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

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

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

NOTE TO REVIEWERS

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

You can view the project description, the web version, or the feedback portal from the Manufacturing Response and Recovery project page.

Comments on this publication may be submitted to: manufacturing_nccoe@nist.gov

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

DOCUMENT CONVENTIONS

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

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

CALL FOR PATENT CLAIMS

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

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

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

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

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

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

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

Such statements should be addressed to: manufacturing_nccoe@nist.gov

Contents

List of Figures

List of Tables

Executive Summary

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

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

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

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

1 Introduction

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

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

1.1 Scope

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

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

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

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

- Establishing case documentation for incidents

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

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

This practice guide focuses on:

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

1.2 Audience

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

- Asset owners and stakeholders
- Technology providers and integrators of ICS systems
- Critical Infrastructure operators
- Public and private utility providers
- State and Local government regulators

1.3 How to Use This Guide

This document is organized as follows:

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

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

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

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

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

2 Project Overview

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

2.1 Project Approach & Assumptions

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

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

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

2.2 Response and Recovery Challenges

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

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

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

In addition, ICS systems are also becoming more integrated with IT in their supporting ecosystem, creating new sets of challenges. Historically, ICS and their networks were isolated from business systems and IT networks. Isolation allowed for a limited attack surface; therefore, systems were designed for enhanced reliability with limited consideration for cyber incidents. As IT and ICS networks become more integrated, this increases the likelihood of an attack, and cybersecurity controls implemented in ICS environments have not kept pace with modern threats. The cyber risk mitigations used in IT networks (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:

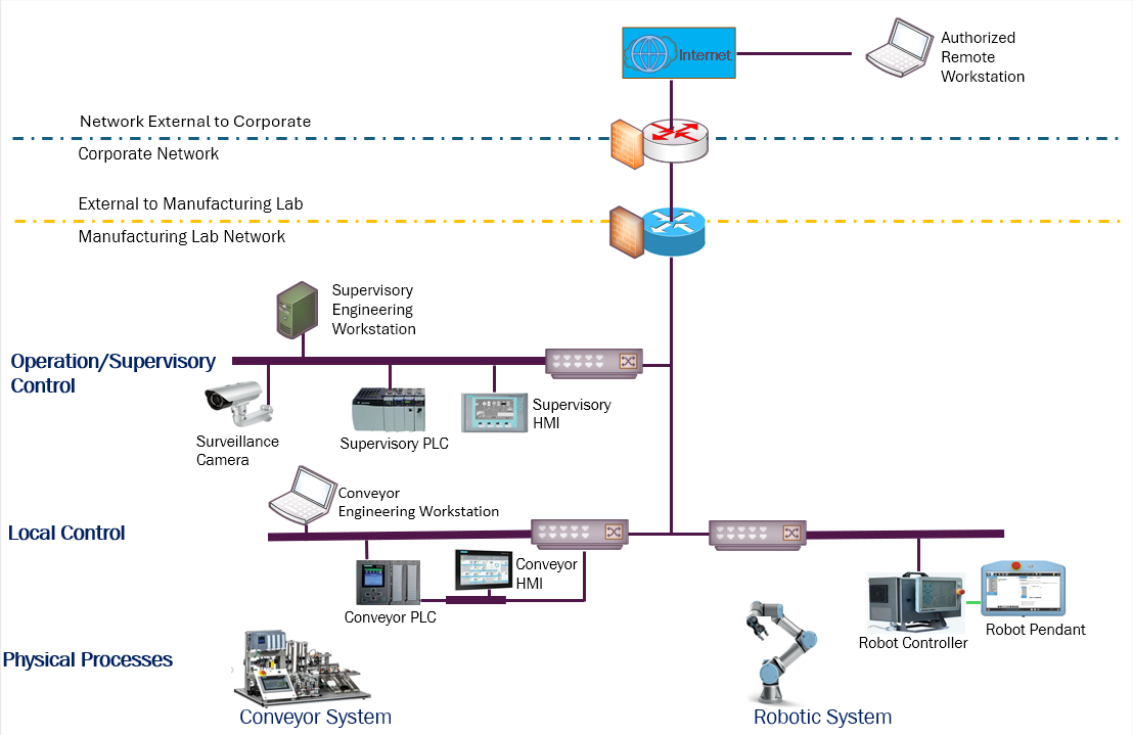
620 **Table 1: List of collaborators, their products, and their functions within the build architecture**

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

2.4 Build Architecture & Collaborator

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



625 **Figure 2-1: Discrete manufacturing without security tools**

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)
Analysis	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
Containment	RS.MI-01	Cisco	Industrial Security Appliance (ISA) 3000
		Siemens	SIBERprotect
Eradication	RS.MI-02	TDi Technologies	ConsoleWorks 5.6
Recovery	PR.DS-11	GreenTec USA	ForceField 1.9
	RC.RP-03 RC.RP-05	Rockwell Automation	FactoryTalk® AssetCentre Disaster Recovery
Resilient Infrastructure	PR.IR-03	Amazon Web Services (AWS)	AWS Infrastructure as a Service (IaaS)
	DE.CM-01	Garland Technology	High Density SPAN/TAP Aggregator INT1G10CSASP

2.4.2 Build Components

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

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

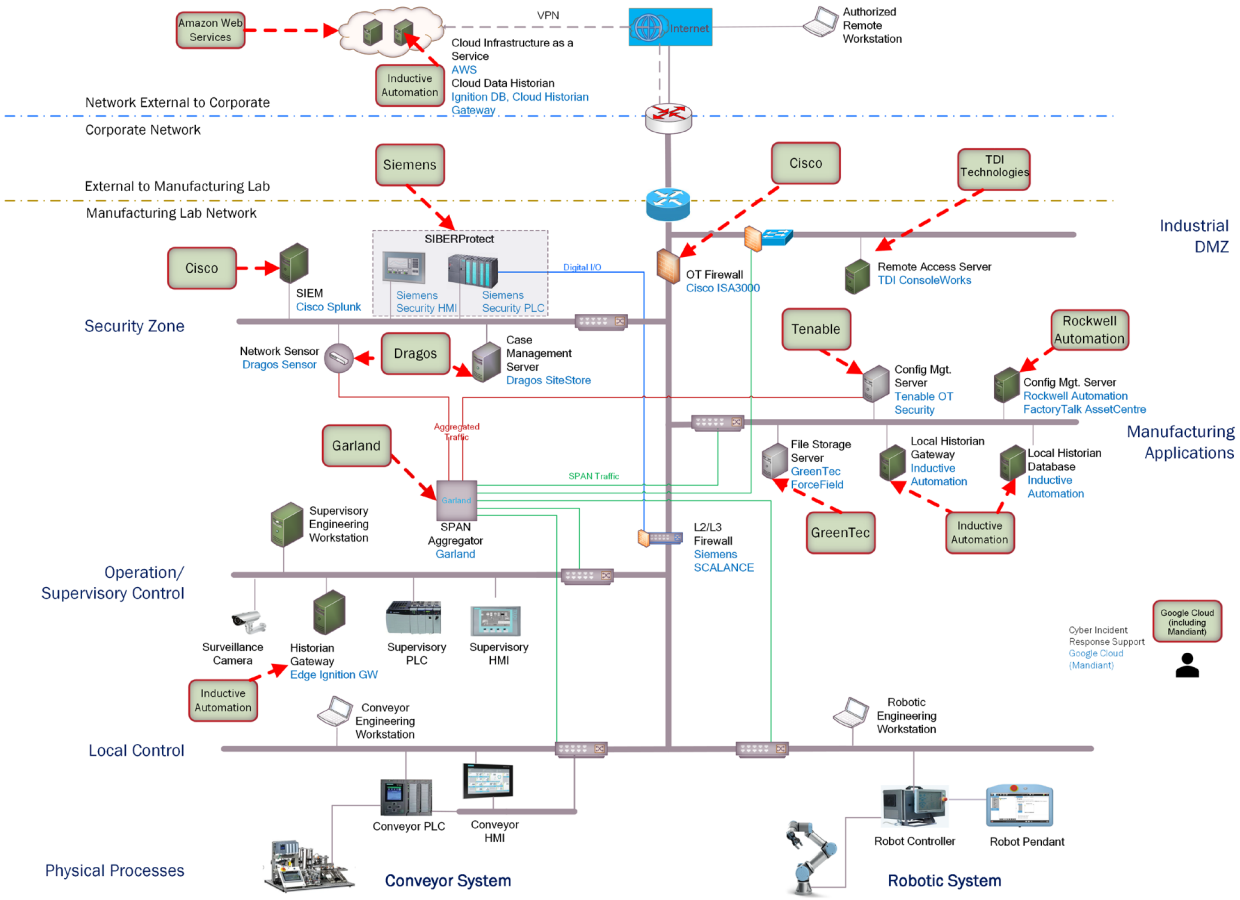
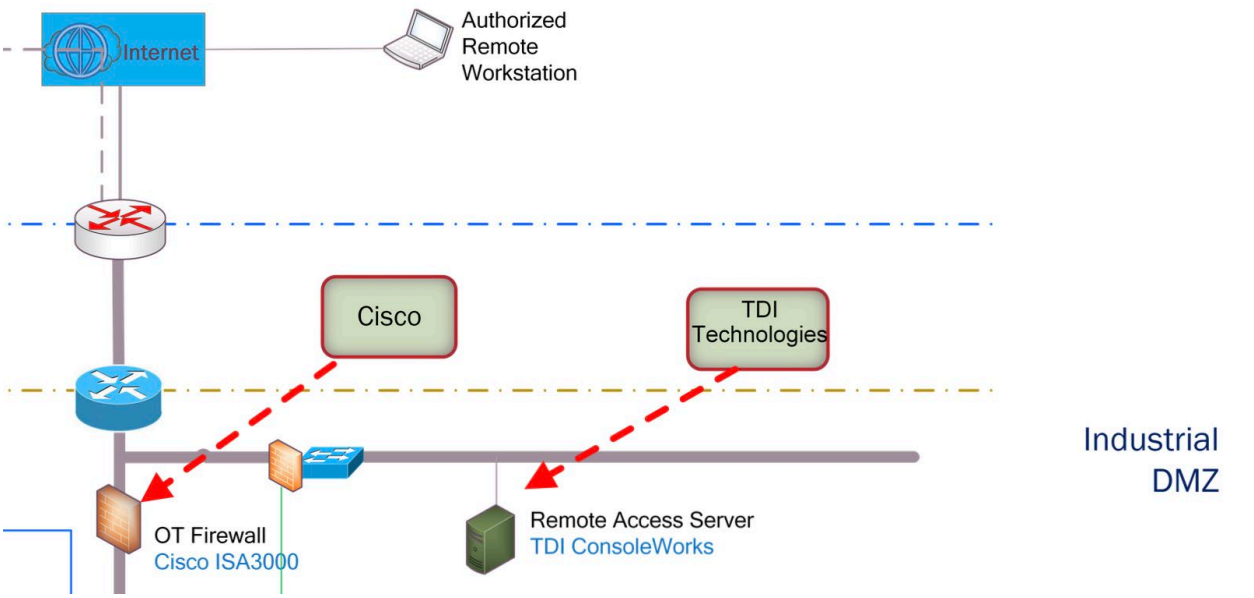
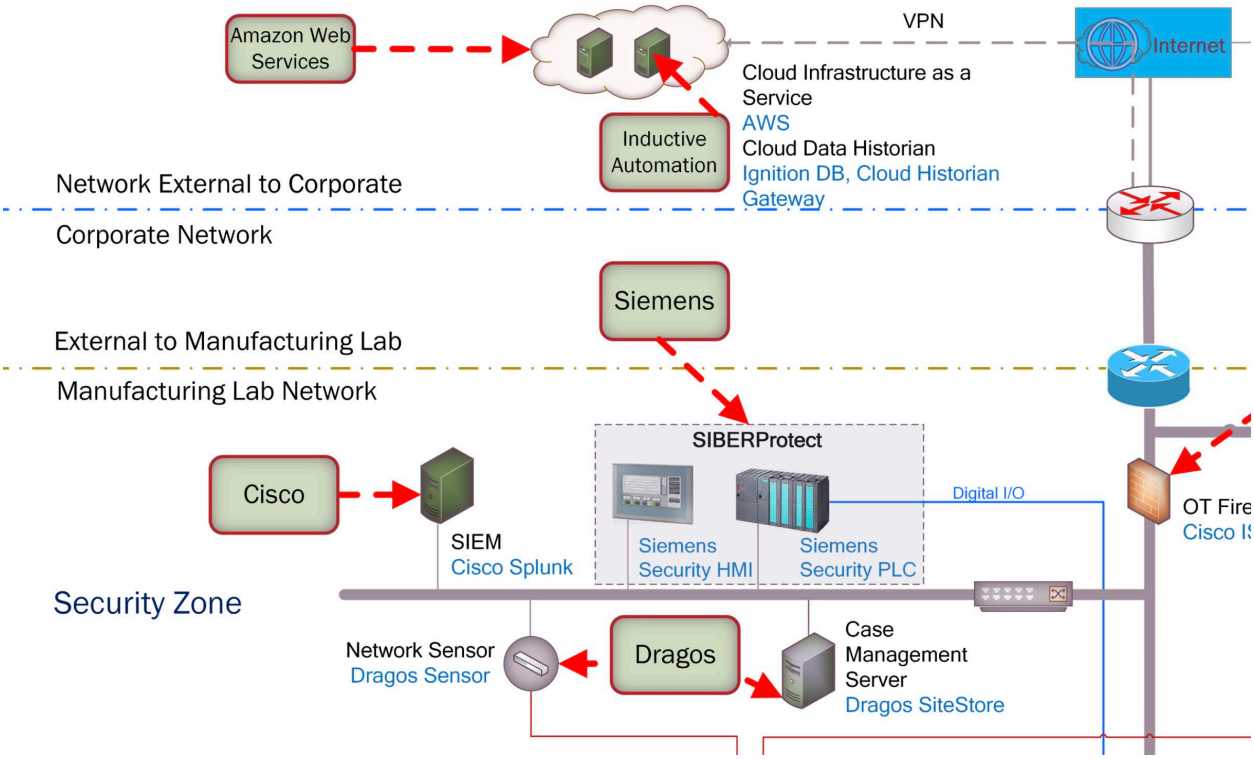


Figure 2-2: Build architecture with security tools

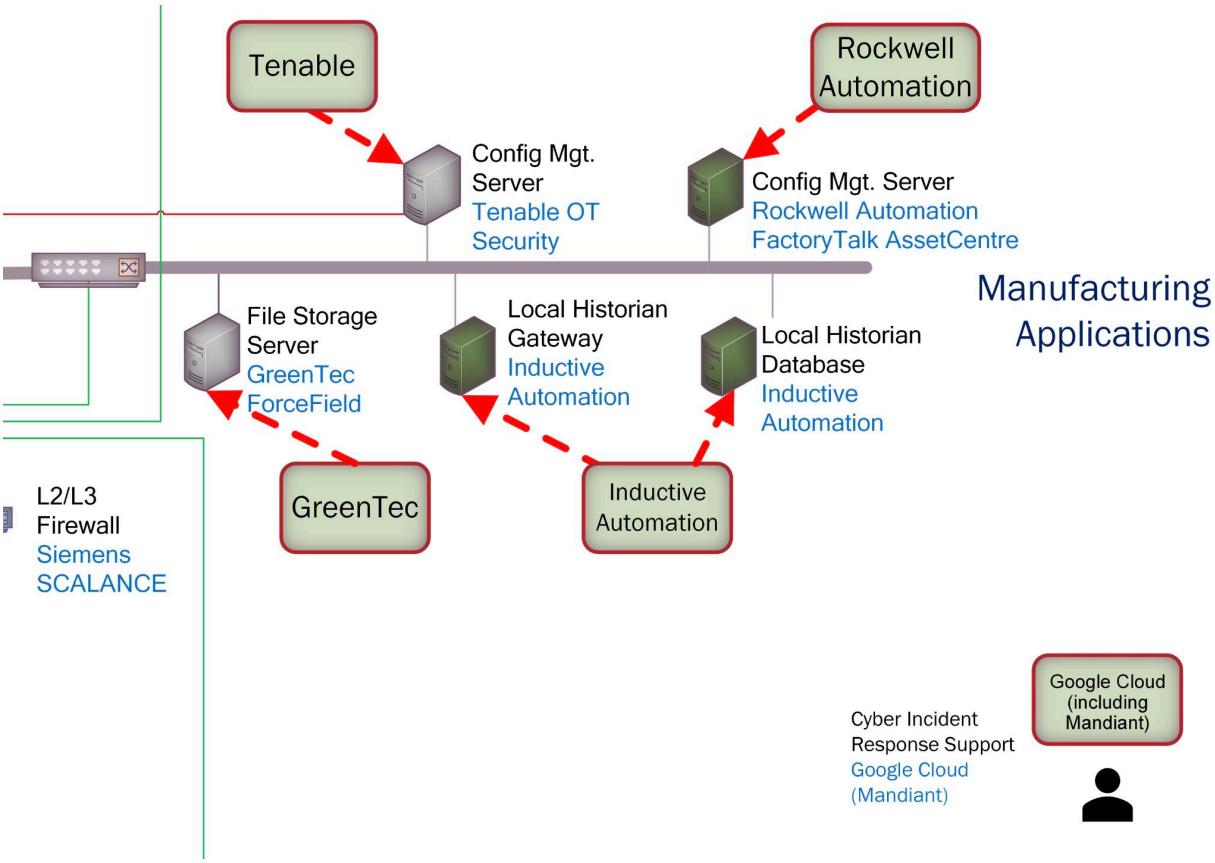
Note: Red borders and arrows in the figures indicate collaborator-provided solutions.



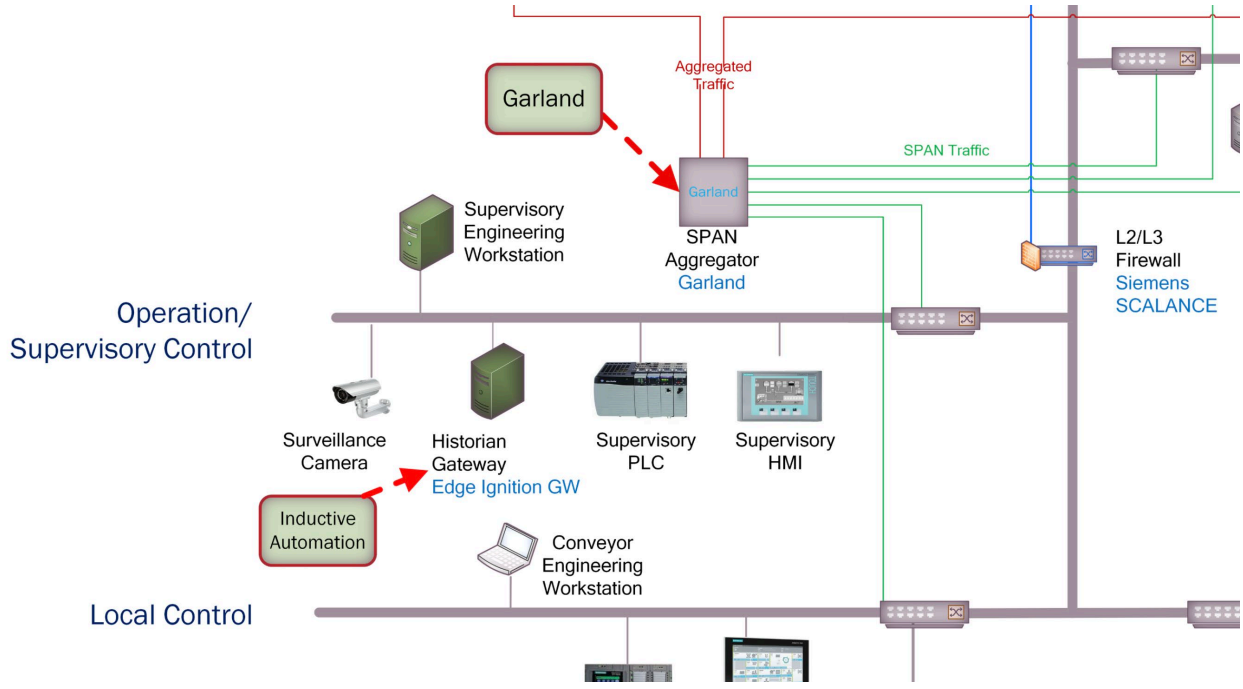
645 **Figure 2-3: Zoomed in top right portion of the build architecture**



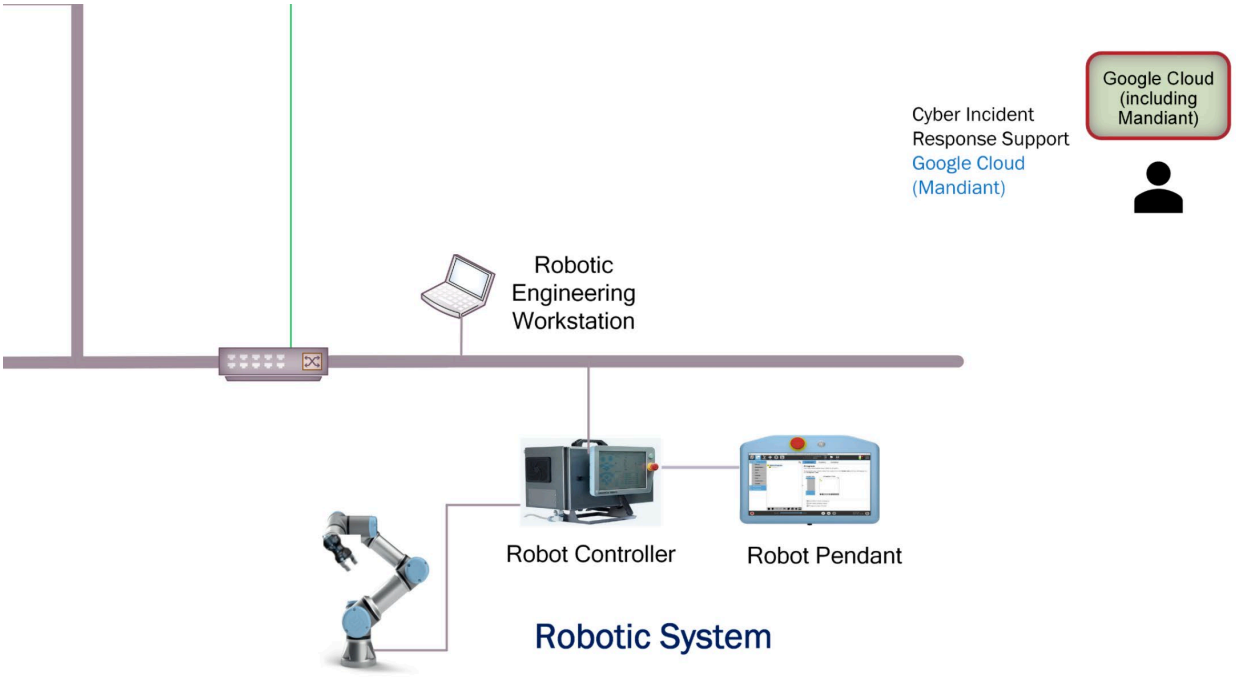
646 **Figure 2-4: Zoomed in top left portion of the build architecture**



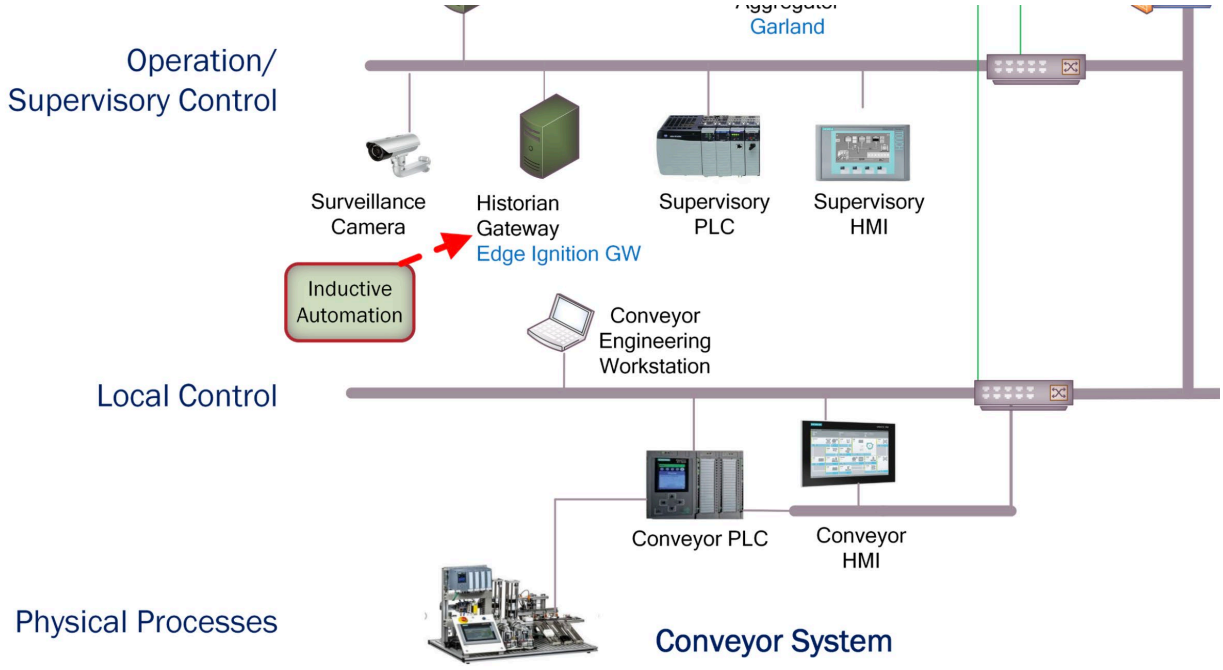
647 **Figure 2-5: Zoomed in middle right portion of the build architecture**



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.

2.4.3.1 Garland Technology

High-Density SPAN/TAP Aggregator INT1G10CSASP

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

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

- Local control for conveyor and robotic systems
- Operation/Supervisory control
- Manufacturing applications
- Security zone
- Industrial DMZ

Aggregated signals are copied to two security solutions:

- Dragos Platform Sensor
- Tenable OT Security Server

2.4.3.2 Dragos

Dragos Platform:

SiteStore Version 2.5.4

Dragos Sensor Version 12.18.15

KP Plus 10.0.2-9.63.0

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

2.4.3.3 Tenable

Tenable OT Security Version 3.17.40

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

2.4.3.4 Amazon Web Services

AWS Infrastructure as a Service

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

2.4.3.5 Inductive Automation

Ignition V8.1.36

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

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

2.4.3.6 Siemens

TIA Portal

S7-1500 CPU and CP Module

SCALANCE 2C

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

2.4.3.7 Rockwell Automation

FactoryTalk® AssetCentre Change Management

FactoryTalk® AssetCentre Disaster Recovery

FactoryTalk® AssetCentre Inventory Agent

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

2.4.3.8 Cisco

ISA3000

Splunk 9.2.2

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

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

2.4.3.9 GreenTec

ForceField 1.9

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

2.4.3.10 TDi Technologies

ConsoleWorks 5.6

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

2.4.3.11 Google Cloud (including Mandiant)

Incident Response Expertise

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

2.5 Assumptions

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

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

- General Project Assumptions – describes the laboratory environment's representativeness and assumed existing cybersecurity functions.

2.5.1 Attack Assumptions

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

2.5.2 Preparation Assumptions

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

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

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

2.5.3 General Project Assumptions

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

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

3 Functional Demonstrations

3.1 Demonstration Methodology

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

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

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

3.2 Demonstration Use Cases

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

Note: Scenario A in this practice guide was developed from Scenario 3 of the project description.

3.2.1.1 Narrative

Background:

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

Simulated Attack:

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

MITRE ATT&CK® References:

Loss of View, Technique T0829 - ICS | MITRE ATT&CK®

3.2.1.2 Capabilities & Tools Demonstrated

- Incident Response Plan (*8428* - Workflow)
- Logging Configuration (Rockwell Automation – FactoryTalk® AssetCentre; Windows Event Viewer)
- SIEM Configuration and Utilization (Cisco – Splunk)
- Network Isolation (Cisco – ISA)
- Disaster Recovery and Change Management (Rockwell Automation –- FactoryTalk® AssetCentre)
- Backup Storage (GreenTec)
- Case Management (Dragos)
- Data Historian (Inductive Automation - Ignition)

3.2.1.3 Targeted Devices

- Supervisory Engineering Workstation (Virtual Machine)
- Supervisory HMI (Physical Machine)
- MFG-Laptop1 Engineering Workstation (Physical Machine)

3.2.1.4 Keywords

- USB

3.2.1.5 Routine Preparation Steps

To enable detection, response, and recovery, the factory routinely configures and monitors logging capabilities. Key preparation steps that enabled response and recovery for Scenario A are found in Scenario A: Technical Details - Preparation.

3.2.2 Scenario A: Response Execution

3.2.2.1 Initial Identification and Reporting

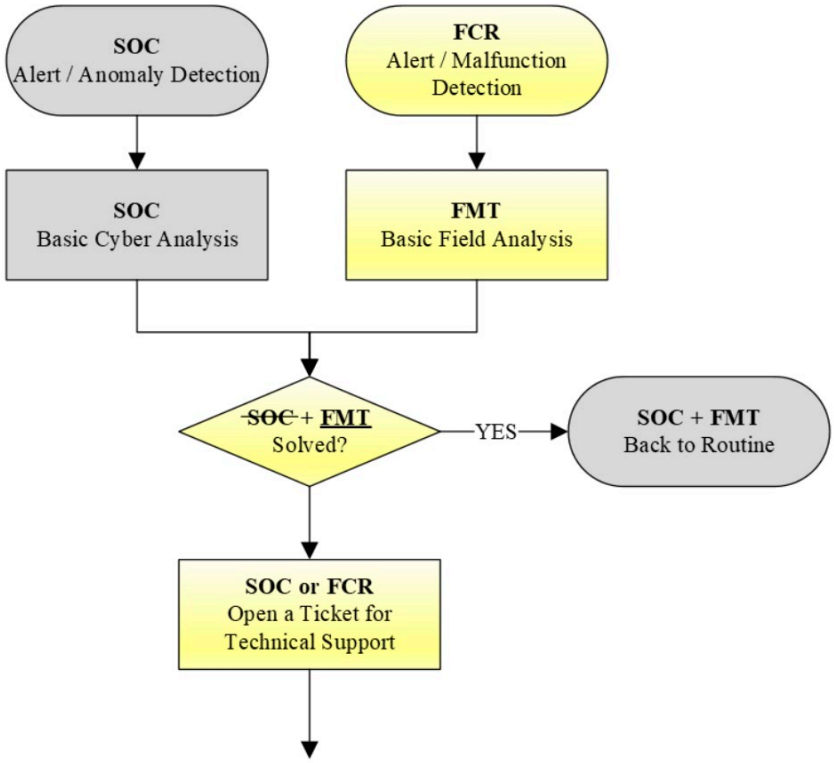


Figure 3-1: *8428* identification, Scenario A

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

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

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

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

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

3.2.2.2 Technical Event Handling

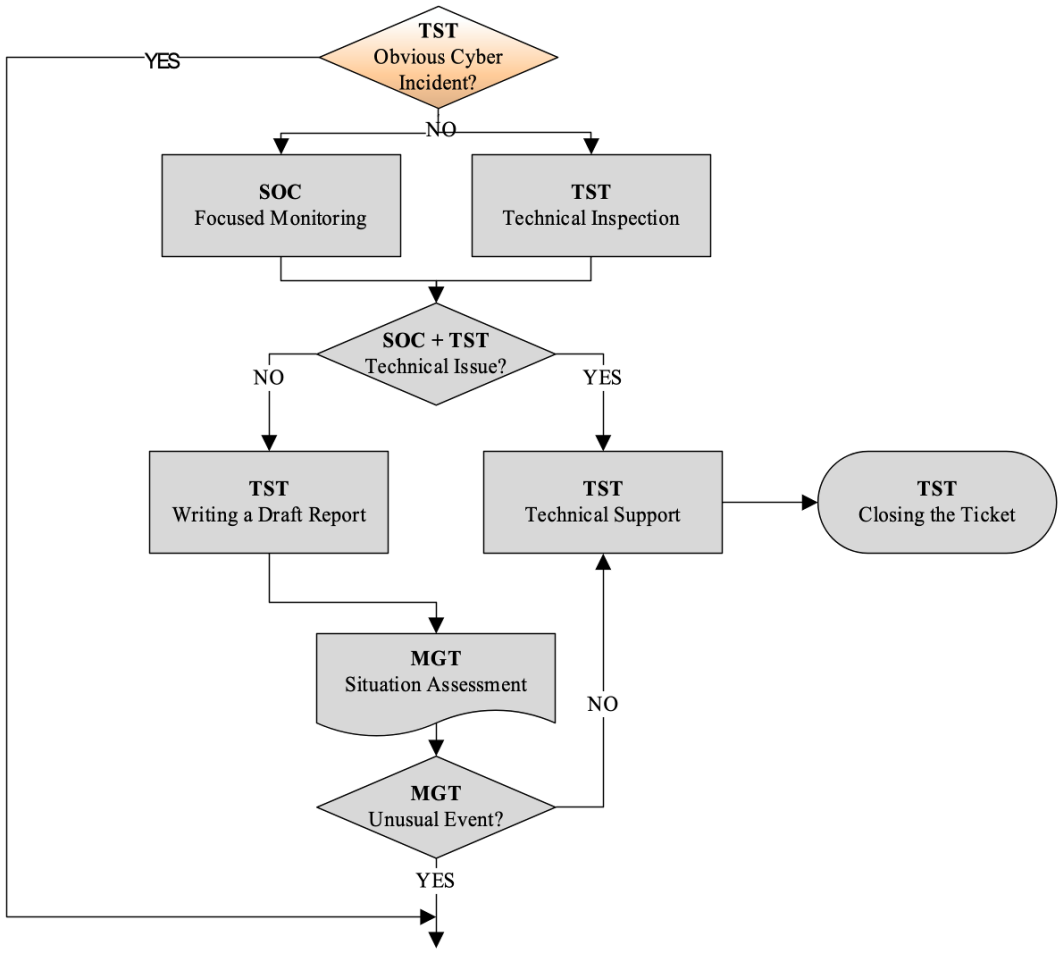


Figure 3-2: *8428* event handling, Scenario A

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

3.2.2.3 Cyber Incident Analysis and Response

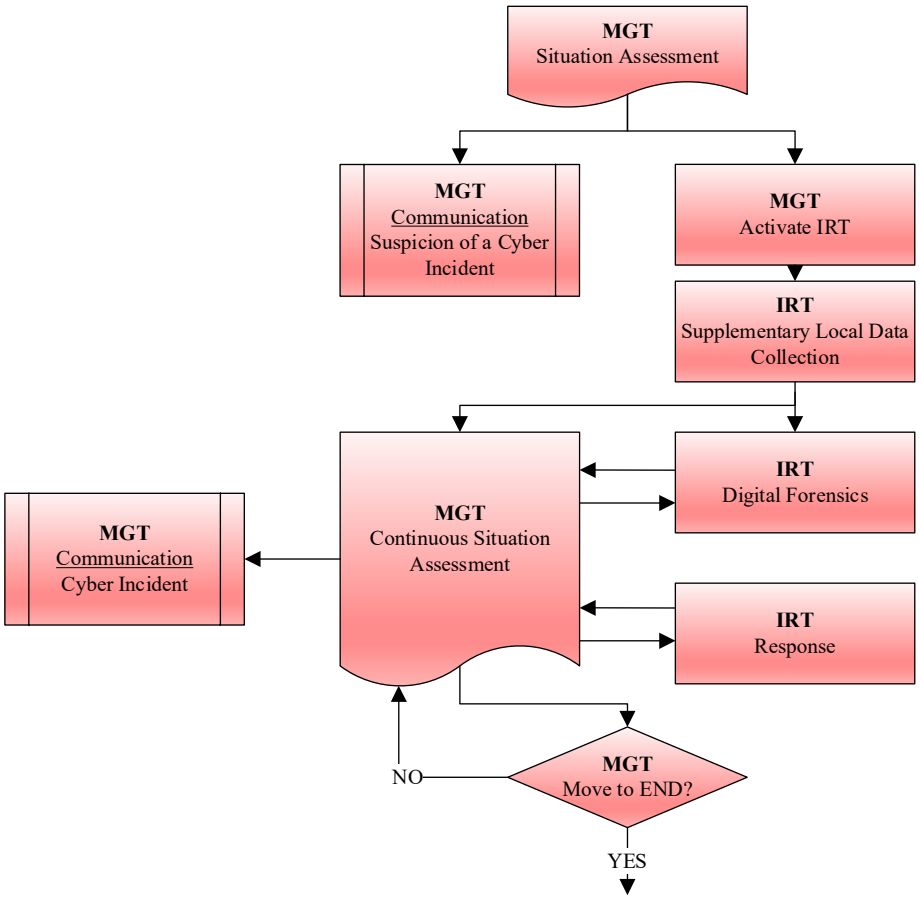


Figure 3-3: *8428* analysis and response, Scenario A

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

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

Operational State: The operator performs a manual shutdown using a safe shutdown procedure. (*800-61:* RS.MI-01, R1)
Note: "Shut down" means the manufacturing process is put into a safe state (e.g., conveyor stops moving) and all computing equipment remains powered. The HMI is not powered off.

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

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

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

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

Response:

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

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

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

b. The engineer uses the network drawing to identify the point of disconnection. The engineer disconnects the workcell from the network. This involves unplugging the Supervisory HMI, Rockwell Automation PanelView™ Plus 7, from the network switch [Isolation of HMI].

Supplemental Local Data Collection / Digital Forensics:

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

a. The SOC Analyst reviews Splunk data to determine if any non-standard behaviors occurred. The Splunk dashboard indicates a USB was inserted just prior to the HMI compromise. Analyst determines to investigate further [Creating a Splunk Dashboard to detect USB Activity].
b. The engineer checks the data historian to verify if any operational changes occurred around the time of the HMI incident [Inductive Automation, Data Historian]. No operational abnormalities found.

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

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

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

Communications: Incident response team discusses findings with Incident Commander and Safety Officer present. They conclude that a USB was inserted just prior to the incident on MFG-Laptop1. They identify the file as NCCoE_Monf_Lab.mer. They determine the next steps to be:

a. Isolate machines directly involved in the attack
b. Scan the network with updated signatures
c. Scan the network for the malicious file

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

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

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

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

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

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

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

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

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

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

3.2.3 Scenario A: Recovery Execution

3.2.3.1 End of Cyber Incident

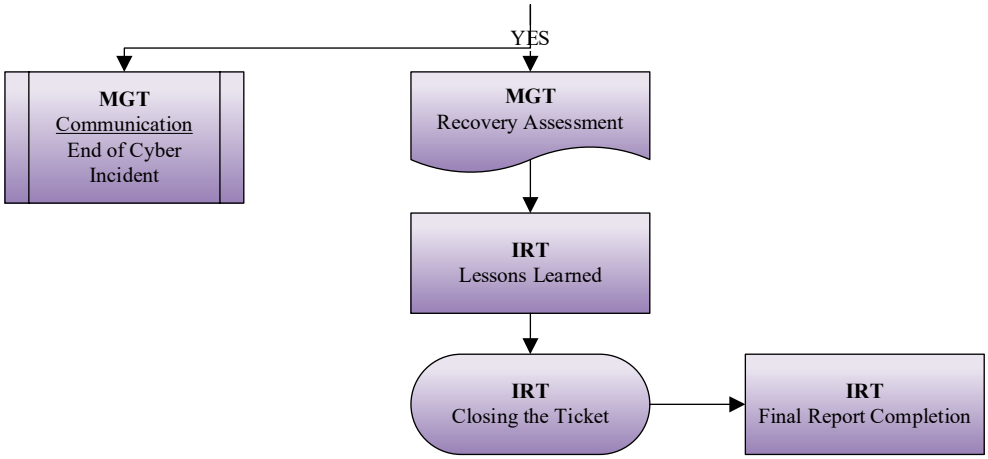


Figure 3-4: *8428* end of incident, Scenario A

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

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

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

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

Backups: Backups were taken of the HMI per the backup procedure, leveraging AssetCentre [Backup the Rockwell PanelView™ HMI] and GreenTec [ForceField Zero Trust Storage] technologies. The backup is validated using Rockwell Automation's AssetCentre and Transfer Utility software.

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

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

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

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

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

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

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

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

3.2.4 Scenario B: Data Exfiltration

Note: Scenario B in this practice guide was developed from Scenario 4 of the project description.

3.2.4.1 Narrative

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

ATT&CK References:

Theft of Operational Information, Technique T0882 - ICS | MITRE ATT&CK®

3.2.4.2 Capabilities & Tools Demonstrated

- Incident Response Plan (*8428* - Workflow)

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

3.2.4.3 Targeted Devices

- Corporate Laptop (Physical Machine)
- Management Console (Virtual Machine)
- Local Historian Database Server (Virtual Machine)

3.2.4.4 Keywords

- Network Traffic Monitoring
- Data Exfiltration

3.2.4.5 Routine Preparation Steps

To enable detection, response, and recovery, the factory routinely configures and monitors logging capabilities. Key preparation steps that enabled response and recovery for Scenario B are found in Scenario B: Technical Details - Preparation.

3.2.5 Scenario B: Response Execution

3.2.5.1 Initial Identification and Reporting

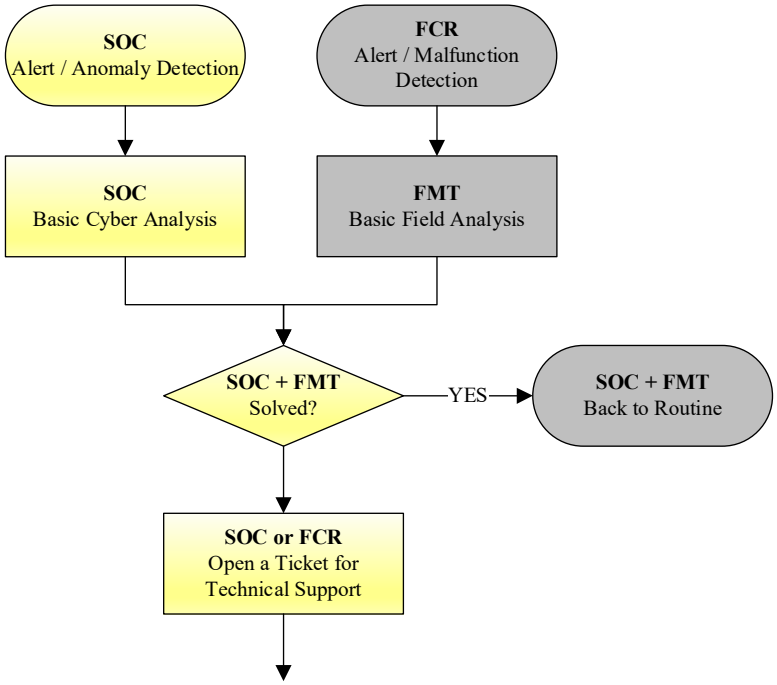


Figure 3-5: 8428 identification, Scenario B

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

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

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

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

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

3.2.5.2 Technical Event Handling

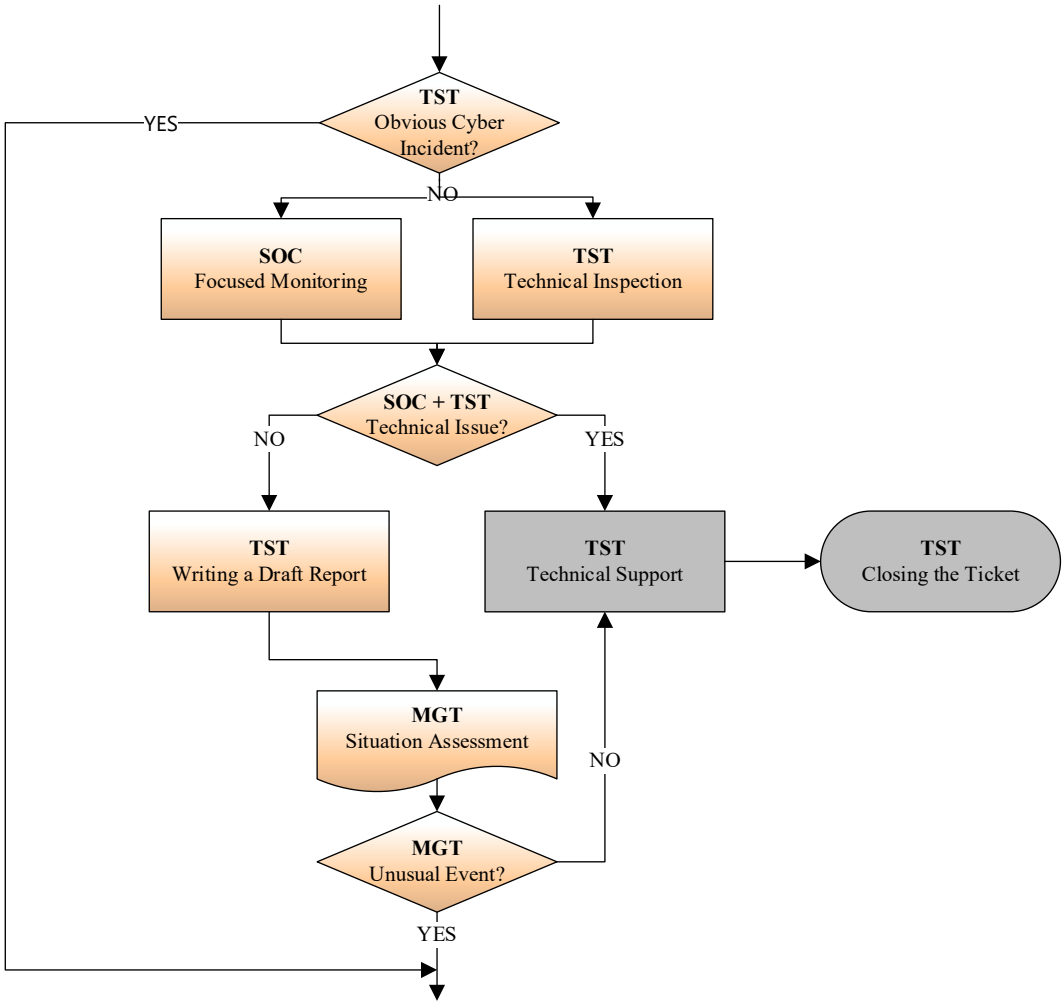


Figure 3-6: *8428* event handling, Scenario B

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

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

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

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

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

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

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

3.2.5.3 Cyber Incident Analysis and Response

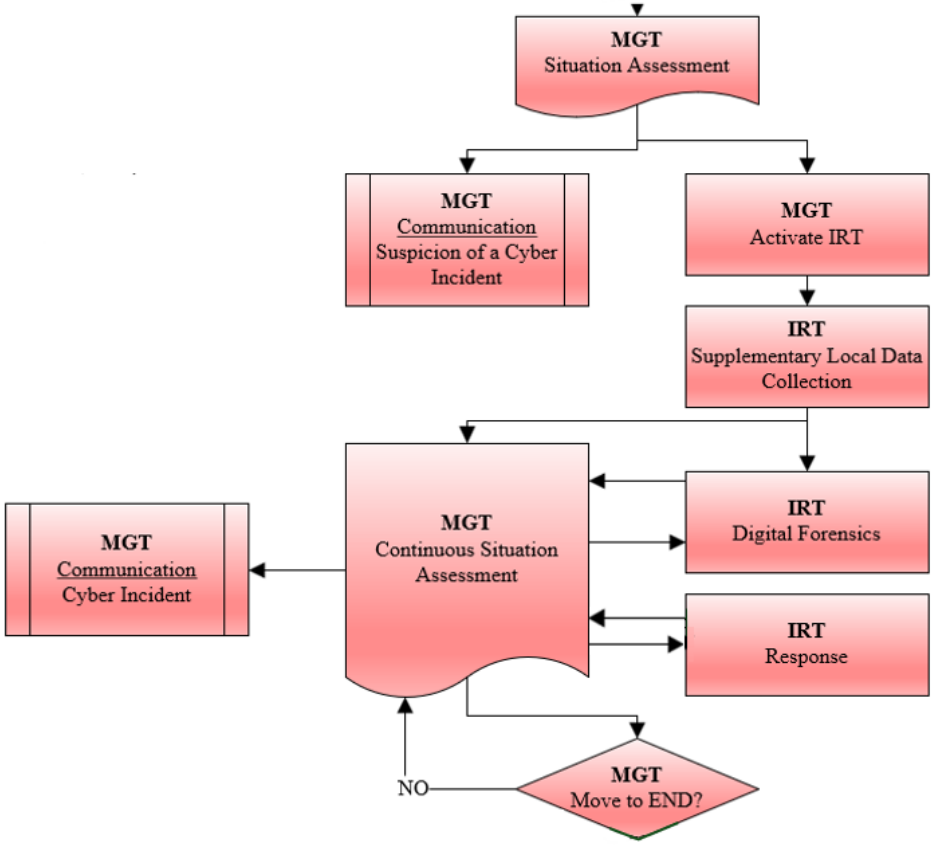


Figure 3-7: *8428* analysis and response, Scenario B

Situation Assessment:

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

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

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

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

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

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

Response:

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

a. The engineer logs into Cisco ISA3000 to create rules to allow AWS outbound and rules to deny all other unnecessary outbound traffic [Isolate ICS DMZ using ISA3000].

b. The engineer disconnects the JumpHost VM from the network [Disconnect JumpHost VM from Network] and takes a snapshot for forensic analysis [Take Snapshot of JumpHost VM].

c. The engineer disconnects the local database and local historian servers from the network [Isolate Local Database and Historian Gateway].

    i. Take a snapshot of both servers for forensic analysis.

    ii. The historian administrator validates that the cloud instance of the historian is still operational [Validate Redundant AWS Cloud Historian].

    iii. Communication: The historian administrator emails their operations and engineering colleagues, notifying them of the outage.

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

Supplemental Local Data Collection / Digital Forensics:

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

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

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

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

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

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

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

Digital Forensics:

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

b. IRT investigates the extent of compromise. IRT views other logins to the database machine. It appears that only jsmith's account was involved in the incident. The jsmith account only logged into the local historian database and the JumpHostVM. There is no indication of additional accesses from that account within the past three weeks. It appears that only the Historian has been impacted, with the historian data being transferred to an external device.

c. The system administrator disables the jsmith account from the Active Directory [Disable Compromised Accounts].

d. Communications: The operations manager calls the owner of the jsmith account again. The manager discloses that the IRT knows the jsmith account was used in the incident. J Smith is able to prove to the operations manager that they have not logged into the database for a long time. They only logged into the database to configure it many months ago and have not logged in since. The manager and employee discussed possible scenarios and discover that J Smith uses the same credentials for their IT login as they do with their ICS login. They also have unnecessary access to administrative accounts when they should only have engineering access for most situations.

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

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

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

3.2.6 Scenario B: Recovery Execution

3.2.6.1 End of Cyber Incident

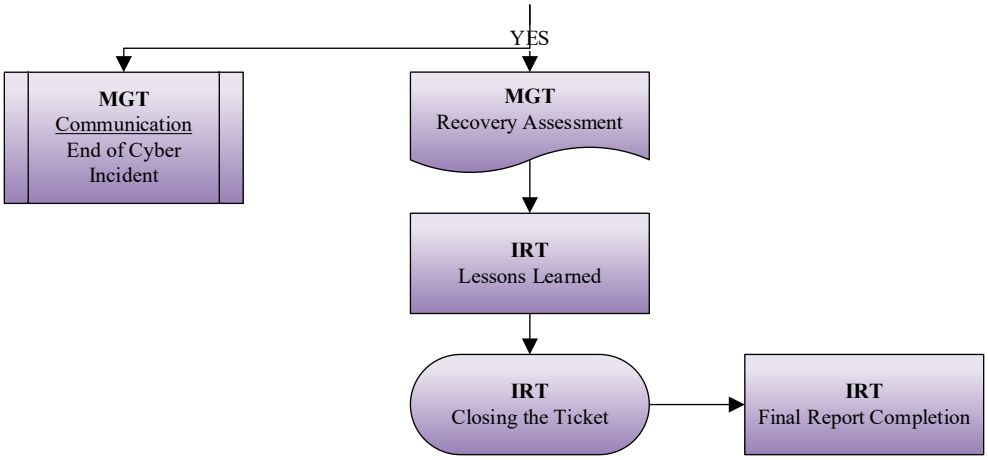


Figure 3-8: *8428* end of incident, Scenario B

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

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

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

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

Recovery:

a) Create a new jsmith_2 account in Active Directory and ConsoleWorks.

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

c) Verify local historian is getting live data.

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

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

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

a) Enable MFA for remote access in ConsoleWorks.

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

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

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

3.2.7 Scenario C: Unauthorized Command Message

Note: Scenario C in this practice guide was developed from Scenario 2 of the project description.

3.2.7.1 Narrative

Background:

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

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

Simulated Attack:

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

ATT&CK References:

Remote Services, Technique T0886 - ICS | MITRE ATT&CK®

Unauthorized Message: Command Message, Sub-technique T1692.001 | MITRE ATT&CK®

Manipulation of Control, Technique T0831 - ICS | MITRE ATT&CK®

3.2.7.2 Capabilities & Tools Demonstrated

- Incident Response Plan (*8428* - Workflow)
- Detection Configuration (Tenable – Tenable OT Security)
- SIEM (Cisco - Splunk)
- Network Isolation (Siemens - SIBERprotect)
- Analysis (Siemens – TIA Portal)
- Data Historian (Inductive Automation - Ignition)
- Backup Management (Rockwell Automation – FactoryTalk® AssetCentre)
- Backup Storage (GreenTec - ForceField)
- Case Management (Dragos - SiteStore)
- Remote Access Monitoring (TDi Technologies – ConsoleWorks)

3.2.7.3 Targeted Devices

- Engineering Workstation (Physical Machine)
- Conveyor System (PLC)
- Remote access server (Virtual Machine)

3.2.7.4 Keywords

- Unauthorized command message
- PLC
- Manipulation of control

3.2.7.5 Routine Preparation Steps

To enable detection, response, and recovery, the factory routinely configures and monitors logging capabilities. Key preparation steps that enabled response and recovery for Scenario C are found in Scenario C: Technical Details – Preparation.

3.2.8 Scenario C: Response Execution

3.2.8.1 Initial Identification and Reporting

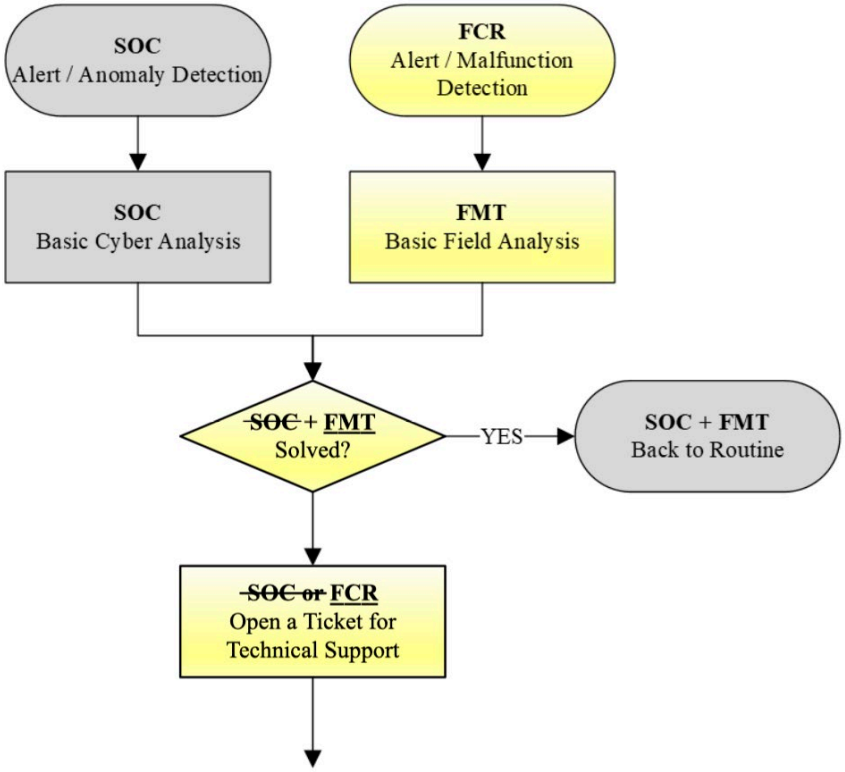


Figure 3-9: *8428* DFIR Identification, Scenario C

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

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

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

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

Next day

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

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

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

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

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

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

Next day

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

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

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

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

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

The engineer sees that the PRG_LCH tag has been modified during the off-shift over the past few days.

Next day

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

Communication: The engineer calls SOC to review for alerts.

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

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

3.2.8.2 Technical Event Handling

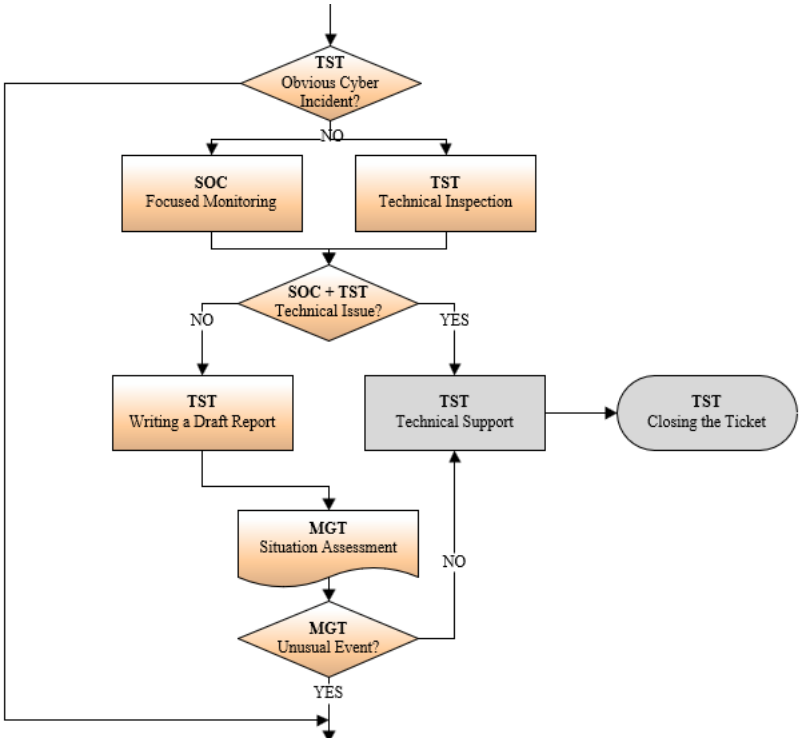


Figure 3-10: *8428* Event Handling, Scenario C

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

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

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

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

Next day

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

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

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

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

3.2.8.3 Cyber Incident Analysis and Response

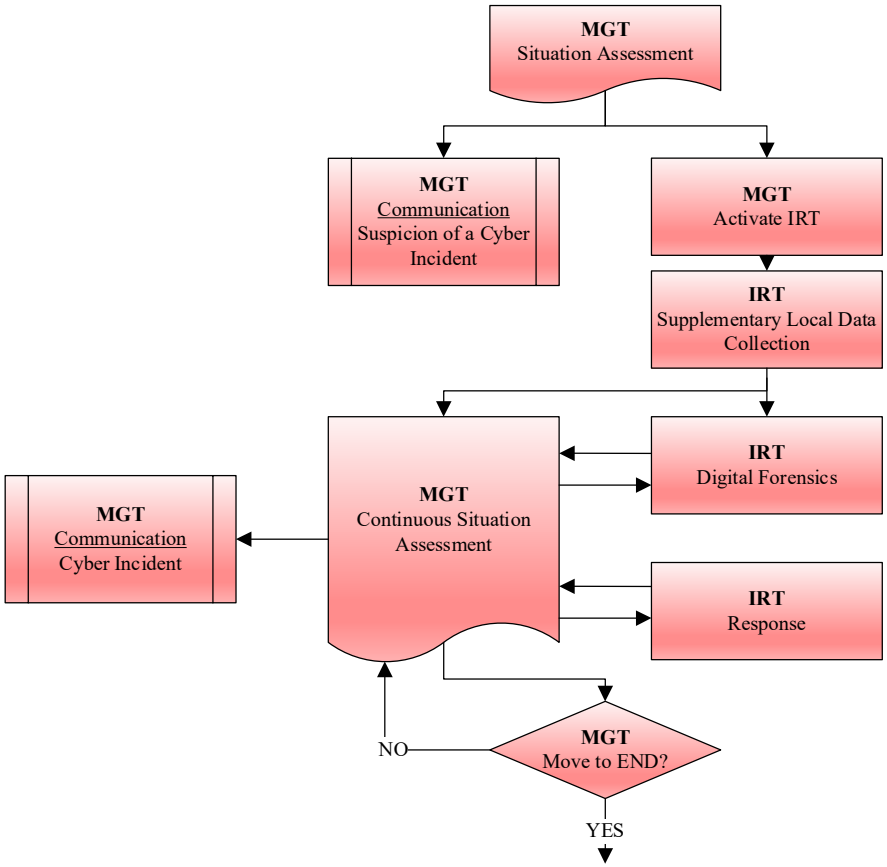


Figure 3-11: *8428* Analysis and Response, Scenario C

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

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

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

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

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

Operational State: Manufacturing operations continue using local HMIs.

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

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

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

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

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

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

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

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

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

Disable the jsmith account from Active Directory.

Change the password of the jsmith account in ConsoleWorks.

[Refer to Scenario B screenshots, Disable Compromised Accounts]

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

Communication: Case Management: The Dragos ticket is updated with the latest findings from the investigation [Managing Dragos Tickets].

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

3.2.9 Scenario C: Recovery Execution

3.2.9.1 End of Cyber Incident

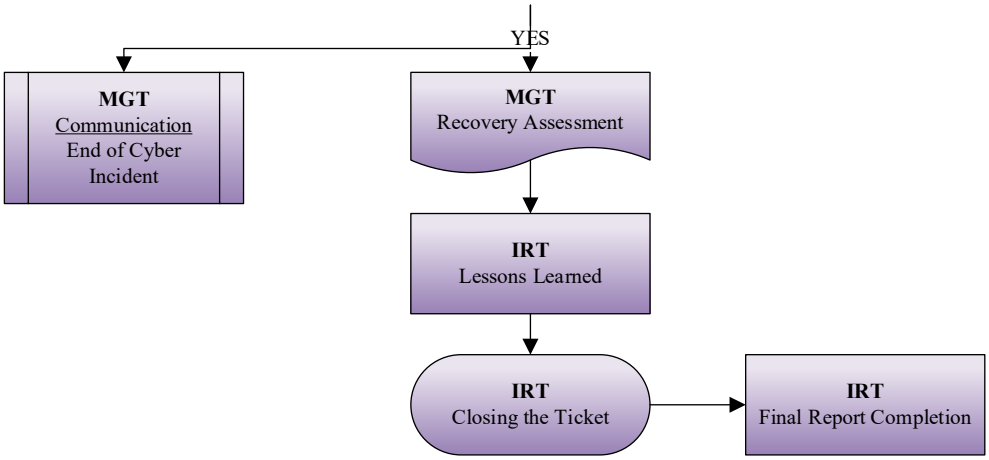


Figure 3-12: *8428* End of Incident, Scenario C

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

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

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

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

Perform a factory reset on the PLC.

Reinstall the PLC program from the known-good file saved in ForceField. [Download PLC Backup Program File from ForceField]

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

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

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

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

Enable MFA for remote access on ConsoleWorks

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

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

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

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

4 General Findings

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

1. Preparation and planning are critical for the successful implementation of response and recovery. The scenarios demonstrate that establishing a predetermined and structured approach to assess potential threats to operations was key to ensuring timely and optimal decision-making. Another area of

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

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

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

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

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

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

Appendix A List of Acronyms

AD	Active Directory
CRADA	Cooperative Research and Development Agreement
CTL	Communications Technology Laboratory
DFIR	Digital Forensics and Incident Response
DMZ	Demilitarized Zone
DNS	Domain Name System
FCR	Facility Control Room
HMI	Human Machine Interface
IP	Internet Protocol
IRP	Incident Response Plan
IRT	Incident Response Team
ISA	(Cisco) Industrial Security Appliance
IT	Information Technology
ITL	Information Technology Laboratory
MFA	Multifactor Authentication
MGT	Management
NCCoE	National Cybersecurity Center of Excellence
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OS	Operating System
OT	Operational Technology
RDP	Remote Desktop Protocol
SIEM	Security Information and Event Management
SP	Special Publication
SOC	Security Operations Center
SSH	Secure Shell
TAP	Test Access Point
TST	Technical Support Team

USB	Universal Serial Bus
VM	Virtual Machine
SP	Special Publication

Appendix B References

[1] National Institute of Standards and Technology (2024), The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29.

[2] Salfati, E. and Pease, M. (2022), Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT), NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8428.

[3] Nelson A, Rekhi S, Souppaya M, Scarfone K (2025), Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3.

[4] Bartock M, Cichonski J, Souppaya M, Smith M, Witte G, Scarfone K (2016), Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-184. https://doi.org/10.6028/NIST.SP.800-184.

[5] Federal Emergency Management Agency (FEMA). (n.d.). *Incident Organization Chart (*ICS 207*)*. https://training.fema.gov/emiweb/is/icsresource/assets/ics%20forms/ics%20form%20207,%20incident%20organization%20chart%20(v3).pdf

[6] (2025), Reducing the Cybersecurity Risks of Portable Storage Media in OT Environments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1334. https://doi.org/10.6028/NIST.SP.1334.

[7] Security Synapse. (2018), *Monitoring USB Storage Activity with Splunk – Part 1 (Connectivity events).* [online], https://securitysynapse.blogspot.com/2018/11/monitoring-usb-storage-activity-part-1.html.

[8] Security Synapse. (2018), *Monitoring USB Storage Activity with Splunk – Part II (Read/Write/Delete/Modify events)*. [online], https://securitysynapse.blogspot.com/2018/11/monitoring-usb-storage-activity-part-2.html.

Appendix C Build Implementation Instructions

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

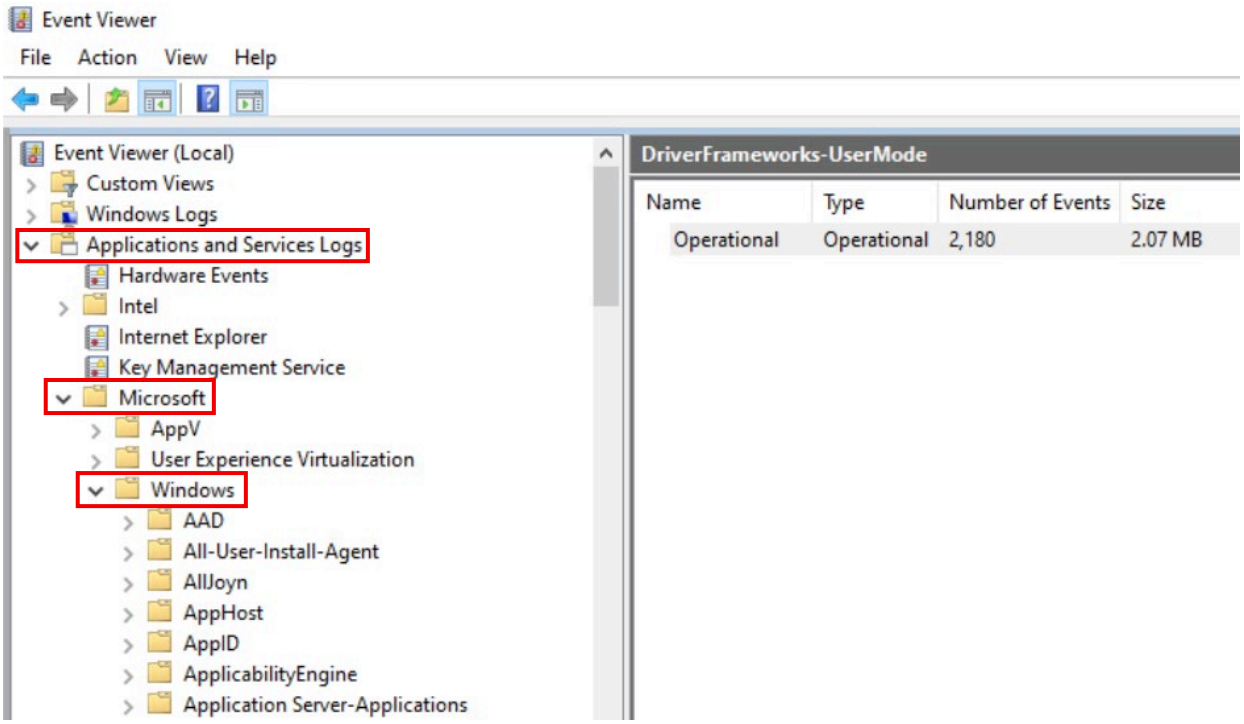
C.1 Scenario A: Technical Details - Preparation

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

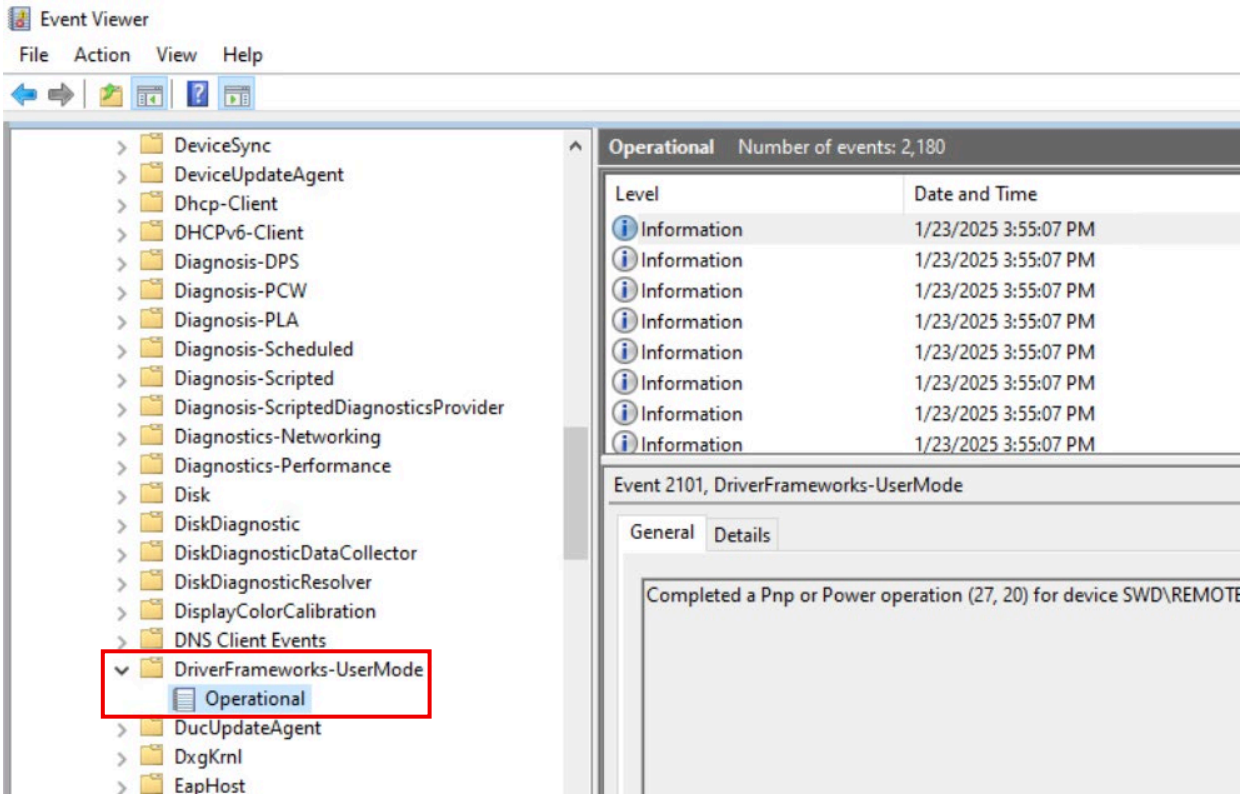
[Return to Scenario A]

C.1.1 Creating a Splunk Dashboard to detect USB Activity

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

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

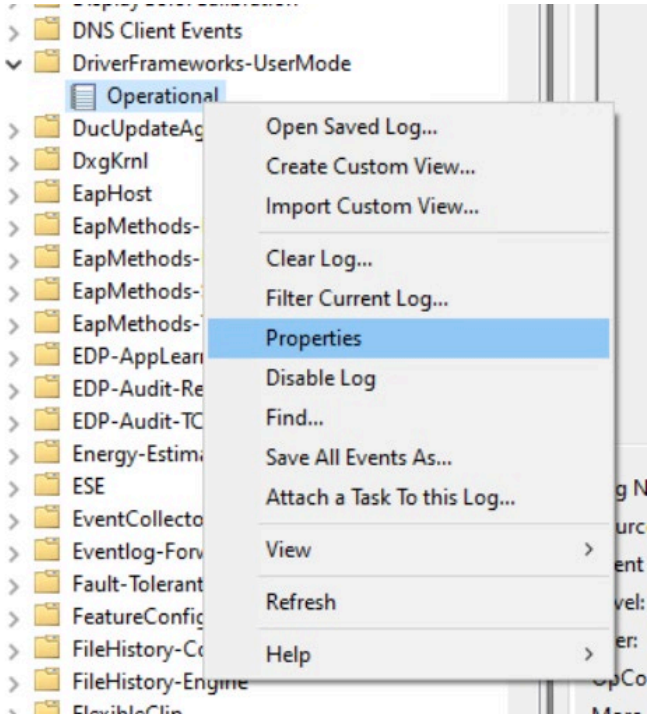
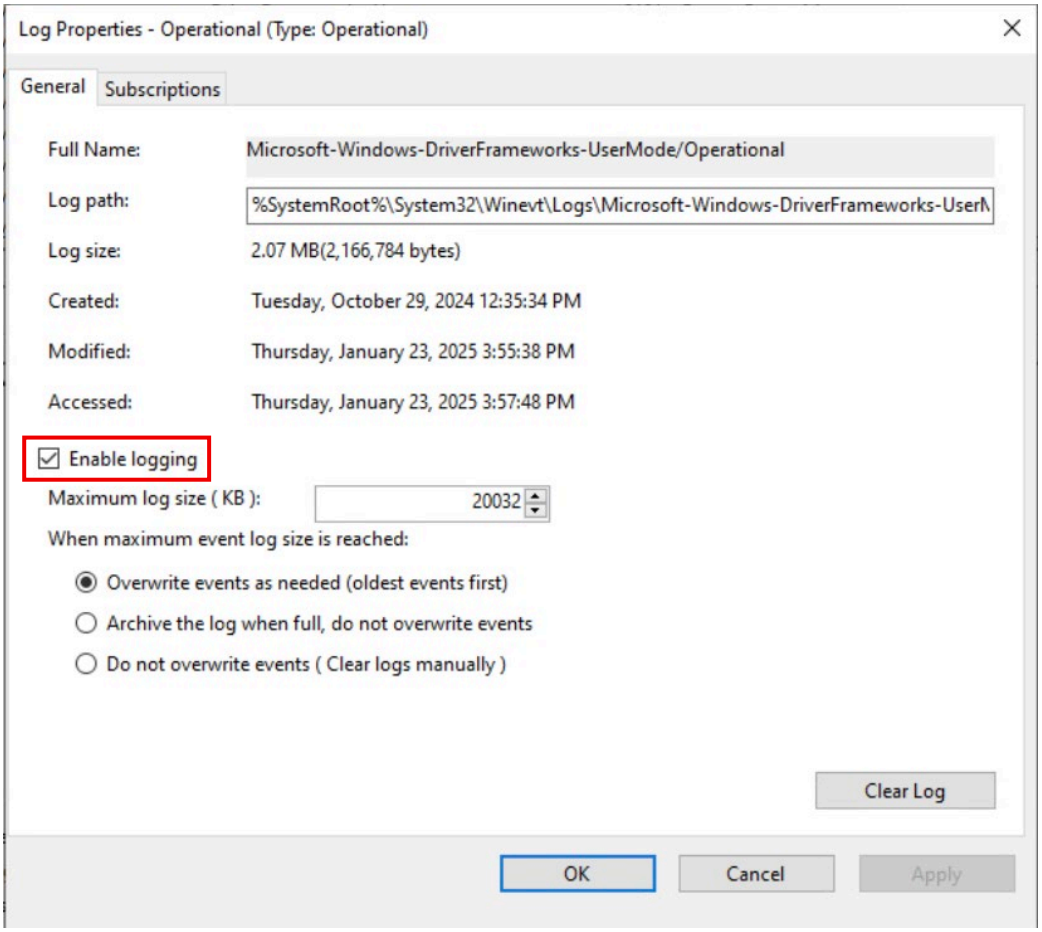


Figure 4-3: Opening the Driver Frameworks Operational logs properties



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`

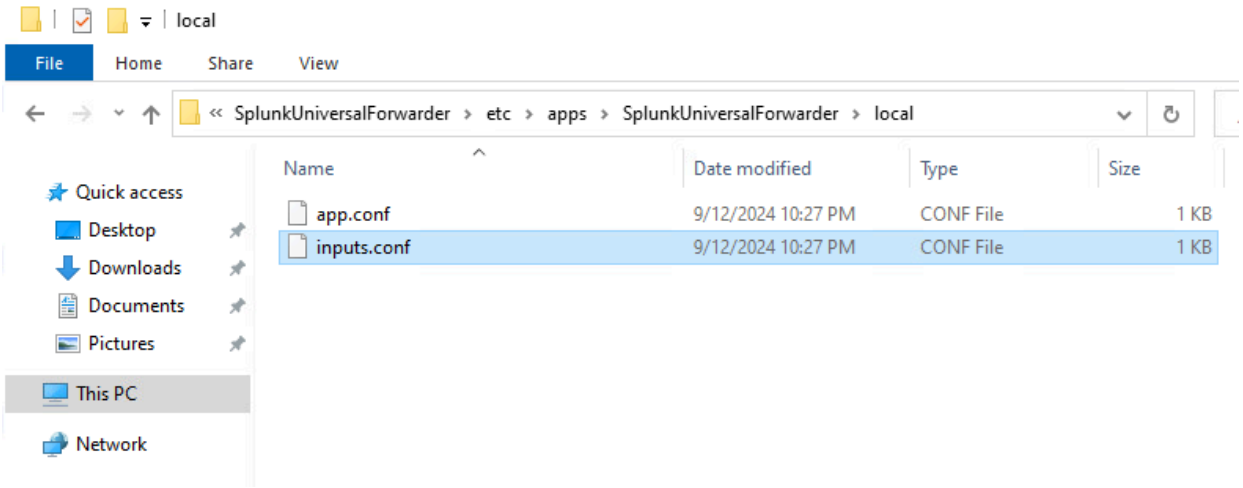
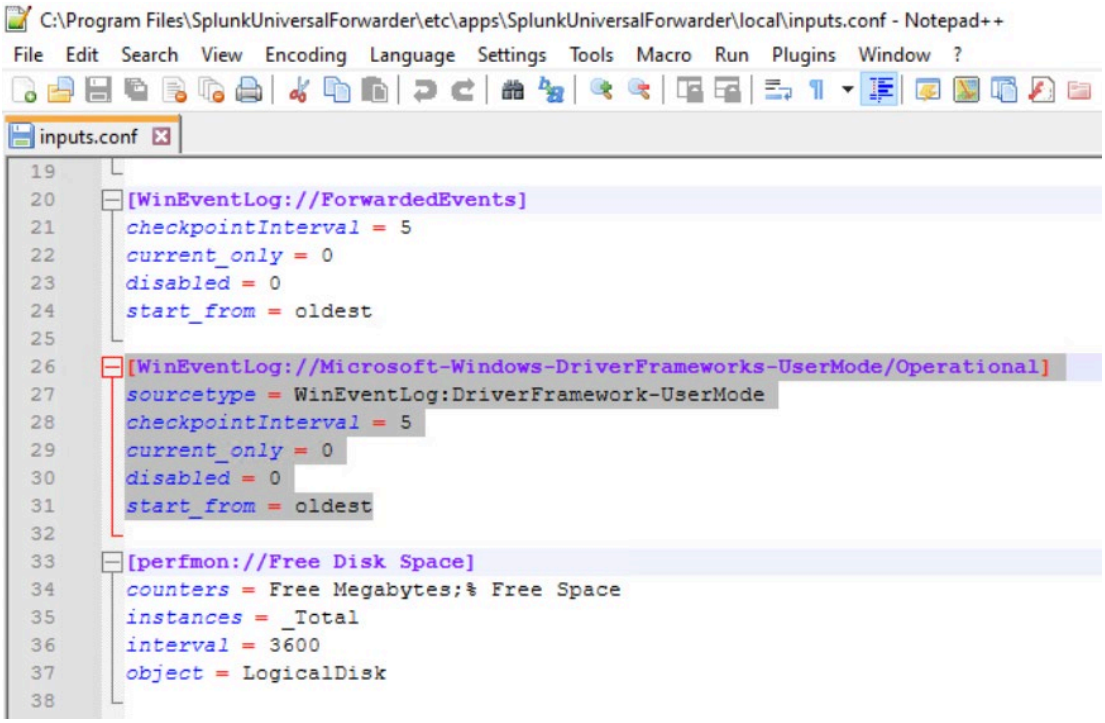


Figure 4-5: The location of the "inputs.conf" file for the Splunk Universal Forwarder

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

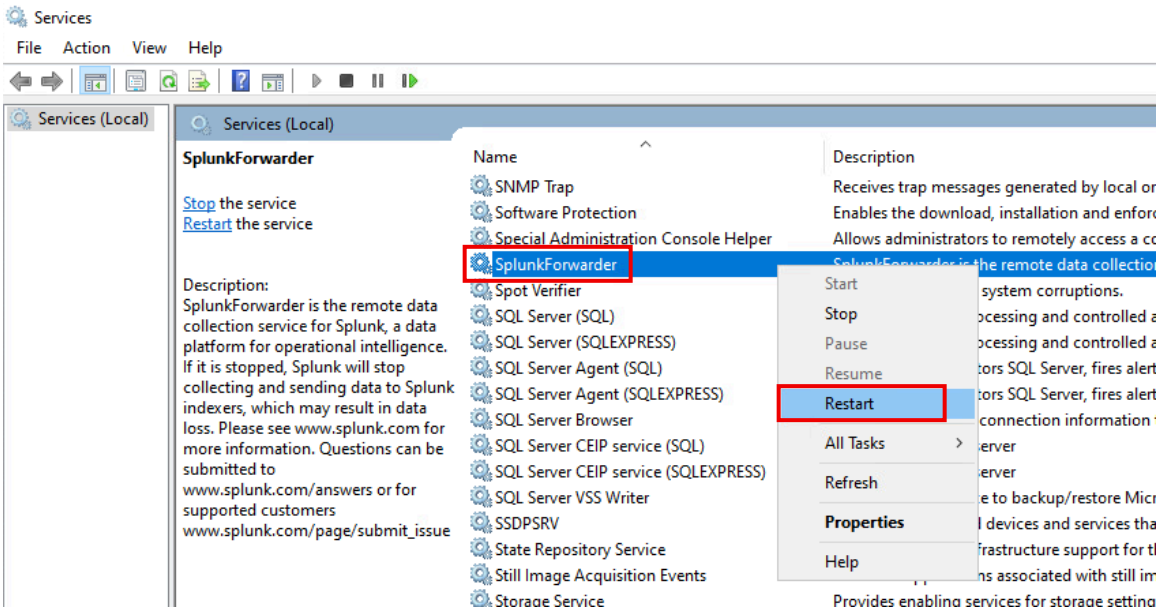
```
[WinEventLog://Microsoft-Windows-DriverFrameworks-UserMode/Operational]
sourcetype = WinEventLog:DriverFramework-UserMode
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
```

See the screenshot below for reference.



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

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

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

- Number of Connect Events
  - A simple count of Connect Events
- Number of Disconnect Events
  - A simple count of Disconnect Events
- Top Hosts with USB Activity
  - The top hosts on the network to have any Connect or Disconnect event
- Top Removable Storage Vendors
  - The vendors associated with the USB device (if that information is available)
- Top Removable Storage Products
  - The USB product type (if information is available)
- Top Serial Numbers
  - The serial numbers associated with the USB device (if that information is available)
- Events Over Time
  - A chart showing the Connect and Disconnect events over time
- Connection Events (EventCode 2003)
  - Each individual Connect Event showing all previous information and the date/time the event occurred
- Disconnect Events (EventCode 2102)
  - Each individual Disconnect Event showing all previous information and the date/time the event occurred

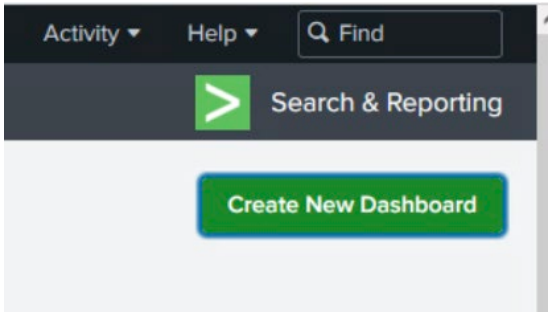
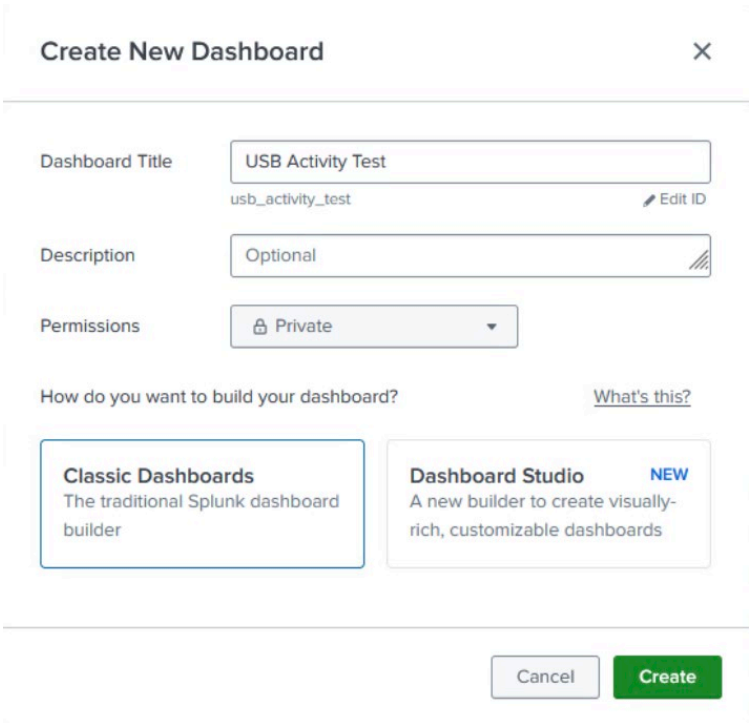


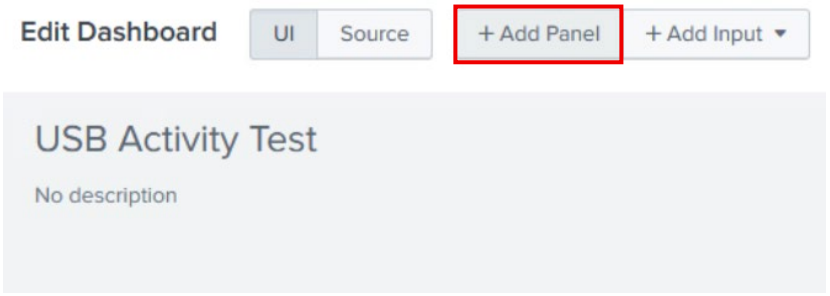
Figure 4-8: The "Create New Dashboard" button on the top-right of the Splunk web interface

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



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

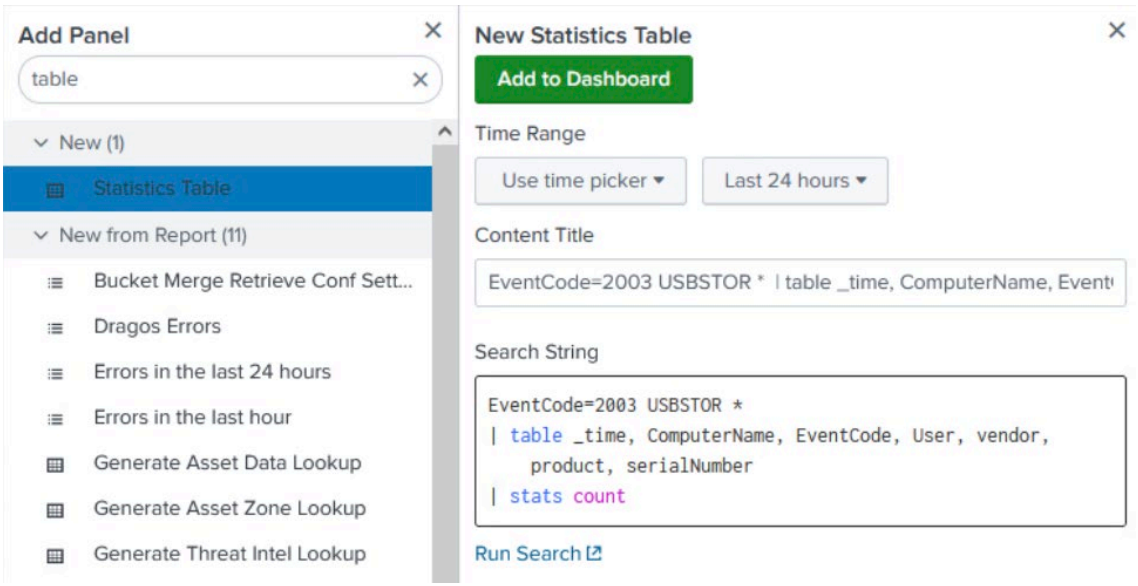
1577 Click the `Add Panel` button.



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
```

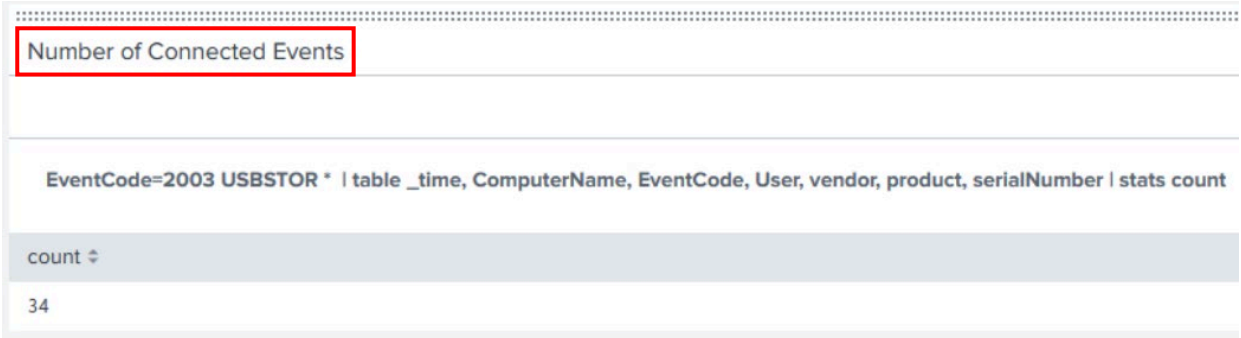


1584 **Figure 4-11: Creating a new "Statistics Table" in a Splunk dashboard, search string included**

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:

Number of Disconnect Events:

```
EventCode=2102 USBSTOR *
| transaction maxspan=5s EventCode, ComputerName, serialNumber
| dedup _time, ComputerName, serialNumber
| table _time, ComputerName, EventCode, User, vendor, product,
serialNumber
| stats count
```

Top Hosts with USB Activity:

```
(EventCode=2003 OR EventCode=2102) USBSTOR *
| transaction maxspan=5s EventCode, ComputerName, serialNumber
| table _time, ComputerName, EventCode, User, vendor, product,
serialNumber
| top limit=0 ComputerName
```

Top Removable Storage Vendors:

```
(EventCode=2003 OR EventCode=2102) USBSTOR *
| dedup serialNumber
| table _time, ComputerName, EventCode, User, vendor, product,
serialNumber
| top limit=0 vendor
```

Top Removable Storage Products:

```
(EventCode=2003 OR EventCode=2102) USBSTOR *
| dedup serialNumber
| table _time, ComputerName, EventCode, User, vendor, product,
serialNumber
| top limit=0 product
```

Top Serial Numbers:

```
(EventCode=2003 OR EventCode=2102) USBSTOR *
| dedup serialNumber
| table _time, ComputerName, EventCode, User, vendor, product,
serialNumber
| top limit=0 serialNumber
```

Events Over Time:

```
(EventCode=2003 OR EventCode=2102) USBSTOR *
| eval action=case(EventCode == 2003, "Connect", EventCode ==
2102, "Connect")
| table _time, ComputerName, action, EventCode, User, vendor,
product, serialNumber
| eval ActionSerial = action + ":" + serialNumber
| timechart dc(serialNumber) by ActionSerial
```

Connection Events (EventCode 2003):

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

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"
```

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

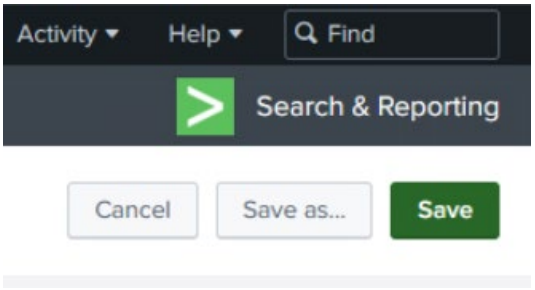
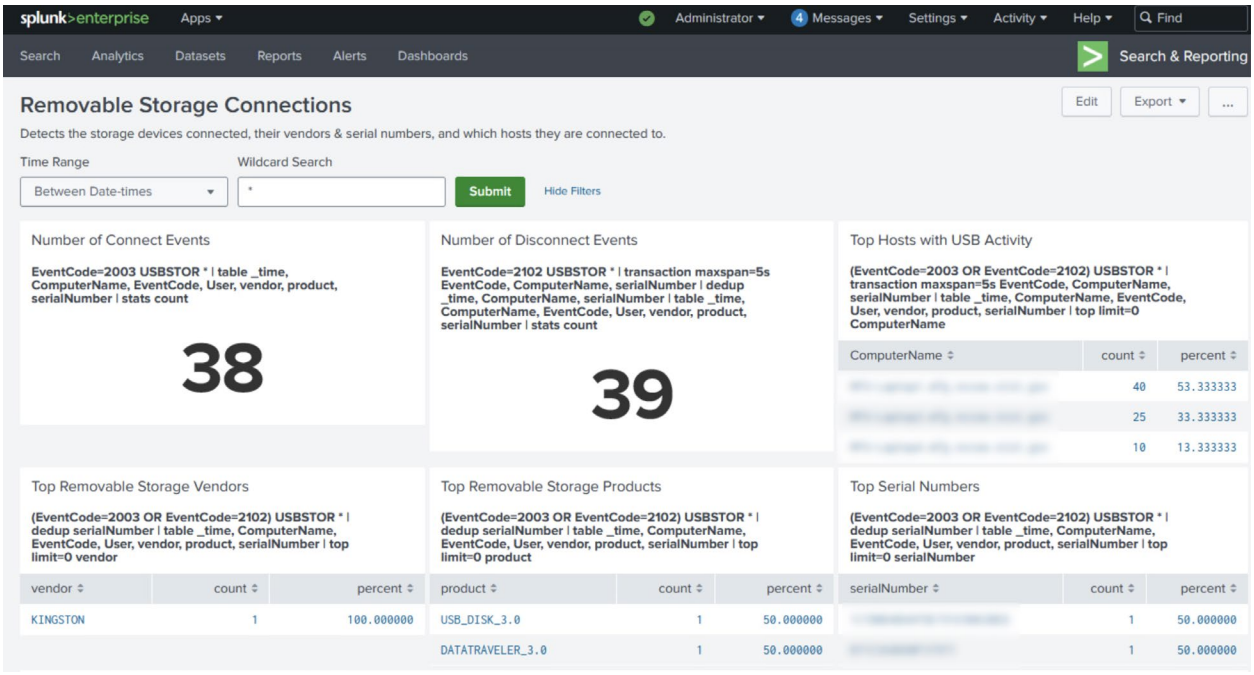


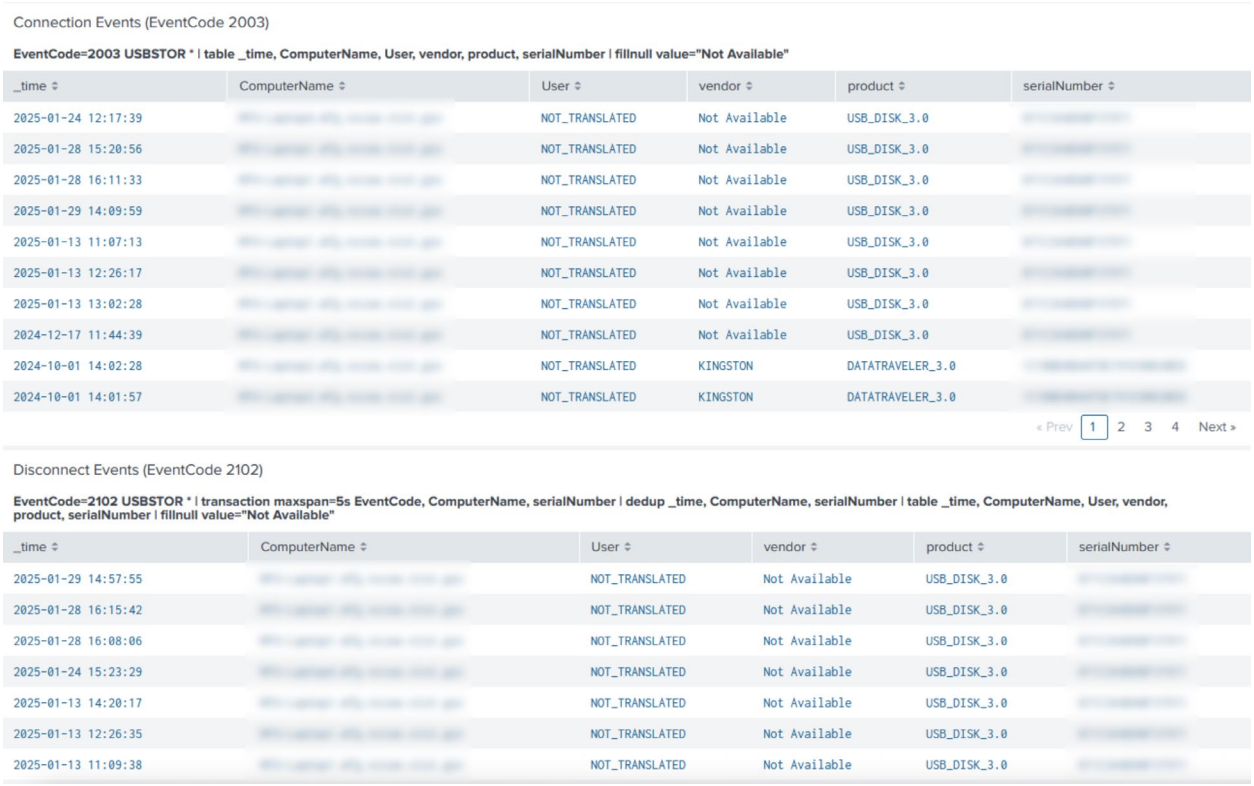
Figure 4-14: Saving the Splunk dashboard once all panels are created

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	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-28 15:20:56	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-28 16:11:33	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-29 14:09:59	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-13 11:07:13	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-13 12:26:17	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-13 13:02:28	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2024-12-17 11:44:39	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2024-10-01 14:02:28	[redacted]	NOT_TRANSLATED	KINGSTON	DATATRAVELER_3.0	[redacted]
2024-10-01 14:01:57	[redacted]	NOT_TRANSLATED	KINGSTON	DATATRAVELER_3.0	[redacted]

« 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	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-28 16:15:42	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-28 16:08:06	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-24 15:23:29	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-13 14:20:17	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-13 12:26:35	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]
2025-01-13 11:09:38	[redacted]	NOT_TRANSLATED	Not Available	USB_DISK_3.0	[redacted]

Figure 4-17: Final "Removable Storage Connections" dashboard in Splunk

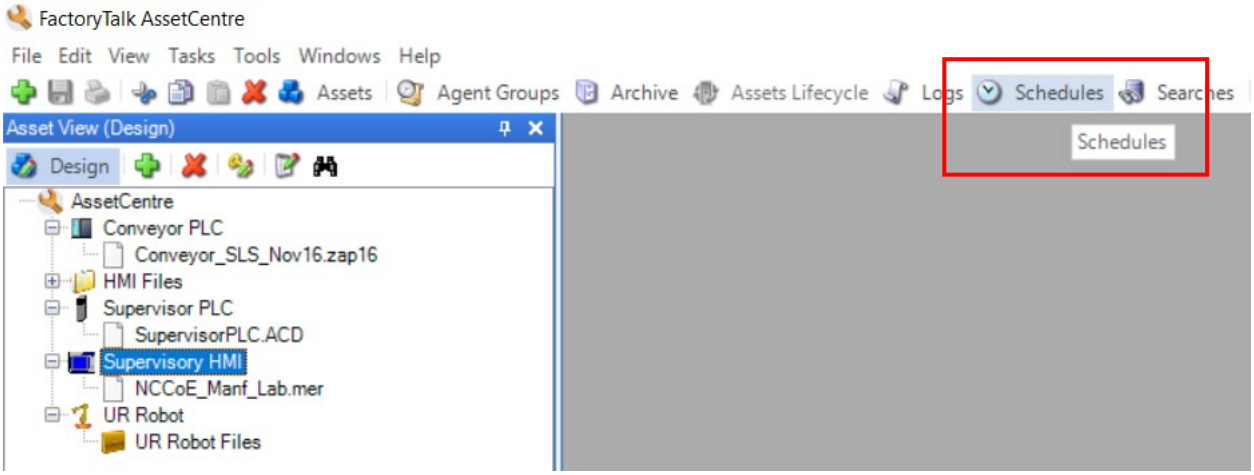
Online resources have been leveraged in the development of these dashboards [7][8].

[Return to Scenario A]

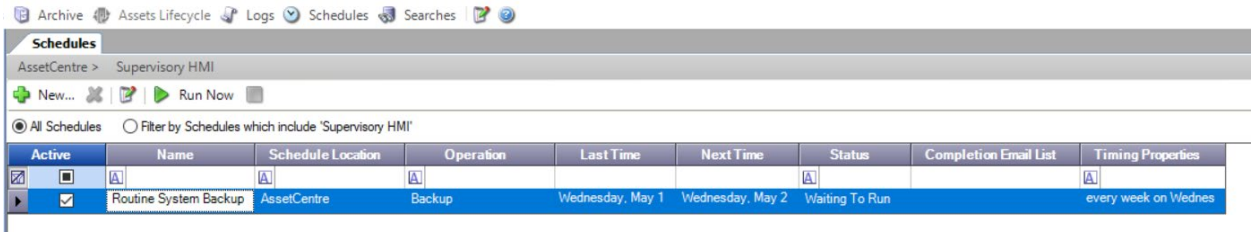
C.1.2 Backup the Rockwell PanelView™ HMI

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

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

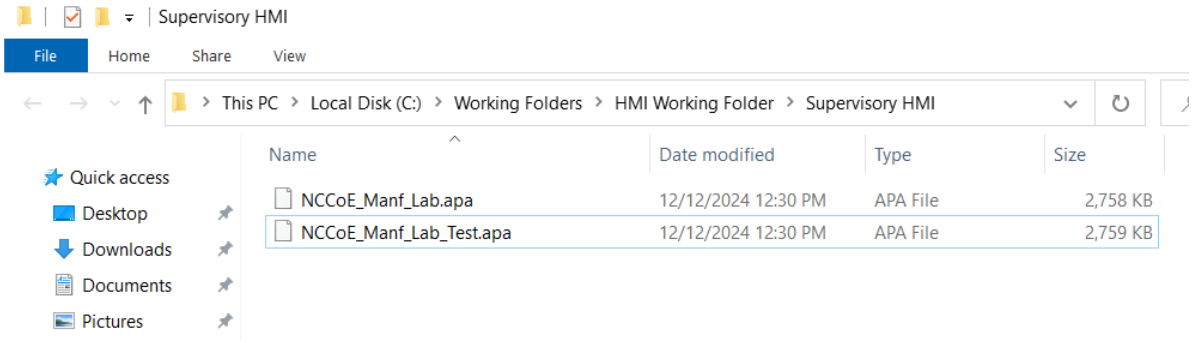


1662 **Figure 4-18: Showing the "Schedules" button in FactoryTalk® AssetCentre**

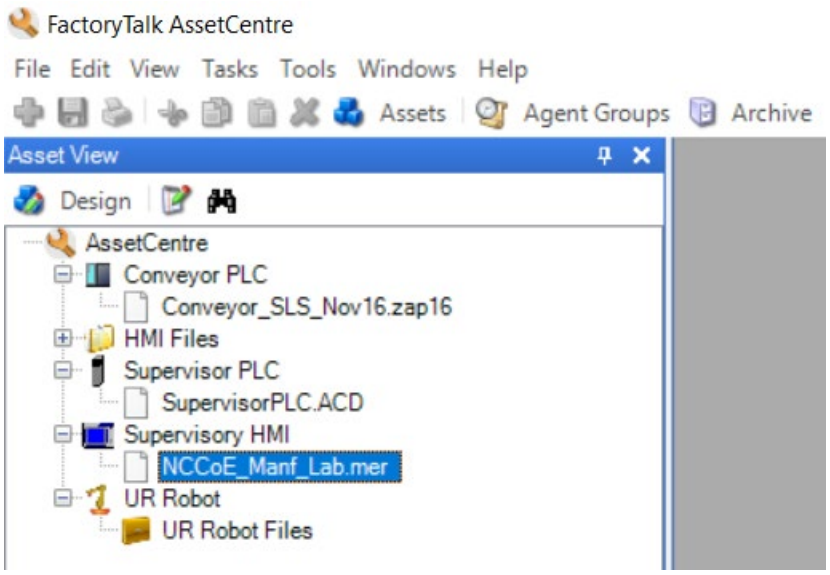


1663 **Figure 4-19: The "Schedules" view in AssetCentre**

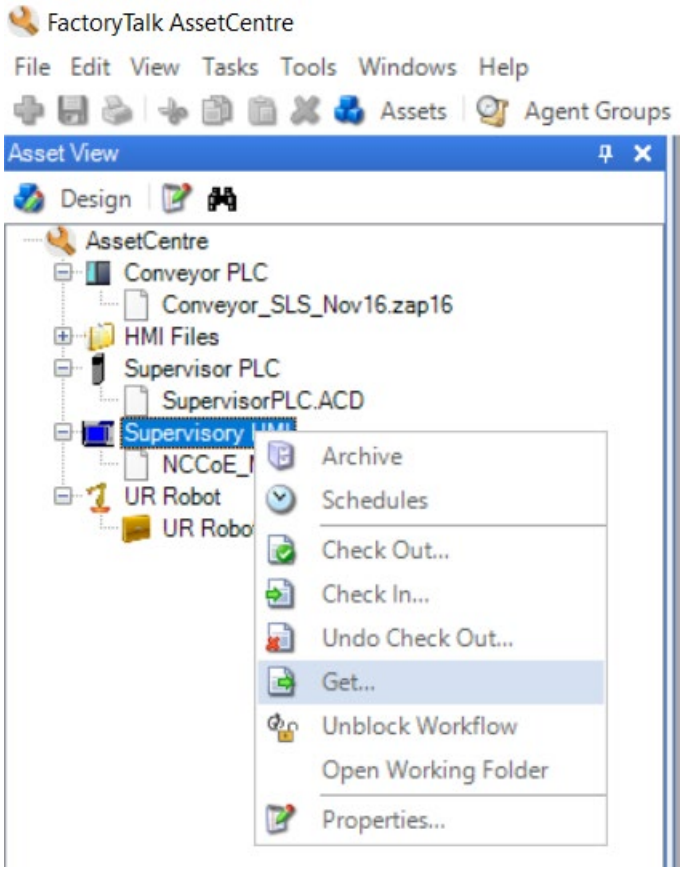
1664 Additionally, the configuration file (`.mer`) can be retrieved using the "get" feature. In the Asset View,
1665 right-click on the Supervisory HMI and click on `get`. This will pull up a menu with optional information.
1666 After confirming, the file will be placed into the Working Folder chosen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



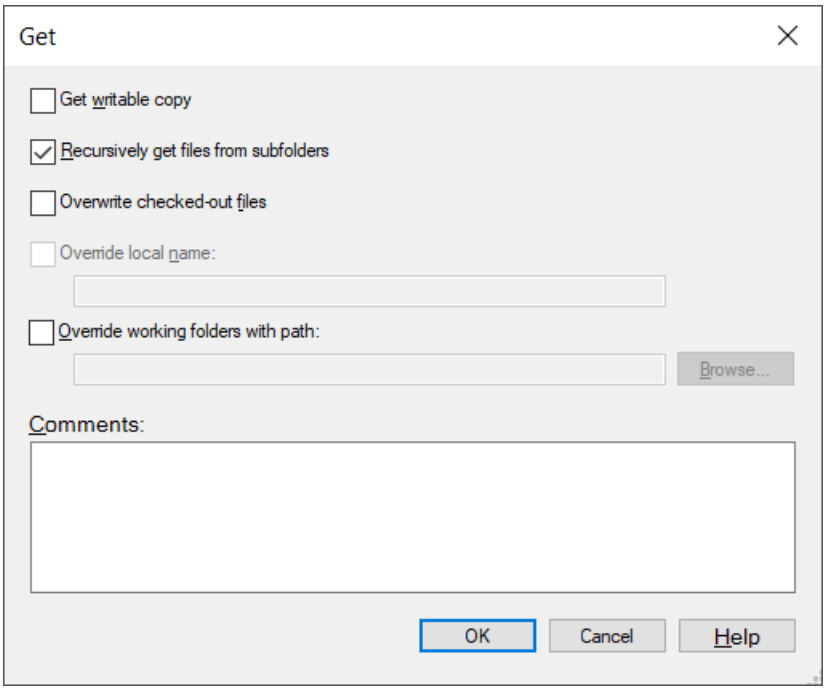
1667 **Figure 4-20: Location of the "Working Folders" without the ".mer" file present**



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**

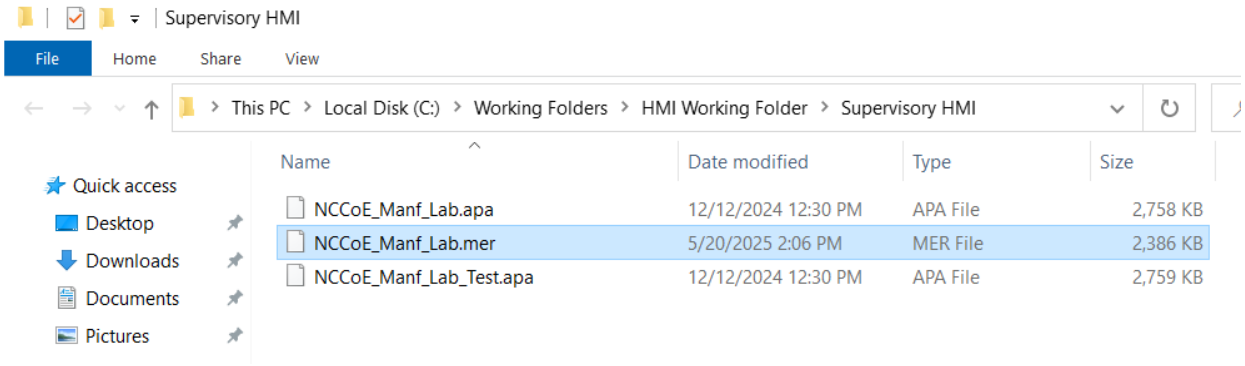


Figure 4-24: ".mer" file now located in the "Working Folders" directory after using the "Get" tool

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

[Return to Scenario A]

C.1.3 ForceField Zero Trust Storage

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

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

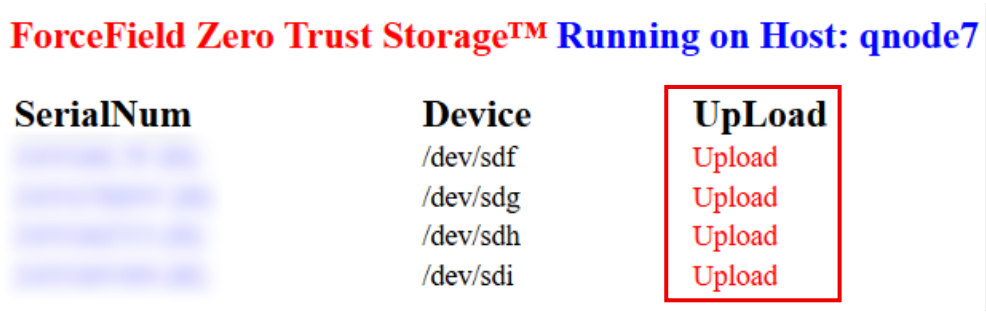
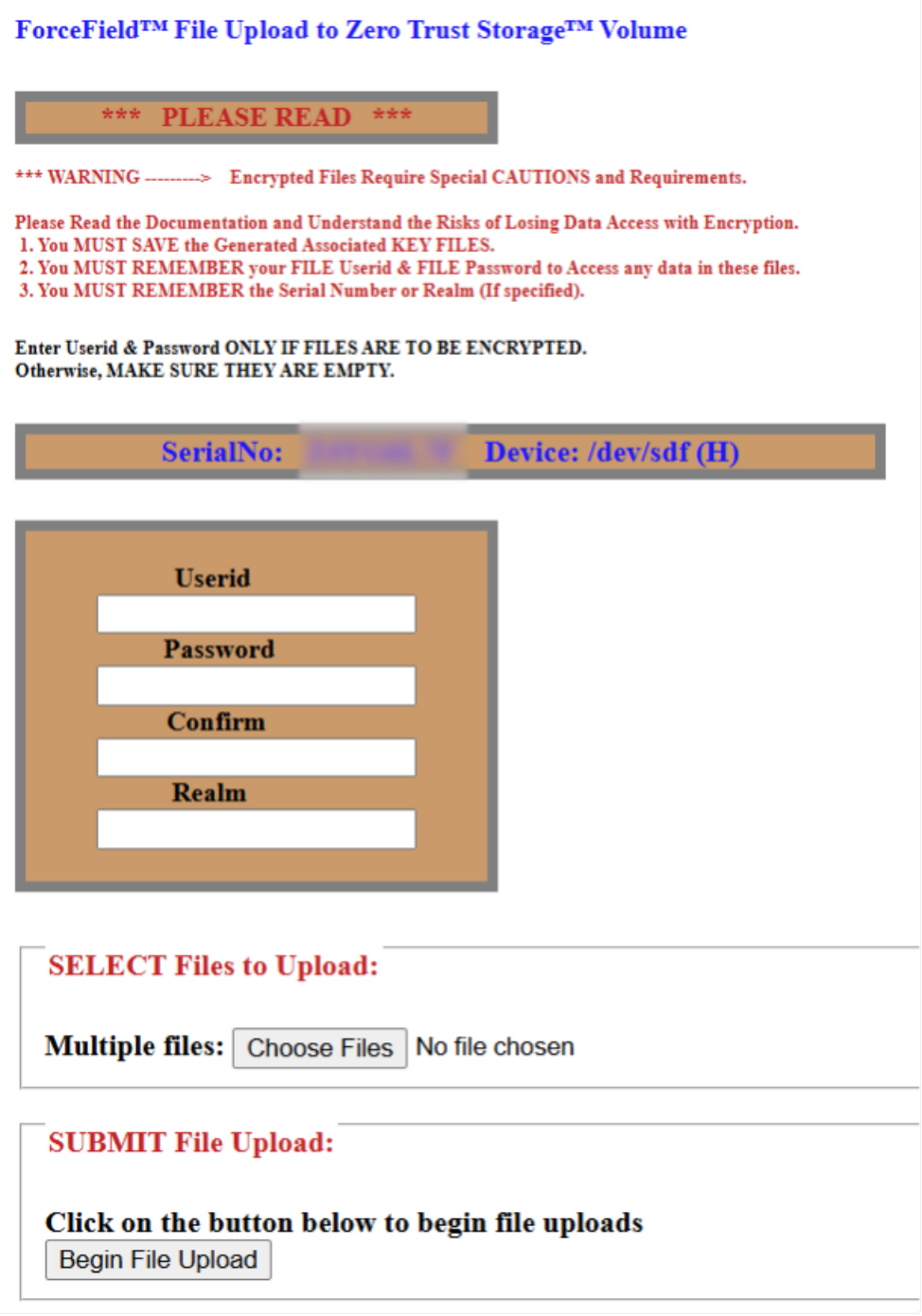


Figure 4-25: The default view after logging into the web interface for ForceField

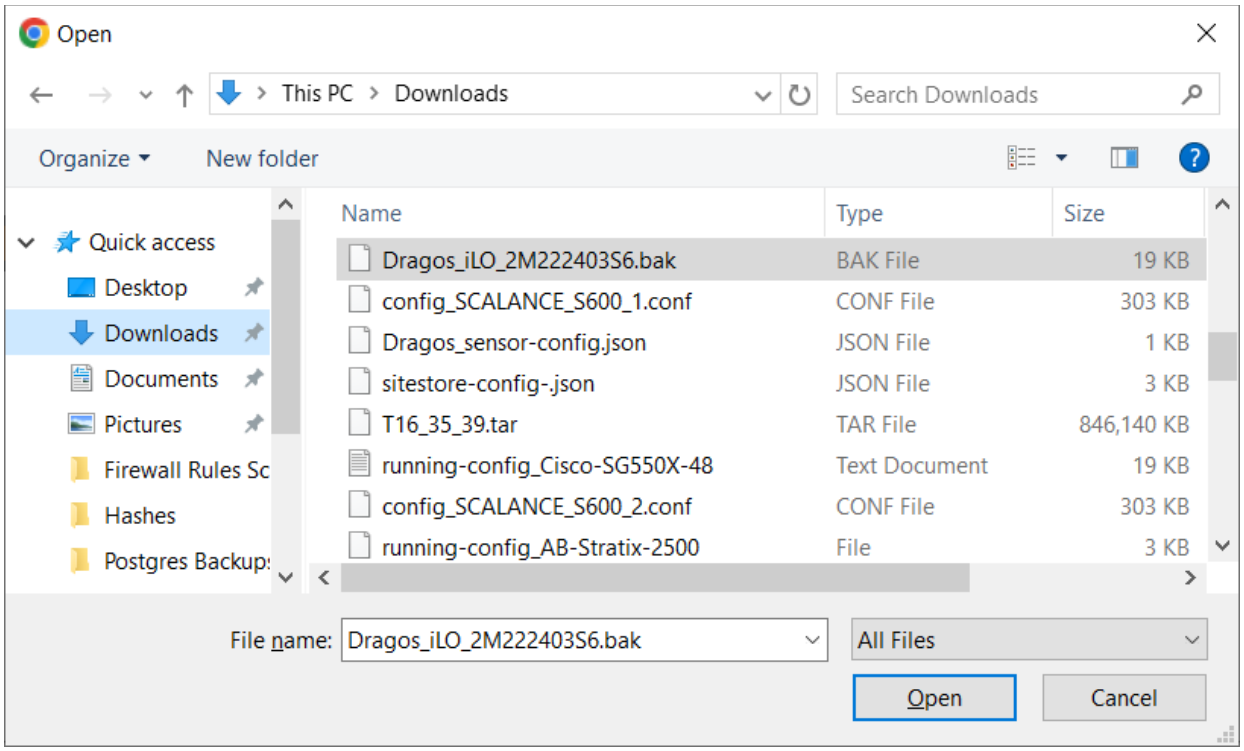
Note: Links on this web interface will not have visual indicators/feedback, but still work when clicked on.

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

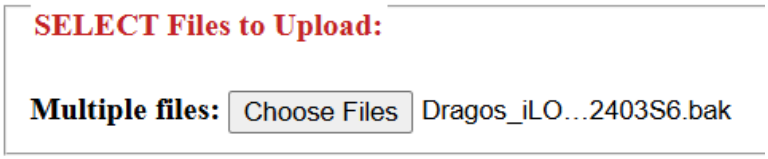


1688 **Figure 4-26: The default view when selecting the "Upload" option in ForceField**

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**

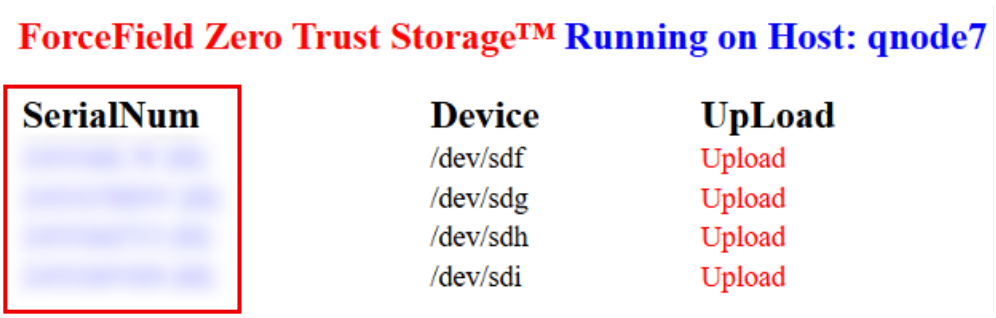


1691 **Figure 4-28: After selected, the files to upload will show here in ForceField**

```
--------------------
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`:



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 [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_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
Dragos_iLO_2M222403S6.bak	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]

C.1.4 FactoryTalk® Logs in Windows Event Viewer

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

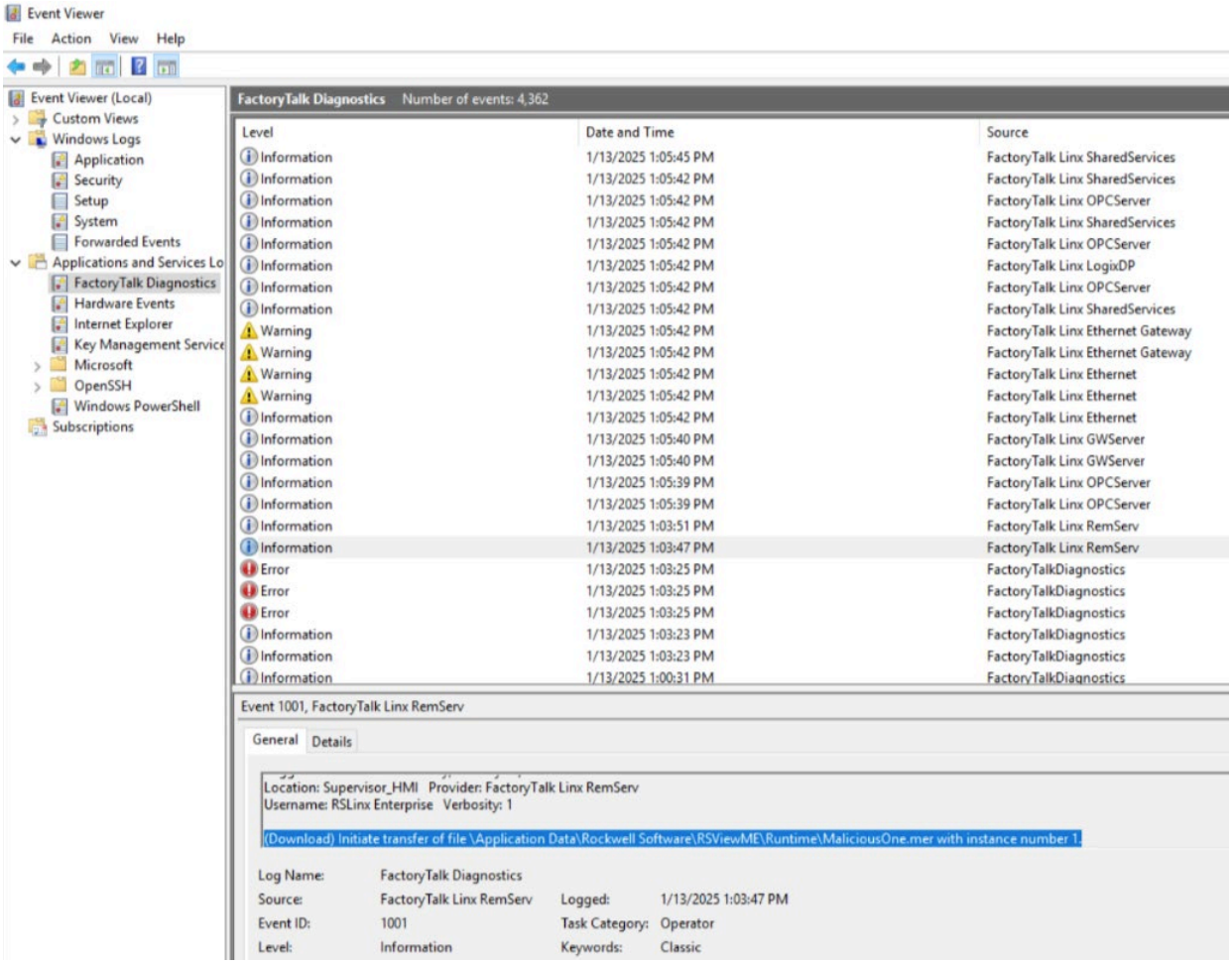
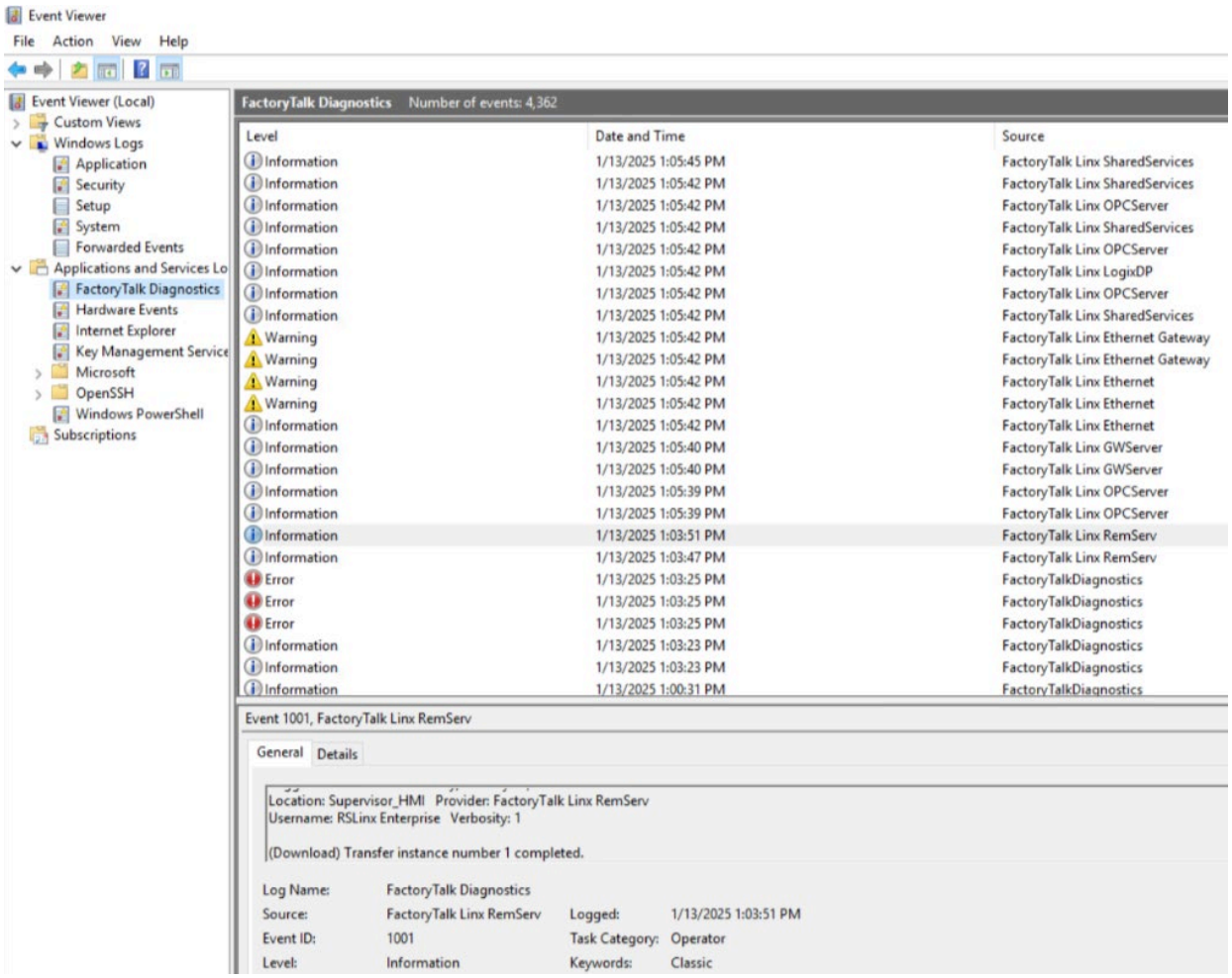
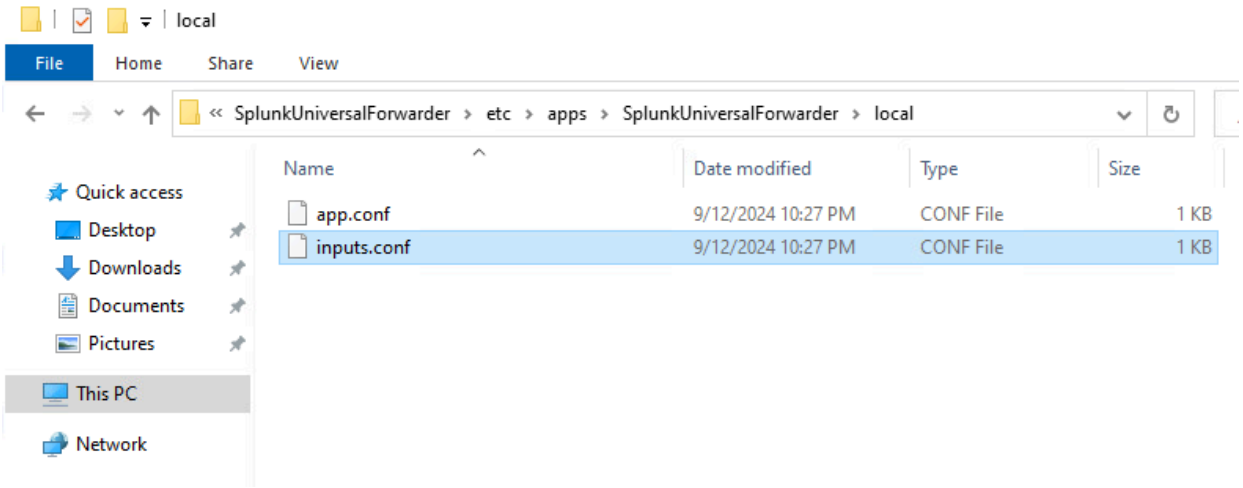


Figure 4-32: The FactoryTalk® Diagnostics logs residing in Event Viewer



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.

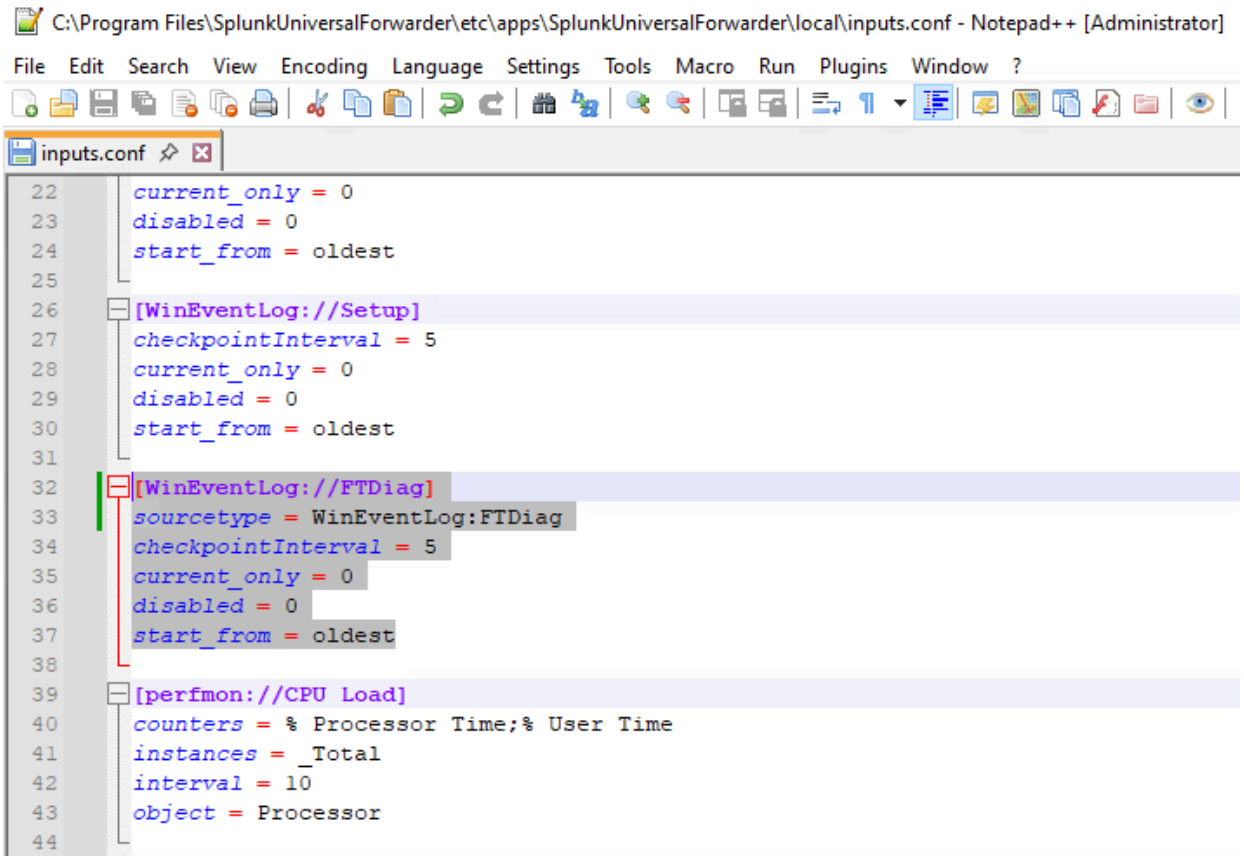


1711 **Figure 4-34: The location of the "inputs.conf" file to edit**

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

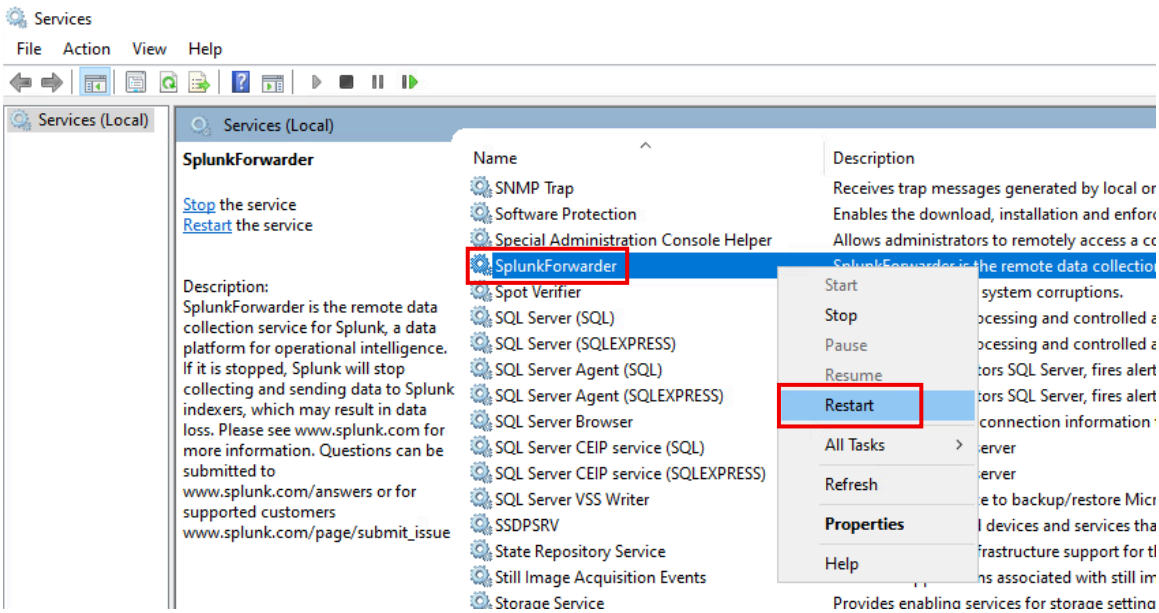
```
1713        [WinEventLog://FTDiag]
1714        Sourcetype = WinEventLog:FTDiag
1715        checkpointInterval = 5
1716        current_only = 0
1717        disabled = 0
1718        start_from = oldest
```

1719 See the screenshot below for reference.



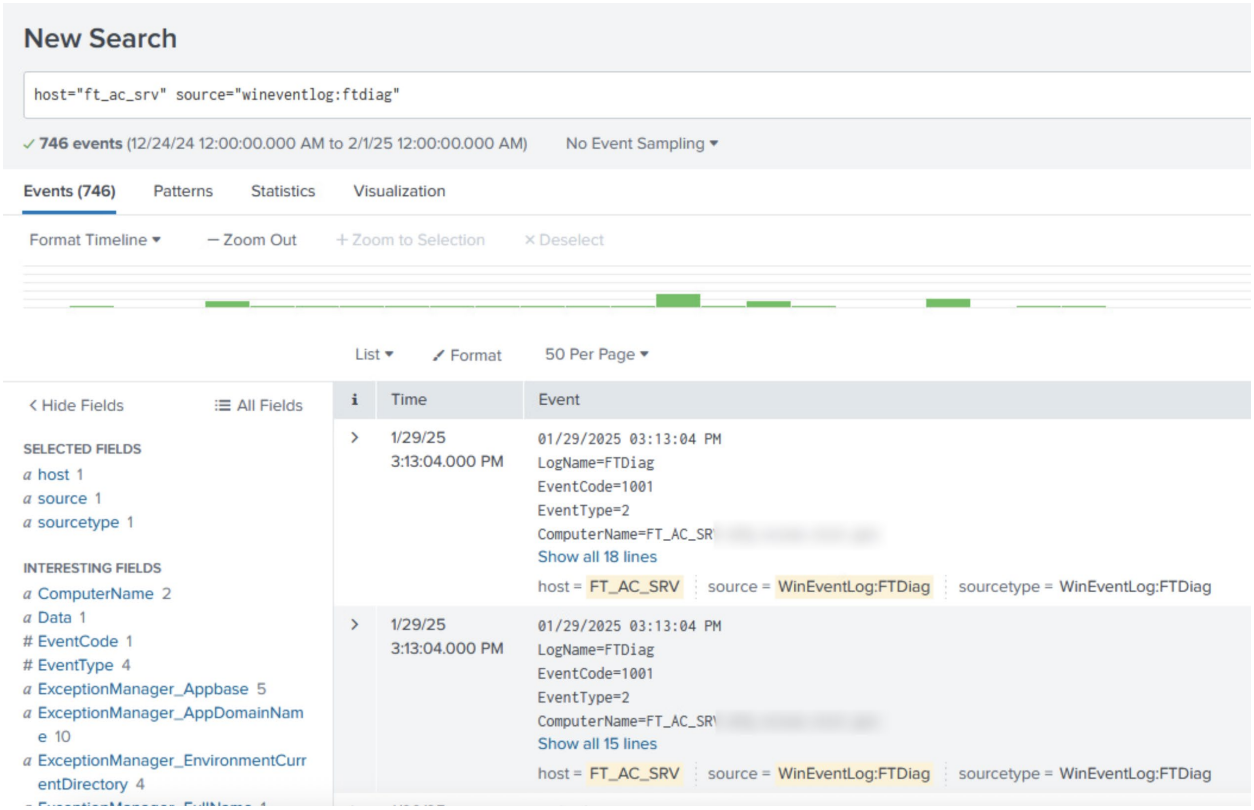
1720 **Figure 4-35: The "inputs.conf" file opened in Notepad++ to add FactoryTalk® logs to the ingest**

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]

C.2 Scenario A: Technical Details – Response

C.2.1 Dragos Case Creation

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

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

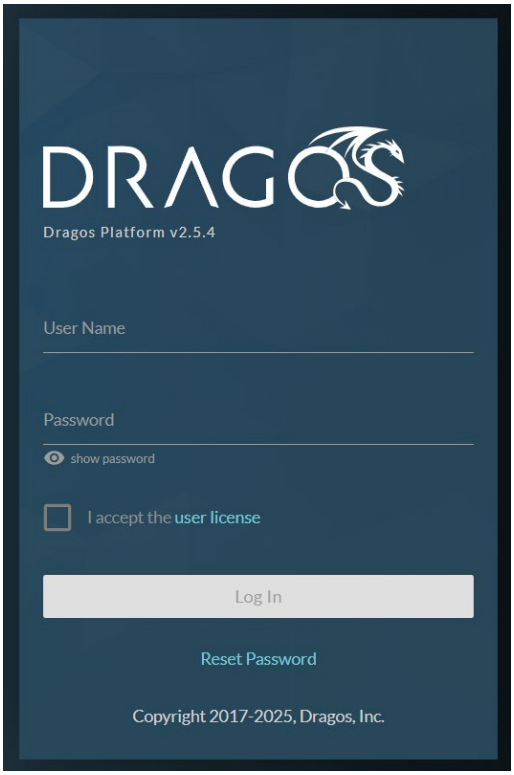
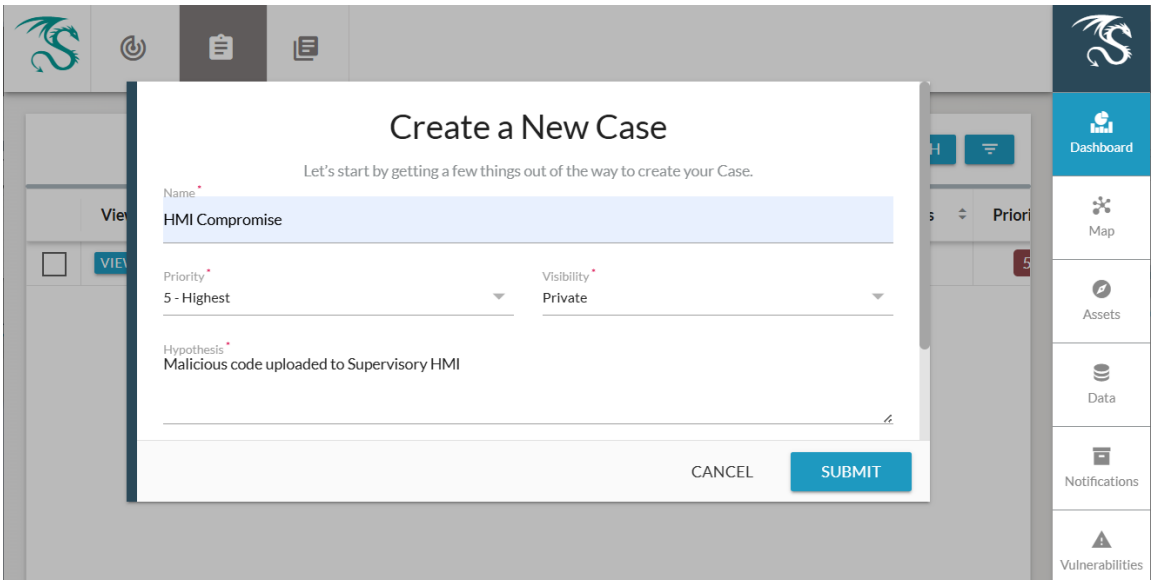


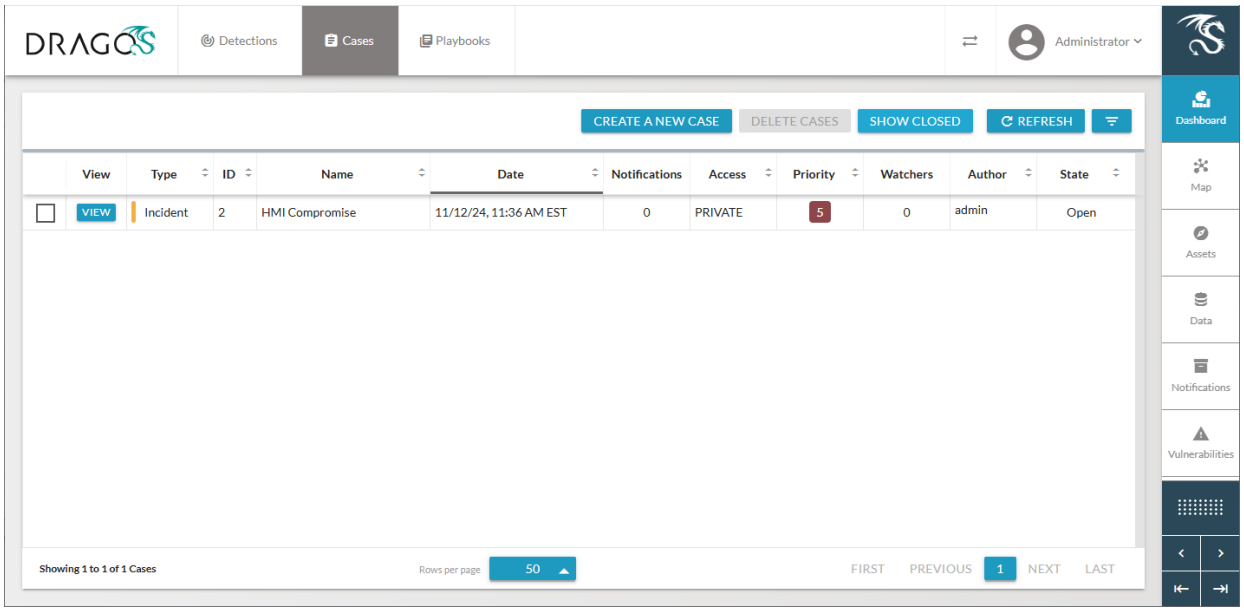
Figure 4-38: Login screen for the web interface of Dragos

Once logged in, go to the Cases Tab to click the Create a New Case button to open a new case entry form. From the entry form, enter the case name, the priority level (0–5, with 5 being highest), visibility (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:



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

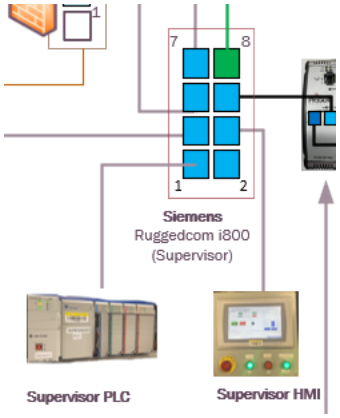
1743 While the ISA3000 has many features that control the flow of network traffic, the IRT determined, based
1744 on the risk of the scenario, to isolate physically between the manufacturing lab network and the
1745 industrial DMZ. To perform this isolation, the Ethernet cable in the WAN port was disconnected.

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]

C.2.4 Inductive Automation, Data Historian

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

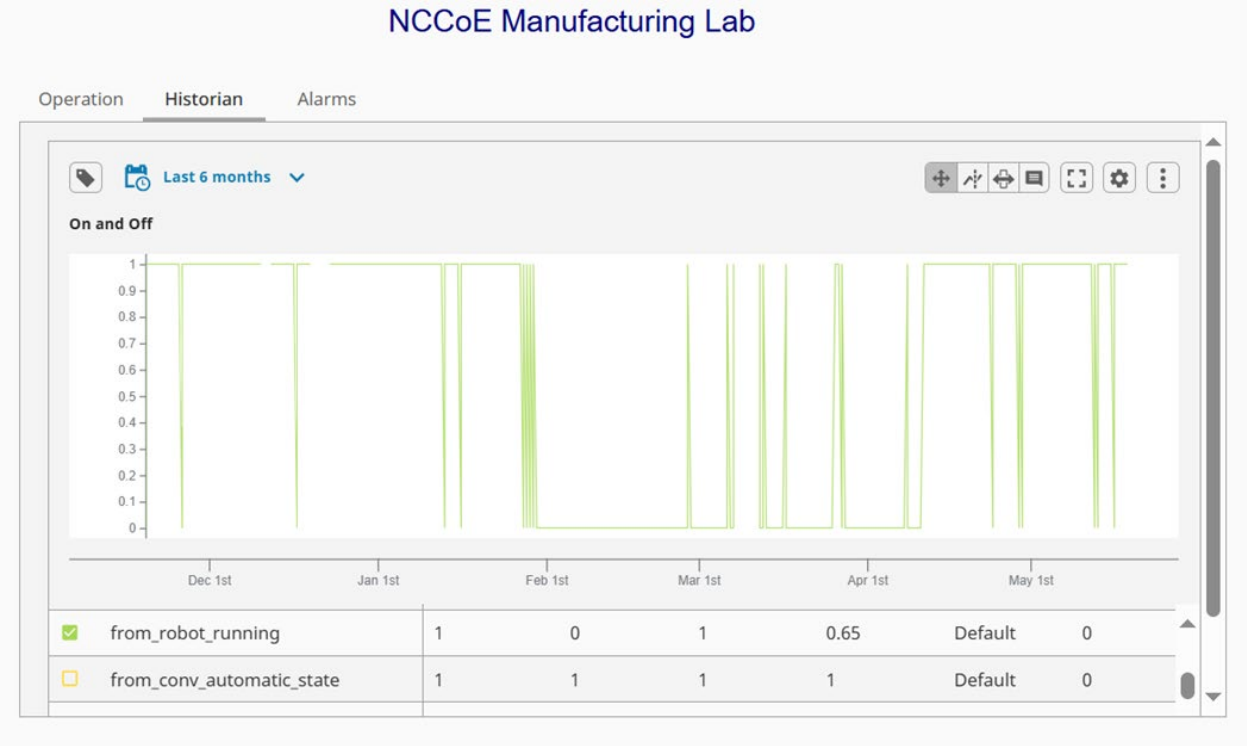


Figure 4-43: Data historian showcasing the tags indicating system start and stops

[Return to Scenario A]

C.2.5 Rockwell FactoryTalk® Transfer Utility

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

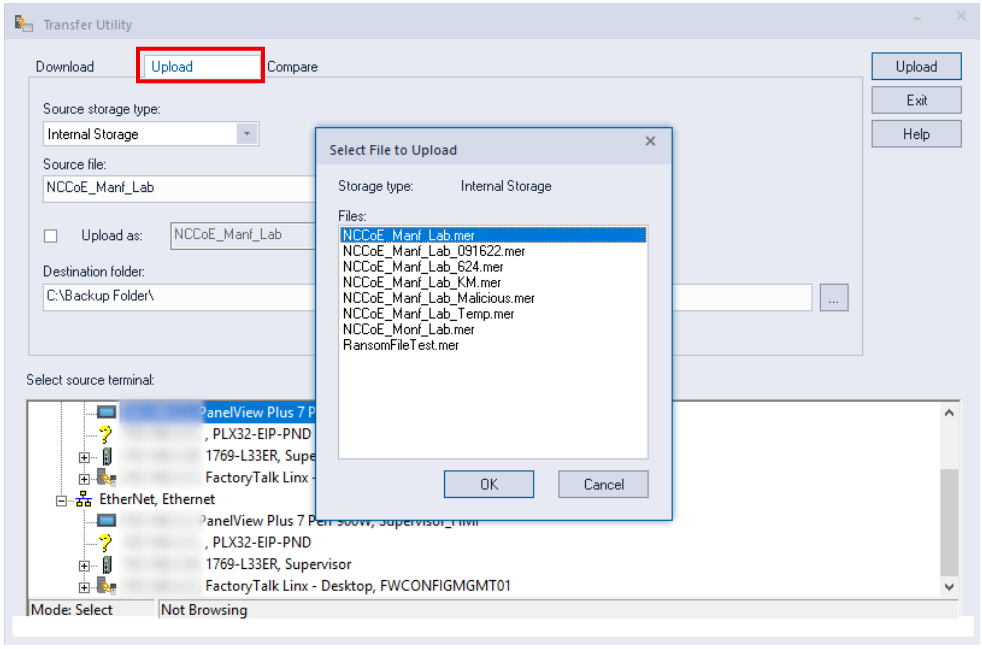


Figure 4-44: Selecting the file to upload using Rockwell's Transfer Utility

The "Compare" tab of Rockwell Automation's Transfer Utility allows the user to determine that the file running on the HMI is different than the desired file found on the Engineering Workstation.

In the following example, the `.mer` configuration file from backup is compared with the running or "Remote file":

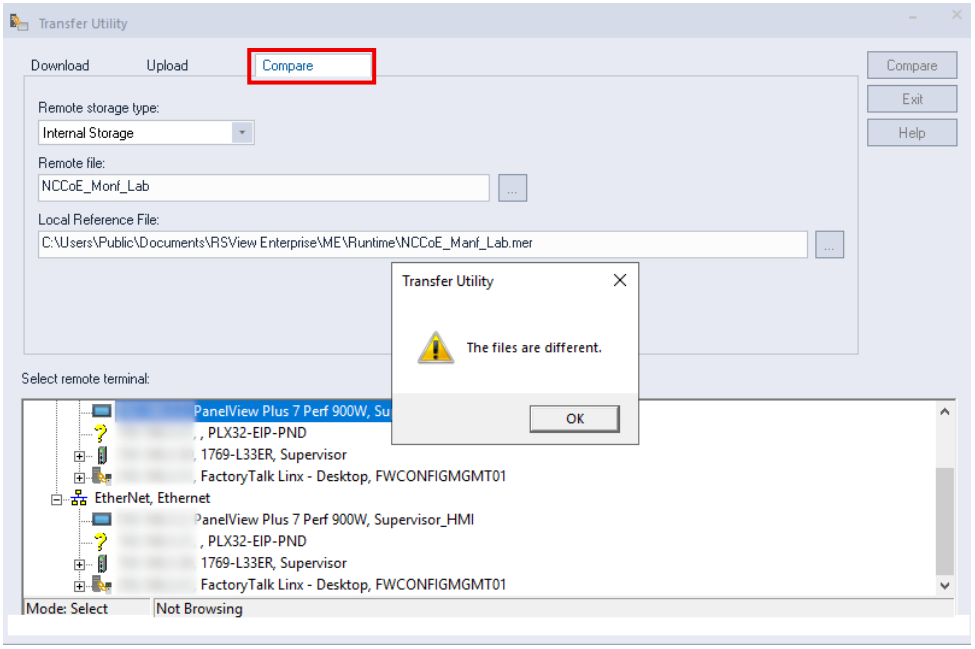


Figure 4-45: Comparing files using Rockwell's Transfer Utility

[Return to Scenario A]

C.2.6 Rockwell Automation FactoryTalk® AssetCentre, Log Review

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

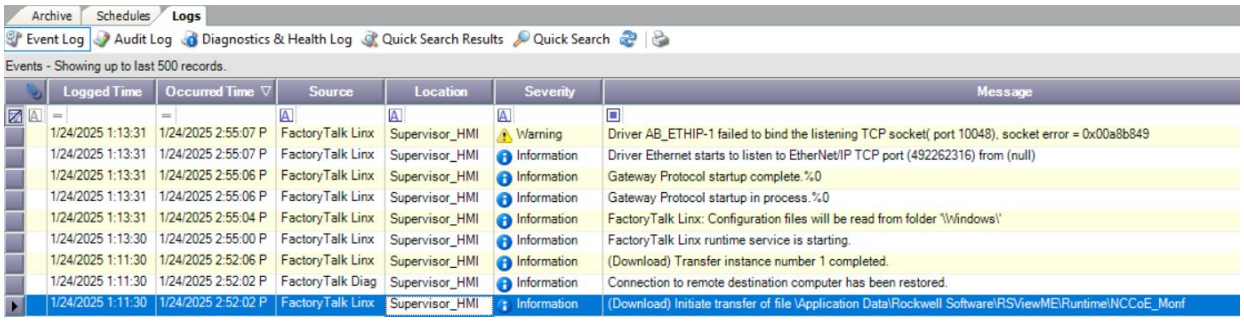


Figure 4-46: Blue line indicating the malicious file name and date of occurrence

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

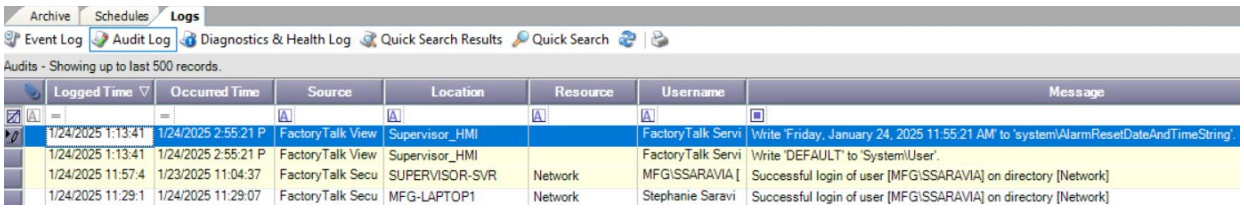


Figure 4-47: Audit log showing which users logged in recently

[Return to Scenario A]

C.2.7 Update Dragos Case

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

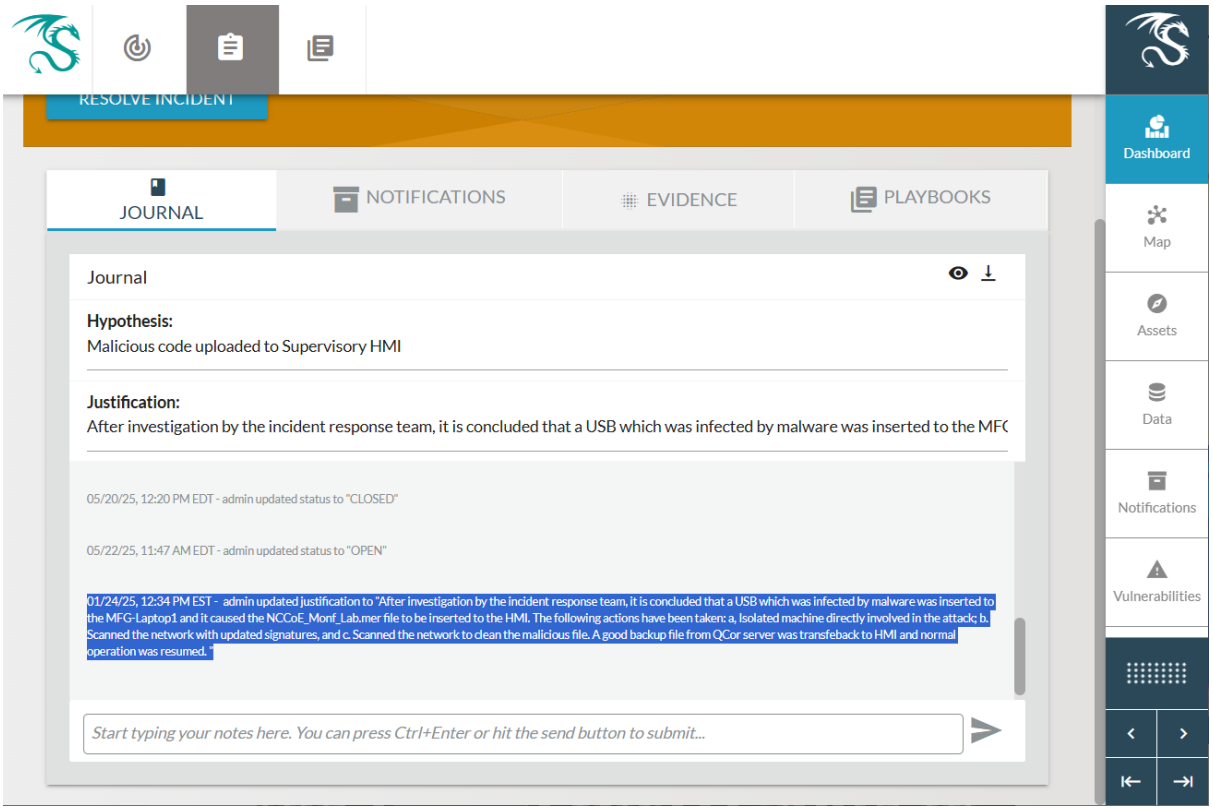
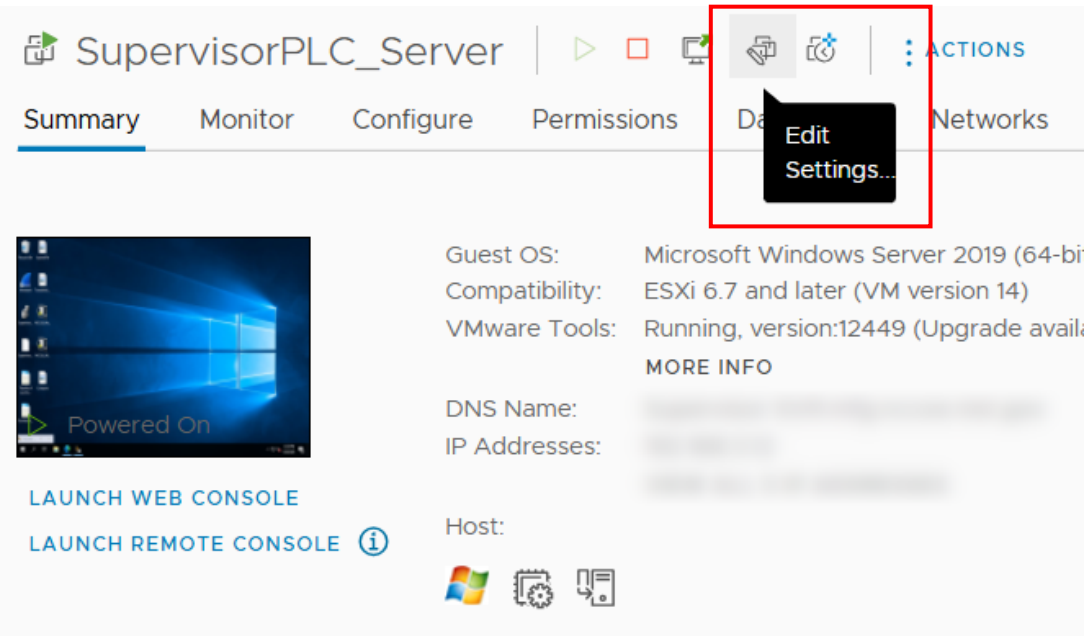


Figure 4-48: Updating a Dragos ticket with a new comment

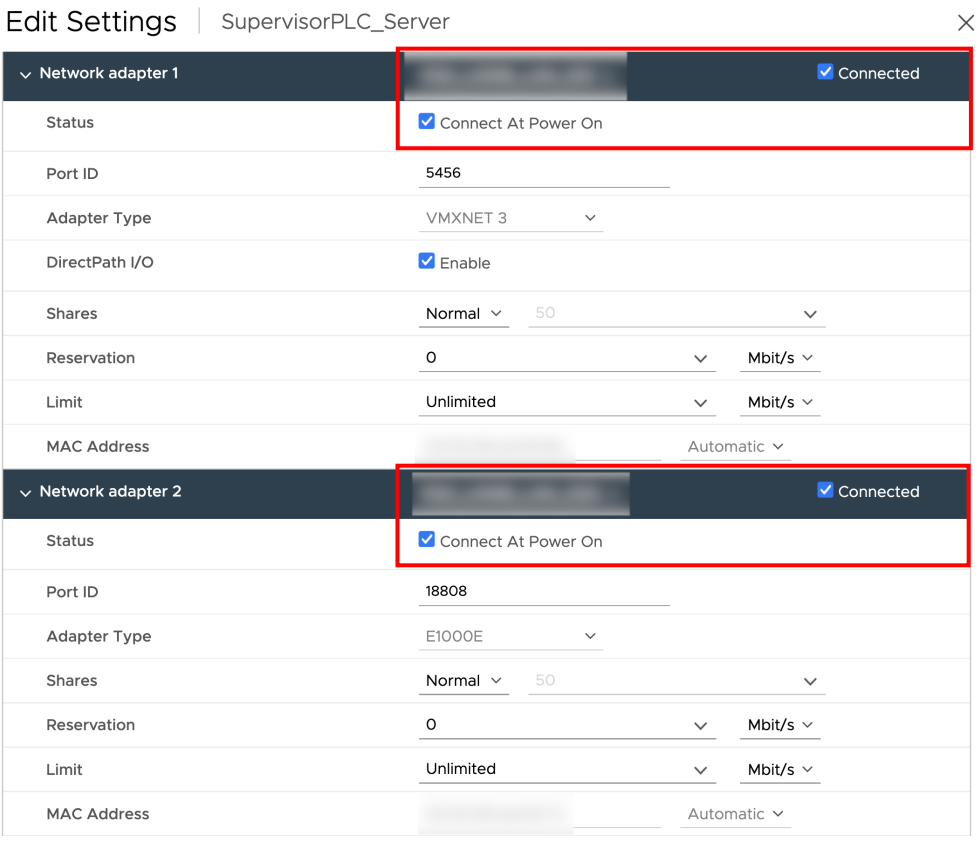
[Return to Scenario A]

C.2.8 Remove Virtual Machine from Network

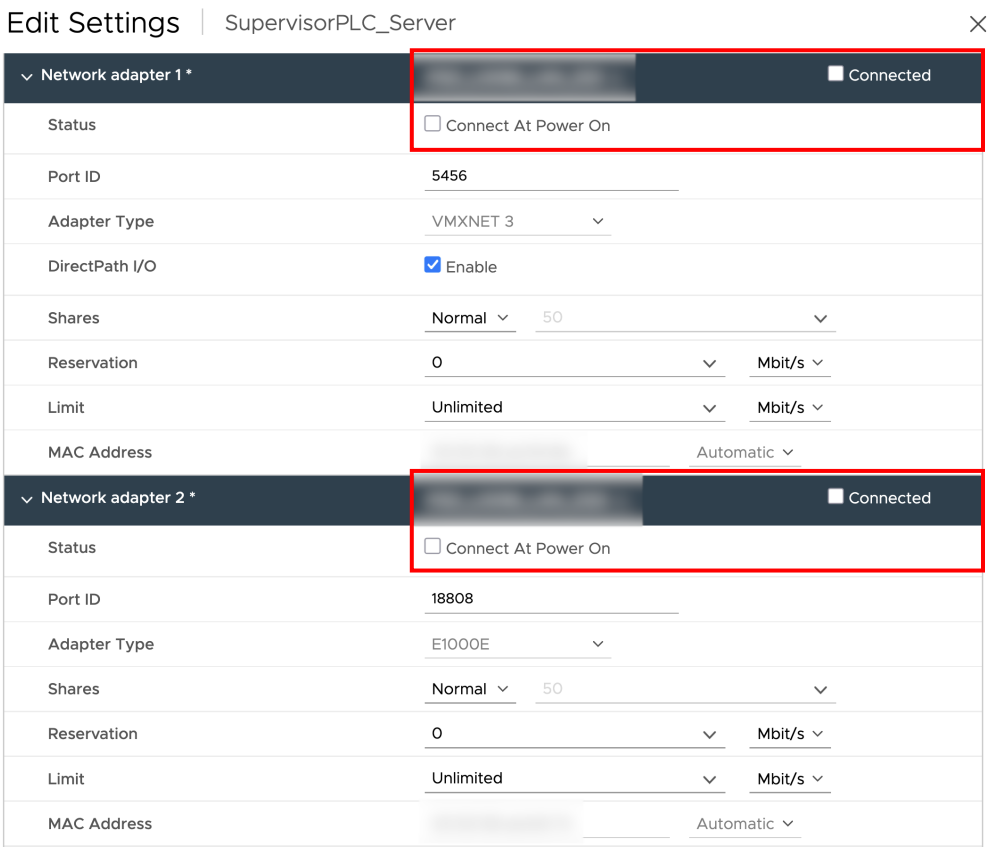
For all scenarios, vSphere was used for the infrastructure of the virtual machines (VMs) (not including AWS). To isolate a virtual machine within a vSphere environment, log into vCenter and find the corresponding VM to remove from the network. The following screenshots provide a step-by-step guide. It starts by demonstrating how to access the VM settings from its `Summary` page, then indicates the location of the network settings and the boxes to uncheck. Once these boxes are unchecked, the VM will 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**



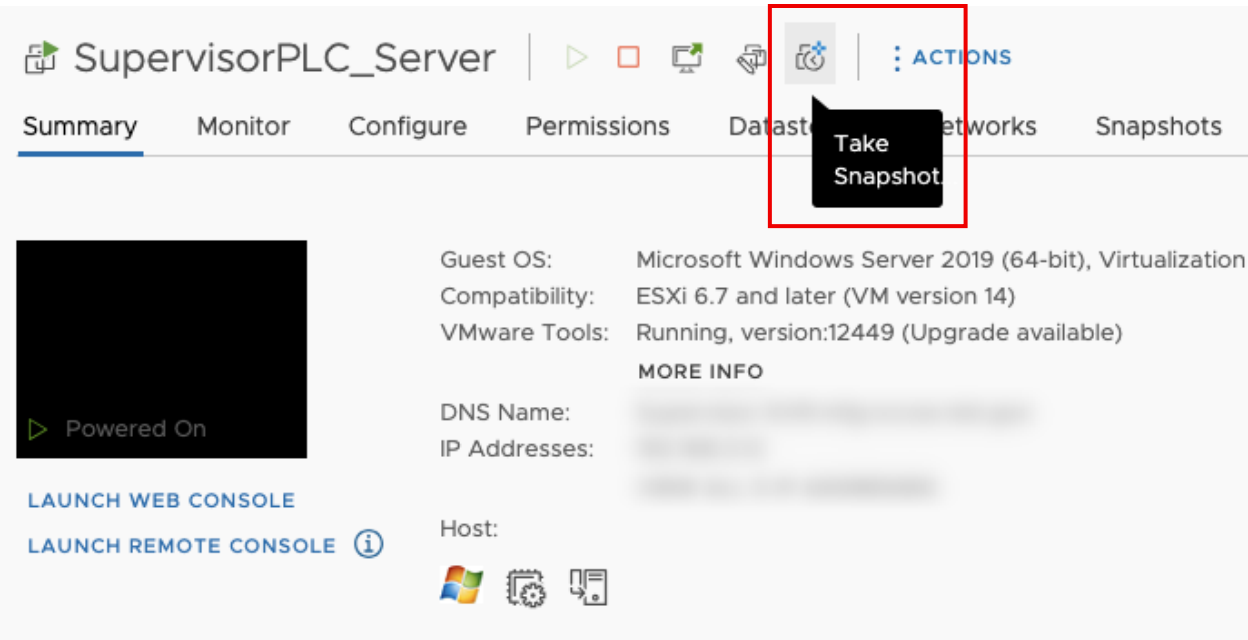
1796 **Figure 4-51: Network settings for a VM turned off in Edit Settings**

1797 [Return to Scenario A]

1798 [Return to C.5.6 - Disconnect JumpHost VM from Network]

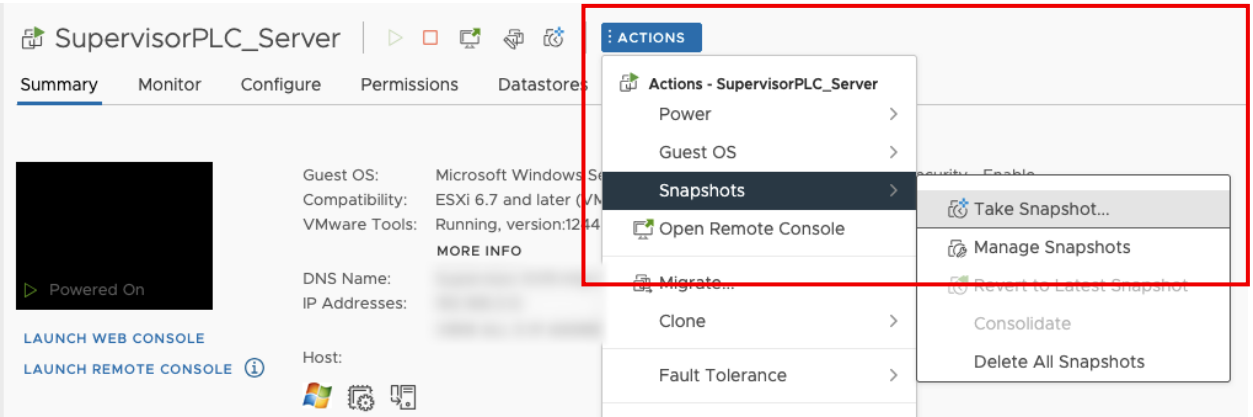
1799 C.2.9 Taking Snapshots of VMs

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.



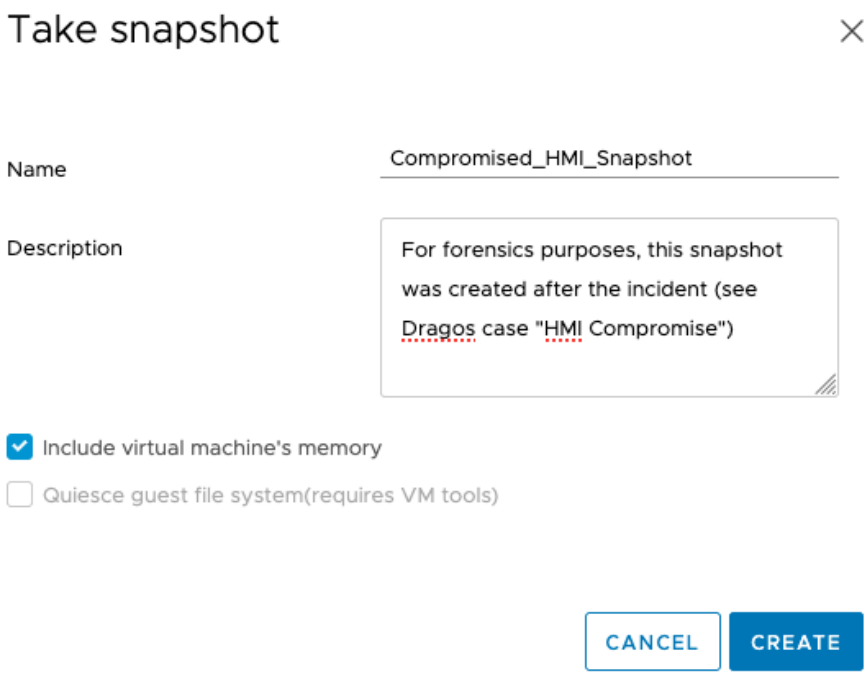
1802 **Figure 4-52: The `Take Snapshot` button on a VM's settings page**

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



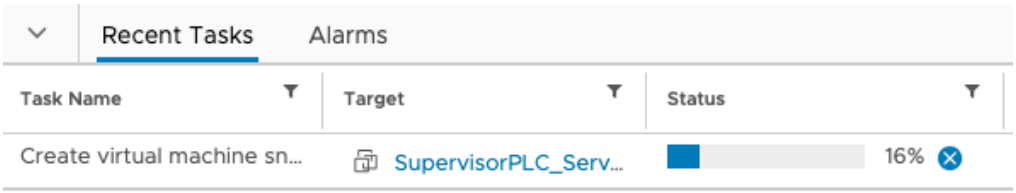
1804 **Figure 4-53: The `Take Snapshot` button in the `Actions` context menu**

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



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

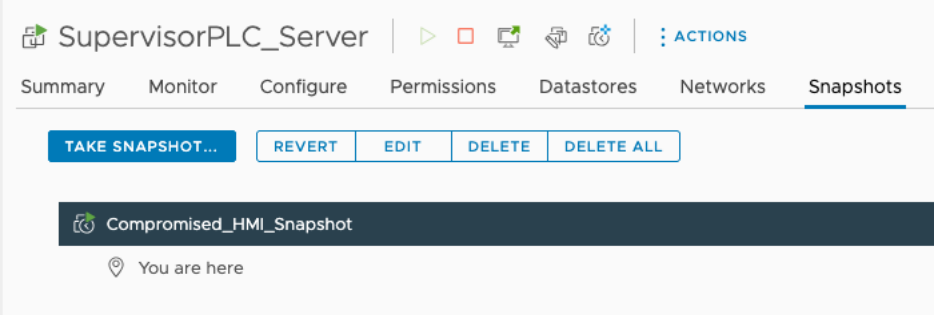
1808 In vCenter's tasks at the bottom of the interface, the progress of the snapshot is shown as a Status:



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:*



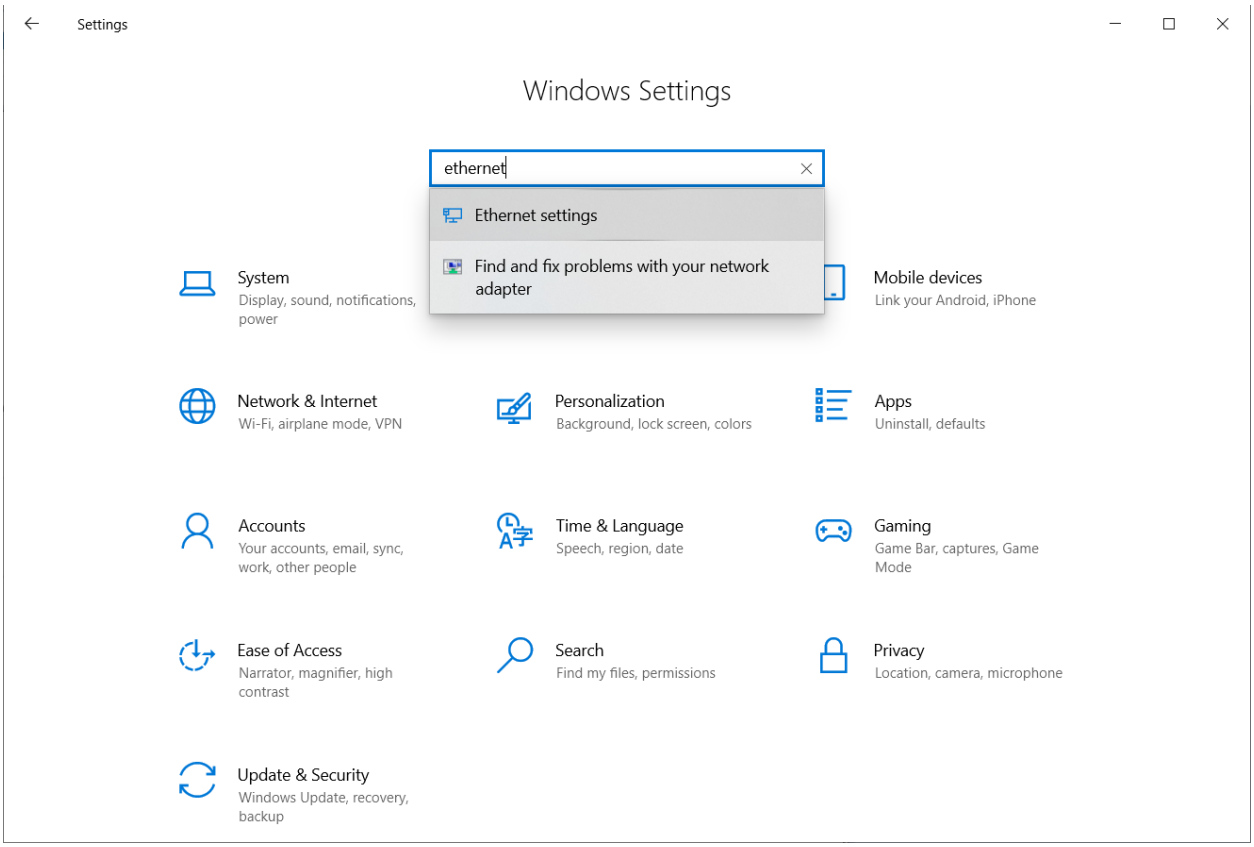
1812 **Figure 4-56: Snapshots in the VM's settings in vCenter**

1813 [Return to Scenario A]

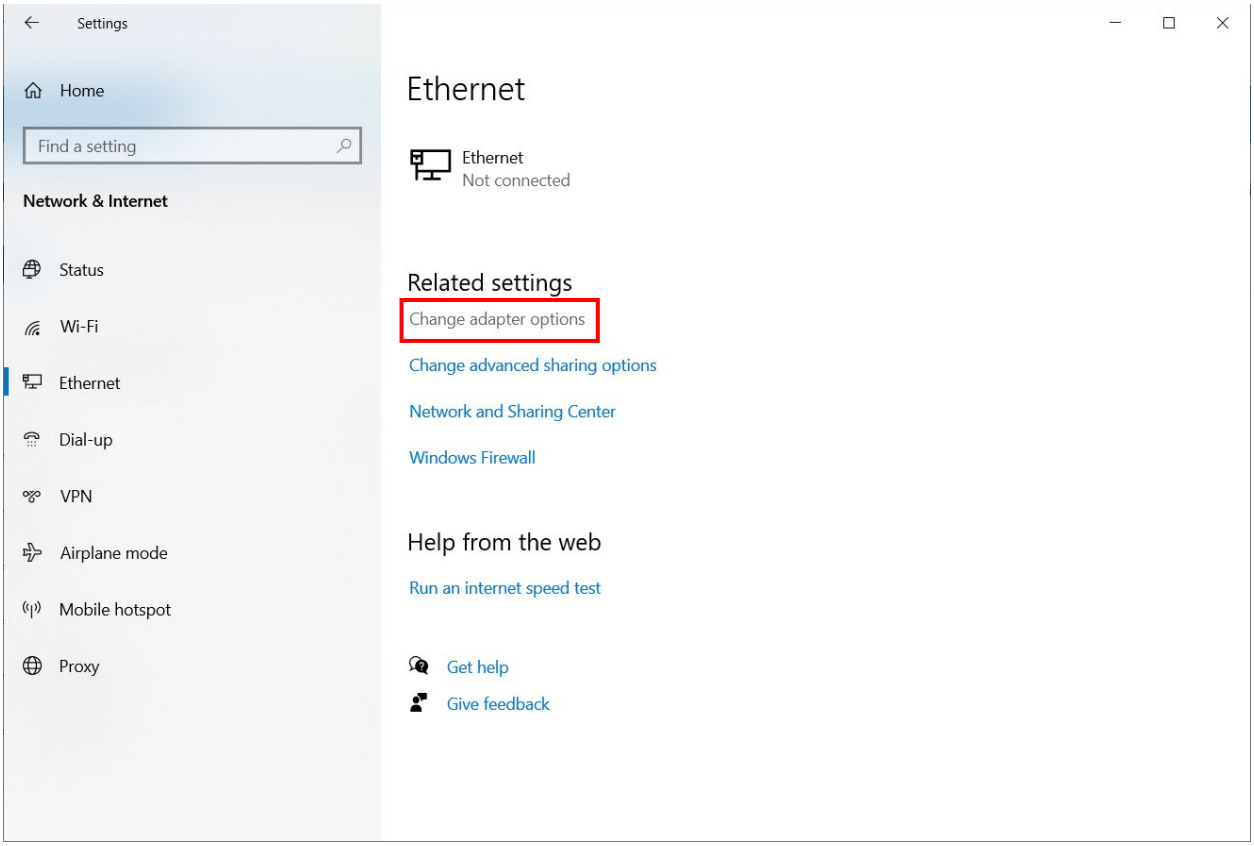
1814 [Return to C.5.7 - Take Snapshot of JumpHost VM]

1815 C.2.10 Remove Physical Device from the Network

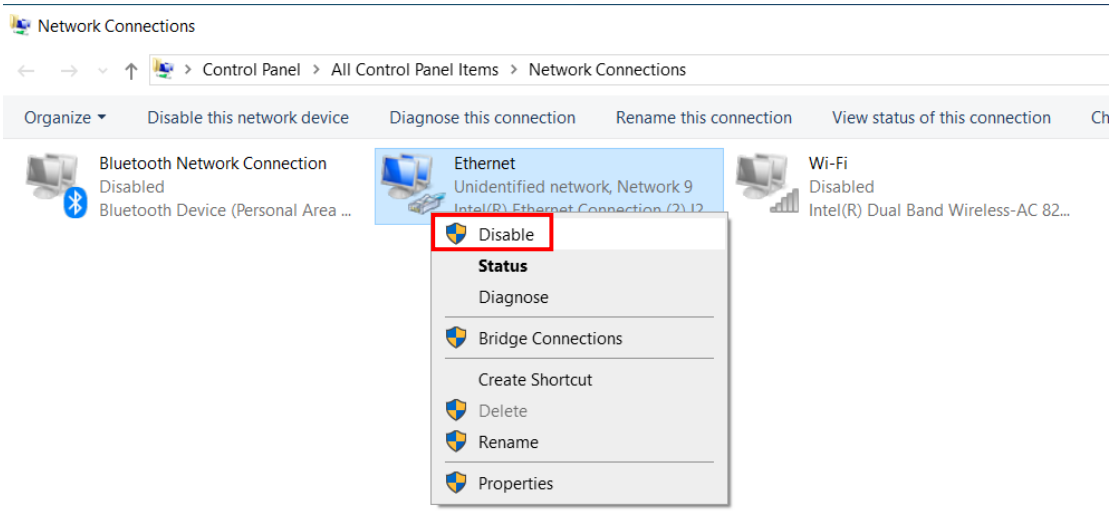
1816 To disconnect a physical device, such as a laptop, from the network, all network adapters should be
1817 disabled. On Windows operating systems, this can be done by going to `Ethernet settings`, clicking
1818 on `Change adapter options`, and right-clicking each active network connection to select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

C.2.11 Antivirus Scan

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

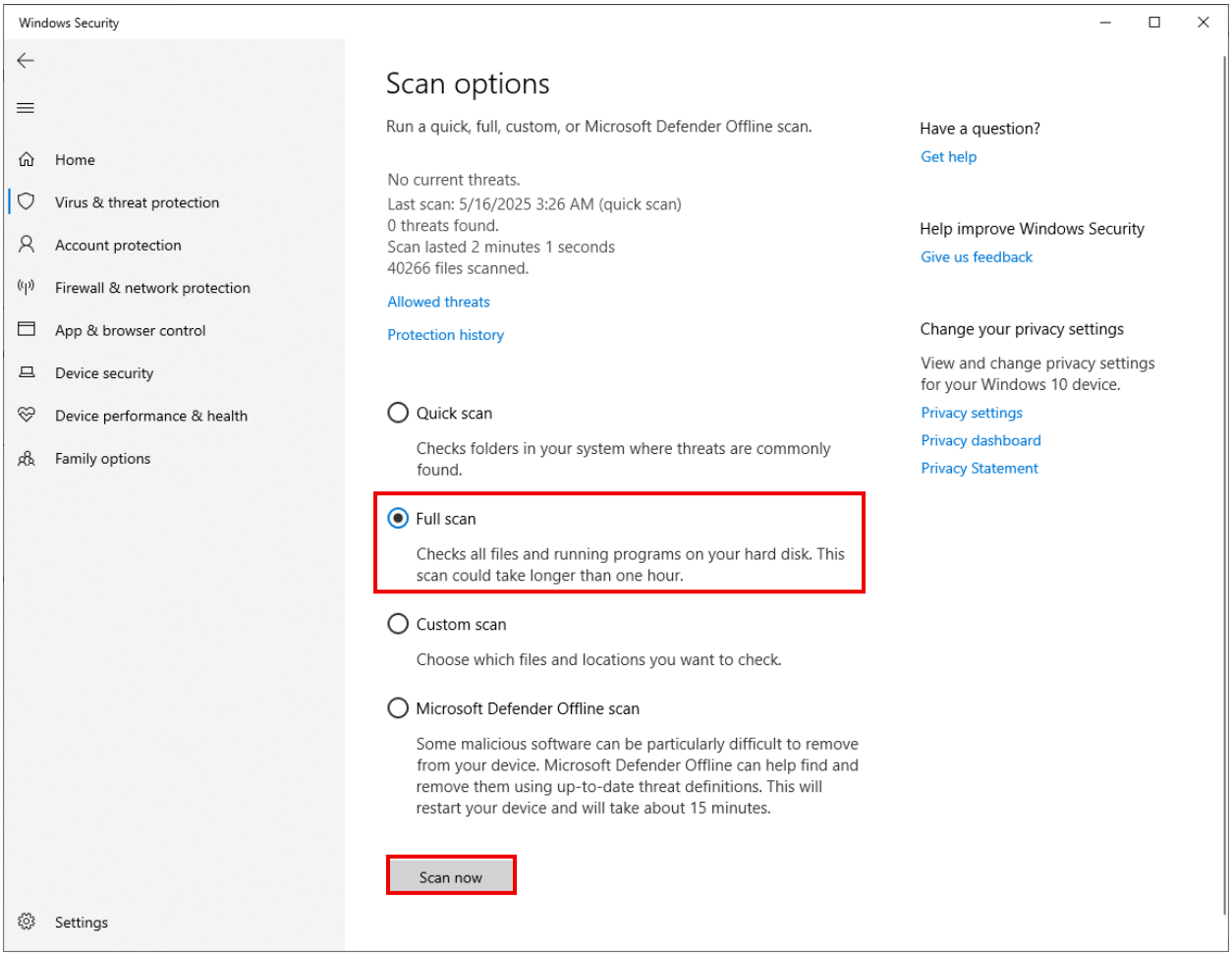
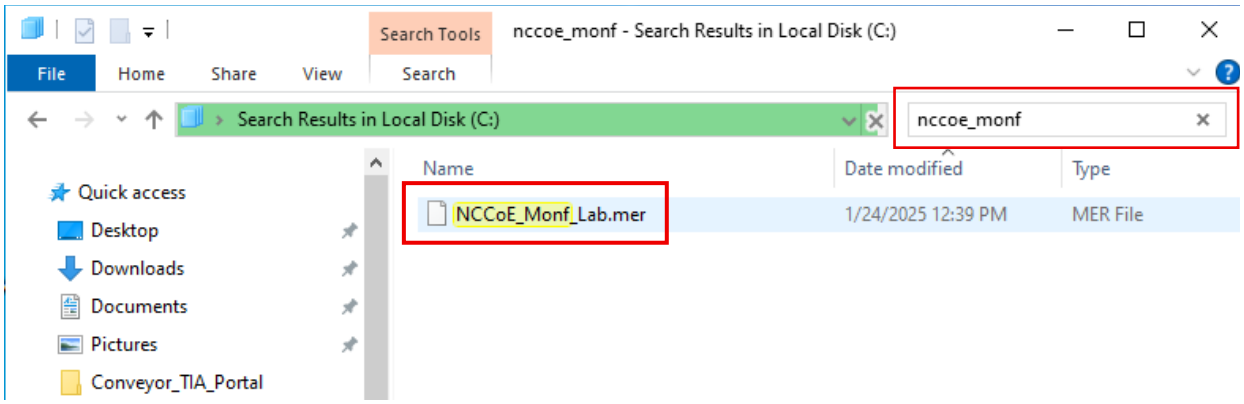


Figure 4-60: Performing a "Full scan" in the "Virus & threat protection" tab of Windows Security

[Return to Scenario A]

C.2.12 Search for Malicious File

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

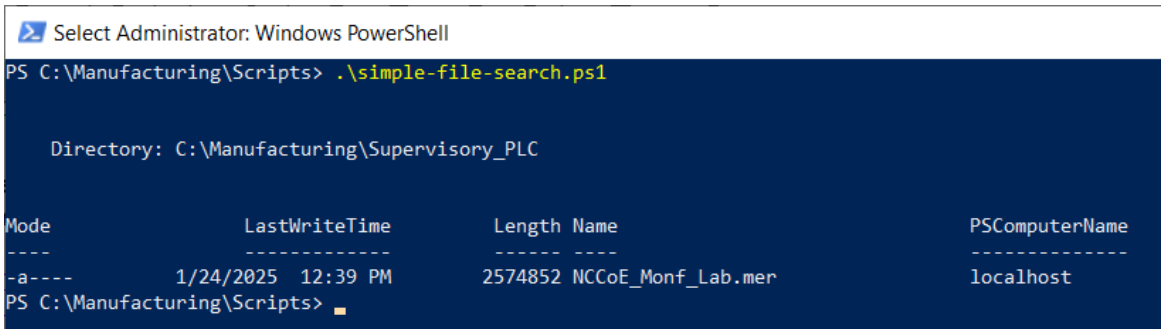
1838 To address this, a PowerShell script can be run on IT or engineering workstations to scan all files for a
1839 suspicious configuration file. In Scenario A, this script was developed to search for the specific malicious
1840 file:

```
<#
    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:



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

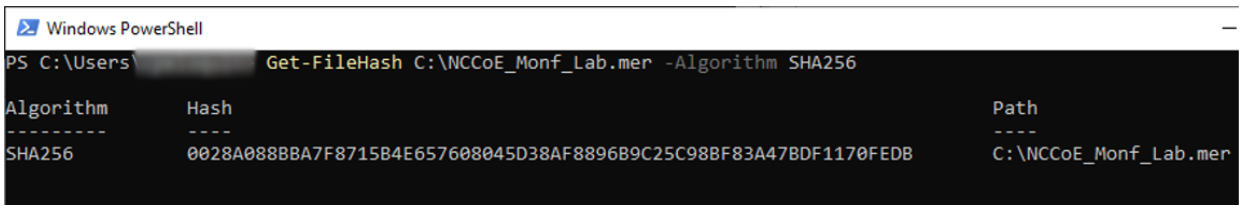
1845 In this scenario, the malicious configuration file has an obvious name. A more thorough method for
1846 identifying a malicious file is to manage the integrity of known clean files. This can be achieved by main-
1847 taining a list of SHA-256 hashes for all known clean files. In the following set 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.



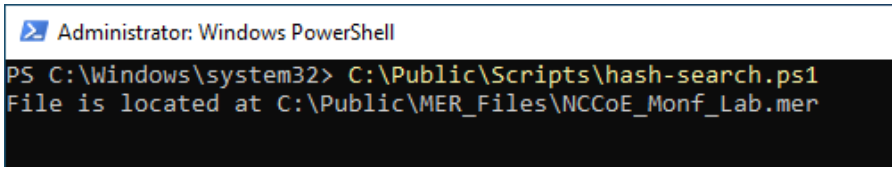
1853 **Figure 4-65: Taking a cryptographic hash of the suspected malicious file to find any variants**

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
$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"

    }
}
```

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:



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]

C.3 Scenario A: Technical Details – Recovery

C.3.1 Downloading Backups from Authoritative Source

Following the incident, system recovery should be initiated by retrieving backups using the configured backup solution. The solution used in this Practice Guide is ForceField. To perform this recovery, navigate to the Forcefield file structure and click on the file name desired for download from the storage 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_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
Dragos_iLO_2M222403S6.bak	1	18.76K	20250520 10:34:19
30 File Extents on this Volume			

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

NOTE: Links on this site will not have visual indicators/feedback, but still work when clicked on.

Once clicked, a prompt appears to save the file onto the local machine. Be sure the machine performing the action is a clean workstation. Section C.3.2 will explore the options to restore this configuration file to the HMI.

[Return to Scenario A]

C.3.2 Restore the HMI

After determining that the HMI is compromised, the HMI device is disconnected from the network. Following this, as production has already ceased, the HMI is removed entirely to achieve isolation on the process network. A new HMI is procured, and at this time, the approved file from qualified backup sources may be loaded.

If any issues arise, a shutdown may be forced on the HMI by placing a probe on the reset pin, located physically on the back of the device, labeled as `default`. This will, on reboot, bring the machine to a reset menu. This can be exited with the `no changes` option.

Following this, a reboot menu on the HMI panel will display. For Allen Bradley PanelView™ Plus, interrupting normal boot operations is performed by either using the touchscreen to engage the white box in the bottom left corner or by connecting a keyboard and pressing F1 to enter the boot menu.

When adding a new file to an HMI via USB, it is recommended to follow NIST SP 1334. There are two methods of placing said file on the terminal. If the PanelView™ Plus terminal recognizes the external storage device, a transfer can occur by navigating to the external storage source in the terminal and initiating a file transfer to internal storage. If this is not possible, the file may be placed in the internal storage location by exiting the machine edition terminal to the Windows CE environment, copying the file from the external storage drive, and copying the file to the location of internal storage.

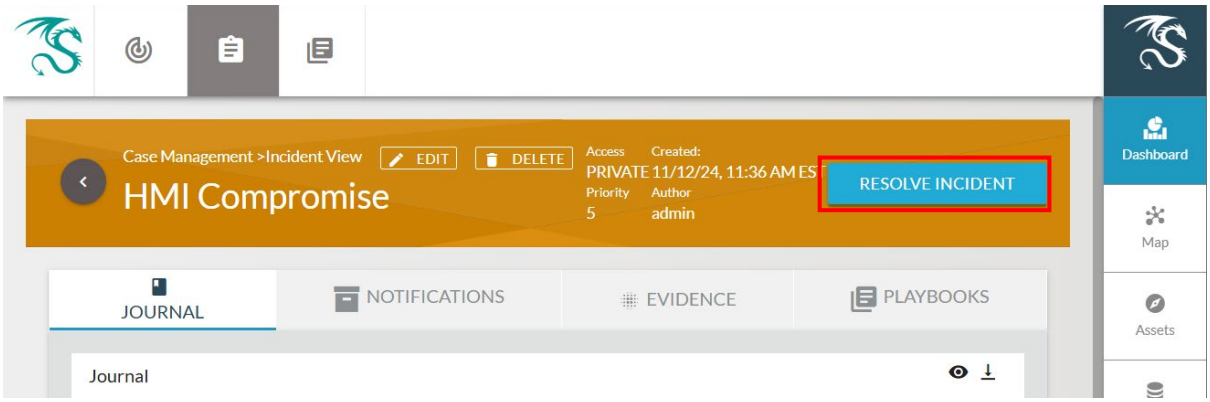
Once the approved file is copied onto the new HMI, the terminal is reloaded, and routine checks are performed to ensure all relevant parameters, such as communication, startup preferences, etc., are set. The `.mer` configuration file may then be loaded and run on the terminal.

[Return to Scenario A]

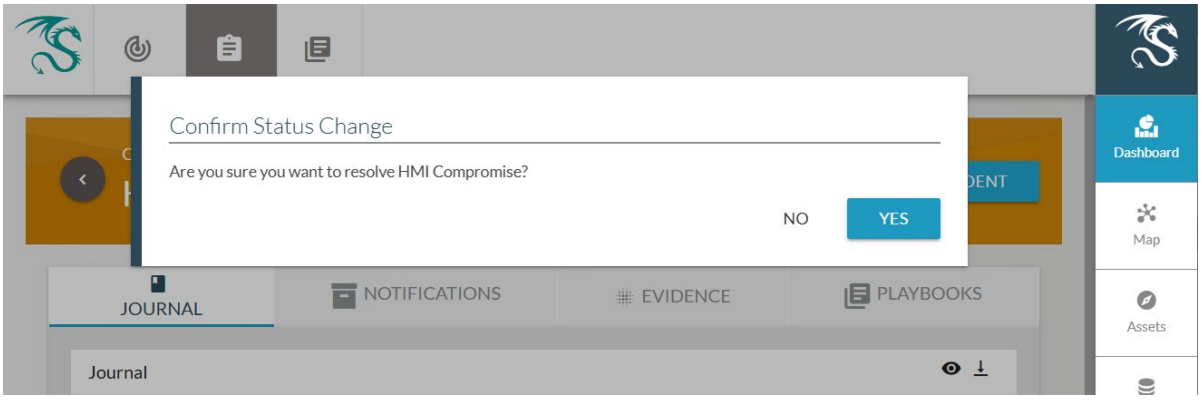
C.3.3 Close Dragos Ticket

Once the investigation is finished and the response and recovery have been completed, the case can be closed with a proper justification note entered.

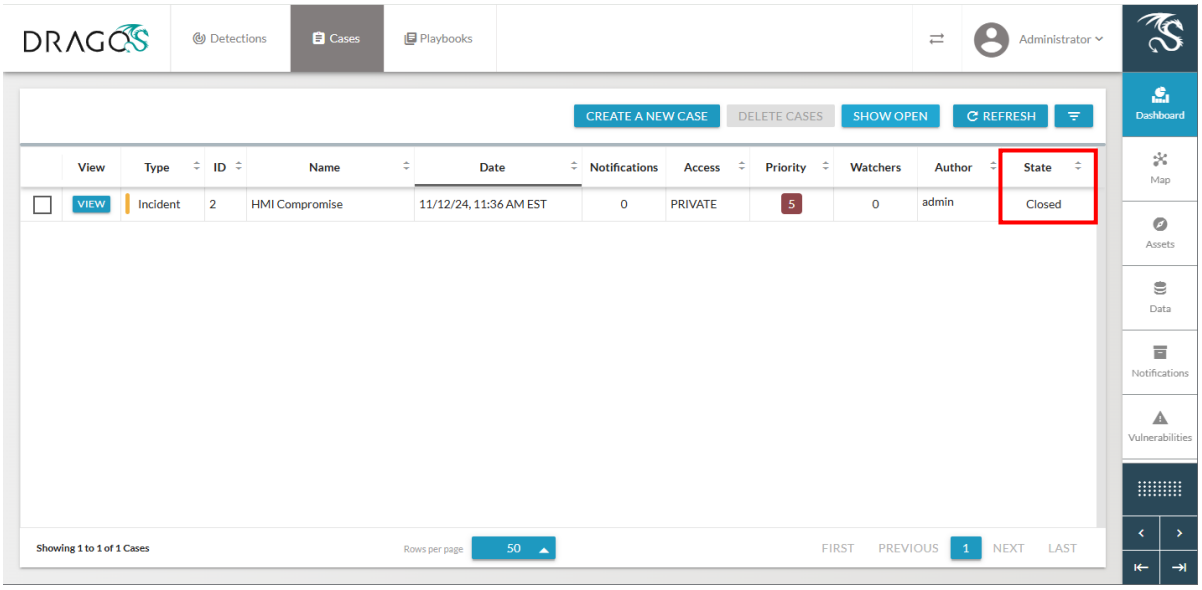
Click the `Resolve Incident` button to close the created case for the incident.



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]

C.4 Scenario B: Technical Details – Preparation

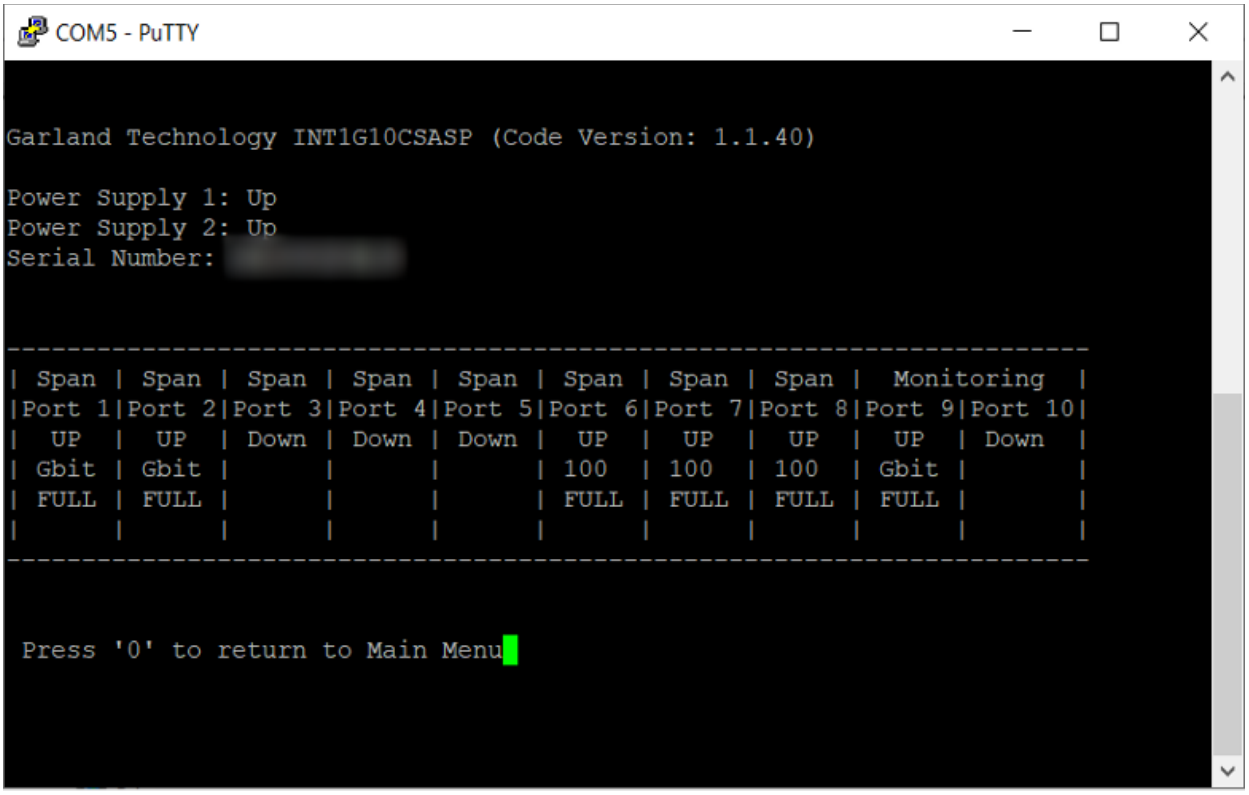
Before an incident occurs, a manufacturer must prepare for incident response and recovery. The following steps were taken to prepare for the Scenario B incident.

[Return to Scenario B]

C.4.1 Configuring Garland to Enable Multiple Detections

Garland was configured to receive SPAN information from several switches throughout the network and send that information to two network sensors, Dragos and Tenable.

Figure 4-72: Garland hardware configuration



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.

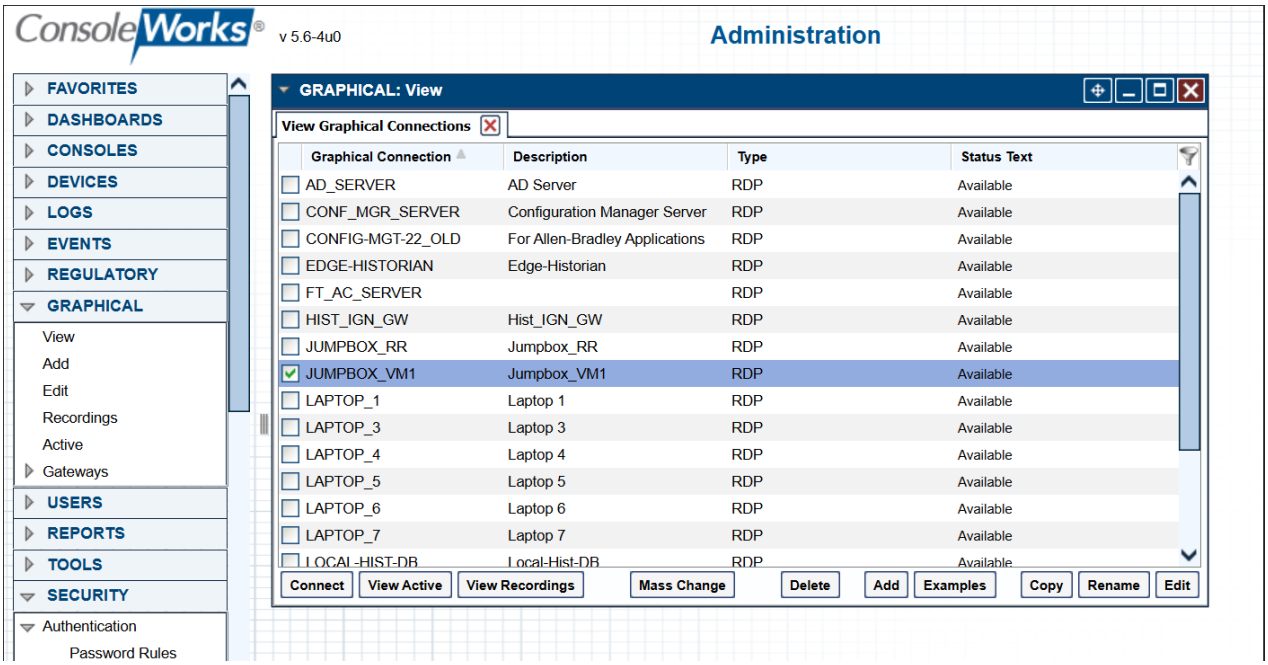
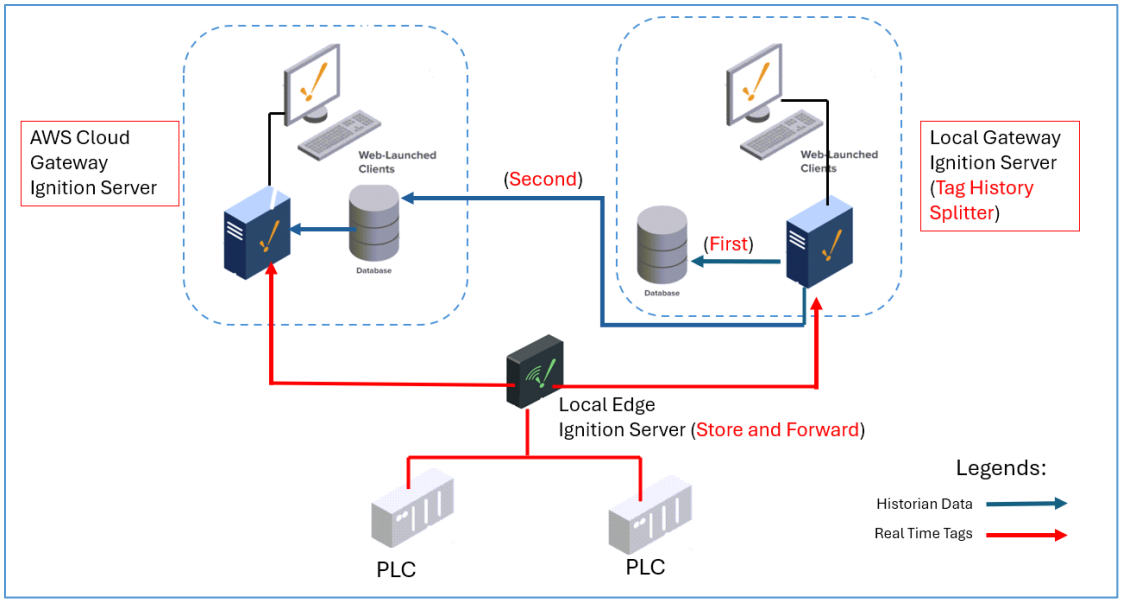


Figure 4-74: ConsoleWorks configured to provide remote access

C.4.3 Creating a Redundant Ignition Instance in AWS

NCCoE uses the Ignition tag splitter feature to implement redundancy. The Tag History Splitter is useful for automatically creating a backup of operational data. The architecture used in this build that is implementing the tag historian splitter is shown in Figure 4-75. There is one edge Ignition server collecting process data from the controllers, two gateway Ignition servers, and two Database servers. One is called local gateway with a local database for storing historian data sitting in OT DMZ.; the other is called AWS cloud gateway ignition with its own dedicated database also hosted in the cloud server. The Tag History Splitter Provider doesn't store history on its own, but with the proper configuration, the splitter will help to log tag history into multiple databases. The local Edge Ignition server connected to the PLCs is responsible for obtaining the real-time tag data from the PLC. Both the local and cloud Ignition servers are connected directly to the local Edge Ignition server to receive live tag data. The real-time tag data and historian data can be displayed from a web-launched client once the dashboard is built from the Ignition designer.

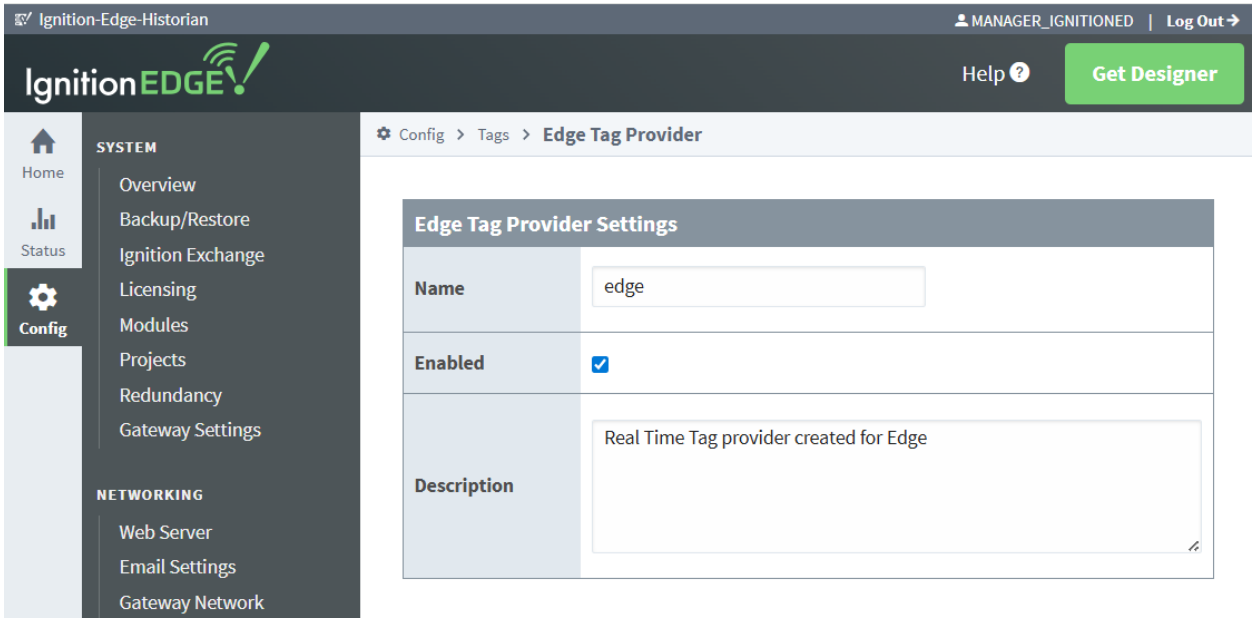
In the event the Local Gateway Server is down, the operational data and the historian data (up to the downtime of the Local Gateway Server) can be viewed in the redundant Web-Launched Client on the cloud.



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**

- Set the Edge Ignition Server to feed real-time tag data to Ignition gateways. One is called the local gateway, and the other is called the cloud gateway, hosted in Amazon AWS. The following edge gateway network setting shows that the outgoing connections are pointed to the local gateway server and the cloud gateway server to forward real-time tag data.

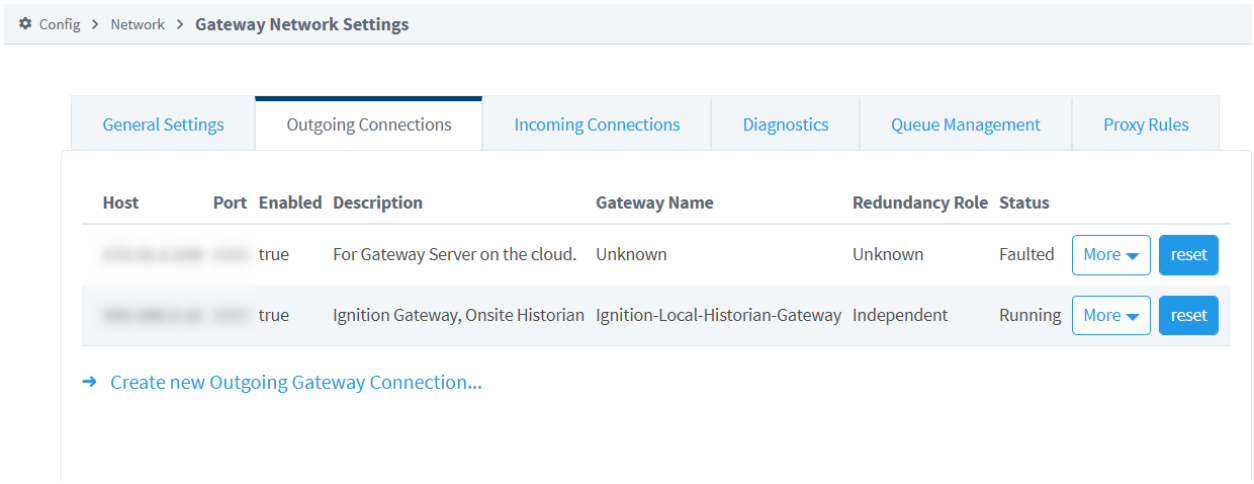


Figure 4-77: Ignition outgoing connections configuration

- Set up the local gateway and cloud gateway to receive real-time tag data from the Edge Gateway. The gateway network setting for the local gateway is shown below:

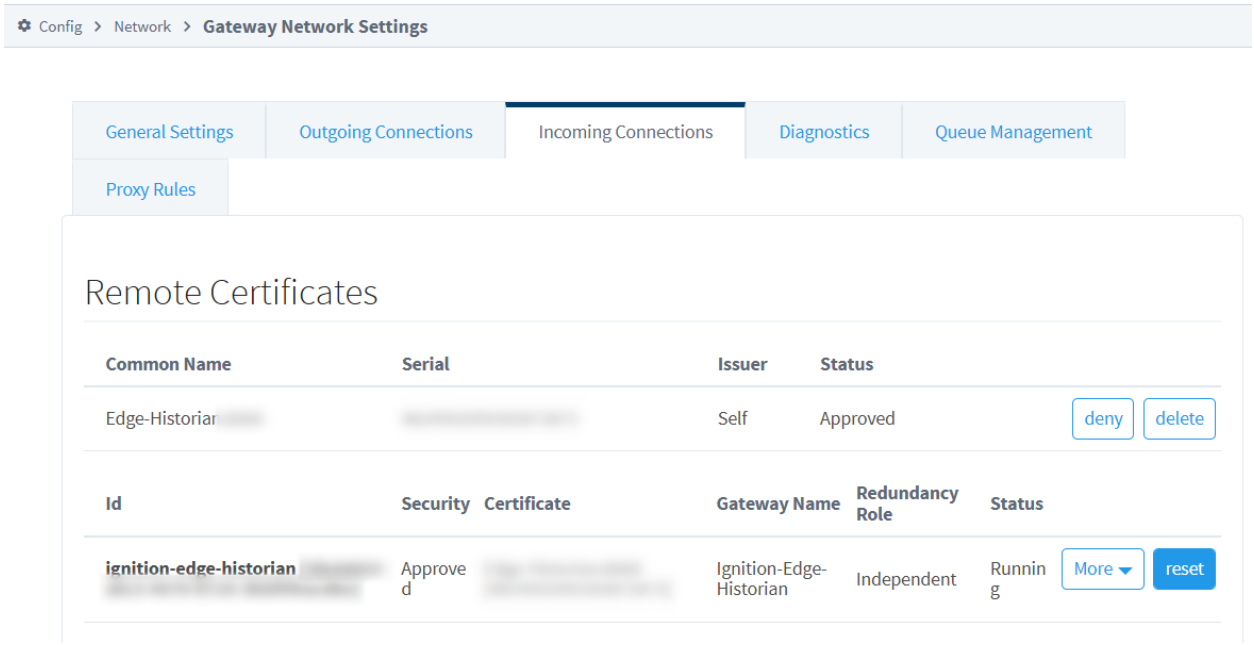


Figure 4-78: Ignition incoming connections configuration

- The local gateway Ignition instance is responsible for splitting the tag data for storing in different databases. The tag splitting setting is shown below. The Tag Provider called `TagSplitter` is configured to send tag data to two storage locations: `IGN_Hist_Onsite`,

which is the local Ignition database, and `IGN_Hist_OnCloud`, which is the AWS cloud Ignition database.

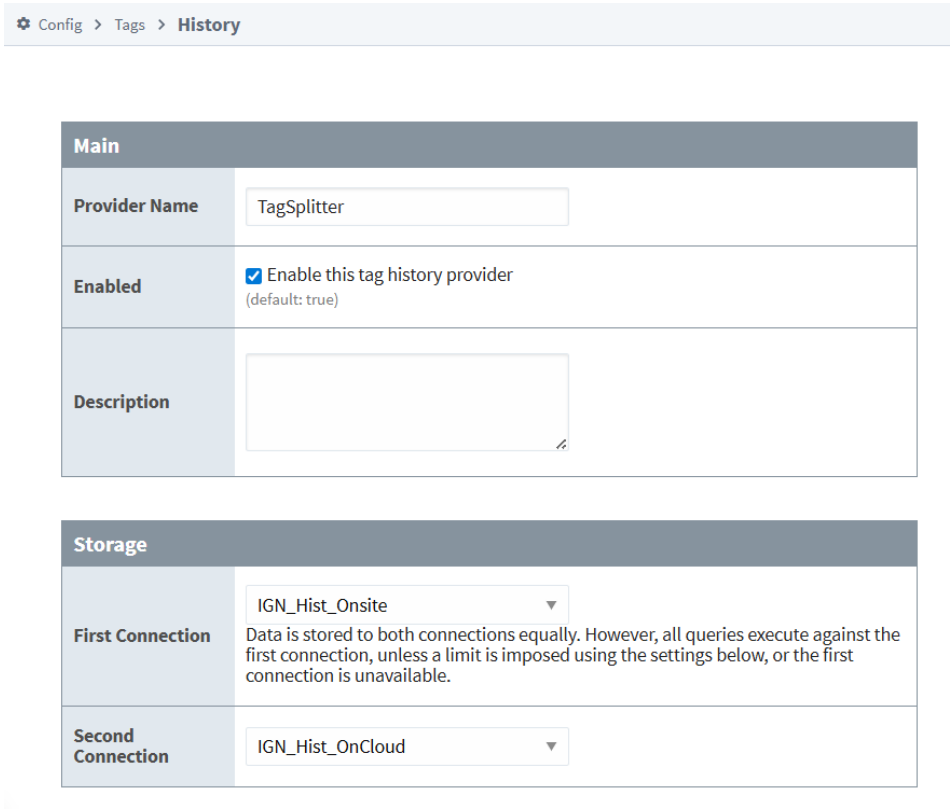
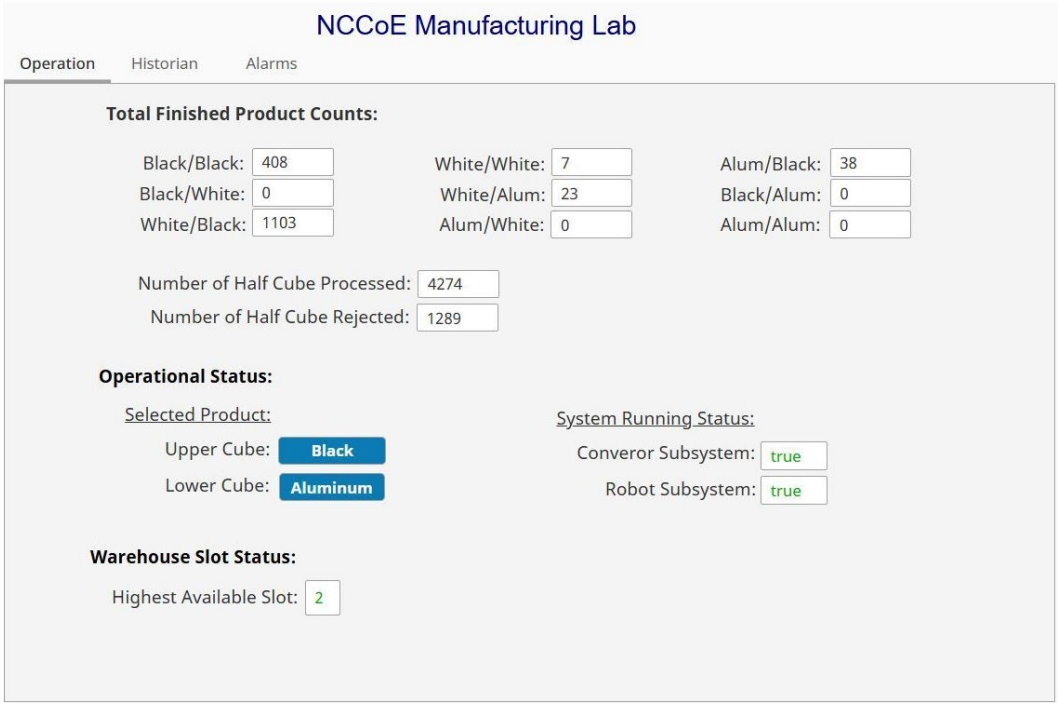
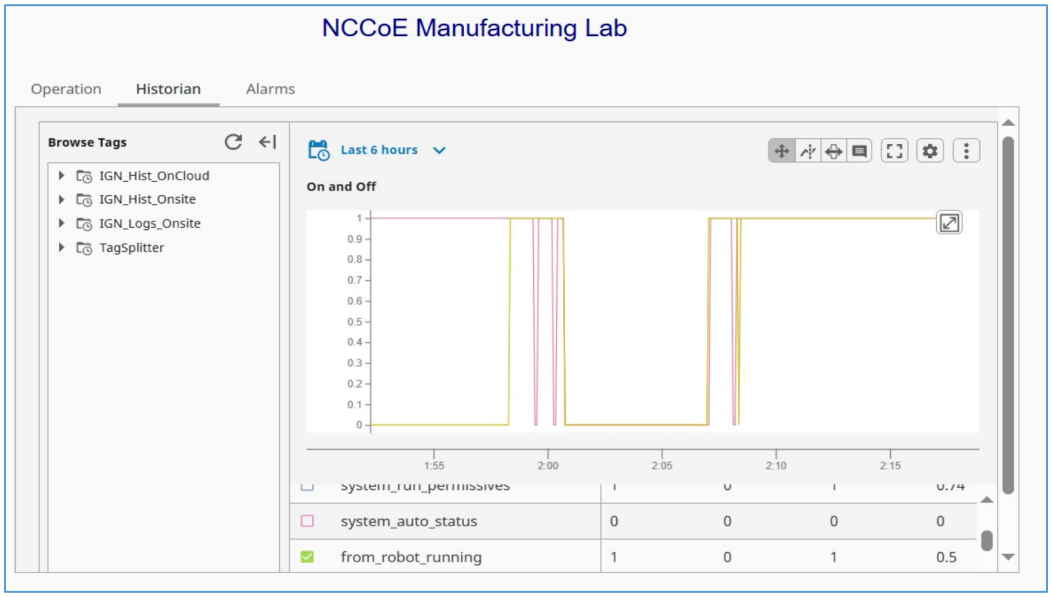


Figure 4-79: Tag Splitter history settings

- 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.

The baseline rule is created by navigating to the Baselines section within the Dragos navigation pane. From there, the option Create Baseline is selected. After creating a name for the baseline, as shown in Figure 4-82, scroll down and select Create New Filter. The filter can be customized as shown in Figure 4-83 and then saved.

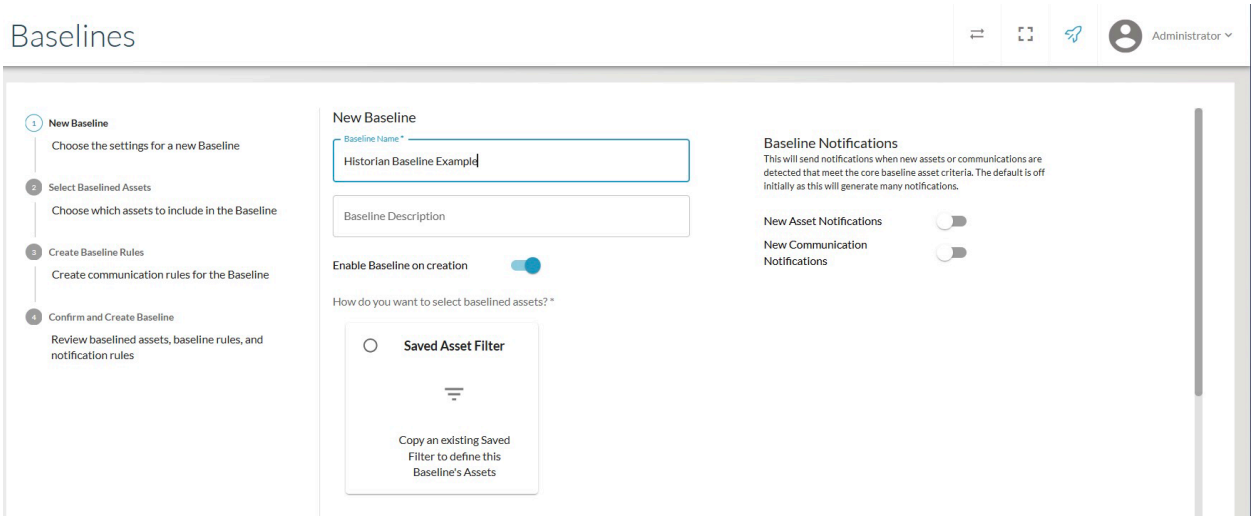


Figure 4-82: Creating a new Dragos baseline rule

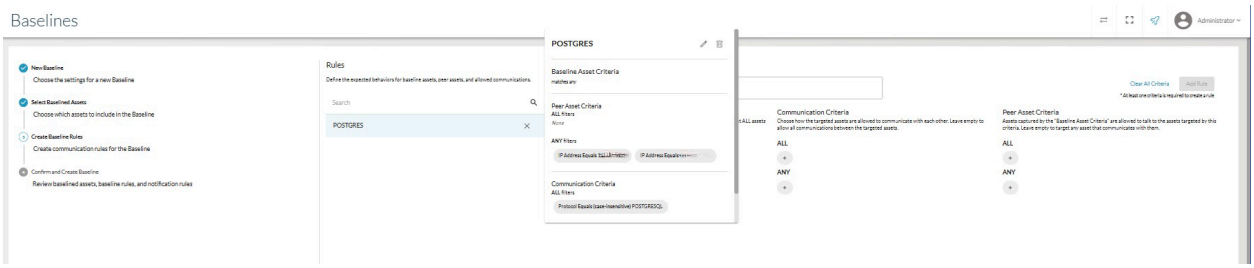


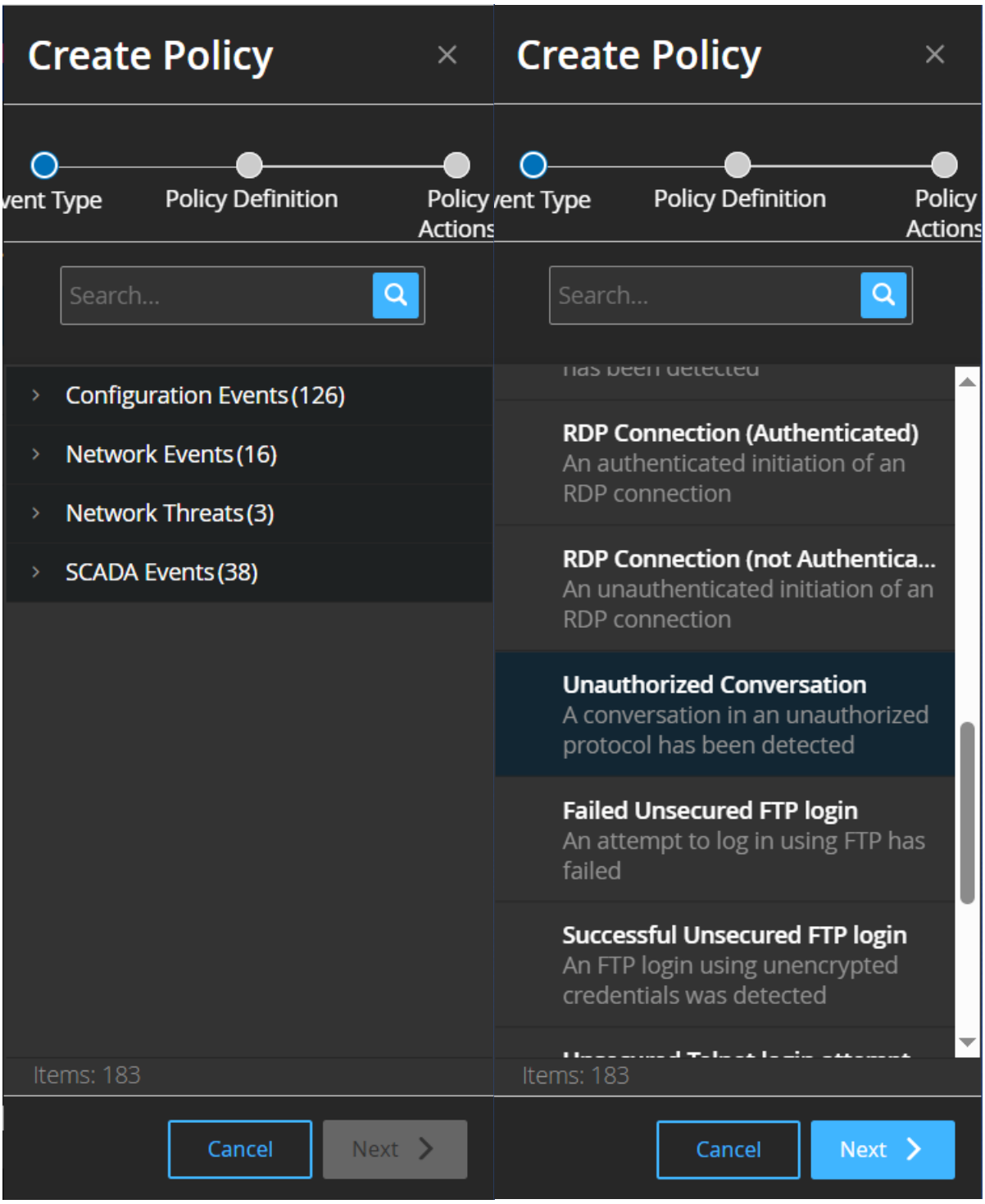
Figure 4-83: Create a custom criteria for the new rule

[Return to Scenario B]

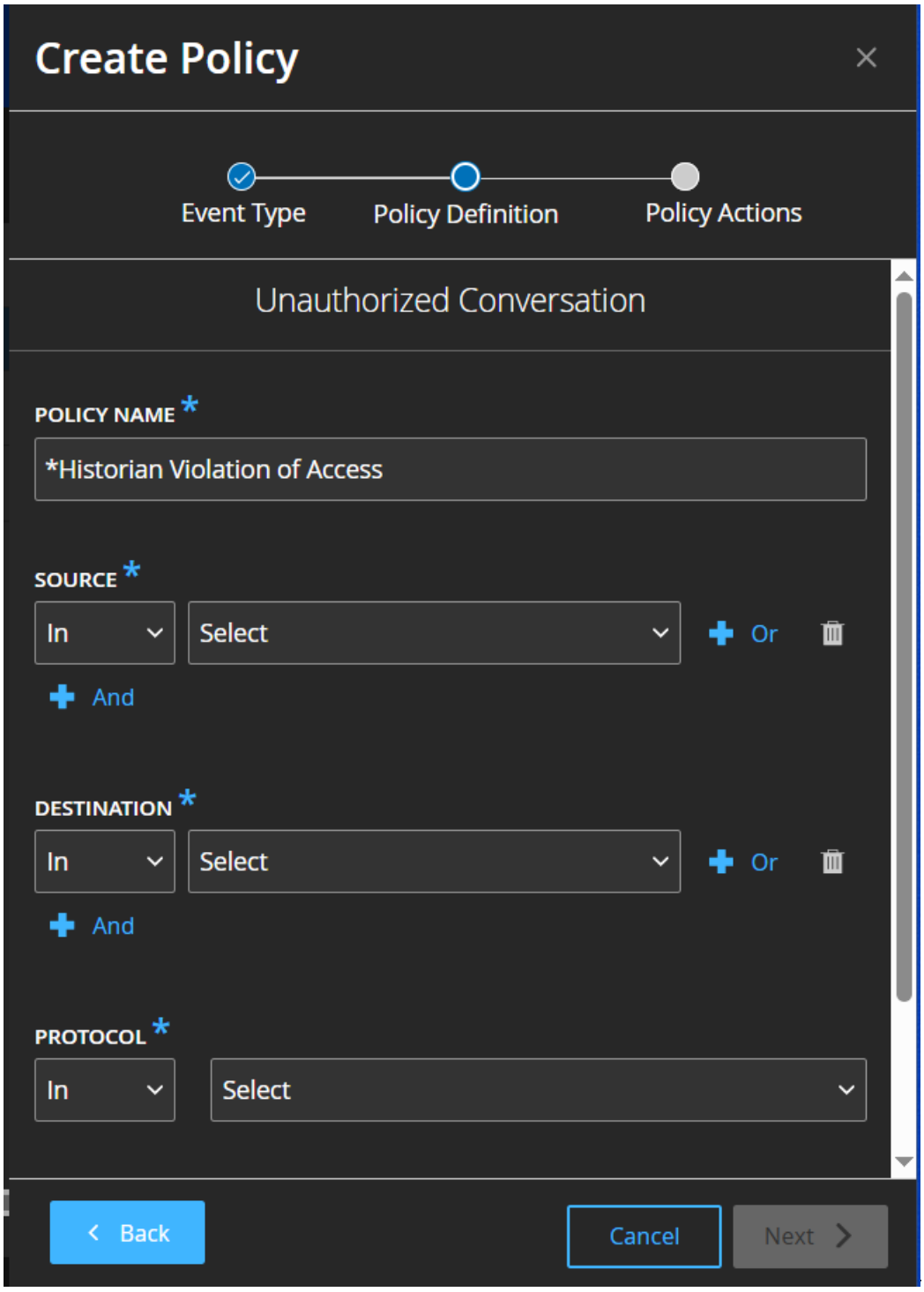
C.4.5 Creating a Baseline Policy in Tenable

A new baseline policy is created in Tenable OT Security, which alerts on any violations of the ruleset. The ruleset is configured to allow PostgreSQL between all devices expected to communicate with the local and cloud historian. Any violation of the baseline policy will generate an alert.

The baseline policy is created by navigating to the Policies section within the Tenable navigation pane. From there, the option Create Policy is selected. From there, Unauthorized Conversation is selected as shown in Figure 4-84. The rule criteria are entered as shown in Figure 4-85. Figure 4-108 provides a view of the baseline Policy alert within the Tenable OT Security platform.



1981 **Figure 4-84: Unauthorized Conversation policy creation in Tenable**



1982 **Figure 4-85: Unauthorized Conversation policy creation in Tenable**

1983 [Return to Scenario B]

C.4.6 Creating a Splunk Dashboard for SQL protocol Activity

This section discusses the steps of creating a dashboard to track PostgreSQL traffic using logs that are coming from both the Tenable and Dragos servers.

Once the detection of a deviation of the baseline has been established within Tenable and Dragos, both tools generate notifications that can then be forwarded to Splunk via syslog. Splunk does not natively contain a dissector for the logs from Dragos, so users can utilize the Field Extractor tool in Splunk to create a custom dissection of the log with the `Regular Expression` (Regex) option. Users can also install the Dragos plugin for Splunk. Logs coming from Tenable were properly dissected already.

Dragos

Looking at an initial search for Dragos logs, the dissector does not split the information from this log in a way that would be useful for a dashboard:

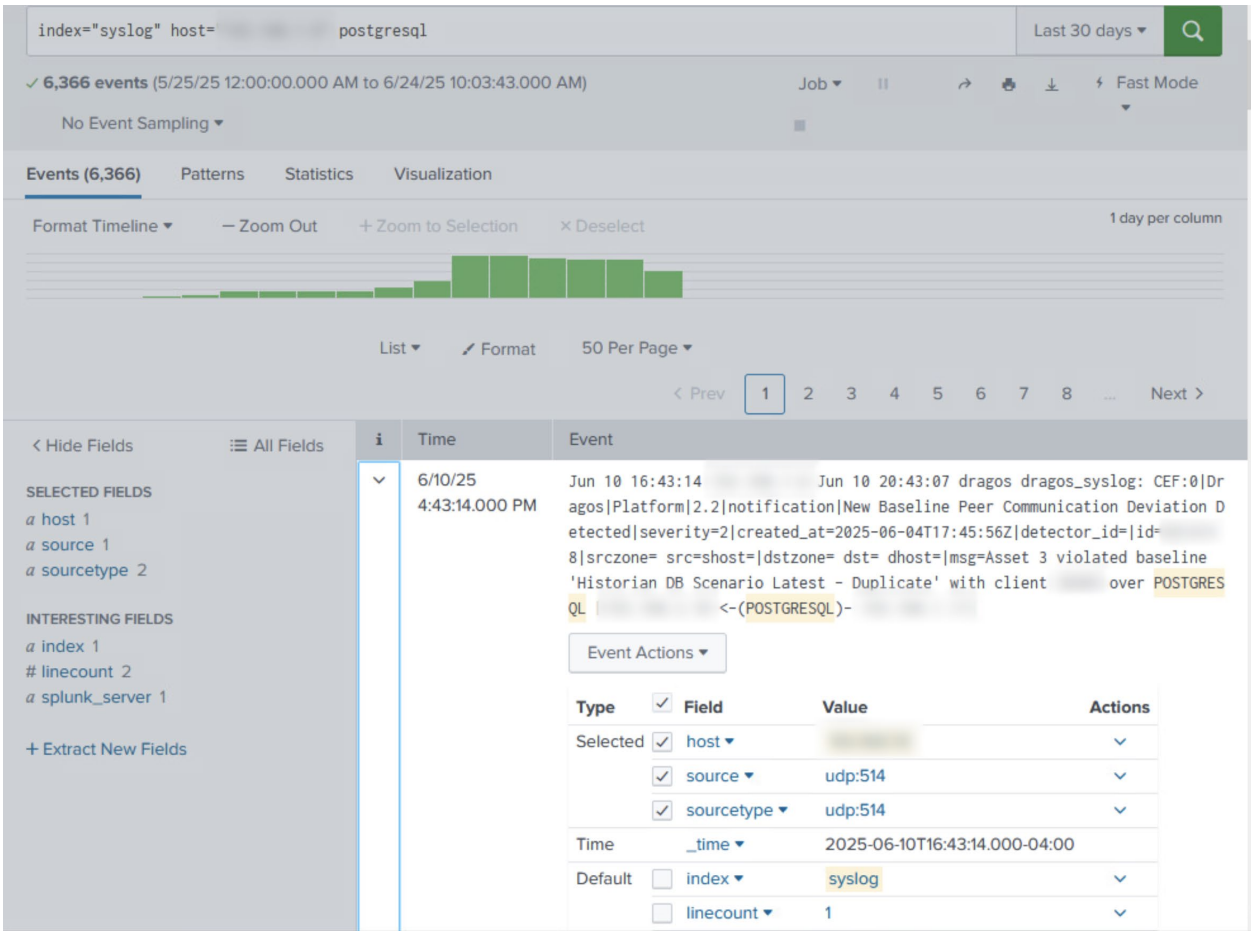
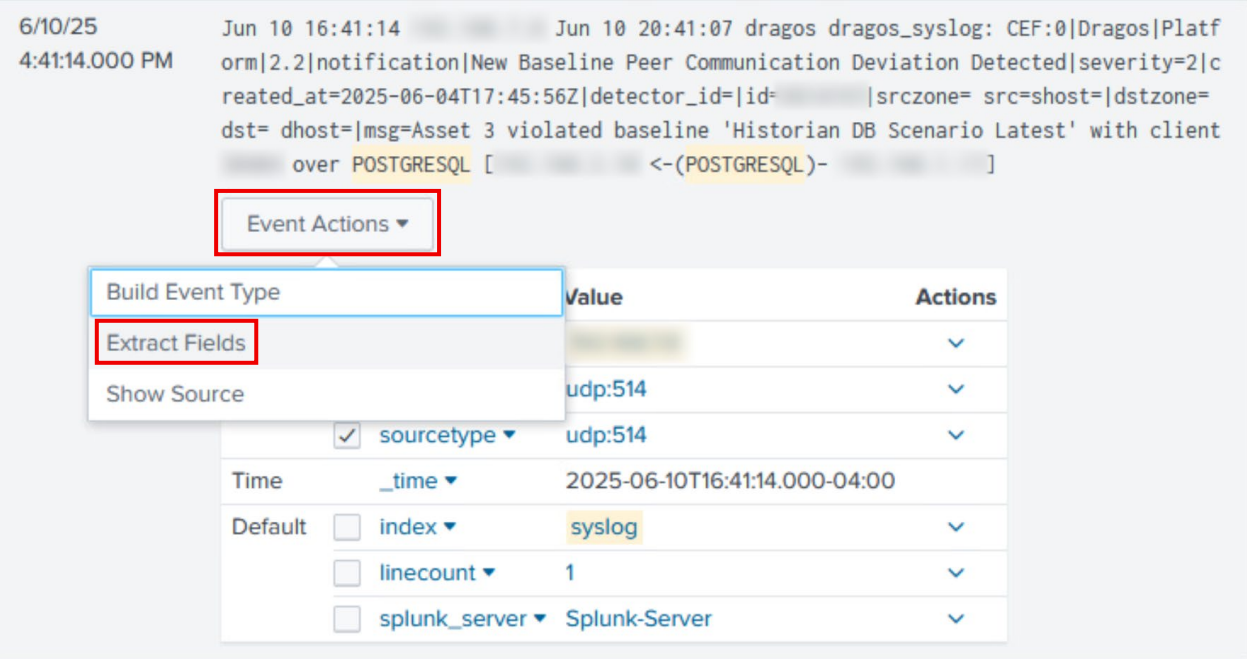


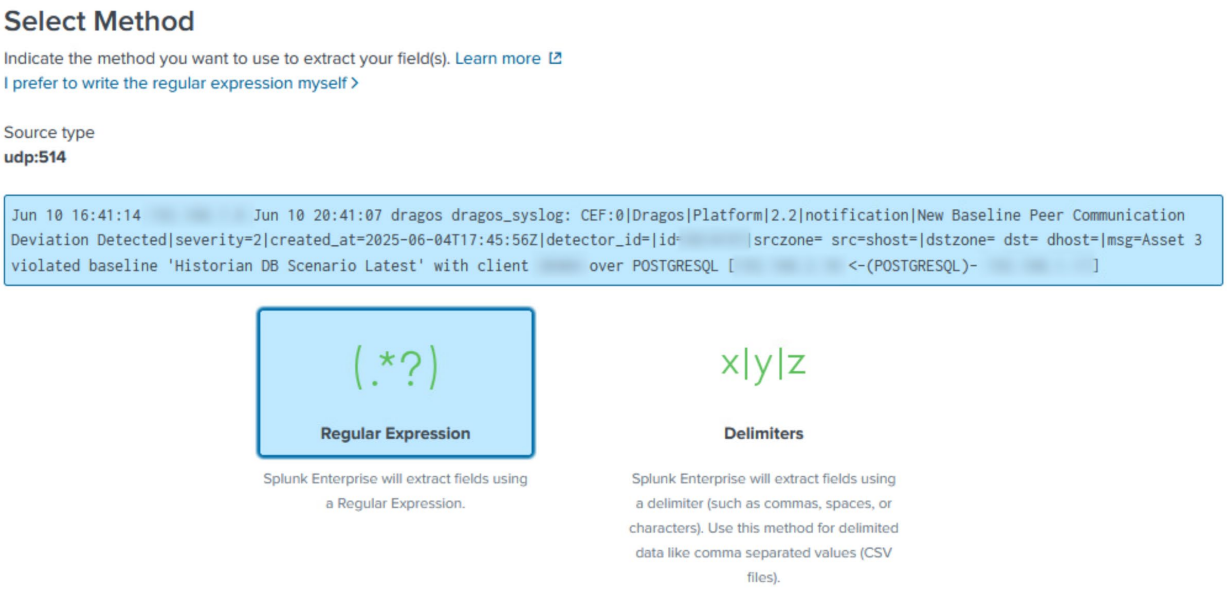
Figure 4-86: A Dragos log showing no dissected fields

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.

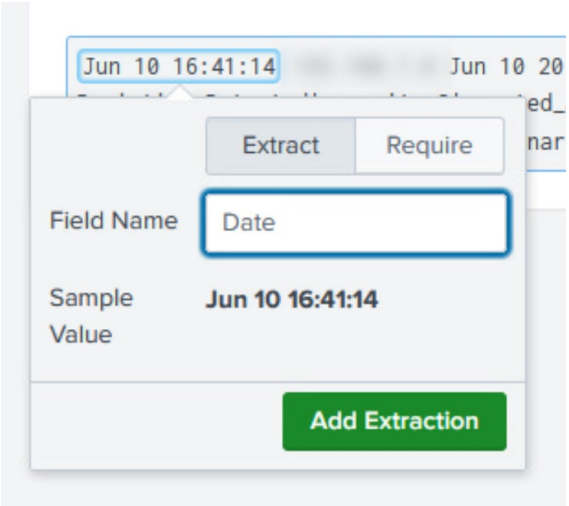


2004 **Figure 4-88: Choosing "Regular Expression" as the field extraction method**

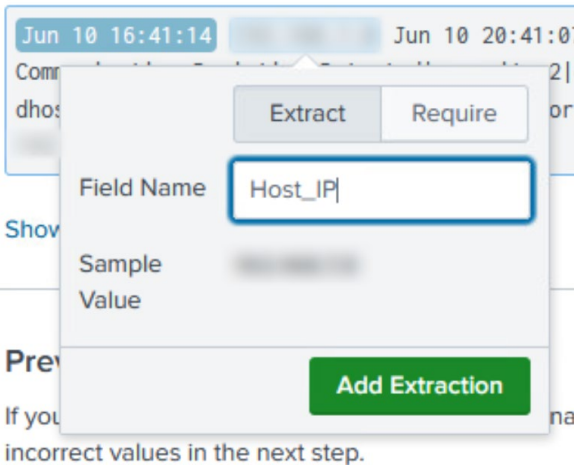
2005 Click `Next` at the top to move to the next section:

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"**

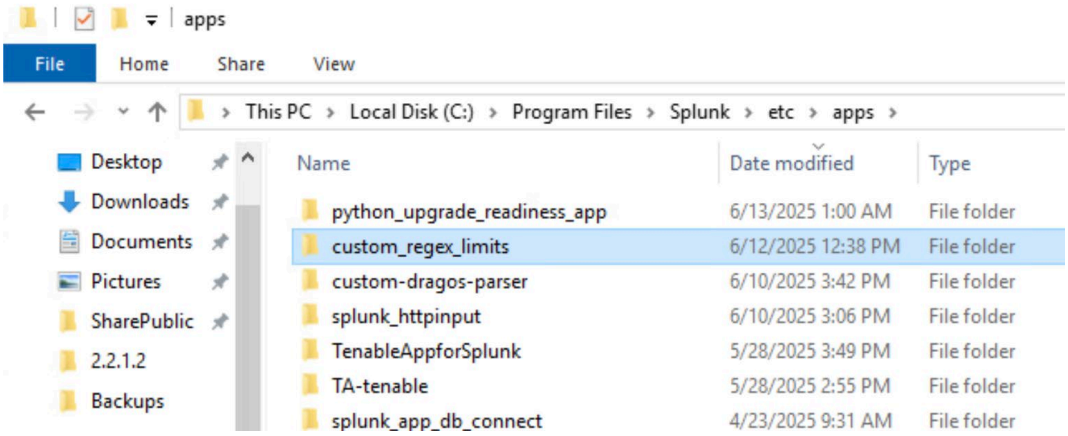


2010 **Figure 4-91: Selecting second custom line to extract as a field, labeled "Host_IP"**

2011 Once all the fields are selected, depending on how long the chosen fields are, this error could prevent
2012 continuation (highlighted in blue):

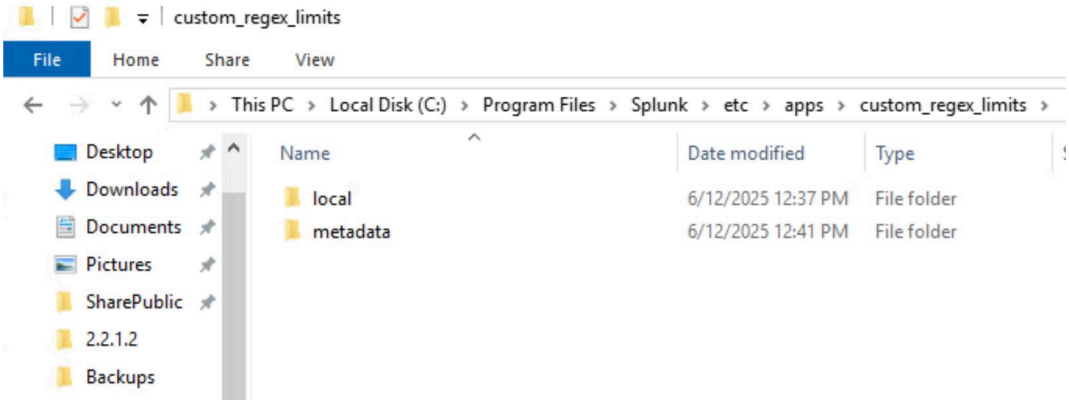
2013 **Figure 4-92: Potential error when selecting too many fields**

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`):



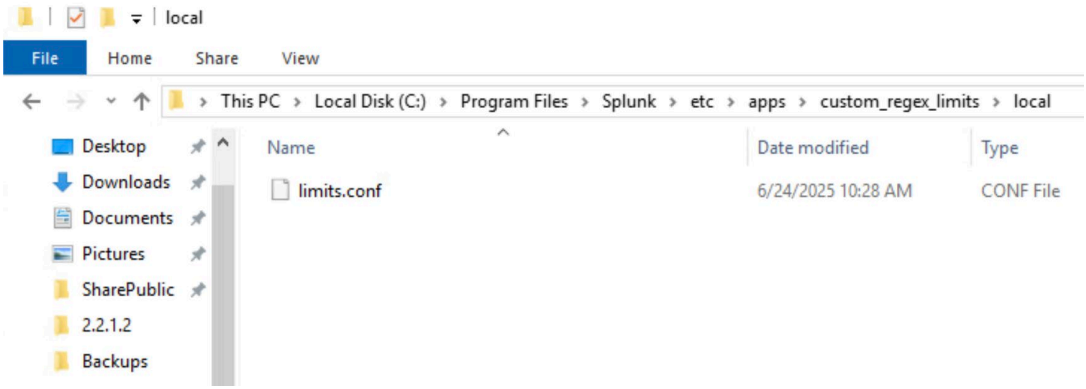
2021 **Figure 4-93: Location of directory to create custom applications in Splunk**

2022 Create two new folders within this new directory, name them `local` and `metadata`:

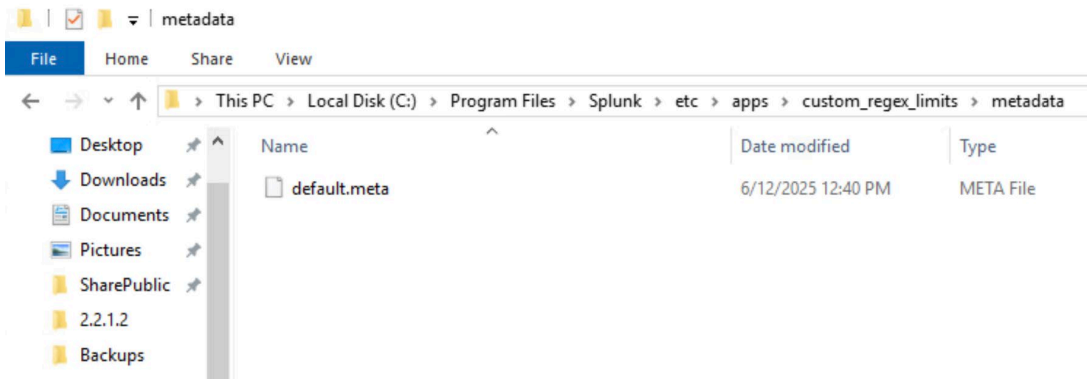


2023 **Figure 4-94: The directory of the custom app, two additional folders created for it**

2024 Within the `local` directory, create the file `limits.conf`, and within the `metadata` directory, create
2025 the `default.meta` file:

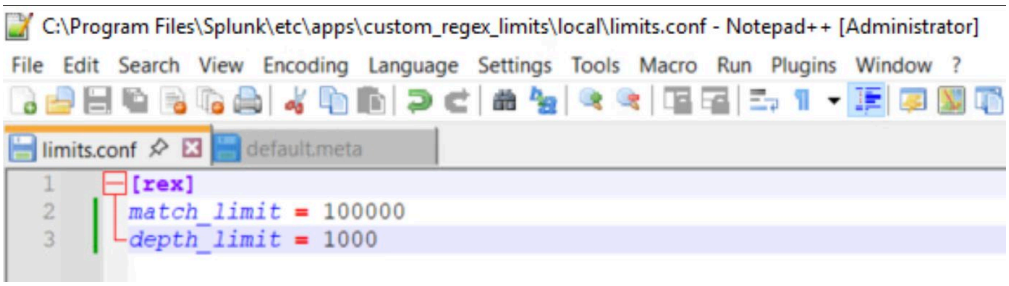


2026 **Figure 4-95: Location of main "limits.conf" file to edit for the custom application**



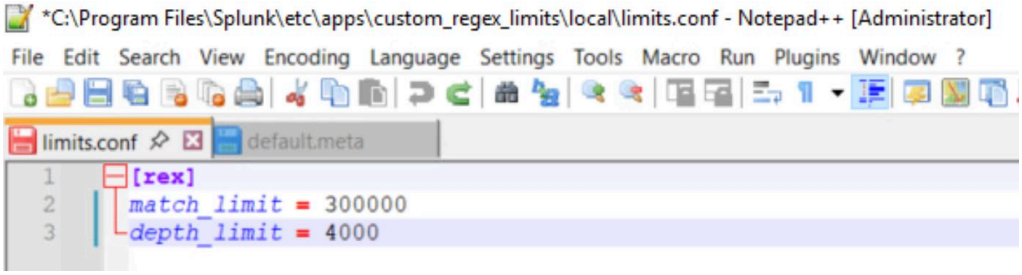
2027 **Figure 4-96: Location of "default.meta" file for the custom application**

2028 The default variable for Regex in the `limits.conf` system file is `rex`. The default values for `rex` are
2029 as shown:



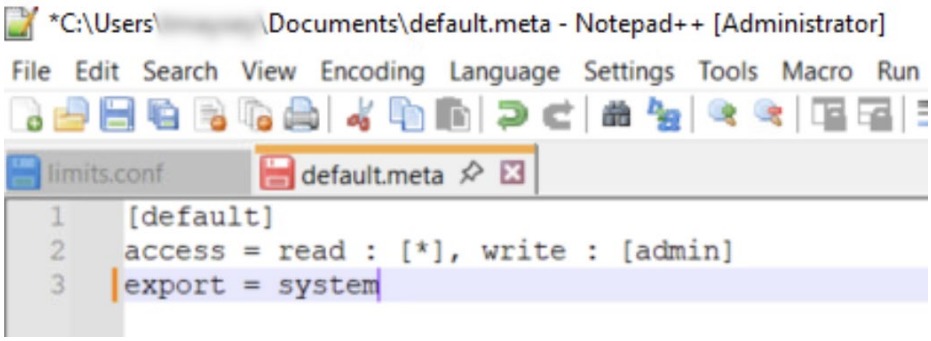
2030 **Figure 4-97: Default values of the "limits.conf" file**

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**

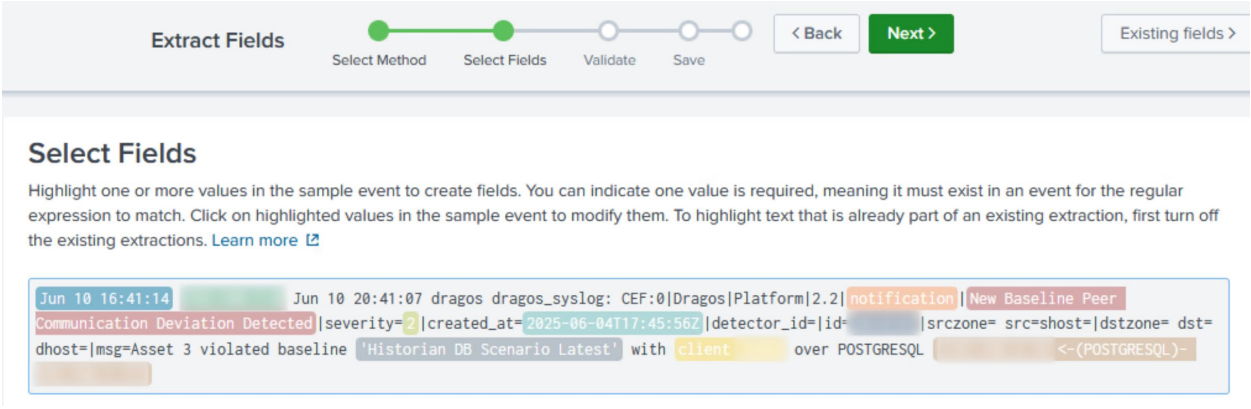
2034 Next, enter the following information into the `default.meta` file. This file defines the metadata for
2035 the app, such as the ownership, export settings, and most importantly, the access controls of the app. In
2036 the screenshot below, access is set so everyone can read the app, but only admins 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**

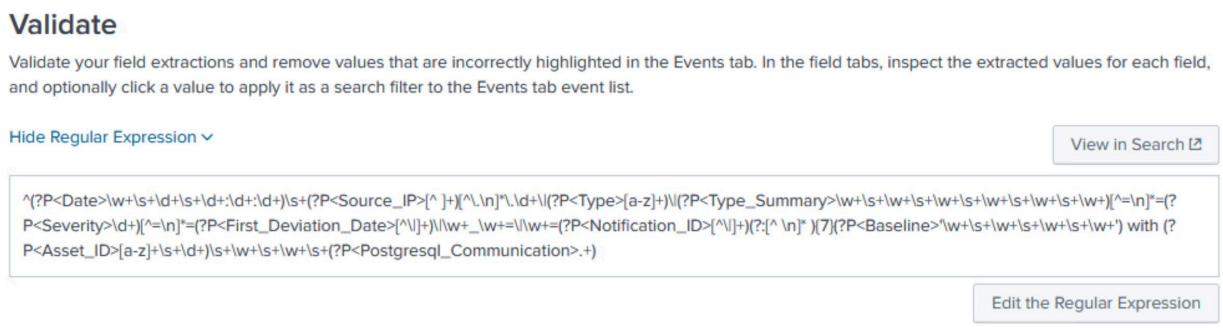
2040 Once this is complete, restart the Splunk service.

2041 When re-creating the field extraction, the error is no longer present:



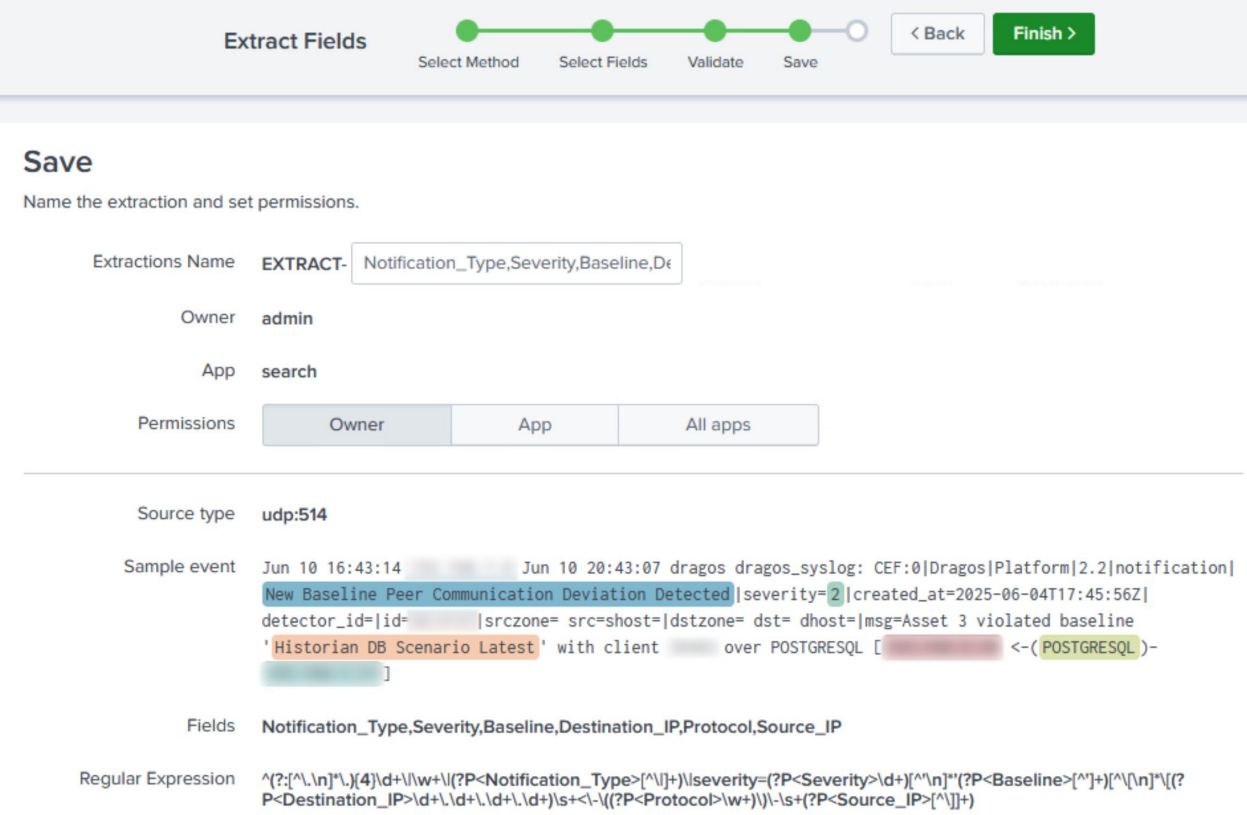
2042 **Figure 4-100: Same extracted fields as before, no more error after increasing Regex limit values**

2043 On the next page, validate the Regex that is produced from this process:



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:



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:

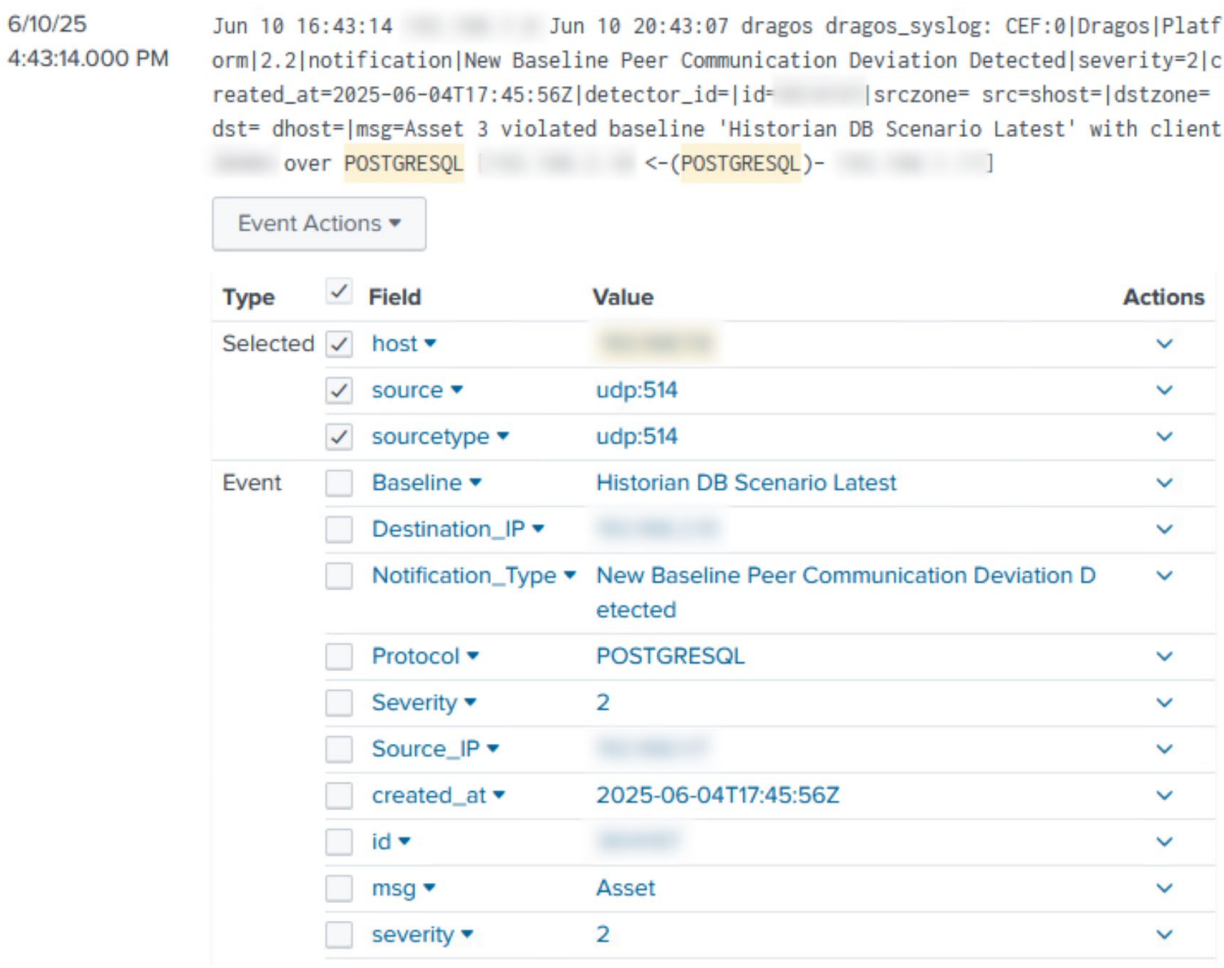
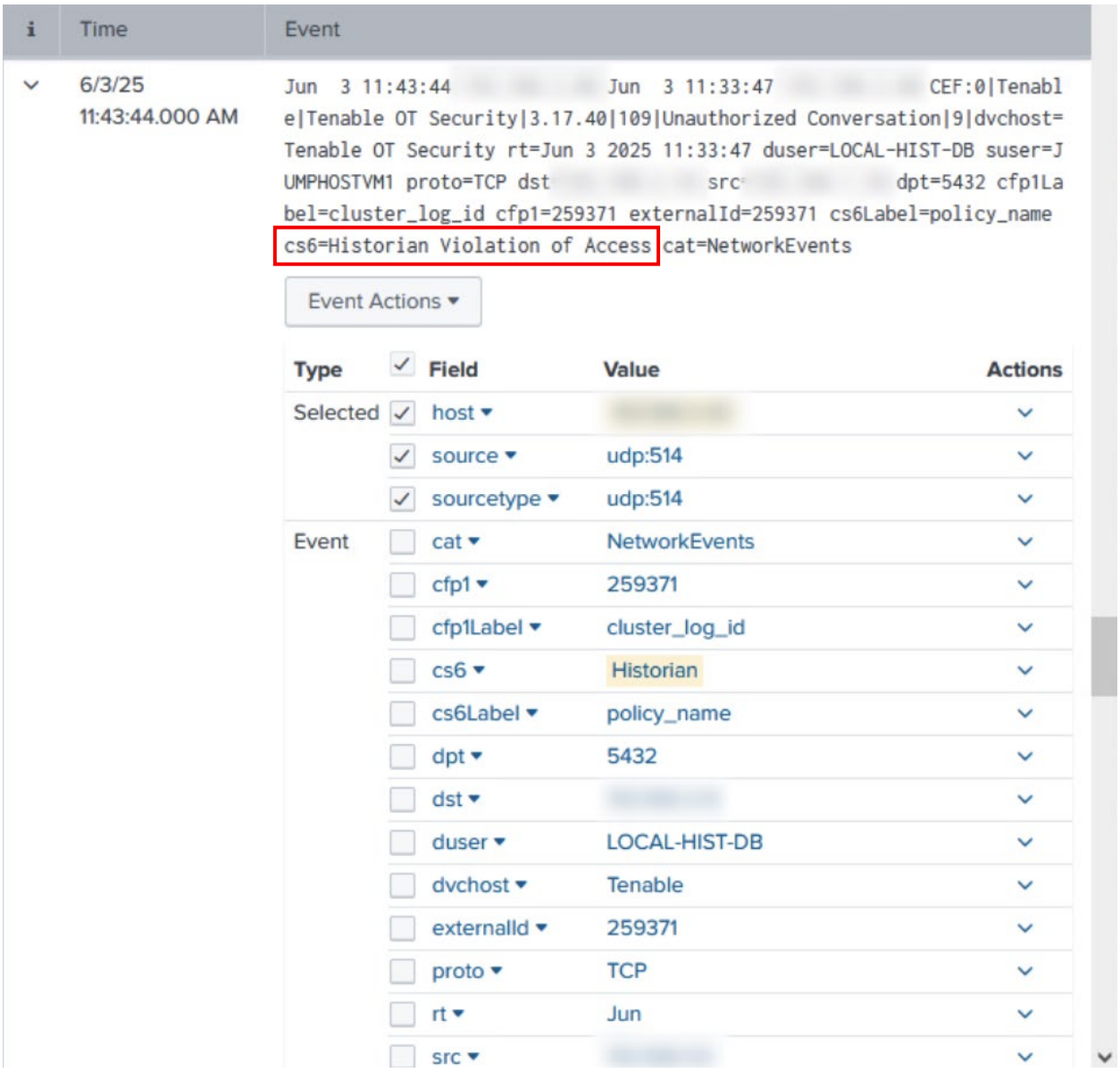


Figure 4-103: Dragos log now properly dissecting fields due to the Field Extractor tool

This whole process is just one method of dissecting this log. When creating a field extractor using regex, it hinges on the logs being the exact same every time, otherwise it will not dissect the logs the exact same way, if at all. In this instance, this method was useful because all the logs coming from Dragos for the PostgreSQL traffic baseline deviations all appeared in the same format. Dragos also has a plugin with Splunk that was not used for this demonstration.

Tenable

Splunk properly dissected the Tenable logs by default. The following screenshot is an example of a log showcasing a trigger of the “Historian Violation of Access” rule that was created in Tenable. Pay attention to the fields to see what has been extracted. An important element to note in the full log is highlighted by the red box:



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.

C.5 Scenario B: Technical Details – Response

C.5.1 Detection using Splunk Dashboard

The following dashboard, created in C.4.6, indicates unauthorized PostgreSQL traffic. It tracks the count of PostgreSQL traffic with the source and destination IP addresses, and PostgreSQL traffic in a time chart for both Dragos and Tenable. Both time charts are potentially helpful, quick visuals to see a spike in baseline deviations or policy violations:

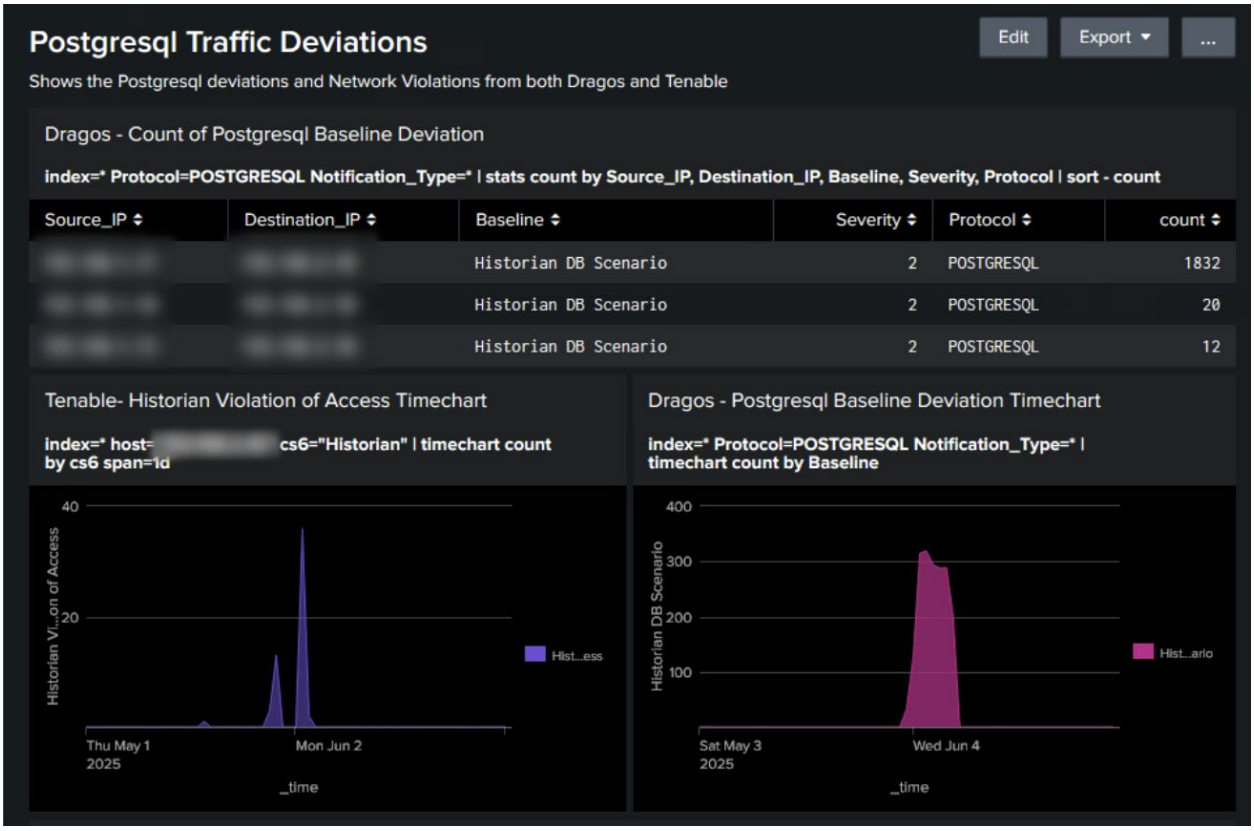


Figure 4-105: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs

Note: Observe the search fields used when creating the databases in the screenshot (e.g., "index=").*

To provide more in-depth detail, a panel was created in the dashboard to showcase a wide range of 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	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	2
2025-06-04T03:47:49Z	Historian DB Scenario	Dragos	[redacted]	[redacted]	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[redacted]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	[redacted]	[redacted]
2025-06-04 13:11:39	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 18:30:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 18:28:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 16:35:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 16:33:39	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 16:30:54	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 16:28:24	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 16:27:09	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]
2025-06-03 16:24:39	Historian Violation of Access	JUMPHOSTVM1	LOCAL-HIST-DB	[redacted]	[redacted]

« Prev 1 2 3 4 Next »

2081 **Figure 4-107: Dashboard created to track PostgreSQL traffic from Dragos and Tenable logs**

Unusual PostgreSQL traffic is being detected by both Dragos and Tenable. Utilizing Splunk dashboards, incident responders can get a quick look into the violations occurring within the traffic. These dashboards can be edited as users see fit. These are just a few examples of how users can set up their dashboards to detect any vital traffic leaving or entering the ICS network.

[Return to Scenario B]

C.5.2 Analyzing Tenable Alert

Because the factory's cyber team developed thorough baseline policies in Tenable, the system alerted when an unauthorized conversation occurred between the JumpHostVM and the local historian database. The Historian Violation of Access alert provides details on which machine was accessing the database using what port.

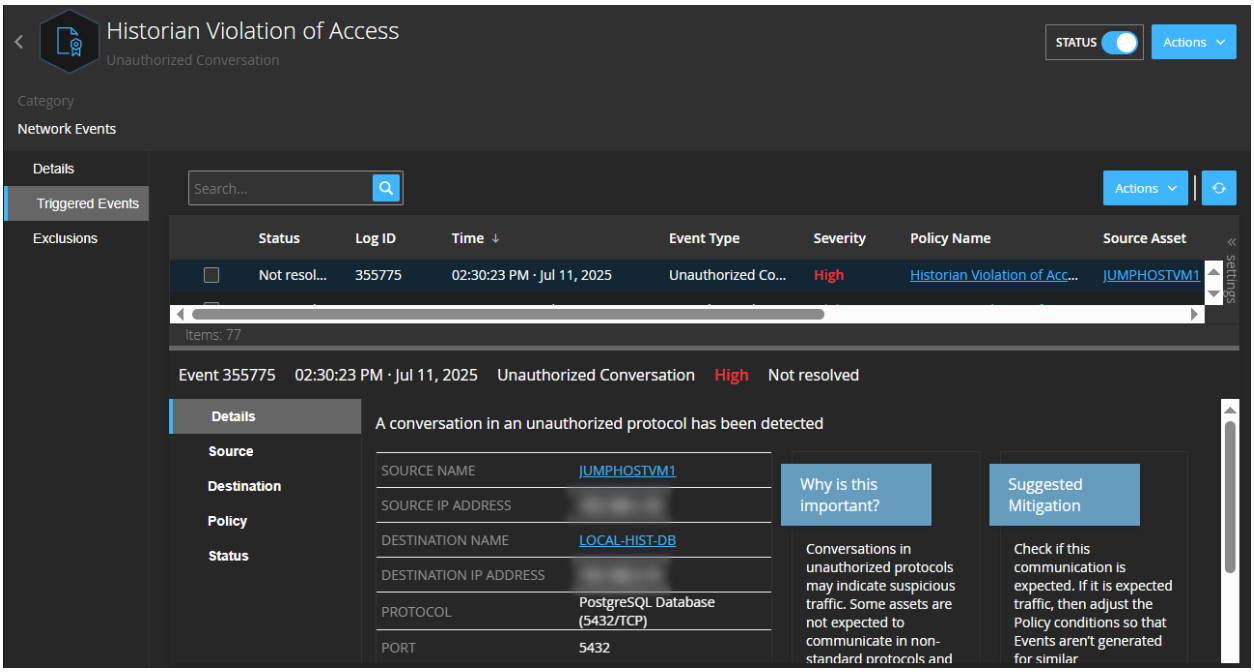


Figure 4-108: An alert generated in Tenable for a Historian Violation of Access policy

[Return to Scenario B]

C.5.3 Analyzing Dragos Deviation Alert

A notification appears in Dragos when a new asset communicates with the historian database, based on the Baseline created in section C.4.4. Details about the event can be investigated from the notification, and a case can be created from the notification.

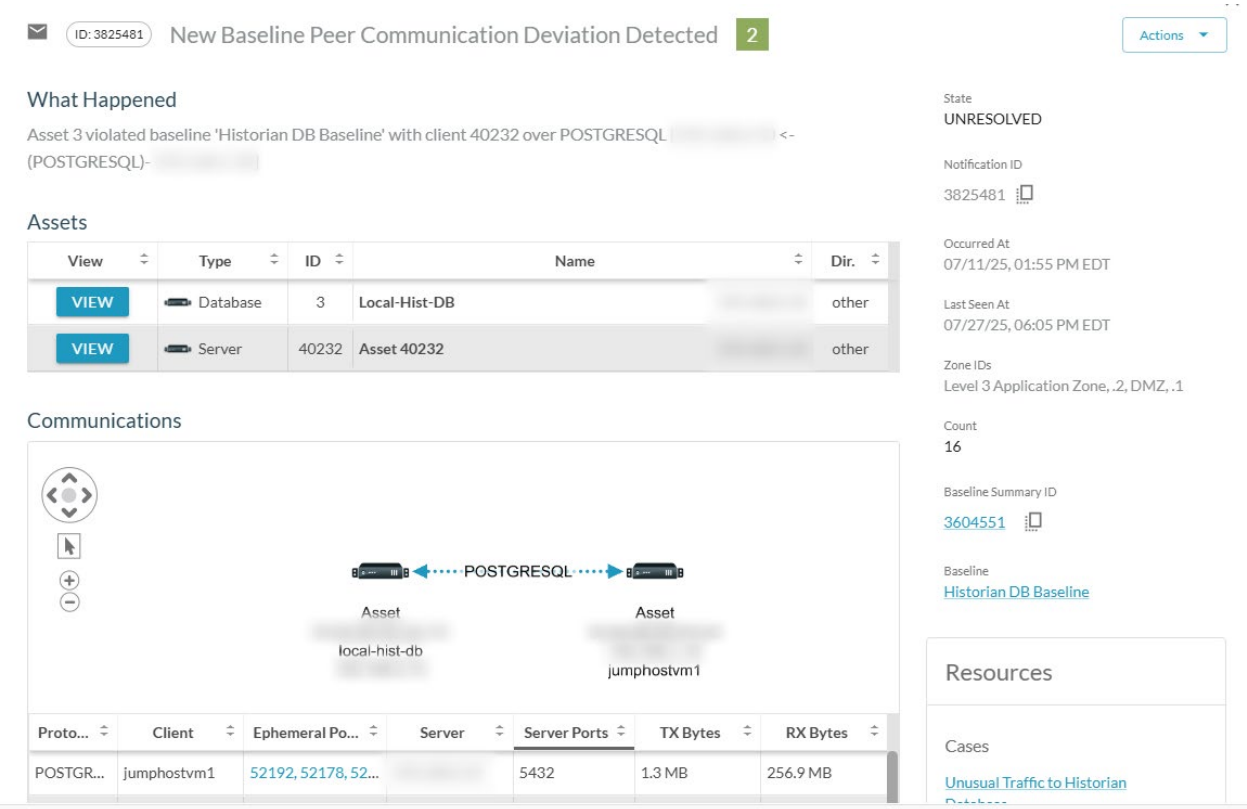
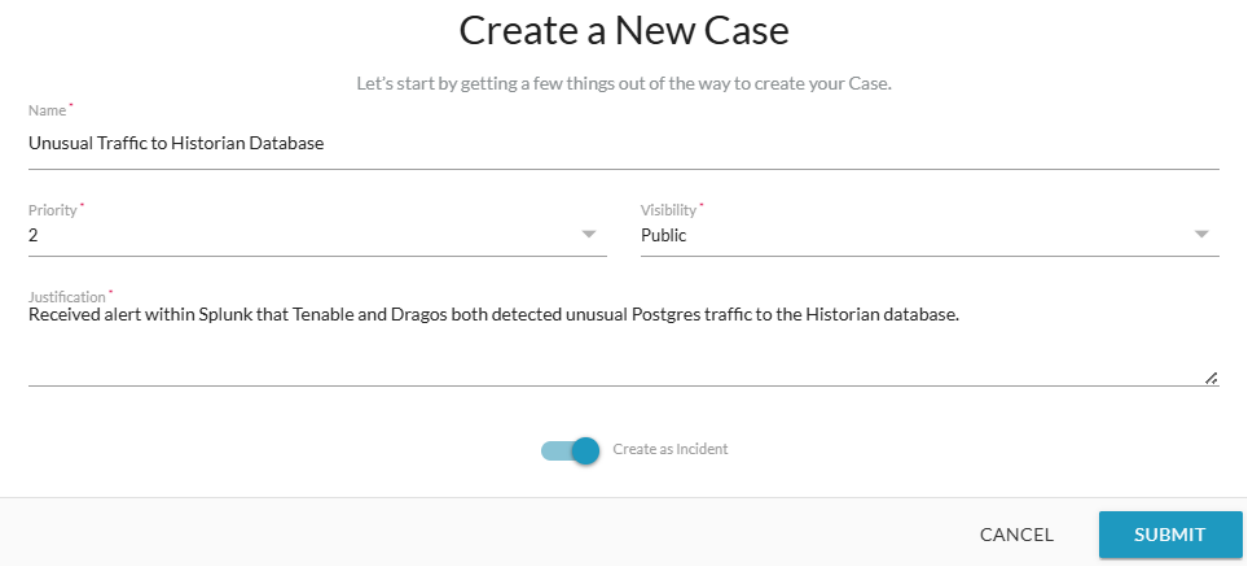


Figure 4-109: Dragos PostgreSQL Historian Baseline Deviation

[Return to Scenario B]

C.5.4 Dragos Case Management

After the SOC team determined that a data exfiltration incident had occurred, an incident case was created using the Dragos SiteStore Platform (Version 2.4.2) Case Management tool to streamline the incident investigation and support cross-team coordination. Analysts should include their hypothesis description about the incident, priority setting, and assignment notification in the case. During the investigation, the case was updated with further evidence collected from the investigation. Once the investigation is done and response actions are taken, the case can be closed for further record. Below is the screenshot for the case created for the Scenario B incident. Priority 2 was given to the ticket based on initial indications from Dragos and Tenable.



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.

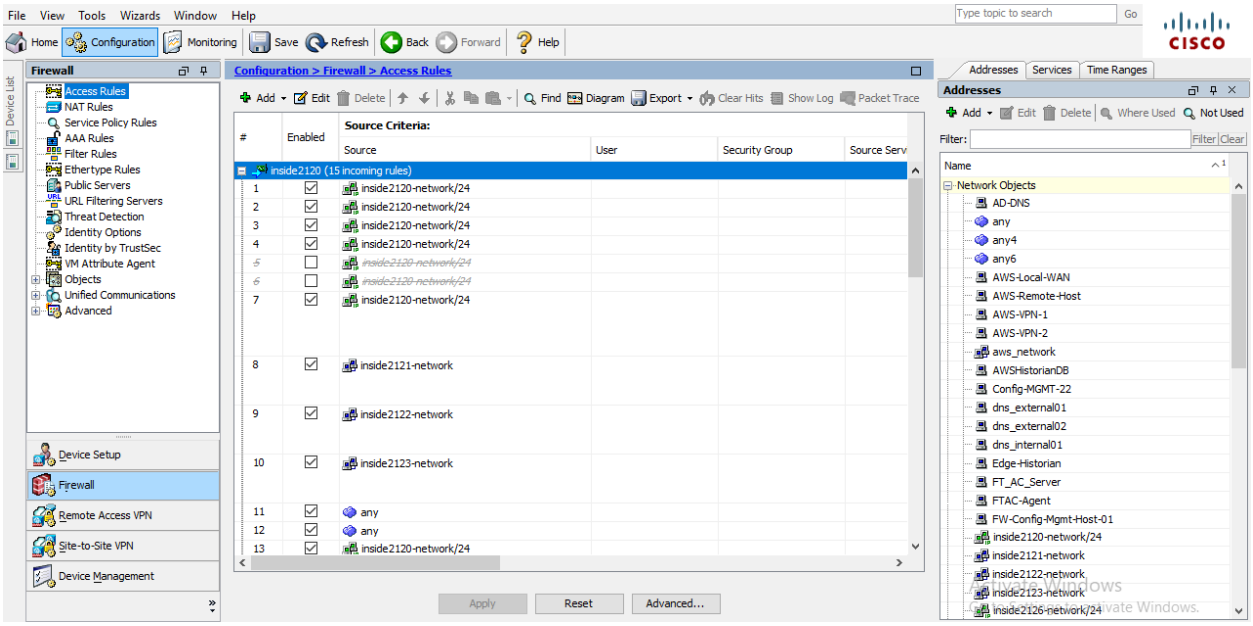
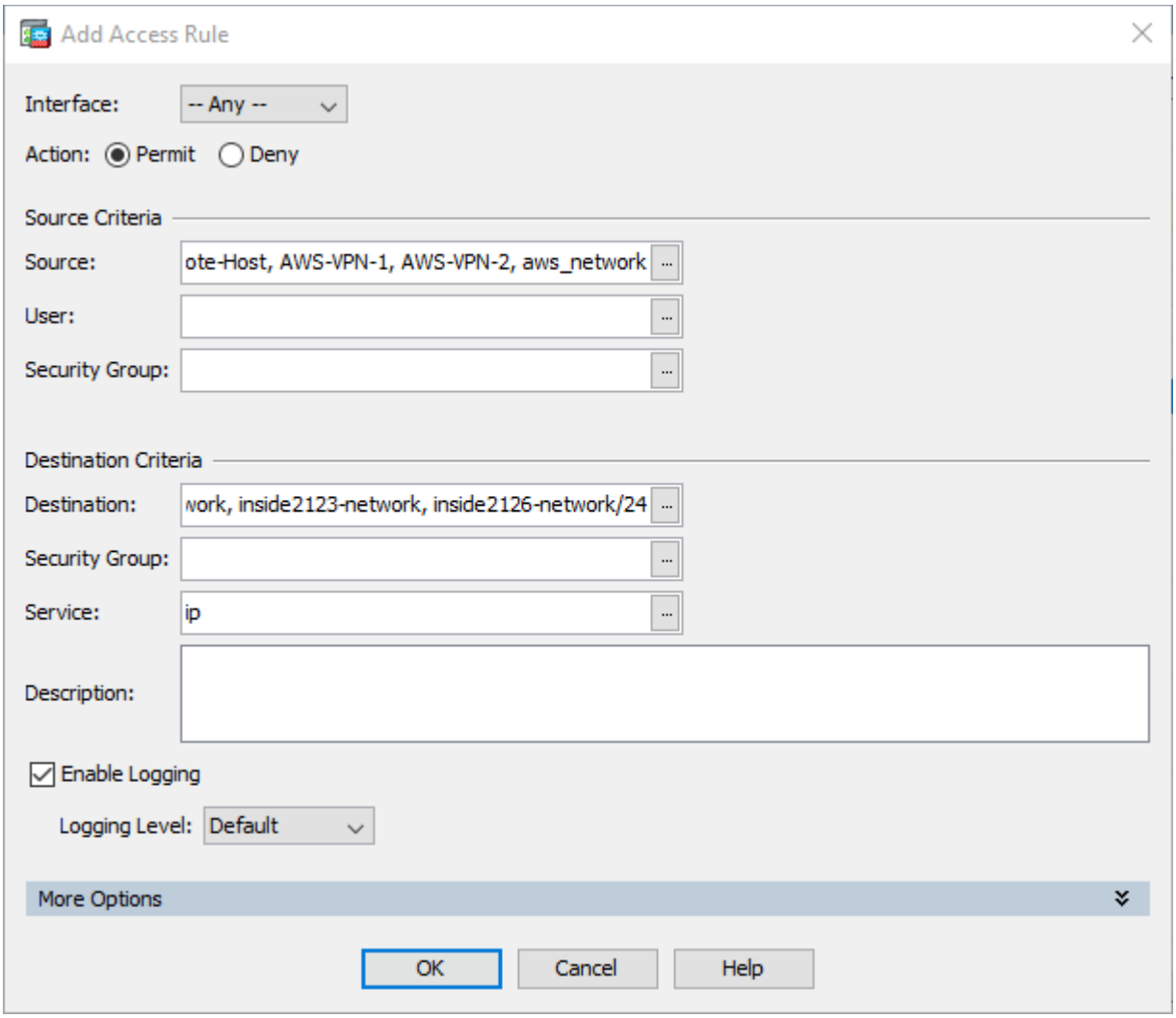


Figure 4-111: Cisco firewall configuration

The following Figure 4-112 and Figure 4-113 show the creation of new rules. Rules are created to ensure access is allowed from the ICS network to AWS and from AWS to the ICS network. Also, a block all rule is created to block all external traffic to internal traffic and vice versa. Placing the block rule after the previous allow rule ensures all traffic is blocked, but communication is still allowed to flow over the site-to-site VPN to AWS networks.



2125 **Figure 4-112: Permit rule for AWS gateway and hosts**

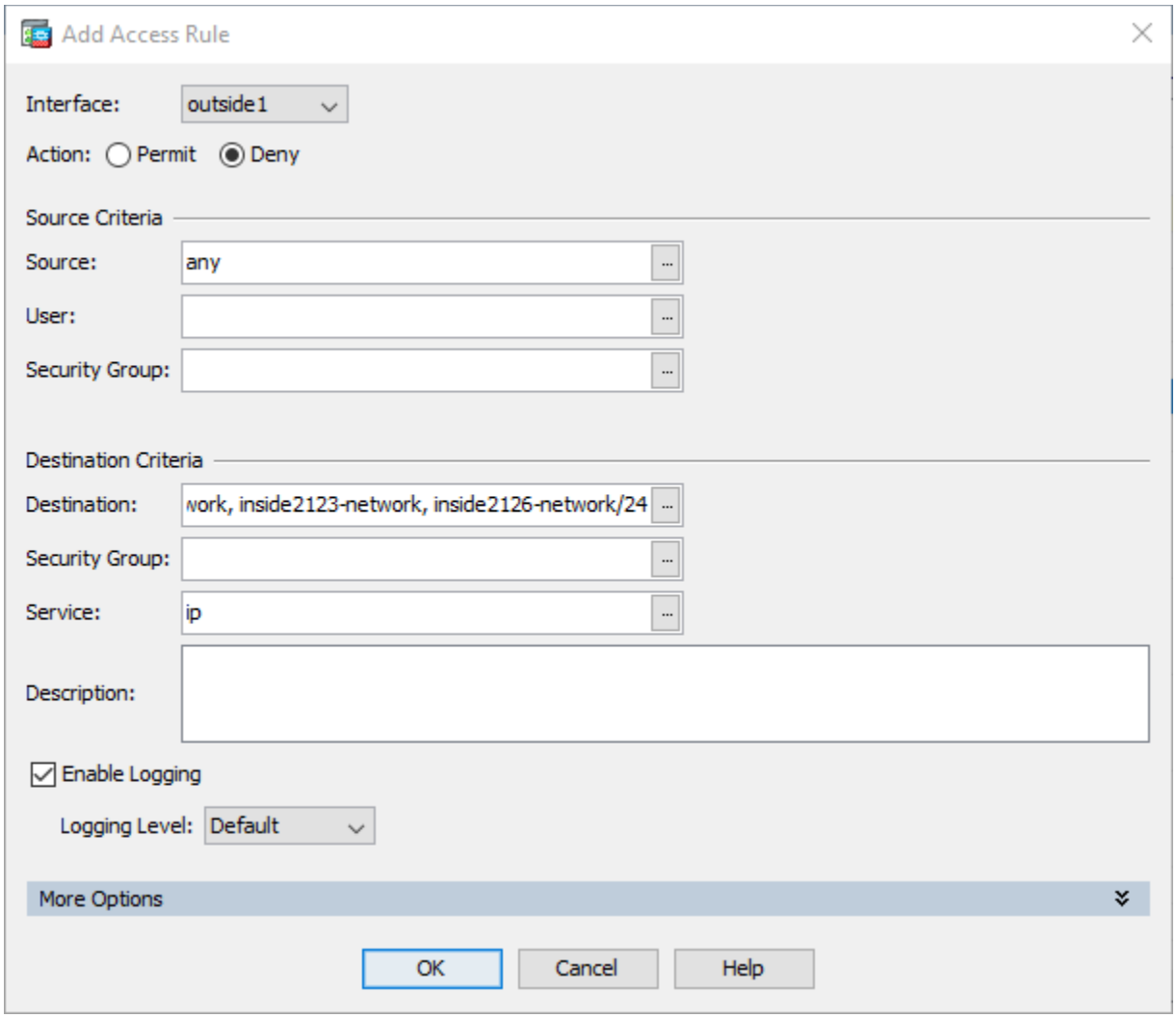


Figure 4-113: Block rule for the ICS network

[Return to Scenario B]

C.5.6 Disconnect JumpHost VM from Network

Refer to section C.2.8 in scenario A on how to remove a VM from the network in vSphere. In this step, be sure to select the correct VM.

[Return to Scenario B]

C.5.7 Take Snapshot of JumpHost VM

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 to select the correct VM. A snapshot of the VM is taken for forensics purposes.

[Return to Scenario B]

C.5.8 Isolate Local Database and Historian Gateway

The local historian gateway and database are isolated from the network as part of the containment step of incident response. Since both the local gateway server and the database server are virtual machines, they can be disconnected using the VMware vSphere client. The process to disconnect the Network Connection for a Virtual machine is shown below:

Log in to the VMware vSphere Client. Once logged in, locate the suspect server (Local-Hist-DB) in the vSphere Client.

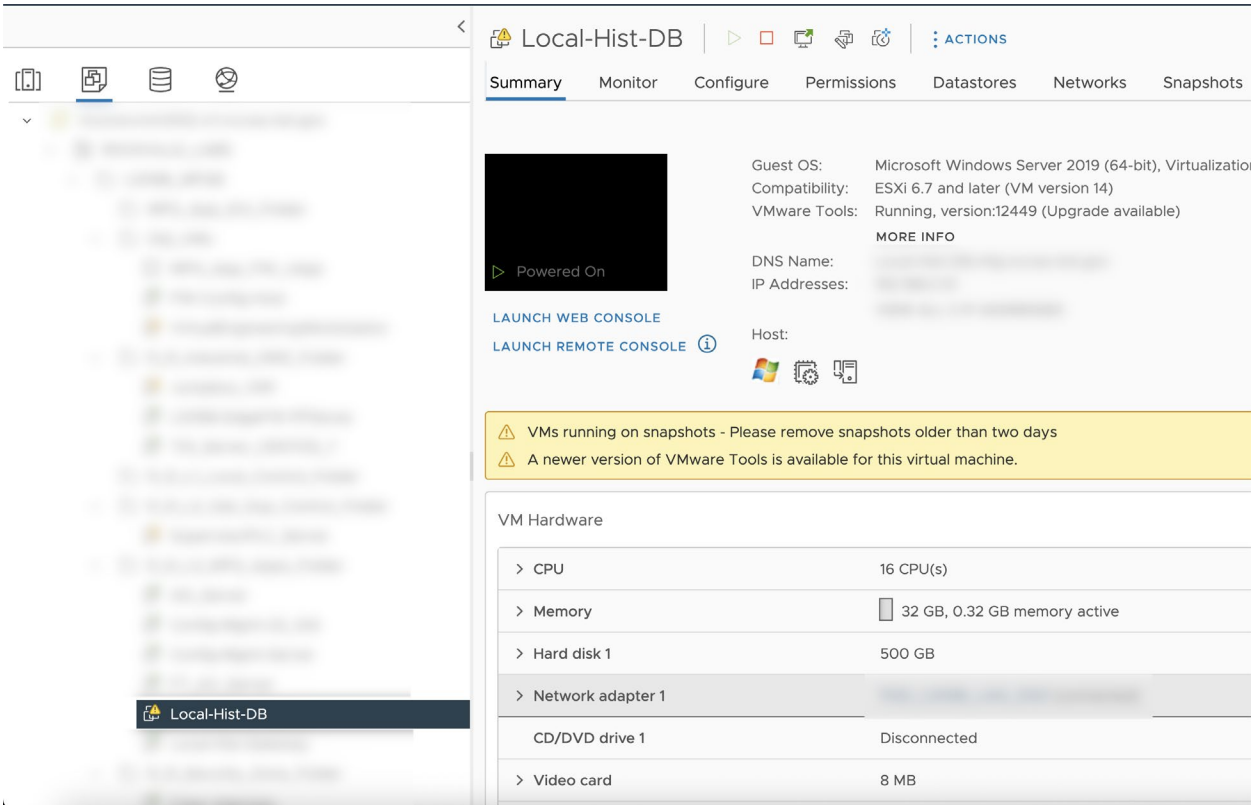
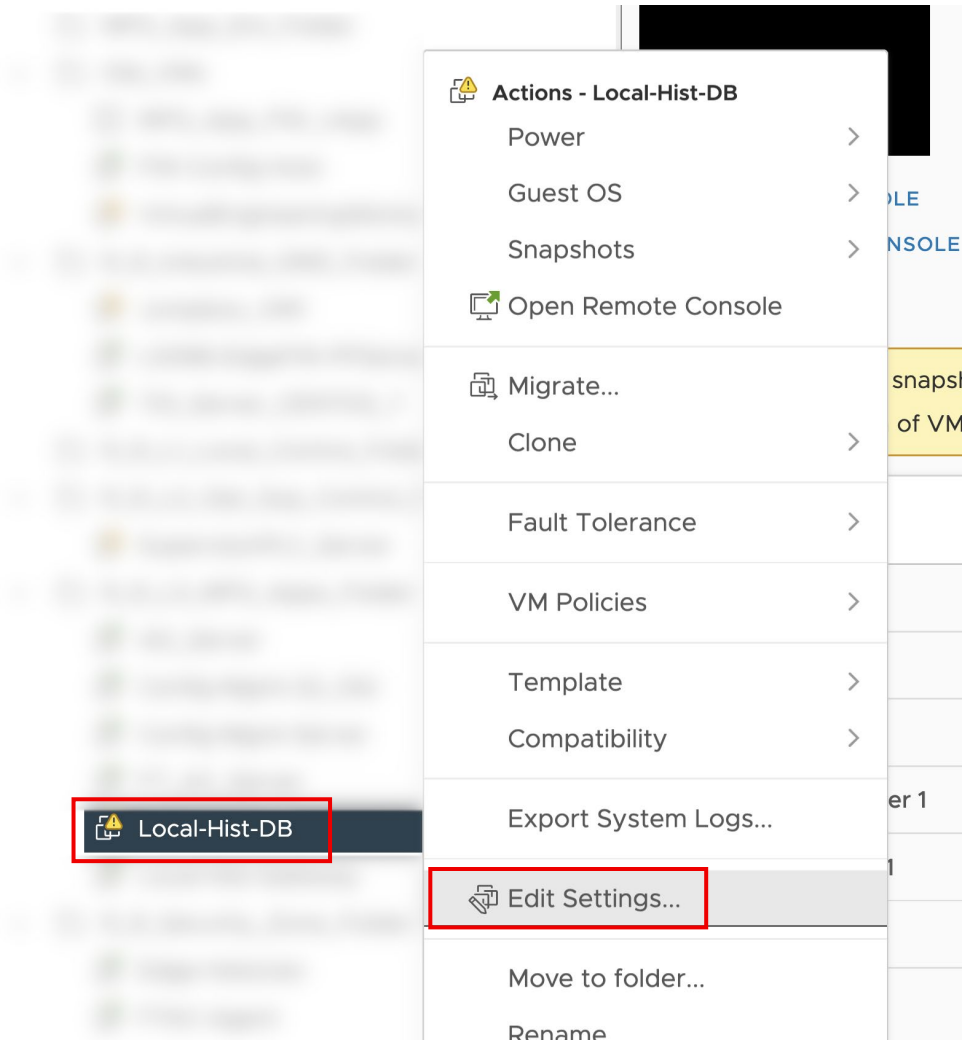
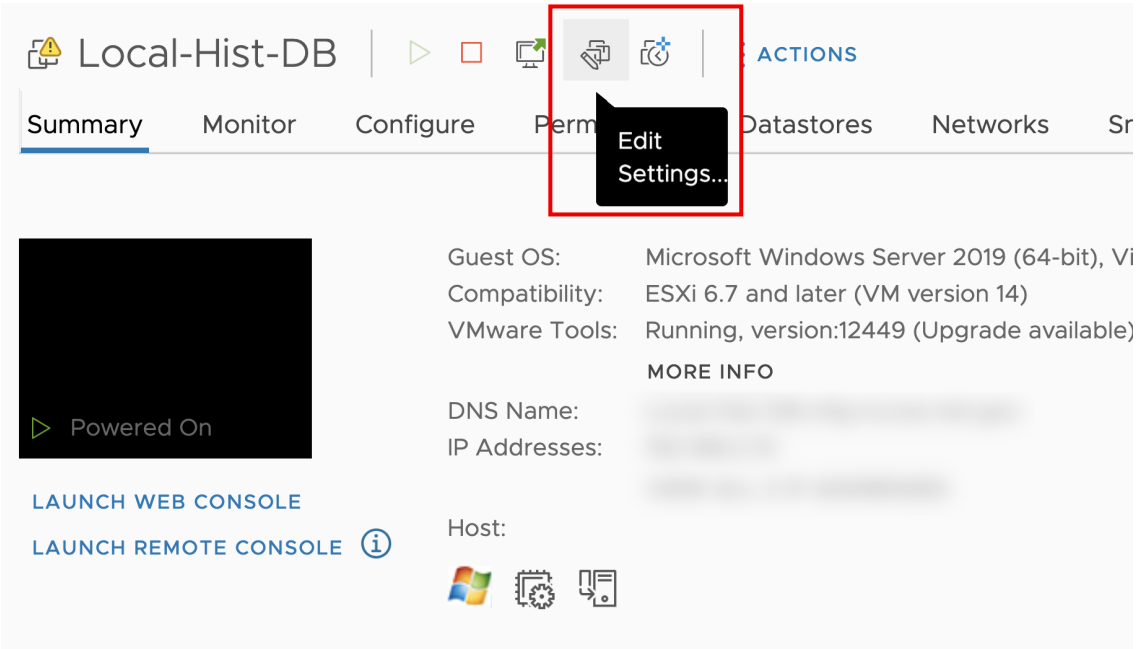


Figure 4-114: Select the local historian database server in vCenter

Edit the settings on the VM. There are a few methods: right-click on the selected server and select `Edit Settings`, or click on the Edit Settings button on the summary page.

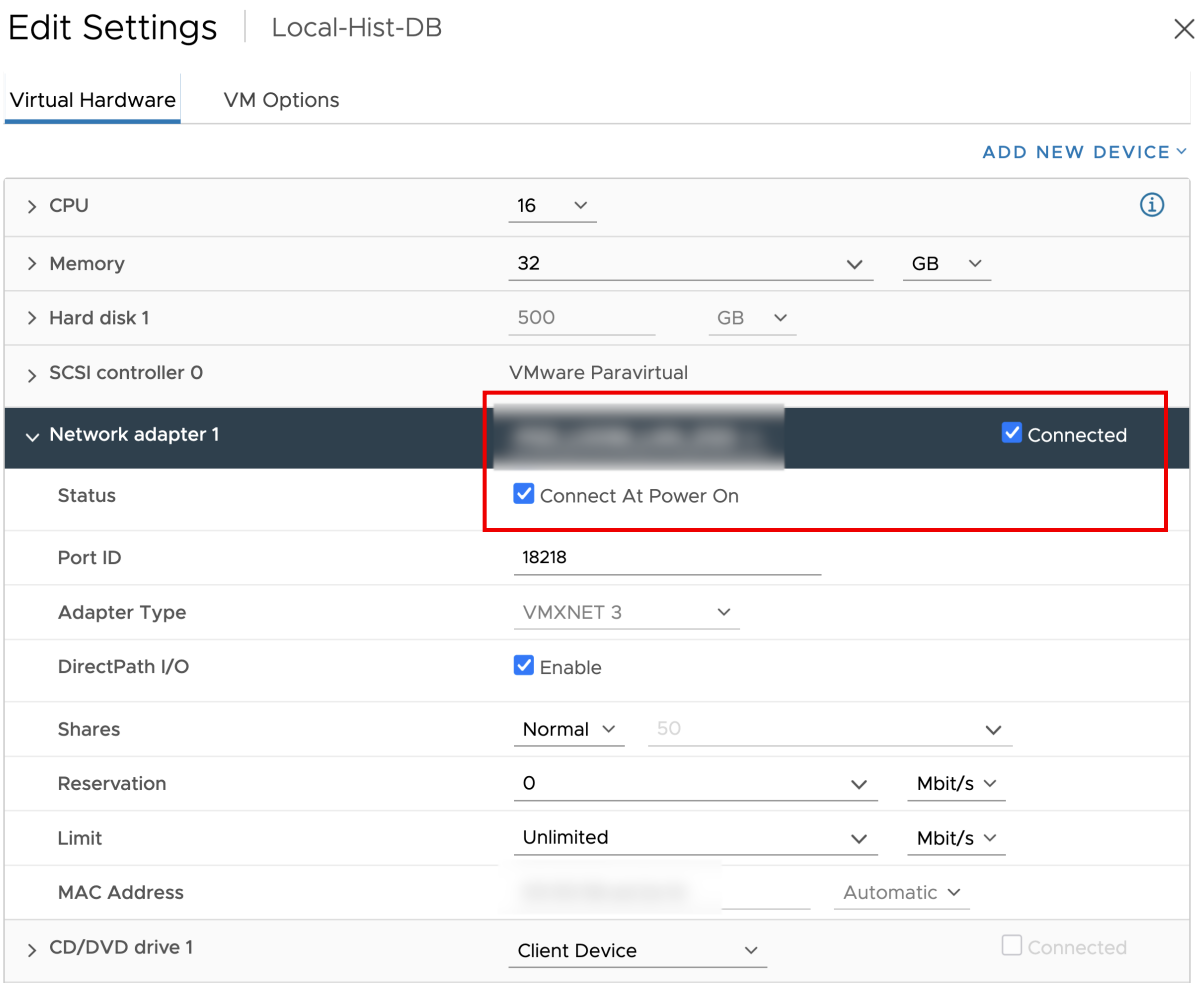


2146 **Figure 4-115: Locate Edit settings for local historian database host in vCenter**

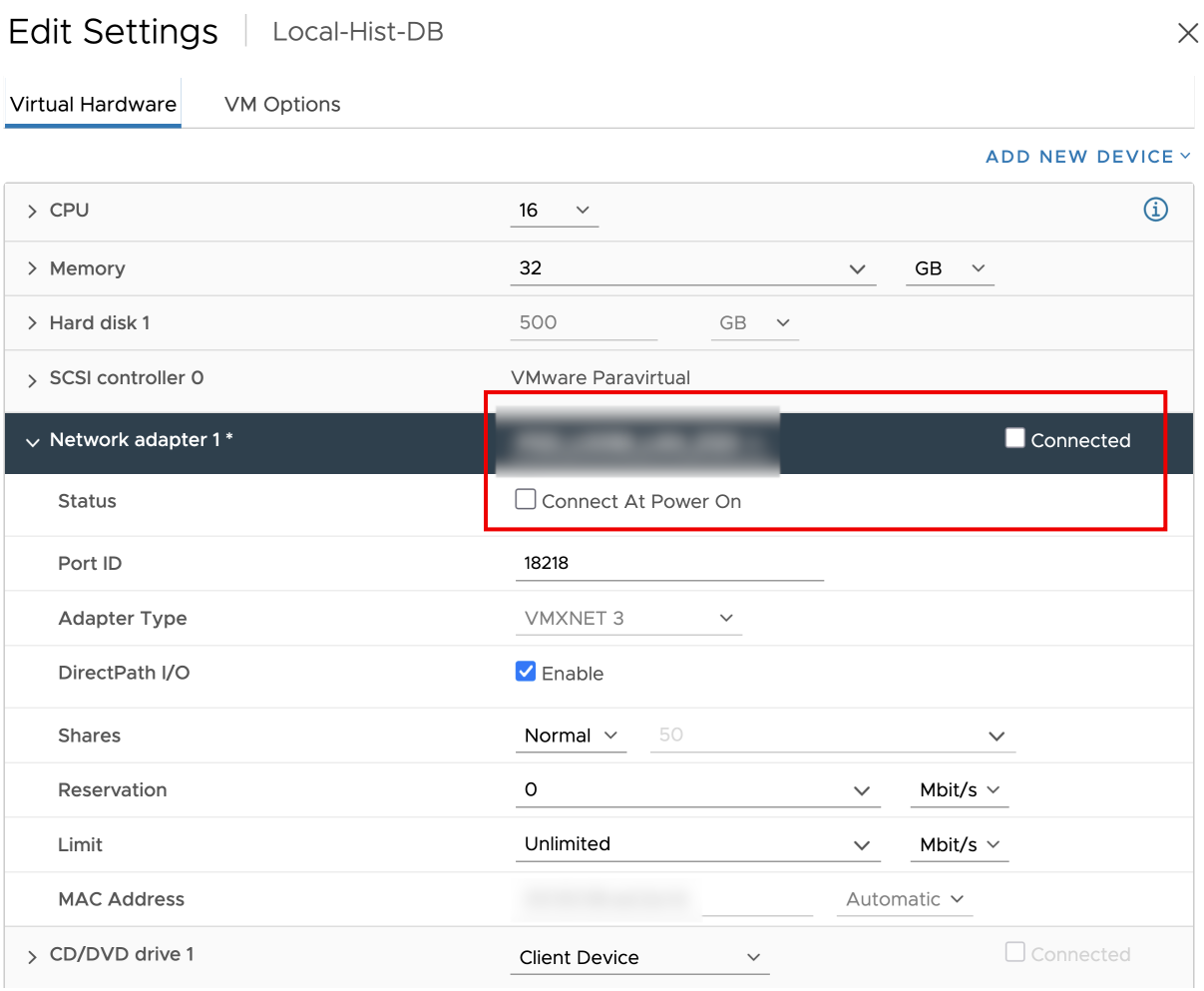


2147 **Figure 4-116: Locate "Edit Settings" for local historian database host in vCenter**

2148 Select the `Network Adapter` and uncheck the `Connected` and `Connect At Power On` check
2149 boxes.



2150 **Figure 4-117: VM Network adapter settings, currently turned on**



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.

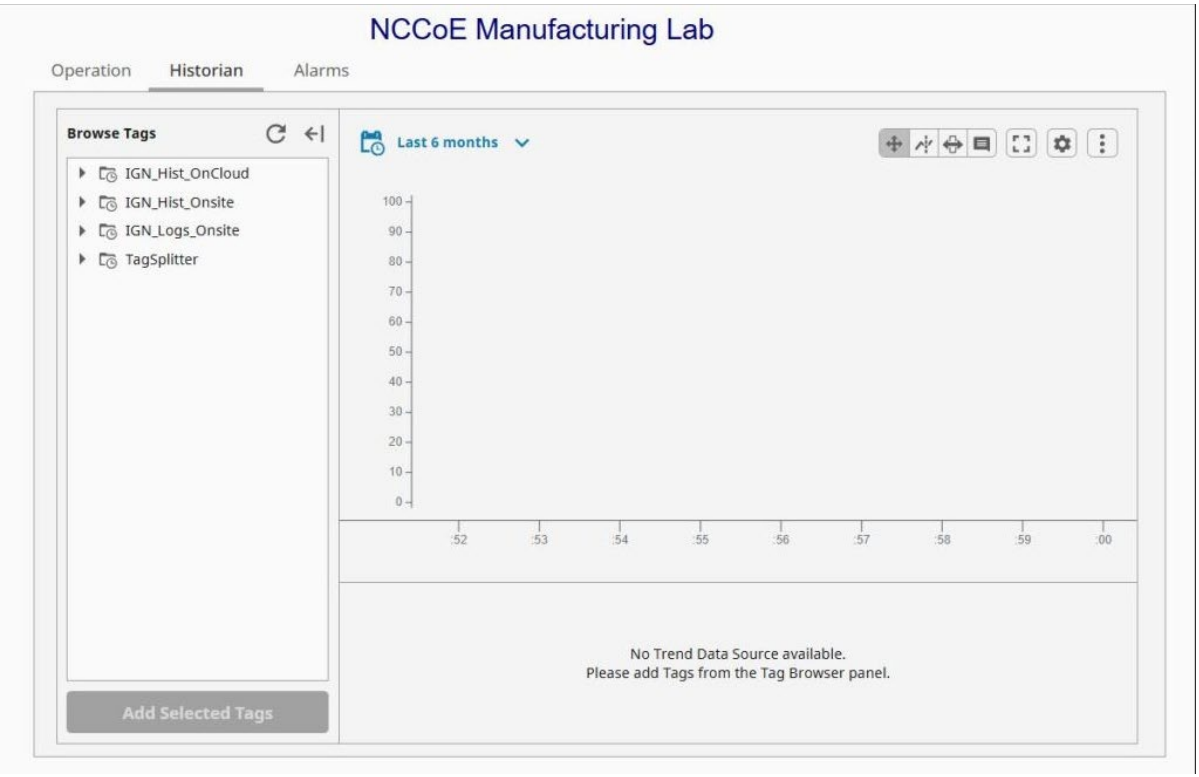


Figure 4-119: No historian data was shown from the local gateway dashboard

This same procedure was followed to disconnect the local historian gateway server from the network.

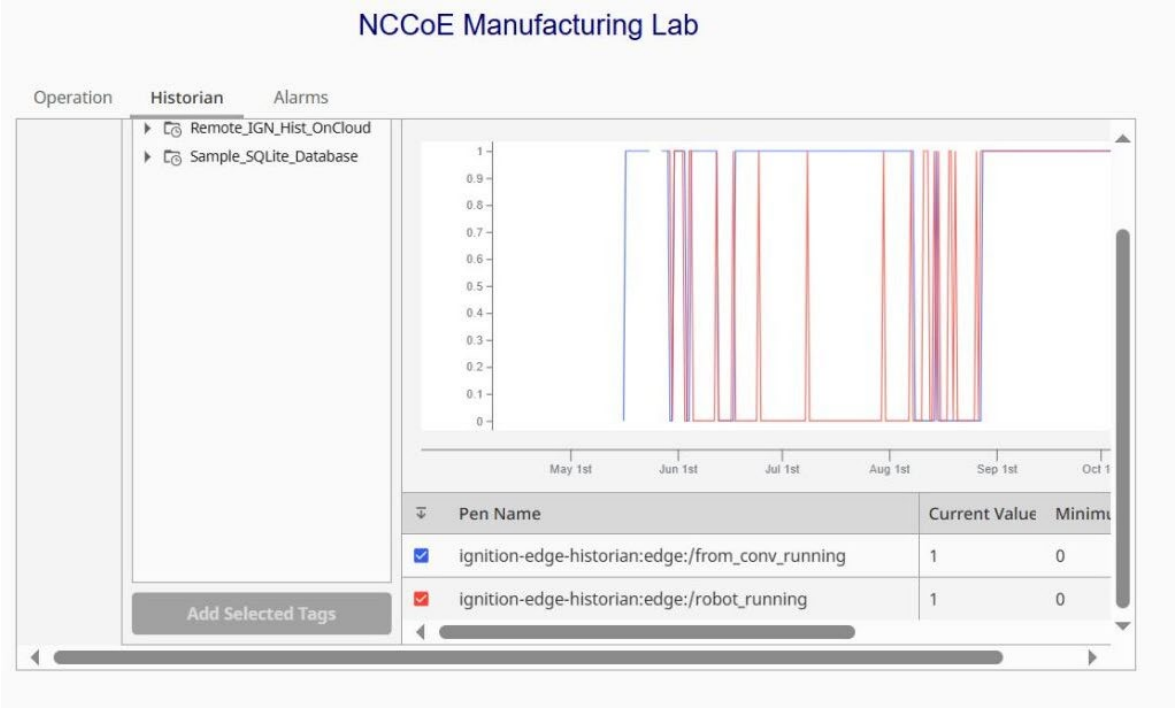
After both the database and the gateway have been disconnected, the local historian is no longer functional. The cloud historian is still operational.

[Return to Scenario B]

C.5.9 Validate Redundant AWS Cloud Historian

A cloud database and historian were configured for redundancy. After isolating the local historian, verify that the redundant server installed in the AWS cloud is still functional.

- Log in to Ignition historian in the cloud.
- 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 <-{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**

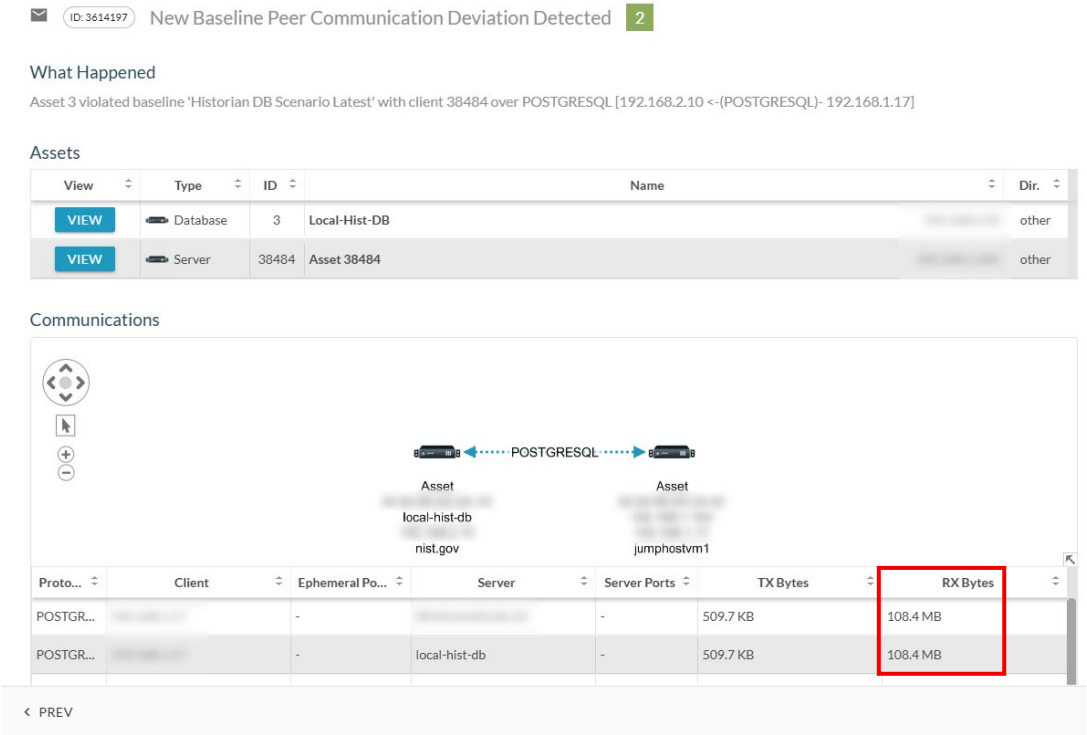


Figure 4-122: Expanding Dragos notification to find additional information

When expanding the notification in Figure 4-123, we can see the number of RX (received) bytes moving between the local historian database and the JumpHostVM1. This information is added to the Dragos ticket:

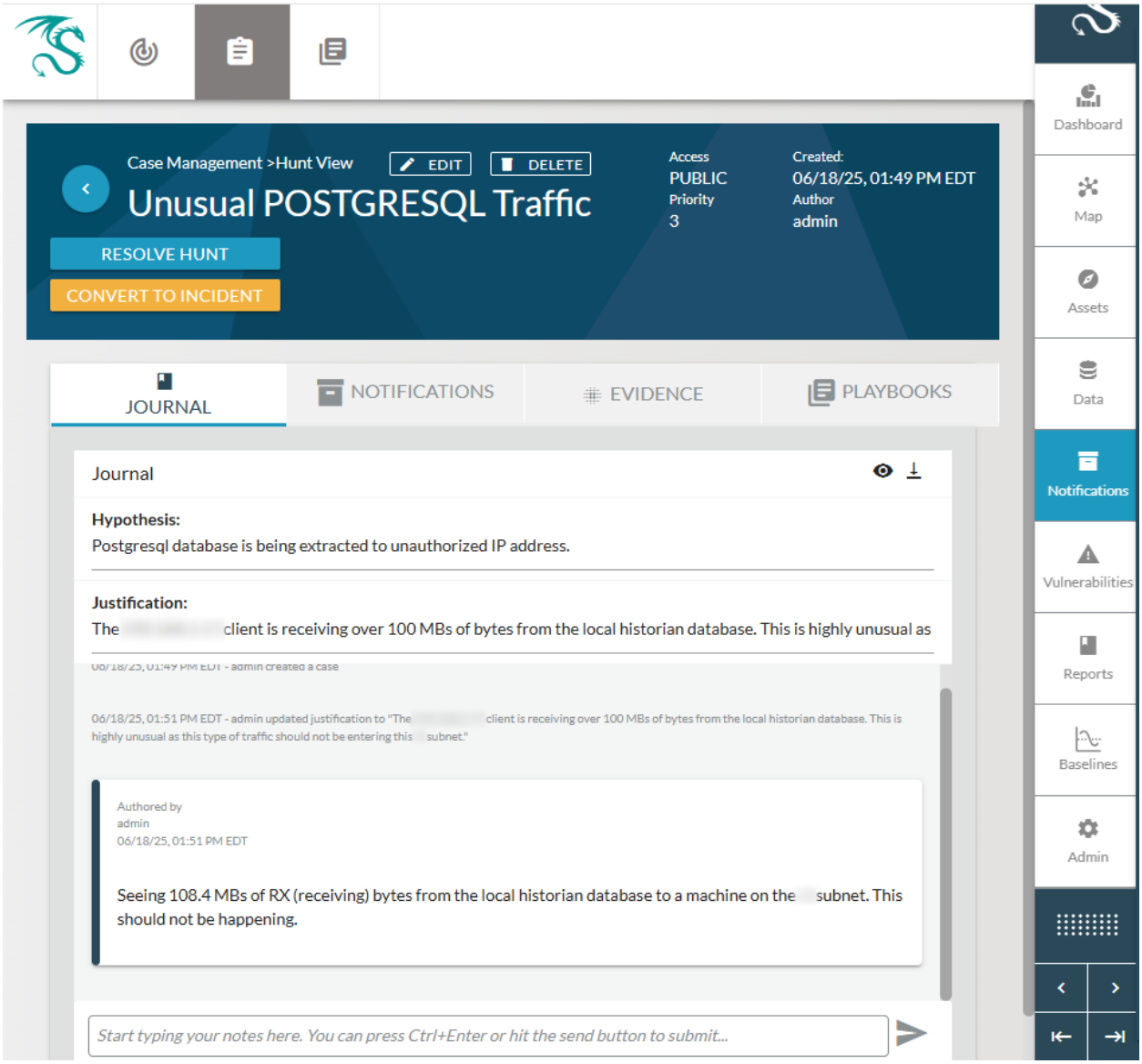
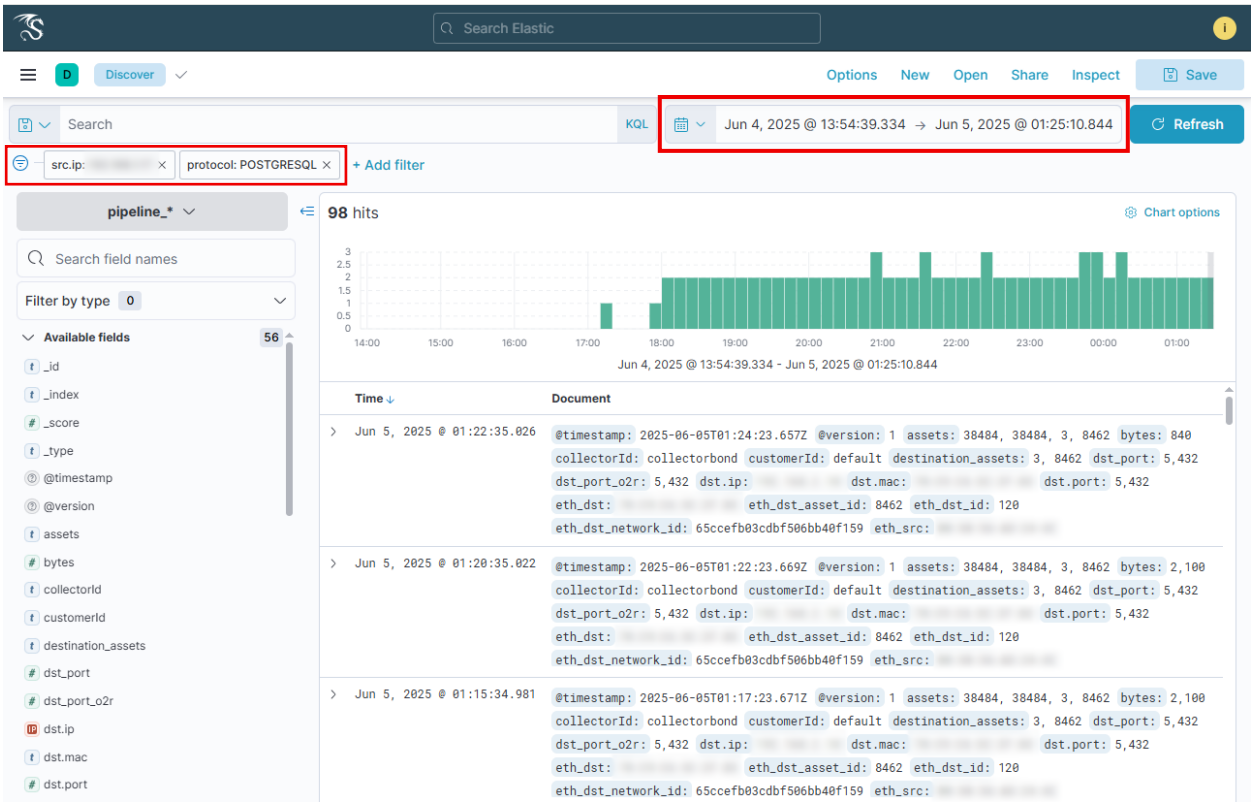


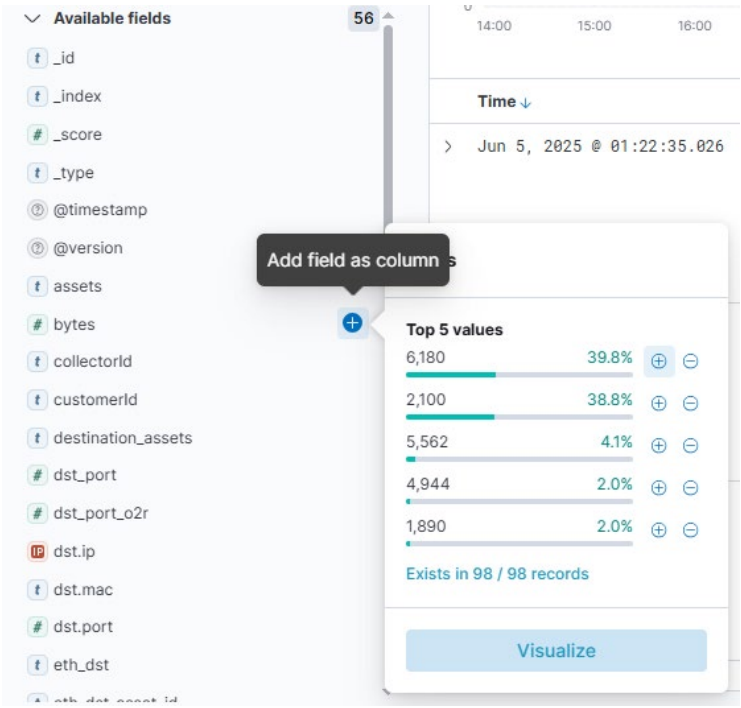
Figure 4-123: Suspicious large file transfer added to Dragos ticket

If more evidence is required, incident responders can dive further into Dragos using the built-in Kibana instance. To gather more evidence, this unusual behavior can be tracked even further by shortening the 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**

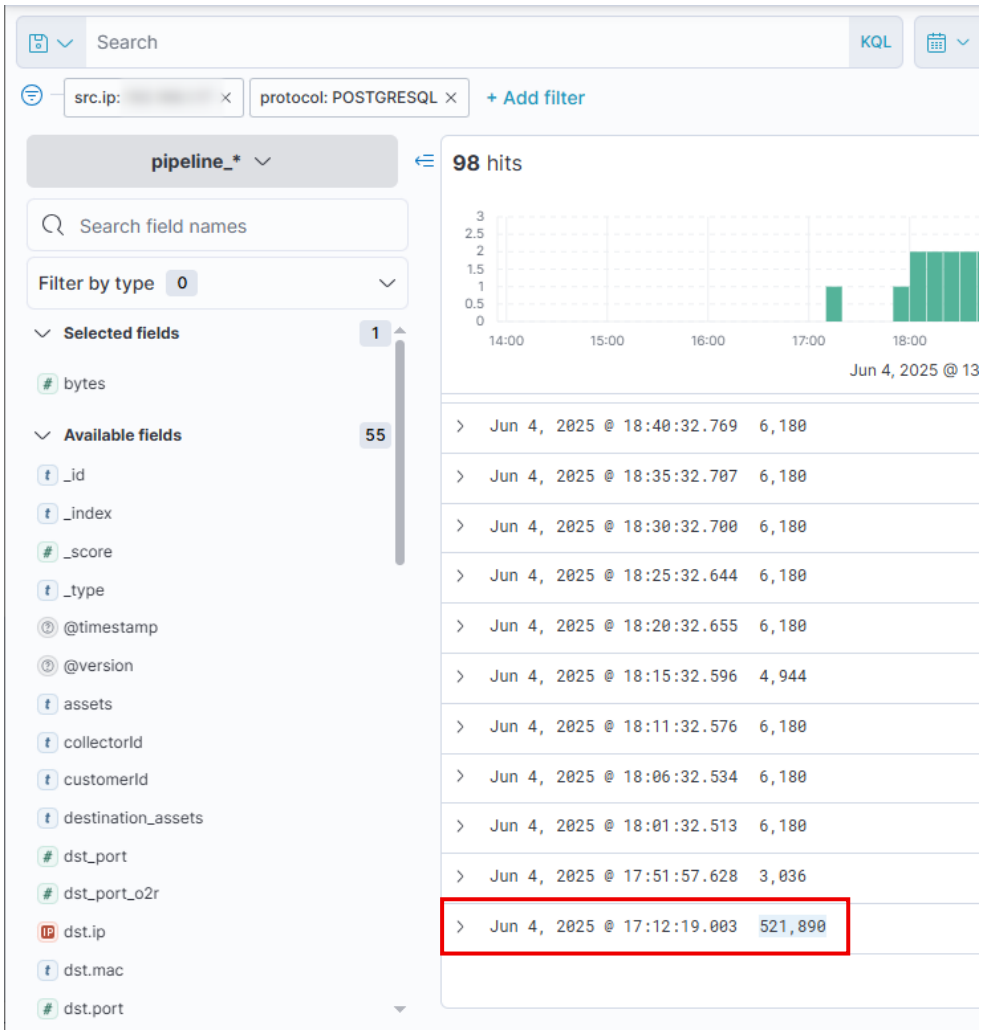
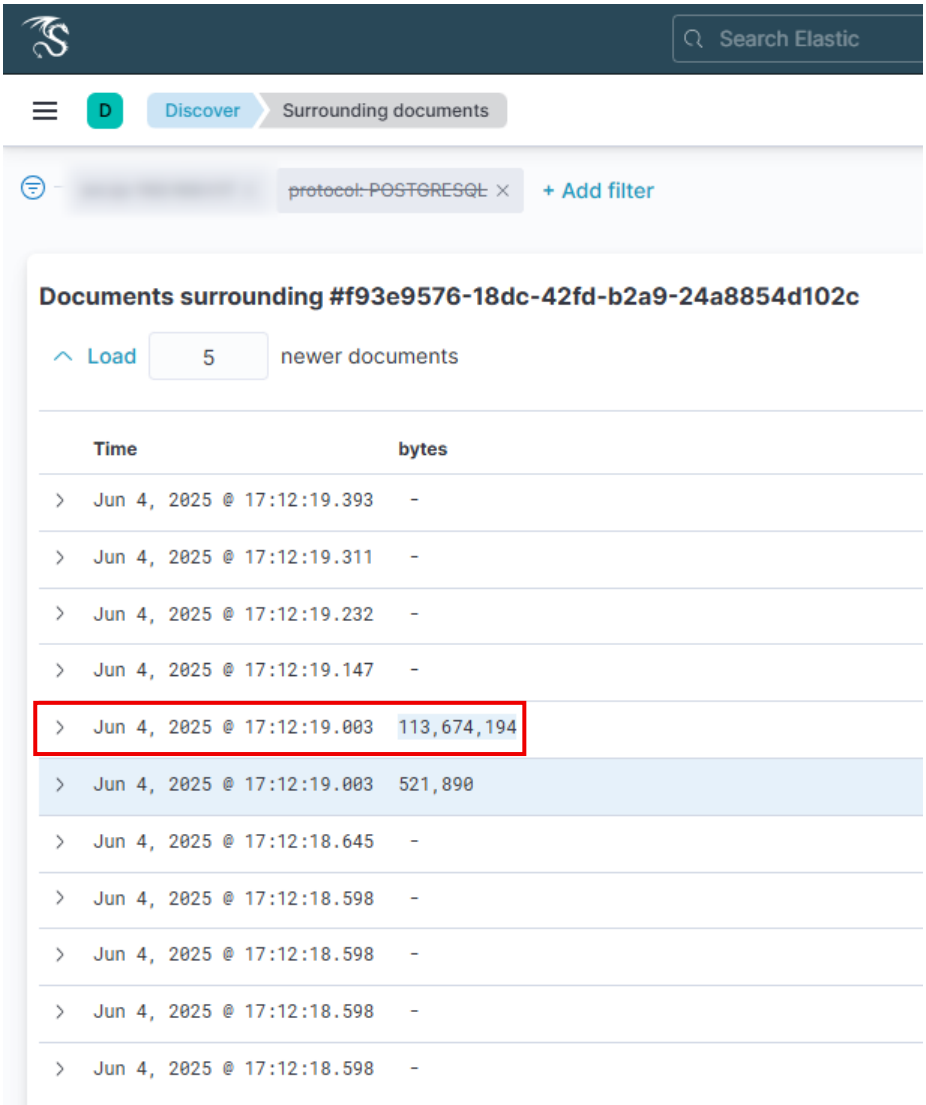


Figure 4-126: Seeing a large number of bytes around the time of the notification

The red box indicates a single log with 521,890 bytes. Not as large as we're looking for, so from here we can view additional logs to get closer to what we're looking for. Start by expanding this log and clicking on the "View surrounding documents" button:

2189 **Figure 4-127: Expanded the log to view its contents**



2190 **Figure 4-128: Larger amounts of data found**

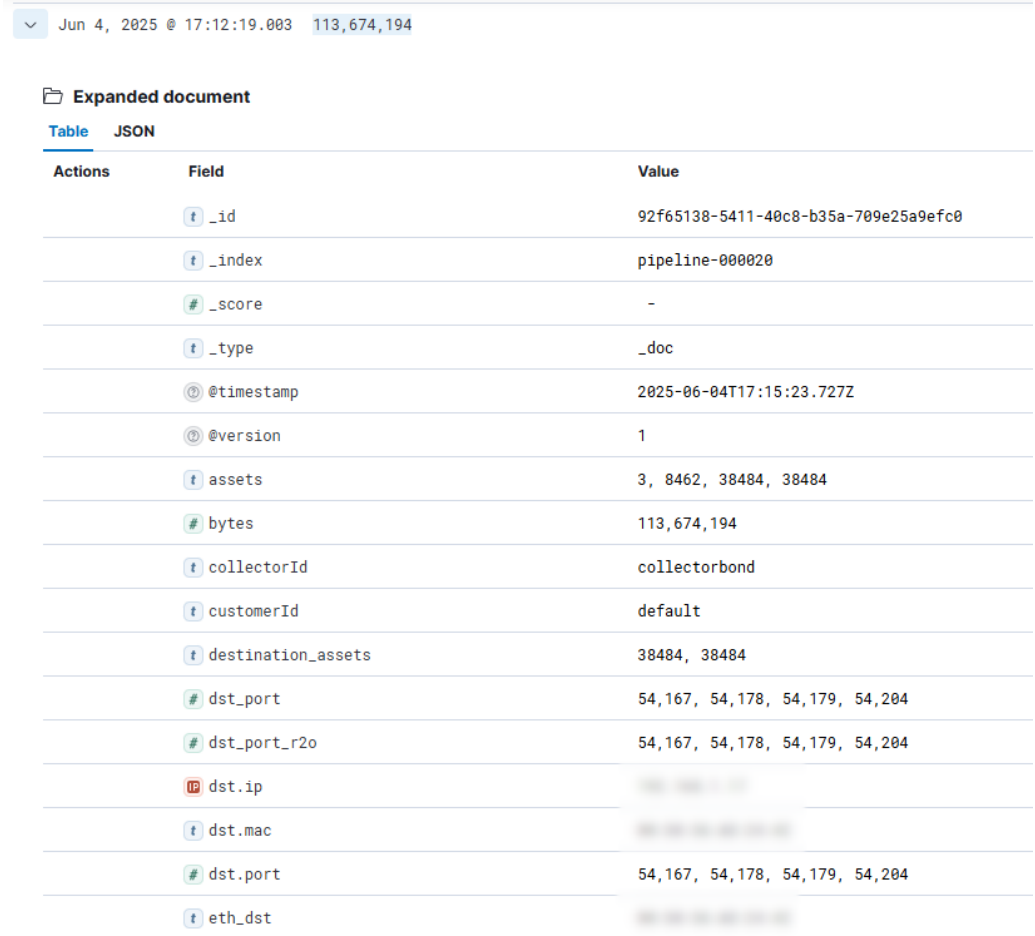


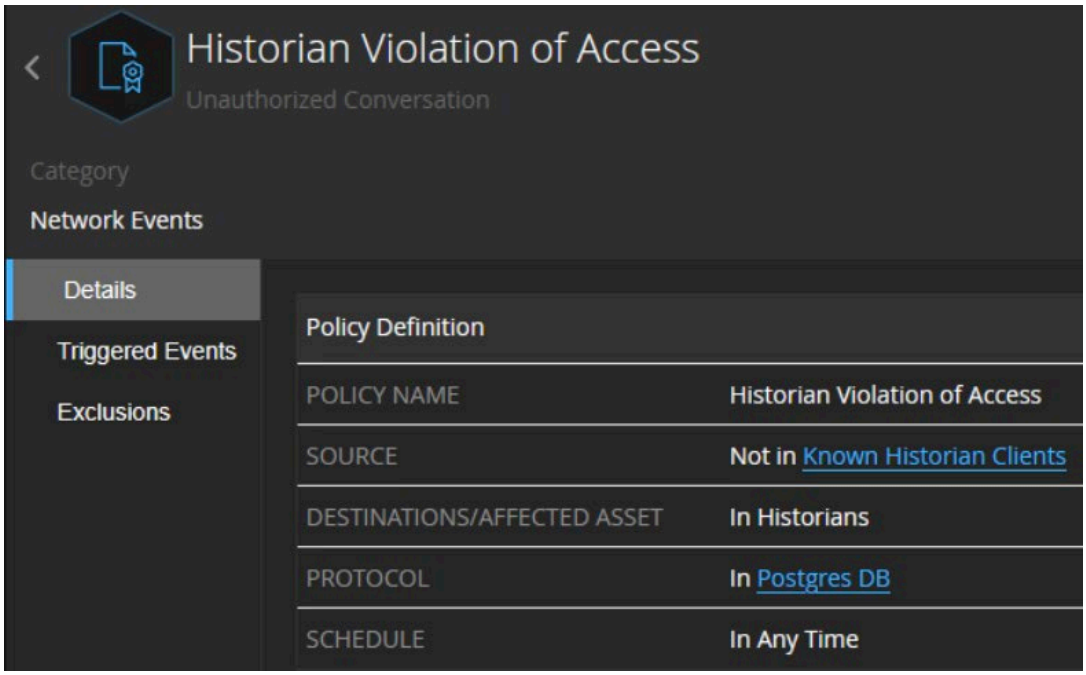
Figure 4-129: Expanded the log to view its contents

Incident responders can utilize Dragos tools to narrow down unusual activity found within the OT network, and these are a few methods to do so.

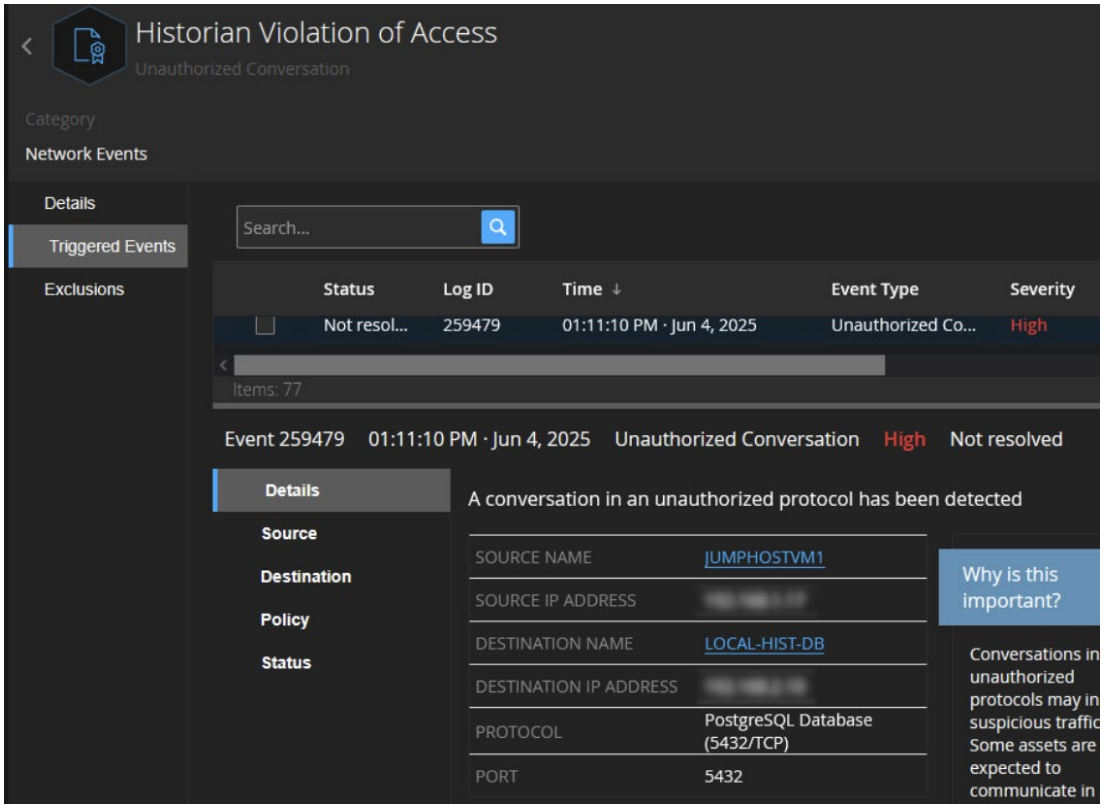
[Return to Scenario B]

C.5.11 Detecting Policy Deviation in Tenable

Although Tenable can be configured with policies that can detect unusual traffic, it may need to be trained to differentiate between expected versus anomalous alerts. In this scenario, expected data historian traffic was initially flagged as malicious, so a policy was set up to establish a baseline of normal behavior by detecting and allowing expected PostgreSQL traffic leaving the data historian. The set of 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]

C.5.12 Browsing Packet Captures from Tenable

With Tenable triggering the alert, along with Dragos, incident responders can use Tenable to pull the network packet captures around the time these violations occurred. Using another tool, Wireshark in this instance, users can attempt to attribute who performed this transfer of data from the data historian. For the scenario, this begins by viewing the Network Summary page under the Network tab on the left-hand side. The following set of screenshots showcases the Network Summary page, starting with the full page, followed by portions of the same screenshot zoomed in for clarity. The time range set for the data shown is the same time frame as the policy violation.

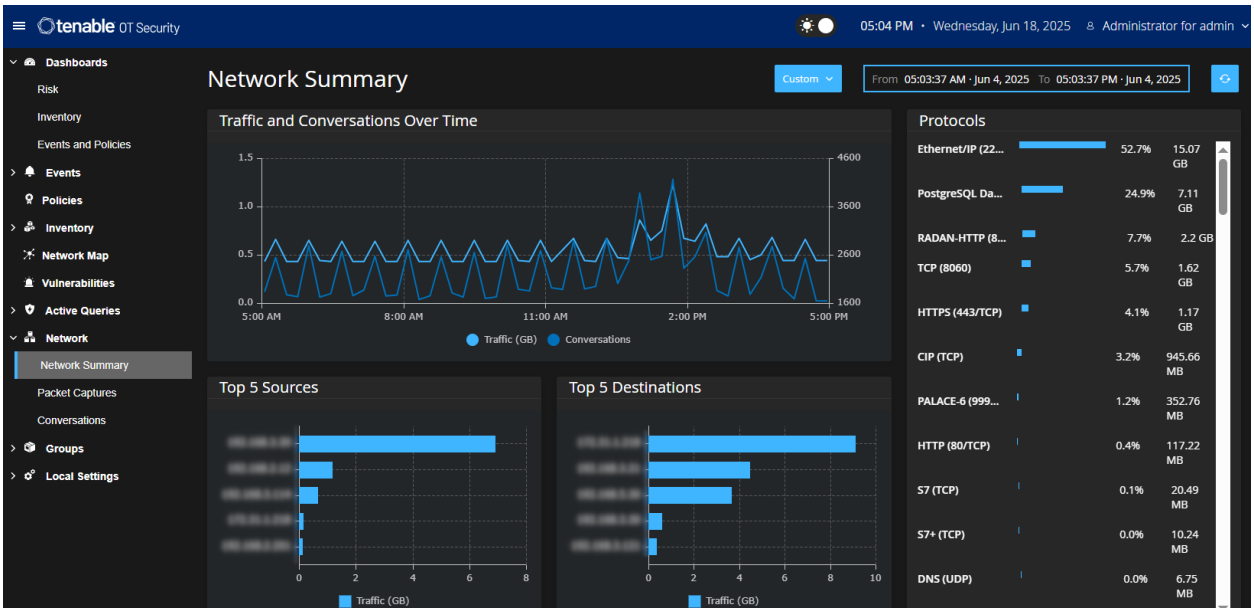
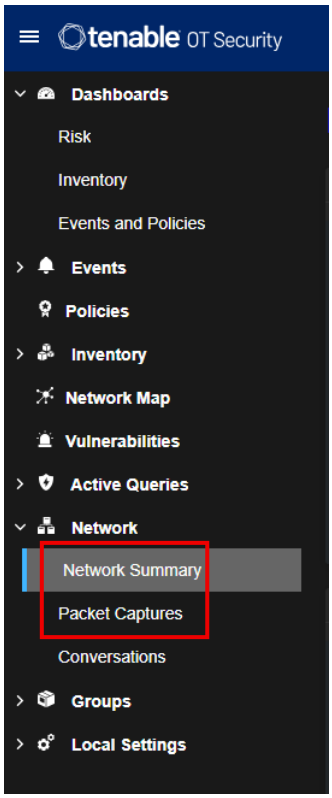
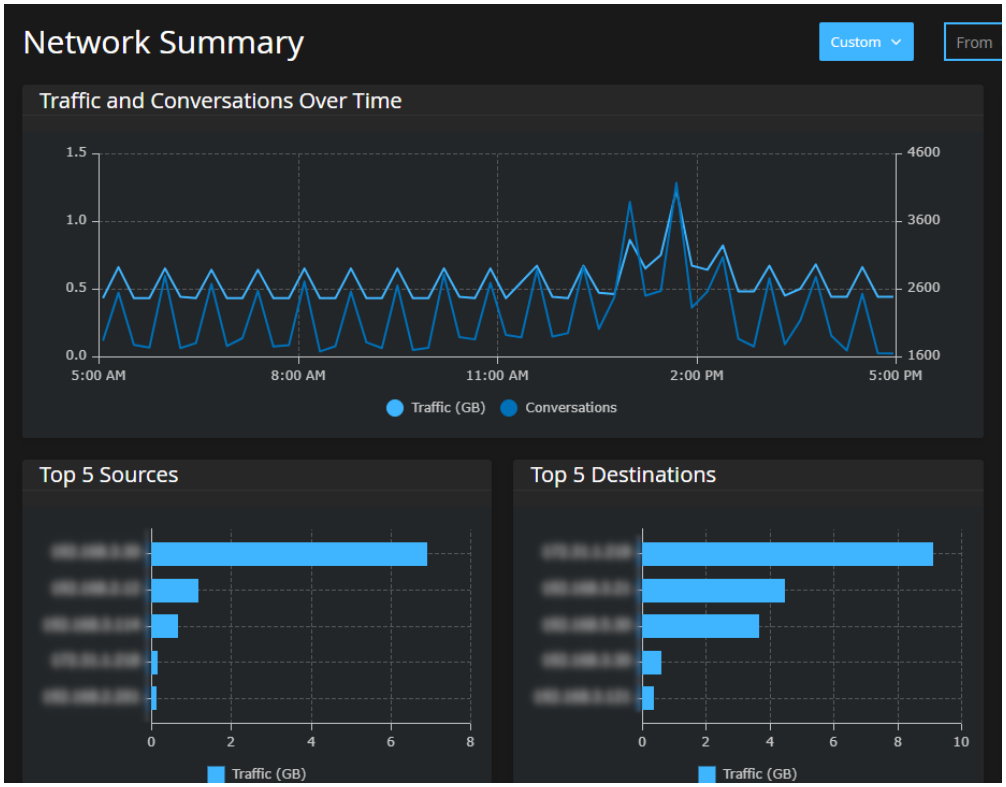


Figure 4-132: Full Network Summary page in Tenable



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**

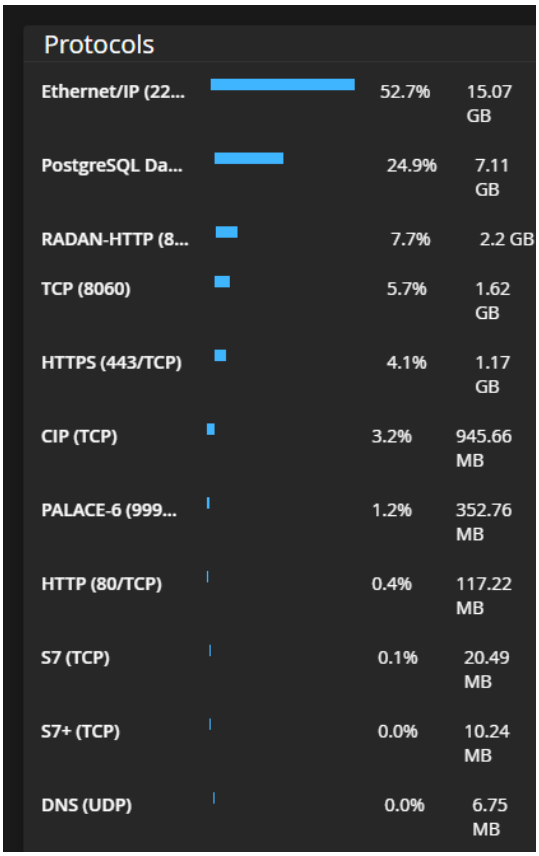
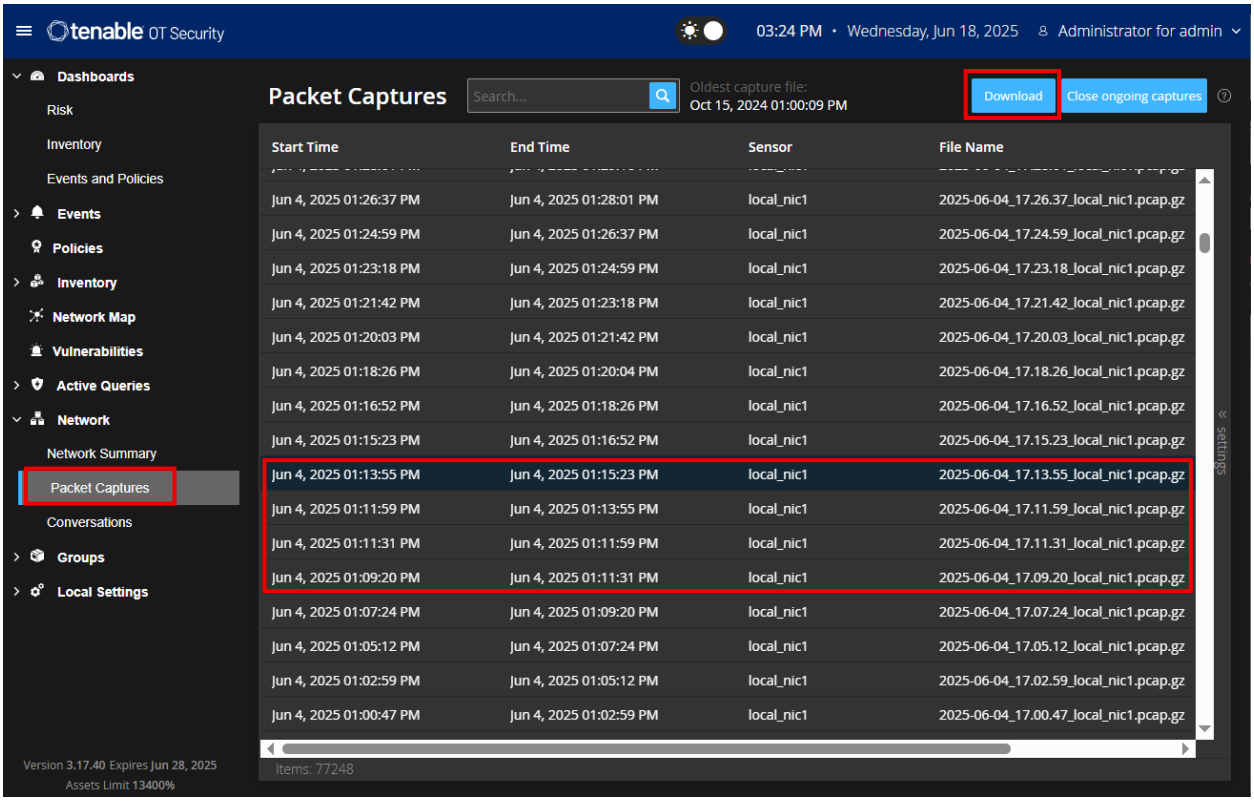


Figure 4-135: Shows the most traffic by GBs based on protocol

As seen above, PostgreSQL traffic is a little high in the timeframe of the policy violation. Depending on the network, this might not be abnormal, but since this is the main database used for the data historian, it's more evidence of suspicious activity.

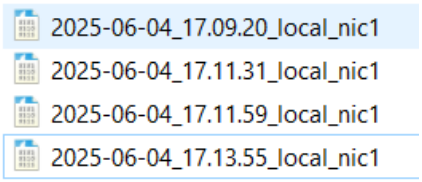
At this point, the incident response team wants to investigate further to determine if they can attribute this flow of data to a specific user. They download the packet capture files (PCAPs) from Tenable to view in the program Wireshark.



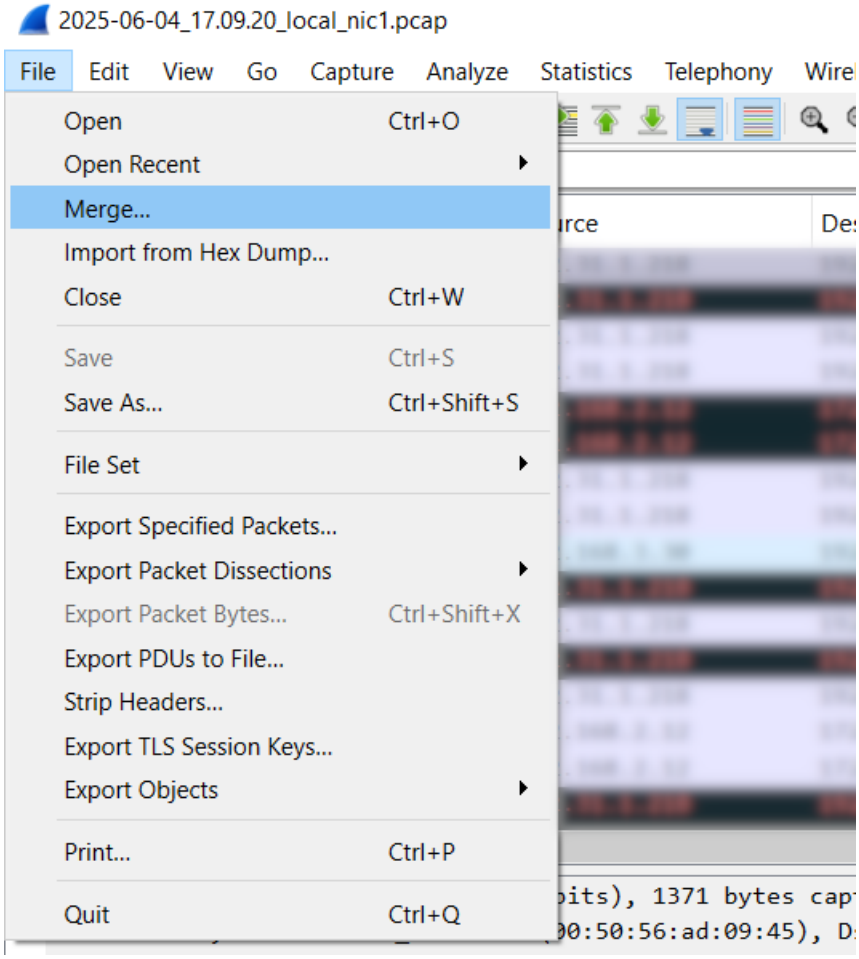
2222 **Figure 4-136: The Packet Captures tab, highlighted areas are the PCAPs used in the scenario**

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.

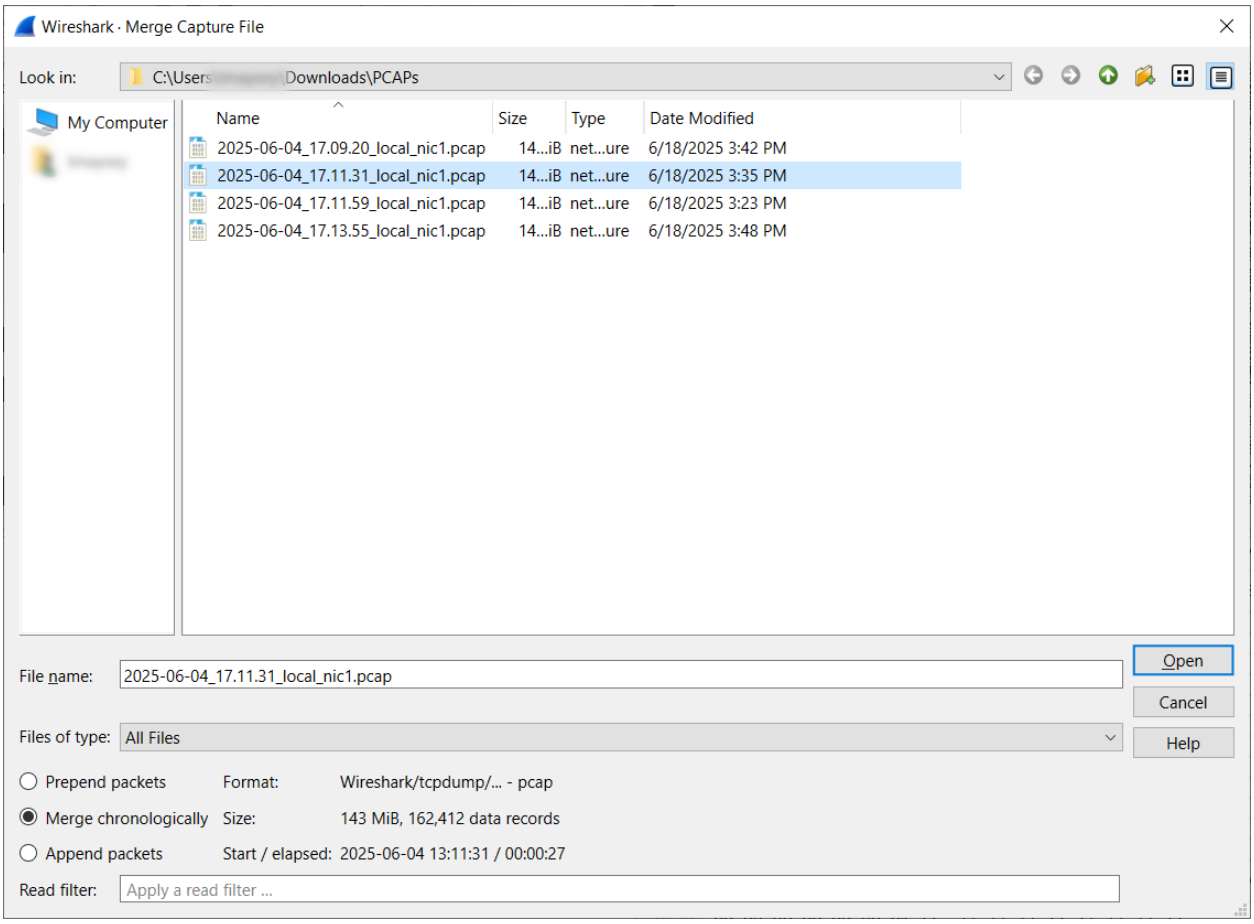
2227 Open a PCAP in Wireshark, then go to “File” and select “Merge…”:



2228 **Figure 4-137: Four downloaded PCAPs from Tenable**

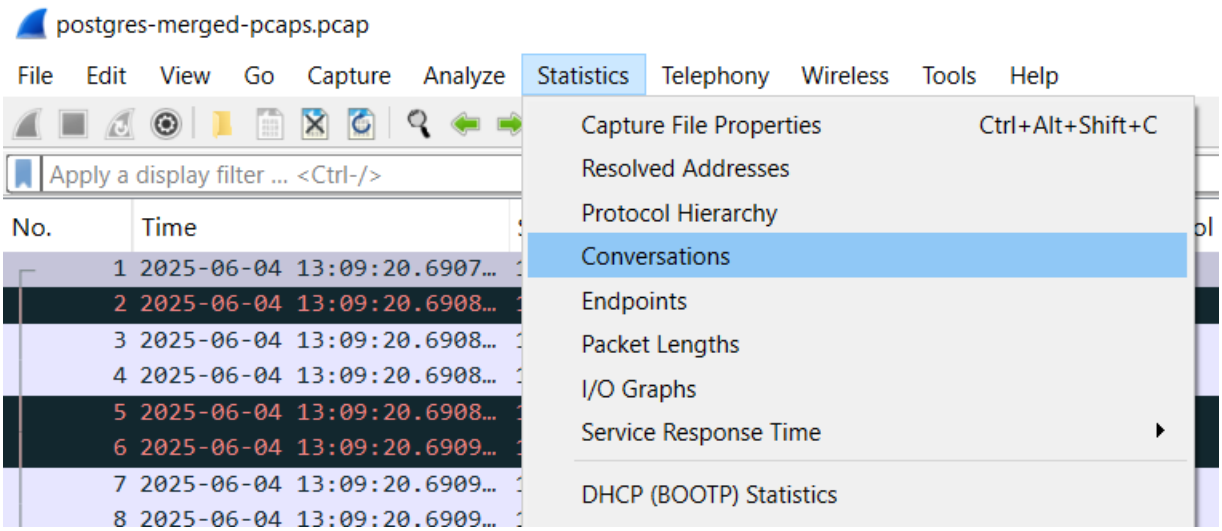


2229 **Figure 4-138: Choosing the option to merge multiple PCAPs together in Wireshark**

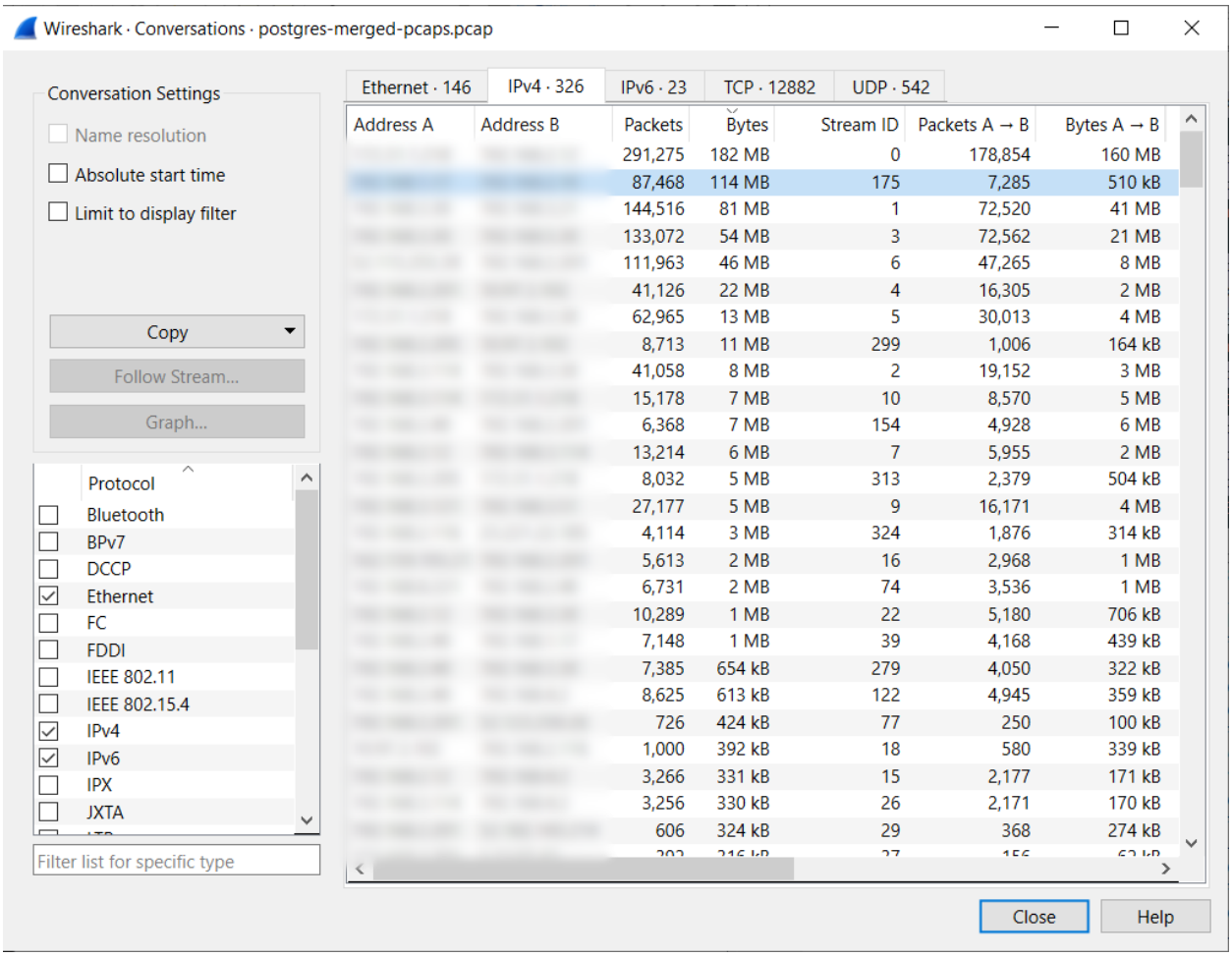


2230 **Figure 4-139: Selecting the four downloaded PCAPs from Tenable to merge**

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**

The conversations window in Wireshark will show all of the communications between various IP addresses. In the above screenshot, the highlighted line is the IP addresses between the data historian database and the JumpHostVM1. From here, right-click on that line and filter the packets based on this communication:

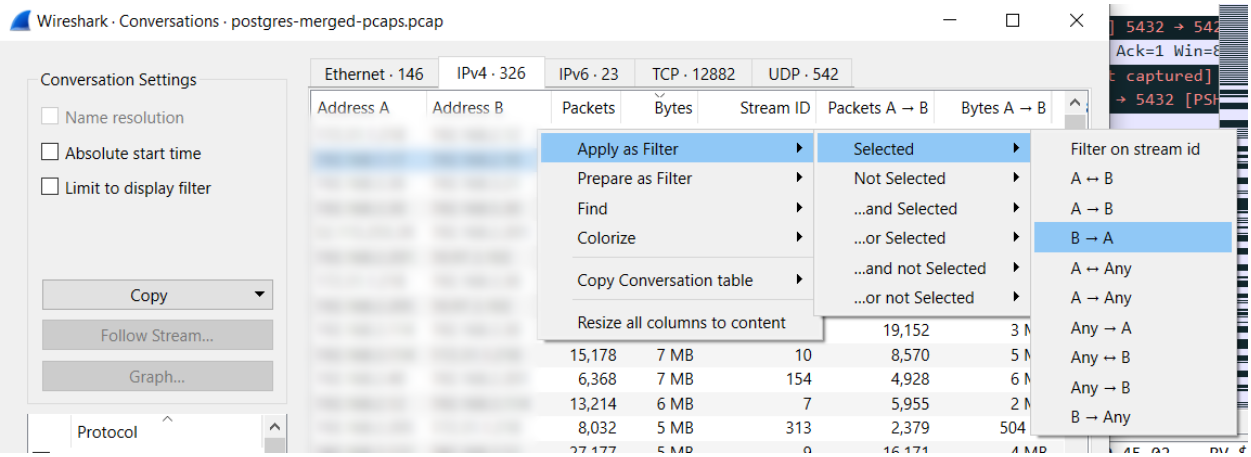
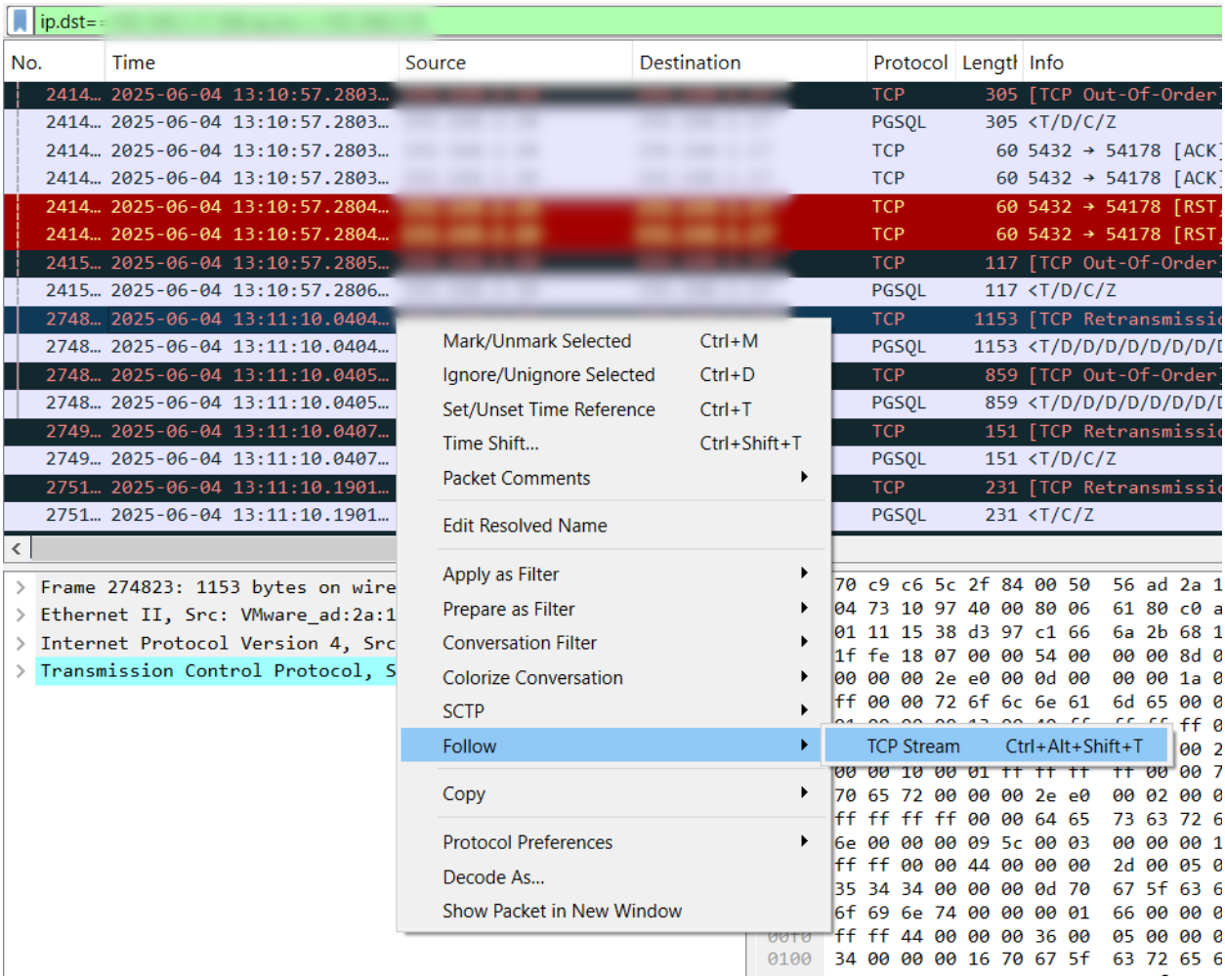
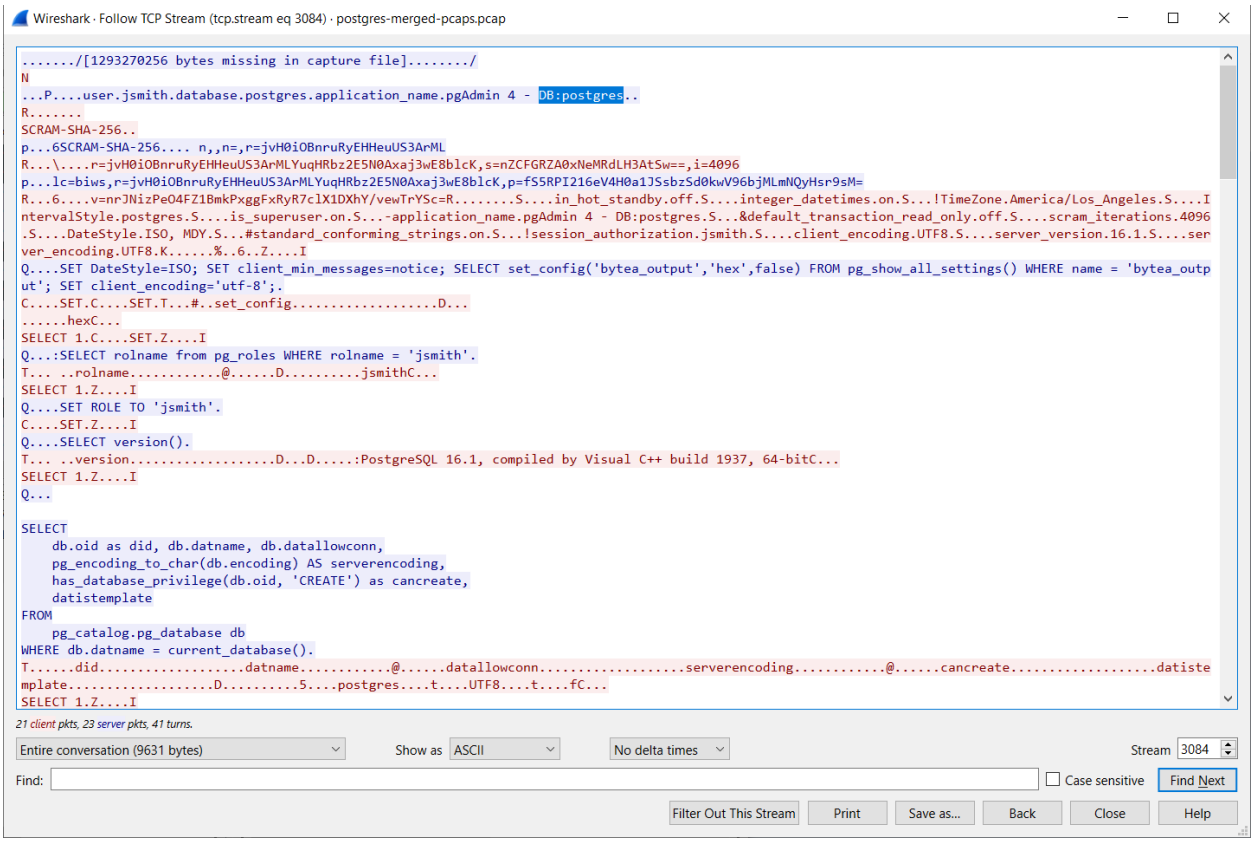


Figure 4-142: Applying a filter in Wireshark based on conversations

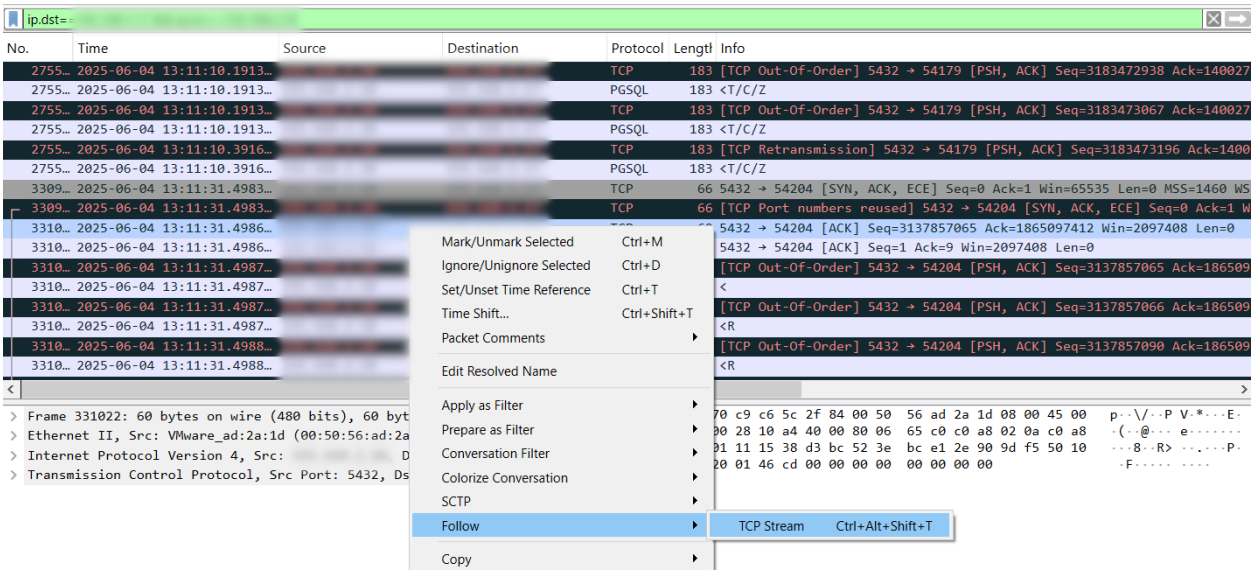
After the filter has been applied, seek a TCP packet with port 5432, the default for PostgreSQL, and the one we used for all scenarios. Once found, right-click, go to “Follow” and then “TCP Stream”. This will open a new window and display reassembled data of all the packets from that specific TCP connection. The default view is ASCII, so this can give a quick glance at the data involved in this communication. The following set of screenshots will show two separate TCP Streams. The first will highlight the main “postgres” database and the jsmith user seen throughout. For the scenario, this TCP Stream didn’t include full information, so we followed another stream to find more evidence.



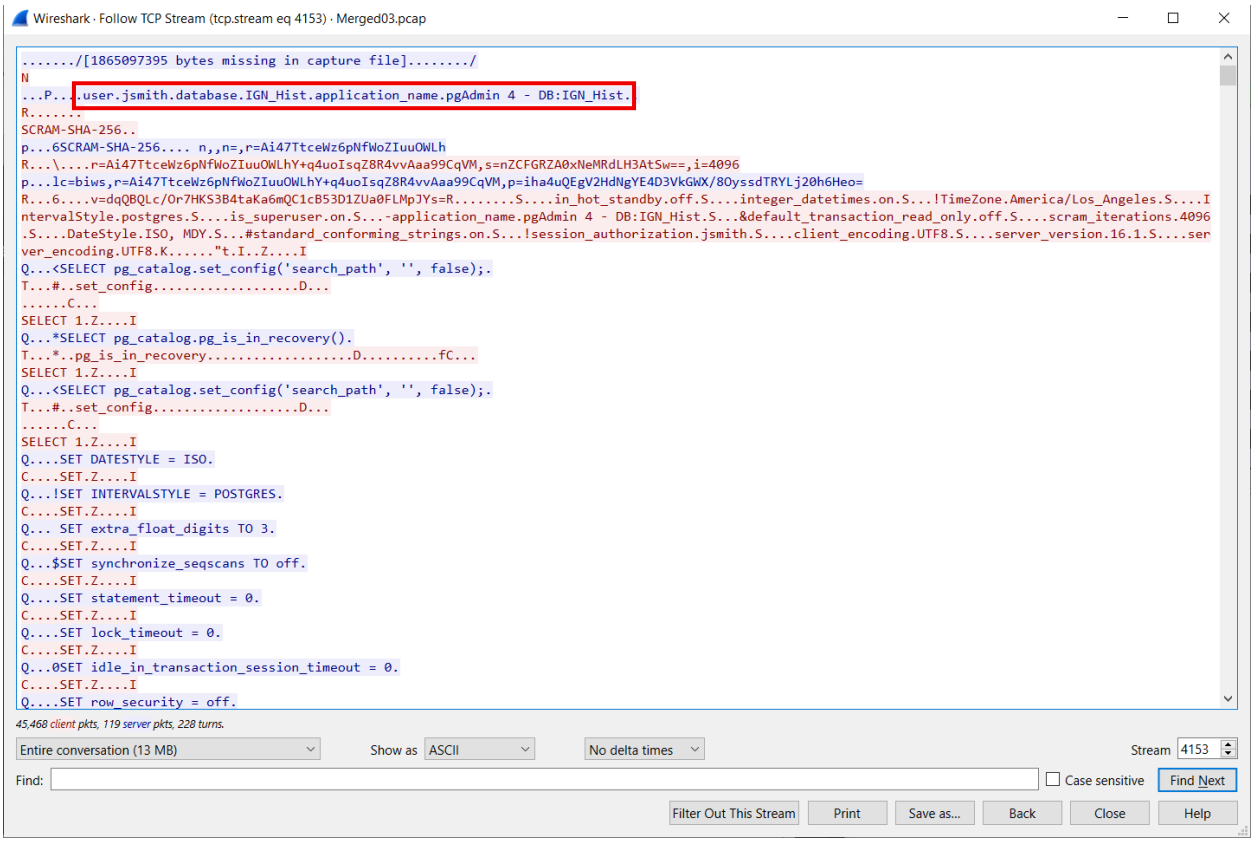
2247 **Figure 4-143: Follow TCP Stream in Wireshark**



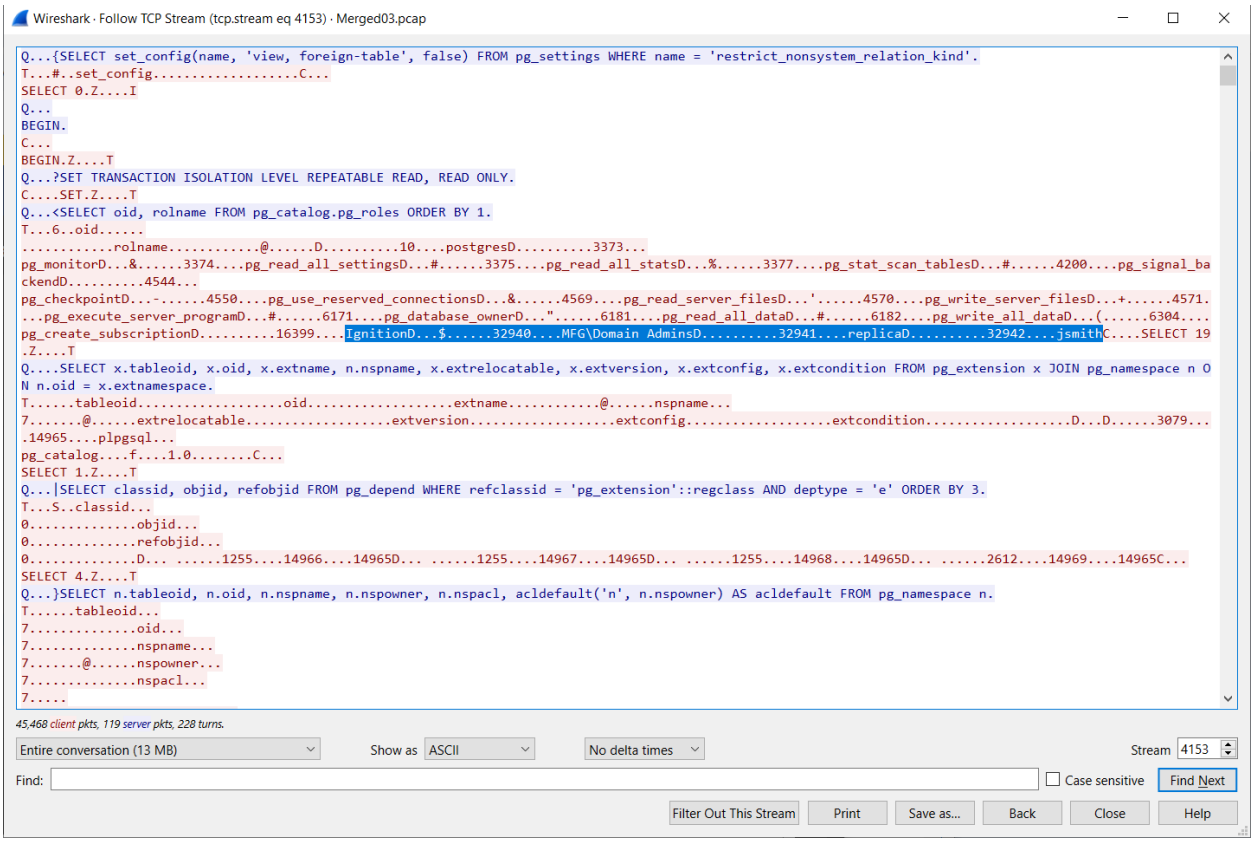
2248 **Figure 4-144: A single TCP Stream for a set of packets**



2249 **Figure 4-145: Following another TCP Stream**



2250 **Figure 4-146: A new TCP Stream showing a different PostgreSQL database being targeted**



2251 **Figure 4-147: Some key phrases found in TCP Stream to use for further investigation**

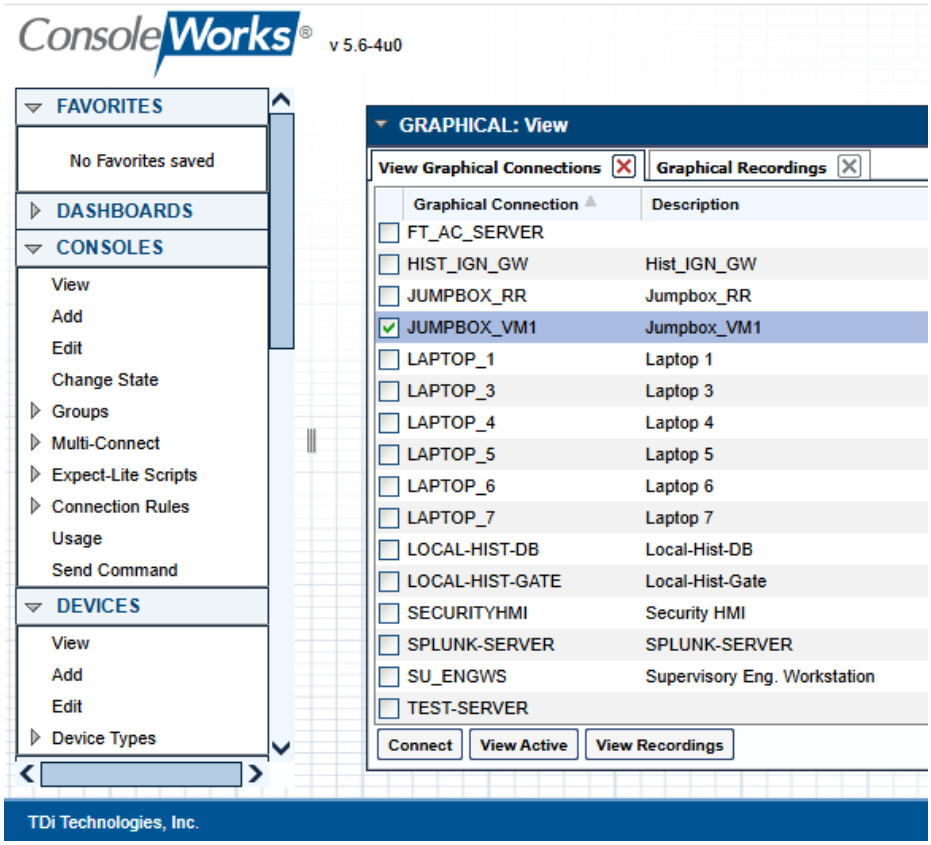
2252 In the second TCP Stream, we see similar items, like the jsmith user being named throughout, but this
2253 time we are now seeing the "IGN_Hist" database, the Domain Admins AD group, and more instances of
2254 the jsmith user. For the scenario, it is deemed enough evidence to question the jsmith user.

2255 [Return to Scenario B]

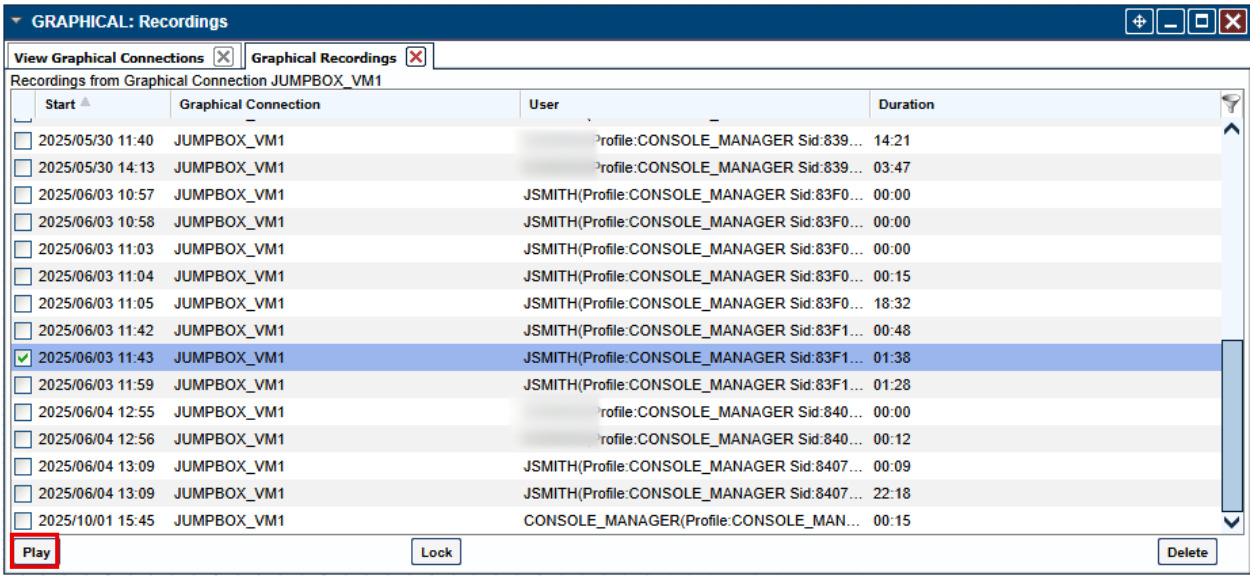
2256 C.5.13 Reviewing ConsoleWorks User Session

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:

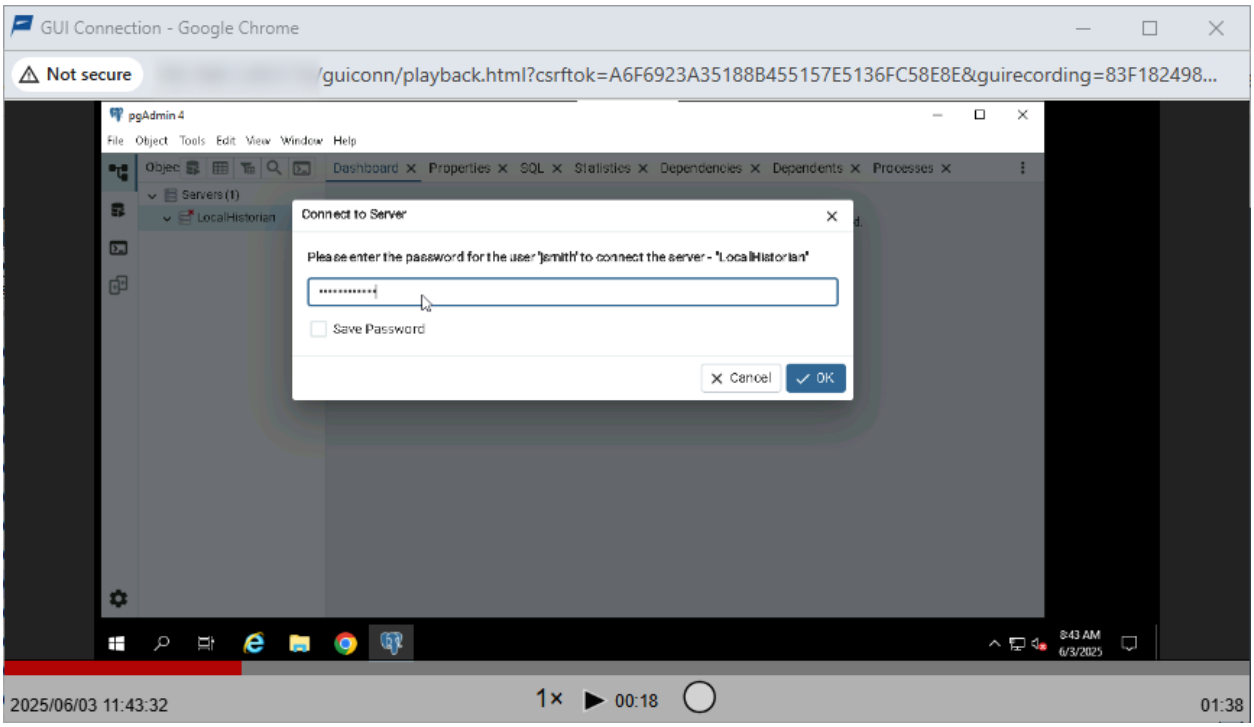
2261 *Note: Not all steps of the backup process in pgAdmin are shown.*



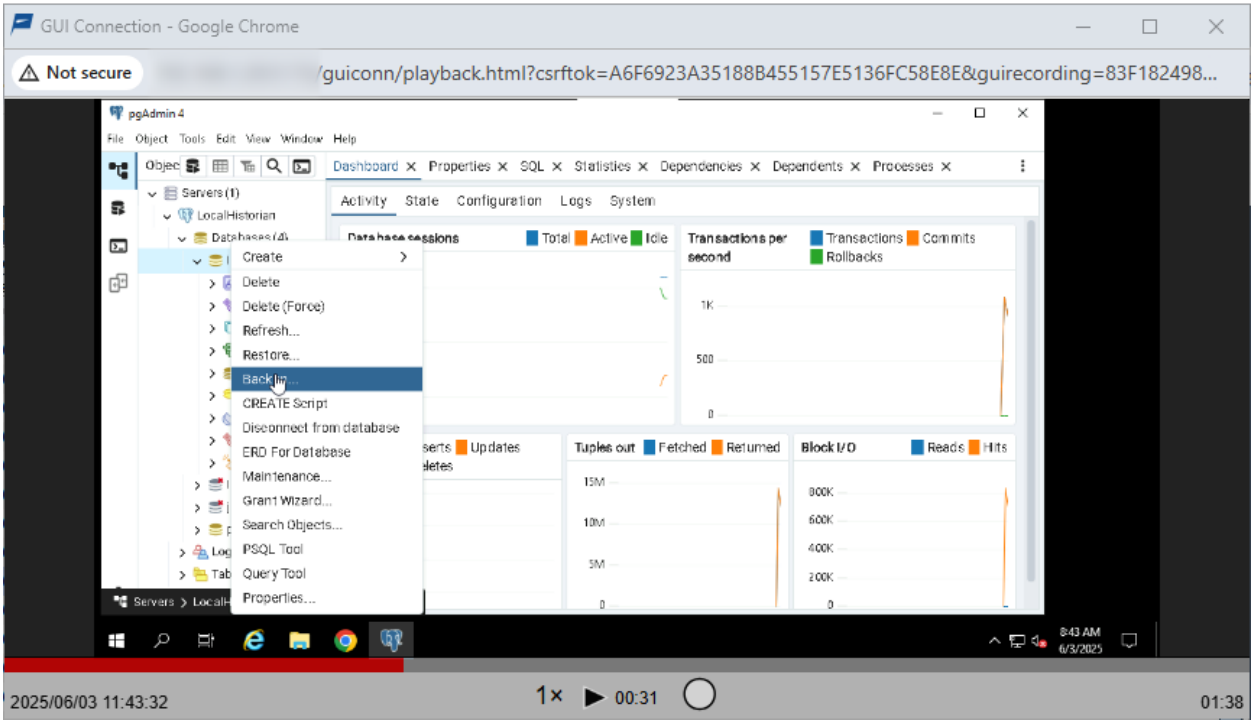
2262 **Figure 4-148: Selecting the JumpBox VM in the graphical view in ConsoleWorks**



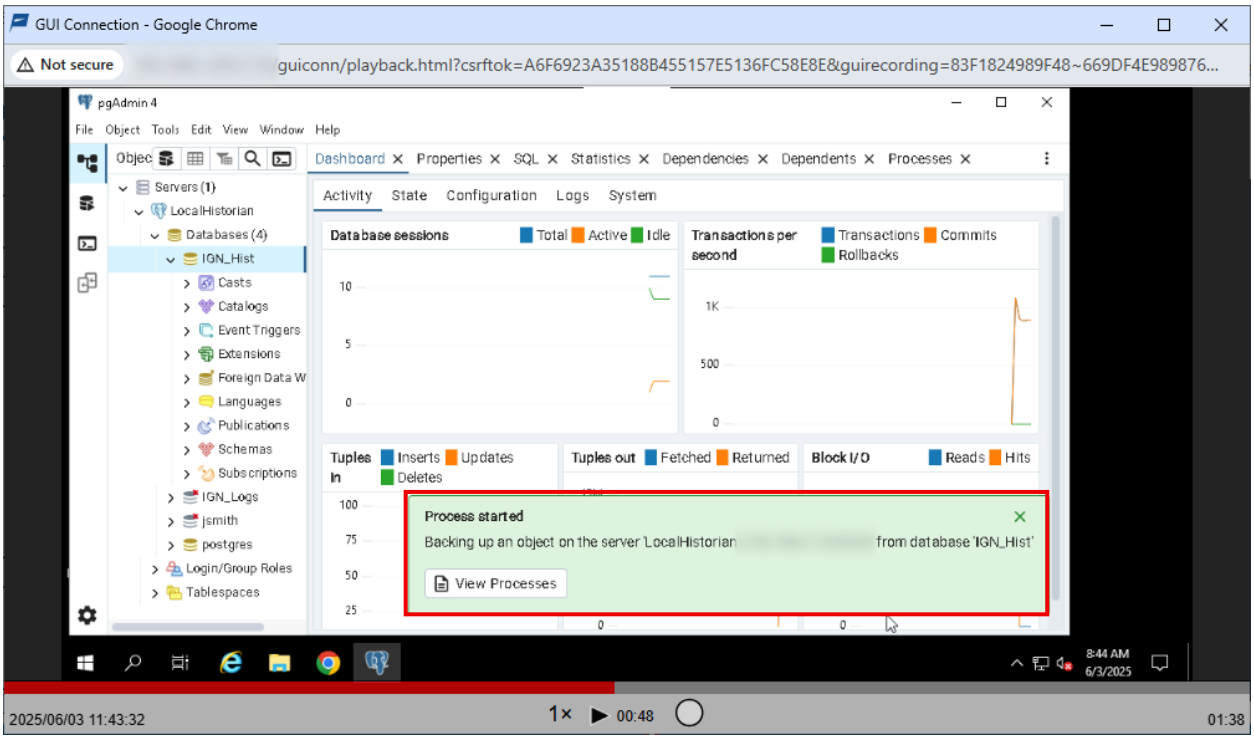
2263 **Figure 4-149: Selecting the appropriate desktop session for the jsmith user**



2264 **Figure 4-150: The jsmith user logging into pgAdmin**



2265 **Figure 4-151: The jsmith user selecting "Backup" for the target database**



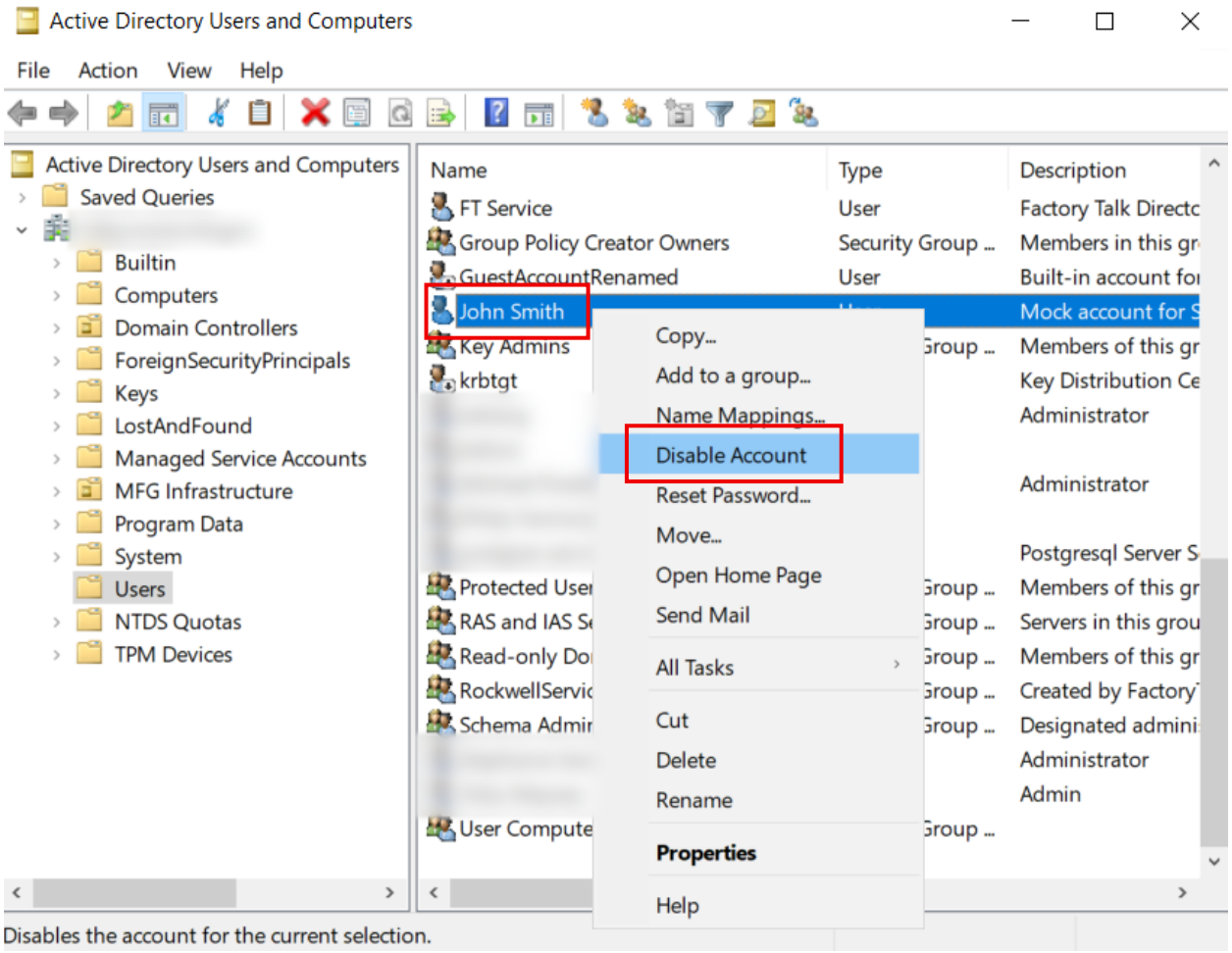
2266 **Figure 4-152: The jsmith user successfully backing up the IGN_Hist database**

2267 [Return to Scenario B]

2268 C.5.14 Disable Compromised Accounts

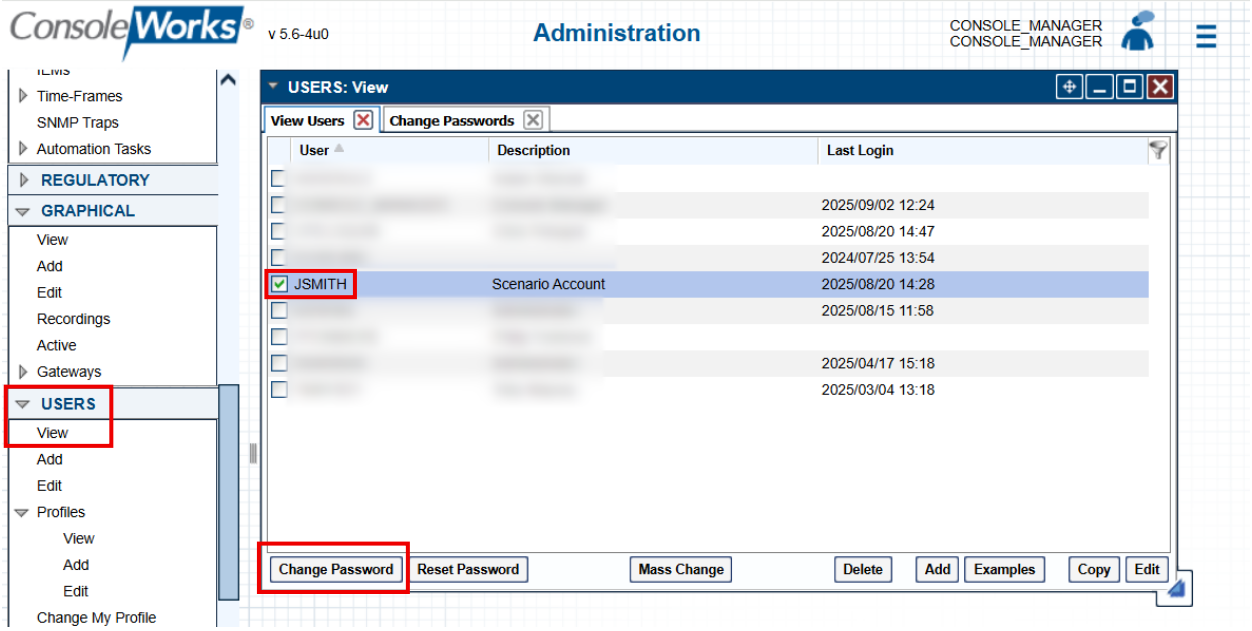
2269 Using Active Directory, corporate IT administrators disabled the remote connection from outside into
2270 the corporate asset that is exfiltrating data. The administrator also forced a password change for the
2271 compromised ConsoleWorks account. The corporate IT administrator made sure that the 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`:

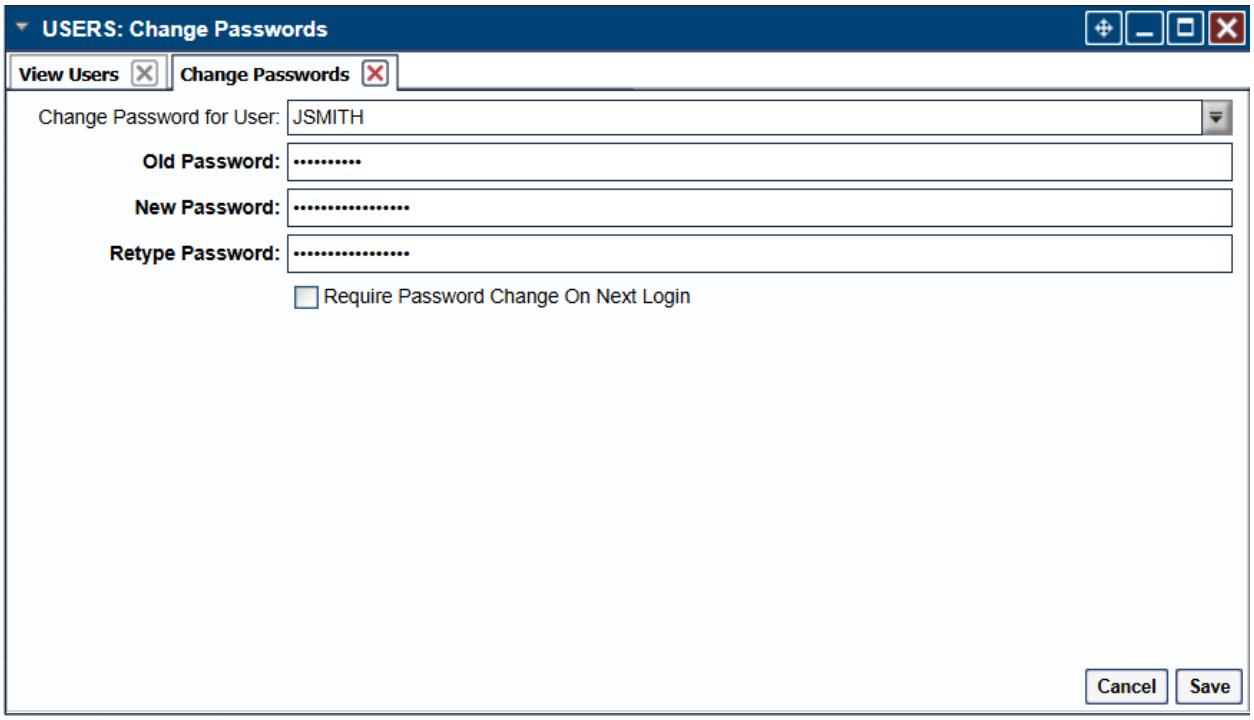


2274 **Figure 4-153: Disabling the jsmith user account in Active Directory**

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.

C.7 Scenario C: Technical Details – Preparation

Before an incident occurs, a manufacturer must prepare for incident response and recovery. The following steps were taken to prepare for the Scenario C incident.

[Return to Scenario C]

C.7.1 Creating Siemens Traffic Detection Policy in Tenable

Using section C.4.5 from Scenario B, follow those steps in creating the policy. The following set of screenshots shows the selections made to create a Tenable policy for detecting unauthorized Siemens network traffic. Two policies are created to trigger an alert every time they identify unauthorized traffic to the Siemens Conveyor PLC:

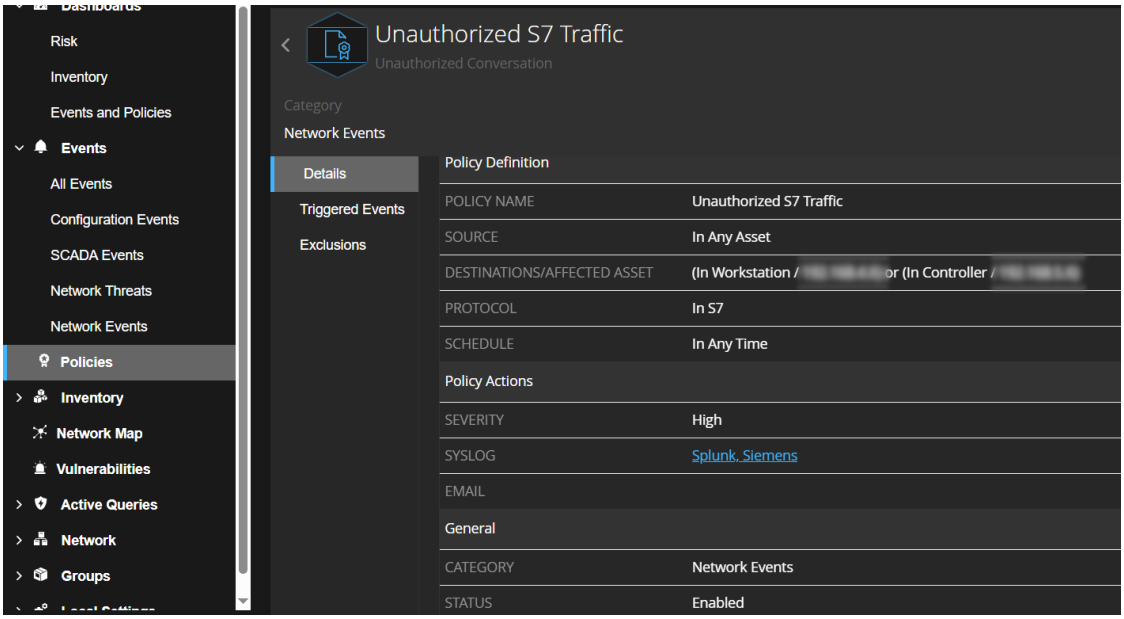


Figure 4-156: Tenable policy to track unauthorized S7 traffic

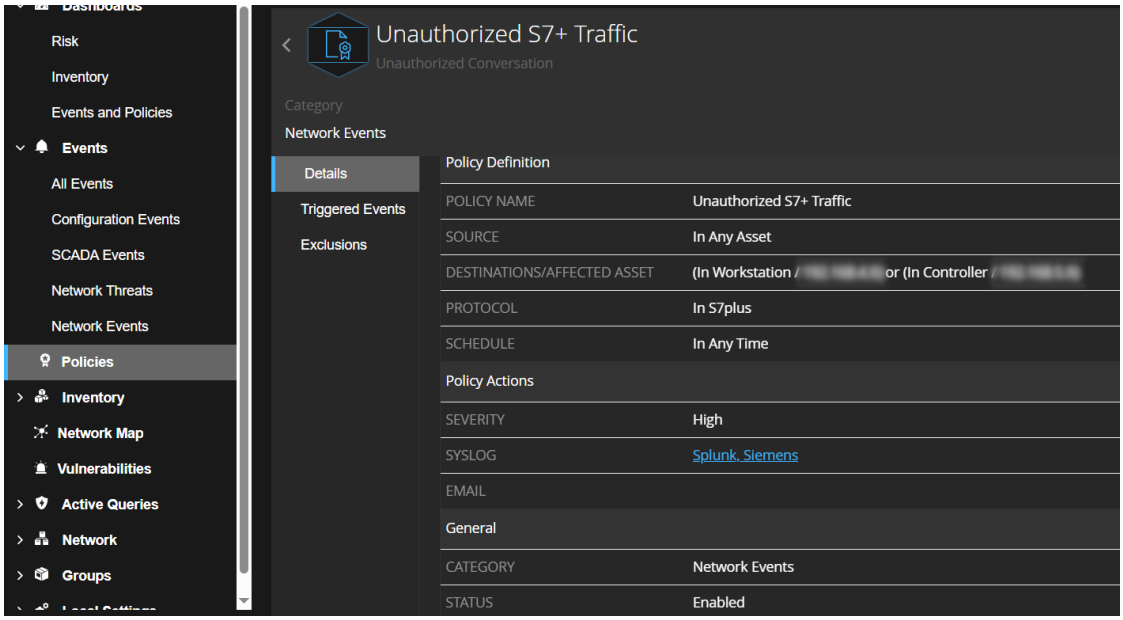


Figure 4-157: Tenable policy to track unauthorized S7+ traffic

[Return to Scenario C]

C.7.2 Creating Splunk dashboard for unauthorized Siemens traffic

Follow the instructions on C.4.6 on creating the dashboards. The following set of screenshots shows the dashboards created for this Scenario:

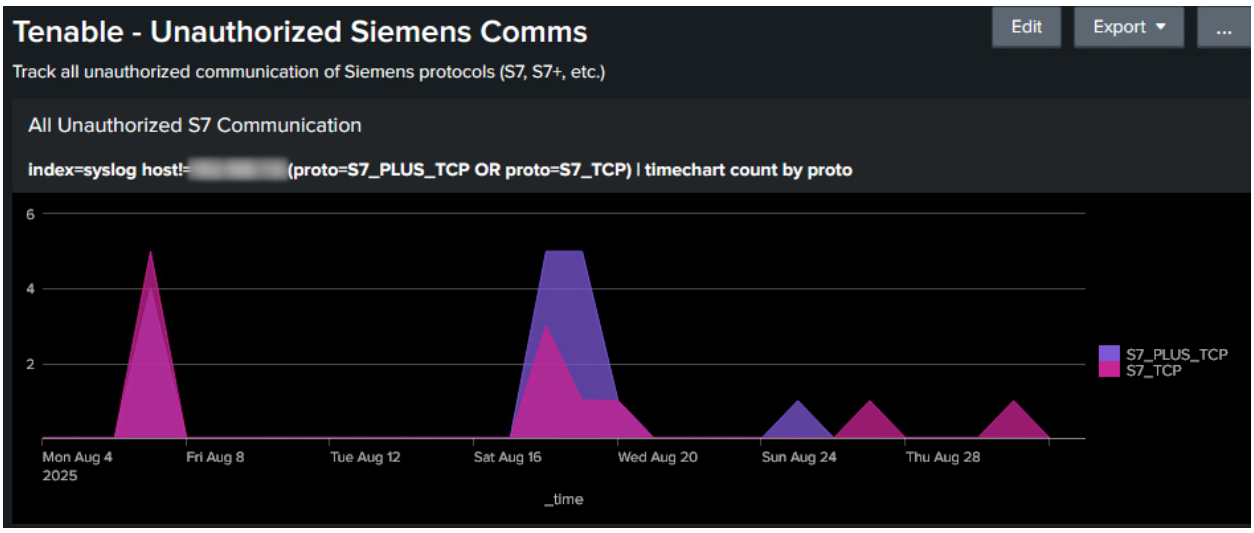
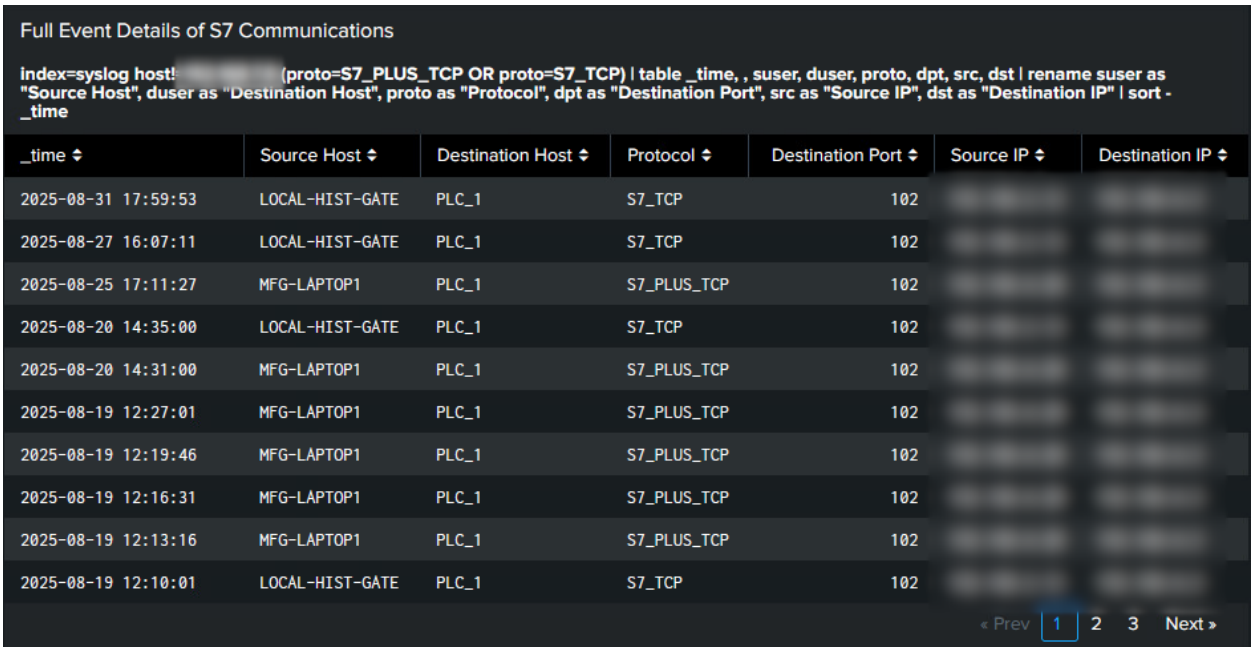
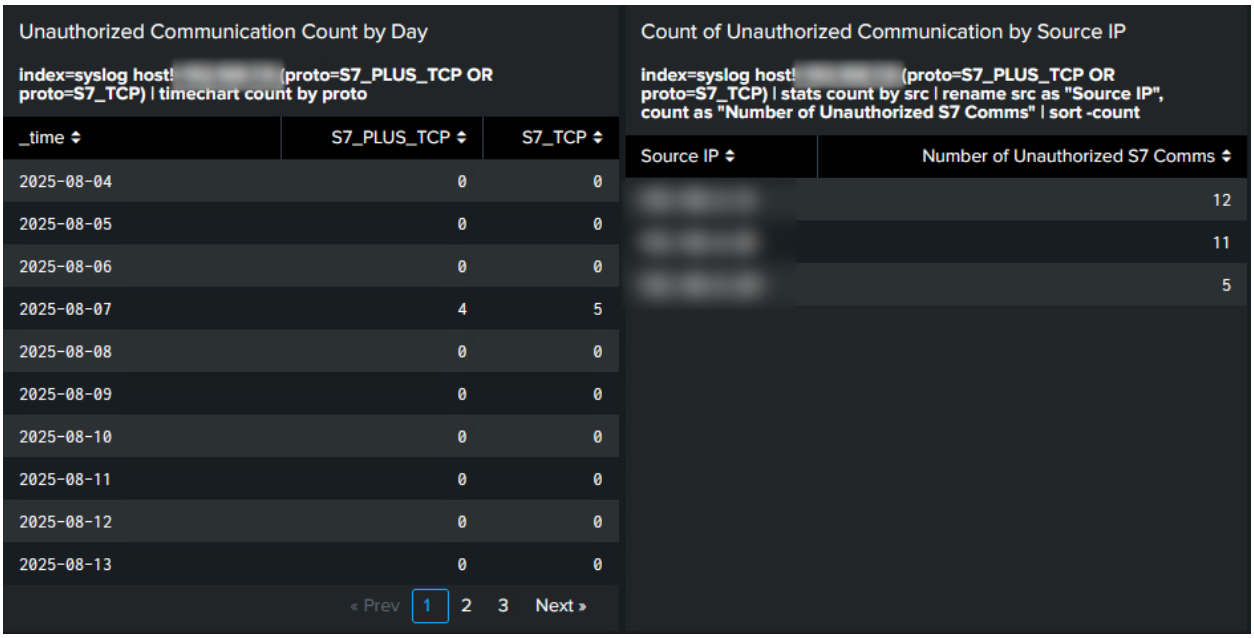


Figure 4-158: Splunk dashboard tracking unauthorized S7 and S7+ traffic



2301 **Figure 4-159: Splunk dashboard tracking unauthorized S7 and S7+ traffic**



2302 **Figure 4-160: Splunk dashboard tracking unauthorized S7 and S7+ traffic**

2303 [Return to Scenario C]

C.8 Scenario C: Technical Details – Response

C.8.1 View Tags in Data Historian

Inductive Automation's Ignition software is used as the data historian. Engineers can use their data Historian of choice to add tags to view when operational changes were made. During the investigation, tags are viewed in the data historian to track when the widgets change from one color to another.

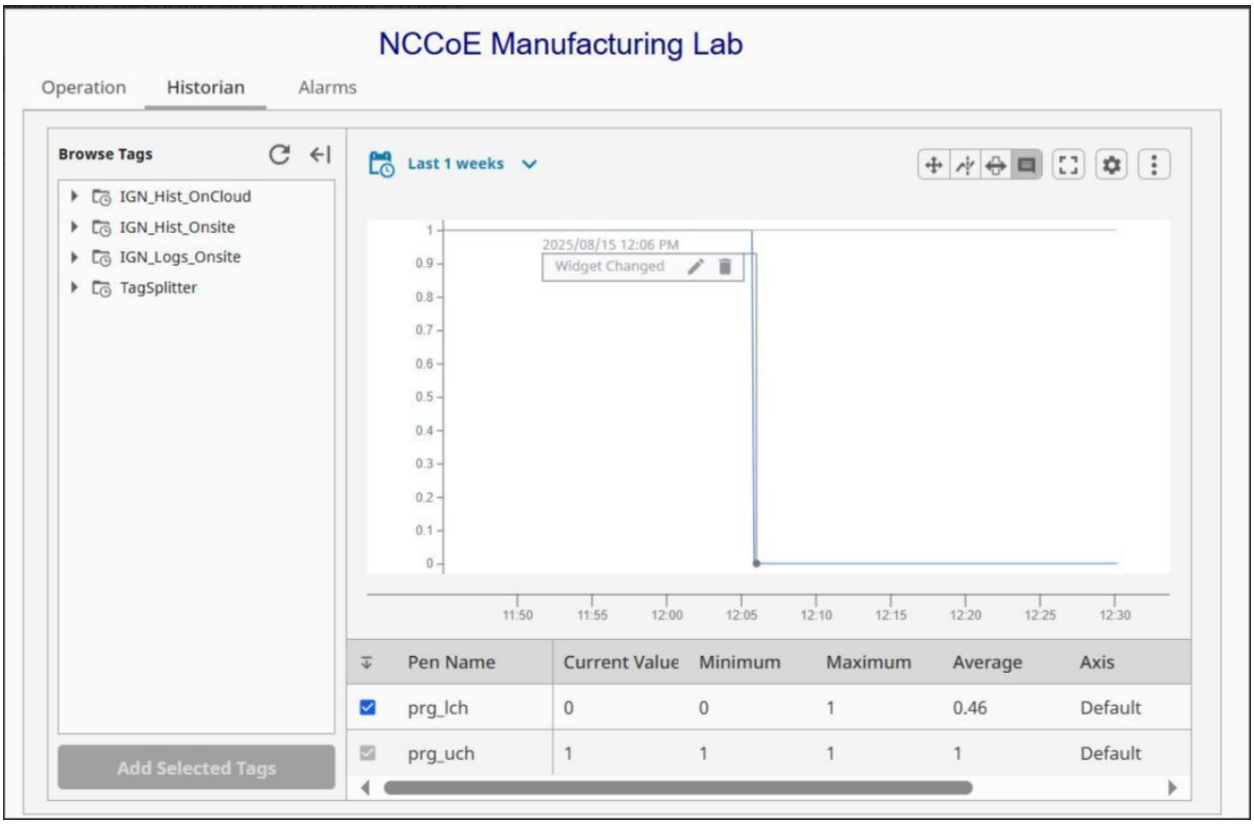
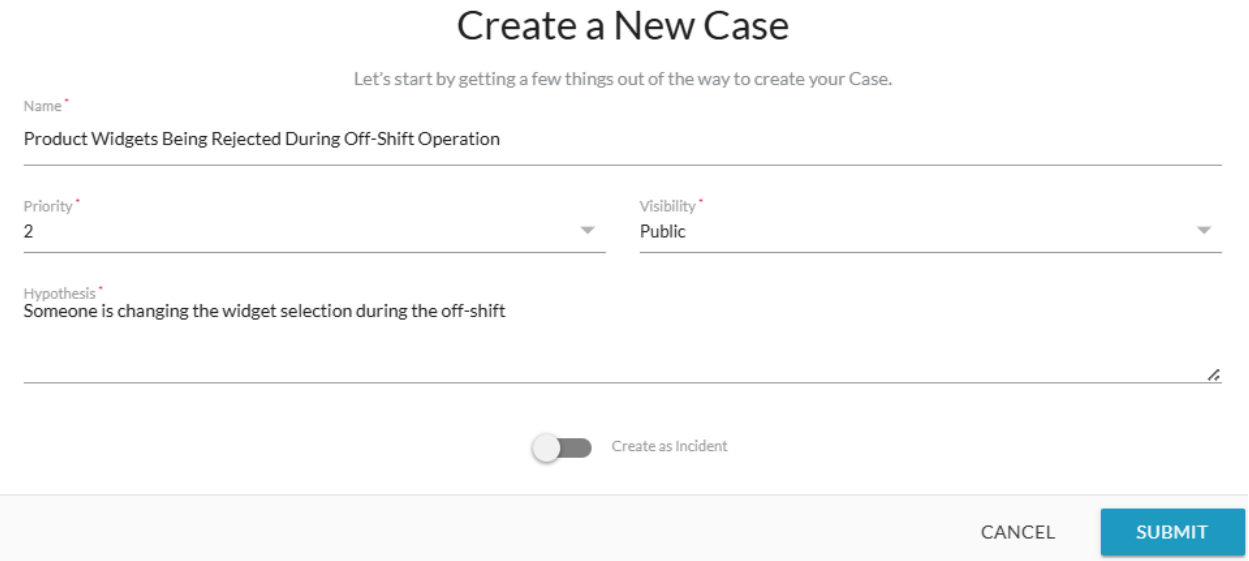


Figure 4-161: Enabling specific tags (PRG_LCH and PRG_UCH) in the data historian

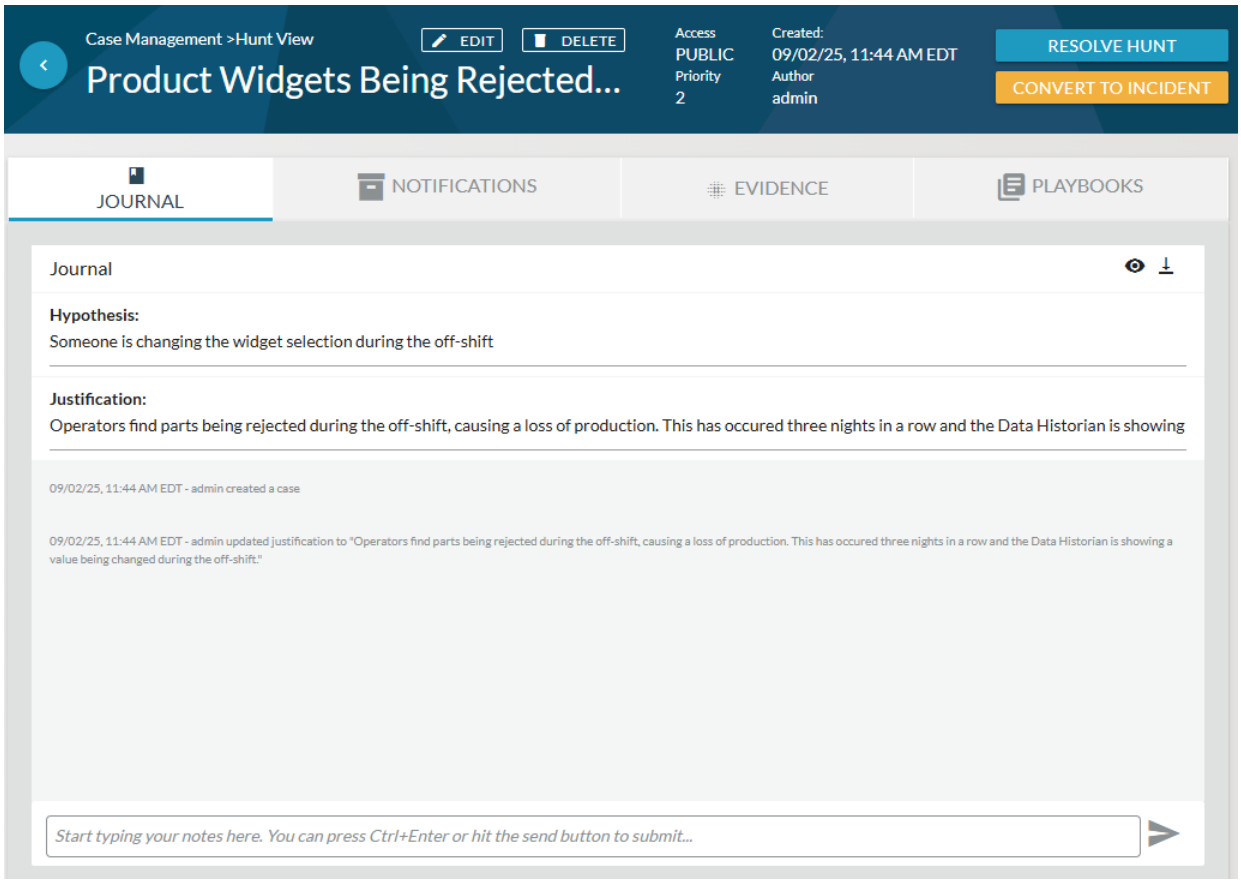
[Return to Scenario C]

C.8.2 Managing Dragos Tickets

Refer to Scenario A sections C.2.1, C.2.7, and C.3.3 on how to create Dragos tickets, add comments, and close tickets. This section will cover multiple steps for the entire investigation of Scenario C.



2314 **Figure 4-162: Creating a new ticket in Dragos**



2315 **Figure 4-163: Adding a justification for the ticket**

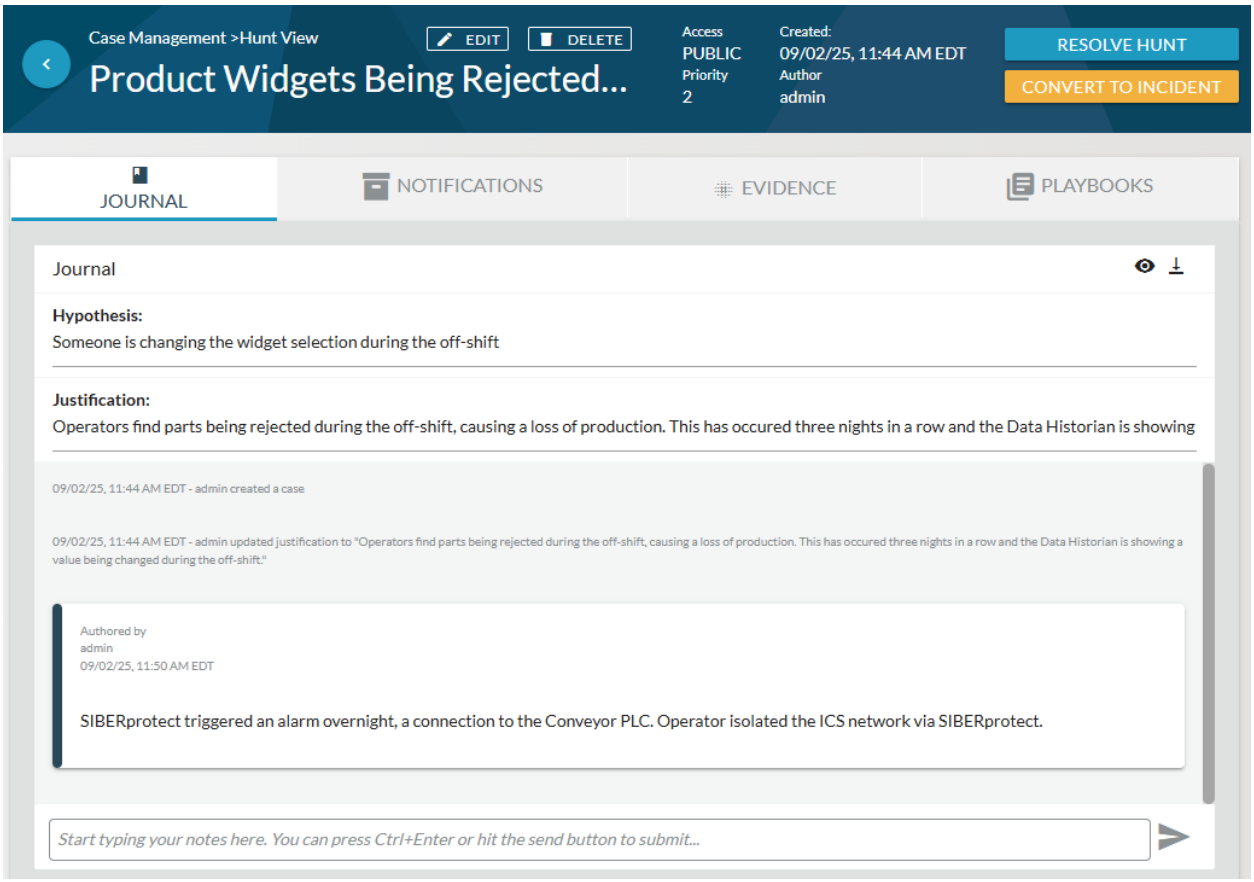
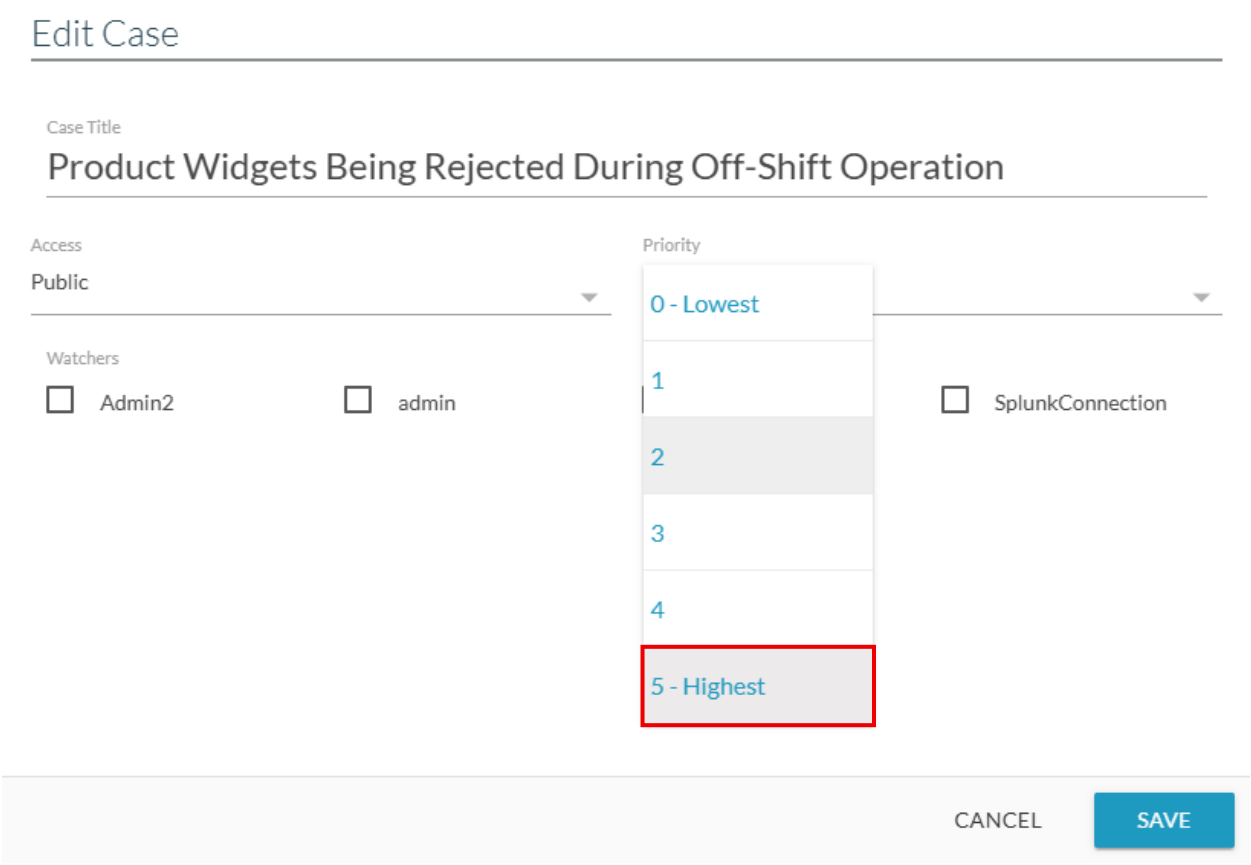
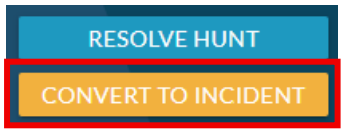


Figure 4-164: Updating the Dragos ticket to include the operator locking down the ICS network

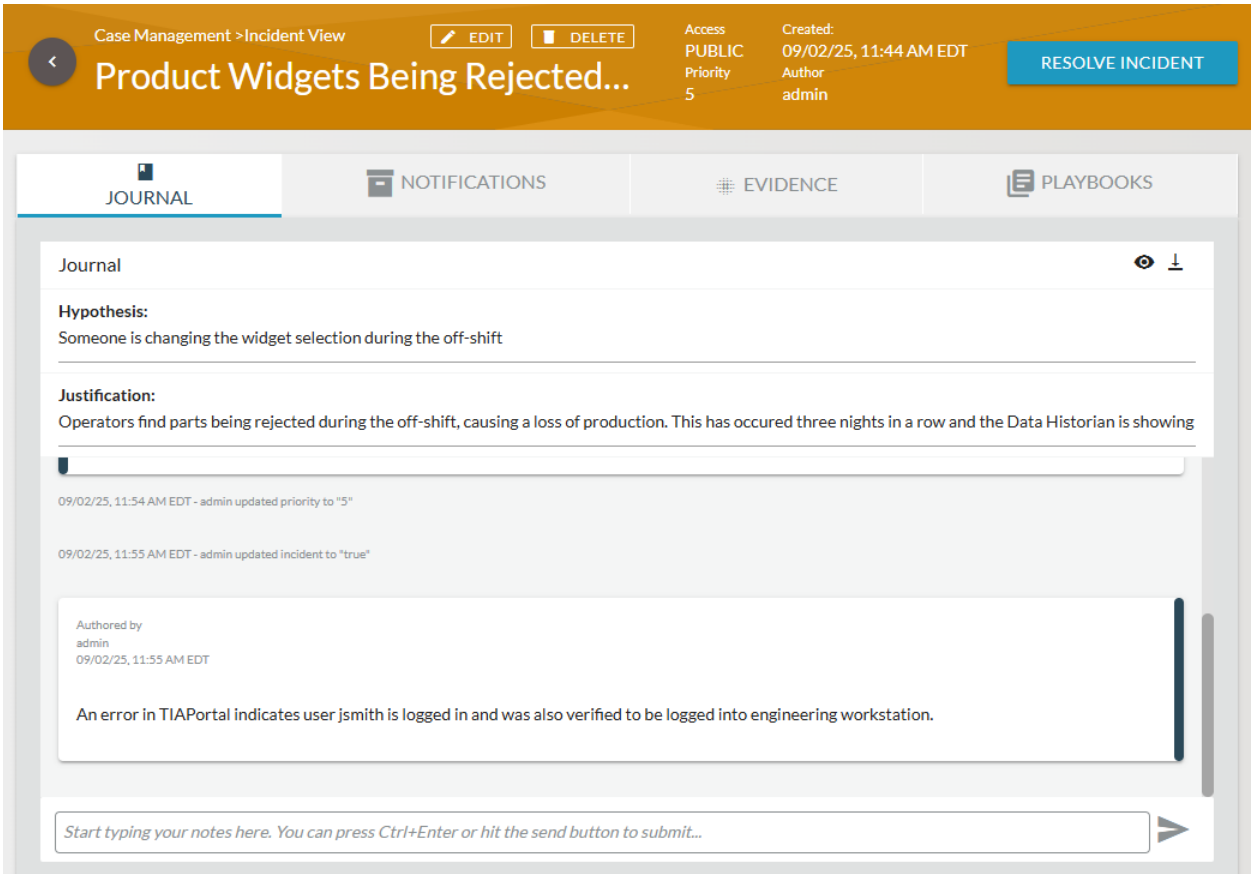
During the investigation of Scenario C, management upgraded the priority from 2 to 5 and converted from `hunt` status to `incident`.



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:

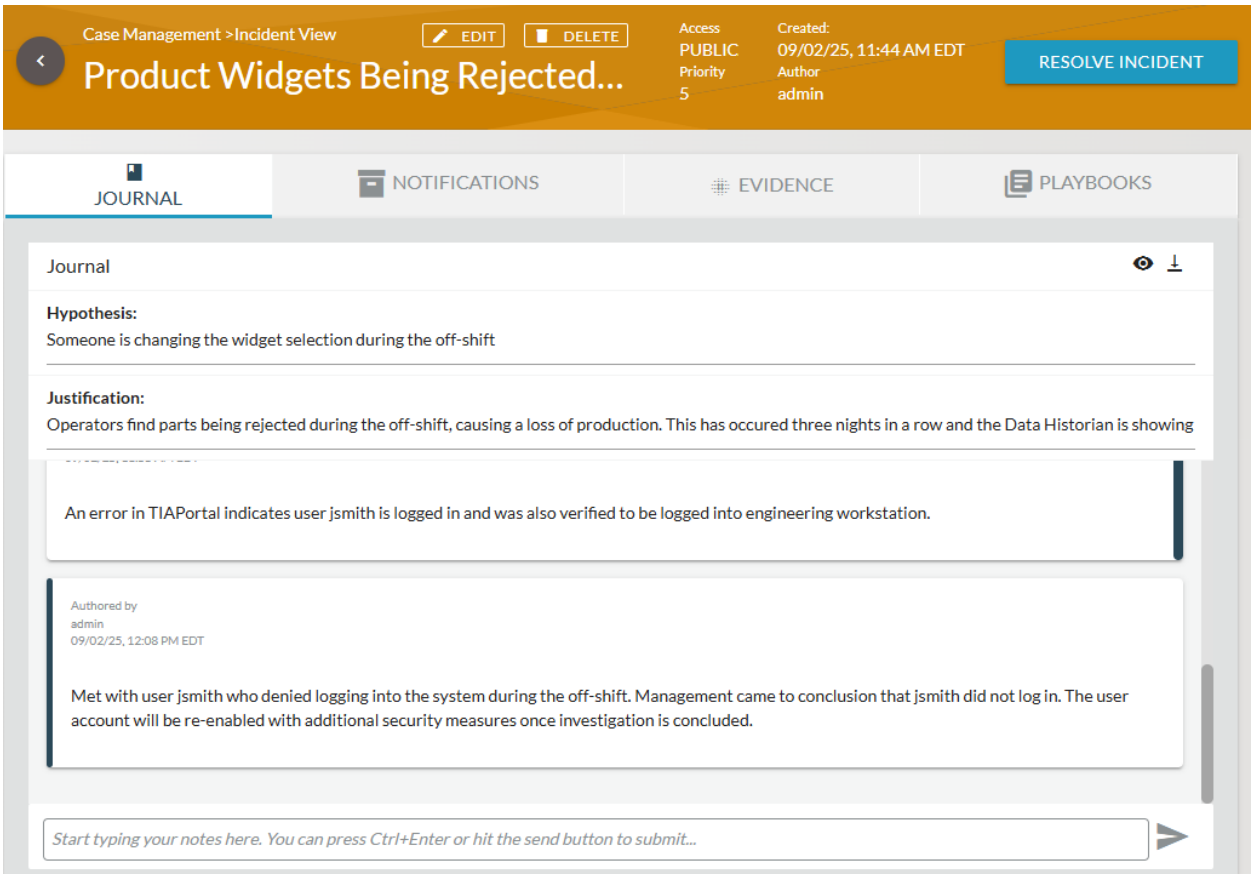


Figure 4-168: Adding additional details to the Dragos ticket about the jsmith user

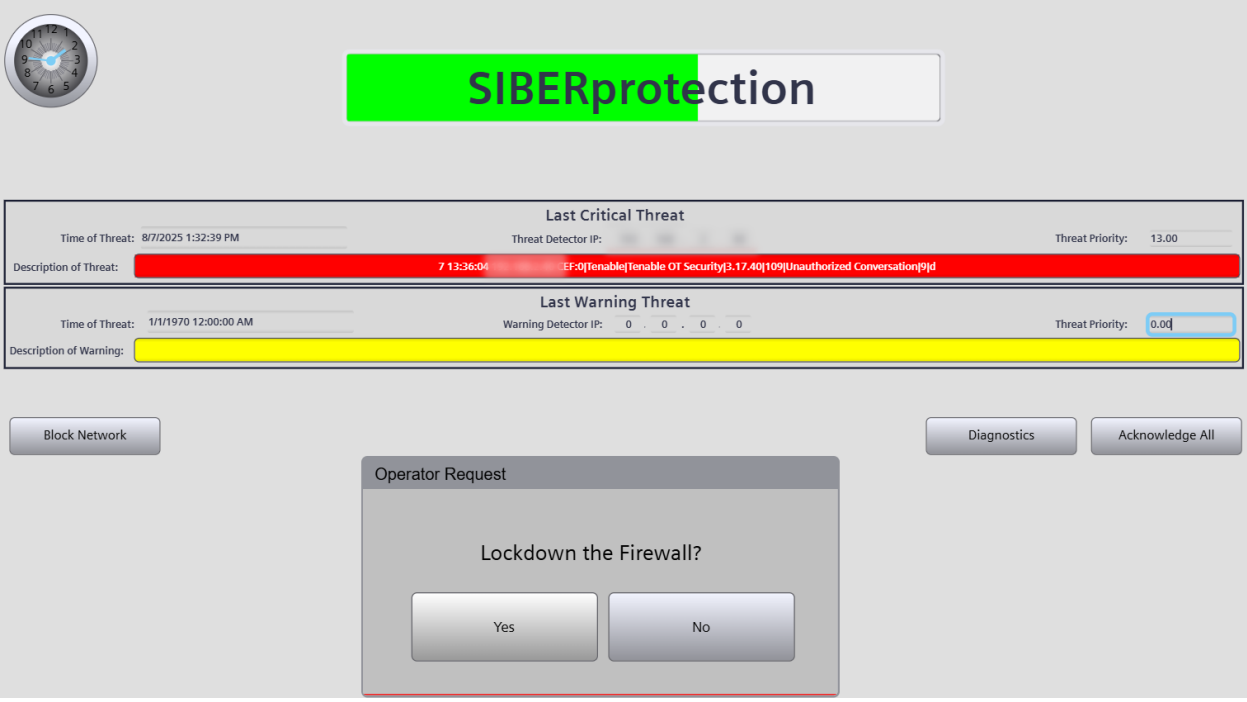
[Return to Scenario C - Initial Identification]

[Return to Scenario C - Technical Event Handling]

[Return to Scenario C - Cyber Incident Analysis and Response]

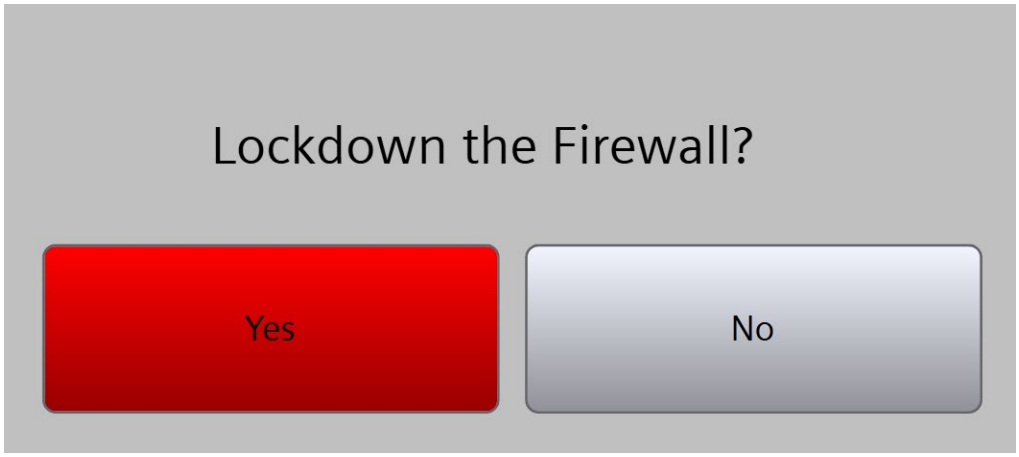
C.8.3 Isolate ICS Network using SIBERprotect

Tenable triggers an alert on the SIBERprotect Security HMI. The operator was informed by the engineer and analyst that a new alert may pop-up if a new system connects to the Conveyor PLC. When the alert pops-up on the Security HMI, the operator takes action to segment the physical components and 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.



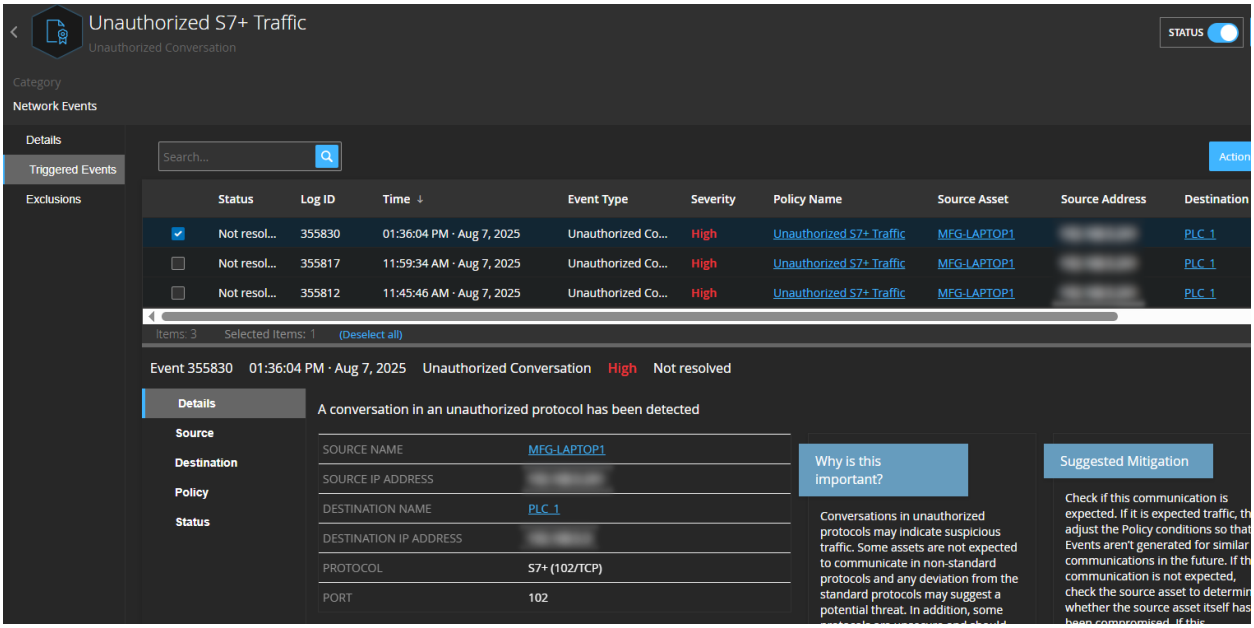
2334 **Figure 4-170: Operator lockdown (segment) selection**

2335 The conveyor and robot are segmented from the rest of the ICS network.

2336 [Return to Scenario C]

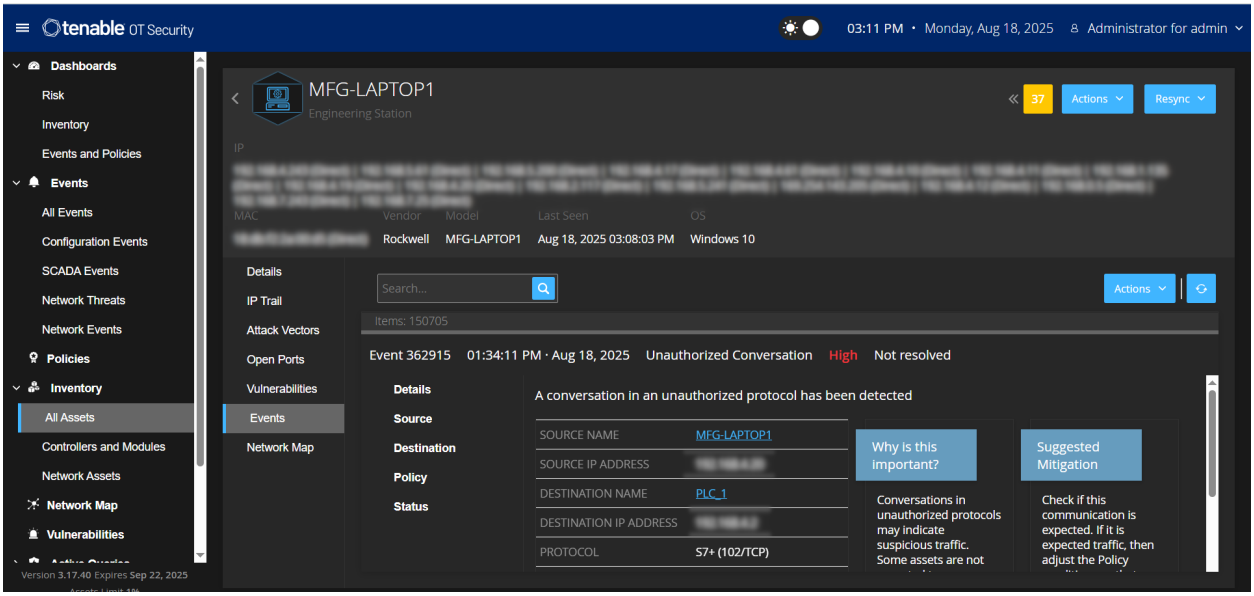
2337 C.8.4 Viewing policy violations in Tenable

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

recently been in the program and disconnected improperly. This helped identify the root cause of the incident.

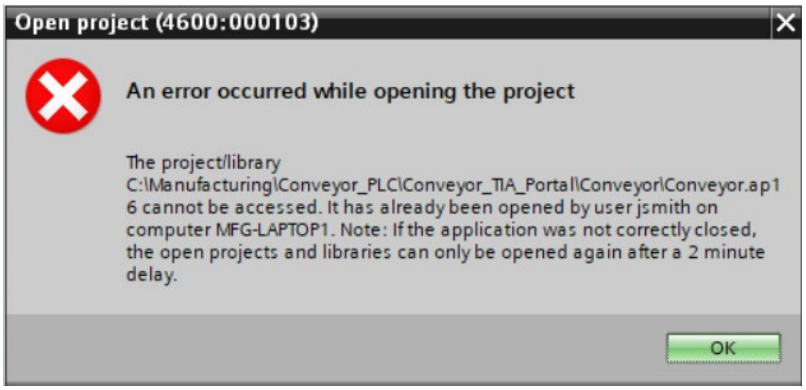


Figure 4-173: Error when opening the TIA Portal showing the user who was still logged into the system

[Return to Scenario C]

C.8.6 Windows Task Manager

Windows offers a Task Manager to identify processes, users, and other details about the system. In this scenario, Task Manager was used to verify that jsmith was recently logged into the machine and that their status is currently labeled as `Disconnected`.

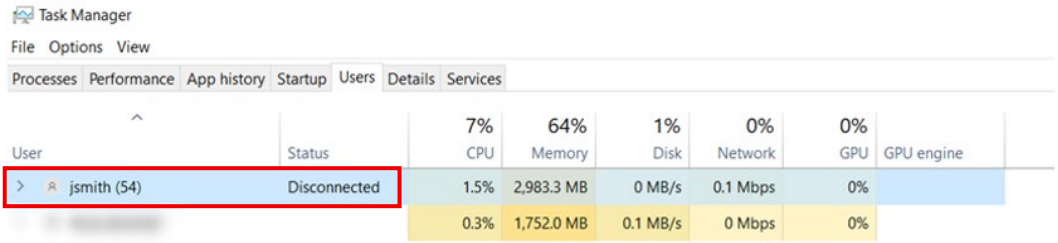
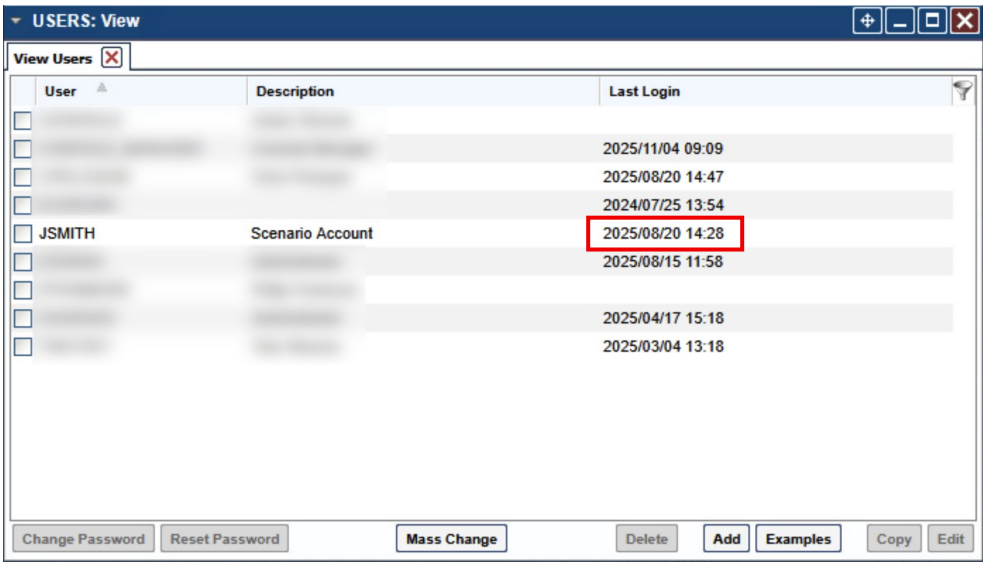


Figure 4-174: Task Manager in Windows showing the jsmith user was disconnected

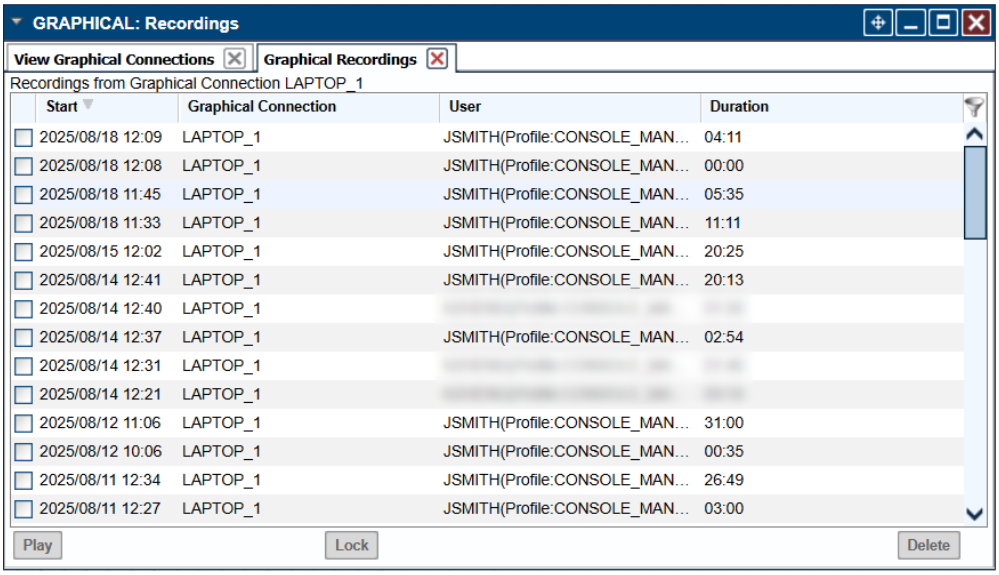
[Return to Scenario C]

C.8.7 Review ConsoleWorks Sessions for User Activity

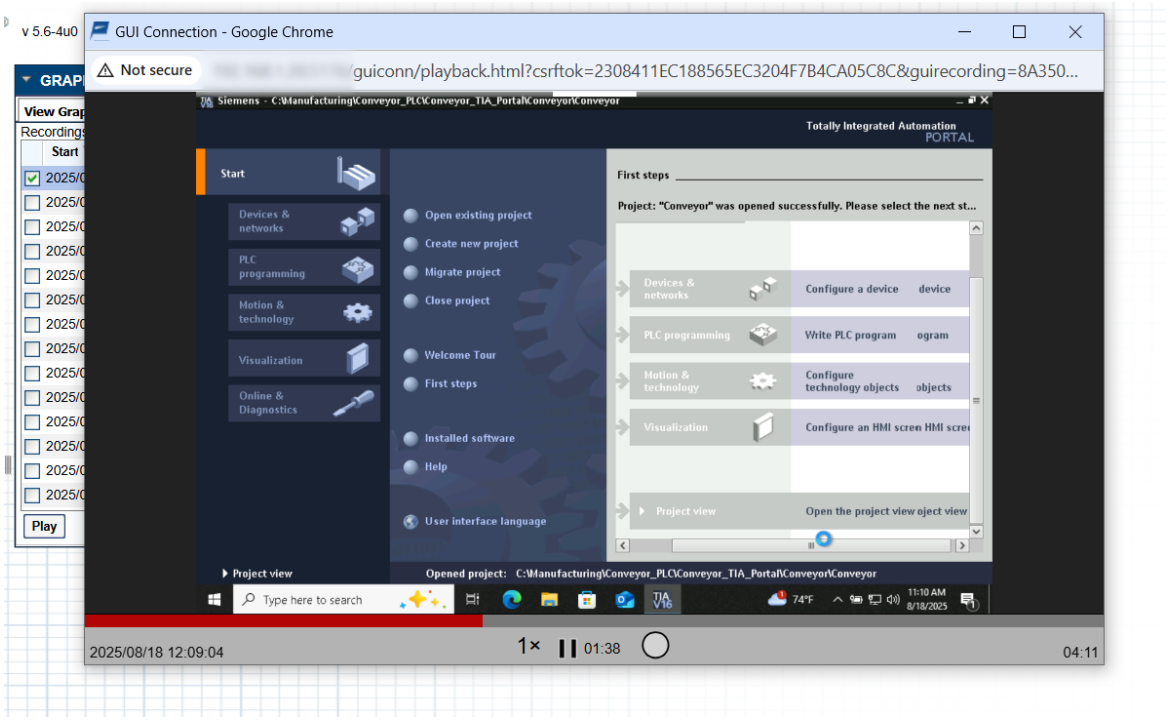
After discovering that a specific user was involved in an incident, ConsoleWorks can be used to view what the user was doing through a screen recording of the session:



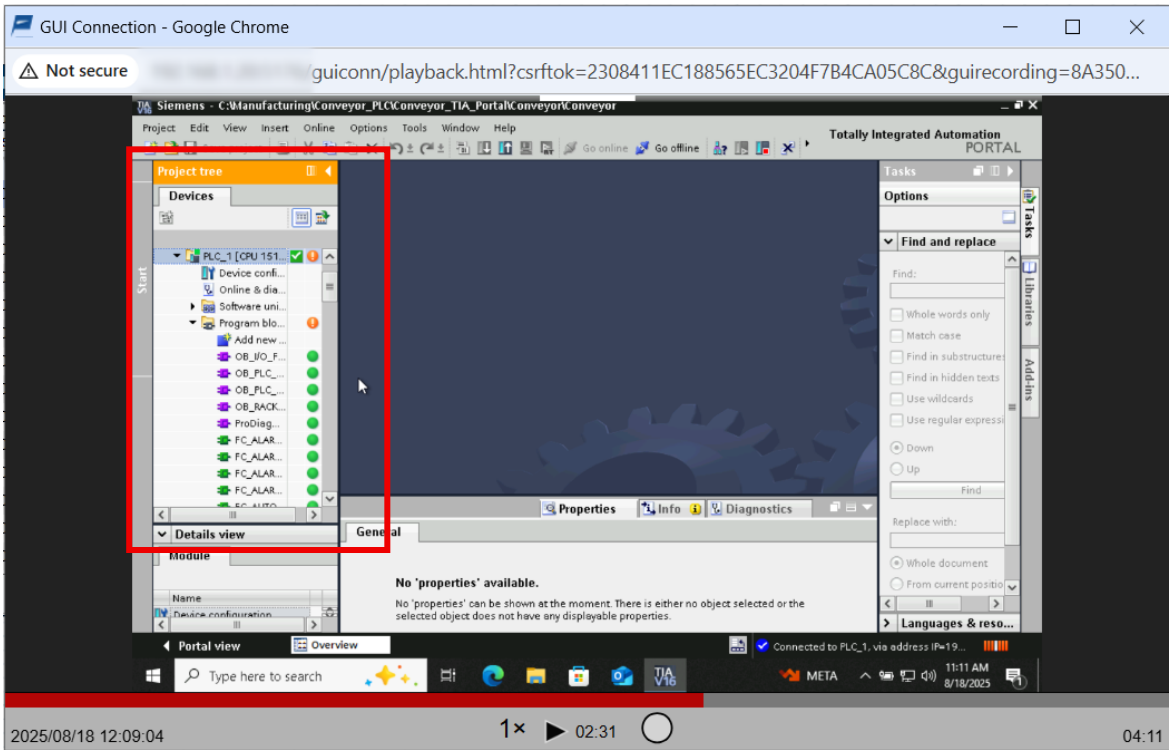
2361 **Figure 4-175: Show the user's last login**



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.

[Return to Scenario C]

C.9 Scenario C: Technical Details – Recovery

C.9.1 TIA Portal Reinstall

The IRT determined that the Engineering Workstation was compromised. The hardware is disconnected from the network and handed over for forensic analysis. The TIA Portal Software is installed on a new machine to allow for recovery of the PLC and continued operation while the investigation is ongoing. The software is downloaded from the Siemens website. Follow the instruction prompts to install TIA Portal with default settings as seen in the following screenshots.

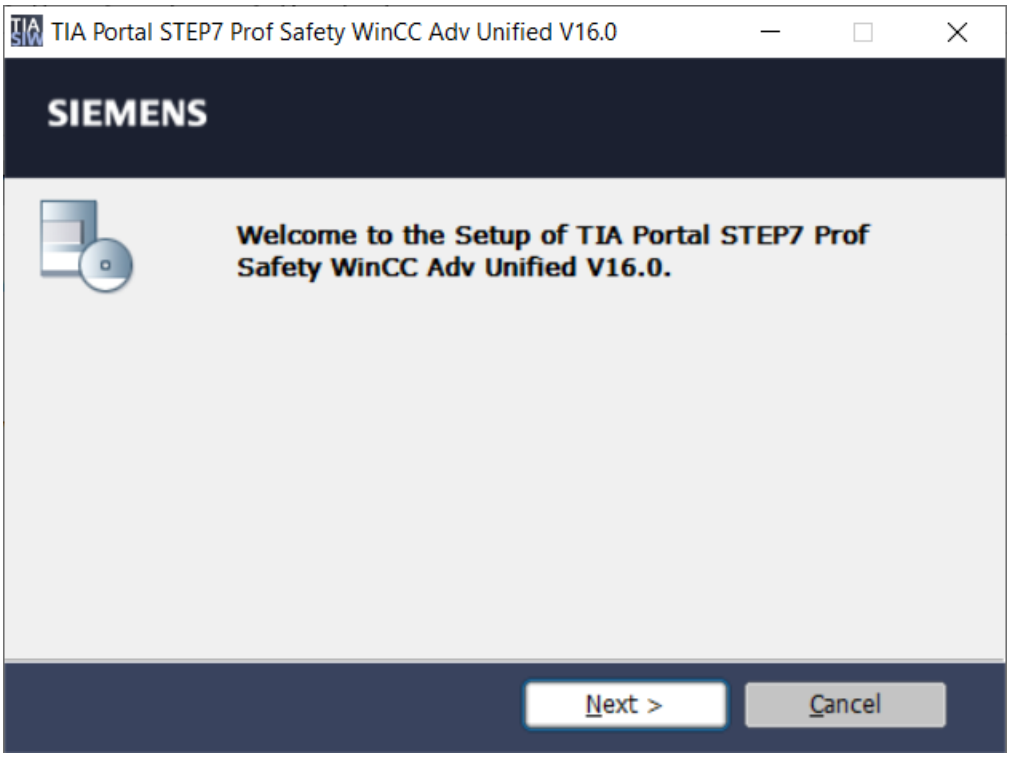
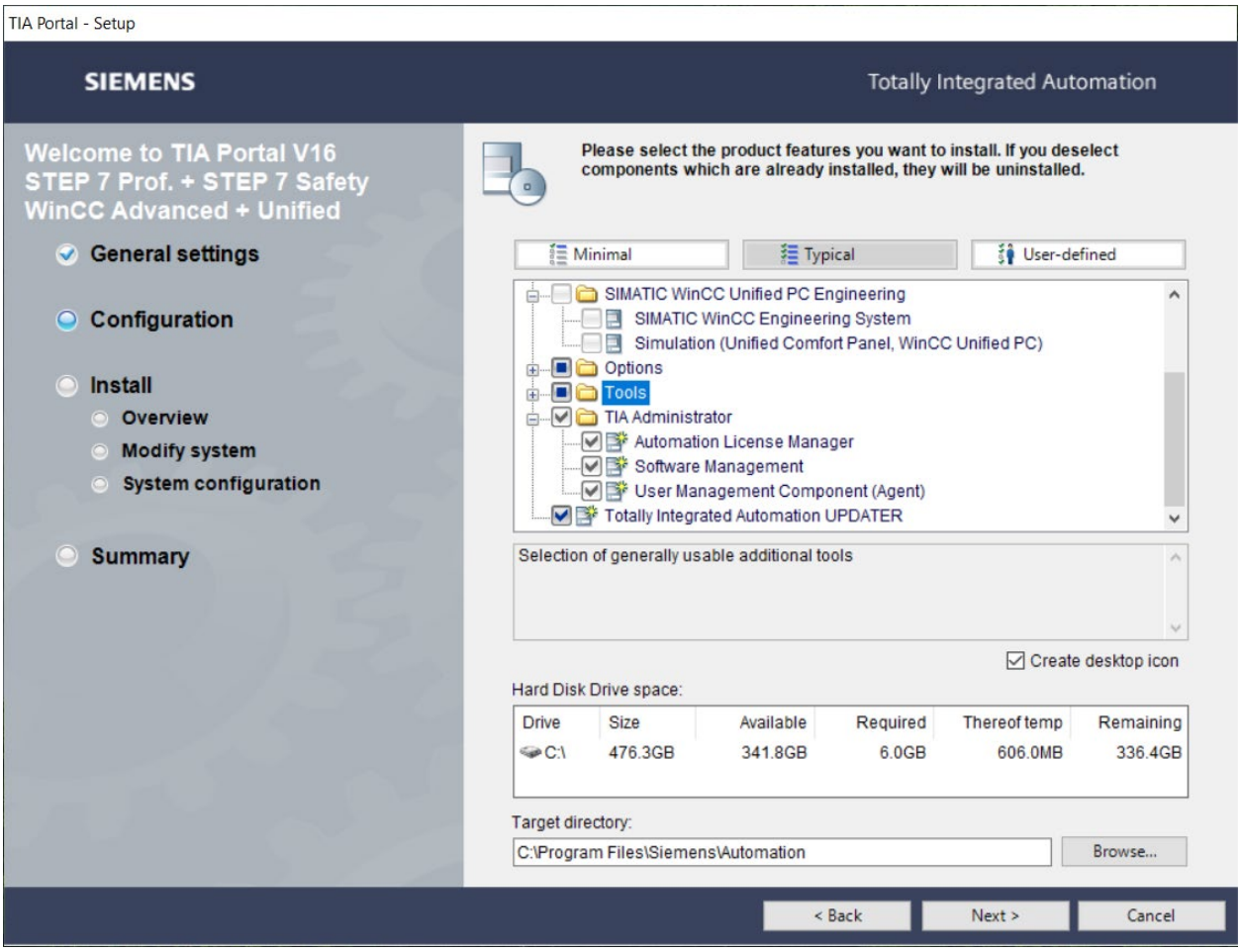


Figure 4-179: TIA Portal install navigation menu

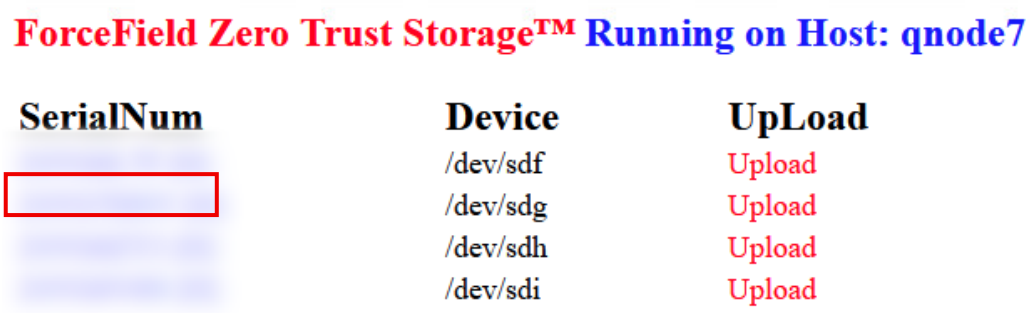


2376 **Figure 4-180: TIA Portal install settings**

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:



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
NIST_NCCoE_Logo.jpg	1	33.77K	20240129 16:25:42
SupervisorPLC.ACD	1	2.06M	20241212 12:34:48
SupervisorPLC.ACD.ASC	1	347	20241212 12:34:52
Conveyor_SLS_Nov16.zap16	1	6.13M	20241212 15:06:51
Conveyor_SLS_Nov16.zap16	2	8.97M	20241212 15:07:02
gripper_tutorial.urp	1	2.65K	20250220 10:44:27
main.urp	1	18.34K	20250220 10:44:27
main_new.urp	1	18.35K	20250220 10:44:28
main_old_july23.urp	1	18.51K	20250220 10:44:28
main-Old.urp	1	18.55K	20250220 10:44:29
Supervisor.ACD	1	1.96M	20250710 14:31:01
Program-Hashes.txt	1	98	20250819 11:02:14
Conveyor_20250819_1036.zap16	1	9.23M	20250819 11:31:40
Program-Hashes.txt	2	202	20250819 11:35:49
Conveyor_20250819_1137.zap16	1	5.46M	20250819 12:34:24
Conveyor_20250819_1137.zap16	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.

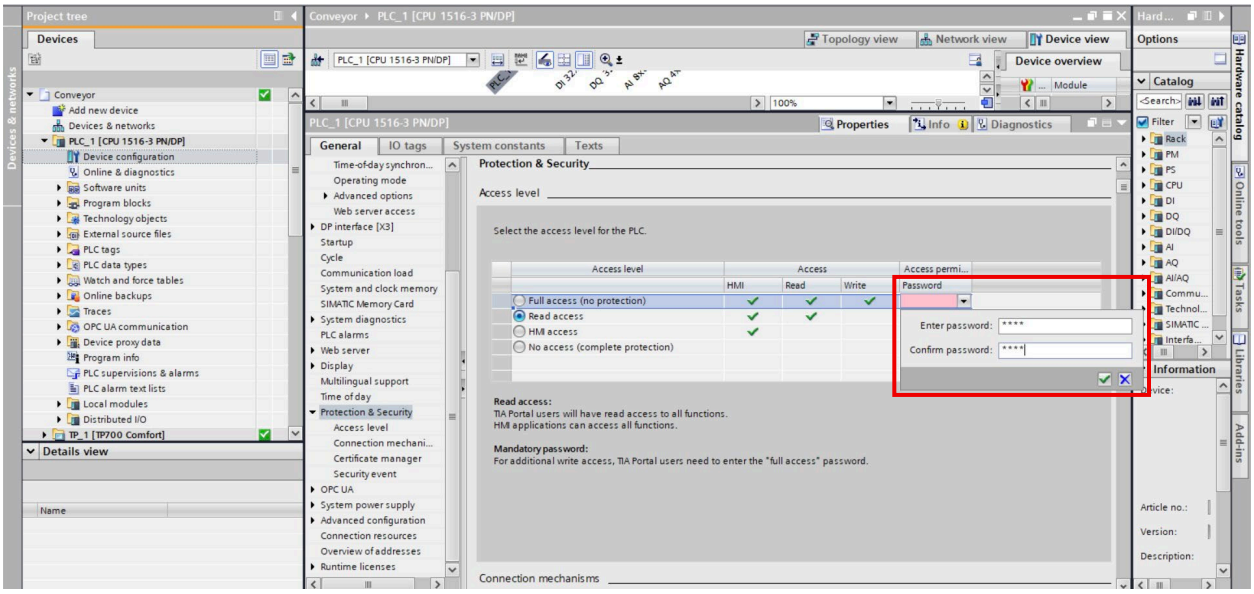
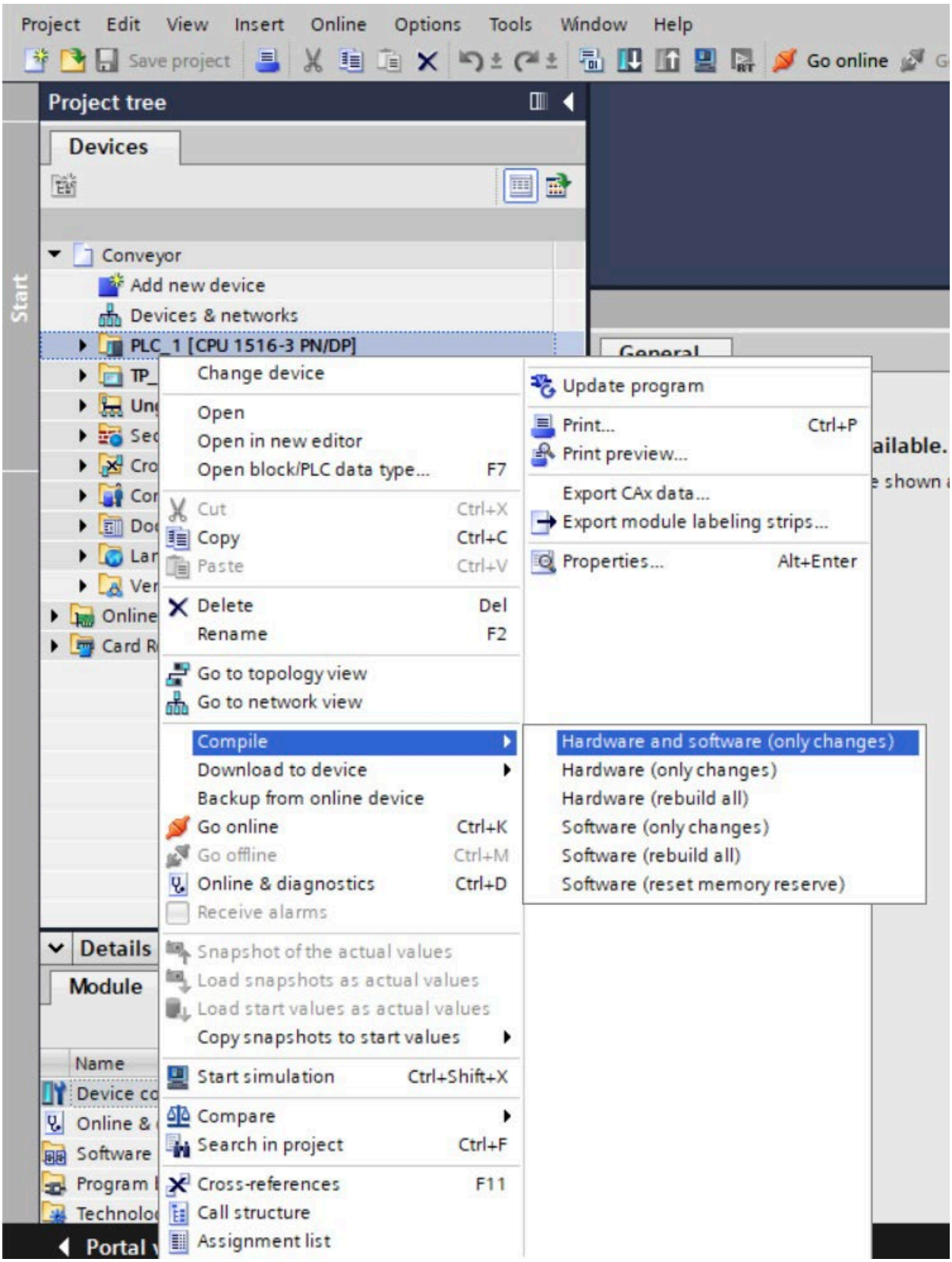
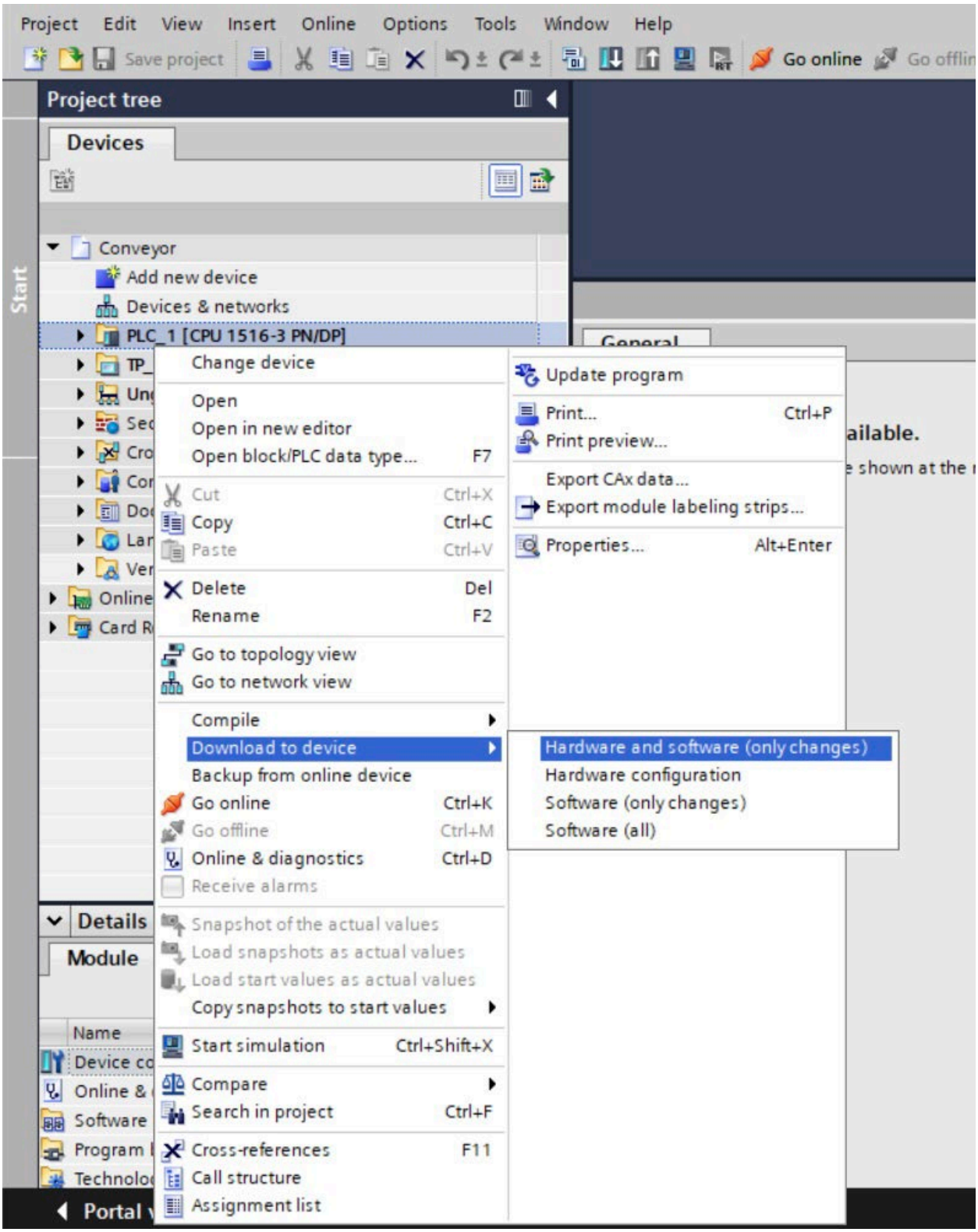


Figure 4-183: Adding a password to Siemens PLC in TIA Portal



2397 **Figure 4-184: Compile PLC program**



2398 **Figure 4-185: Download configuration to PLC**

2399 [Return to Scenario C]