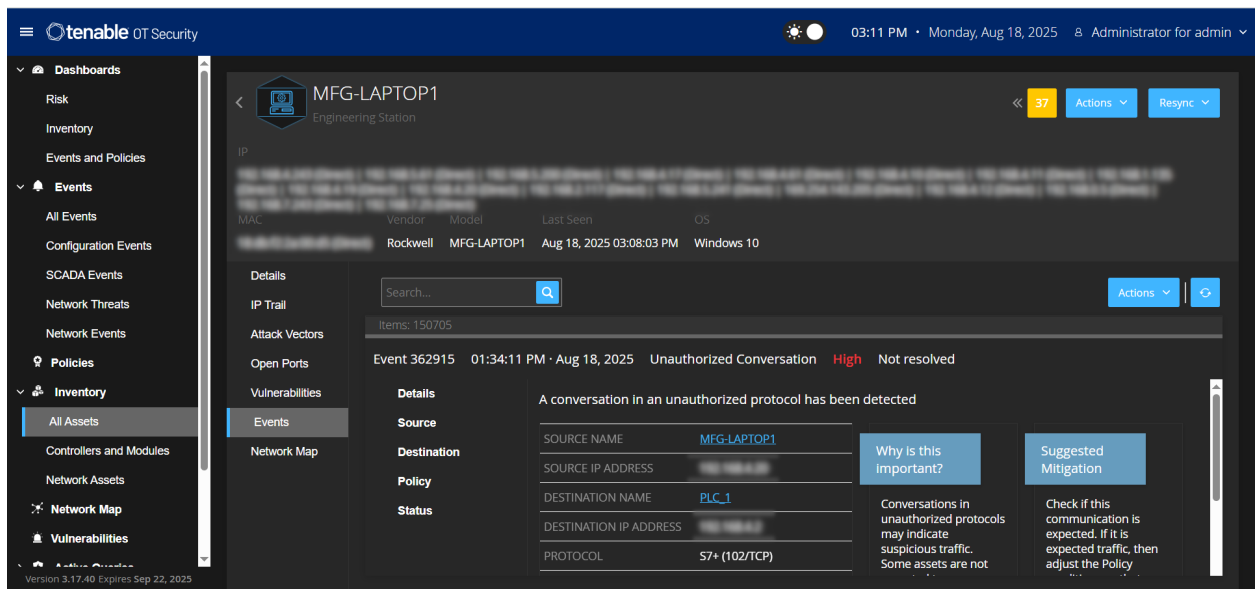
### 2337 C.8.4 Viewing policy violations in Tenable

2338 After Splunk indicates a policy violation, the analyst and engineer look in Tenable to identify further  
2339 details about this violation.



2340 Figure 4-171: All recent logs from the unauthorized S7+ traffic policy in Tenable

2341 Click on the source asset to dive deeper into the specific assets that were involved:

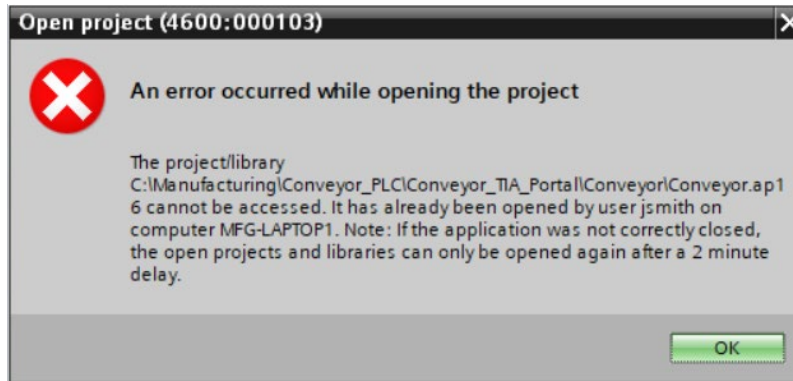


2342 Figure 4-172: Tenable alert showing the engineering workstation accessing PLC via S7+ connection

### 2343 C.8.5 TIA Portal Diagnostics

2344 Engineers can log into TIA Portal from the engineering workstation to troubleshoot issues with the  
 2345 manufacturing process. The software can be used to connect with the PLC, take backups of the program,  
 2346 modify logic, or monitor live variable information. During the course of the investigation, an engineer  
 2347 attempted to open the program file but was greeted with an error code that indicated another user had

2348 recently been in the program and disconnected improperly. This helped identify the root cause of the  
 2349 incident.



2350 **Figure 4-173: Error when opening the TIA Portal showing the user who was still logged into the system**

2351 [\[Return to Scenario C\]](#)

## 2352 C.8.6 Windows Task Manager

2353 Windows offers a Task Manager to identify processes, users, and other details about the system. In this  
 2354 scenario, Task Manager was used to verify that jsmith was recently logged into the machine and that  
 2355 their status is currently labeled as `Disconnected`.

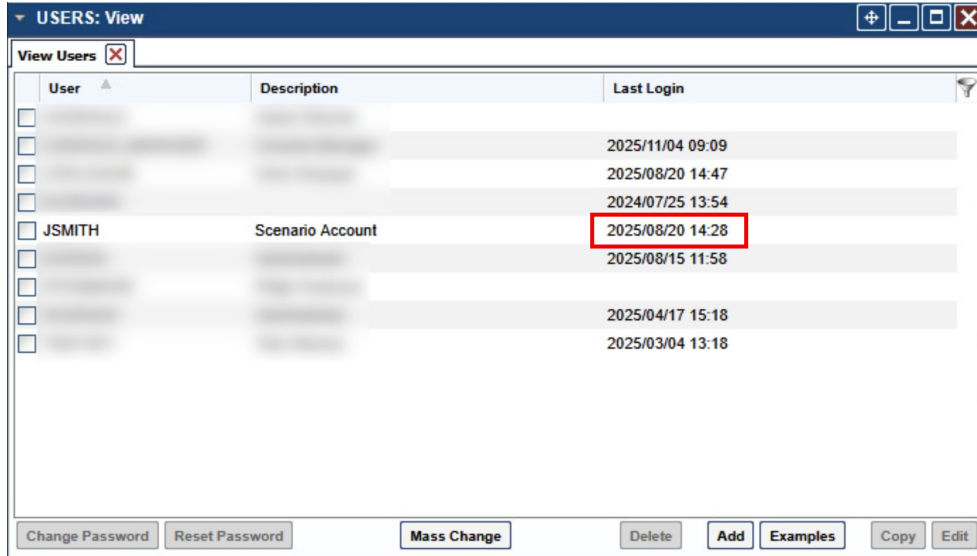
User	Status	CPU	Memory	Disk	Network	GPU	GPU engine
> jsmith (54)	Disconnected	1.5%	2,983.3 MB	0 MB/s	0.1 Mbps	0%	
		0.3%	1,752.0 MB	0.1 MB/s	0 Mbps	0%	

2356 **Figure 4-174: Task Manager in Windows showing the jsmith user was disconnected**

2357 [\[Return to Scenario C\]](#)

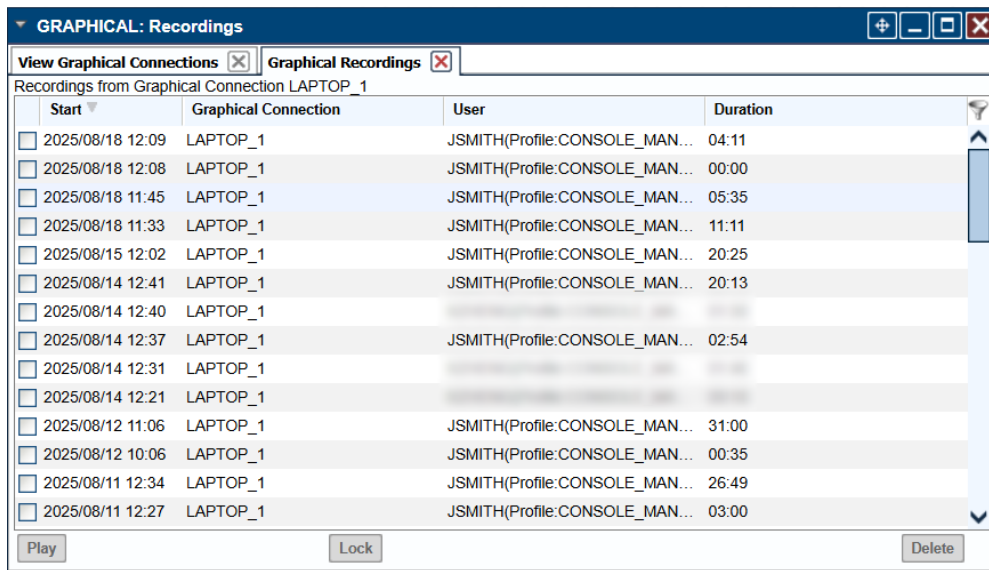
## 2358 C.8.7 Review ConsoleWorks Sessions for User Activity

2359 After discovering that a specific user was involved in an incident, ConsoleWorks can be used to view  
 2360 what the user was doing through a screen recording of the session:



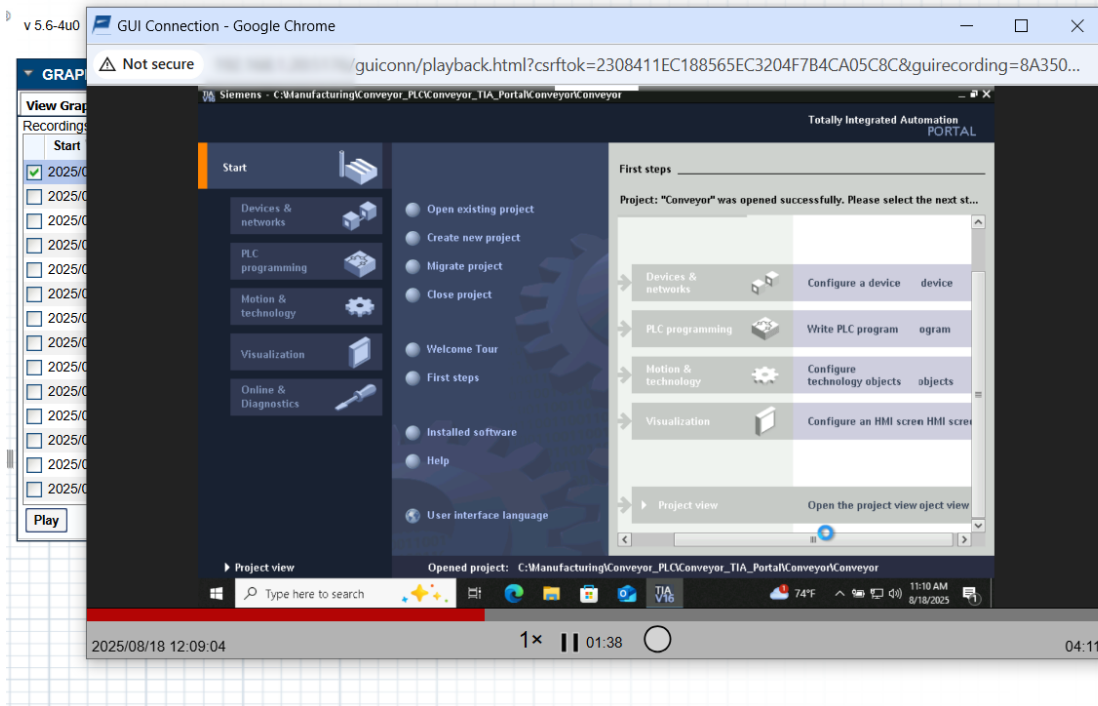
2361

Figure 4-175: Show the user's last login

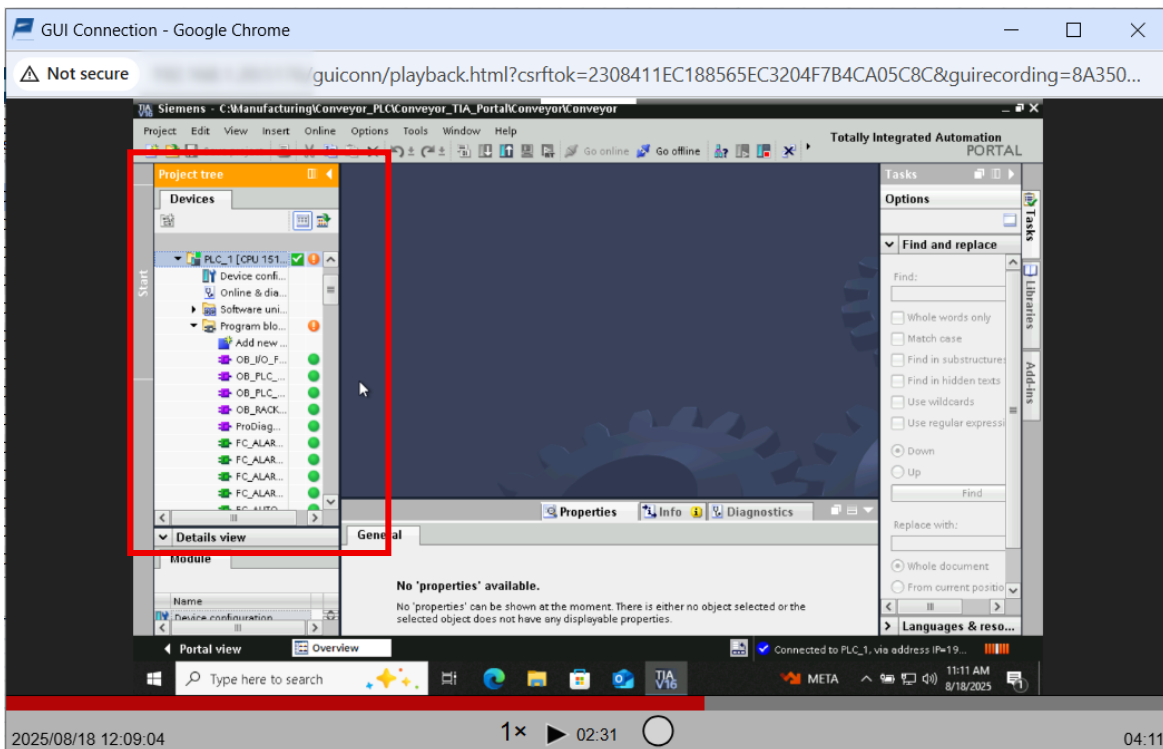


2362

Figure 4-176: Viewing the latest desktop recording of users



2363 Figure 4-177: Watching a recording of the jsmith user logging into the TIA Portal



2364 Figure 4-178: Recording of the jsmith user accessing PLC Tags

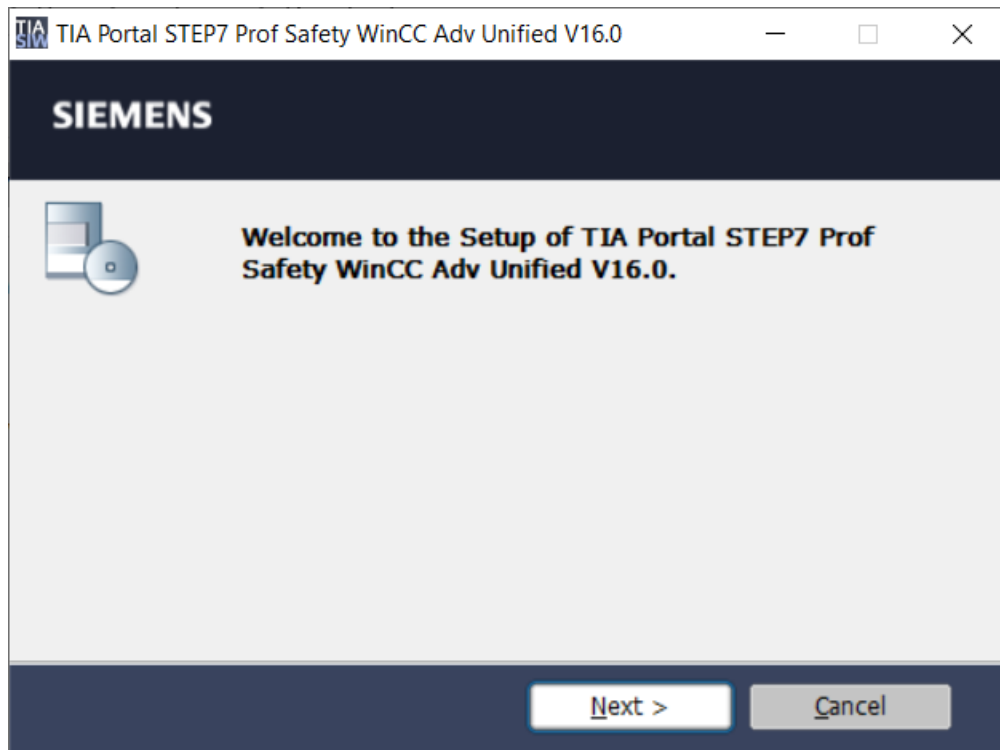
2365 Using ConsoleWorks Graphical view, the IRT sees the jsmith account change the process variable during  
 2366 live production. With this evidence, the user’s account can be either removed or disabled.

2367 [\[Return to Scenario C\]](#)

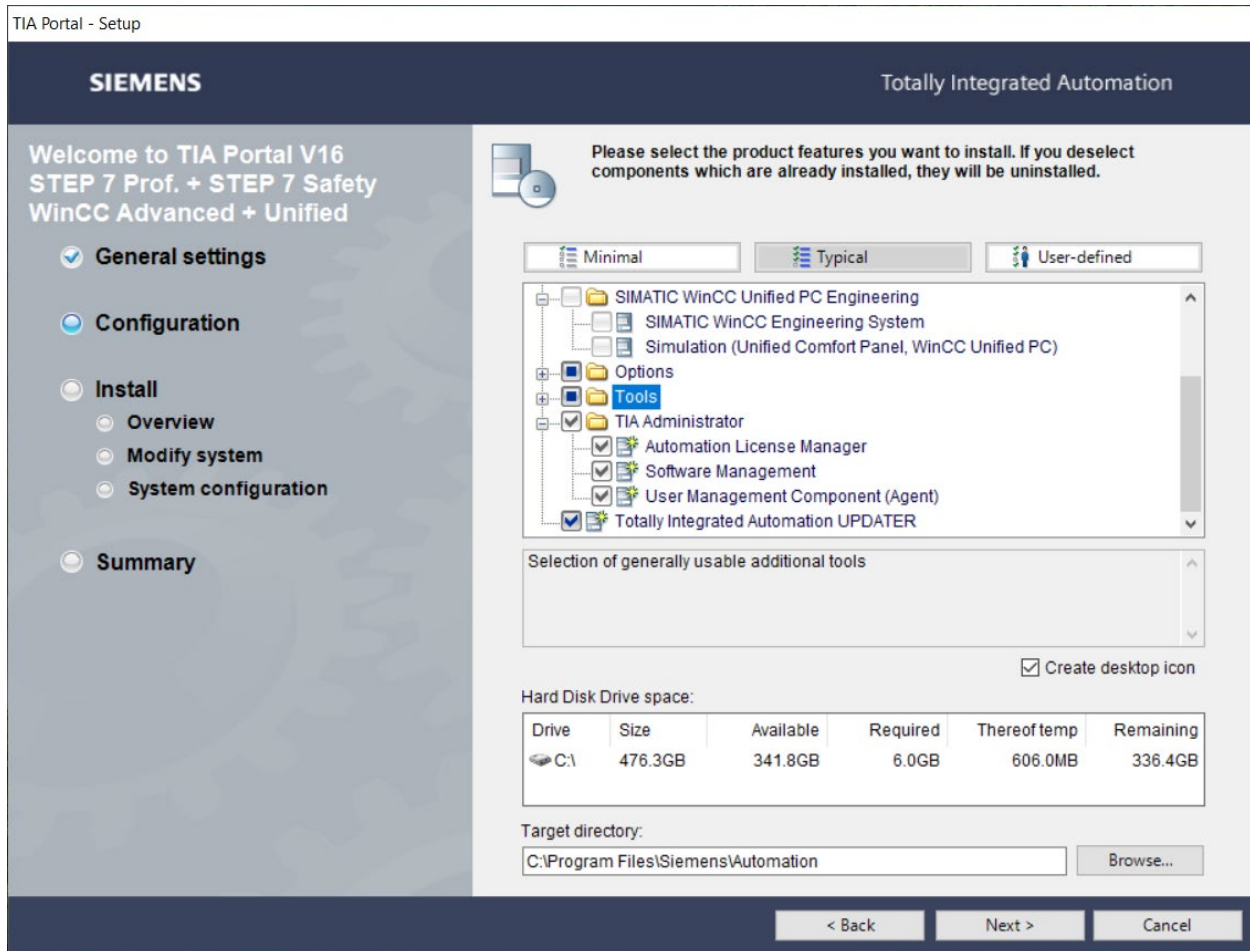
## 2368 C.9 Scenario C: Technical Details – Recovery

### 2369 C.9.1 TIA Portal Reinstall

2370 The IRT determined that the Engineering Workstation was compromised. The hardware is disconnected  
2371 from the network and handed over for forensic analysis. The TIA Portal Software is installed on a new  
2372 machine to allow for recovery of the PLC and continued operation while the investigation is ongoing.  
2373 The software is downloaded from the Siemens website. Follow the instruction prompts to install TIA  
2374 Portal with default settings as seen in the following screenshots.



2375 **Figure 4-179: TIA Portal install navigation menu**



2376 Figure 4-180: TIA Portal install settings

2377 [\[Return to Scenario C\]](#)

## 2378 C.9.2 Download PLC Backup Program File from ForceField

2379 Once the factory reset has been performed on the PLC, download the latest known-good version from  
 2380 the ForceField backup server:

## ForceField Zero Trust Storage™ Running on Host: qnode7

SerialNum	Device	UpLoad
[Redacted]	/dev/sdf	Upload
[Redacted]	/dev/sdg	Upload
[Redacted]	/dev/sdh	Upload
[Redacted]	/dev/sdi	Upload

2381 **Figure 4-181: ForceField web interface**

2382 *Note: We blurred out sensitive information. Users should click on the name of the device’s serial number*  
 2383 *to access the stored files.*

**Host: qnode7**      **Listing of WFS DEVICE=/dev/sdg, SERIALNO=**

Filename	Ext#	Size	Created
<a href="#">NIST_NCCoE_Logo.jpg</a>	1	33.77K	20240129 16:25:42
<a href="#">SupervisorPLC.ACD</a>	1	2.06M	20241212 12:34:48
<a href="#">SupervisorPLC.ACD.ASC</a>	1	347	20241212 12:34:52
<a href="#">Conveyor_SLS_Nov16.zap16</a>	1	6.13M	20241212 15:06:51
<a href="#">Conveyor_SLS_Nov16.zap16</a>	2	8.97M	20241212 15:07:02
<a href="#">gripper_tutorial.urp</a>	1	2.65K	20250220 10:44:27
<a href="#">main.urp</a>	1	18.34K	20250220 10:44:27
<a href="#">main_new.urp</a>	1	18.35K	20250220 10:44:28
<a href="#">main_old_july23.urp</a>	1	18.51K	20250220 10:44:28
<a href="#">main-Old.urp</a>	1	18.55K	20250220 10:44:29
<a href="#">Supervisor.ACD</a>	1	1.96M	20250710 14:31:01
<a href="#">Program-Hashes.txt</a>	1	98	20250819 11:02:14
<a href="#">Conveyor_20250819_1036.zap16</a>	1	9.23M	20250819 11:31:40
<a href="#">Program-Hashes.txt</a>	2	202	20250819 11:35:49
<a href="#">Conveyor_20250819_1137.zap16</a>	1	5.46M	20250819 12:34:24
<a href="#">Conveyor_20250819_1137.zap16</a>	2	9.24M	20250819 12:34:34

16 File Extents on this Volume

2384 **Figure 4-182: Selecting the latest known-good backup for the Conveyor program**

2385 *Note: Links on this web interface will not have visual indicators/feedback, but still work when clicked on.*

2386 [\[Return to Scenario C\]](#)

### 2387 C.9.3 Add Password and Restore from Backup with TIA Portal

2388 It is determined that the PLC should be restored from backup as part of recovery and that password  
 2389 protection should be added to control access to the PLC. The backup file is downloaded to a newly  
 2390 provisioned engineering workstation with a fresh install of TIA Portal V16. The project file is opened in  
 2391 TIA Portal V16. From the navigation pane, PLC is expanded, and Device configuration is selected. As  
 2392 shown in Figure 4-183, under Protection & Security, the option to enter a password is selected, and a  
 2393 secure password is entered. The new project file must be compiled prior to downloading to the PLC. The

2394 PLC is selected from the navigation pane via a right-click from there is the option to compile the project,  
 2395 as shown in Figure 4-184. After compiling the project, it is downloaded to the PLC as shown in Figure  
 2396 4-185.

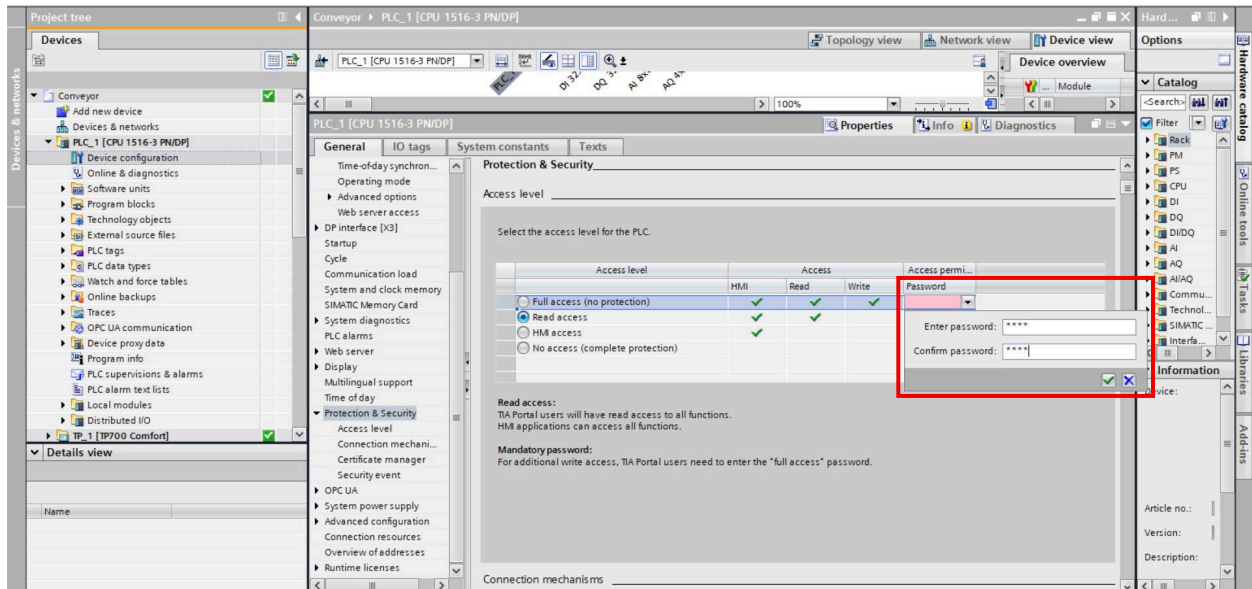
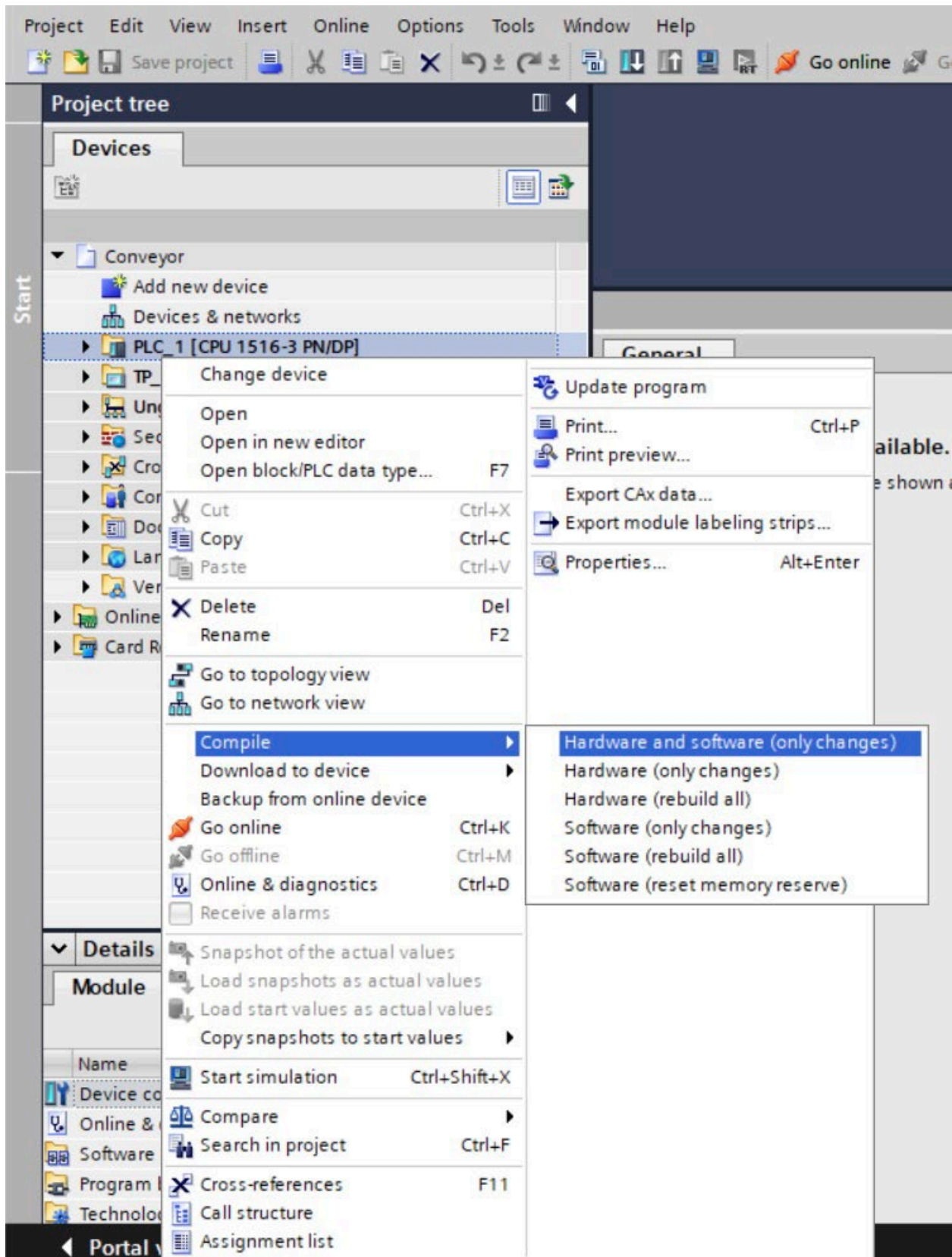
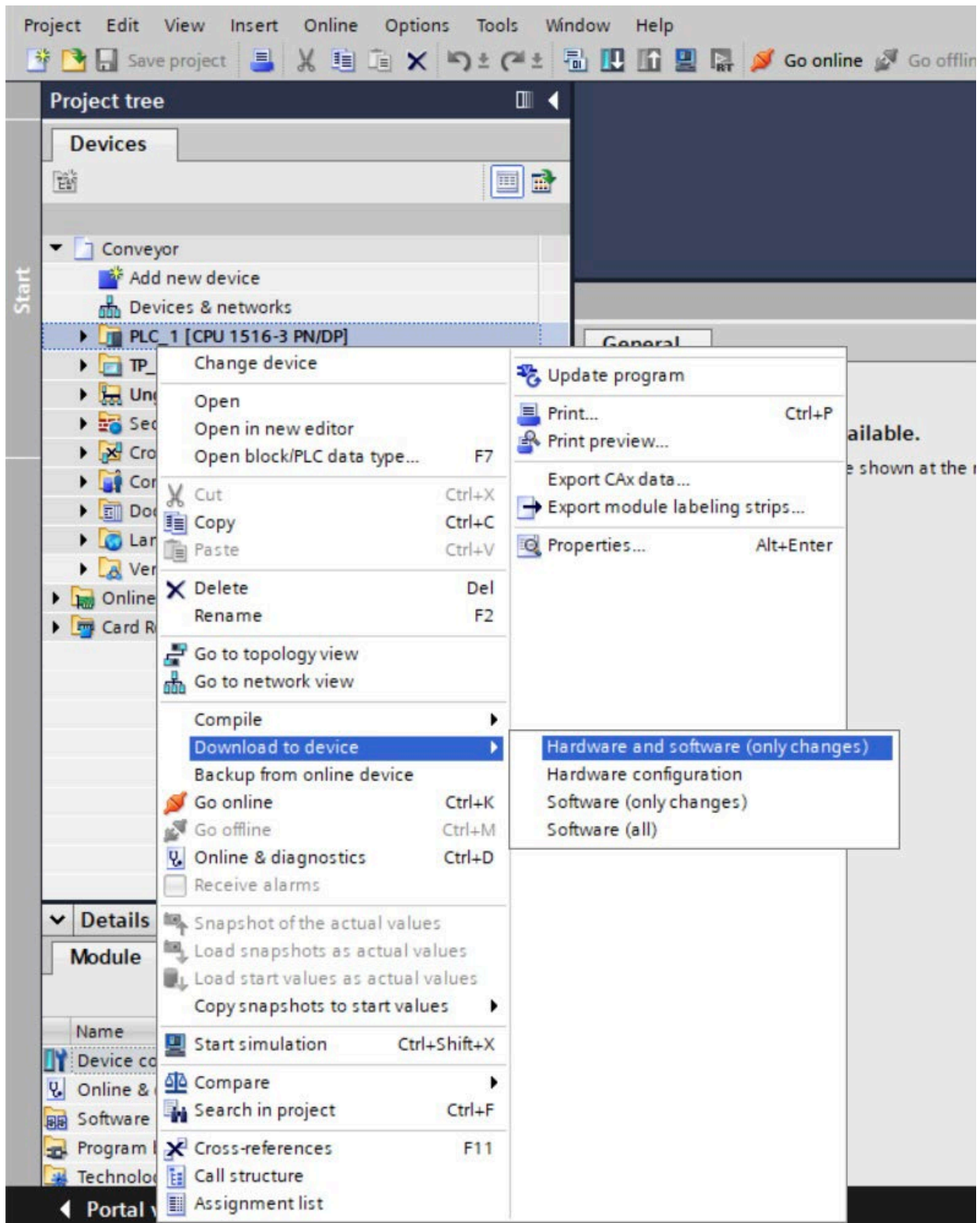


Figure 4-183: Adding a password to Siemens PLC in TIA Portal



2397

Figure 4-184: Compile PLC program



2398

Figure 4-185: Download configuration to PLC

2399 [\[Return to Scenario C\]](#)