NIST SPECIAL PUBLICATION 1800-10B

Protecting Information and System Integrity in Industrial Control System Environments:

Cybersecurity for the Manufacturing Sector

Volume B:
Approach, Architecture, and Security Characteristics

Michael Powell
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Michael Pease
Keith Stouffer
CheeYee Tang
Timothy Zimmerman
Engineering Laboratory
National Institute of Standards and Technology

Matthew Zopf
Strativia
Largo, Maryland

Joseph Brule
Chelsea Deane
John Hoyt
Mary Raguso
Aslam Sherule
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

FINAL

March 2022

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-10

The first draft of this publication is available free of charge from
https://www.nccoe.nist.gov/publications/practice-guide/protecting-information-and-system-integrity-industrial-control-system-draft

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.

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

National Institute of Standards and Technology Special Publication 1800-10B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-10B, 149 pages, March 2022, CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at manufacturing_nccoe@nist.gov.

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

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, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST *Cybersecurity Framework* (CSF) 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 more easily 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

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

The architecture and solutions presented in this guide are built upon standards-based, commercially available products, and represent some of the possible solutions. The solutions implement standard cybersecurity capabilities such as behavioral anomaly detection (BAD), application allowlisting (AAL), file

integrity-checking, change control management, and user authentication and authorization. The solution was tested in two distinct lab settings: a discrete manufacturing workcell, which represents an assembly line production, and a continuous process control system (PCS), which represents chemical manufacturing industries.

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

The security capabilities of the example solution are mapped to the *NIST Cybersecurity Framework*, the *National Initiative for Cybersecurity Education Framework*, and *NIST Special Publication 800-53*.

KEYWORDS

Application allowlisting; behavioral anomaly detection; file integrity checking; firmware modification; industrial control systems; manufacturing; remote access; software modification; user authentication; user authorization.

ACKNOWLEDGEMENTS

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

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

Name	Organization
Josh Carlson	Dragos
Alex Baretta	Dragos

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

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

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.

PATENT DISCLOSURE NOTICE

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Contents

List of Figures

List of Tables

1 Summary

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

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

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

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

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

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

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

- destructive malware
- insider threats
- unauthorized software
- unauthorized remote access

- loss of historical data
- anomalous network traffic
- unauthorized modification of systems

This document contains the following sections:

Section 1, Summary, presents the challenges addressed by the NCCoE project, with a look at the solutions demonstrated to address the challenge, as well as benefits of the solutions.

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

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

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

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

Section 6, Future Build Considerations, identifies additional areas that should be reviewed in future practice guides.

Section Appendix D, Scenario Execution Results, describes, in detail, the test results of the scenarios, including screenshots from the security products captured during the tests.

1.1 Challenge

Manufacturing organizations that rely on ICS to monitor and control physical processes face risks from malicious and non-malicious insiders along with external threats in the form of increasingly

sophisticated cyber attacks. A compromise to system or information integrity may very well pose a significant threat to human safety and can adversely impact an organization's operations, resulting in financial loss and harm production for years to come.

Manufacturing organizations may be the targets of malicious cyber actors or may be incidentally impacted by a broader malware event such as ransomware attacks. ICS components remain vulnerable to cyber attacks for numerous reasons, including adoption and integration of enhanced connectivity, remote access, the use of legacy technologies, flat network topologies, lack of network segmentation, and the lack of cybersecurity technologies (e.g., anti-virus, host-based firewalls, encryption) typically found on IT systems.

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

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

1.2 Solution

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

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

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

- application allowlisting (AAL)
- behavior anomaly detection (BAD)

- file integrity
- user authentication and authorization
- remote access

1.2.1 Relevant Standards and Guidance

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

- NIST Special Publication (SP) 800-167: *Guide to Application Whitelisting* [2]
- Department of Homeland Security, *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance* [3]
- Executive Order no. 13636: *Improving Critical Infrastructure Cybersecurity* [4]
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity* [5]
- NIST Interagency Report (NISTIR) 8219: *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection* [6]
- NIST Internal Report (NISTIR) 8183: *Cybersecurity Framework Manufacturing Profile* [7]
- NISTIR 8089: *An Industrial Control System Cybersecurity Performance Testbed* [8]
- NIST SP 800-53 Rev. 5: *Security and Privacy Controls for Federal Information Systems and Organizations* [9]
- NIST SP 800-181: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* [10]
- NIST Special Publication 1800-25: *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events* [11]
- NIST Interagency or Internal Report 7298 Rev 3: *Glossary of Key Information Security Terms* [12]
- U.S.-Canada Power System Outage Task Force [13]
- NIST SP 800-82 Rev. 2: *Guide to Industrial Control Systems (ICS) Security* [14]

1.3 Benefits

This NCCoE practice guide can help organizations:

- mitigate cybersecurity risk
- reduce downtime for operations
- provide a reliable environment that can detect cyber anomalies
- respond to security alerts through automated cybersecurity-event products

- develop and execute an OT cybersecurity strategy for which continuous OT cybersecurity monitoring is a foundational building block
- implement current cybersecurity standards and best practices

2 How to Use This Guide

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

This guide contains three volumes:

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

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

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

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

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

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

- Section 3.4.4, which maps the security characteristics of the example solutions to cybersecurity standards and best practices

IT and OT professionals who want to implement an approach like this will find the whole practice guide useful, particularly the how-to portion, NIST SP 1800-10C, which provides step-by-step details to replicate all, or parts of the example solutions created in our lab. Volume C does not re-create the

product manufacturers' documentation, which is generally widely available. Rather, Volume C shows how we integrated the products together to create an example solution.

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

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

This document provides initial guidance. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to manufacturing_nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

3 Approach

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

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

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

3.1 Audience

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

3.2 Scope

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

The scope of this project is to assist organizations in maintaining the integrity of information and systems by:

- Preventing execution or installation of unapproved software
- preventing unauthorized access to systems and information
- detecting anomalous behavior on the network that affects system or information integrity
- detecting hardware, software, or firmware modification

Organizational cybersecurity policies and procedures, as well as response and recovery functions, are out of scope for this document. The scenarios and security capabilities covered in this practice guide

should be part of a comprehensive OT/ICS security plan that addresses the NIST *Cybersecurity Framework* Protect and Detect functions.

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

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

3.3 Assumptions

This project makes the following assumptions:

- Each solution is comprised of several readily available products. The modularity of the solutions might allow organizations to consider swapping one or more products, depending on their specific requirements.
- A cybersecurity stakeholder might implement all or part of a solution in a manner that is compatible with their existing environment.
- Organizations will test and evaluate the compatibility of the solutions with their ICS devices prior to production implementation and deployment. Response and recovery functions are beyond the scope of this guide.
- Events detected by the security tools are passed on to the security operation team for further action.

3.4 Risk Assessment

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

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

3.4.1 Threats

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

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

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

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

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

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

3.4.2 Vulnerabilities

A vulnerability as defined in NISTIR 7298, Glossary of Key Information Security Terms [12] is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

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

NIST SP 800-82 categorizes ICS vulnerabilities into the following categories with examples [14]:

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

The first step in understanding the vulnerabilities and securing an organization's ICS infrastructure is knowledge of deployed assets and their interfaces. The knowledge of an asset's location and baselining

its behavior enable detection of anomalous behavior, via network monitoring, that may be the result of a successfully exploited vulnerability. The ability to reliably detect changes in asset behavior and knowing an asset's attributes are key in responding to potential cybersecurity incidents.

3.4.3 Risk

The risk to an organization is the intersection of:

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

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

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

3.4.4 Security Control Map

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

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

For more information on the security controls, the *NIST SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations* is available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

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

Table 3-1 Security Control Map

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	IA-2, IA-4, IA-5, IA-7, IA-9, IA-10, IA-12	SP-DEV-001, OM-ADM-001, OV-PMA-003
		PR.AC-3: Remote access is managed	AC-17, AC-19	SP-SYS-001, OM-ADM-001, PR-INF-001
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-14, AC-24	OM-STS-001, OM-ADM-001
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	AC-14, IA-2, IA-4, IA-5	OM-STS-001, OM-ADM-001
	Data Security (PR.DS): Information and records	PR.DS-1: Data-at-rest is protected	MP-7, SC-28	SP-DEV-002, SP-SYS-002, OM-DTA-001

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
	(data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	OM-DTA-001
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-4: Backups of information are conducted, maintained, and tested	CP-9	SP-SYS-001, SP-SYS-002, OM-DTA-001
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	MA-3	SP-SYS-001, OM-ANA-001
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	MA-4	SP-SYS-001, OM-ANA-001
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	CM-2, SI-4	SP-ARC-001, PR-CDA-001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	CA-7, SI-4 RA-5	OM-DTA-002, PR-CDA-001, CO-OPS-001
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	CA-7, SI-4	OM-DTA-002, PR-CDA-001,

Function	Category	Subcategory	NIST SP 800-53 Rev. 5	NIST SP 800-181 Rev. 1 (NICE Framework) Work Roles
				PR-CIR-001, CO-OPS-001
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	AU-12, CA-7, CM-3, SC-7, SI-4	OM-NET-001, PR-CDA-001, PR-CIR-001
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AU-12, CA-7, CM-11	PR-CDA-001, AN-TWA-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, SI-4	PR-CDA-001, PR-CIR-001, AN-TWA-001, CO-OPS-001

3.5 Technologies

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

Table 3-2 Products and Technologies

Capability	Product	Function	NIST *Cybersecurity Framework* Subcategories Mapping
AAL	VMWare Carbon Black		

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

Capability	Product	Function	NIST *Cybersecurity Framework* Subcategories Mapping
User Authentication and User Authorization	TDi ConsoleWorks	Provides a central location for managing password changes. Provides a security perimeter for all devices within the OT environment.	PR.AC-1, PR.AC-3, PR.AC-4, PR.MA-1, PR.MA-2, DE.AE-2, DE.AE-3, DE.CM-3, DE.CM-7
	Dispel		
Remote Access	Dispel	Provides secure remote access. Records and logs user activity for each session.	PR.AC-3, PR.MA-2, DE.AE-2, DE.CM-7
	Cisco AnyConnect (Note: This component was not provided by collaborator. It was a component of the existing lab infrastructure.)		

4 Architecture

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

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

This modular approach, focusing on specific products and outcomes, demonstrates how solutions might be tailored to the operating environment. Table 4-1 provides a summary of the four builds and how the products were distributed across them. Detailed descriptions of the installation, configuration, and integration of these builds are included in Volume C of this guide.

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

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

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

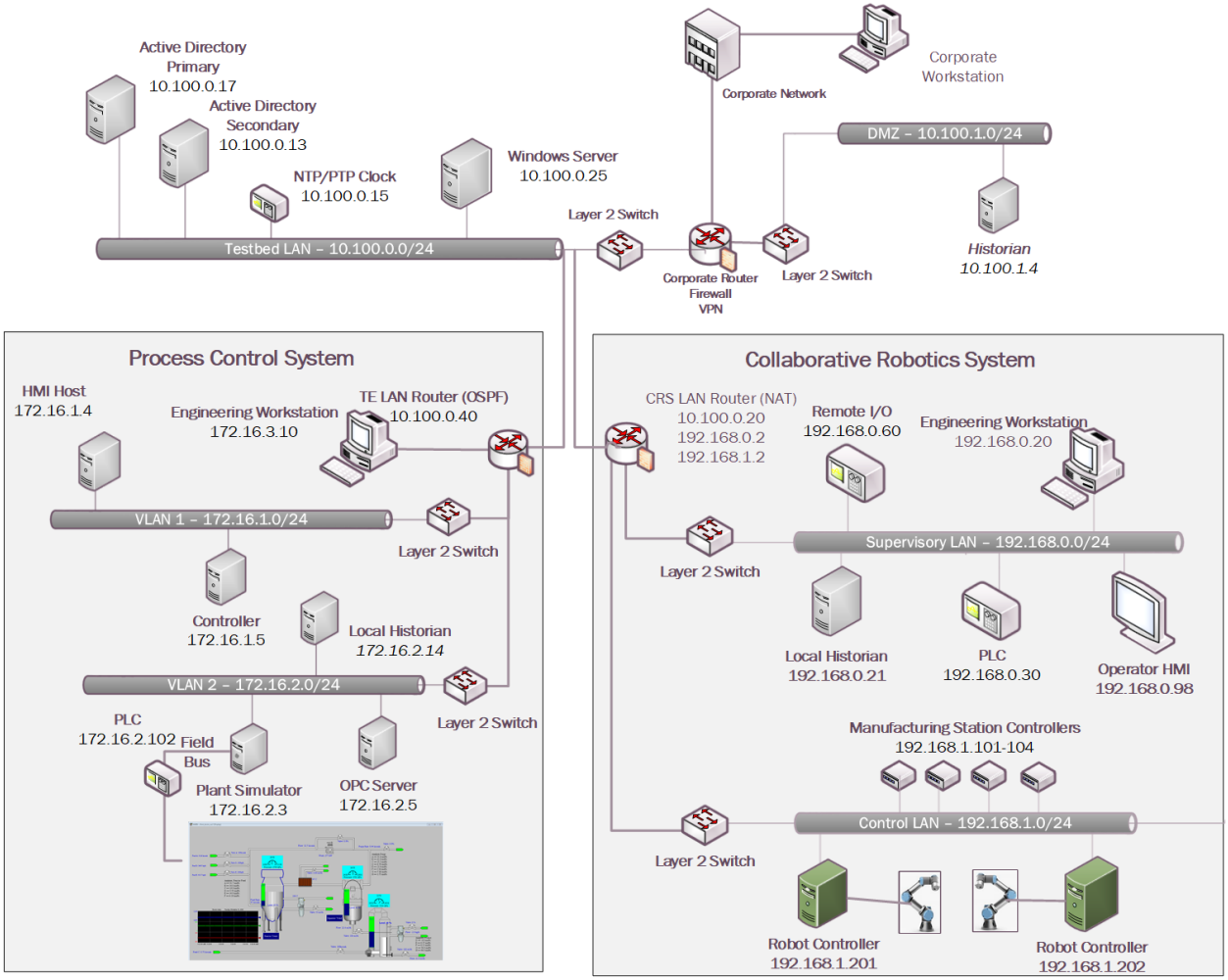
4.1 Manufacturing Process and Control System Description

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

4.2 Cybersecurity for Smart Manufacturing Systems Architecture

Figure 4-1 depicts a high-level architecture for the demonstration environment consisting of a testbed local area network (LAN), a demilitarized zone (DMZ), the PCS, and the CRS. The environment utilizes a combination of physical and virtual systems and maintains a local network time protocol server for time synchronization. Additionally, the environment utilizes virtualized Active Directory servers for domain services. The tools used to support information and system integrity are deployed and integrated in the DMZ, Testbed LAN, PCS, and CRS according to vendor recommendations and standard practices as described in the detailed sections for each build.

Figure 4-1: CSMS Network Architecture



4.3 Process Control System

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

The PCS emulates the Tennessee-Eastman (TE) chemical reaction process. The TE problem, presented by Downs and Vogel [15], is a well-known process-control problem in continuous chemical manufacturing. A control loop is required in the PCS to maintain a steady and stable chemical production. The PCS

presents a real-world scenario in which a cybersecurity attack could represent a real risk to human safety, environmental safety, and economic viability. This allows the PCS to be used to assess the impact of cybersecurity attacks on the continuous process manufacturing environment.

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

Figure 4-2 Simplified Tennessee Eastman Process Model

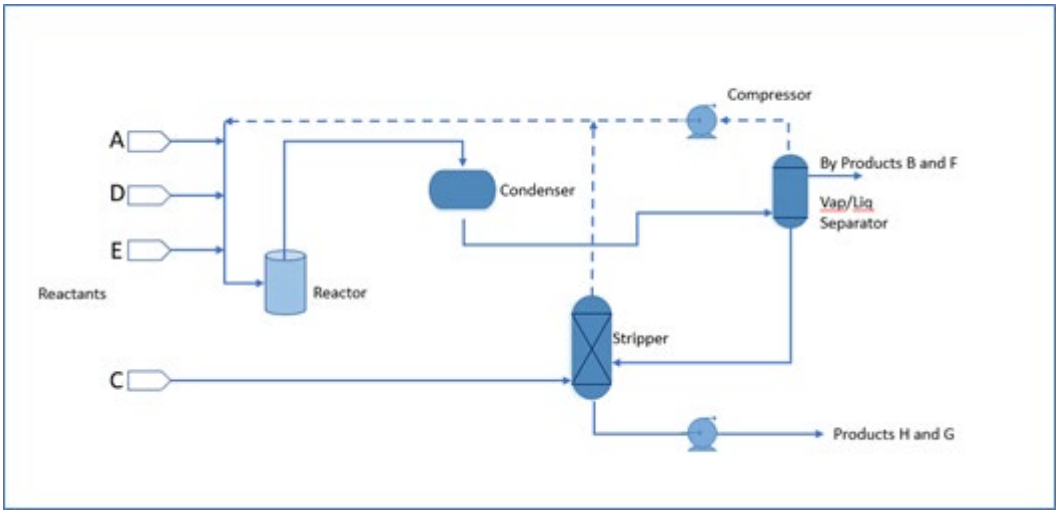
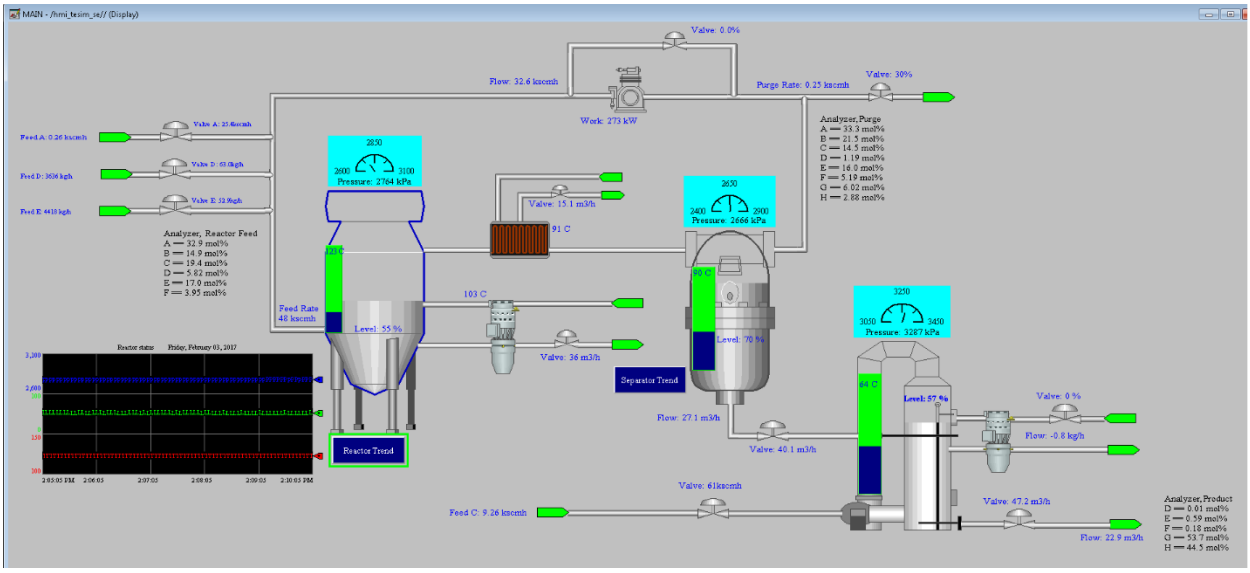


Figure 4-3 HMI Screenshot for the PCS Showing the Main Components in the Process

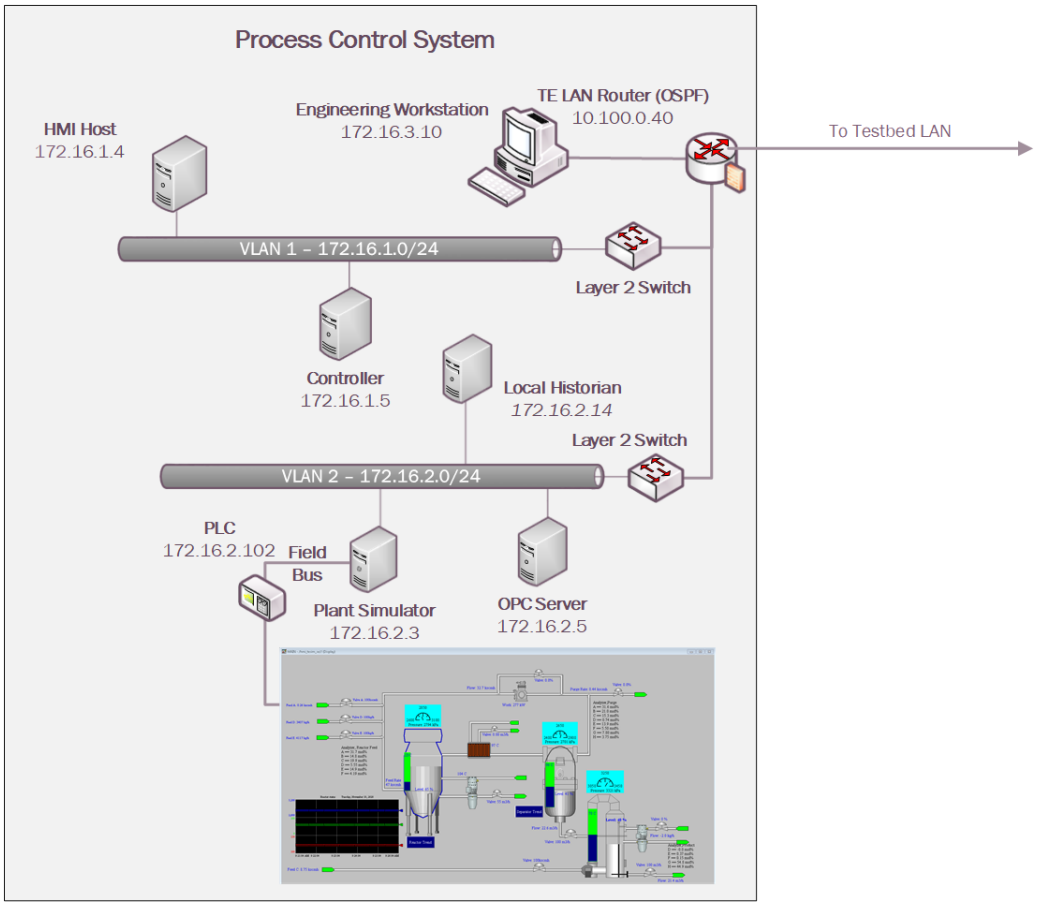


The PCS network architecture is shown in Figure 4-4. The PCS network is connected to the Testbed LAN via a boundary router. The boundary router is an Allen-Bradley Stratix 8300. All network traffic is going through the boundary router to access the Testbed LAN and the DMZ. The PCS environment is segmented into three local networks, namely the engineering LAN, Operations LAN (VLAN1), and the Supervisory LAN (VLAN2). Each of these local networks is connected using an industrial network switch, an Allen-Bradley Stratix 5700. The engineering workstation is hosted in the engineering LAN. The HMI and the Plant Controller are hosted in the operations LAN. The Plant Simulator is hosted in the supervisory LAN along with the Local Historian, OPC Server, and the Supervisory PLC.

The Operations LAN (VLAN1) simulates a central control room environment. The supervisory LAN (VLAN2) simulates the process operation/ manufacturing environment, which typically consists of the operating plant, PLCs, OPC server, and data historian.

An OPC DA server is the main data gateway for the PLC and the simulated controller. The PLC reads in the manufacturing process sensor data from the Plant Simulator using the DeviceNet connection and communicates the data to the OPC DA server. The PLC also retrieves actuator information from the controller through the OPC DA and transmits to the Plant Simulator. The controller uses a MATLAB Simulink interface to communicate with the OPC DA server directly.

Figure 4-4 PCS Network



4.4 Collaborative Robotics System (CRS)

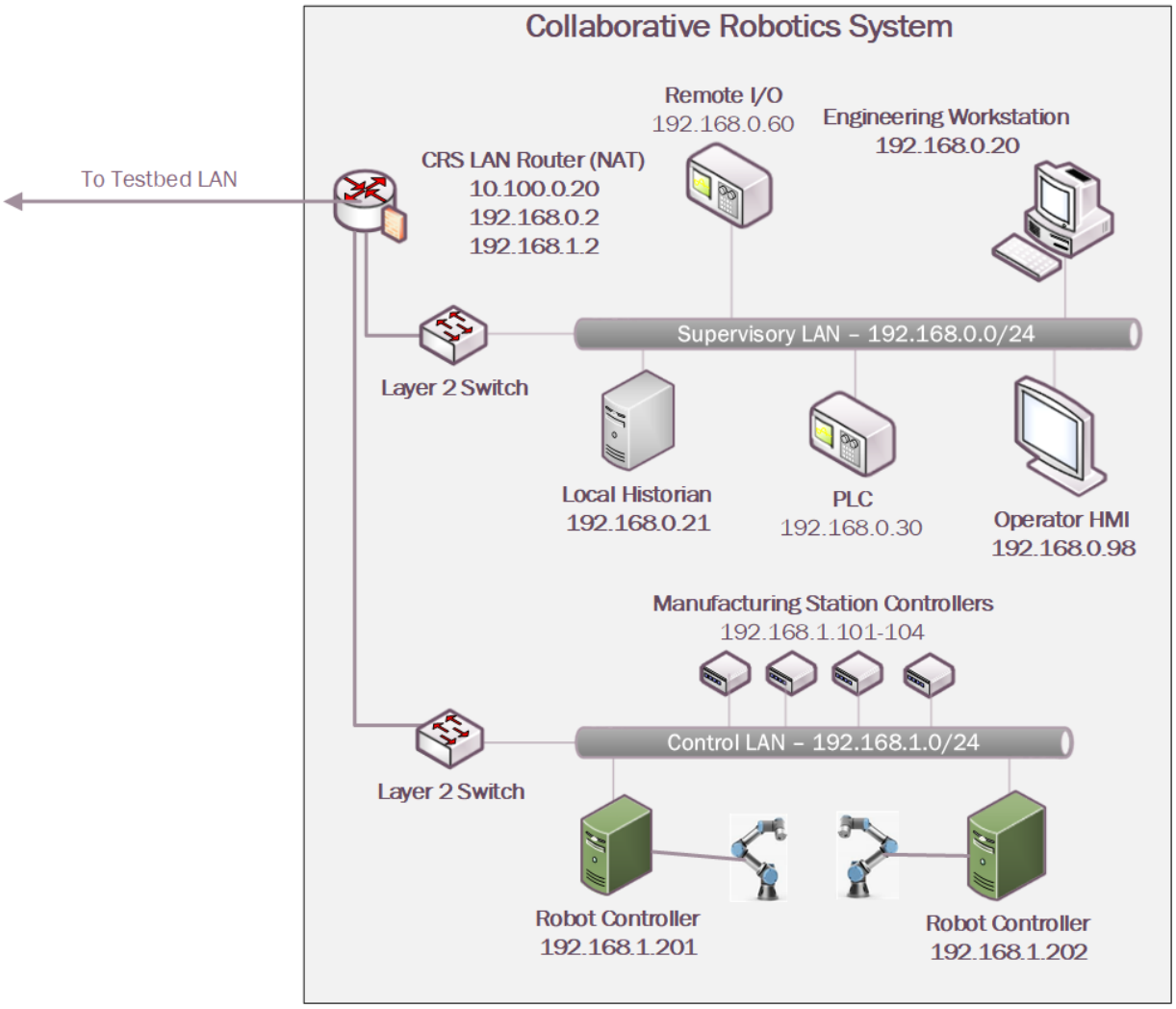
The CRS workcell, shown in Figure 4-5, contains two robotic arms that perform a material handling process called machine tending [8]. Robotic machine tending utilizes robots to interact with machinery, performing physical operations a human operator would normally perform (e.g., loading and unloading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

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

Figure 4-5 The CRS Workcell

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

Figure 4-6 CRS Network



4.5 Logical Network and Security Architectures

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

4.5.1 Build 1

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

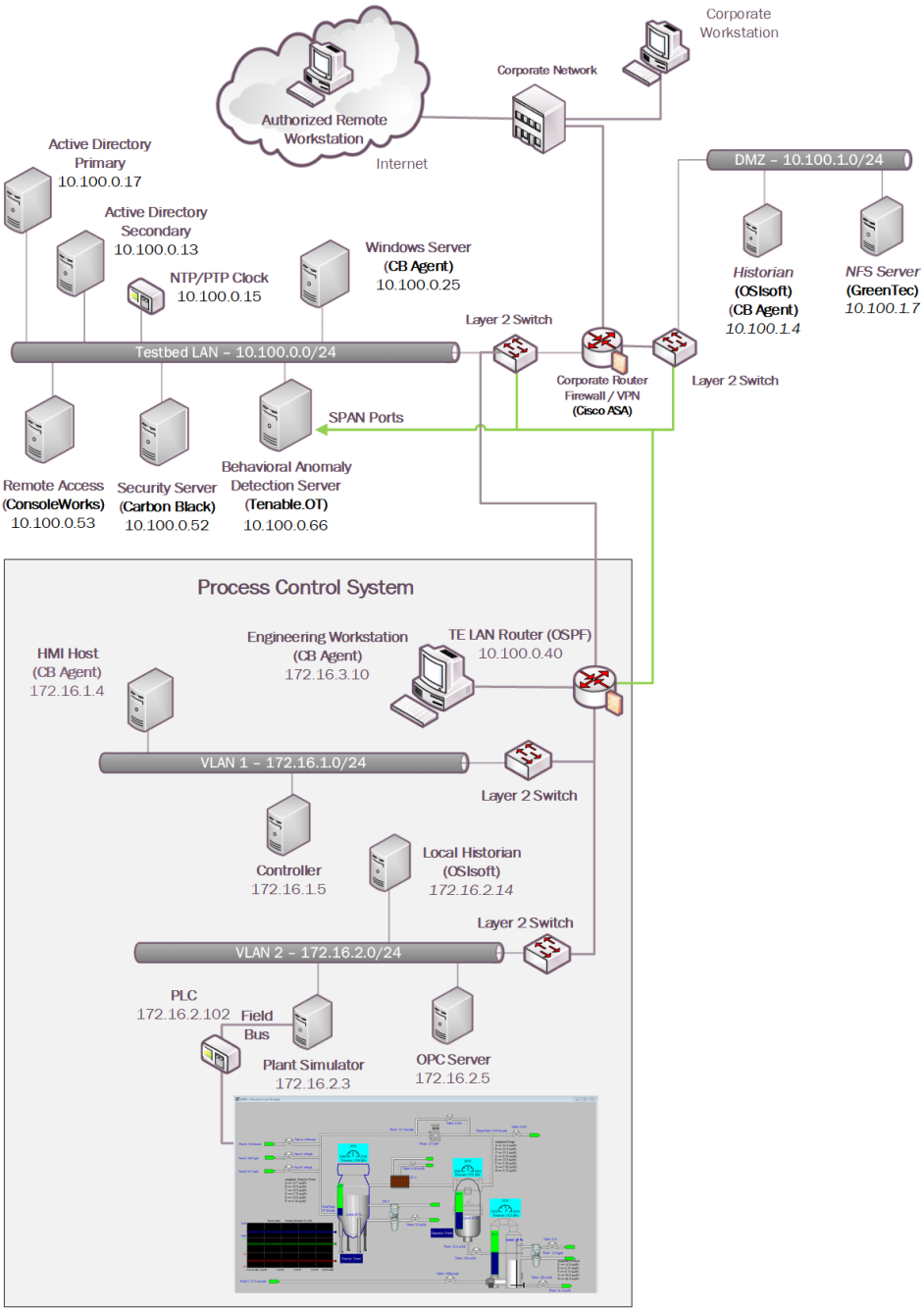
Table 4-2 Build 1 Technology Stack to Capabilities Map

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

Capability	Products	Description
User Authentication and Authorization	ConsoleWorks	Deployed to centralize the access and management of the systems and credentials. ConsoleWorks is deployed to the Testbed LAN to allow connections to the PCS environment.
Remote Access	AnyConnect	Supports authenticated VPN connections to the environment with limited access to only the TDI ConsoleWorks web interface.

The technology was integrated into the lab environment as shown in Figure 4-7.

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



4.5.2 Build 2

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

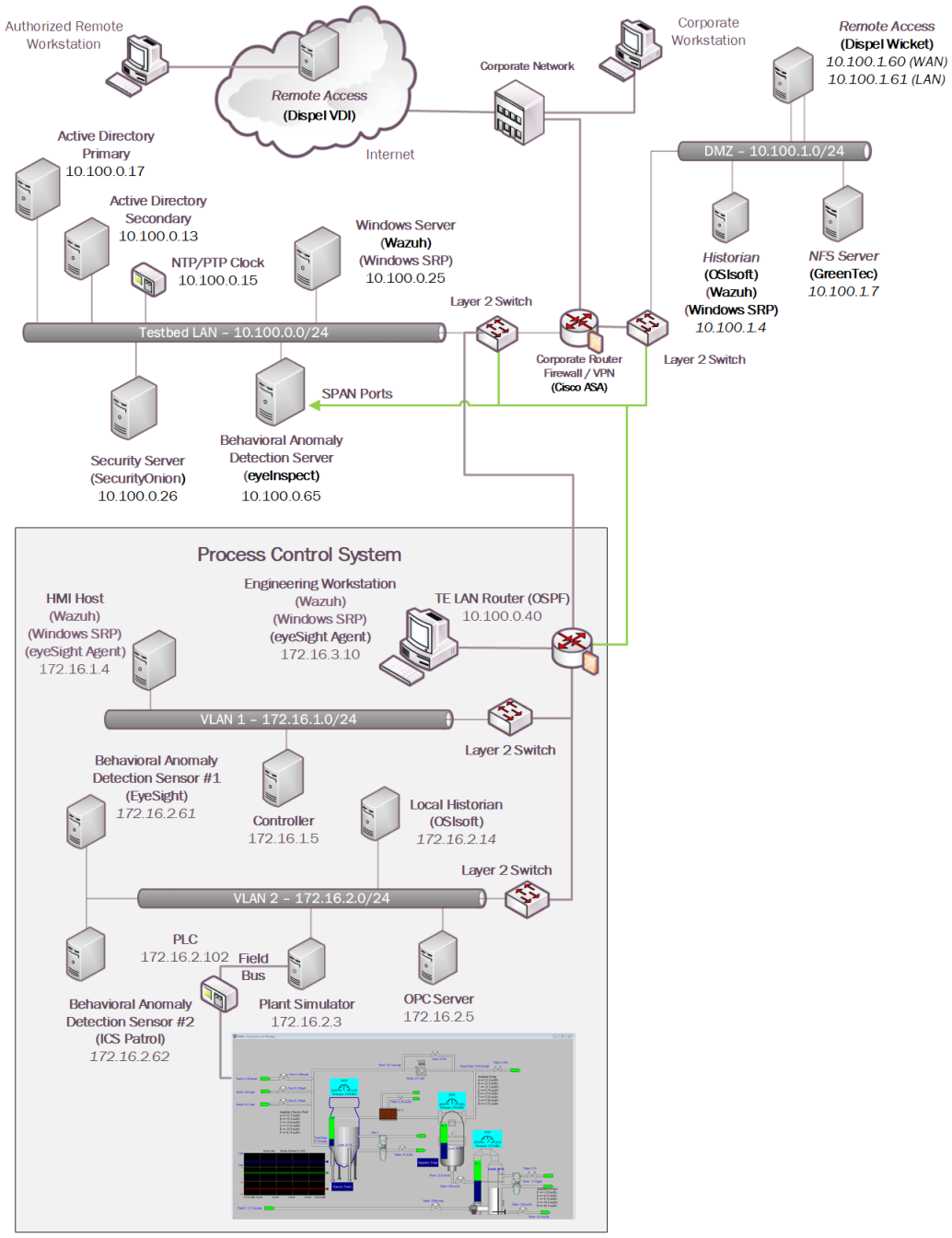
Table 4-3 Build 2 Technology Stack to Capabilities Map

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

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

The technology was integrated into the lab environment as shown in Figure 4-8.

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



4.5.3 Build 3

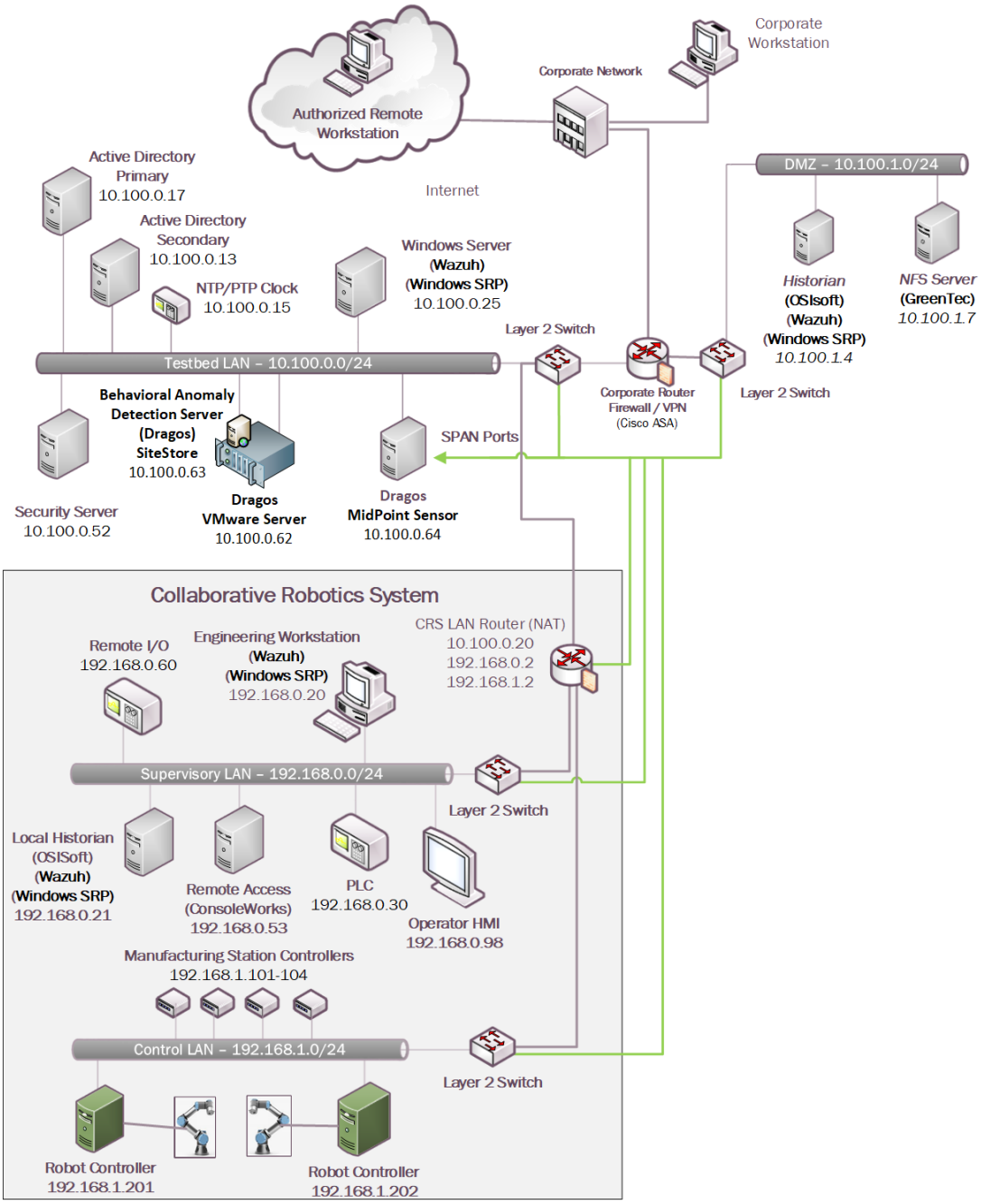
The technologies in Table 4-4 were integrated into the CRS for Build 3 to enhance system and data integrity capabilities.

Table 4-4 Build 3 Technology Stack to Capabilities Map

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

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

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



4.5.4 Build 4

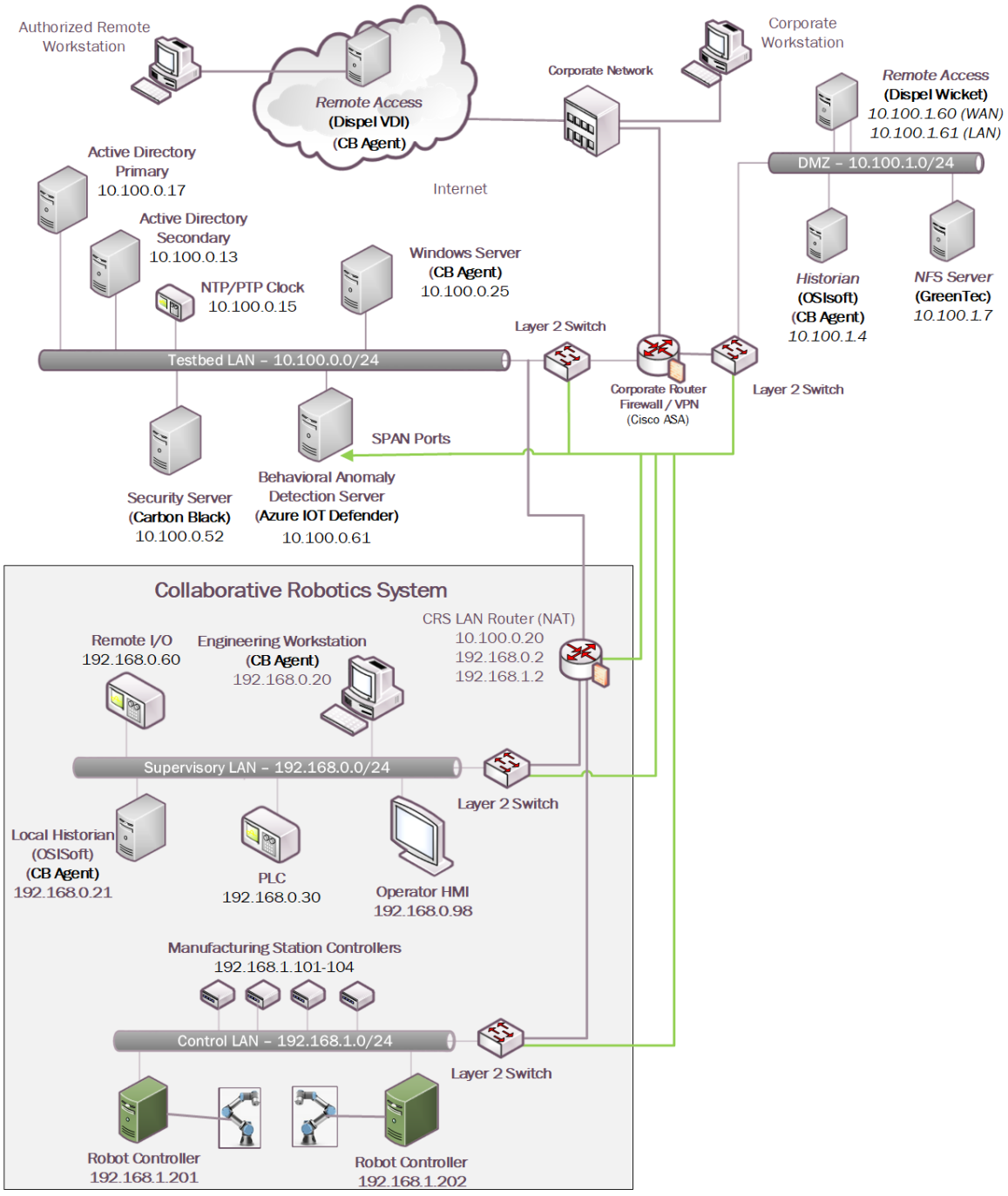
For Build 4, the technologies in Table 4-5 were integrated into the CRS, Testbed LAN, and DMZ segments of the testbed environment to enhance system and data integrity capabilities.

Table 4-5 Build 4 Technology Stack to Capabilities Map

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

The technology was integrated into the lab environment as shown in Figure 4-10.

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



5 Security Characteristic Analysis

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

5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure.

5.2 Example Solution Testing

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

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

Additional information for each scenario such as screenshots captured during the execution of the test procedures and detailed results from the security capabilities are presented in Appendix D.

5.2.1 Scenario 1: Protect Host from Malware Infection via USB

Objective	This test demonstrates blocking the introduction of malware through physical access to a workstation within the manufacturing environment.
Description	An authorized user transports executable files into the manufacturing system via a USB flash drive that contains malware.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-2, DE.AE-2
Assumptions	▪ User does not have administrative privileges on the target machine. ▪ User has physical access to the target machine.
Security Capabilities and Products	Build 1: ▪ Carbon Black: AAL Build 2: ▪ Windows SRP: AAL Build 3: ▪ Windows SRP: AAL Build 4: ▪ Carbon Black: AAL
Test Procedures	1. Attempt to execute malware on the target machine.
Expected Results	▪ The AAL tool will detect and stop the malware upon execution.
Actual Test Results	▪ The AAL technology successfully blocks and alerts on the execution of the application on the workstation in all builds.
Overall Result	PASS

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

Objective	This test demonstrates the detection of malware introduced from the network.

Description	An attacker pivoting from the corporate network into the manufacturing environment attempts to insert malware to establish persistence in the manufacturing environment.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	▪ The attacker has completed reconnaissance and initial access, gaining the ability to pivot into the manufacturing environment.
Security Capabilities and Products	Build 1: ▪ Carbon Black: AAL ▪ Tenable.ot: BAD Build 2: ▪ Windows SRP: AAL ▪ Forescout eyeInspect: BAD Build 3: ▪ Windows SRP: AAL ▪ Dragos: BAD Build 4: ▪ Carbon Black: AAL ▪ Azure Defender for IoT: BAD
Test Procedures	1. Attacker pivots into the manufacturing environment. 2. Attacker copies malware to the server in Testbed LAN. 3. Attacker attempts to execute malware on server in Testbed LAN.
Expected Results	▪ The AAL capabilities installed on target systems will block execution of the malicious code. ▪ The BAD tool will capture the suspicious traffic and generate an alert.

Actual Test Results	▪ The AAL technology successfully blocks and alerts on the execution of the application on the workstation in all builds. ▪ The BAD tool is able to detect and alert on activity pivoting into manufacturing systems.
Overall Result	PASS

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

Objective	This test demonstrates blocking malware that is attempting to infect the manufacturing system through authorized remote access connections.
Description	A remote workstation authorized to use a remote access connection has been infected with malware. When the workstation is connected to the manufacturing environment through the remote access connection, the malware attempts to pivot and spread to vulnerable host(s).
Relevant NIST *Cybersecurity Framework* Subcategories	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-7, PR.MA-1, PR.MA-2, DE.CM-3, DE.CM-7
Assumptions	▪ Infection of the remote workstation occurs prior to remote access session.

Security Capabilities and Products	Build 1: ▪ Cisco VPN: Remote Access ▪ ConsoleWorks: User Authentication and User Authorization Build 2: ▪ Dispel: User Authentication and User Authorization, and Remote Access Build 3: ▪ Cisco VPN: Remote Access ▪ ConsoleWorks: User Authentication and User Authorization Build 4: ▪ Dispel: User Authentication and User Authorization, and Remote Access
Test Procedures	1. Authorized remote user connects to the manufacturing environment. 2. Malware on remote host attempts to pivot into the manufacturing environment.
Expected Results	▪ Malware will be blocked from propagation by the remote access capabilities.
Actual Test Results	▪ Remote access connection blocks malware attempts to pivot into the manufacturing environment.
Overall Result	PASS

5.2.4 Scenario 4: Protect Host from Unauthorized Application Installation

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

Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	▪ User does not have administrative privileges on the target machine. ▪ Applications to be installed are unapproved applications.
Security Capabilities and Products	Build 1: ▪ Carbon Black: AAL ▪ Tenable.ot: BAD Build 2: ▪ Windows SRP: AAL ▪ eyeInspect: BAD Build 3: ▪ Windows SRP: AAL ▪ Dragos: BAD Build 4: ▪ Carbon Black: AAL ▪ Azure Defender for IoT: BAD
Test Procedures	1. The user copies software to a host in the manufacturing environment. 2. The user attempts to install the software on the host. 3. The user attempts to execute software that does not require installation.
Expected Results	▪ The AAL tool will detect and stop the execution of the software installation or executable file. ▪ The BAD tool will capture the suspicious traffic and generate an alert.
Actual Test Results	▪ The AAL technology successfully blocks and alerts on the execution of the application on the workstation in all builds. ▪ The BAD tool is able to detect and alert on activity in the manufacturing system.

Overall Result	PASS

5.2.5 Scenario 5: Protect from Unauthorized Addition of a Device

Objective	This test demonstrates detection of an unauthorized device connecting to the manufacturing system.
Description	An individual authorized to access the physical premises connects and uses an unauthorized device on the manufacturing network.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	▪ Ports on switch are active and available.
Security Capabilities and Products	Build 1: ▪ Tenable.ot: BAD Build 2: ▪ eyeInspect: BAD Build 3: ▪ Dragos: BAD Build 4: ▪ Azure Defender for IoT: BAD
Test Procedures	1. The individual connects the unauthorized device to the manufacturing network. 2. The individual uses an unauthorized device to access other devices on the manufacturing network.
Expected Results	▪ The BAD detection tool will capture the suspicious traffic and generate an alert.
Actual Test Results	▪ The BAD detection tool is able to detect and alert on activity in the manufacturing system.
Overall Result	PASS

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

Objective	This test demonstrates detection of unauthorized communications between devices.
Description	A device authorized to be on the network attempts to establish an unapproved connection.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	▪ The environment has a predictable communications pattern.
Security Capabilities and Products	Build 1: ▪ Tenable.ot: BAD. Build 2: ▪ eyeInspect: BAD. Build 3: ▪ Dragos: BAD Build 4: ▪ Azure Defender for IoT: BAD
Test Procedures	1. The device attempts to establish an unapproved connection.
Expected Results	▪ The BAD tool will capture the suspicious traffic and generate an alert.
Actual Test Results	▪ The BAD tool is able to detect and alert on activity in manufacturing systems.
Overall Result	PASS

5.2.7 Scenario 7: Protect from Unauthorized Deletion of Files

Objective	This test demonstrates protection of files from unauthorized deletion both locally and on network file share.

Description	An authorized user attempts to delete files on an engineering workstation and a shared network drive within the manufacturing system.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-1, PR.DS-6, PR.IP-4, PR.MA-1, DE.AE-2
Assumptions	▪ User does not have administrative privileges on the target machine.
Security Capabilities and Products	Build 1: ▪ Carbon Black: File Integrity Checking. ▪ WORMdisk: File Integrity Protection. Build 2: ▪ Security Onion: File Integrity Checking. ▪ WORMdisk: File Integrity Protection. Build 3: ▪ Security Onion: File Integrity Checking. ▪ WORMdisk: File Integrity Protection. Build 4: ▪ Carbon Black: File Integrity Checking. ▪ WORMdisk: File Integrity Protection.
Test Procedures	1. User attempts to delete files located on a workstation in the manufacturing system. 2. User attempts to delete files from the network file share containing the golden images for the manufacturing system.
Expected Results	▪ Deletion of files on the workstation will be detected and alerted on by the file integrity checking tool. ▪ Deletion of files on the network file share will be prevented by the file integrity checking tool.
Actual Test Results	▪ Host-based file integrity checking is able to detect and alert on deletion of files.

	▪ Protected network file share is able to prevent deletion of files on the network file share.
Overall Result	PASS

5.2.8 Scenario 8: Detect Unauthorized Modification of PLC Logic

Objective	This test demonstrates detection of PLC logic modification.
Description	An authorized user performs an unapproved or unauthorized modification of the PLC logic from an engineering workstation.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.AC-3,PR.AC-7, PR.DS-6, PR.MA-1, PR.MA-2, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	None
Security Capabilities and Products	Build 1: ▪ Tenable.ot: BAD and Software Modification ▪ Cisco VPN: Remote Access ▪ ConsoleWorks: User Authentication, User Authorization, and Remote Access Build 2: ▪ eyeInspect: BAD and Software Modification ▪ Dispel: User Authentication and User Authorization, and Remote Access Build 3: ▪ Dragos: BADand Software Modification ▪ Cisco VPN: Remote Access ▪ ConsoleWorks: User Authentication, User Authorization, and Remote Access Build 4: ▪ Azure Defender for IoT: BAD and Software Modification ▪ Dispel: User Authentication and User Authorization, and Remote Access

Test Procedures	1. The authorized user remotely connects to a manufacturing environment. 2. The user modifies and downloads a logic file to the PLC.
Expected Results	▪ The BAD tool will capture the suspicious traffic and generate an alert. ▪ The user authentication/authorization/remote access is able to remotely access the engineering systems as intended.
Actual Test Results	▪ The BAD is able to detect and alert on activity accessing the PLC.
Overall Result	PASS

5.2.9 Scenario 9: Protect from Modification of Historian Data

Objective	This test demonstrates blocking of modification of historian archive data.
Description	An attacker coming from the corporate network pivots into the manufacturing environment and attempts to modify historian archive data.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-1, DE.AE-2
Assumptions	▪ The attacker has completed reconnaissance and initial access, gaining the ability to pivot into the manufacturing environment.
Security Capabilities and Products	Build 1: ▪ Tenable.ot: BAD ▪ ForceField WFS: File Integrity Protection. Build 2: ▪ eyeInspect: BAD ▪ ForceField WFS: File Integrity Protection.

	Build 3: ▪ Dragos: BAD ▪ ForceField WFS: File Integrity Protection. Build 4: ▪ Azure Defender for IoT: BAD ▪ ForceField WFS: File Integrity Protection.
Test Procedures	1. Attacker pivots into the manufacturing environment from the corporate network. 2. Attacker attempts to delete historian archive data file. 3. Attacker attempts to replace historian archive data file.
Expected Results	▪ The file operations will be blocked by the file integrity checking tool.
Actual Test Results	▪ File integrity checking tool is able to prevent file operations on the protected files.
Overall Result	PASS

5.2.9.1 Scenario 10: Detect Sensor Data Manipulation

Objective	This test demonstrates detection of atypical data reported to the historian.
Description	A sensor in the manufacturing system begins sending atypical data values to the historian.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.IP-4, PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	▪ Devices in the manufacturing system (HMI and PLCs) are not validating sensor data.
Security Capabilities and Products	▪ PI Server: BAD
Test Procedures	1. A sensor sends invalid data to the historian.

Expected Results	▪ The BAD capability will detect atypical sensor data and generate alerts.
Actual Test Results	▪ The BAD tool is able to detect atypical data and create an event frame.
Overall Result	PASS

5.2.9.2 Scenario 11: Detect Unauthorized Firmware Modification

Objective	This test demonstrates detection of device firmware modification.
Description	An authorized user performs a change of the firmware on a PLC.
Relevant NIST *Cybersecurity Framework* Subcategories	PR.DS-6, PR.MA-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-3, DE.CM-7
Assumptions	None

Security Capabilities and Products	Build 1: ▪ Cisco VPN: Remote Access. ▪ ConsoleWorks: Remote Access, User Authentication, and User Authorization. ▪ Tenable.ot: BAD and Firmware Modification. Build 2: ▪ Dispel: Remote Access, User Authentication, and User Authorization. ▪ eyeInspect and ICSPatrol: BAD and Firmware Modification. Build 3: ▪ Cisco VPN: Remote Access. ▪ ConsoleWorks: Remote Access, User Authentication, and User Authorization. ▪ Dragos: BAD and Firmware Modification. Build 4: ▪ Dispel: Remote Access, User Authentication, and User Authorization. ▪ Azure Defender for IoT: BAD and Firmware Modification.
Test Procedures	1. Authorized remote user connects to manufacturing environment. 2. The user changes firmware on the PLC component.
Expected Results	▪ The behavioral anomaly detection tool will identify the change to the PLC and generate an alert for review.
Actual Test Results	▪ The BAD is able to detect and generate alerts for updates to PLC component firmware.
Overall Result	PASS

5.3 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The NIST *Cybersecurity Framework* Subcategories were used to provide structure to the security assessment by consulting the specific

sections of each standard that are cited in reference to a Subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the NIST *Cybersecurity Framework* Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the necessary security characteristics.

5.3.1 PR.AC-1: Identities and Credentials are Issued, Managed, Verified, Revoked, and Audited for Authorized Devices, Users, and Processes

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

5.3.2 PR.AC-3: Remote Access is Managed

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

5.3.3 PR.AC-4: Access Permissions and Authorizations are Managed, Incorporating the Principles of Least Privilege and Separation of Duties

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

5.3.4 PR.AC-7: Users, Devices, and Other Assets are Authenticated (e.g., single-factor, multi-factor) Commensurate with the Risk of the Transaction (e.g., Individual Security and Privacy Risks and Other Organizational Risks)

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

5.3.5 PR.DS-1: Data-at-Rest is Protected

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

5.3.6 PR.DS-6: Integrity Checking Mechanisms are Used to Verify Software, Firmware, and Information Integrity

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

5.3.7 PR.IP-4: Backups of Information are Conducted, Maintained, and Tested

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

5.3.8 PR.MA-1: Maintenance and Repair of Organizational Assets are Performed and Logged, with Approved and Controlled Tools

This NIST *Cybersecurity Framework* Subcategory is supported by a combination of tools including AAL, the user authentication and user authorization tools, and the behavior anomaly detection tools. User authentication and user authorization tools provide a controlled environment for authorized users to interact with the manufacturing environment. Behavior anomaly detection tools provide a means to detect maintenance activities in the environment such as PLC logic modification or PLC firmware updates via the network. This information can be combined with data from a computerized maintenance management system to ensure that all maintenance activities are appropriately approved and logged. Also, AAL prevents unapproved software from running on systems to ensure that only approved tools are used for maintenance activities.

5.3.9 PR.MA-2: Remote Maintenance of Organizational Assets is Approved, Logged, and Performed in a Manner that Prevents Unauthorized Access

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

5.3.10 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and Systems is Established and Managed

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

5.3.11 DE.AE-2: Detected Events are Analyzed to Understand Attack Targets And Methods

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

5.3.12 DE.AE-3: Event Data are Collected and Correlated from Multiple Sources and Sensors

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

5.3.13 DE.CM-1: The Network is Monitored to Detect Potential Cybersecurity Events

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

5.3.14 DE.CM-3: Personnel Activity is Monitored to Detect Potential Cybersecurity Events

This NIST *Cybersecurity Framework* Subcategory is supported by the authentication and authorization tools that allow for monitoring personnel activity while connected through these tools. Further, AAL and

file integrity checking tools provide the ability to monitor user actions on hosts. Additionally, BAD tools monitor and record events associated with personnel actions traversing network traffic. Each tool provides a different perspective in monitoring personnel activity within the environment. The resulting alerts and logs from these tools can be monitored individually or collectively to support investigations for potential malicious or unauthorized activity within the environment.

5.3.15 DE.CM-7: Monitoring for Unauthorized Personnel, Connections, Devices, and Software is Performed

This NIST *Cybersecurity Framework* Subcategory is supported by BAD, AAL, user authentication and user authorization, and remote access capabilities of the solutions. The BAD tools established an information baseline for approved assets and connections. Then the manufacturing network is monitored using the BAD capability for any deviation by the assets and connections from the established baseline. If any deviation is detected, an alert is generated. Additionally, the AAL tool blocks any unauthorized application installation or execution and generates an alert on these events. User authentication and user authorization tools monitor for unauthorized personnel connecting to the environment. Remote access capabilities monitor for unauthorized connections to the environment.

6 Future Build Considerations

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

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

Appendix A List of Acronyms

AAL	Application Allowlisting
BAD	Behavioral Anomaly Detection
CRS	Collaborative Robotic System
CRADA	Cooperative Research and Development Agreement
CSF	NIST *Cybersecurity Framework*
CSMS	Cybersecurity for Smart Manufacturing Systems
DMZ	Demilitarized Zone
EL	Engineering Laboratory
FOIA	Freedom of Information Act
ICS	Industrial Control System
IoT	Internet of Things
IT	Information Technology
LAN	Local Area Network
NCCoE	National Cybersecurity Center of Excellence
NFS	Network File Share
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
OT	Operational Technology
PCS	Process Control System
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block
SP	Special Publication
SPAN	Switched Port Analyzer

SRP	Software Restriction Policies
SSH	Secure Shell
TE	Tennessee-Eastman
VDI	Virtual Desktop Interface
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Appendix B Glossary

Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009
Architecture	A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability). SOURCE: FIPS 201-2
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: FIPS 200
Authorization	The right or a permission that is granted to a system entity to access a system resource. SOURCE: NIST SP 800-82 Rev. 2
Backup	A copy of files and programs made to facilitate recovery if necessary. SOURCE: NIST SP 800-34 Rev. 1
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. SOURCE: NIST SP 800-137
CRADA	Collaborative Research and Development Agreement SOURCE: NIST SP 1800-5b, NIST SP 1800-5c
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. SOURCE: CNSSI 4009-2015 (NSPD-54/HSPD-23)
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. SOURCE: NIST SP 800-30 Rev. 1

Data	A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. SOURCE: CNSSI-4009
File Integrity Checking	Software that generates, stores, and compares message digests for files to detect changes made to the files. SOURCE: NIST SP 800-115
Firmware	Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs. SOURCE: CNSSI 4009-2015
Industrial Control Systems	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. SOURCE: NIST SP 800-30 Rev. 1
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. SOURCE: FIPS 199 (44 U.S.C., Sec. 3542)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. SOURCE: FIPS 200 (44 U.S.C., Sec. 3502)
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. SOURCE: FIPS 200
Log	A record of the events occurring within an organization's systems and networks. SOURCE: NIST SP 800-92
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system. SOURCE: NIST SP 800-111

Network Traffic	Computer network communications that are carried over wired or wireless networks between hosts. SOURCE: NIST SP 800-86
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). SOURCE: NIST SP 800-37 Rev. 2
Privacy	Assurance that the confidentiality of, and access to, certain information about an entity is protected. SOURCE: NIST SP 800-130
Remote Access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). SOURCE: NIST SP 800-128 under Remote Access from NIST SP 800-53
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: FIPS 200
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis. SOURCE: NIST SP 800-63-2
Risk Management Framework	The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. SOURCE: NIST SP 800-82 Rev. 2 (NIST SP 800-37)
Security Control	A protection measure for a system SOURCE: NIST SP 800-123
Virtual Machine	Software that allows a single host to run one or more guest operating systems SOURCE: NIST SP 800-115

Appendix C References

[1] C. Singleton et al., X-Force Threat Intelligence Index 2021, IBM, February 2021, https://www.ibm.com/security/data-breach/threat-intelligence

[2] A Sedgewick et al., *Guide to Application Whitelisting*, NIST SP 800-167, NIST, Oct. 2015. Available: http://dx.doi.org/10.6028/NIST.SP.800-167.

[3] Department of Homeland Security, Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance, 2015. Available: https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/critical-manufacturing-framework-implementation-guide-2015-508.pdf.

[4] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity, DCPD201300091*, Feb. 12, 2013. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, V1.1 April 16, 2018. Available: https://doi.org/10.6028/NIST.CSWP.04162018.

[6] J. McCarthy et al., Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection, NIST Interagency Report (NISTIR) 8219, NIST, Nov. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf.

[7] K. Stouffer et al., Cybersecurity Framework Manufacturing Profile, NIST Internal Report 8183, NIST, May 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

[8] R. Candell et al., An Industrial Control System Cybersecurity Performance Testbed, NISTIR 8089, NIST, Nov. 2015. Available: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf.

[9] Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53 Revision 5, NIST, Apr. 2013. Available: https://doi.org/10.6028/NIST.SP.800-53r5.

[10] W. Newhouse et al., National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST SP 800-181, Aug. 2017. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[11] J. Cawthra et al., *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800-25 Dec. 2020, https://doi.org/10.6028/NIST.SP.1800-25.

[12] Celia Paulsen, Robert Byers, Glossary of Key Information Security Terms NISTIR 7298, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf.

[13] U.S.-Canada Power Systems Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Available: https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/Outage_Task_Force_-_DRAFT_Report_on_Implementation.pdf

[14] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82 Revision 2, NIST, June 2015, Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[15] J. J. Downs and E. F. Vogel, "A Plant-wide Industrial Problem Process," Comput. Chem. Eng., vol. 17, no. 3, 1993, pp. 245–255

Appendix D Scenario Execution Results

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

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

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

D.1.1 Build 1

D.1.1.1 Configuration

- Application Allowlisting: Carbon Black
  - Agent installed on an HMI Workstation and configured to communicate to the Carbon Black Server.

D.1.1.2 Test Results

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

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

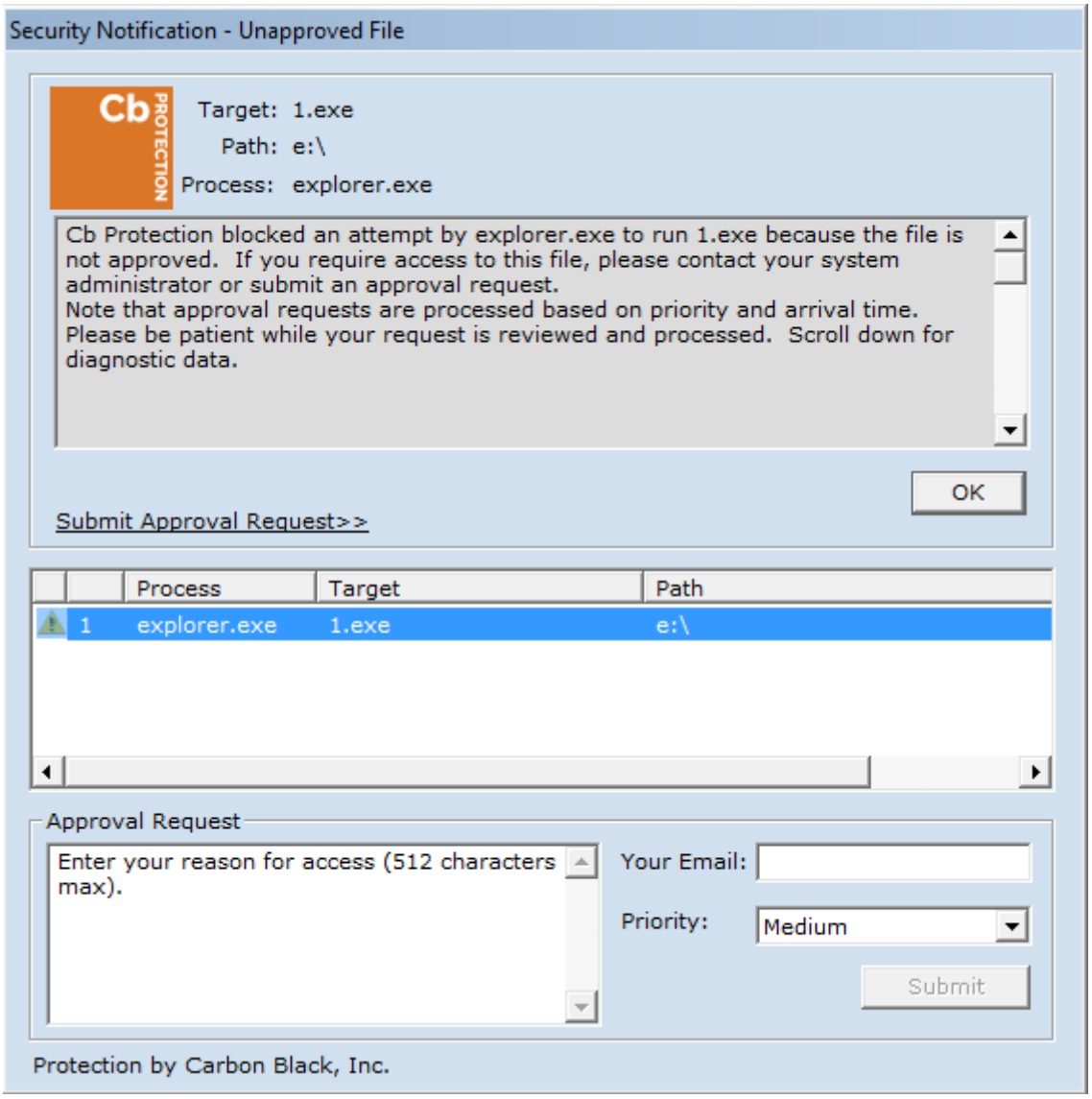


Figure D-2: Carbon Black's Server Provides Additional Details and Logs of the Event

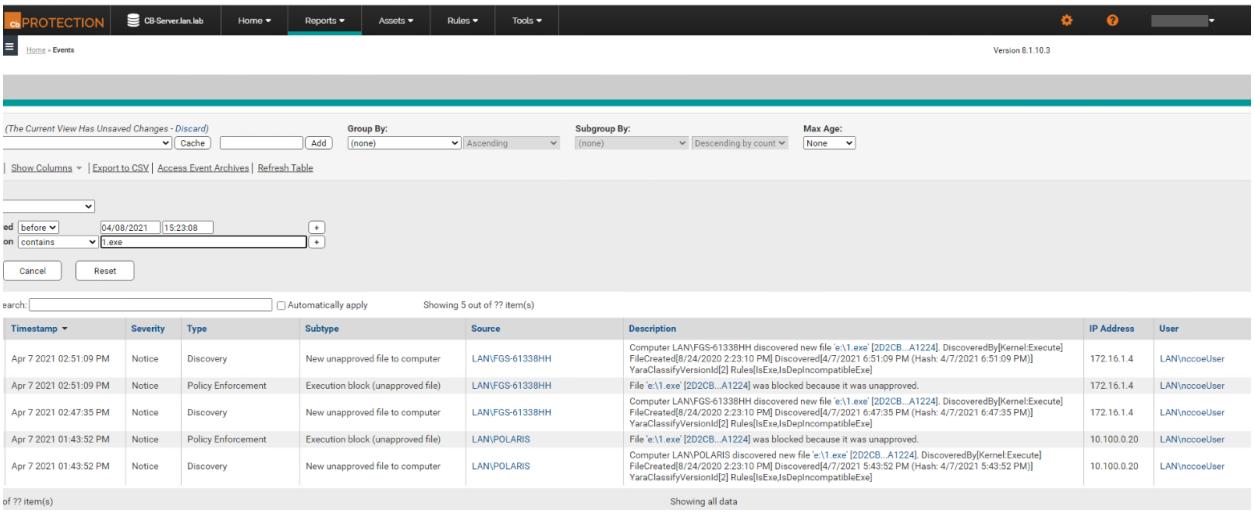
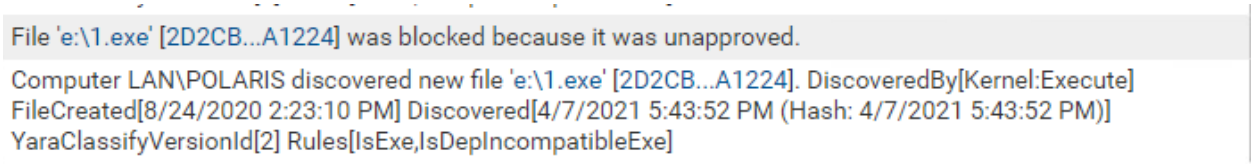


Figure D-3 Carbon Black's Server Log of the Event



D.1.2 Build 2

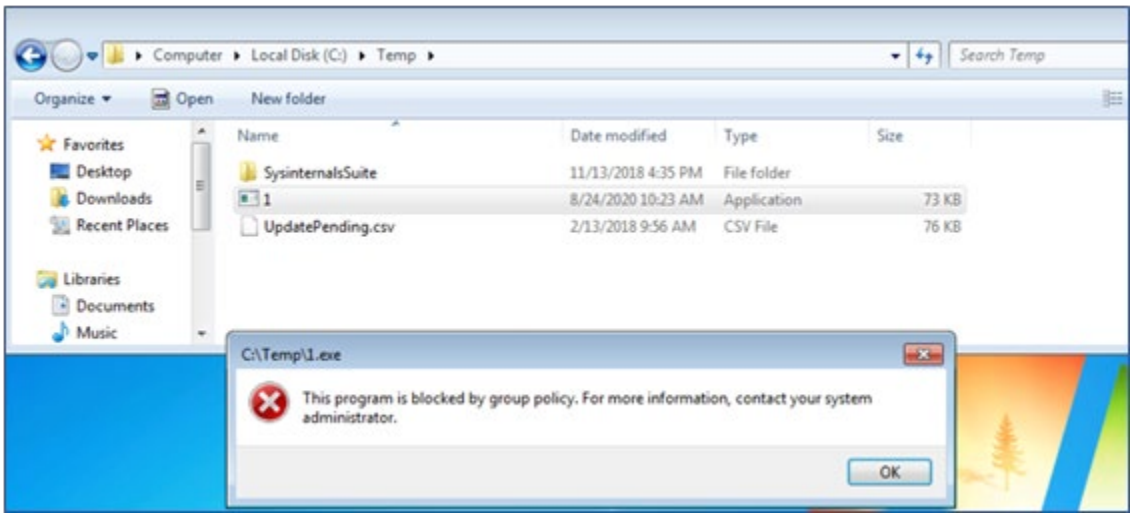
D.1.2.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to HMI Workstation.

D.1.2.2 Test Results

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

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



D.1.3 Build 3

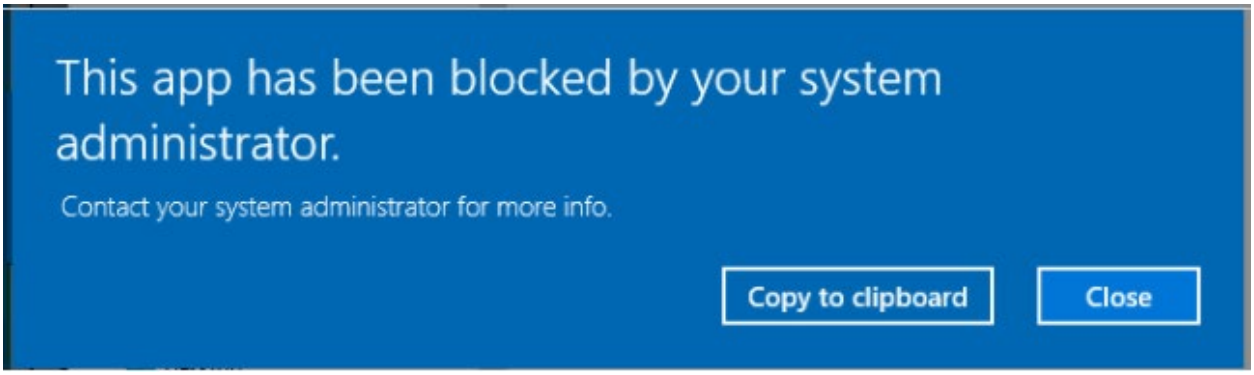
D.1.3.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to Engineering Workstation.

D.1.3.2 Test Results

For Build 3, Windows SRP application allowlisting is enabled in the Collaborative Robotics environment. Figure D-5 shows that the executable is blocked on the CRS workstation.

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



D.1.4 Build 4

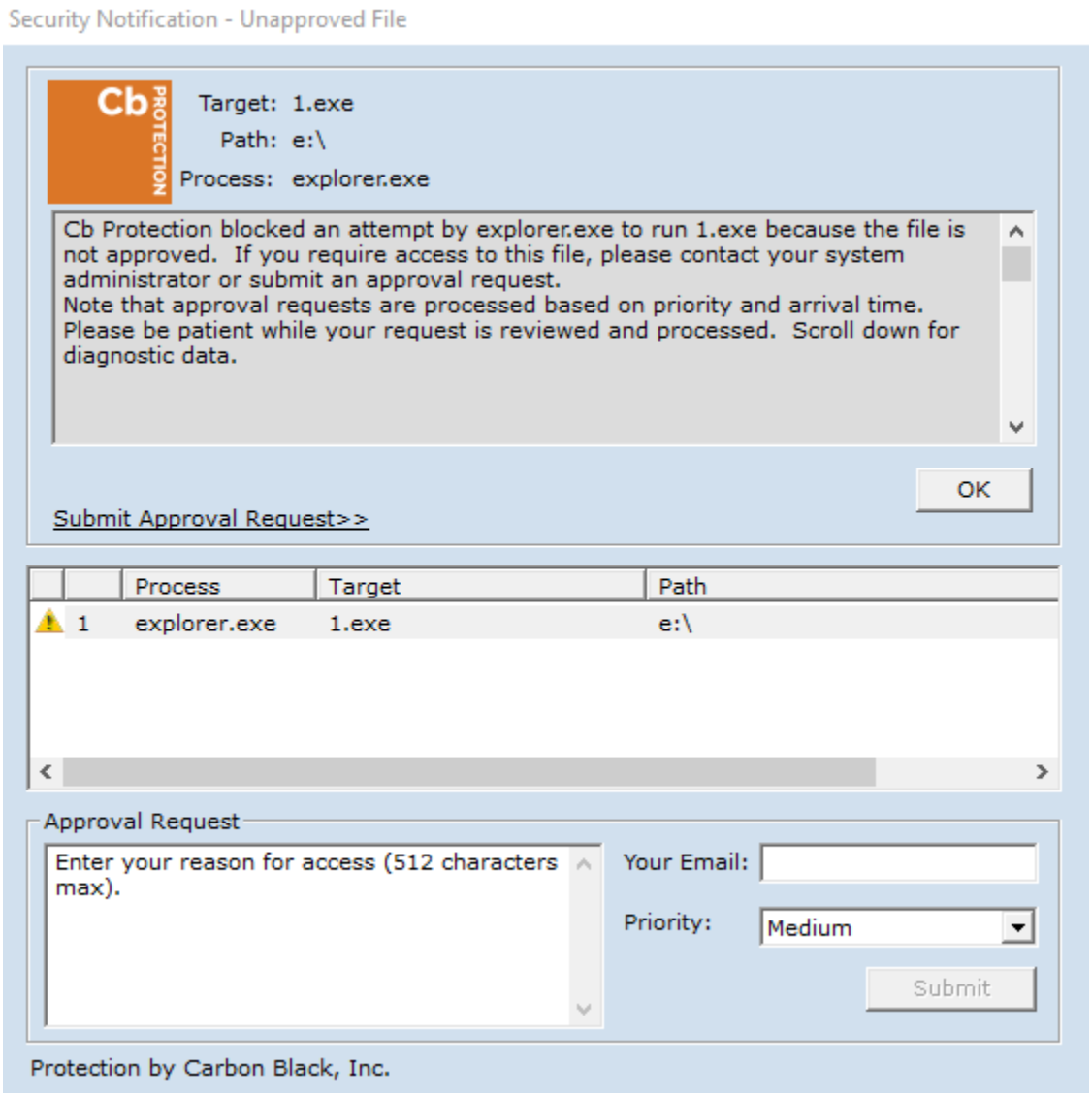
D.1.4.1 Configuration

- Application Allowlisting : Carbon Black
  - Agent installed on Engineering Workstation and configured to communicate to the Carbon Black Server.

D.1.4.2 Test Results

Carbon Black successfully detects and blocks the malicious file as shown by the Carbon Black notification in Figure D-6.

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



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

An attacker who has already gained access to the corporate network attempts to pivot into the ICS environment through the DMZ. From a system in the DMZ, the attacker scans for vulnerable systems in the Testbed LAN environment to continue pivoting toward the ICS environments. In an attempt to establish a persistent connection into the ICS environment, the malicious file (1.exe) is copied to a system in the Testbed LAN environment and executed. The expected outcome is that the malicious file is

blocked by the application allowlisting tool, and the RDP and scanning network activity is observed by the behavioral anomaly detection tool.

D.2.1 Build 1

D.2.1.1 Configuration

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

D.2.1.2 Test Results

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

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

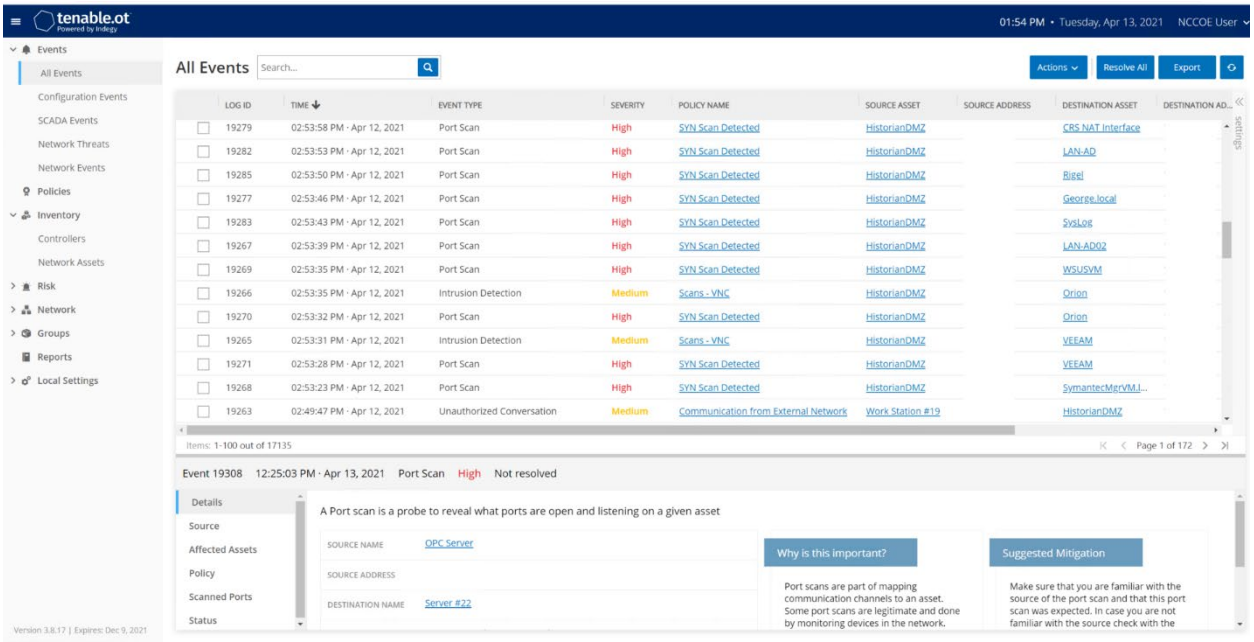


Figure D-8 Detected RDP Session Activity from External System to DMZ System

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

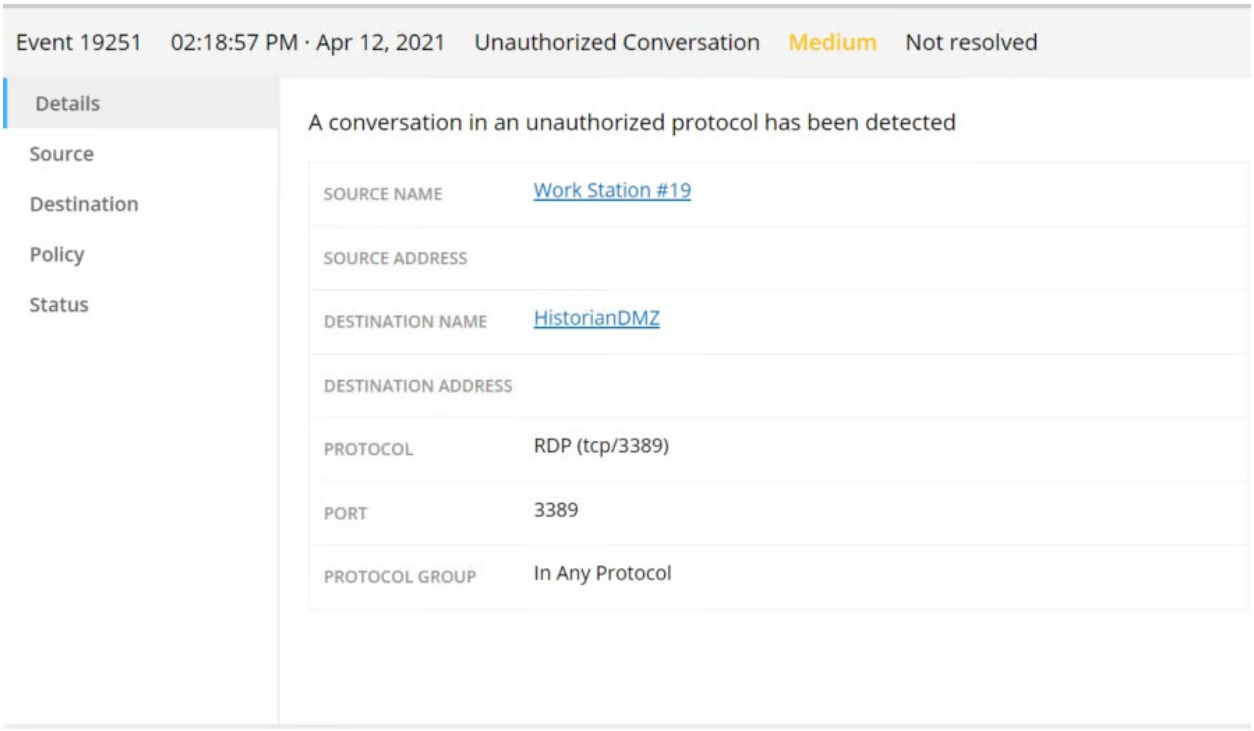


Figure D-10 Tenable.ot Detected VNC Connection Between the DMZ and the Testbed LAN

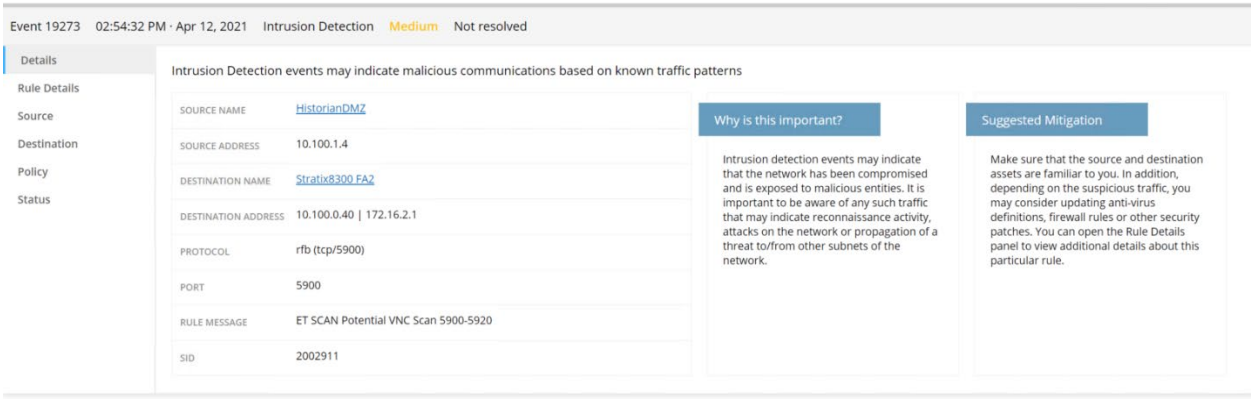


Figure D-11 Tenable.ot Event Detail for a Detected Port Scan from a DMZ System Targeting a System in the Testbed LAN

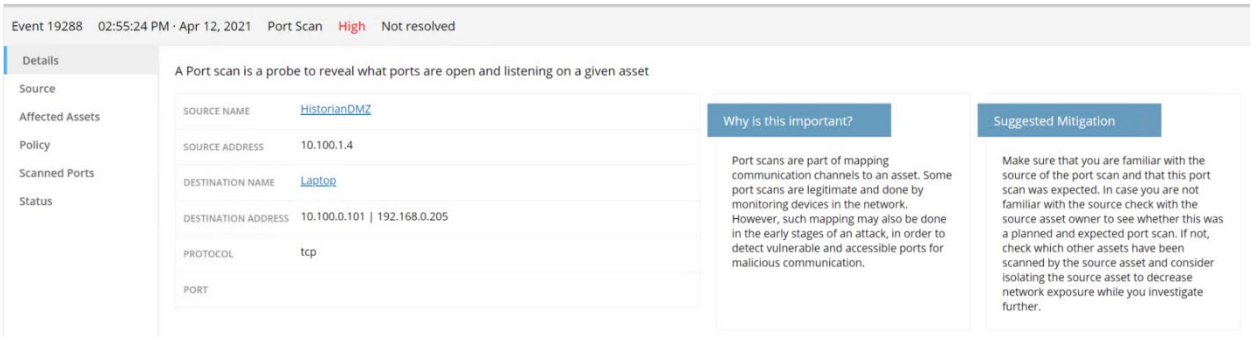


Figure D-12 Detected RDP from a DMZ system to a Testbed LAN system

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

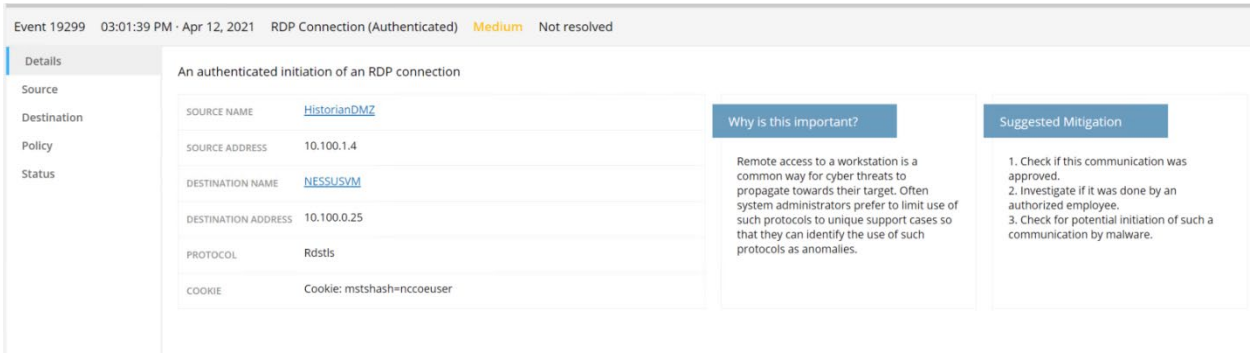
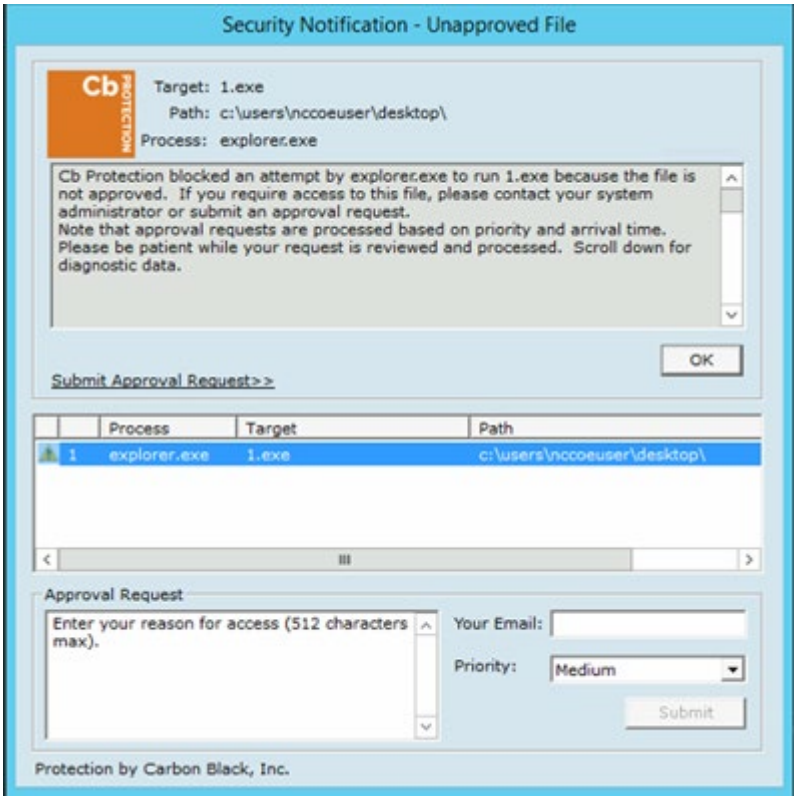


Figure D-14 Attempt to Execute 1.exe Failed



D.2.2 Build 2

D.2.2.1 Configuration

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

D.2.2.2 Test Results

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

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

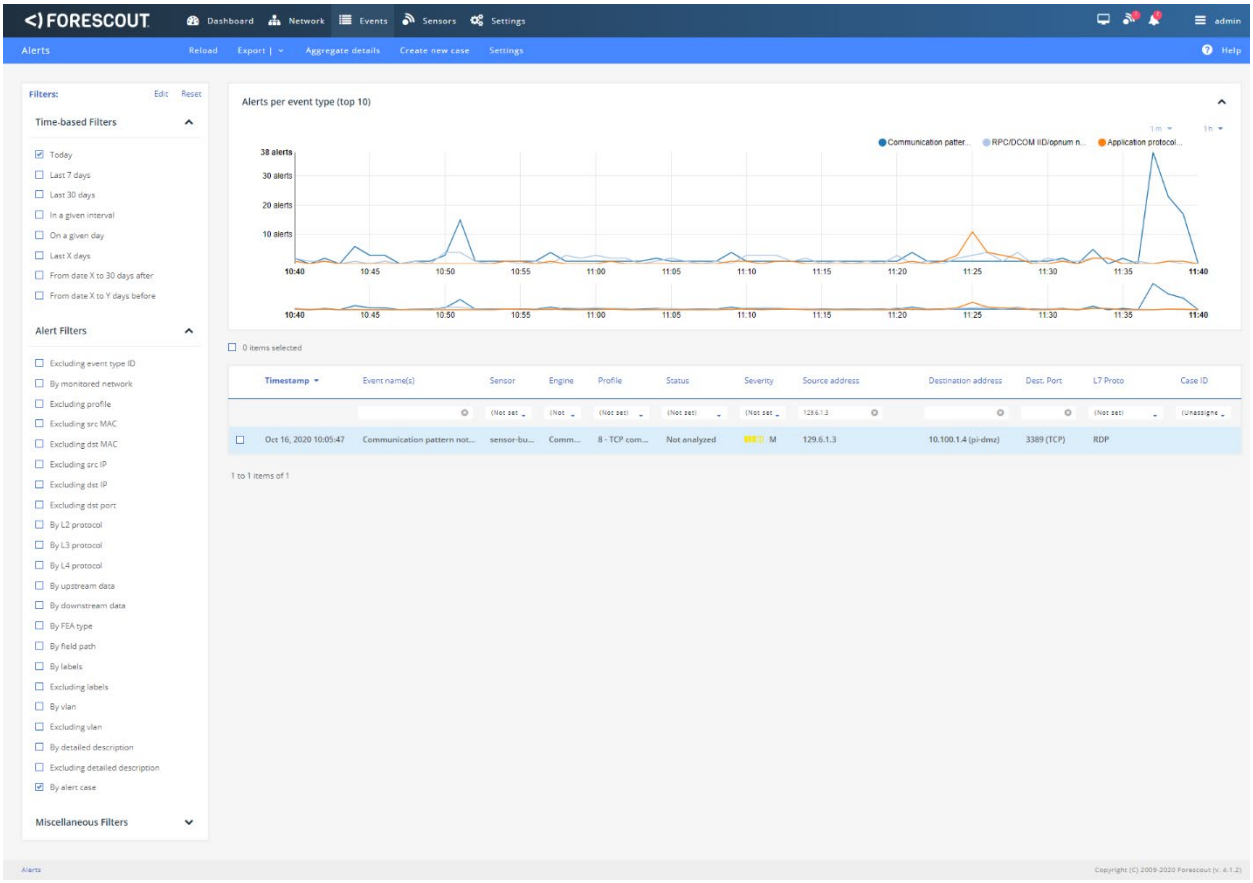


Figure D-16 Details of the Detected RDP Session Activity from an External System to DMZ System

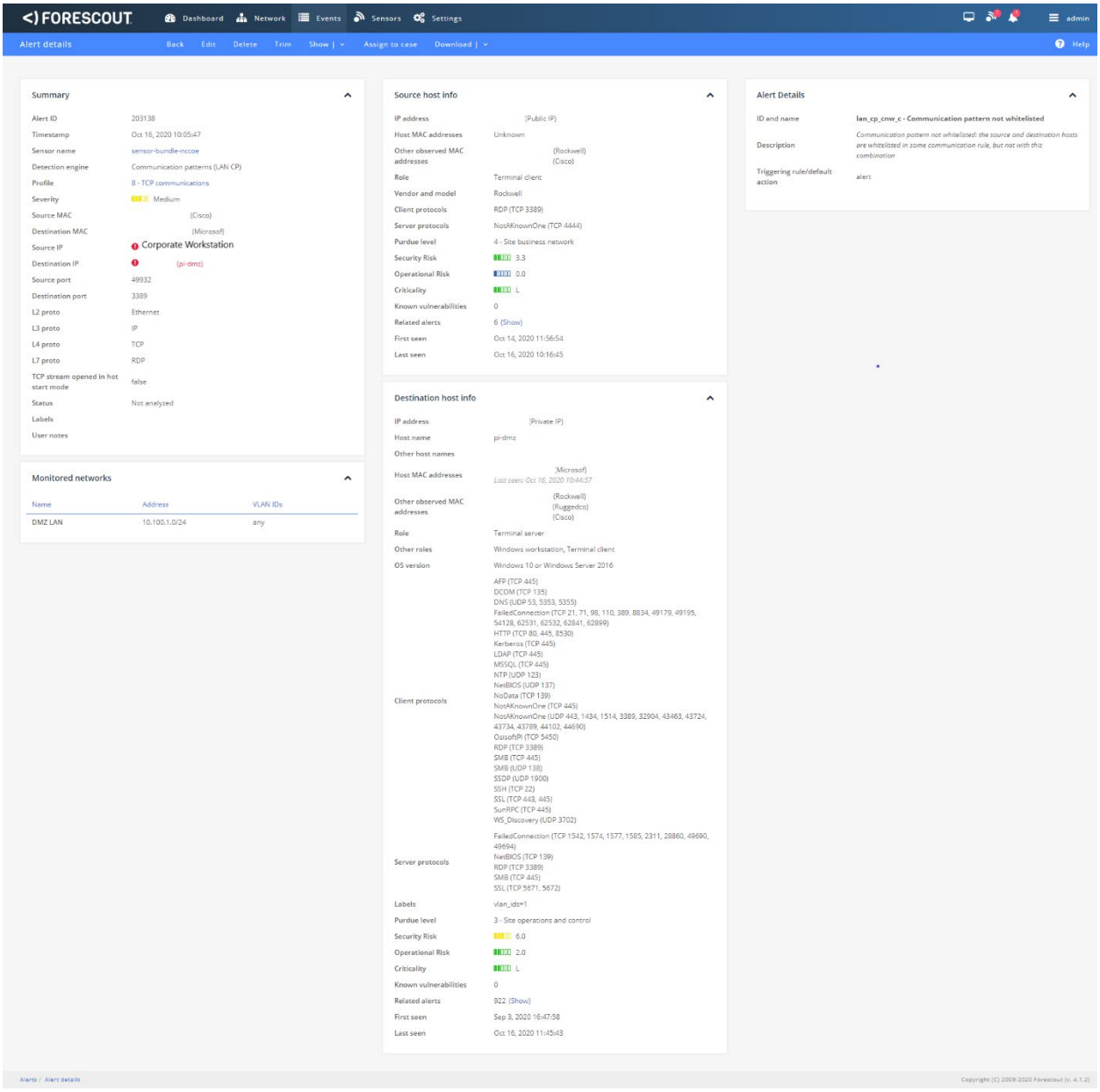


Figure D-17 Detection of Scanning Traffic and RDP Connection into Manufacturing Environment

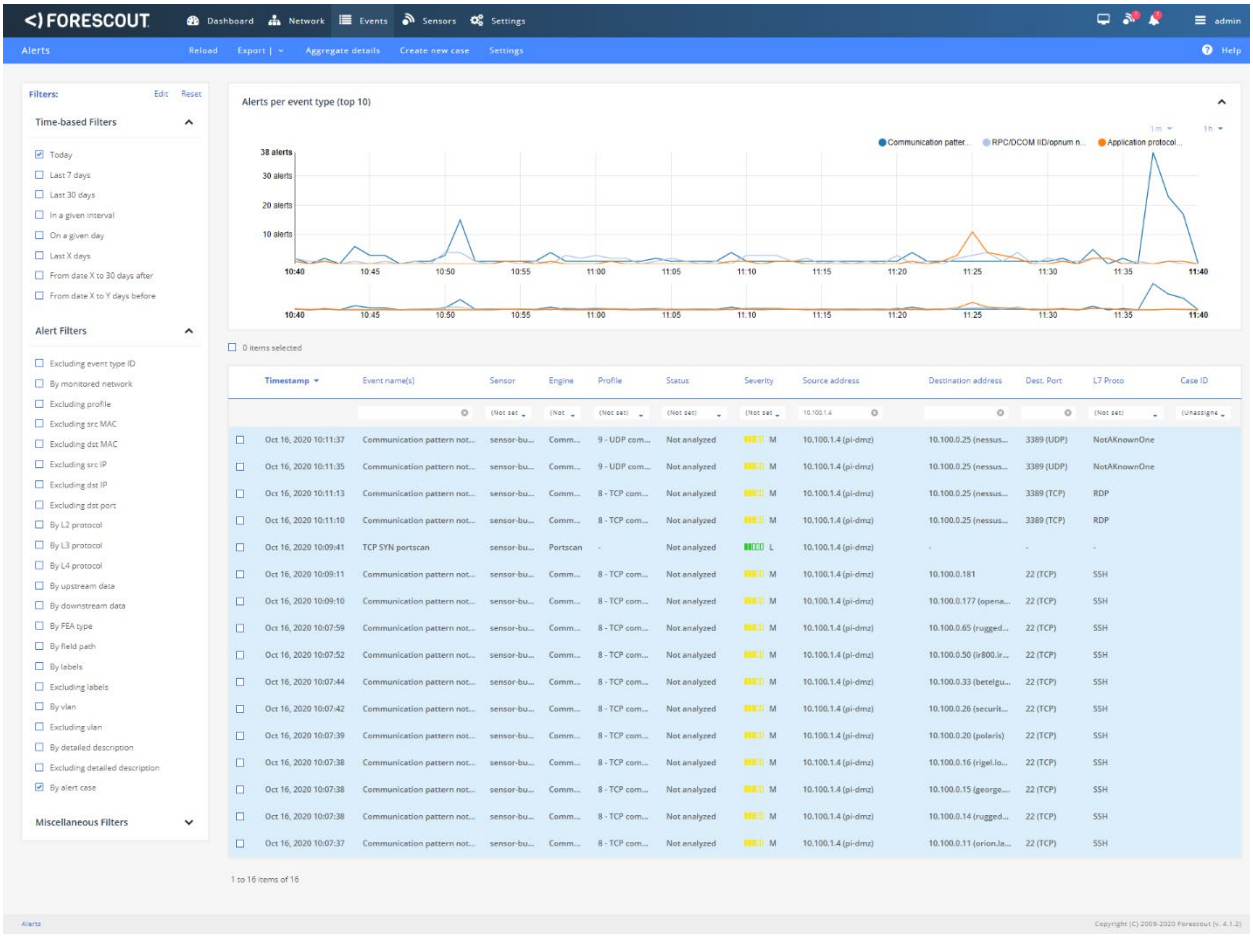


Figure D-18 Details of One of the Port Scan Alerts

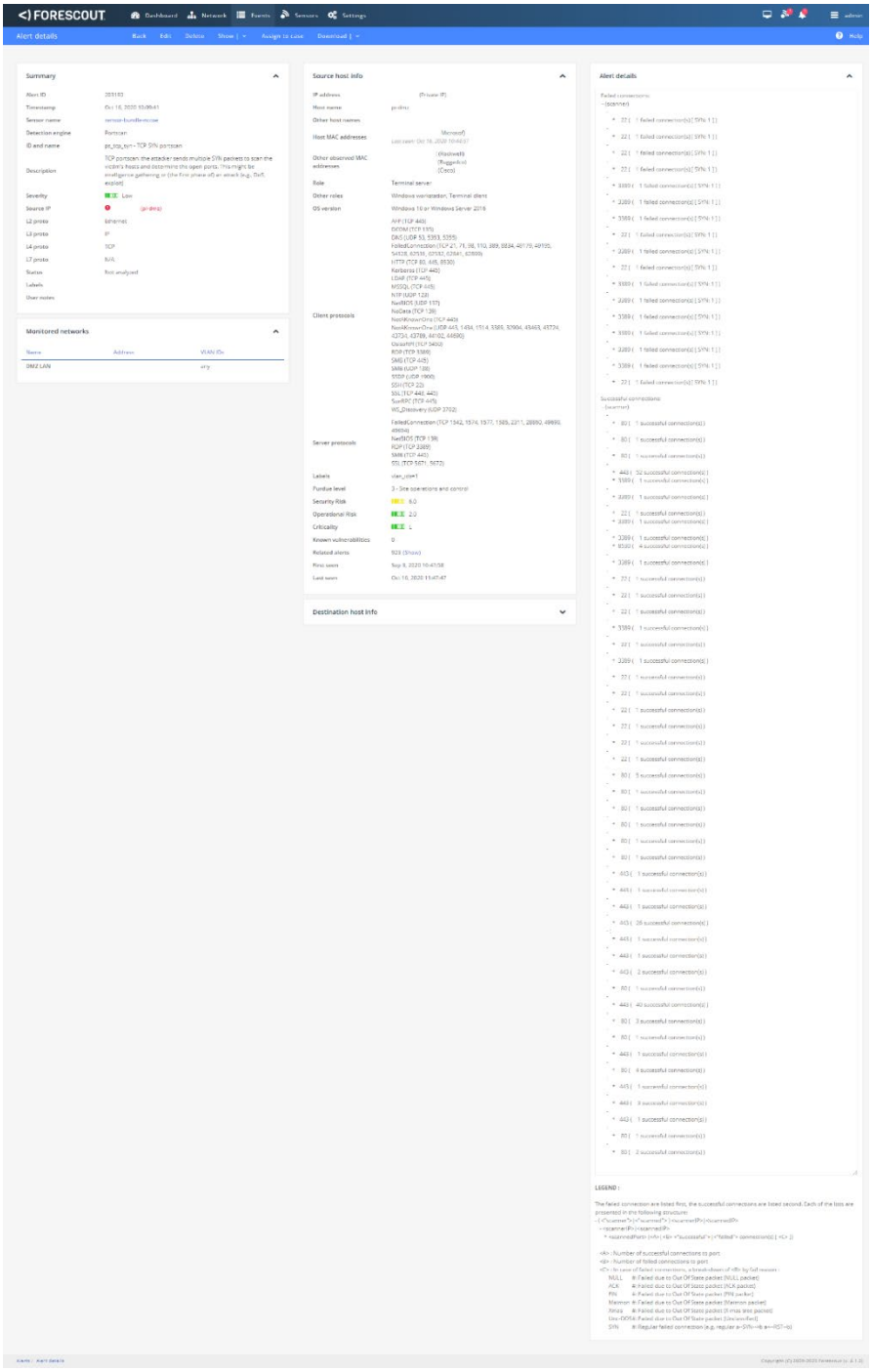


Figure D-19 Details of Alert for RDP Connection into Manufacturing Environment

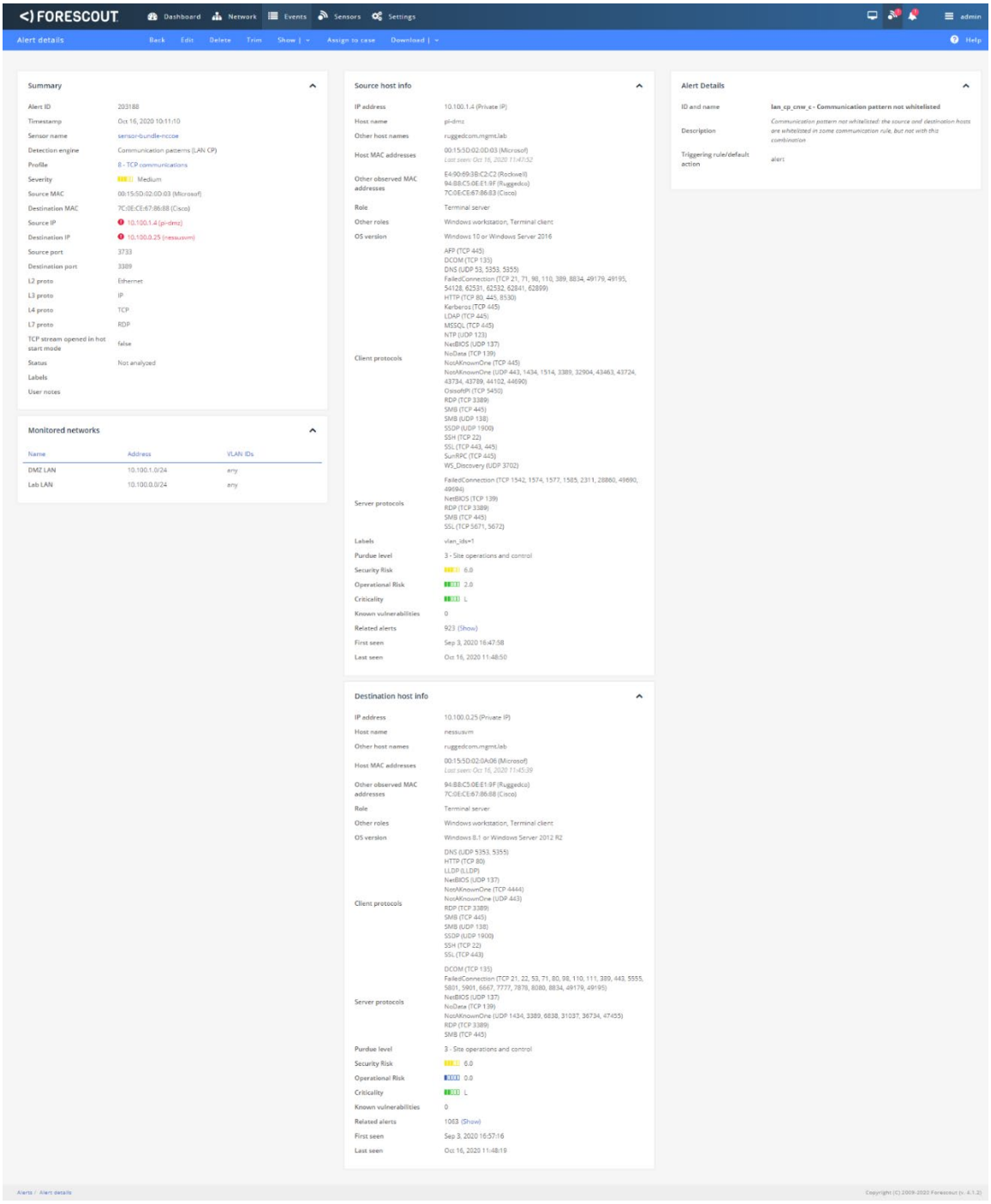
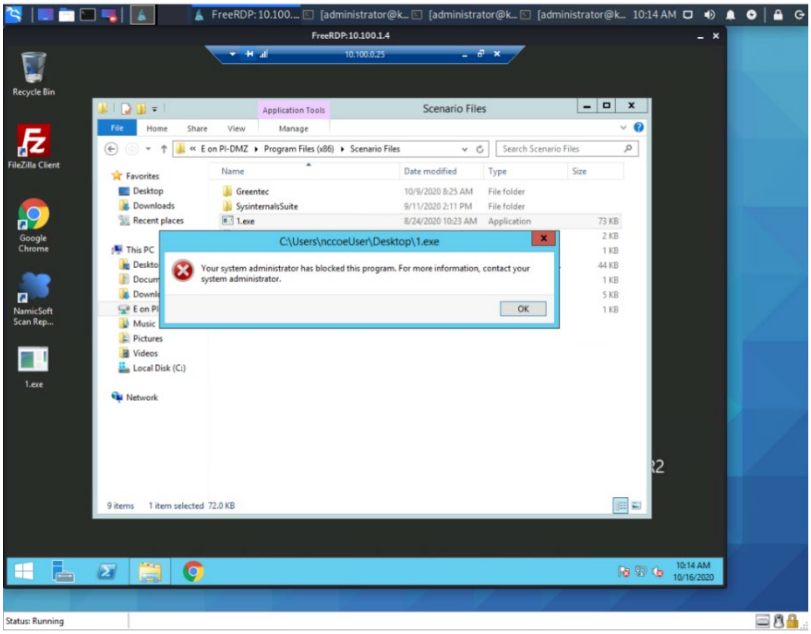


Figure D-20 Dialog Message Showing 1.exe was Blocked from Executing



D.2.3 Build 3

D.2.3.1 Configuration

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

D.2.3.2 Test Results

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

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

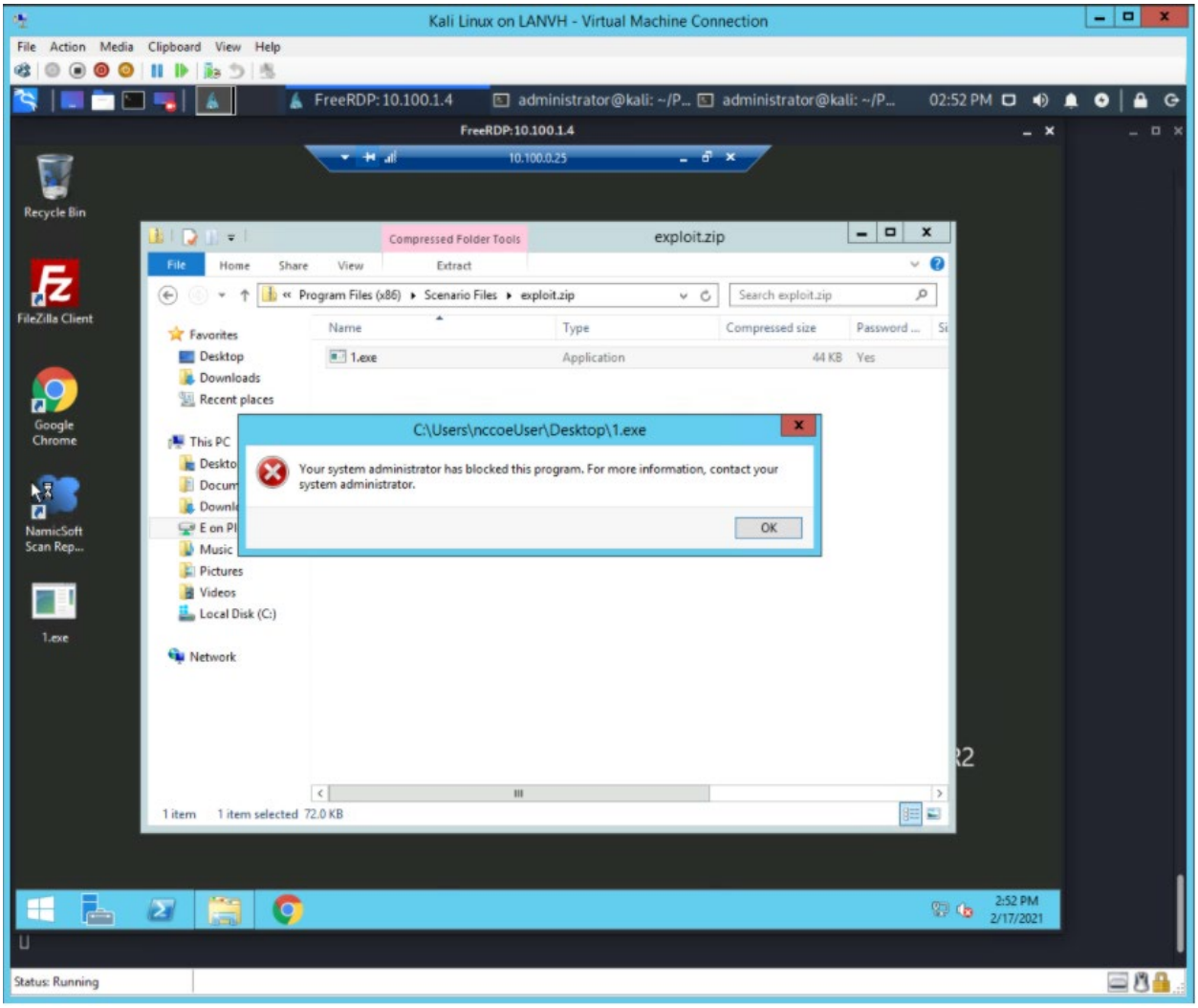


Figure D-22 Log of Alerts Detected by Dragos

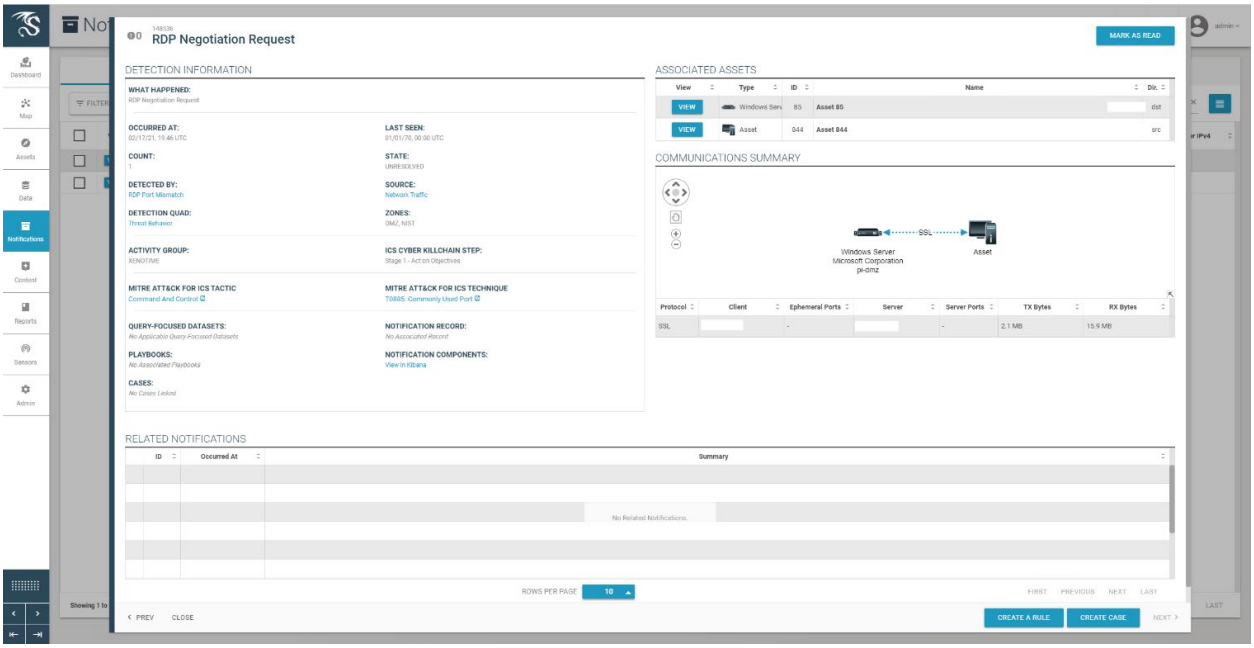


Figure D-23 Detail of RDP Session Activity Between an External System and a DMZ System

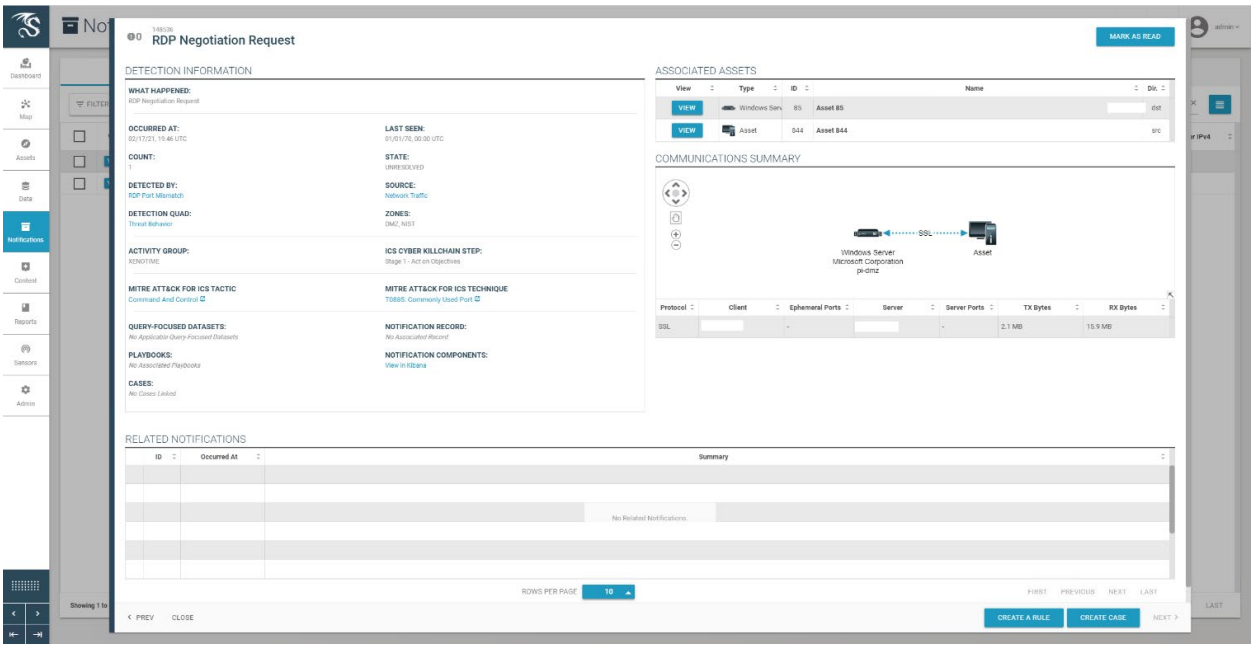


Figure D-24 Detail for Network Scanning Alert

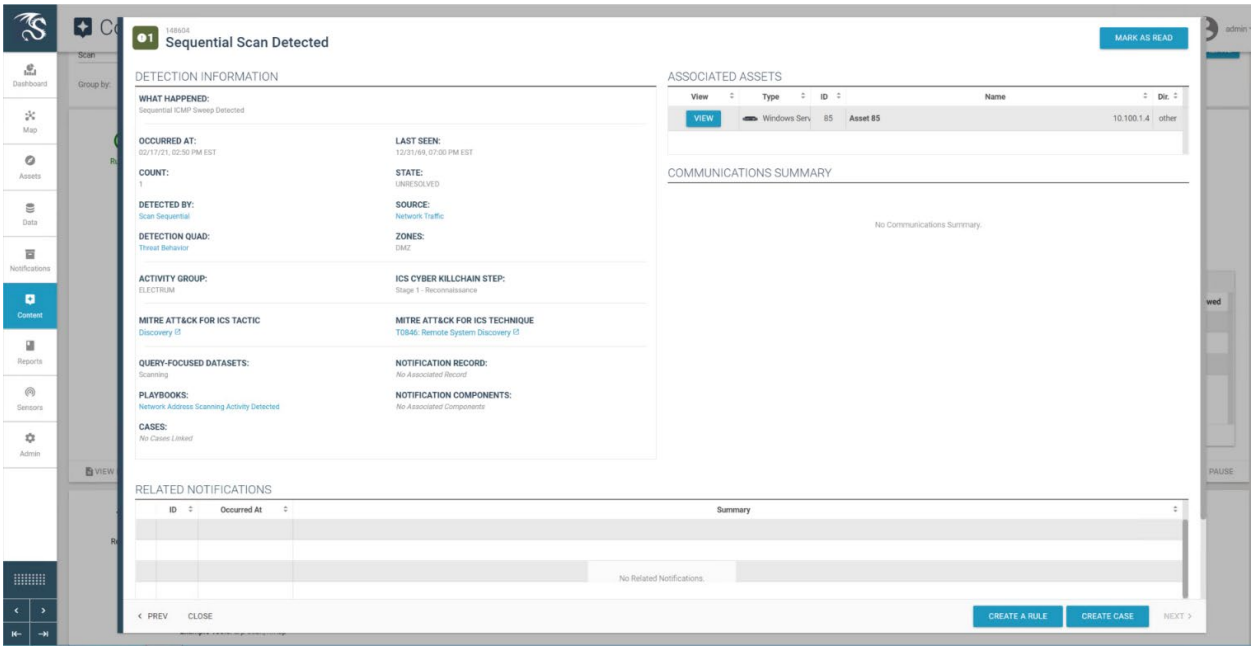
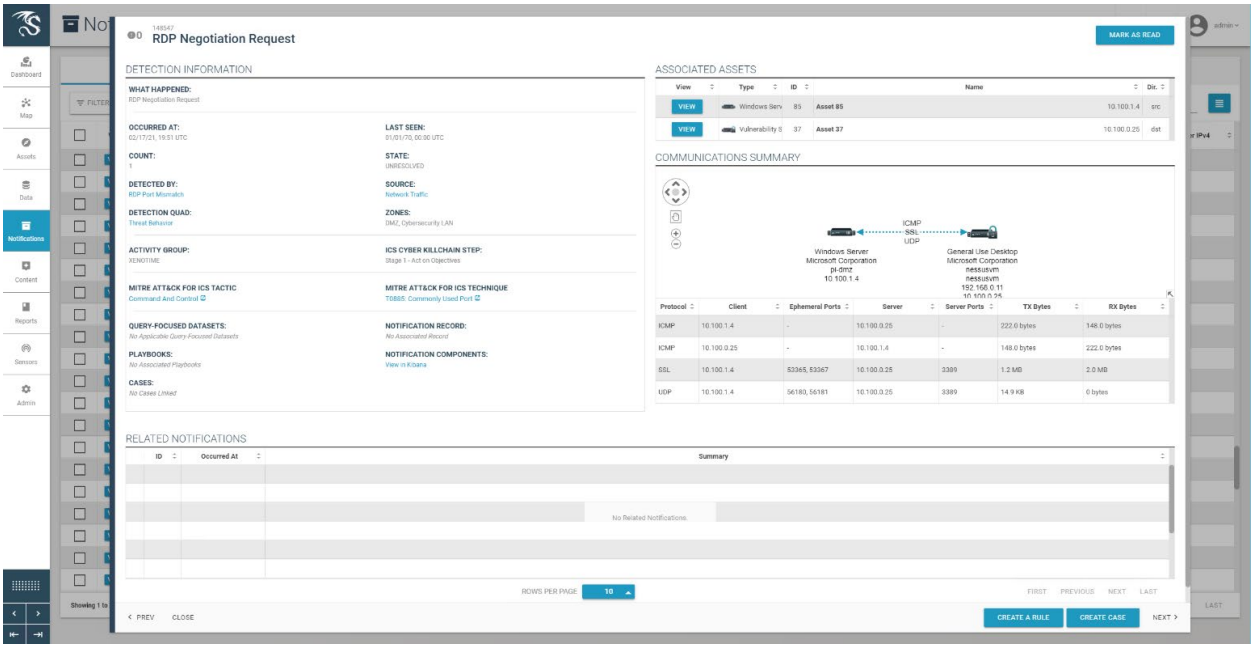


Figure D-25 Detail of RDP Session Activity Between a DMZ System and a Testbed LAN System



D.2.4 Build 4

D.2.4.1 Configuration

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

D.2.4.2 Test Results

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

Figure D-26 Azure Defender for IoT "info" Event Identified Remote Access Connection to the DMZ

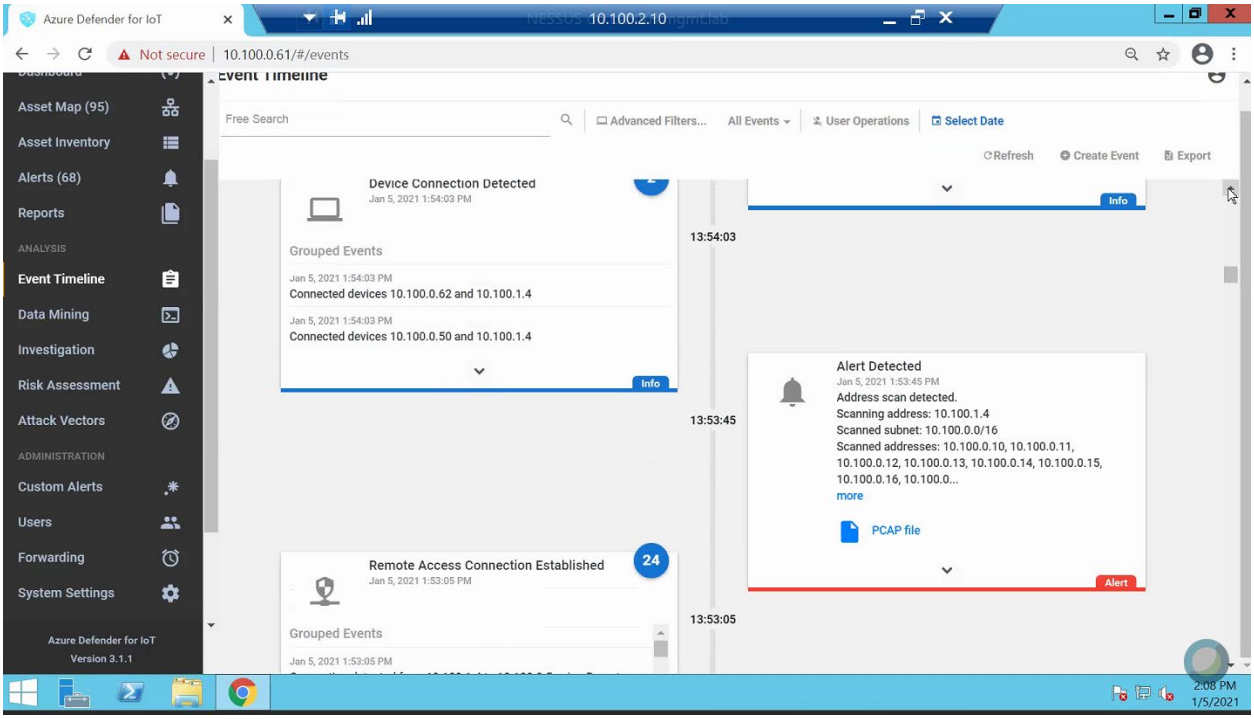


Figure D-27 Alert for Scanning Activity

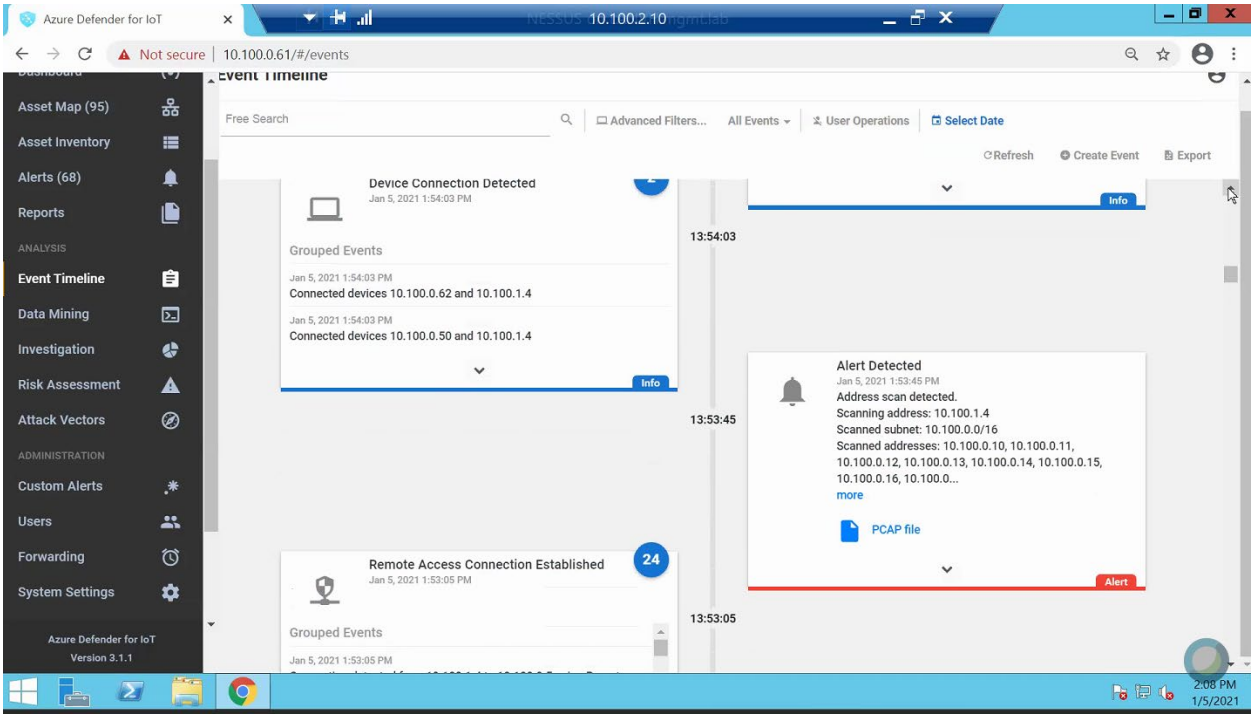


Figure D-28 Details for the Scanning Alert

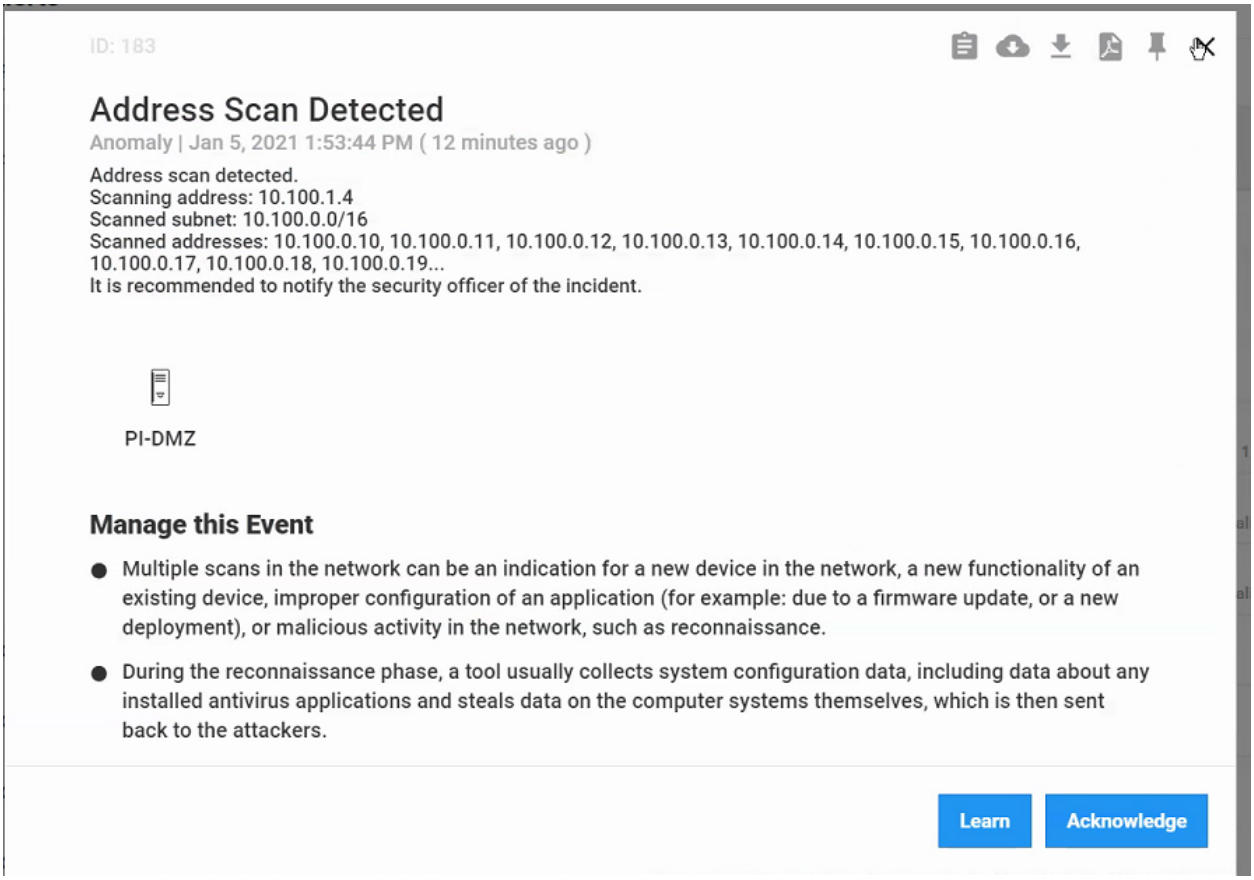


Figure D-29 Detection of RDP Connection into the Manufacturing Environment

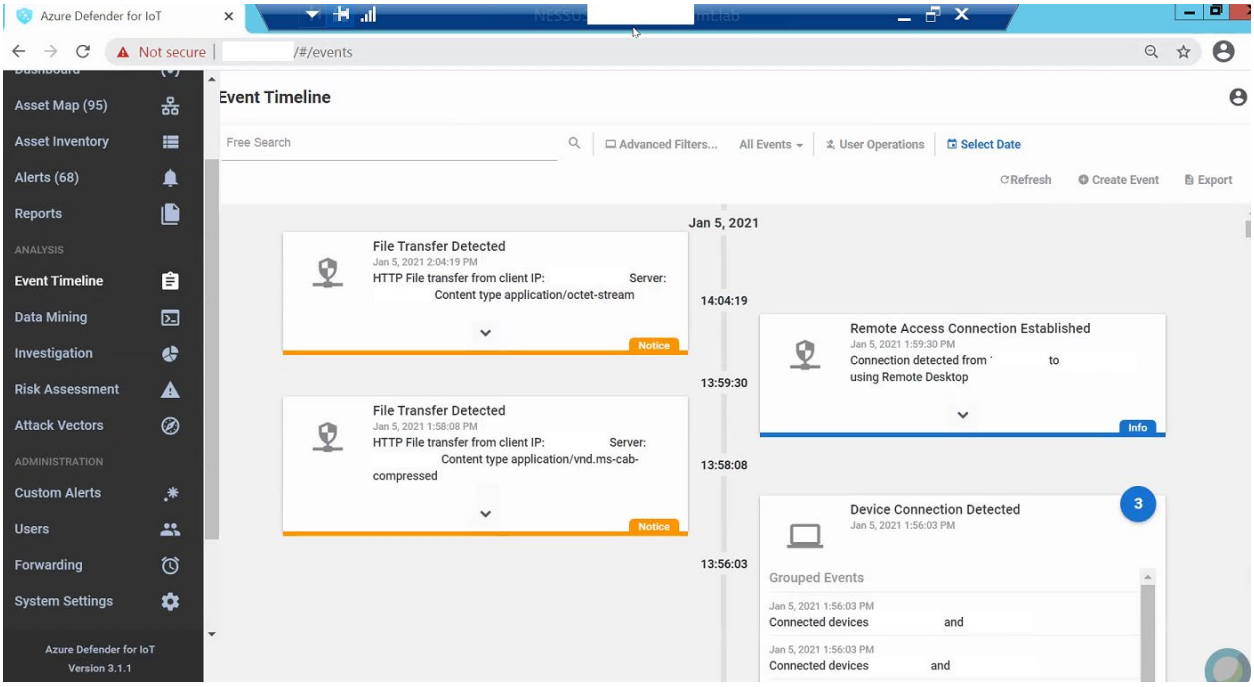
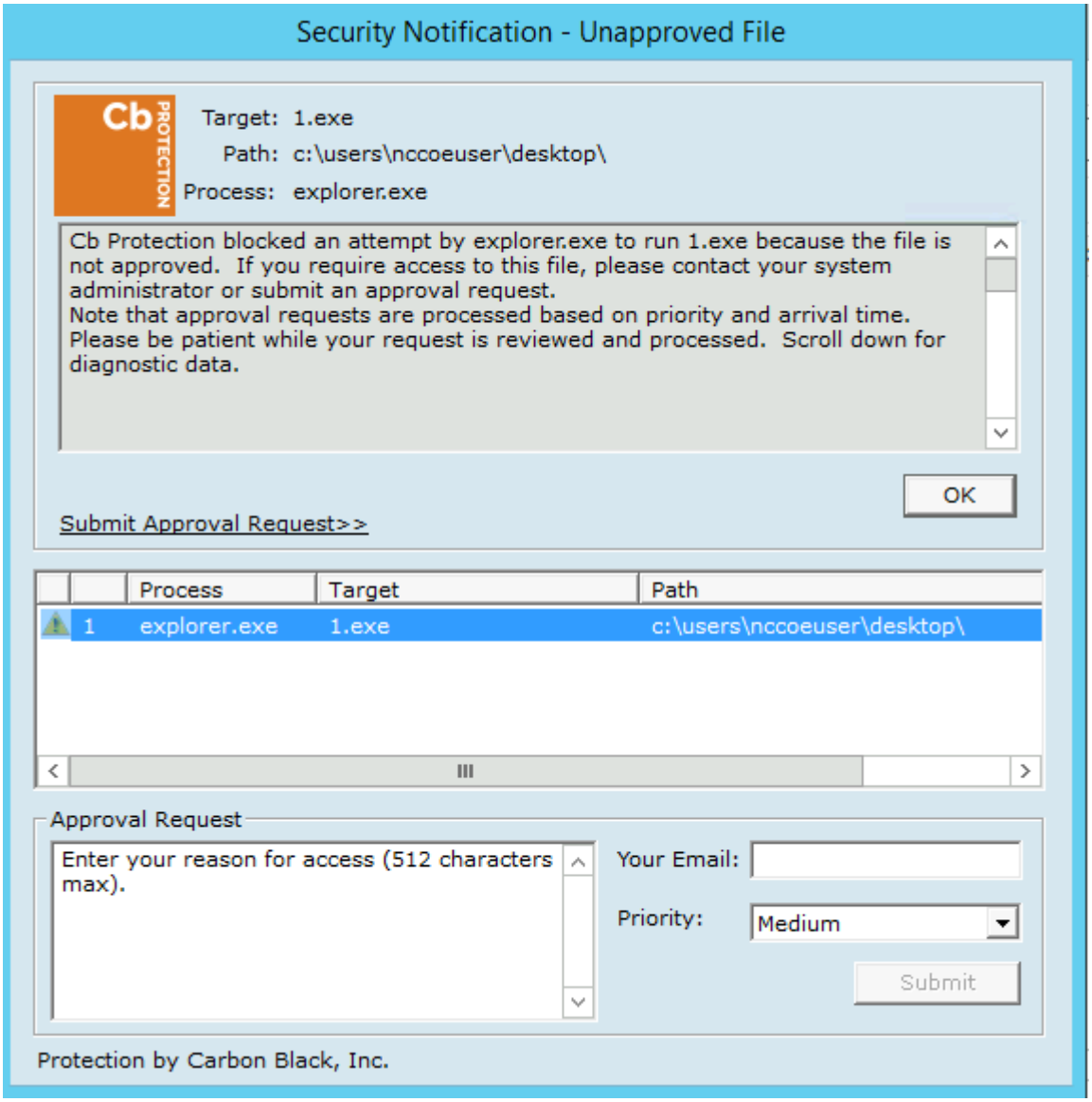


Figure D-30 Carbon Black Shows an Alert for Blocking File 1.exe



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

An authorized user with an authorized remote workstation, infected with a worm-type malware, connects via remote access capabilities to the manufacturing environments. The malware on the remote host attempts to scan the manufacturing environment to identify vulnerable hosts. The expected result

is that the remote access tools effectively stop the worm-type malicious code from propagating to the manufacturing environment from the infected remote workstation.

D.3.1 Build 1

D.3.1.1 Configuration

- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for access PCS environment.

D.3.1.2 Test Results

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

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

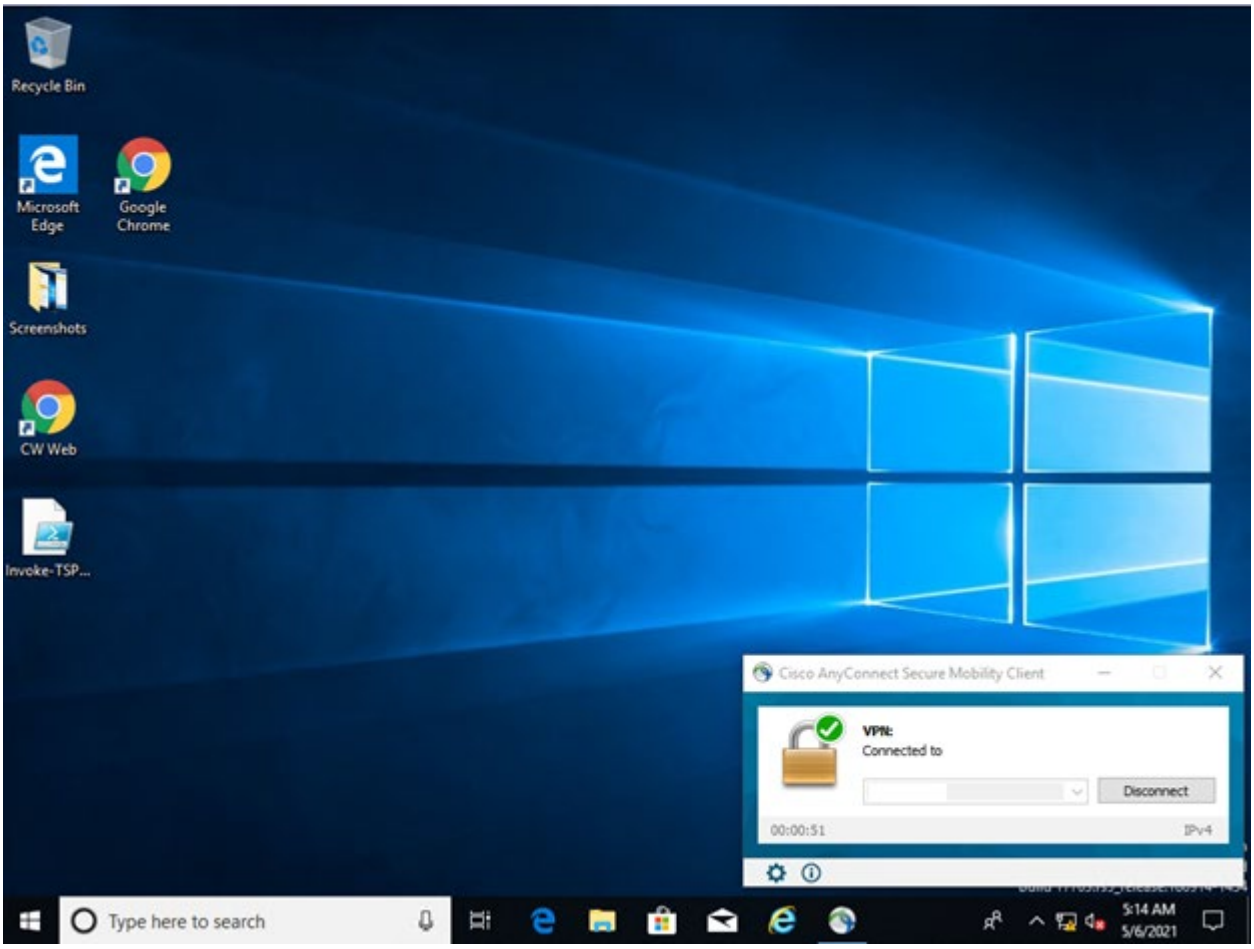
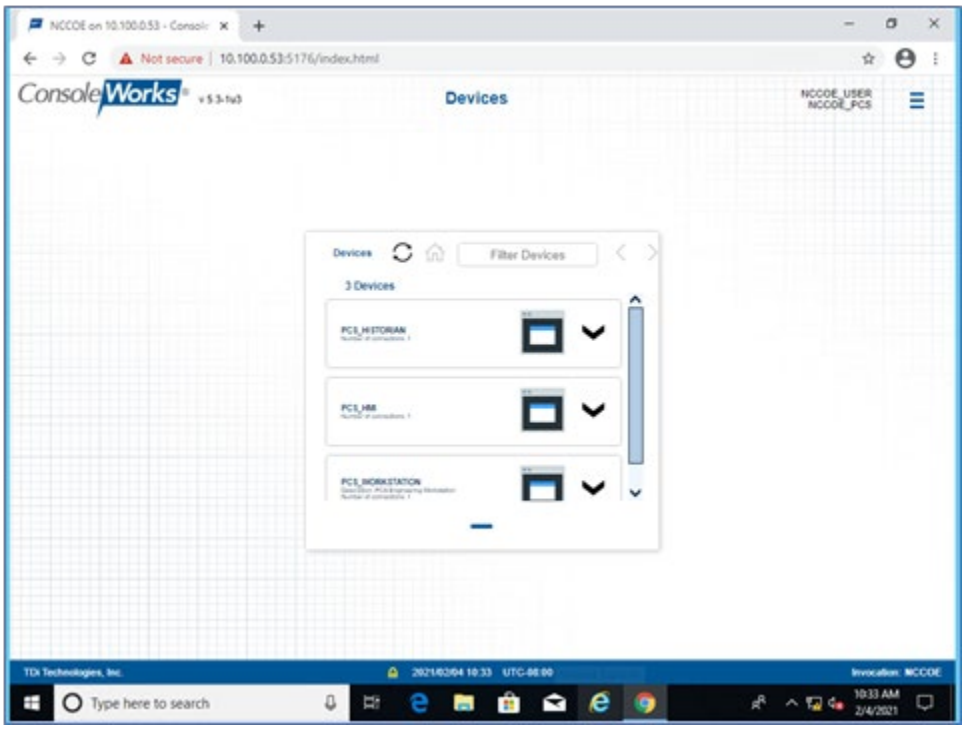


Figure D-32 Remote Access is Being Established Through ConsoleWorks



D.3.2 Build 2

D.3.2.1 Configuration

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

D.3.2.2 Test Results

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

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

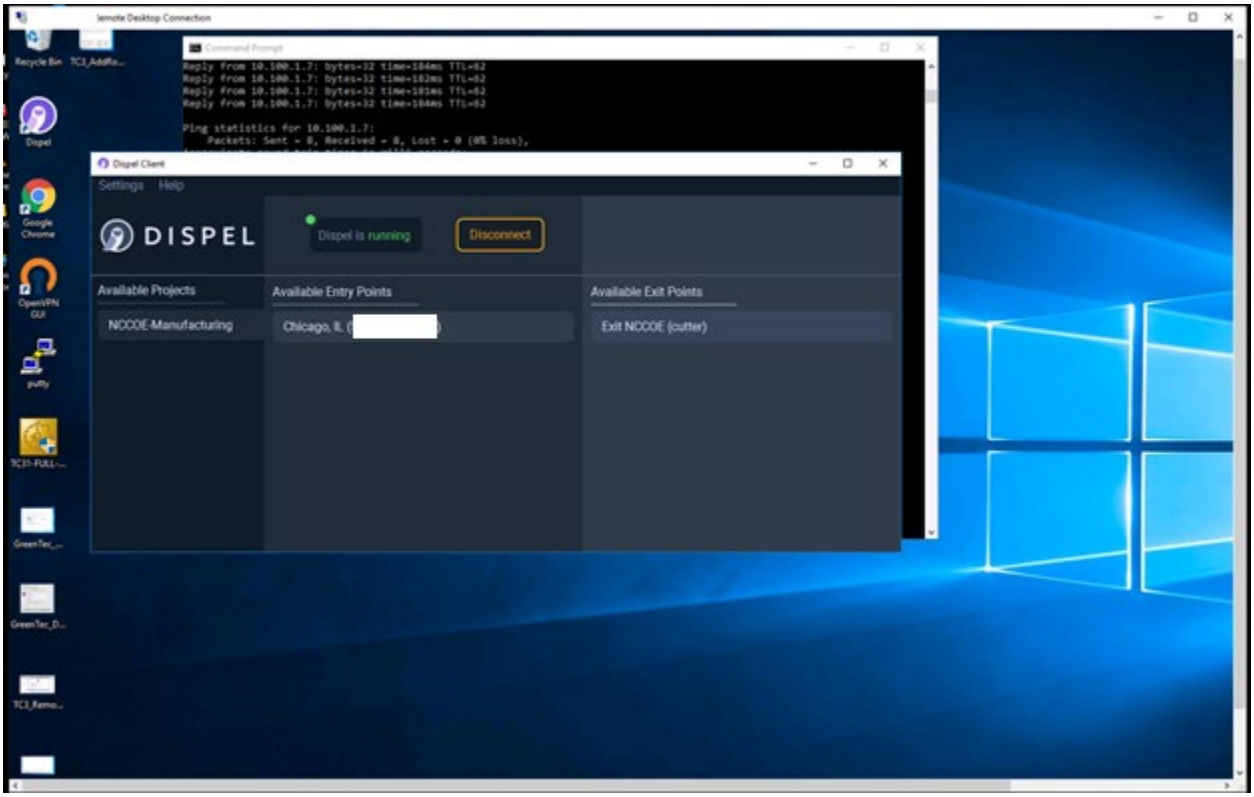


Figure D-34 Nested RDP Session Showing Dispel Connection into the PCS Workstation

D.3.3 Build 3

D.3.3.1 Configuration

- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users to access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for access CRS environment.

D.3.3.2 Test Results

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

Figure D-35 VPN Connection to Manufacturing Environment

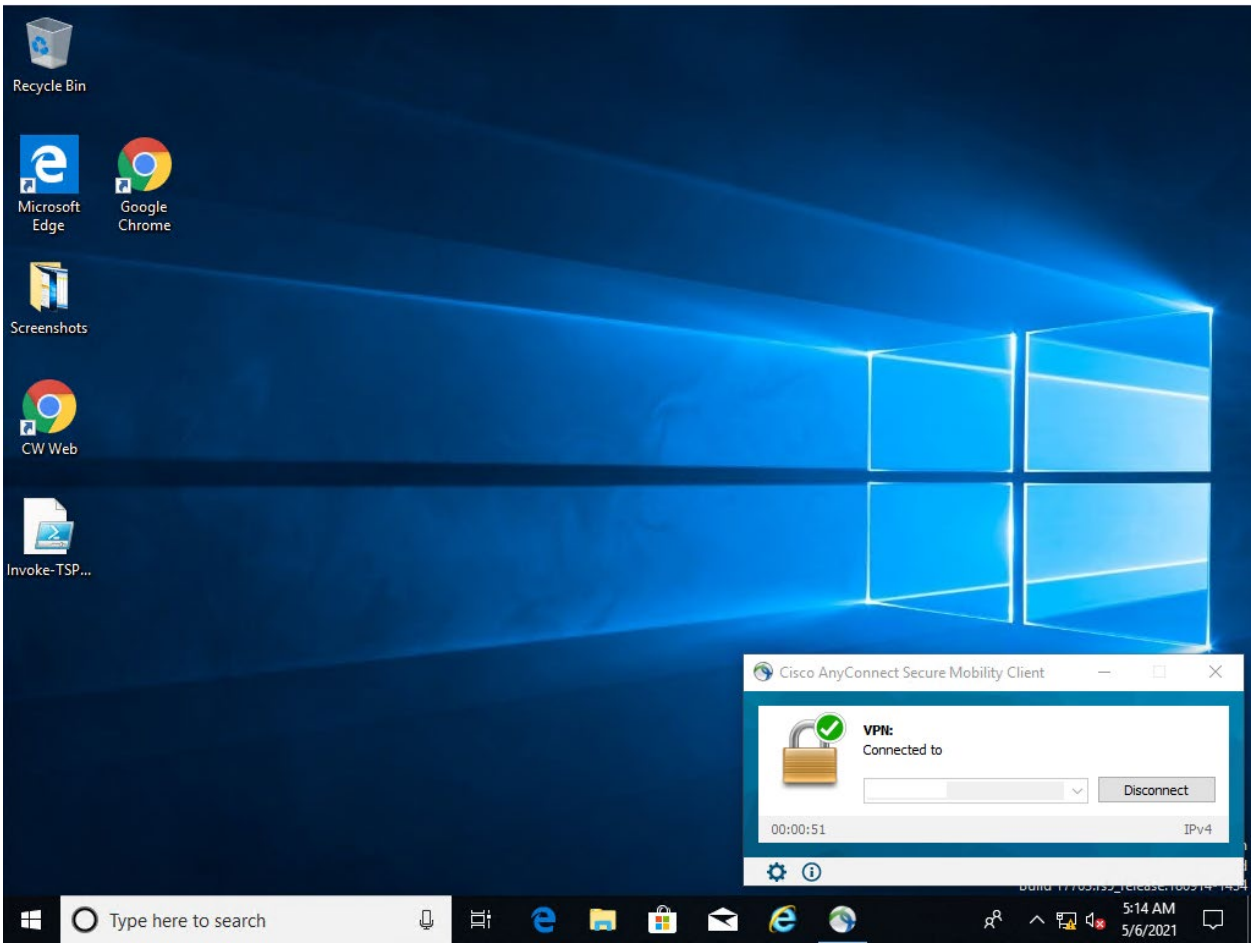
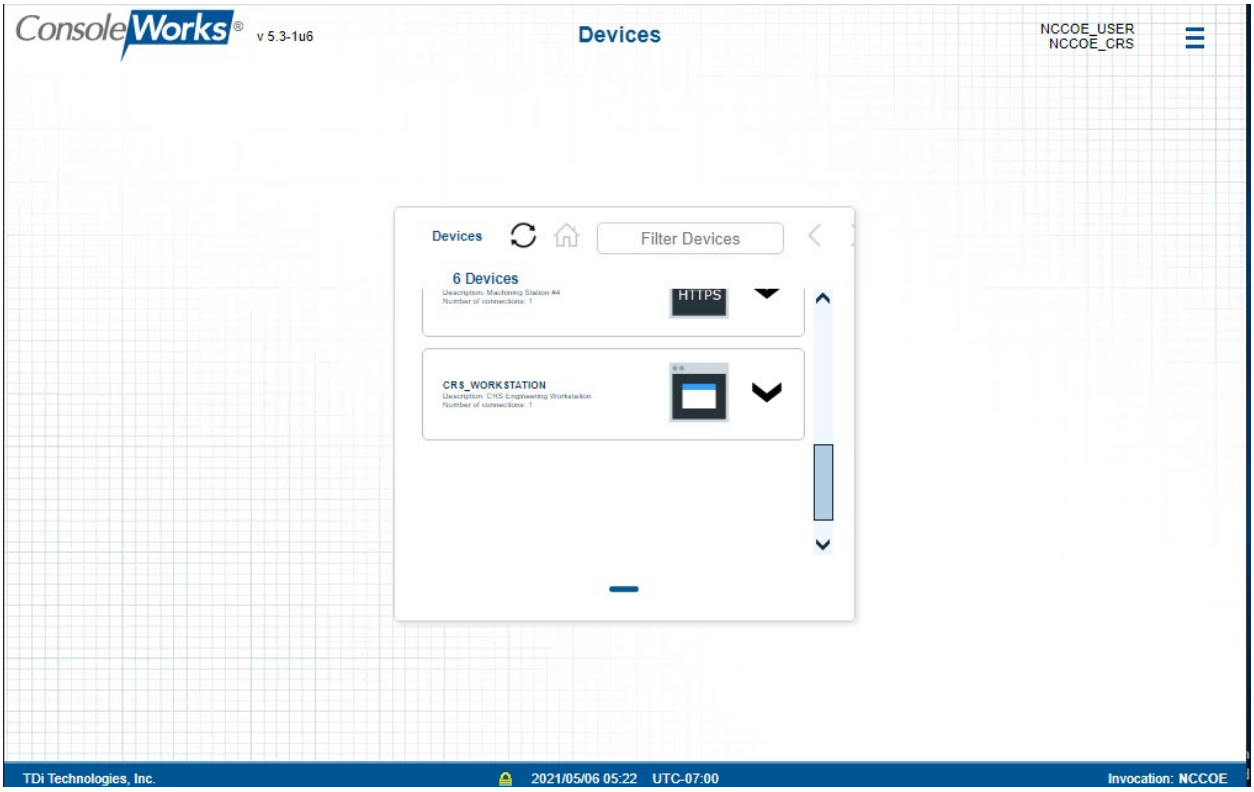


Figure D-36 Remote Access is Being Established Through ConsoleWorks



D.3.4 Build 4

D.3.4.1 Configuration

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

D.3.4.2 Test Results

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

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

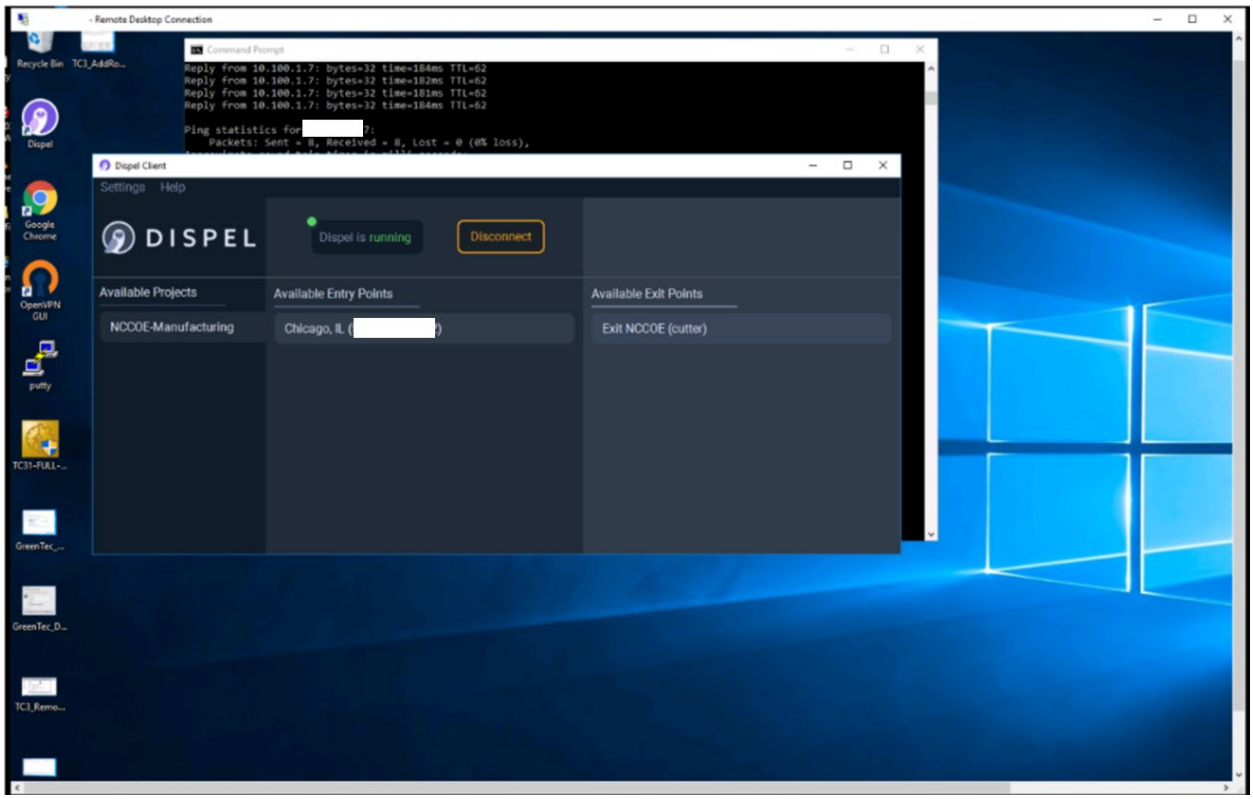
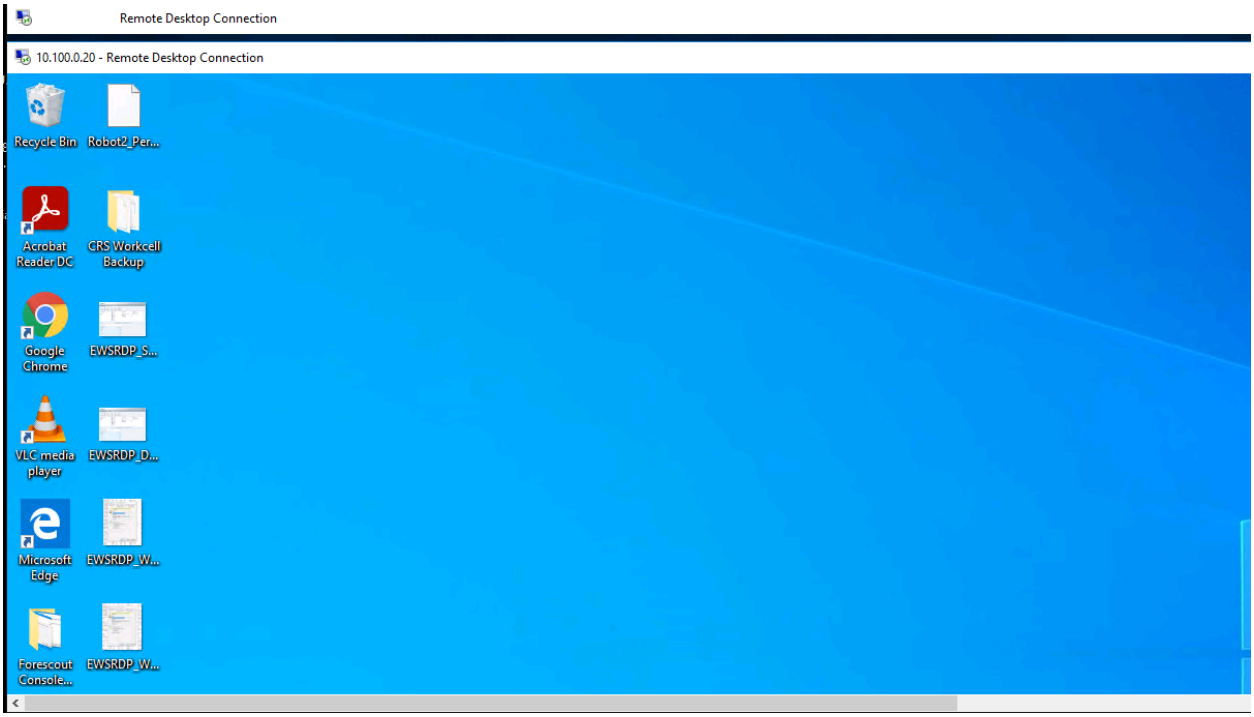


Figure D-38 Nested RDP Session Showing Dispel Connection into the CRS Workstation



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

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

D.4.1 Build 1

D.4.1.1 Configuration

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

D.4.1.2 Test Results

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

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

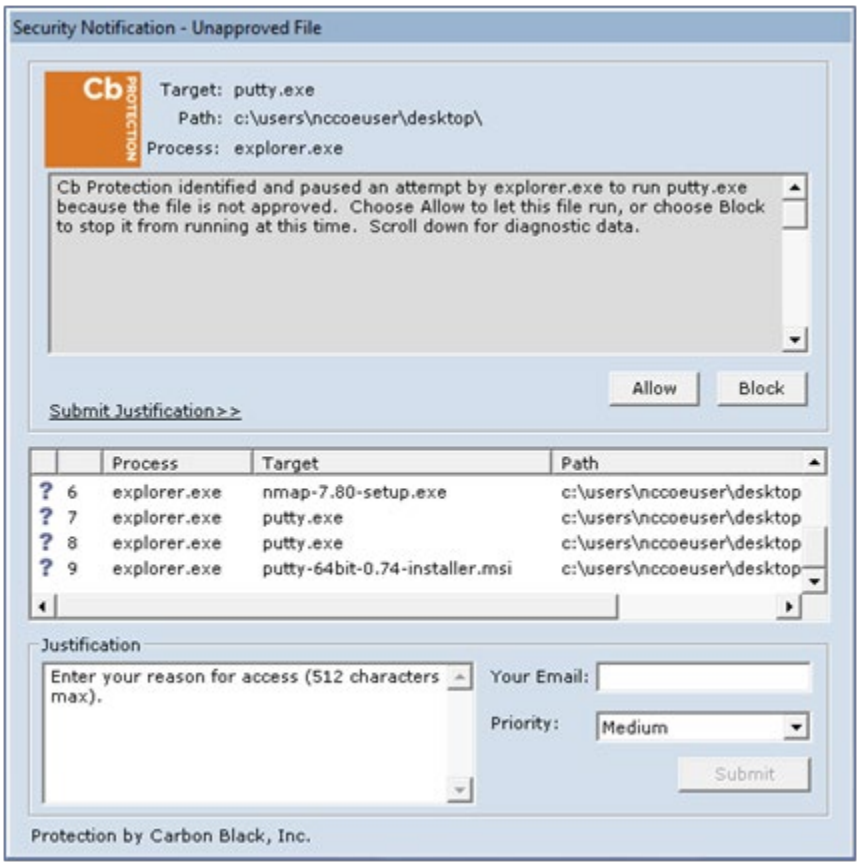


Figure D-40 Tenable.ot Alert With the SMB Connection Between the HMI and the GreenTec Server

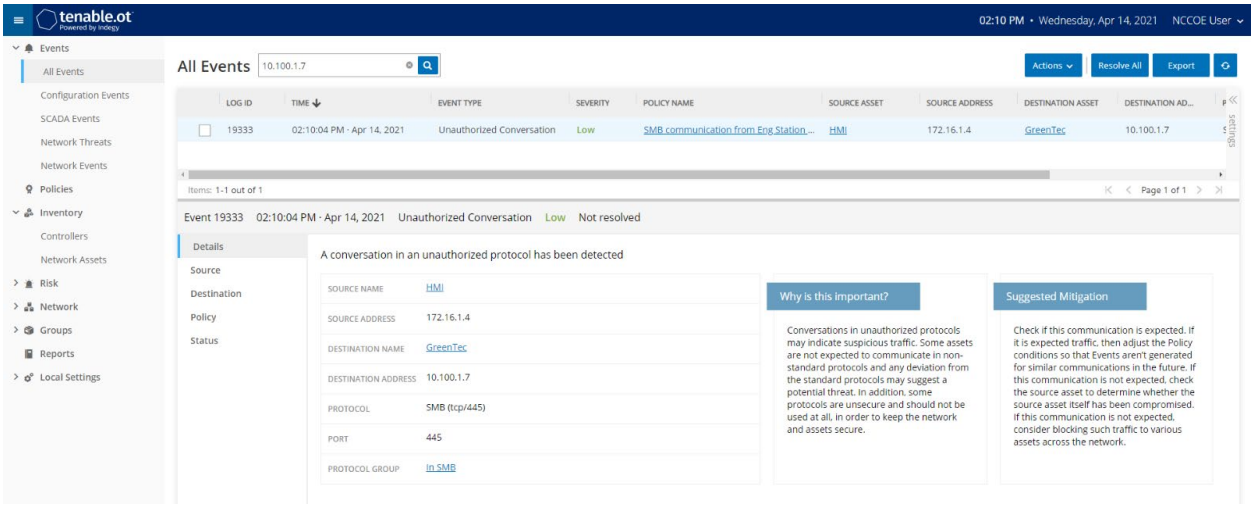
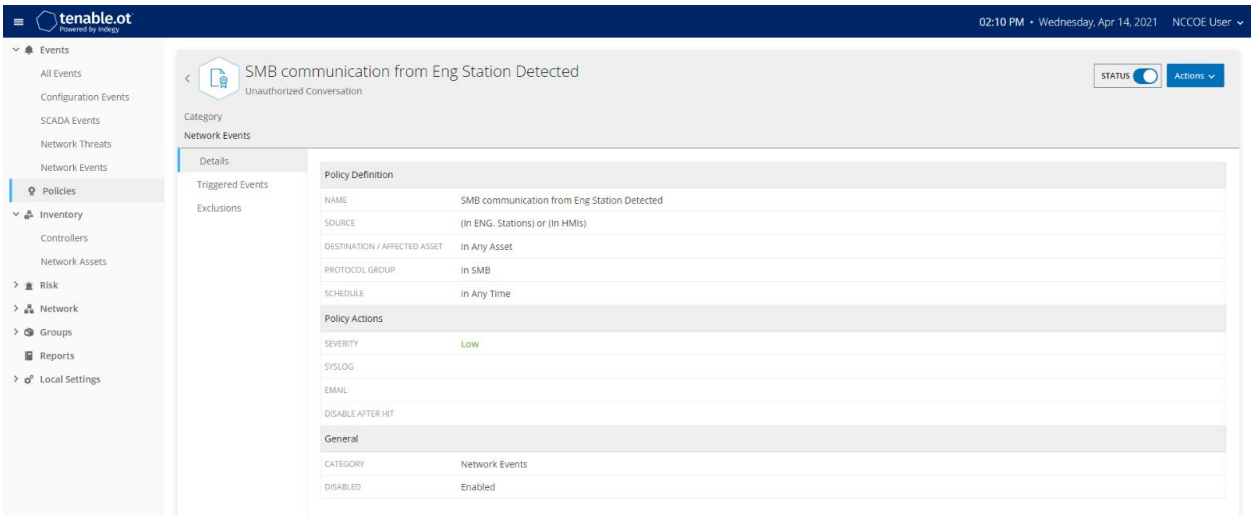


Figure D-41 Tenable.ot Alert Details of the SMB Connection Between the HMI and the network file system (NFS) Server in the DMZ



D.4.2 Build 2

D.4.2.1 Configuration

- Application Allowlisting: Windows SRP
  - Allowlisting policies are applied to systems in the DMZ, Testbed LAN, and PCS VLAN 1 and 2.

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

D.4.2.2 Test Results

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

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

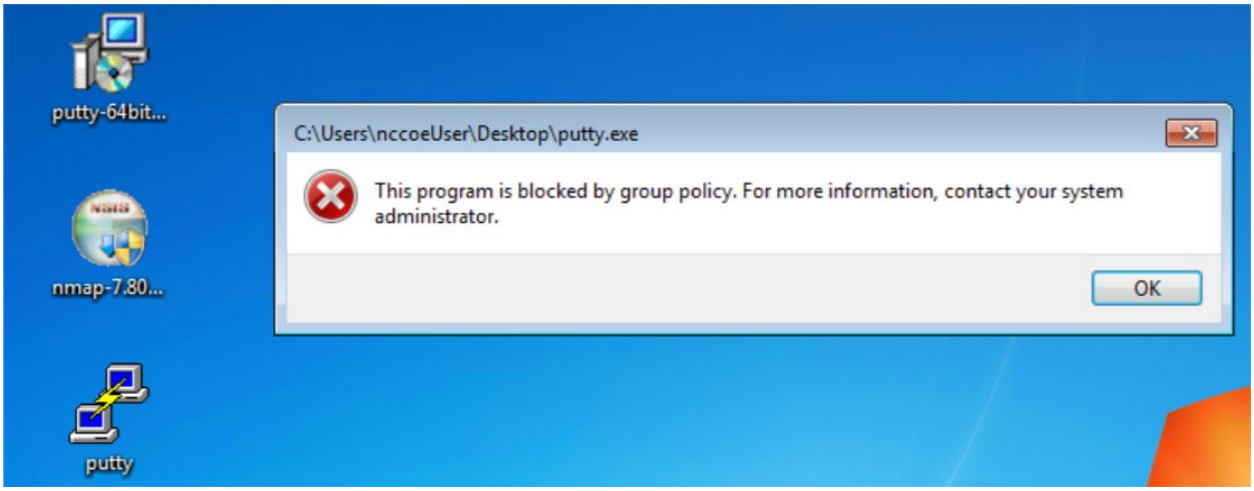


Figure D-43 putty-64bit-0.74-installer.msi is blocked by Windows SRP

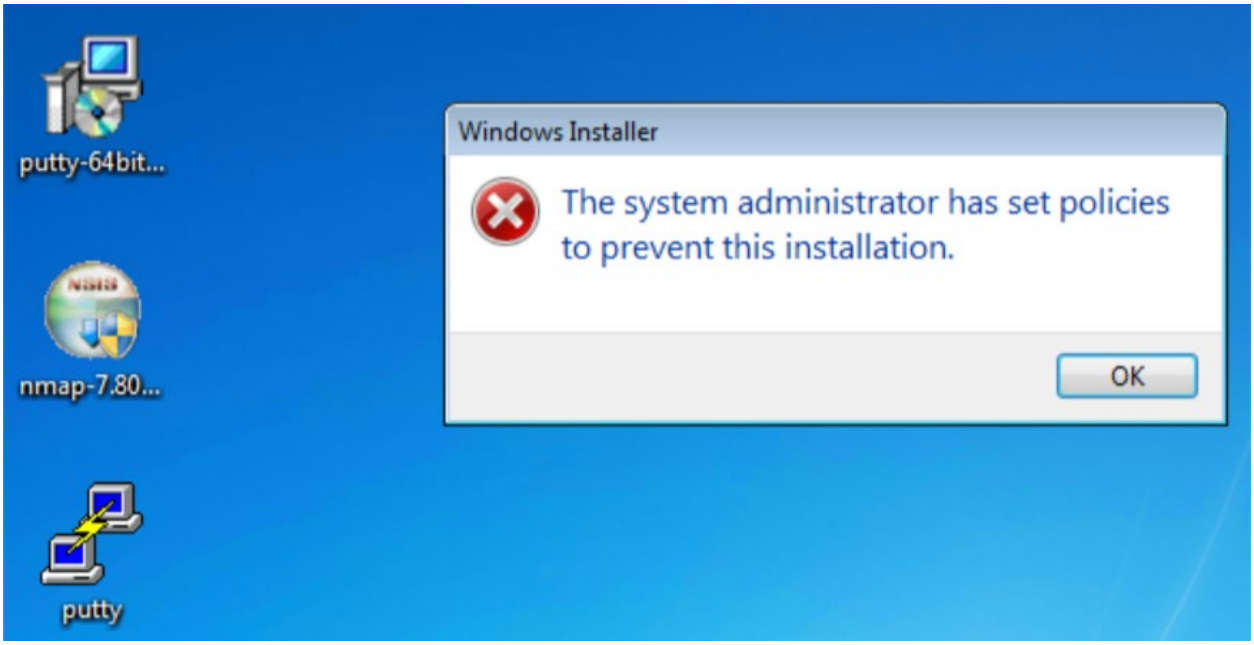


Figure D-44 Forescout Alert on the File Transfer Activity

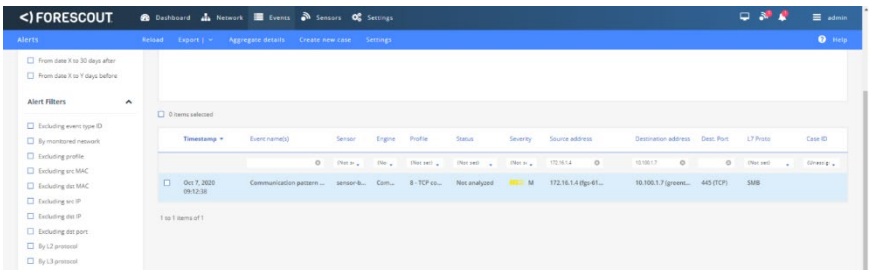
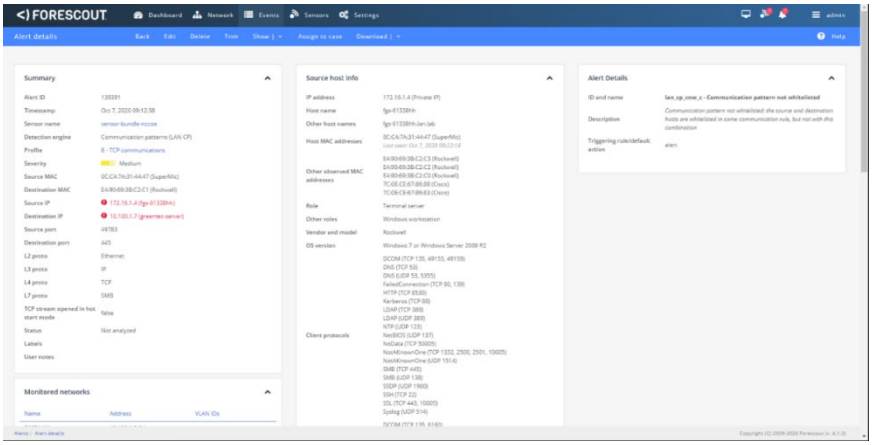


Figure D-45 Forescout Alert Details for the File Transfer Activity



D.4.3 Build 3

D.4.3.1 Configuration

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

D.4.3.2 Test Results

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

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

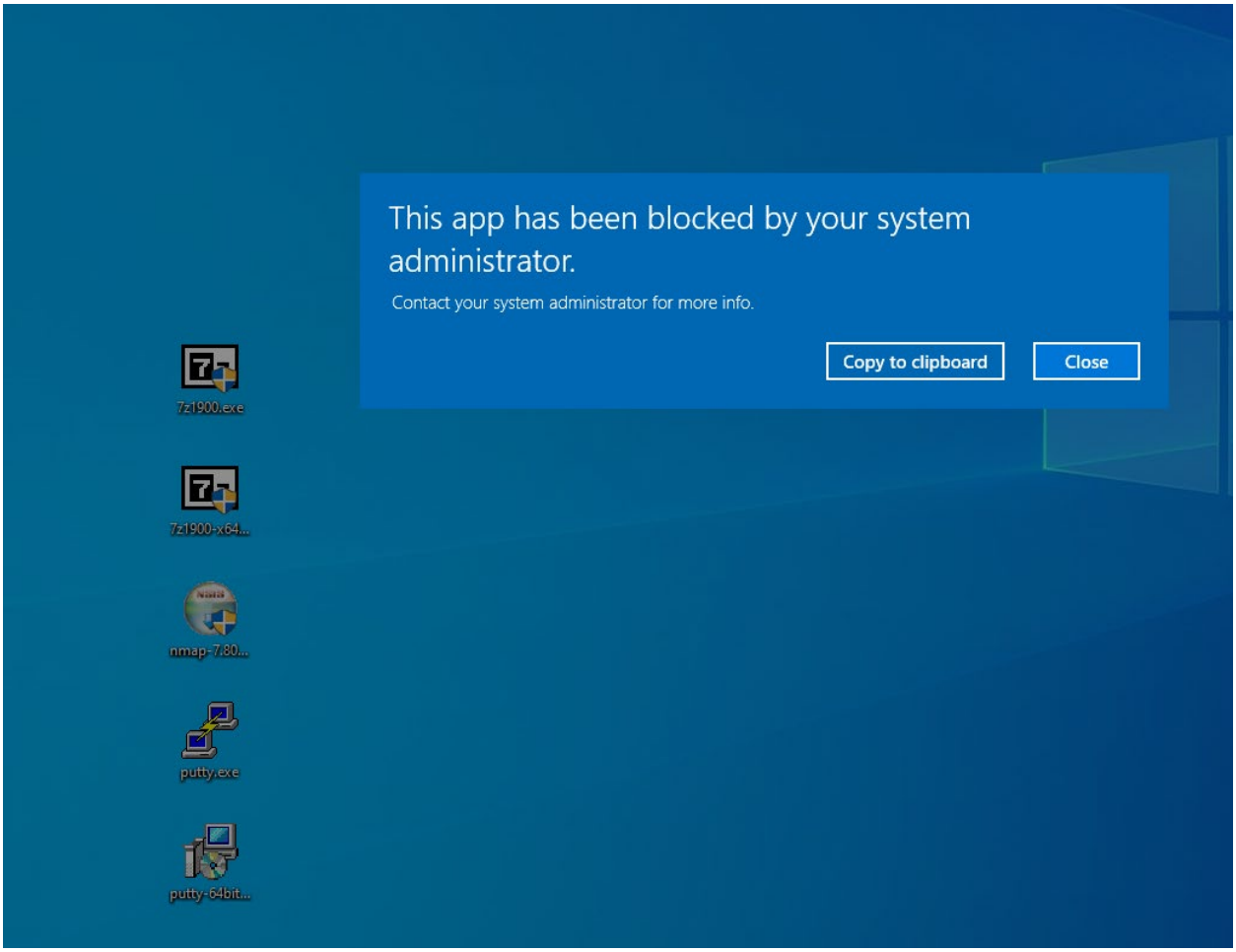


Figure D-47 putty-64bit-0.74-installer.msi is Blocked by Windows SRP

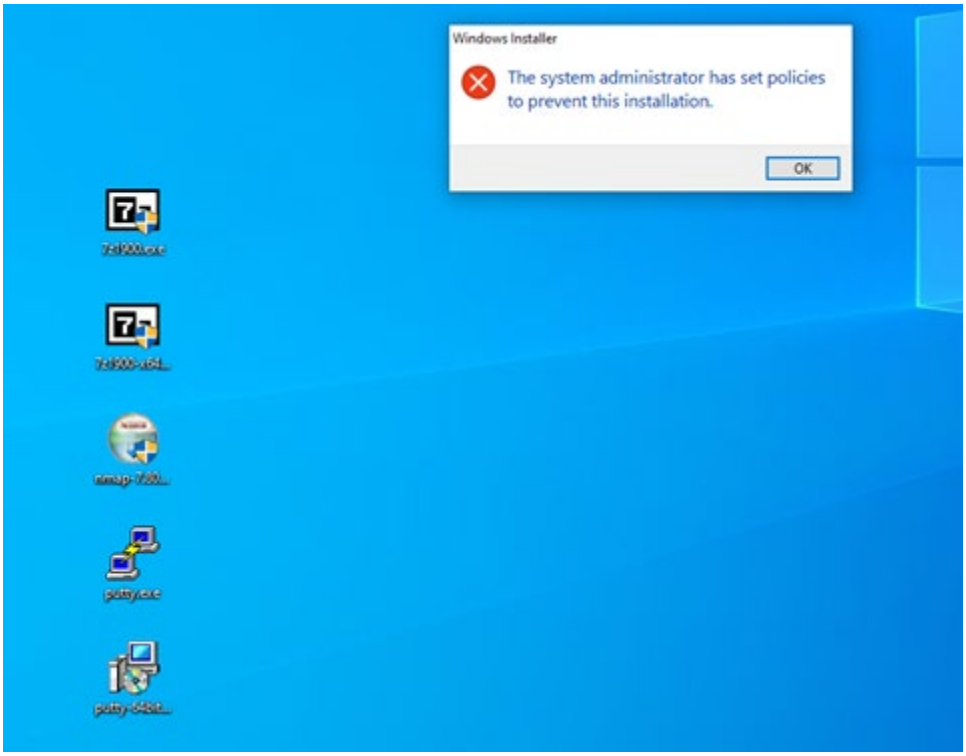


Figure D-48 Dragos Alert on the File Transfer Activity

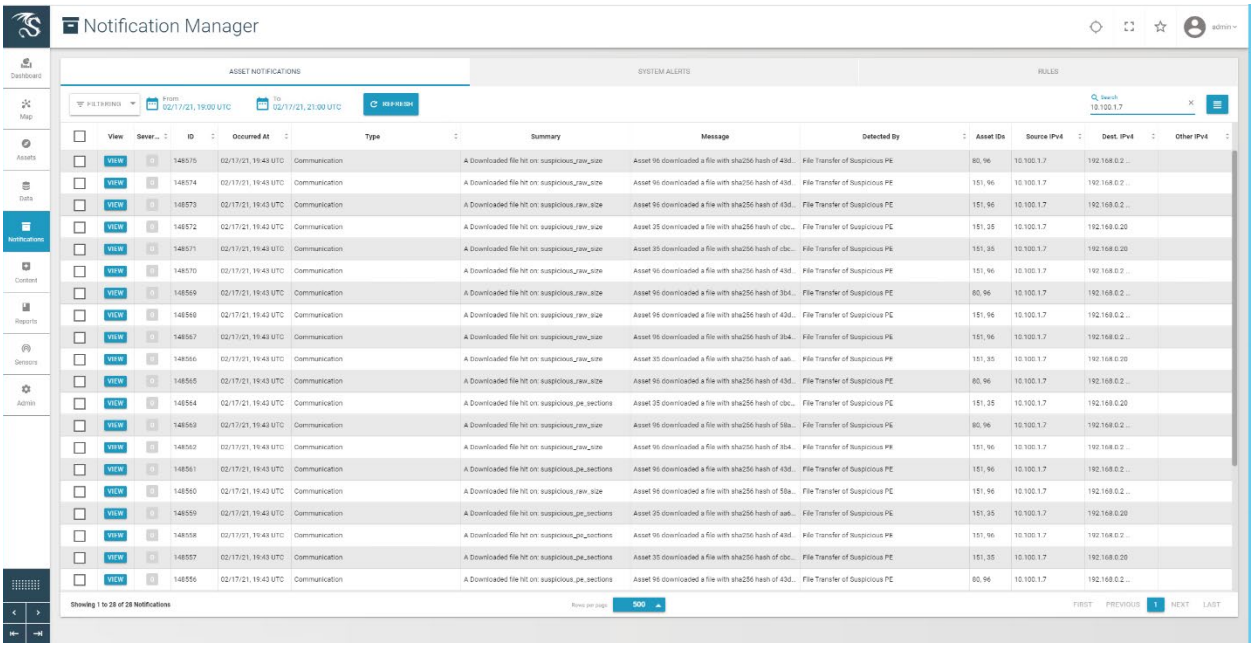
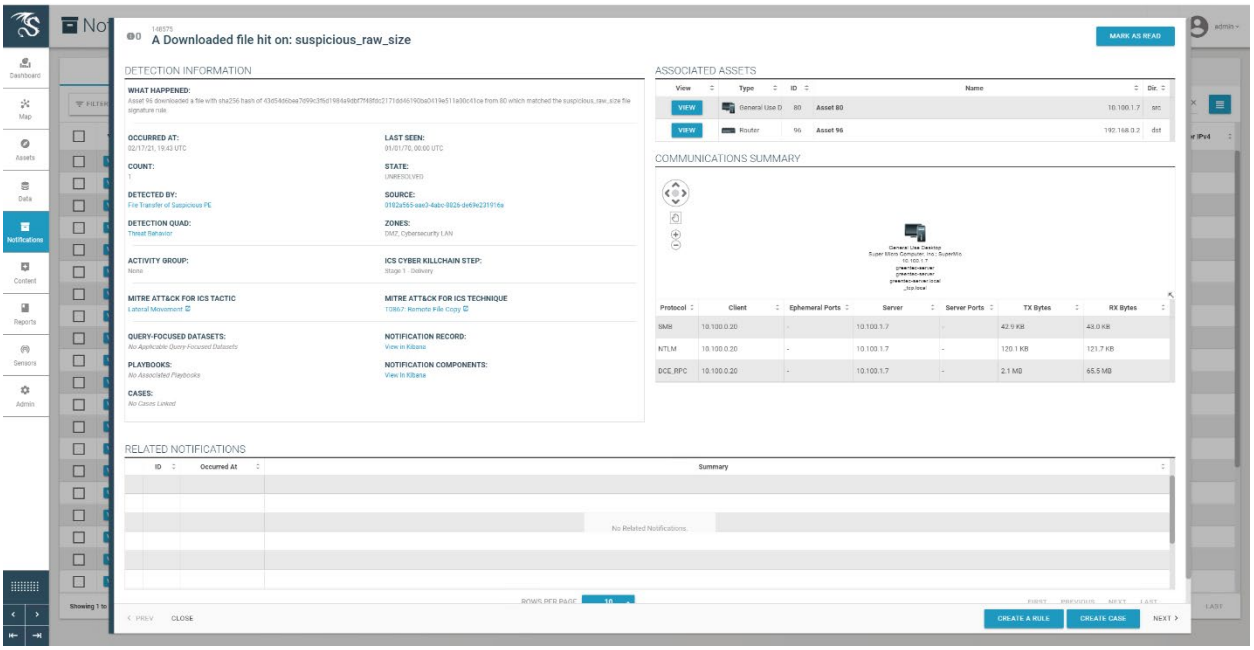


Figure D-49 Dragos Alert Details of the File Transfer Alert



D.4.4 Build 4

D.4.4.1 Configuration

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

D.4.4.2 Test Results

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

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

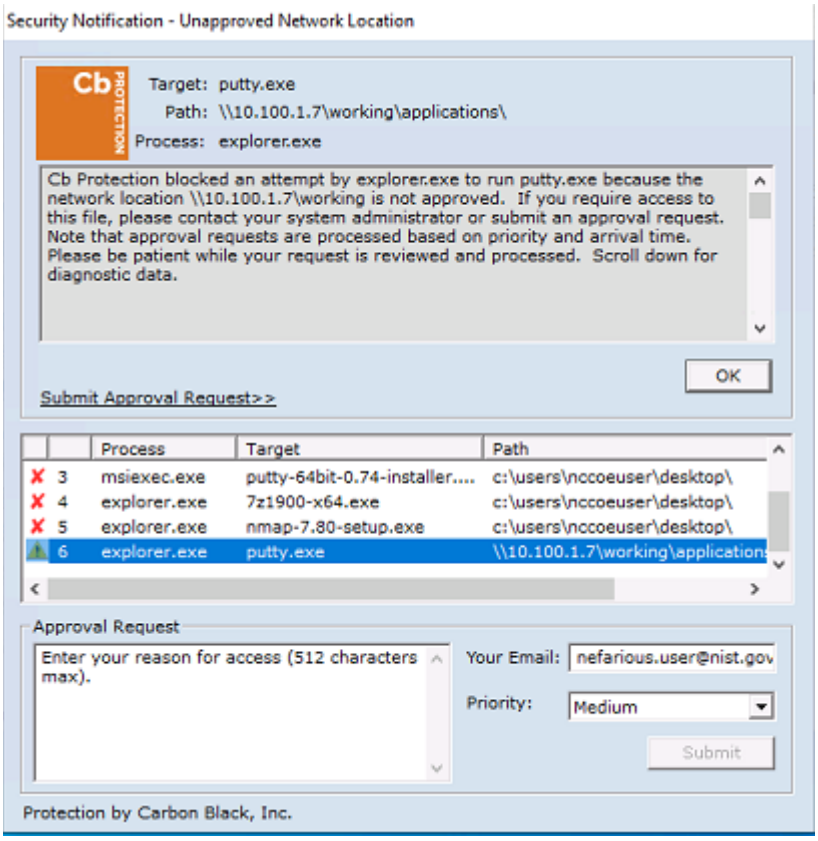


Figure D-51 Carbon Black Alert Showing Execution of putty-64bit-0.74-installer.msi Being Blocked

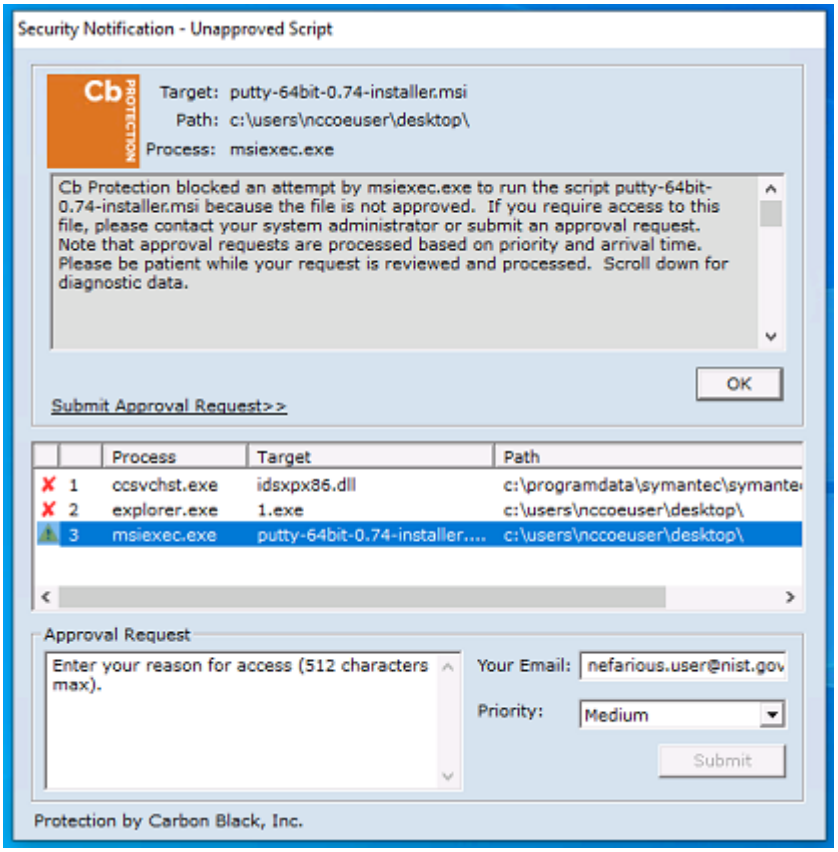


Figure D-52 Azure Defender for IoT Alert Dashboard Showing Detection of a New Activity

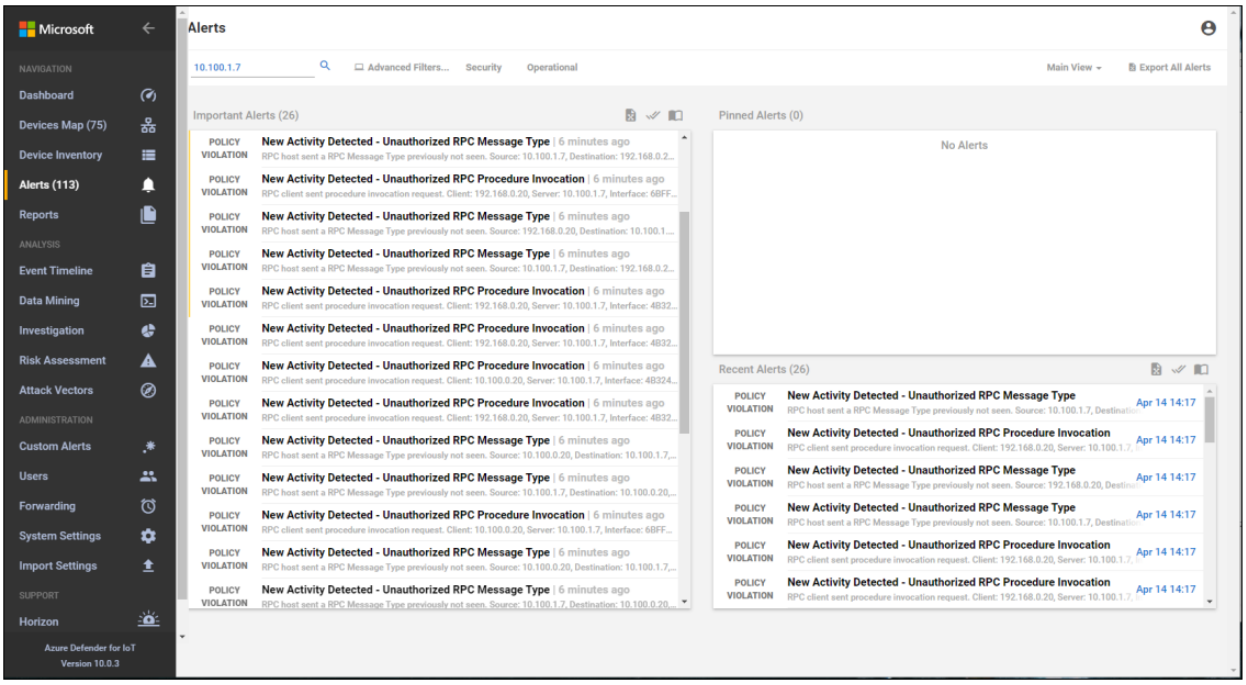


Figure D-53 Azure Defender for IoT Alert Details Showing RPC Connection Between the DMZ and the Testbed LAN

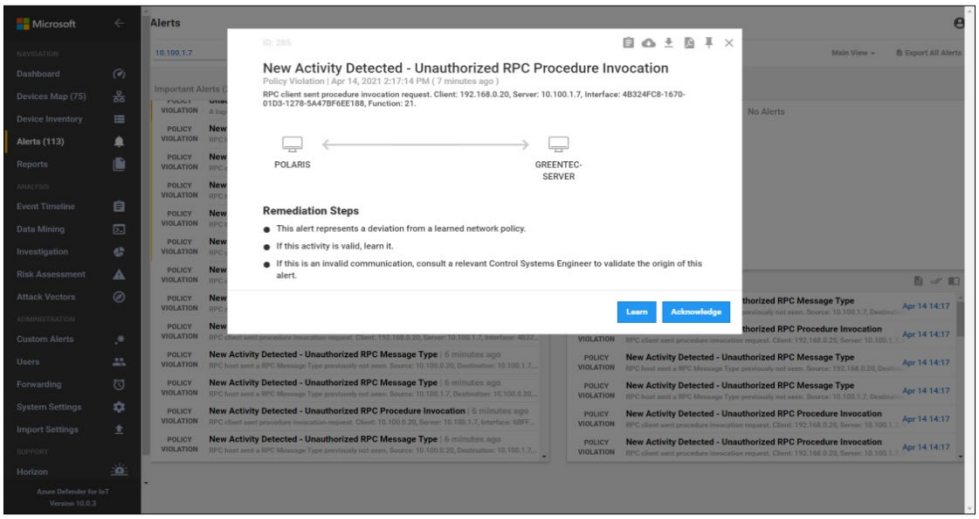
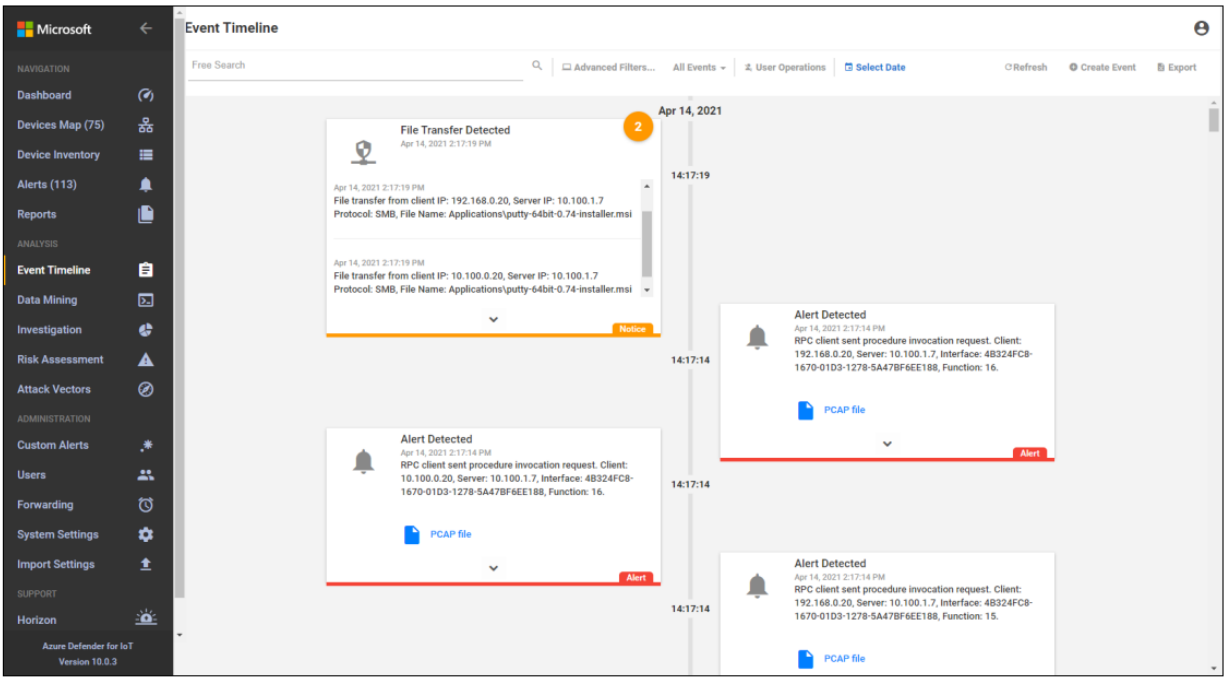


Figure D-54 Azure Defender for IoT Event Alert Timeline Showing the File Transfer



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

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

D.5.1 Build 1

D.5.1.1 Configuration

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

D.5.1.2 Test Results

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

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

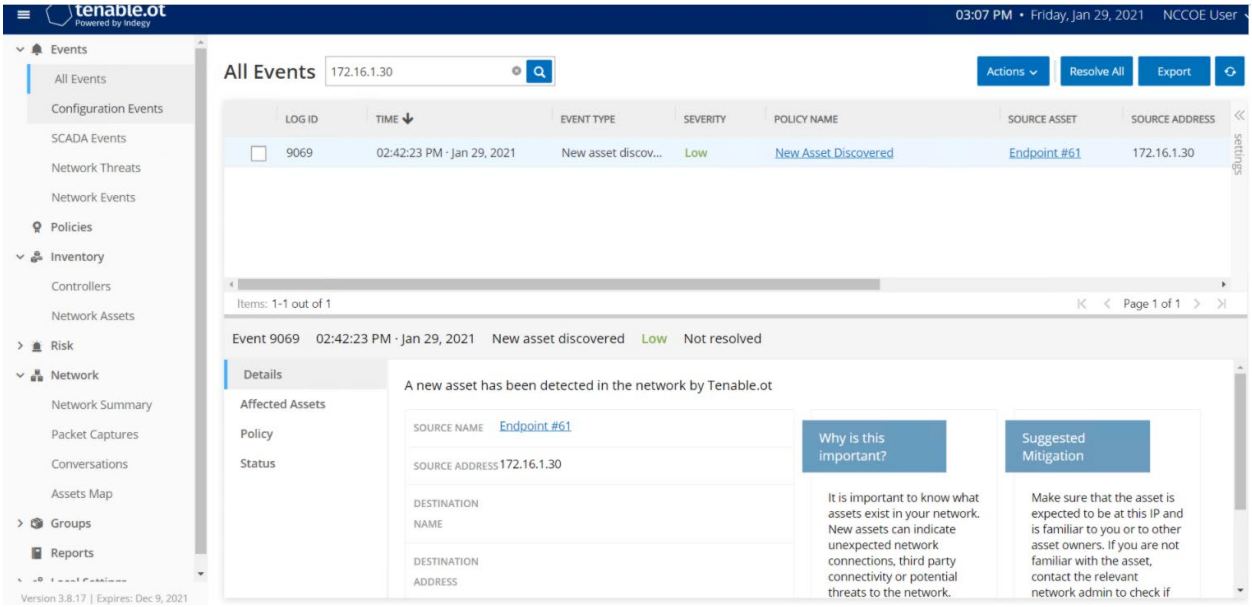
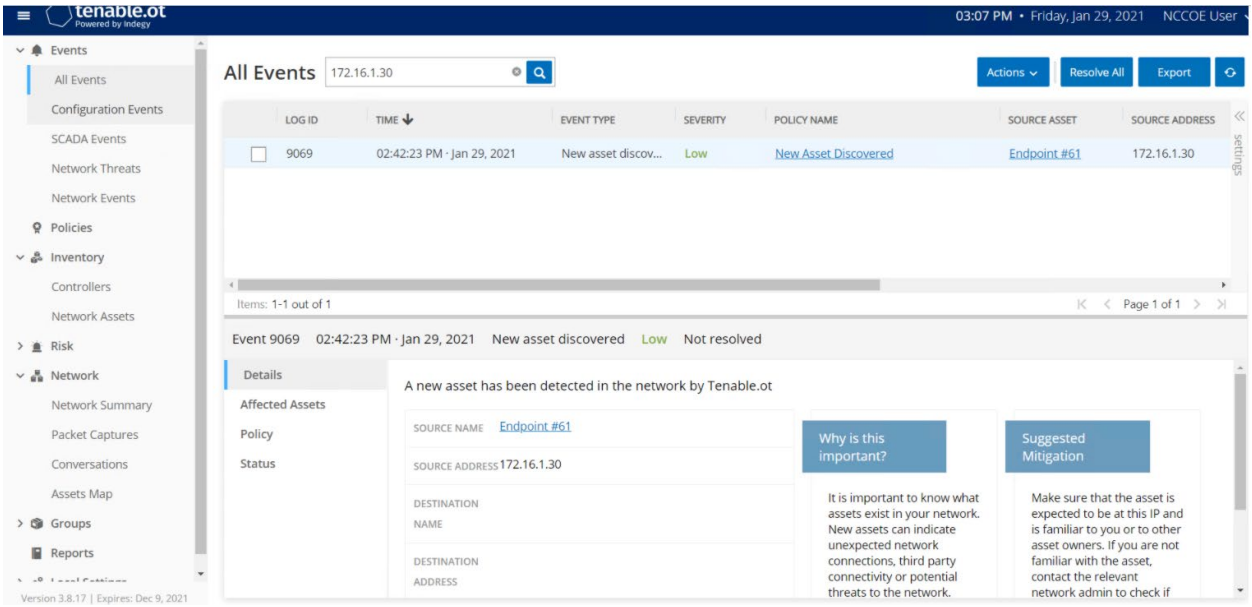


Figure D-56 Tenable.ot Event Showing Unauthorized SSH Activities



D.5.2 Build 2

D.5.2.1 Configuration

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

D.5.2.2 Test Results

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

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

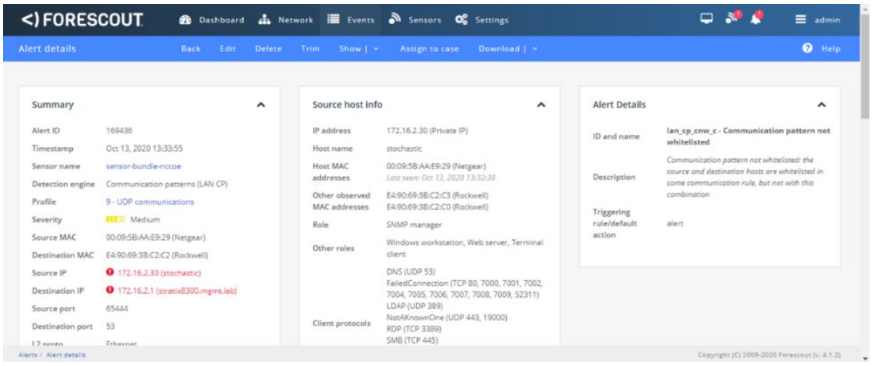
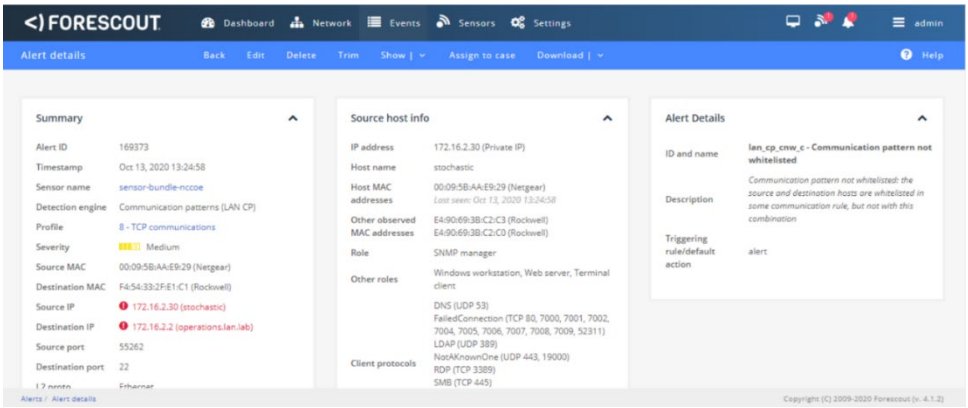


Figure D-58 Forescout alert showing the SSH connection

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



D.5.3 Build 3

D.5.3.1 Configuration

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

D.5.3.2 Test Results

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

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

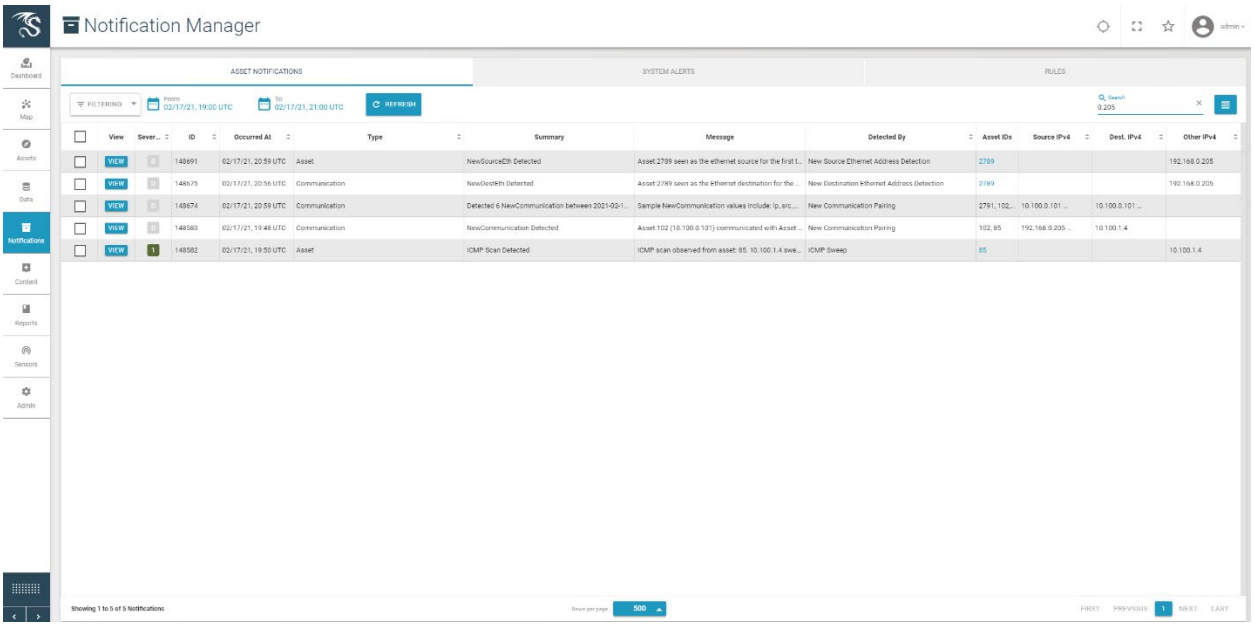


Figure D-61 Details of Network Scanning Activity

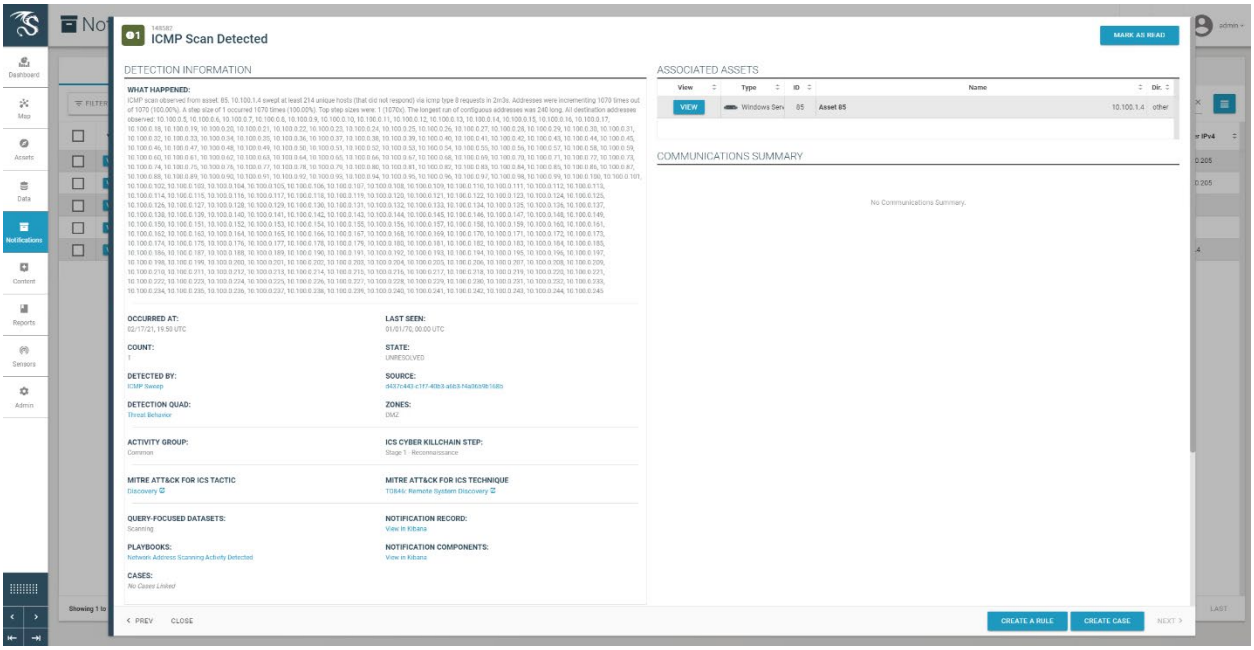


Figure D-62 Additional Details of Network Scanning Activity

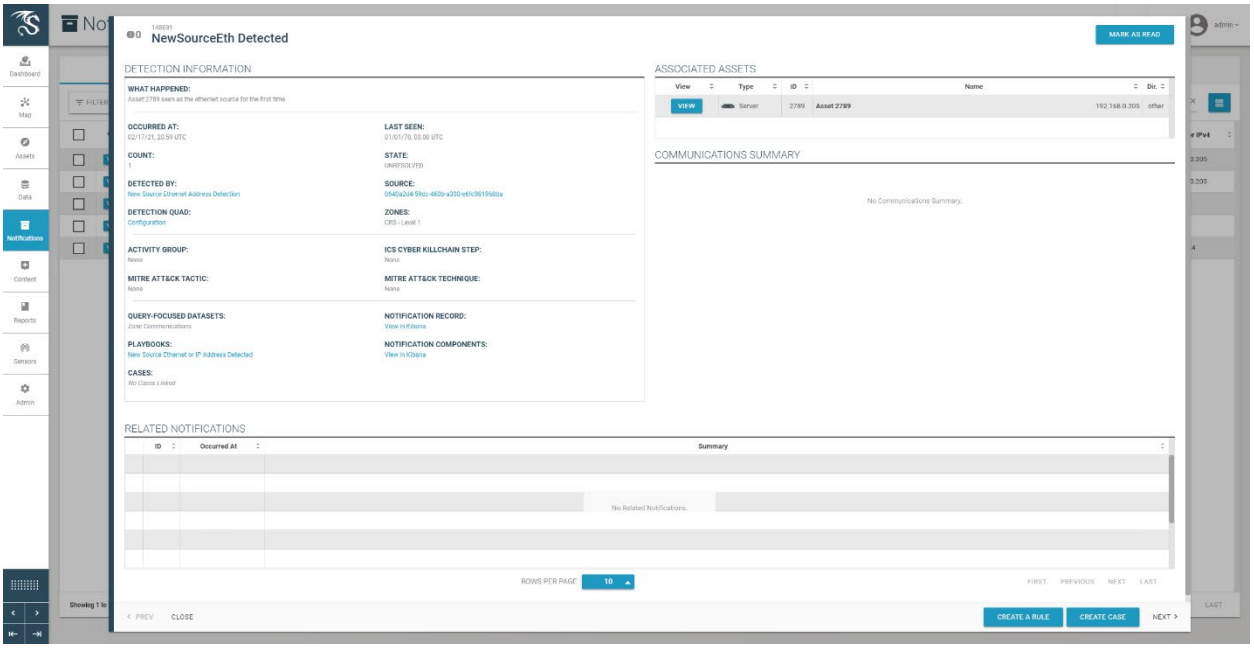
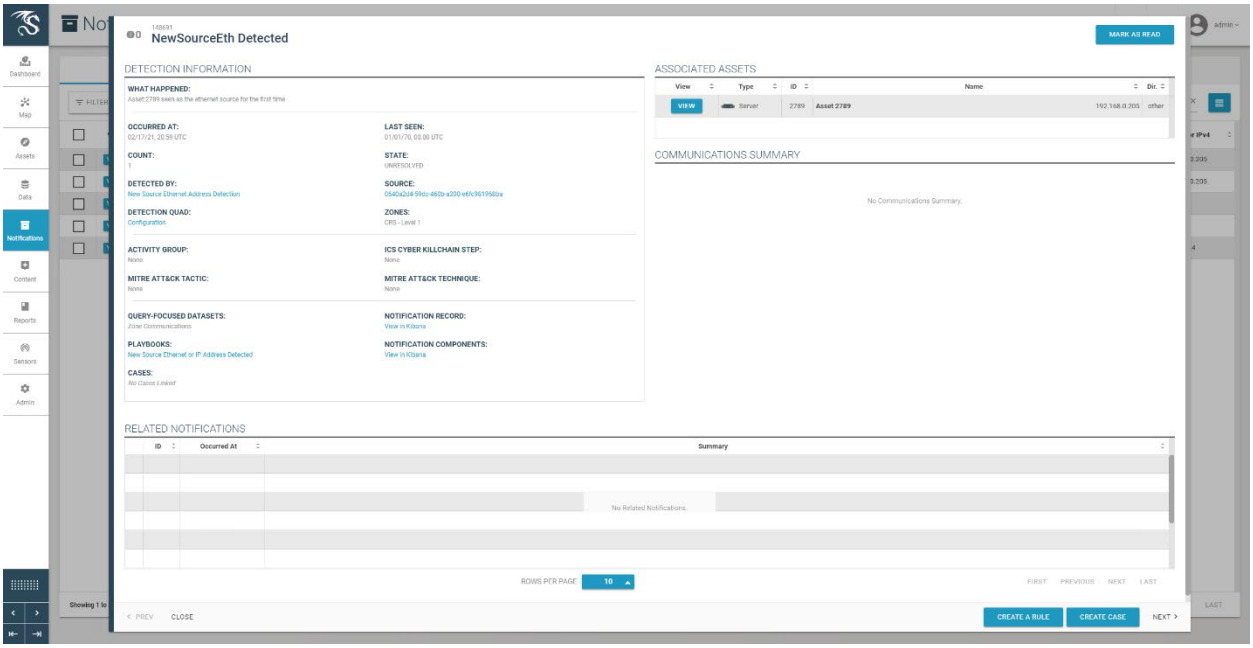


Figure D-63 Alert for New Asset on the Network



D.5.4 Build 4

D.5.4.1 Configuration

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

D.5.4.2 Test Results

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

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

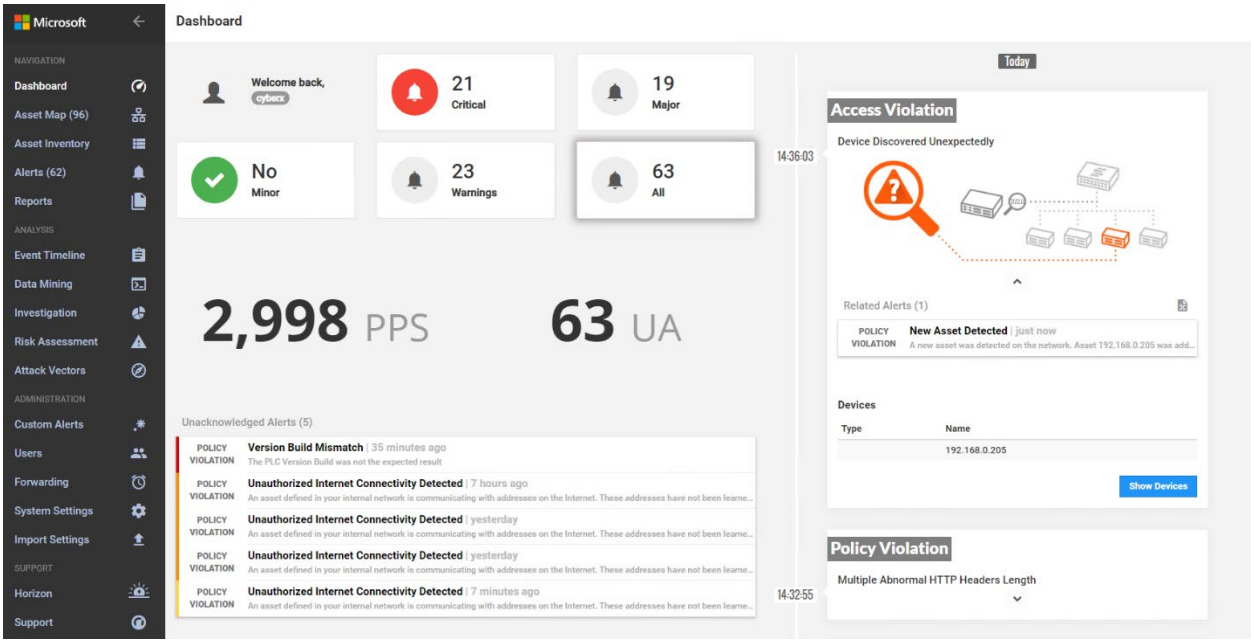


Figure D-65 Azure Defender for IoT Detects New Asset in the Environment

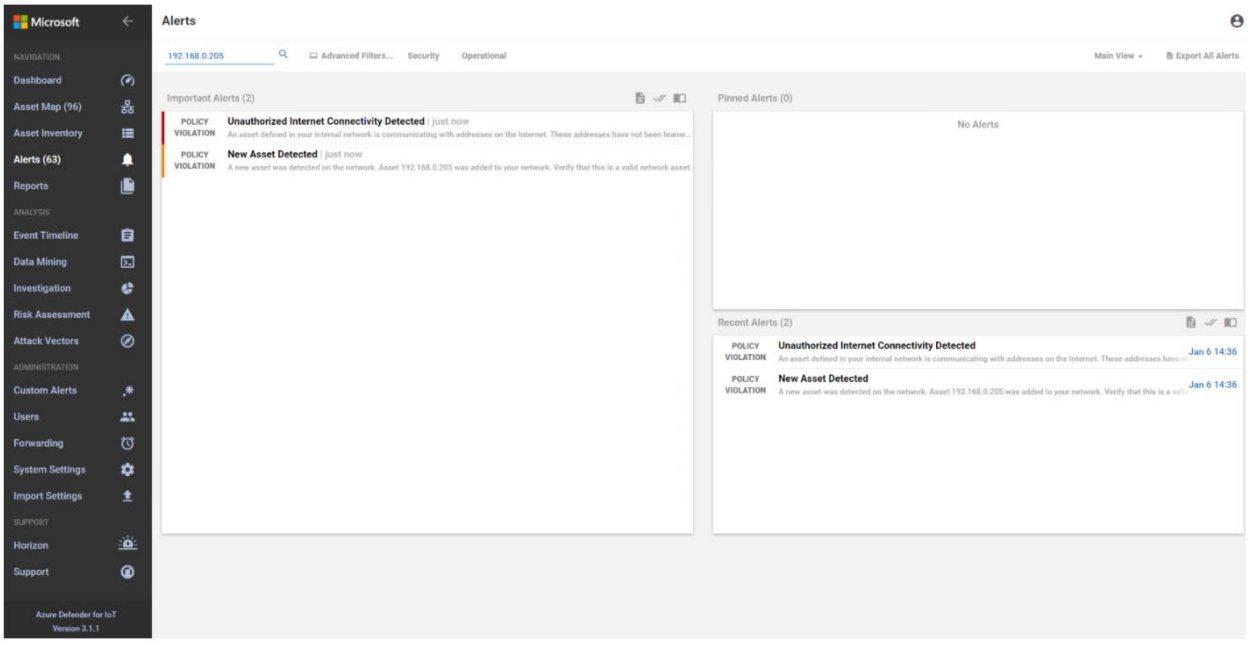


Figure D-66 Azure Defender for IoT Alert Management Options

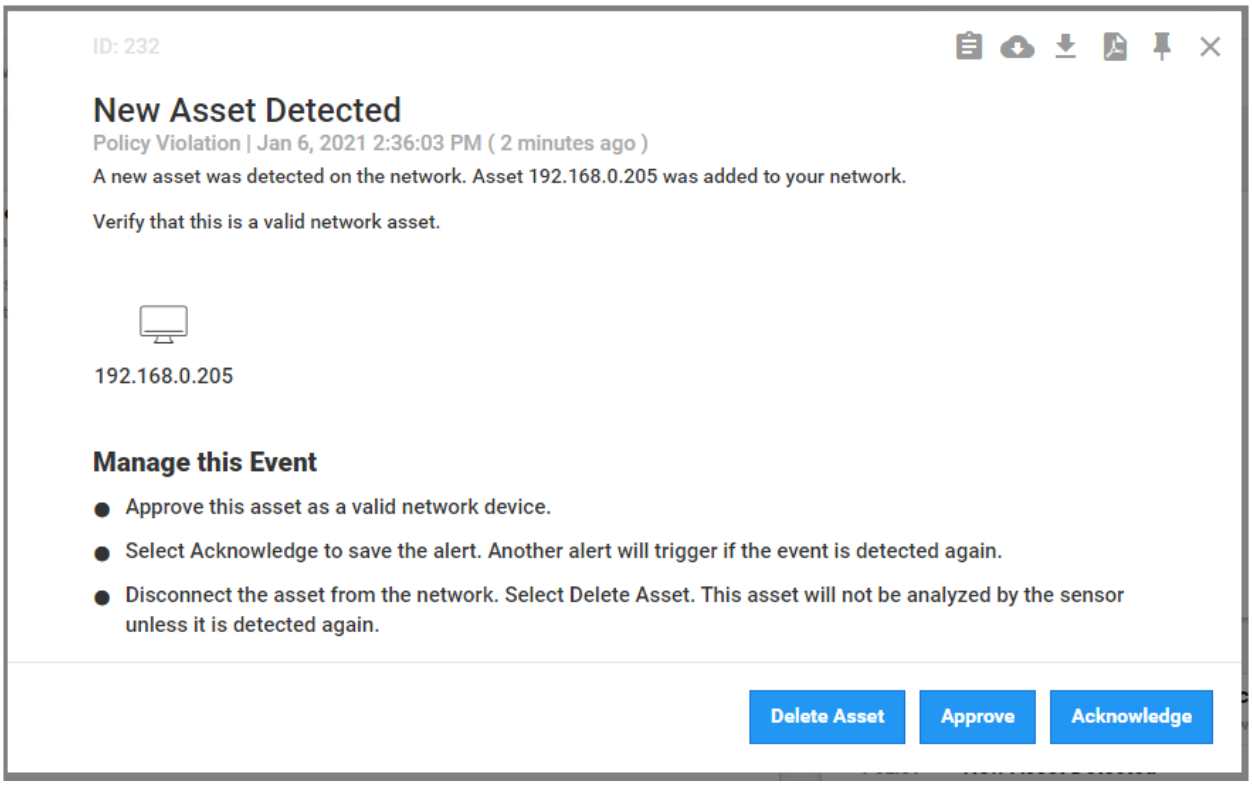
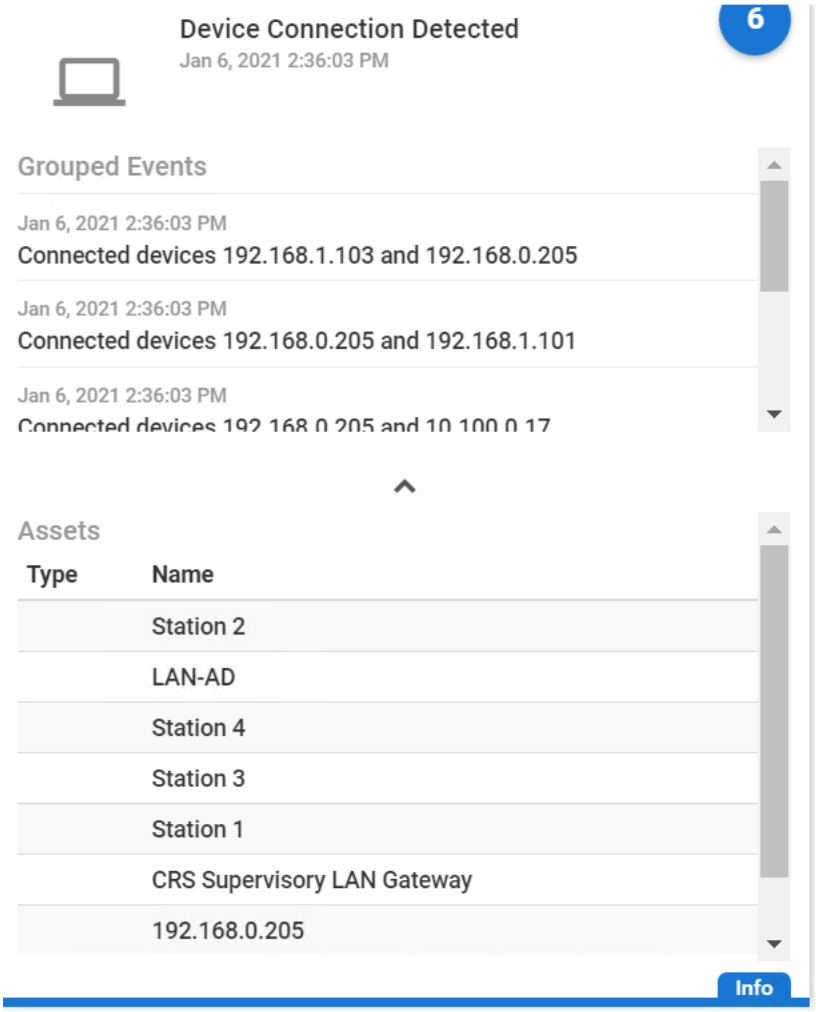


Figure D-67 Details for Network Scanning Alert



D.6 Executing Scenario 6: Detect Unauthorized Device-to-Device Communications

An authorized device that is installed on the network attempts to establish an unapproved connection that is not recorded in the baseline. The expected result is the behavioral anomaly detection products alert on the non-baseline network traffic.

D.6.1 Build 1

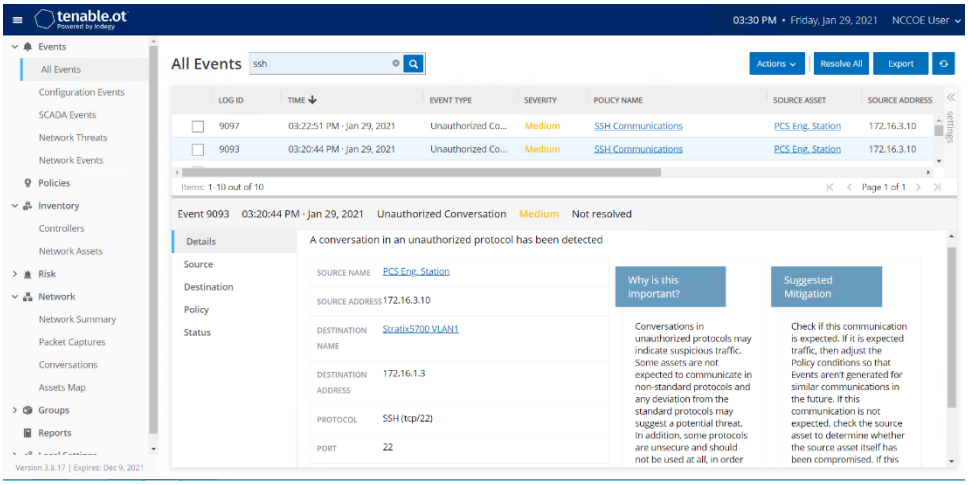
D.6.1.1 Configuration

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

D.6.1.2 Test Results

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

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



D.6.2 Build 2

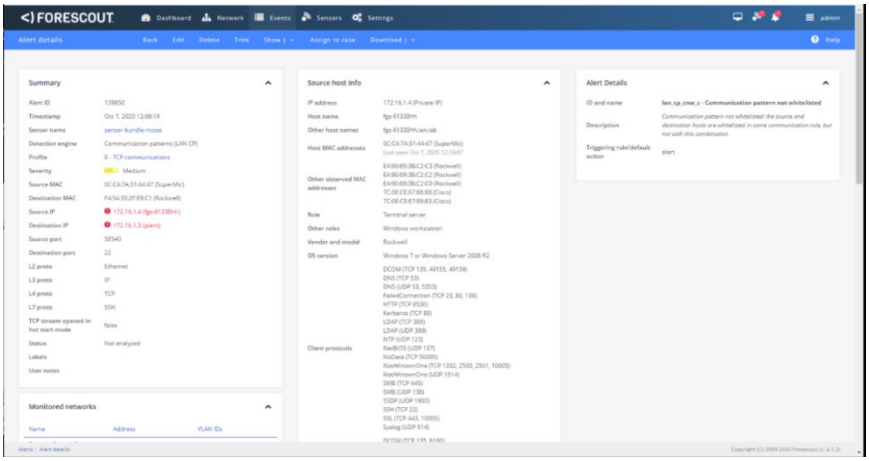
D.6.2.1 Configuration

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

D.6.2.2 Test Results

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

Figure D-69 Forescout Alert Showing the Unapproved SSH Traffic



D.6.3 Build 3

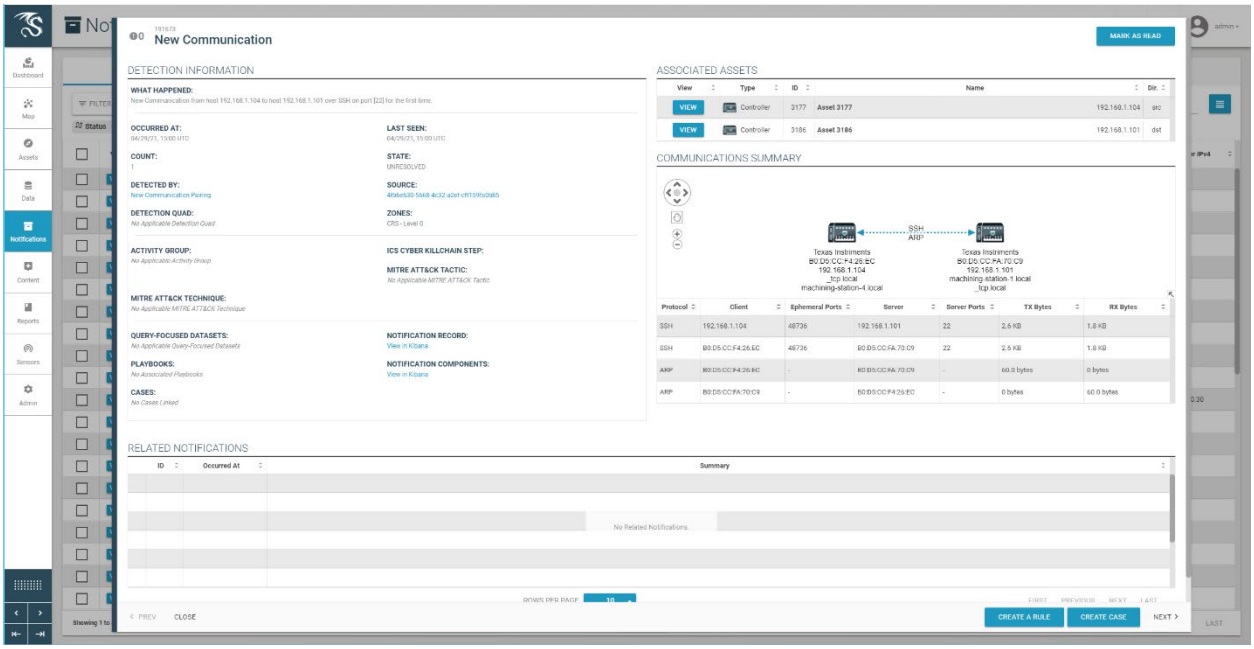
D.6.3.1 Configuration

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

D.6.3.2 Test Results

Dragos detected the non-baseline SSH traffic as shown in Figure D-70.

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



D.6.4 Build 4

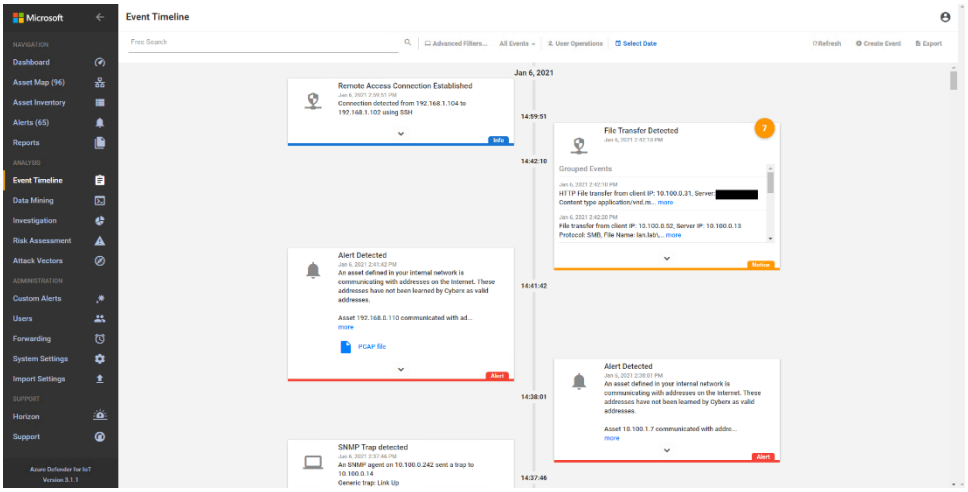
D.6.4.1 Configuration

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

D.6.4.2 Test Results

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

FigureD-71 Azure Defender for IoT Event Identified the Unauthorized SSH Connection



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

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

D.7.1 Build 1

D.7.1.1 Configuration

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

D.7.1.2 Test Results

Carbon Black reports file deleting activities as shown in Figure D-72. GreenTec protects the files on its drive from being deleted.

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

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

D.7.2 Build 2

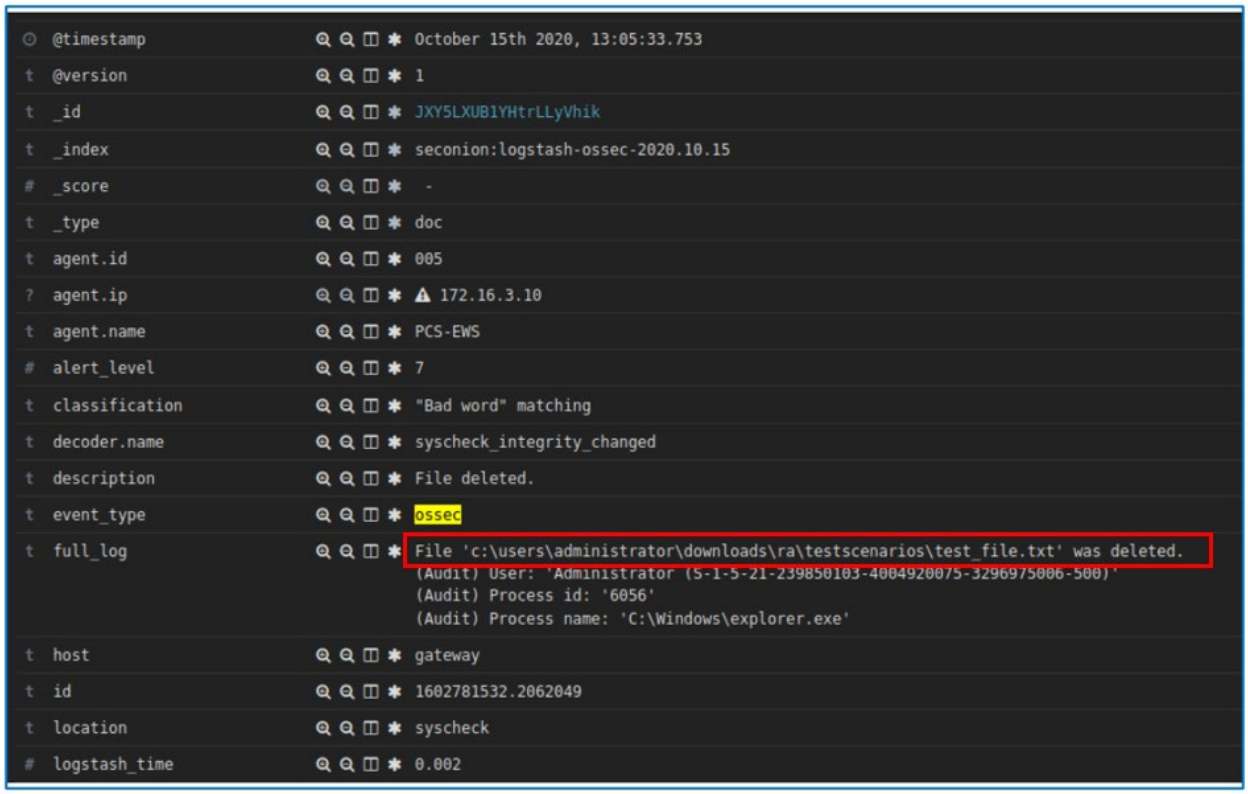
D.7.2.1 Configuration

- File Integrity Checking: Security Onion
  - The agent is installed on workstations and configured to communicate to the Security Onion Server.
- File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

D.7.2.2 Test Results

Security Onion Wazuh alerts on file deletion as shown in Figure D-73. Files stored on a storage drive protected by GreenTec are protected from deletion.

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



D.7.3 Build 3

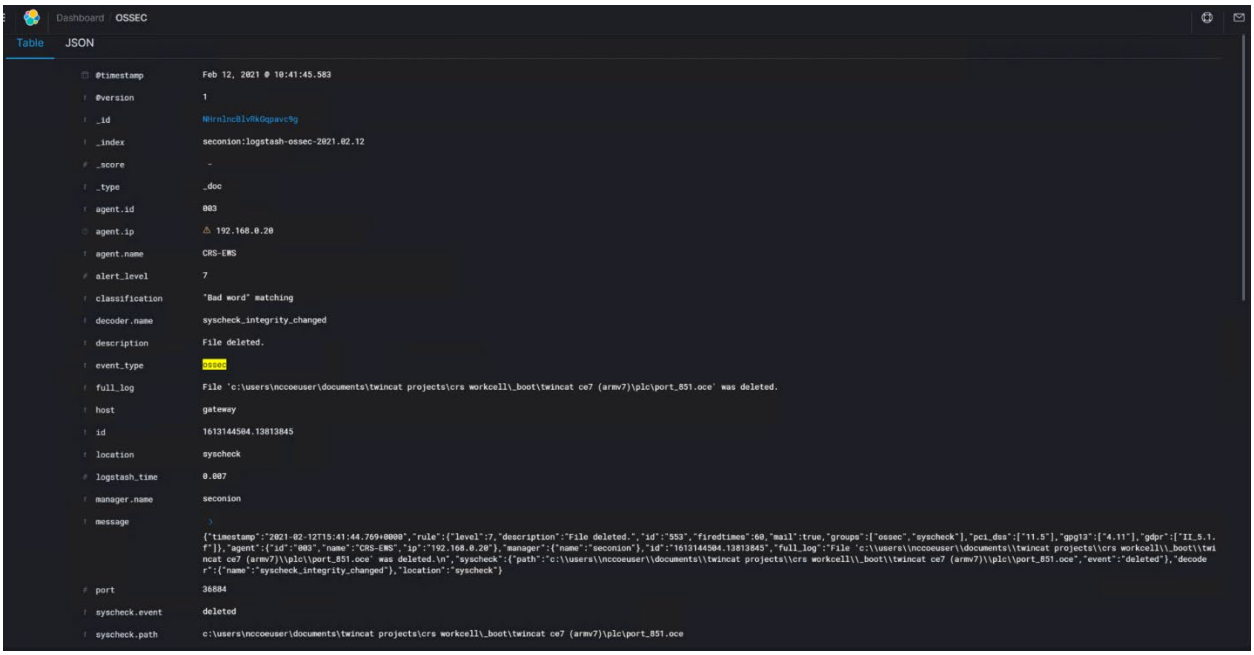
D.7.3.1 Configuration

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

D.7.3.2 Test Results

Security Onion Wazuh detected the file deletions as shown in the Security Onion Server log in Figure D-74. Files stored on a storage drive protected by GreenTec are protected from deletion.

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



D.7.4 Build 4

D.7.4.1 Configuration

- File Integrity Checking: Carbon Black

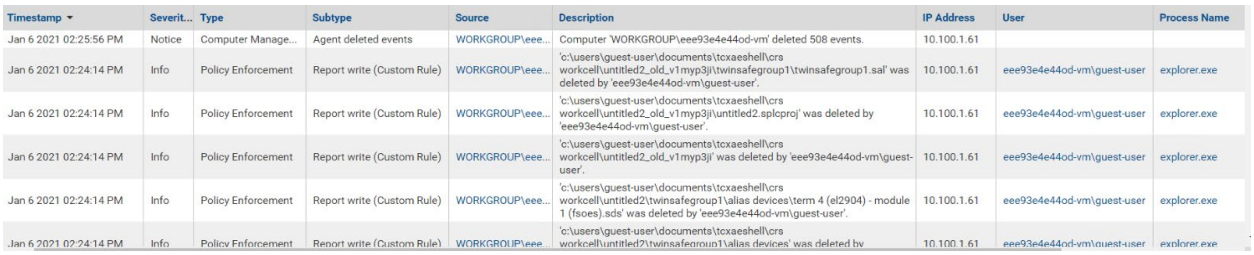
- Agent installed on workstations and configured to communicate to the Carbon Black Server.

- File Integrity Checking: WORMdisk
  - Network file share on server is configured to use WORMdisk.

D.7.4.2 Test Results

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

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



Timestamp	Severit...	Type	Subtype	Source	Description	IP Address	User	Process Name
Jan 6 2021 02:25:56 PM	Notice	Computer Manage...	Agent deleted events	WORKGROUP\eee...	Computer 'WORKGROUP\eee93e4e44od-vm' deleted 508 events.	10.100.1.61		
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2_old_v1myp3ji\twinsafegroup1\twinsafegroup1.sal' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2_old_v1myp3ji\untitled2.splcproj' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2_old_v1myp3ji' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2\twinsafegroup1\alias devices\term 4 (el2904) - module 1 (fsoes).sds' was deleted by 'eee93e4e44od-vm\guest-user'.	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe
Jan 6 2021 02:24:14 PM	Info	Policy Enforcement	Report write (Custom Rule)	WORKGROUP\eee...	'c:\users\guest-user\documents\tcxaeshell\crs workcell\untitled2\twinsafegroup1\alias devices' was deleted by	10.100.1.61	eee93e4e44od-vm\guest-user	explorer.exe

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

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

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

D.8.1 Build 1

D.8.1.1 Configuration

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

D.8.1.2 Test Results

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

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

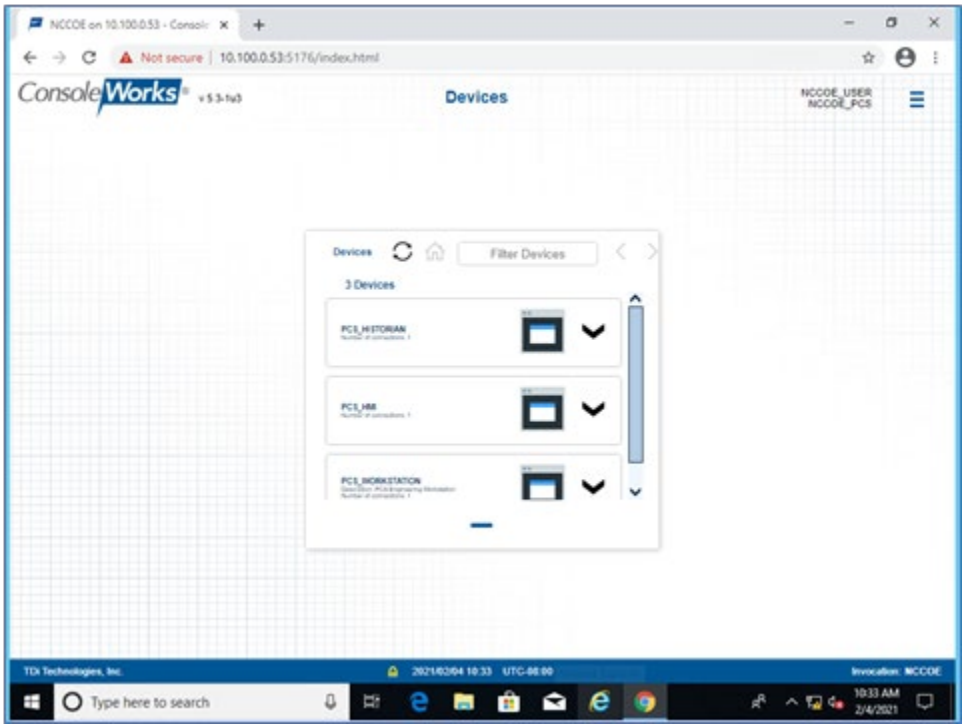


Figure D-77 Remote Session into Studio 5000 to Perform PLC File Operations

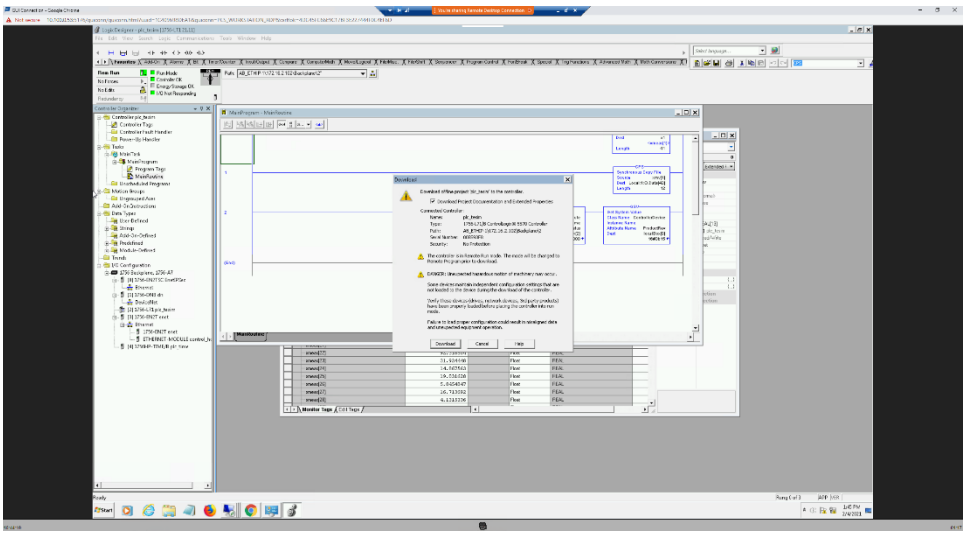


Figure D-78 Tenable.ot Detected the Transfer of PLC Logic File to the Rockwell PLC

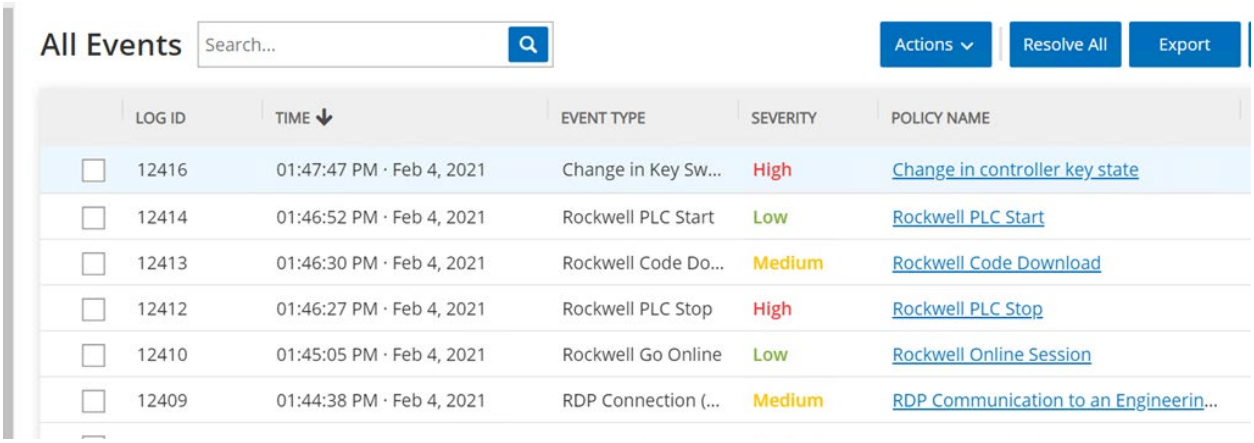


Figure D-79 Tenable.ot PLC Stop alert details

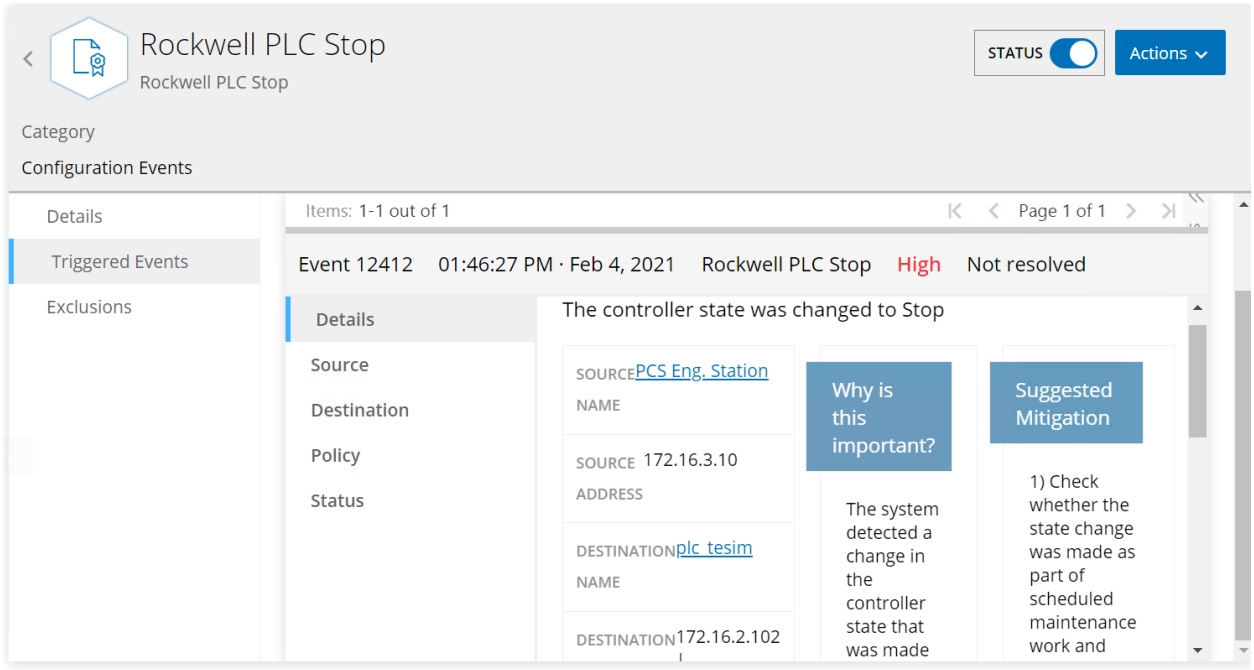
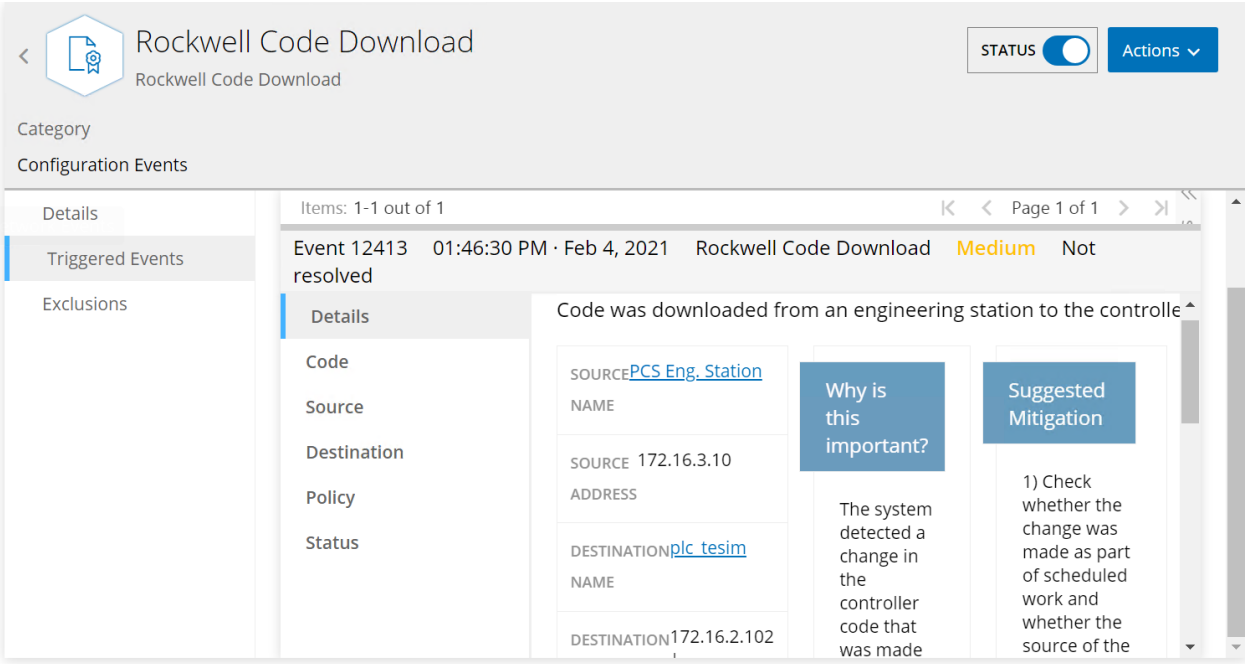


Figure D-80 Tenable.ot PLC Program Download Alert Details



D.8.2 Build 2

D.8.2.1 Configuration

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

D.8.2.2 Test Results

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

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

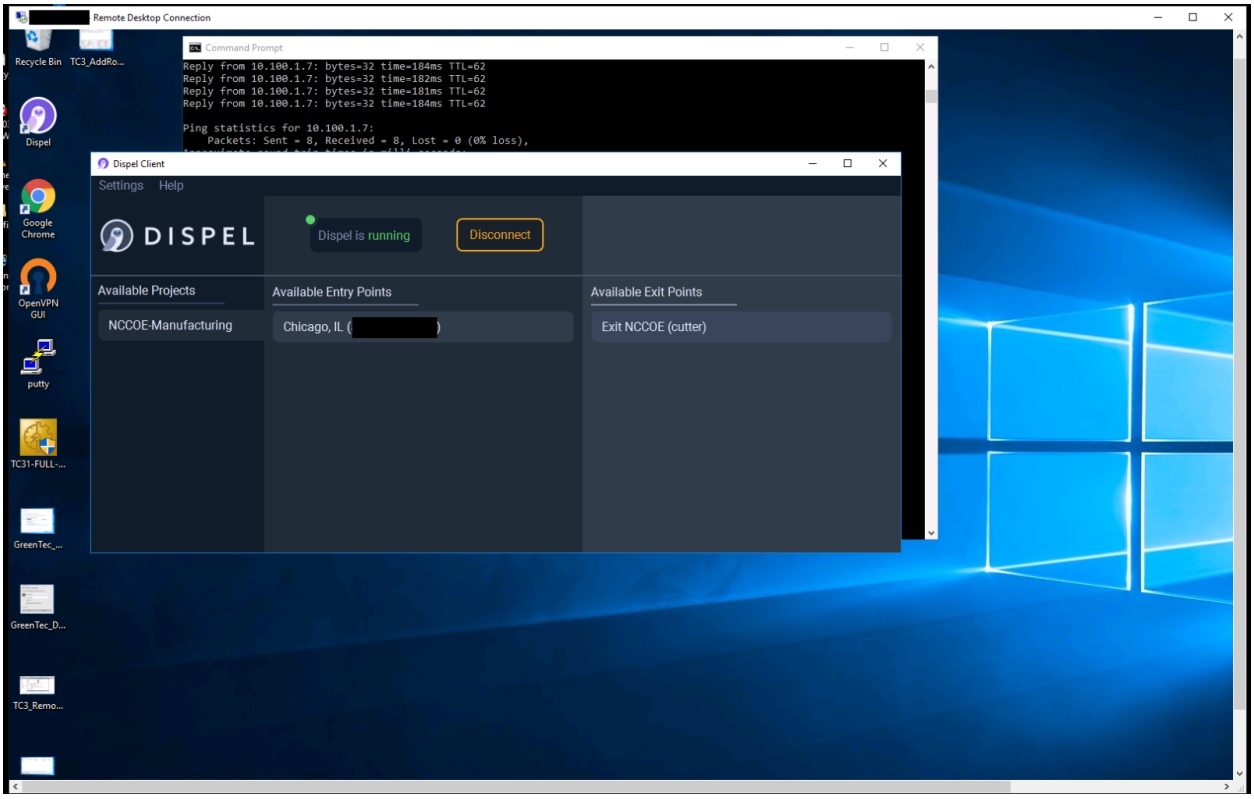


Figure D-82 Modifying the Parameters for the Allen-Bradley PLC Controller Using Studio 5000

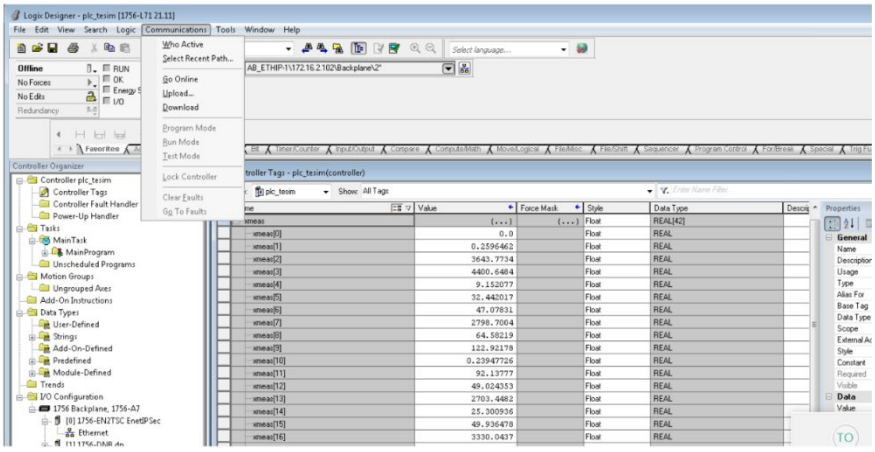


Figure D-83 Forescout Alerts Showing It Detected the Traffic Between the Engineering Workstation and the PLC

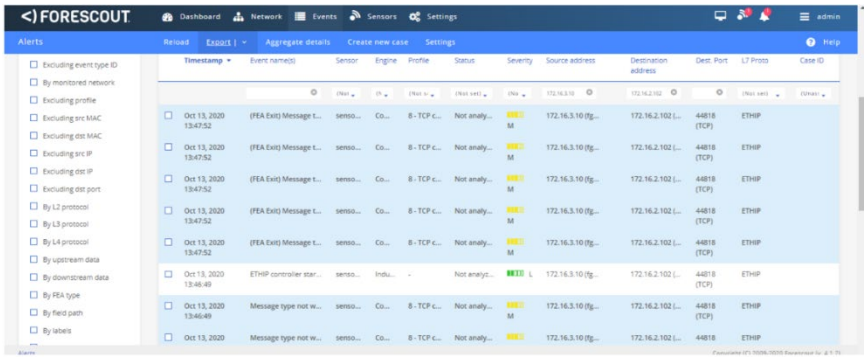


Figure D-84 Forescout Alert Details for the Stop Command Issued to the PLC

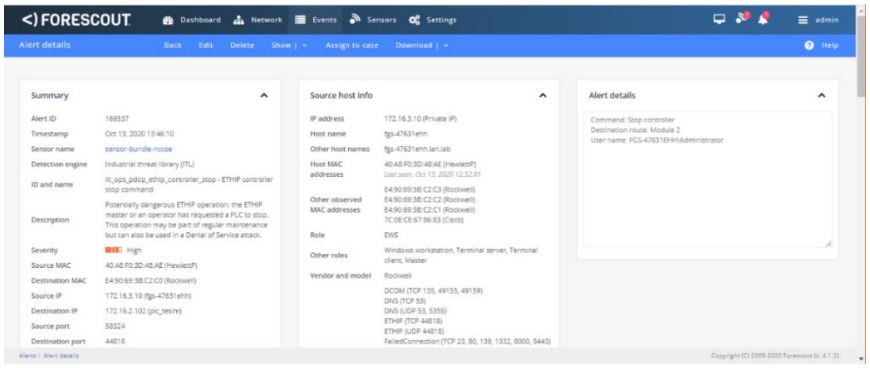
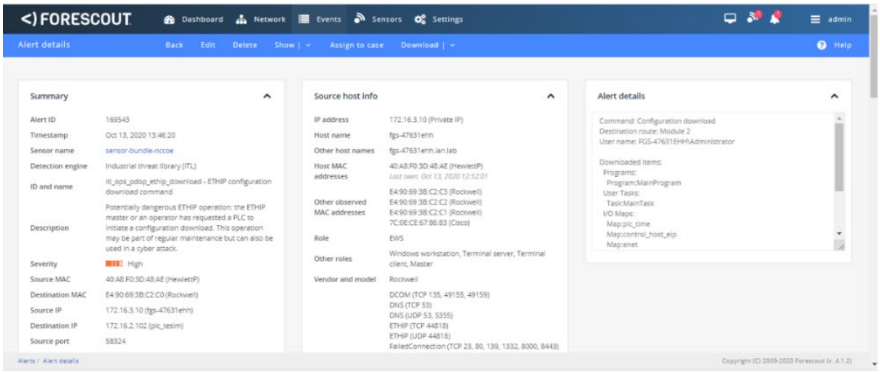


Figure D-85 Forescout Alert Details for the Configuration Download Command



D.8.3 Build 3

D.8.3.1 Configuration

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

D.8.3.2 Test Results

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

Figure D-86 VPN Connection to the Manufacturing Environment

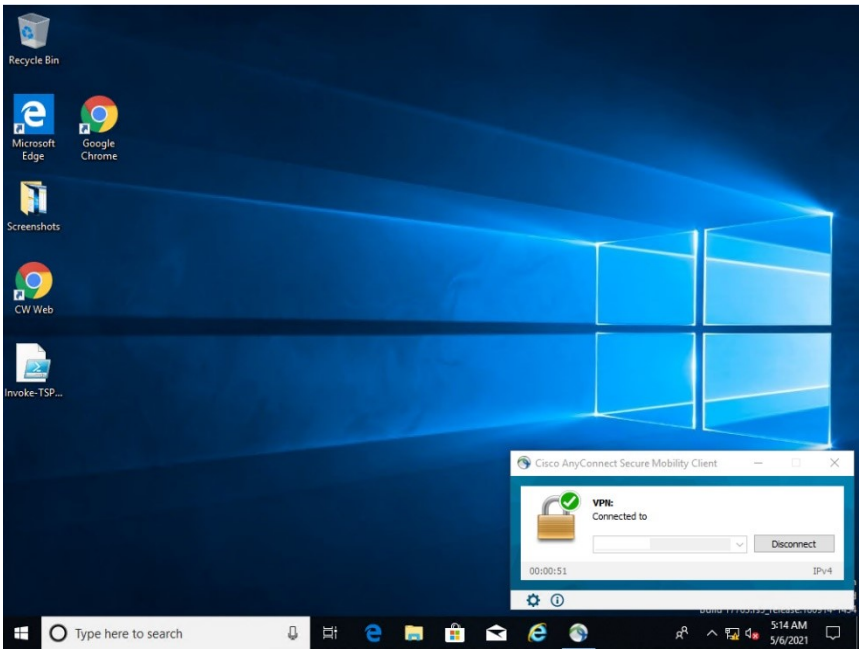


Figure D-87 Remote Access is Being Established through ConsoleWorks

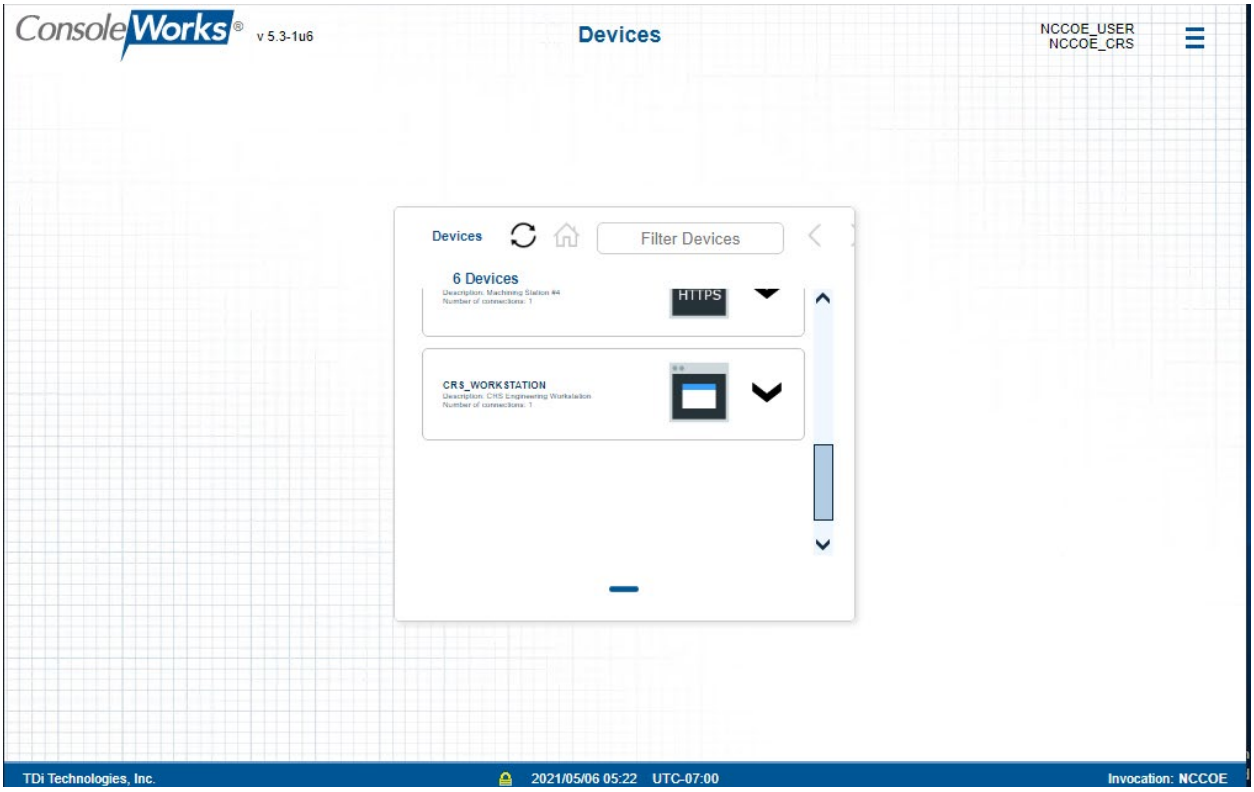


Figure D-88 Dragos Notification Manager Showing Detection of the Transfer of PLC Logic File to the Beckhoff PLC

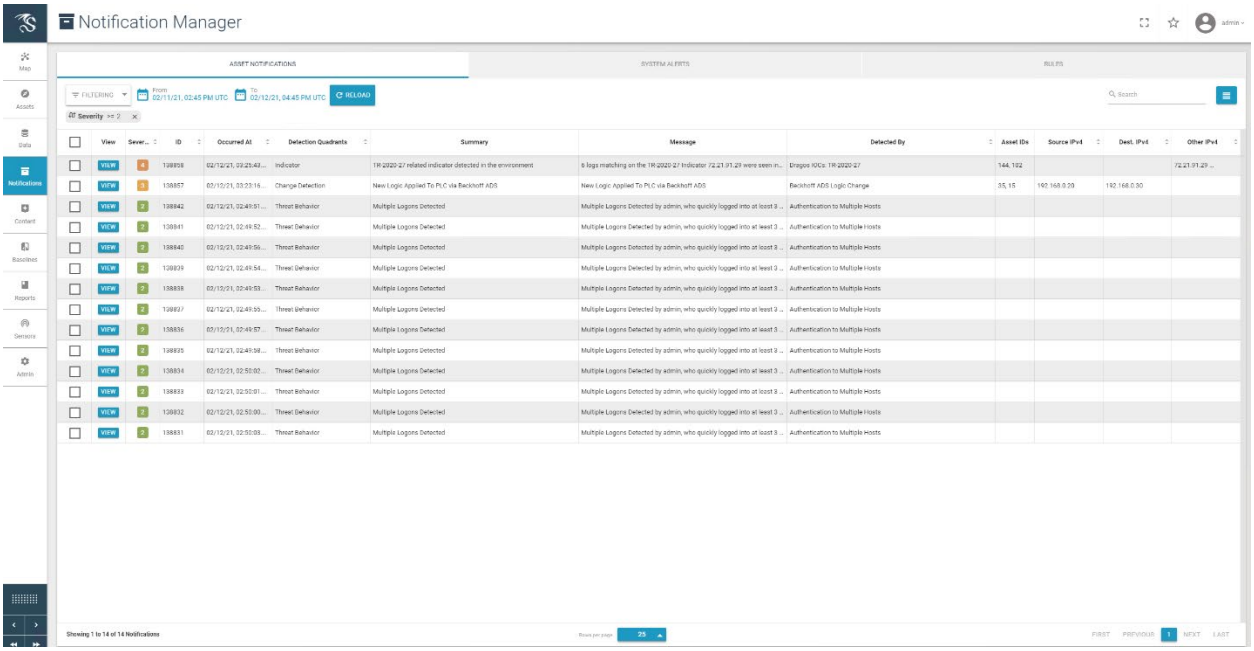
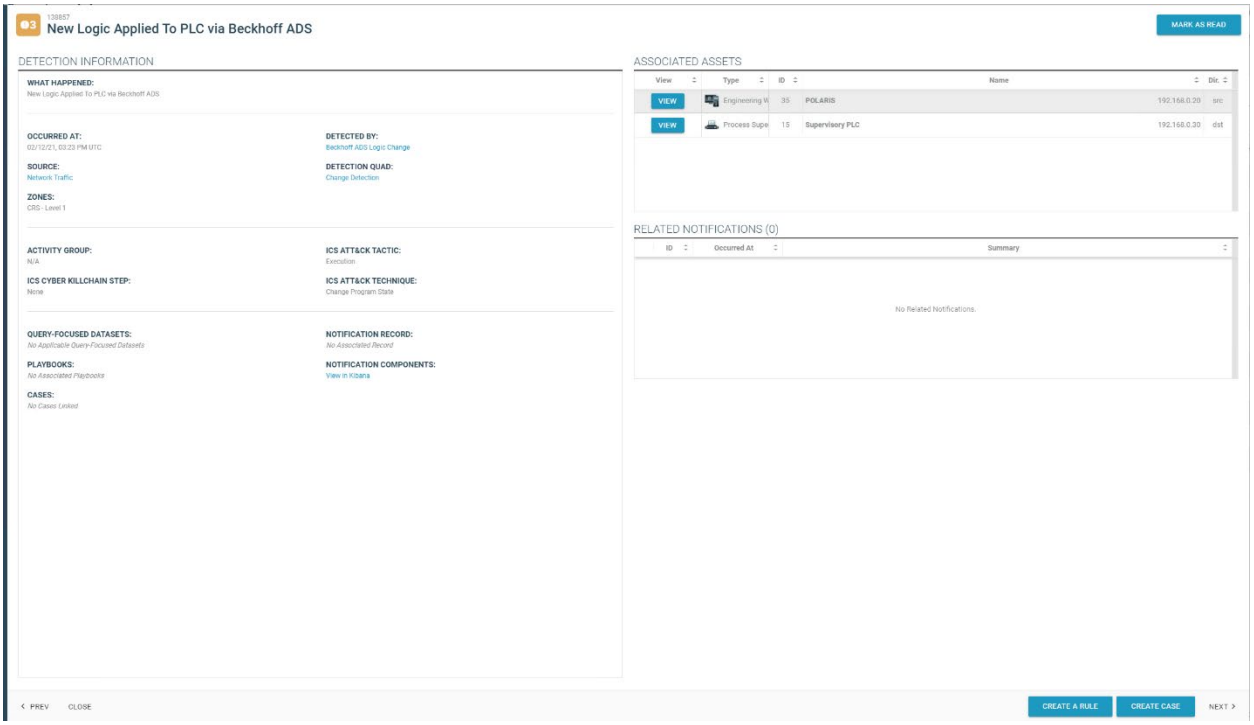


Figure D-89 Dragos Alert Details for the PLC Logic File Download



D.8.4 Build 4

D.8.4.1 Configuration

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

D.8.4.2 Test Results

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

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

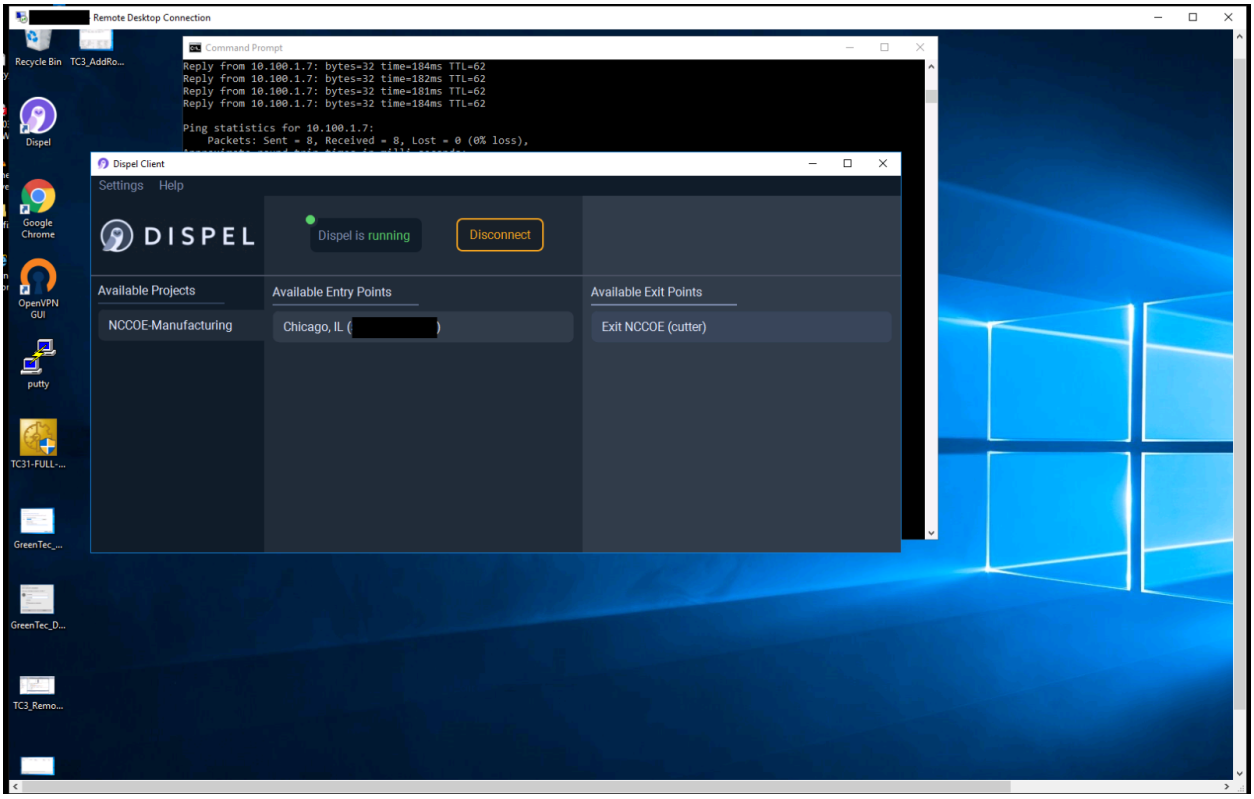


Figure D-91 Nested RDP Connections Showing Dispel Connection into the CRS Workstation

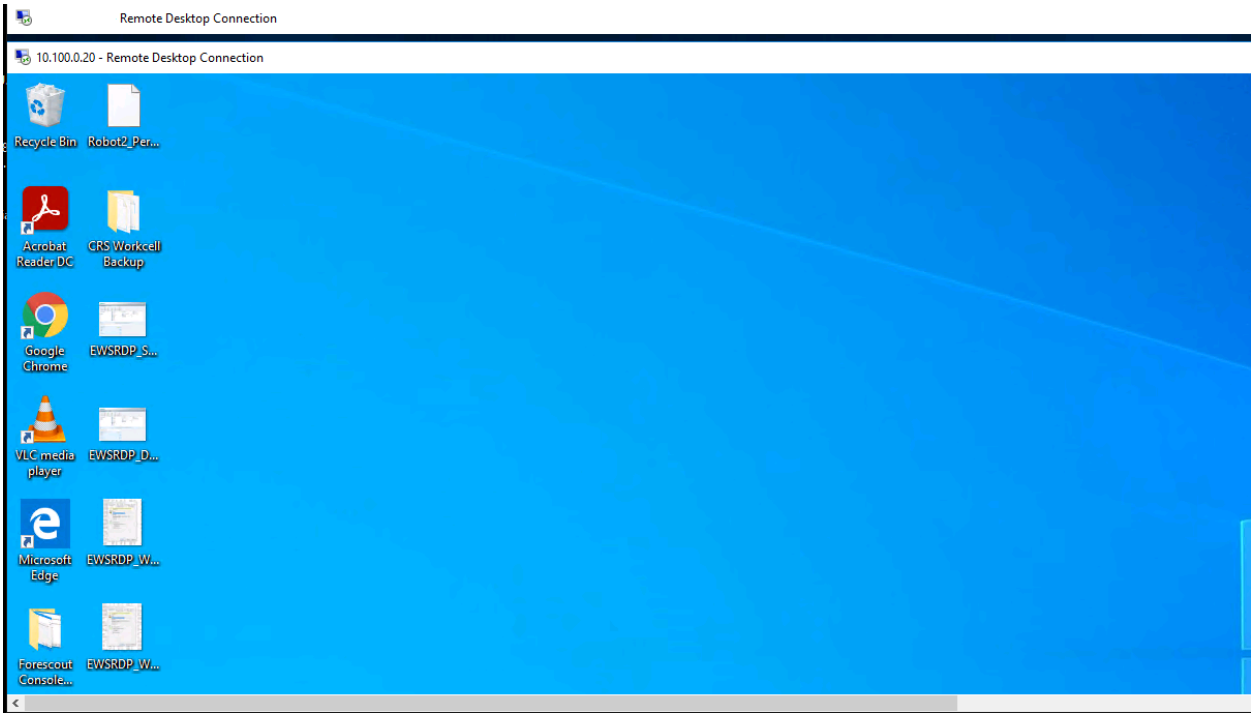
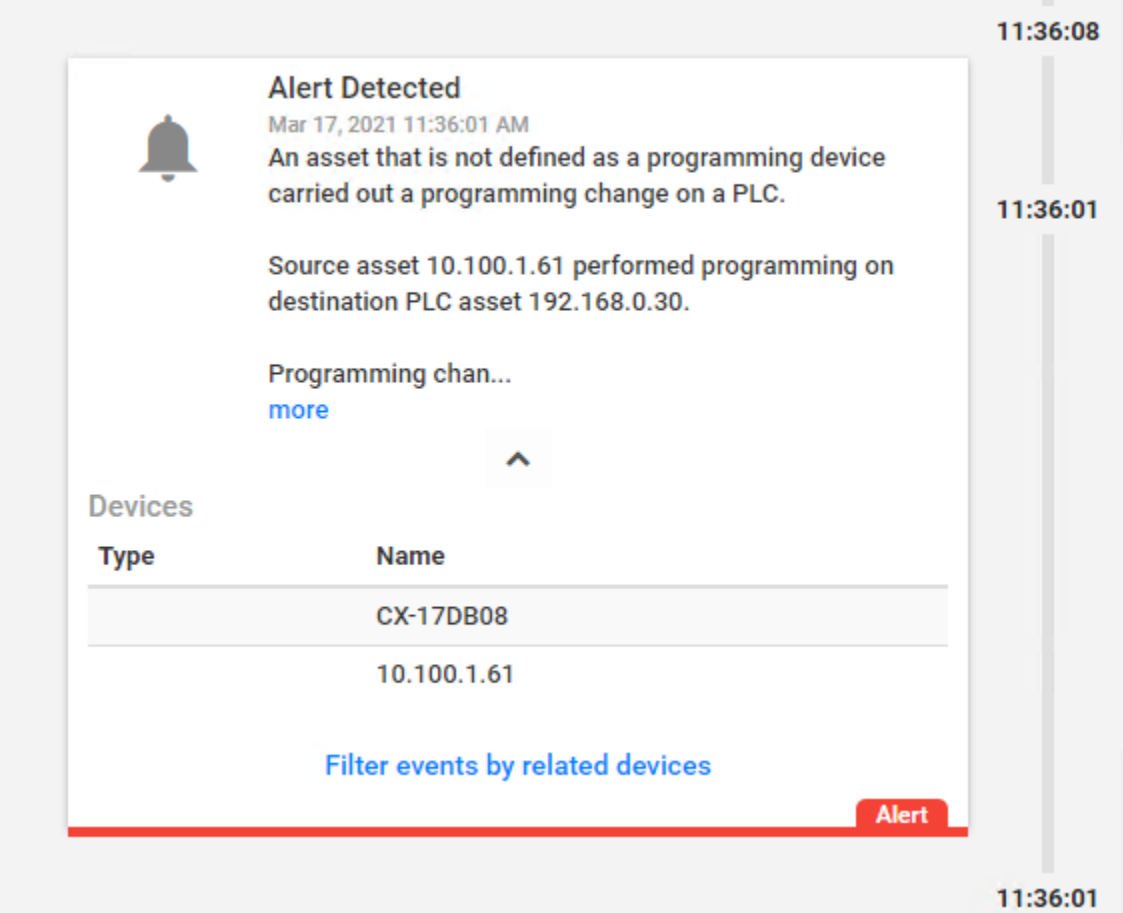


Figure D-92 Azure Defender for IoT Alert for Unauthorized PLC Programming



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

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

D.9.1 Build 1

D.9.1.1 Configuration

- Behavior Anomaly Detection: Tenable.ot

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

- File Integrity Checking: ForceField
  - PI Server is configured to use ForceField drive.

D.9.1.2 Test Results

Figure D-93 shows Tenable.ot detecting the remote access connections. Figure D-94 shows that GreenTec successfully blocks the attacker from deleting archive data.

Figure D-93 Tenable.ot alert Shows SMB Connection from External Workstation to the Historian

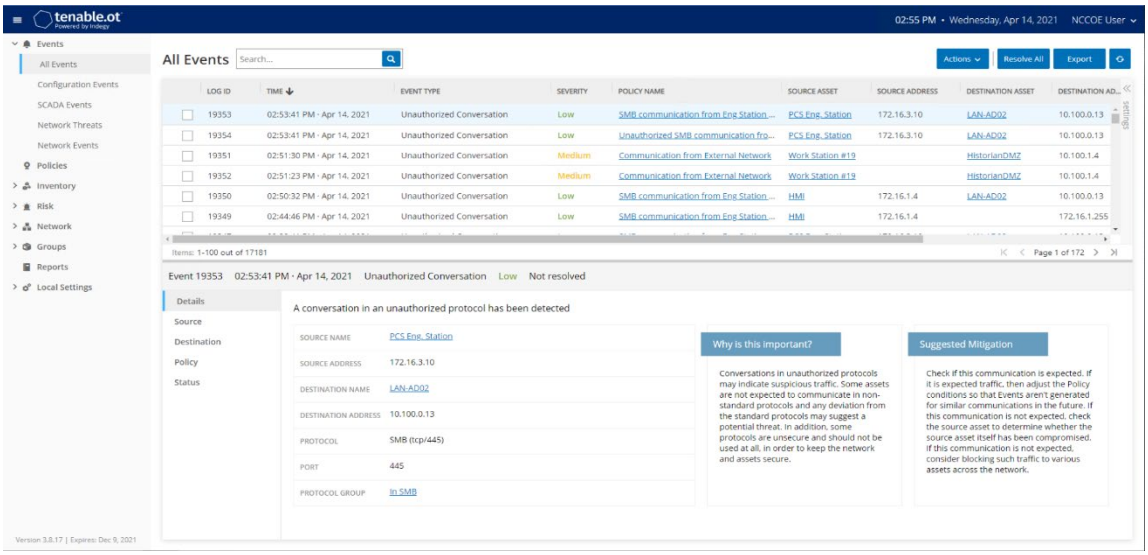
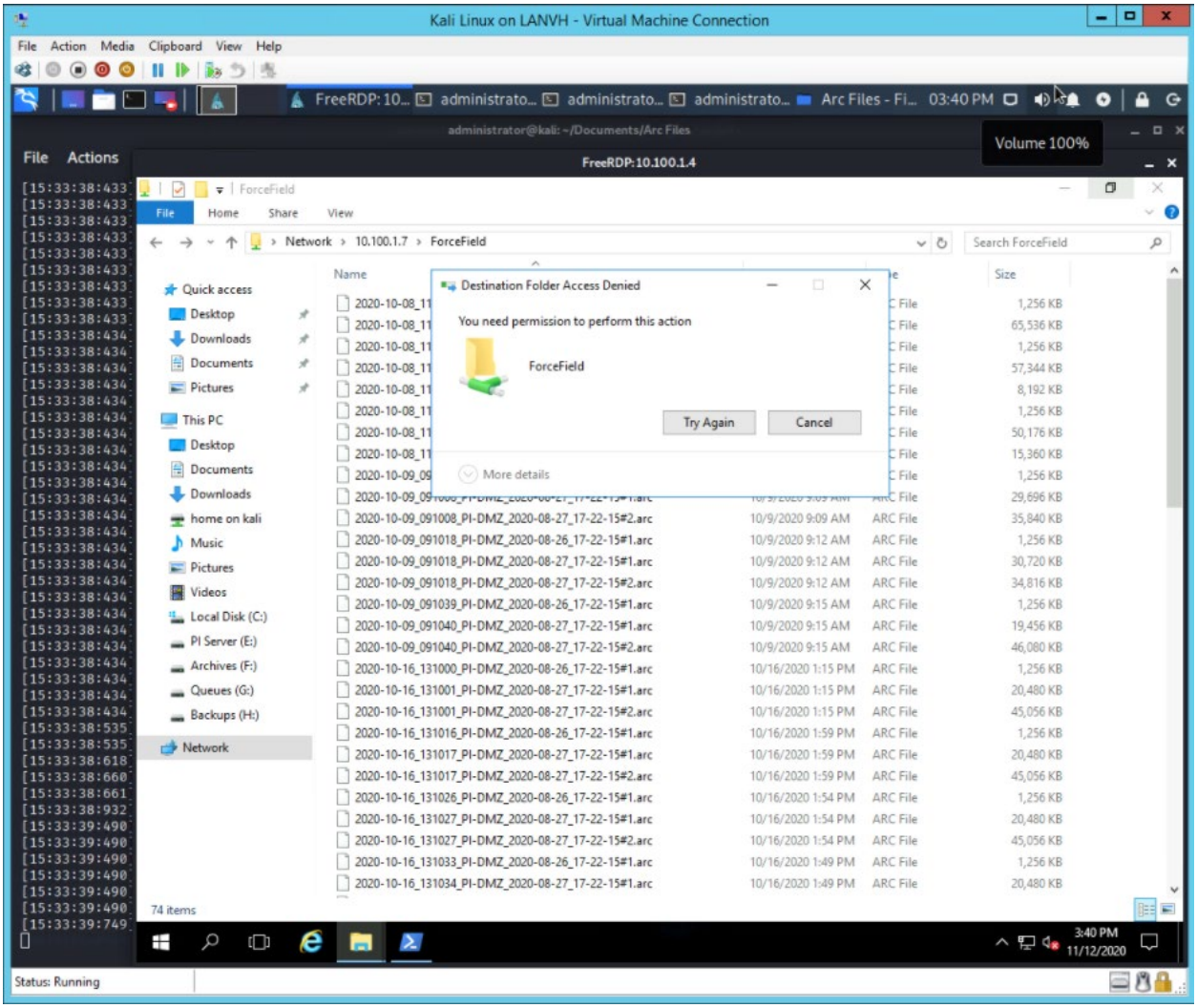


Figure D-94 GreenTec Denies Modification and Deletion File Operations in the Protected Drive



D.9.2 Build 2

D.9.2.1 Configuration

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

D.9.2.2 Test Results

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

Figure D-95 Forescout Alert Shows Network Connection from Corporate Network to the Historian

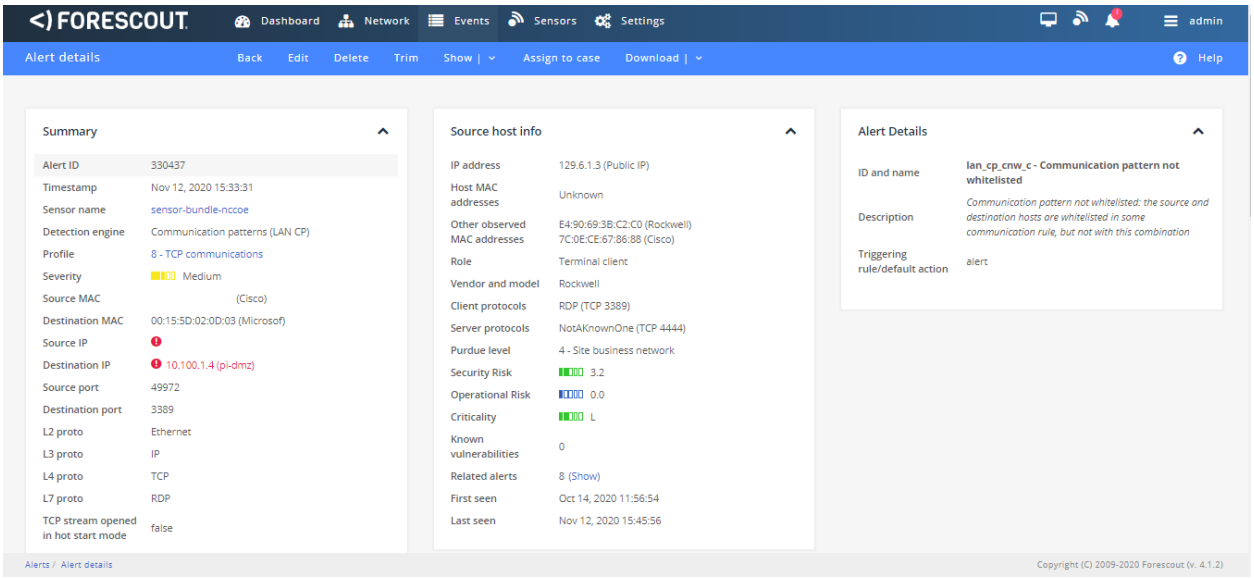
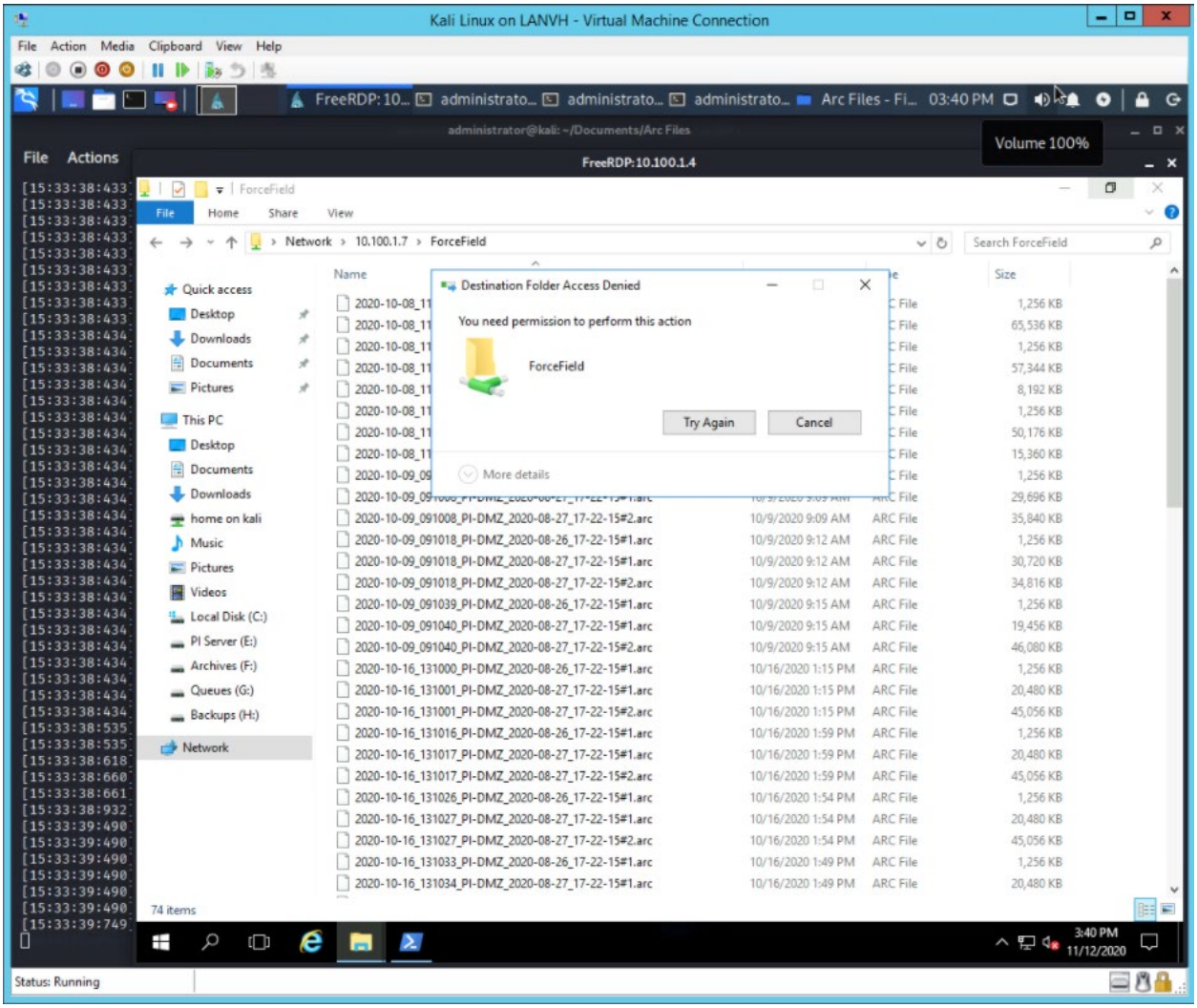


Figure D-96 GreenTec Denies Modification and Deletion File Operations in the Protected Drive



D.9.3 Build 3

D.9.3.1 Configuration

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

D.9.3.2 Test Results

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

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

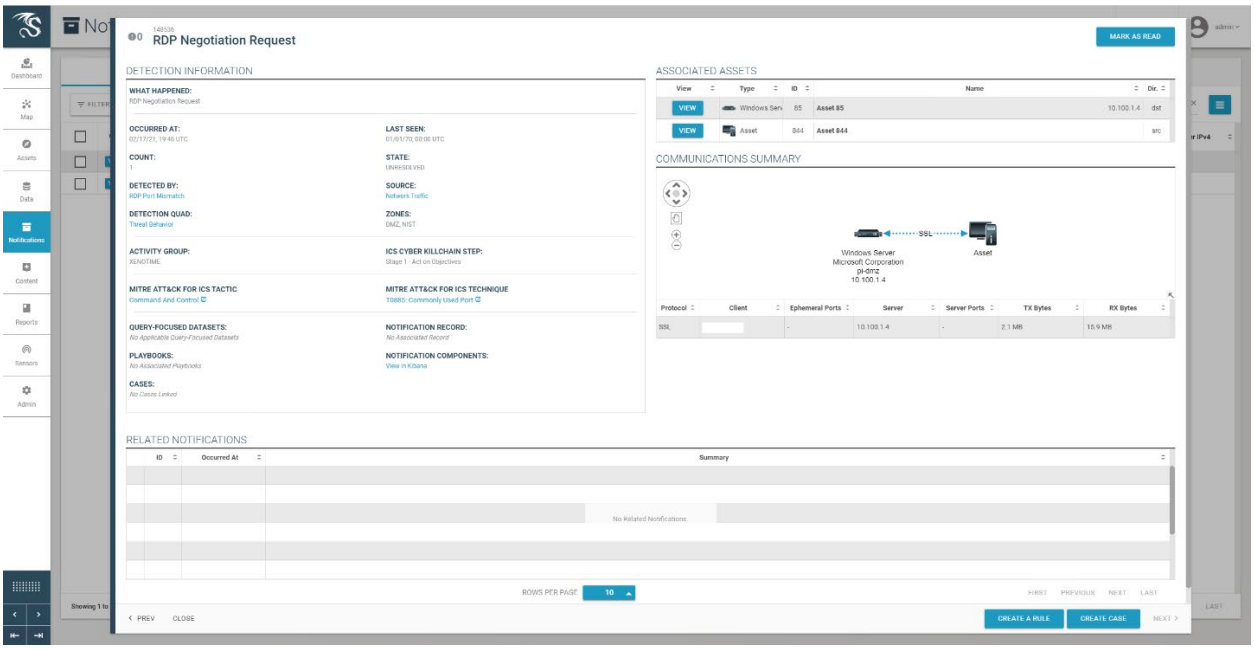
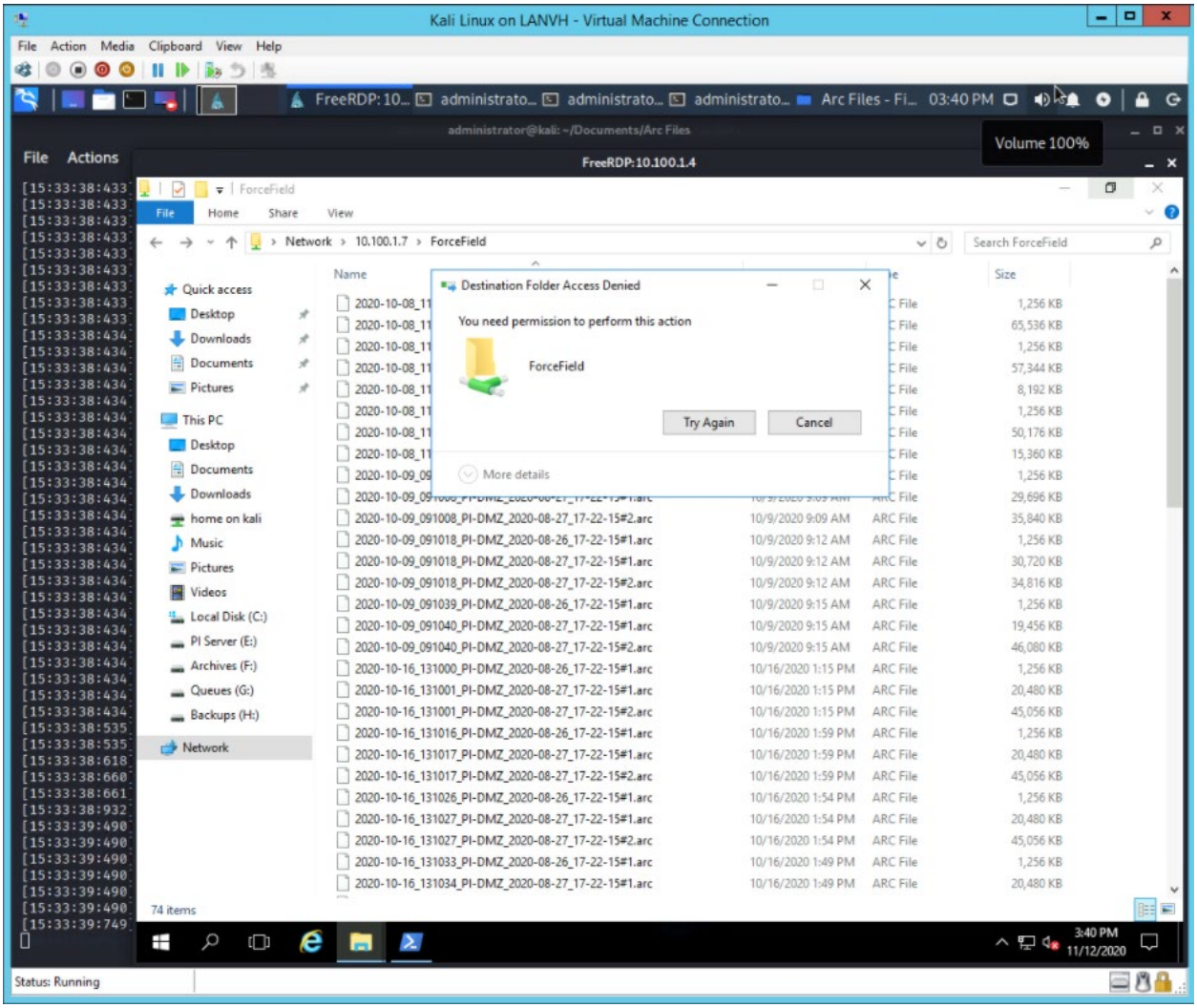


Figure D-98 GreenTec Denies Modification and Deletion File Operations in the Protected Drive



D.9.4 Build 4

D.9.4.1 Configuration

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

D.9.4.2 Test Results

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

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

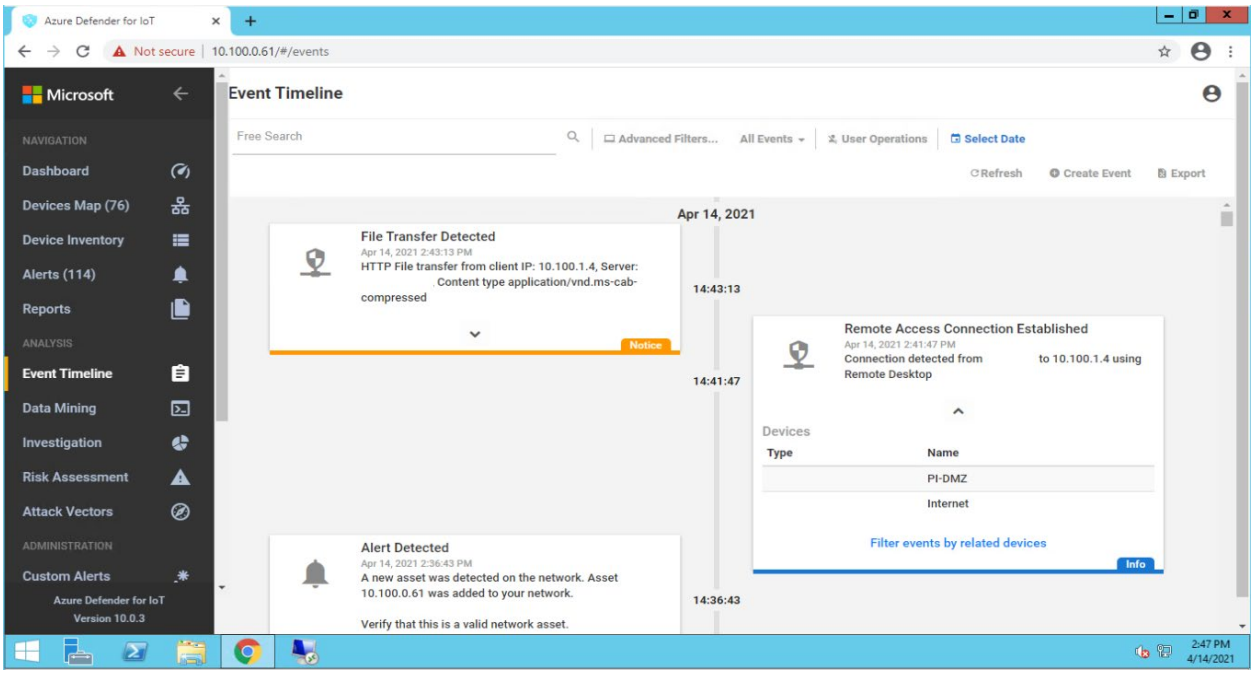
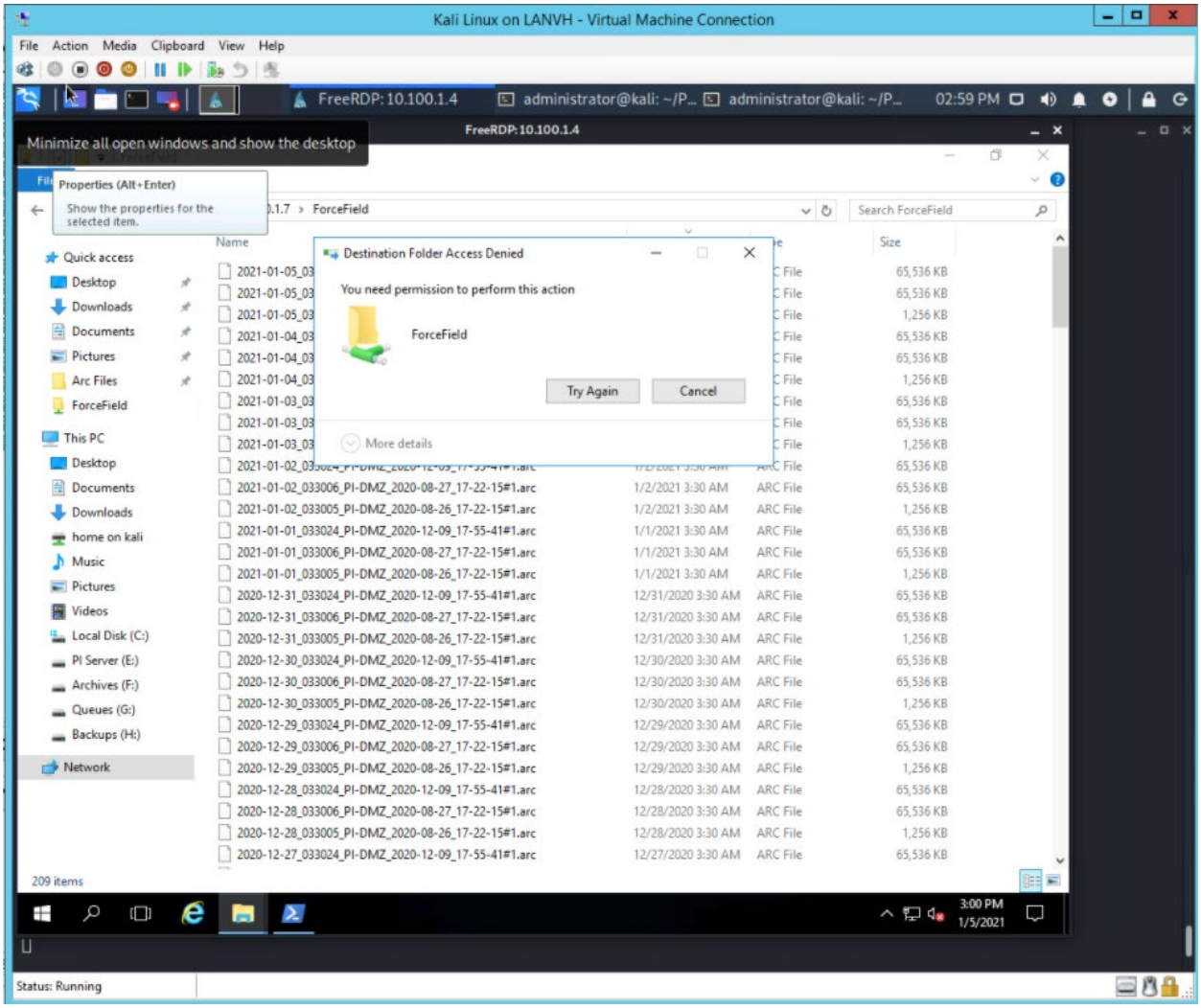


Figure D-100 GreenTec Denies Modification and Deletion File Operations in the Protected Drive



D.10 Executing Scenario 10: Detect Sensor Data Manipulation

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

D.10.1 All Builds

D.10.1.1 Configuration

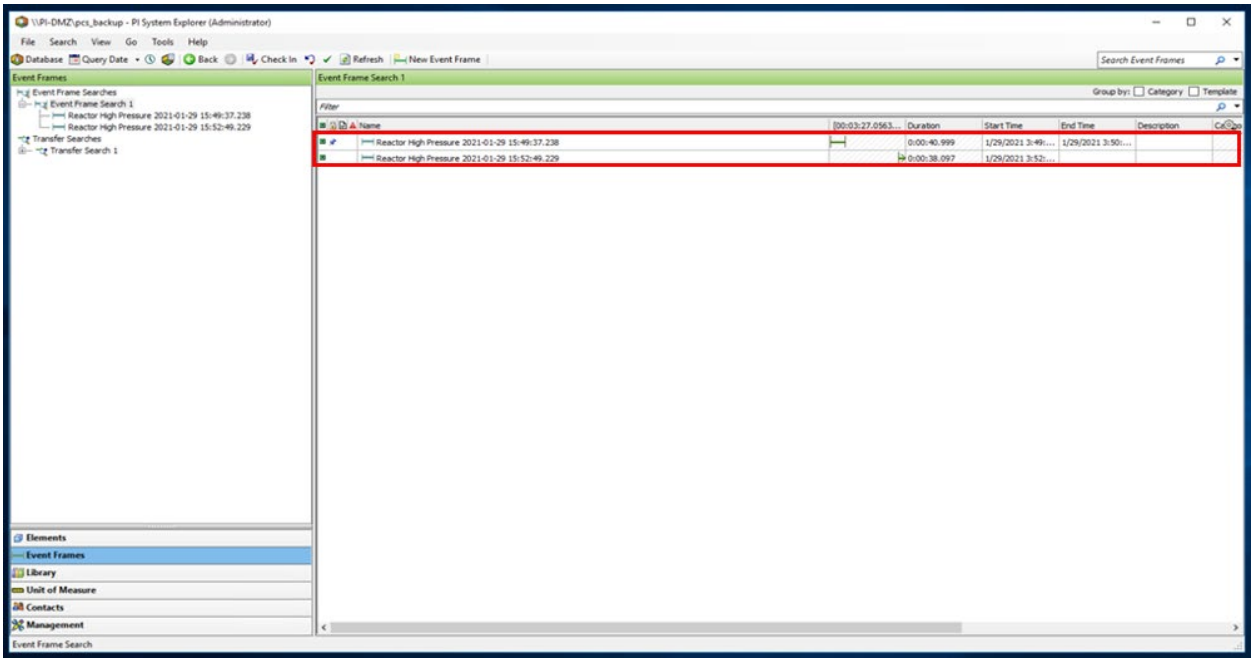
- Behavior Anomaly Detection: PI Server
  - Configured to receive process data from across the manufacturing system.

- Configured to perform analysis on incoming data points.

D.10.1.2 Test Results

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

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



D.11 Executing Scenario 11: Detect Unauthorized Firmware Modification

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

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

D.11.1 Build 1

D.11.1.1 Configuration

- Behavior Anomaly Detection: Tenable.ot

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

- Remote Access: Cisco VPN
  - Configured to allow authorized VPN users access to ConsoleWorks web interface.
- User Authentication/User Authorization: ConsoleWorks
  - Configured for accessing the PCS environment.

D.11.1.2 Test Results

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

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

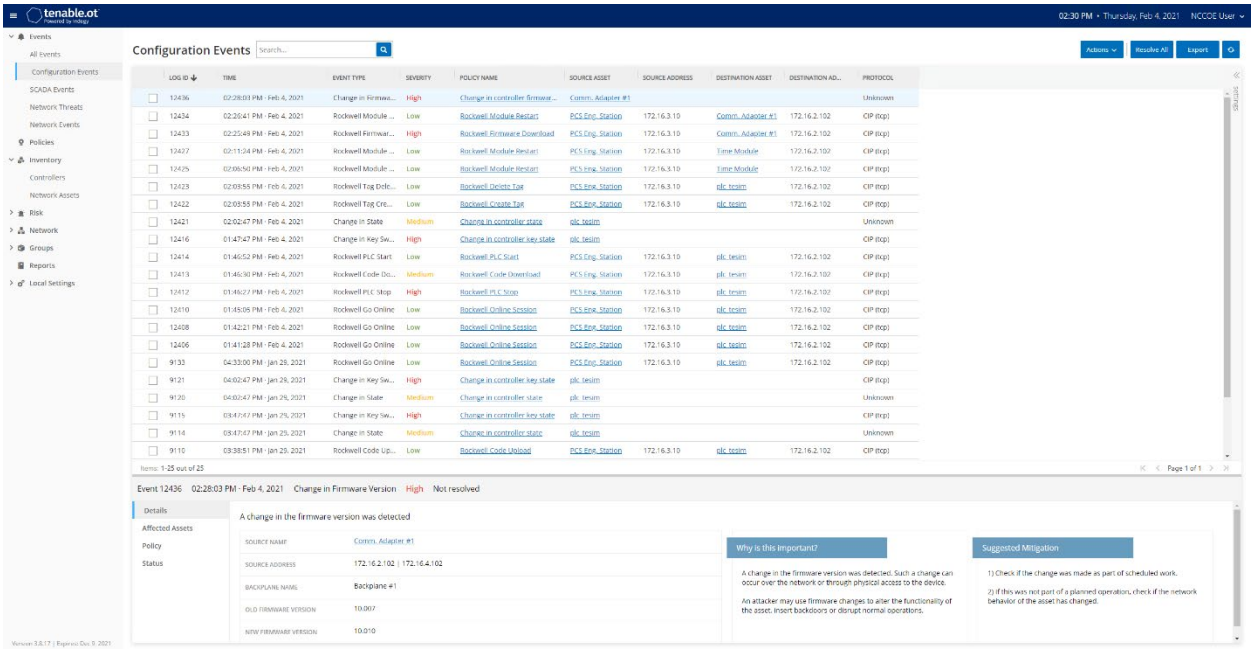


Figure D-103 Details for One of the Alerts Showing the Firmware Change

D.11.2 Build 2

D.11.2.1 Configuration

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

D.11.2.2 Test Results

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

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

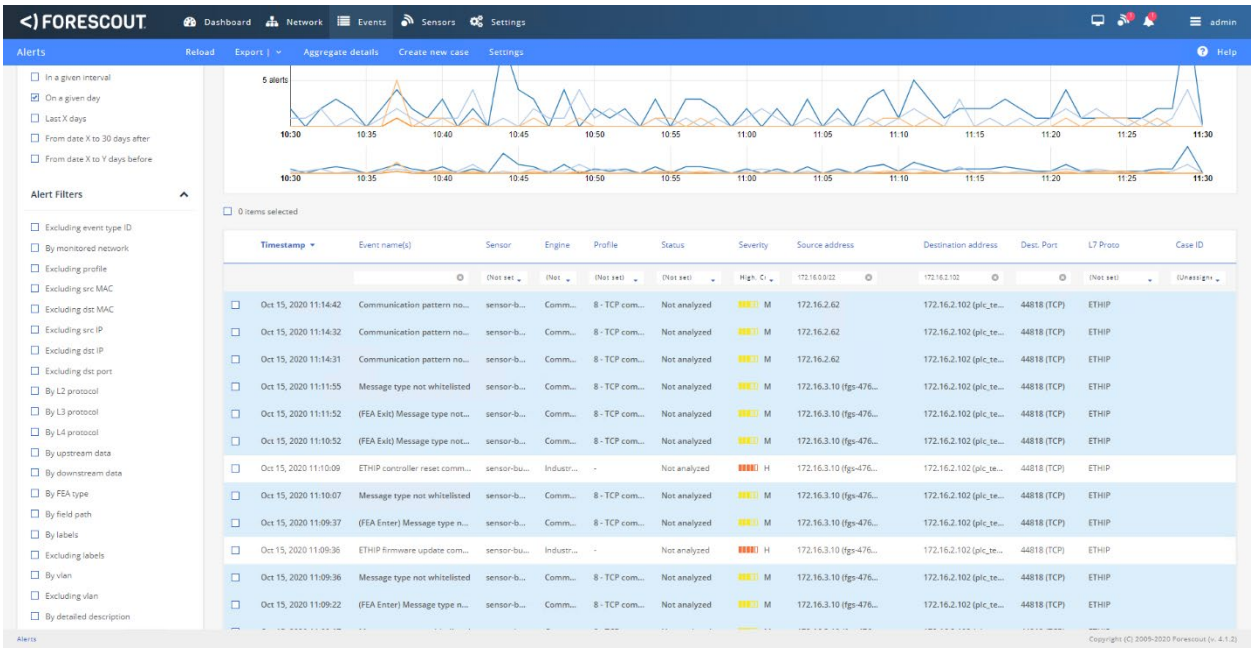


Figure D-105 Alert Details Detected by Forescout for the Firmware Change

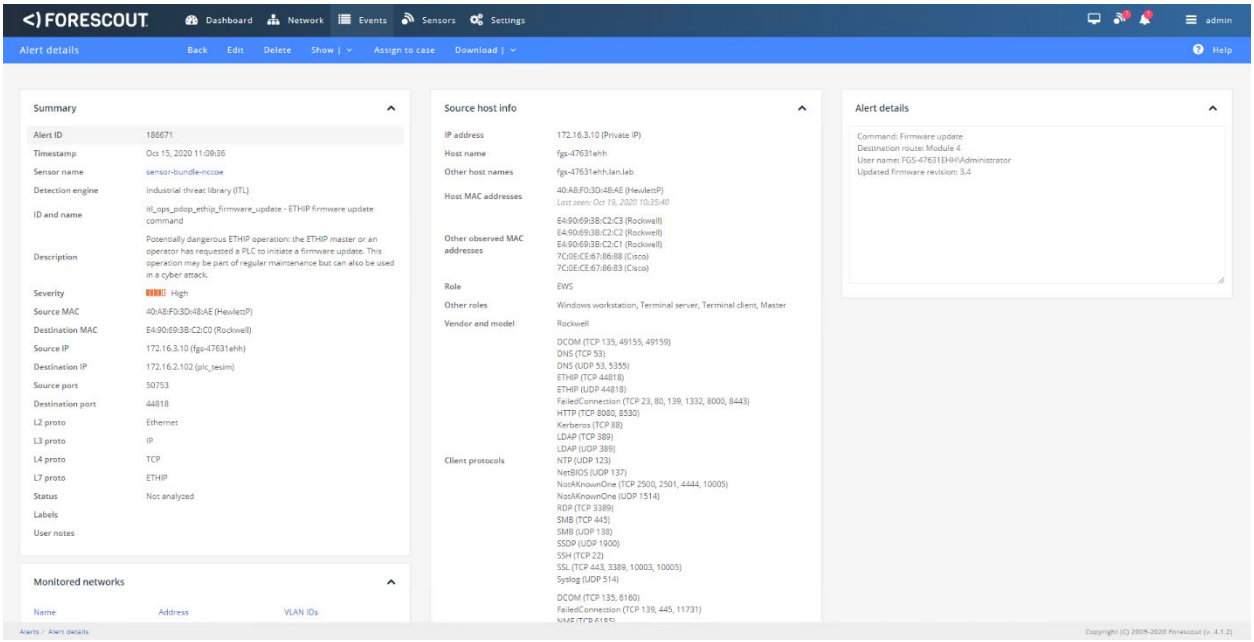
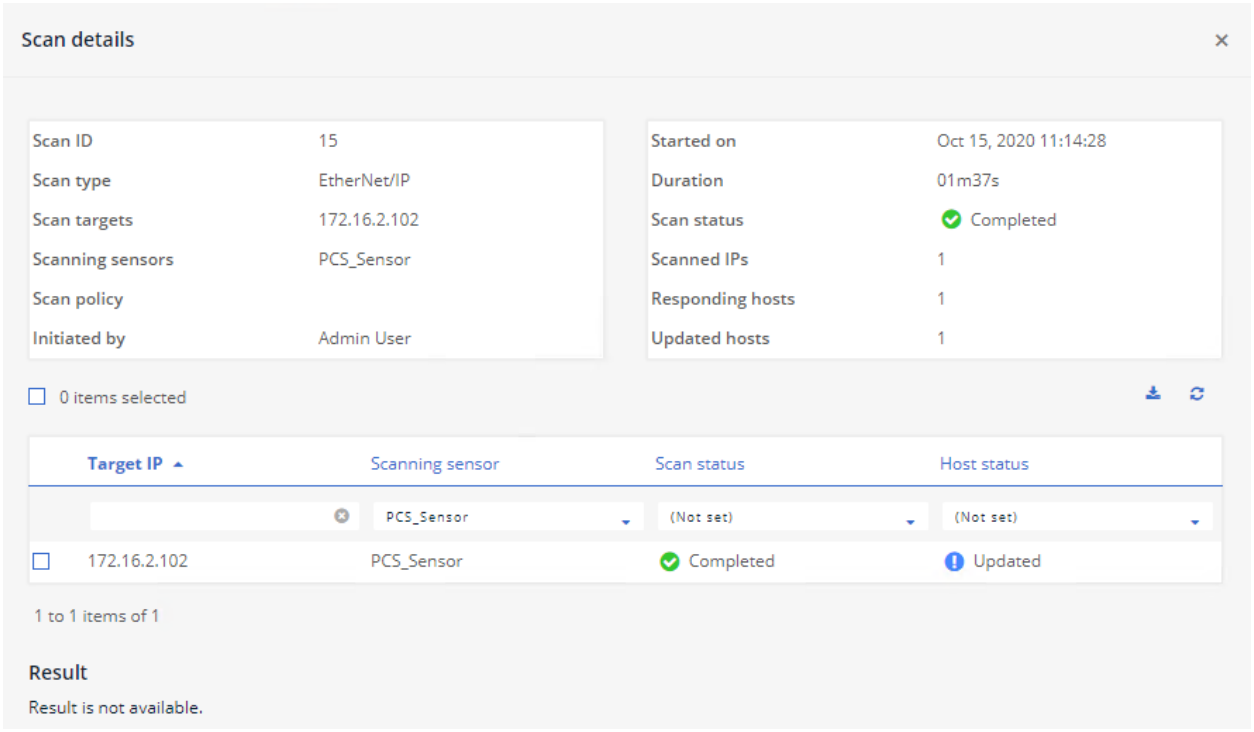


Figure D-106 ICS Patrol Scan Results Showing a Change Configuration was Made



D.11.3 Build 3

D.11.3.1 Configuration

- Remote Access: Cisco VPN
  - configured to allow authorized VPN users to access only the ConsoleWorks web interface
- User Authentication/User Authorization: ConsoleWorks
  - configured to allow remote access to hosts in manufacturing environment
- Behavior Anomaly Detection: Dragos
  - configured to receive packet streams from DMZ, Testbed LAN, Supervisory LAN, and Control LAN

D.11.3.2 Test Results

Dragos detects the change to the firmware as shown on the dashboard in Figure D-107with details shown in Figure D-108.

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

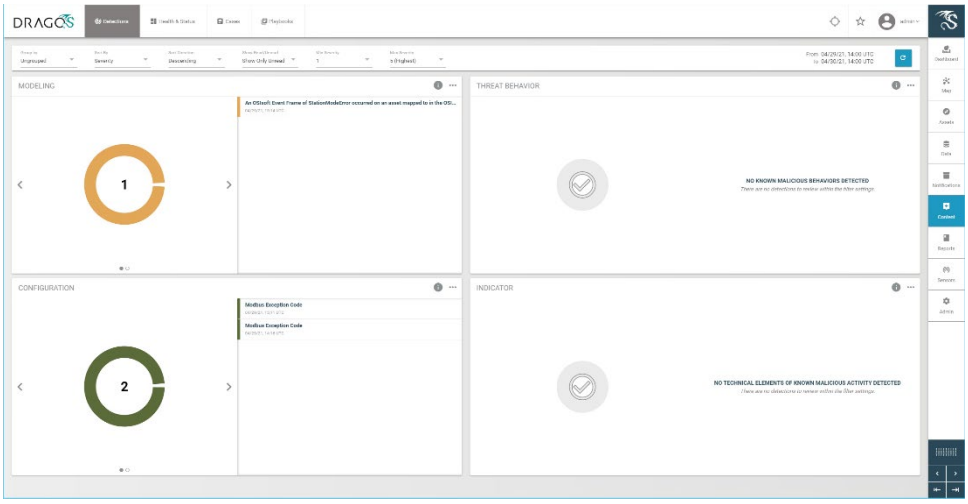
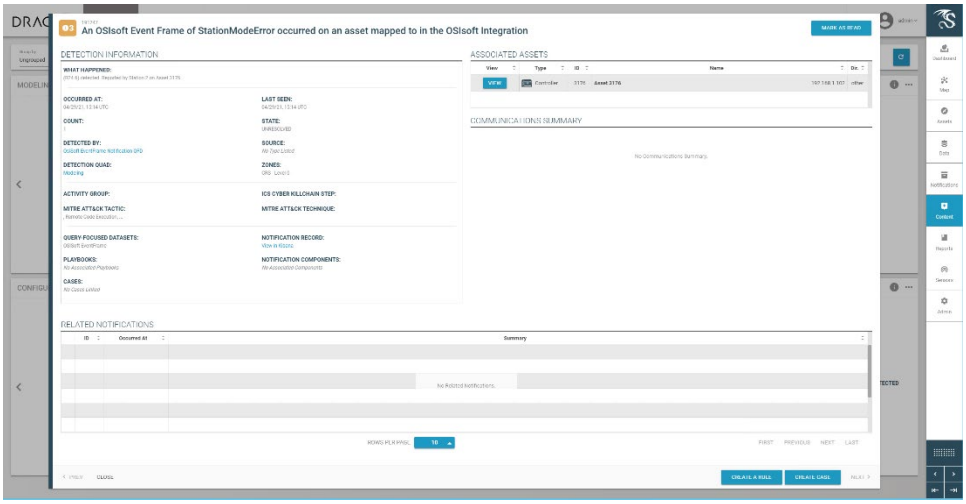


Figure D-108 Details for Firmware Change Alert



D.11.4 Build 4

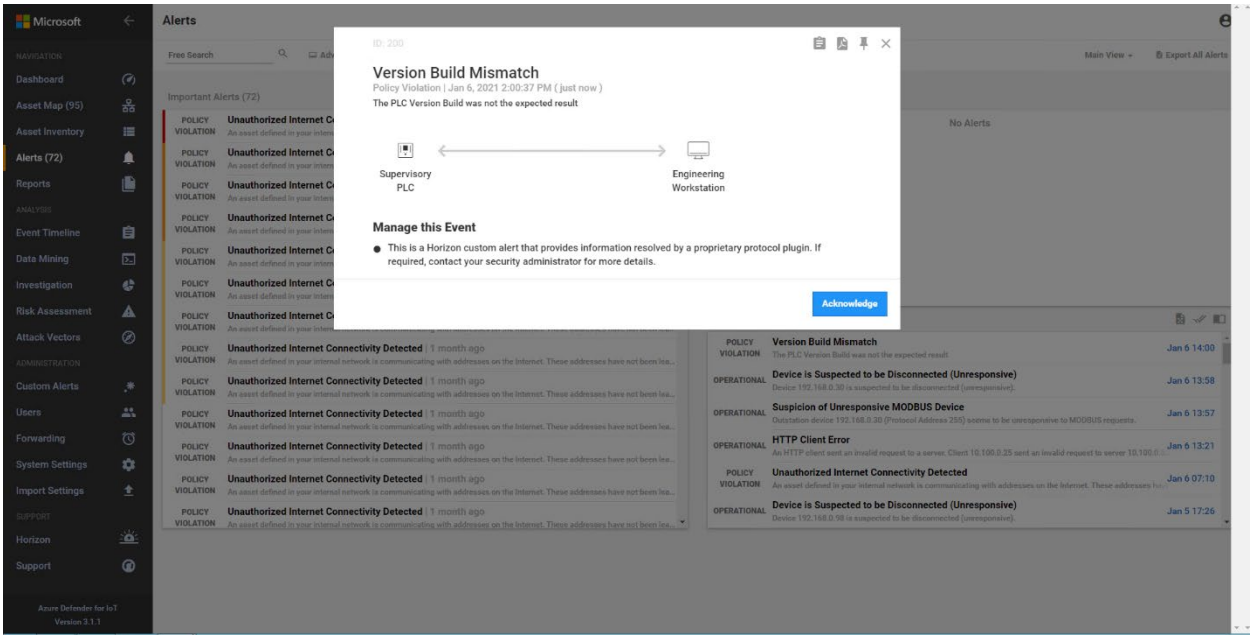
D.11.4.1 Configuration

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

D.11.4.2 Test Results

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

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



Appendix E Benefits of IoT Cybersecurity Capabilities

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

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

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

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

E.1 Device Capabilities Mapping

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

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

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

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	▪ Ability to uniquely identify the IoT device logically. ▪ Ability to uniquely identify a remote IoT device. ▪ Ability for the device to support a unique device ID. ▪ Ability to configure IoT device access control policies using IoT device identity. ▪ Ability to verify the identity of an IoT device. ▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access. ▪ Ability to set and change authentication configurations, policies, and limitations settings for the IoT device. ▪ Ability to create unique IoT device user accounts. ▪ Ability to identify unique IoT device user accounts. ▪ Ability to create organizationally defined	▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing the details necessary to require unique identifiers for each IoT device associated with the system and critical system	AC-2 IA-2 IA-4 IA-5 IA-8 IA-12

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	accounts that support privileged roles with automated expiration conditions. ▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface. ▪ Ability to enable automation and reporting of account management activities. ▪ Ability to establish conditions for shared/group accounts on the IoT device. ▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.	components within which it is used. ▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources. ▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems. ▪ Providing education explaining how to enforce authorized access at the system level.	
PR.AC-3: Remote access is managed.	▪ Ability to configure IoT device access control policies using IoT device identity. ▪ Ability for the IoT device to differentiate between authorized and unauthorized remote users. ▪ Ability to authenticate external users and systems. ▪ Ability to securely interact with authorized external, third-party systems.	N/A	AC-17 AC-19 AC-20

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	▪ Ability to identify when an external system meets the required security requirements for a connection. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks. ▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including: • usage restrictions • configuration requirements • connection requirements • manufacturer established requirement ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to prevent external access to the IoT device management interface. ▪ Ability to control the IoT device's logical interface (e.g., locally or remotely). ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors.		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	▪ Ability to assign roles to IoT device user accounts. ▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary). • Ability to establish user accounts to support role-based logical access privileges. • Ability to administer user accounts to support role-based logical access privileges. • Ability to use organizationally defined roles to define each user account's access and permitted device actions. • Ability to support multiple levels of user/process account functionality and roles for the IoT device. ▪ Ability to apply least privilege to user accounts. • Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege. • Ability to apply least privilege settings within	▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device. ▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces, such as for specific support, updates, ongoing maintenance, and other purposes. ▪ Providing documentation with instructions for the IoT device customer to follow for how to restrict interface connections that enable specific activities. ▪ Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis. ▪ Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis. ▪ Providing documentation and/or other communications describing how to implement management and operational	AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions). • Ability to limit access to privileged device settings that are used to establish and administer authorization requirements. • Ability for authorized users to access privileged settings. ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to enable automation and reporting of account management activities. ▪ Ability to establish conditions for shared/group accounts on the IoT device. ▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.	controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing a detailed description of the other types of devices and systems that will access the IoT device during customer use of the device, and how they will access it. ▪ Providing communications and detailed instructions for implementing a hierarchy of privilege levels to use with the IoT device and/or necessary associated information systems. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources. ▪ Providing education explaining how to control access to IoT devices	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5

	▪ Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on:
	  • run-time access control decisions facilitated by dynamic privilege management.
	  • organizationally defined actions to access/use device.
	▪ Ability to allow information sharing capabilities based upon the type and/or role of the user attempting to share the information.
	▪ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization.
	▪ Ability to establish limits on authorized concurrent device sessions.
	▪ Ability to restrict updating actions to authorized entities.
	▪ Ability to restrict access to the cybersecurity state indicator to authorized entities.
	▪ Ability to revoke access to the IoT device.
		implemented within IoT device customer information systems.
		▪ Providing education explaining how to enforce authorized access at the system level.
		▪ Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that communicate or interface with the device.
		▪ Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device.
		▪ Providing education and supporting materials for how to establish roles to support IoT device policies, procedures, and associated documentation.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	▪ Ability for the IoT device to require authentication prior to connecting to the device. ▪ Ability for the IoT device to support a second, or more, authentication method(s) such as: • temporary passwords or other one-use log-on credentials • third-party credential checks • biometrics • hard tokens ▪ Ability to authenticate external users and systems. ▪ Ability to verify and authenticate any update before installing it.	▪ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication. ▪ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques. ▪ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.	AC-7 AC-8 AC-9 AC-12 AC-14 IA-2 IA-3 IA-4 IA-5 IA-8 IA-11
PR.DS-1: Data-at-rest is protected.	▪ Ability to execute cryptographic mechanisms of appropriate strength and performance. ▪ Ability to obtain and validate certificates. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to change keys securely. ▪ Ability to generate key pairs.	▪ Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device. ▪ Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet	SC-28 MP-2 MP-4 MP-5

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	▪ Ability to store encryption keys securely. ▪ Ability to cryptographically store passwords at rest, as well as device identity and other authentication data. ▪ Ability to support data encryption and signing to prevent data from being altered in device storage. ▪ Ability to secure data stored locally on the device. ▪ Ability to secure data stored in remote storage areas (e.g., cloud, server). ▪ Ability to utilize separate storage partitions for system and user data. ▪ Ability to protect the audit information through mechanisms such as: • encryption • digitally signing audit files • securely sending audit files to another device • other protections created by the device manufacturer	requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.	
PR.DS-6: Integrity checking mechanisms are used to verify software, firm-	▪ Ability to identify software loaded on the IoT device based on IoT device identity.	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data	SC-16 SI-7 MP-4

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
ware, and information integrity.	▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.	MP-5

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.IP-4: Backups of information are conducted, maintained, and tested.	N/A	▪ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary. ▪ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored. ▪ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.	CP-4 CP-9
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	N/A	▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.	MA-2 MA-3 MA-5 MA-6

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		▪ Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used. ▪ Providing the details necessary for IoT device customers to implement only organizationally approved IoT device diagnostic tools within their system. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		maintenance operations that the IoT device customer is required to perform. If such comprehensive IoT device maintenance operations documentation does not exist, the manufacturer should clearly communicate to IoT device customers that the user must perform these operations themselves. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities. ▪ Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization. ▪ Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing the details necessary for customers to document attempts to obtain IoT device components or IoT device information system service documentation when such documentation is either unavailable or nonexistent, and documenting the appropriate response for manufacturer employees, or	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		supporting entities, to follow. ▪ Providing a process for IoT device customers to contact the manufacturer to ask questions or obtain help related to the IoT device configuration settings. ▪ Providing information to allow for in-house support from within the IoT device customer organization. ▪ Providing education explaining how to inspect IoT device and/or use maintenance tools to ensure the latest software updates and patches are installed. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing education that explains the legal requirements governing IoT device maintenance responsibilities or how to meet specific types of legal requirements when using the IoT device.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	N/A	▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the	MA-4

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		manufacturer's supporting entities. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities. ▪ Providing the details necessary for maintaining records for nonlocal IoT device maintenance and diagnostic activities. ▪ Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel. ▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
		the IoT device customer's organization. ▪ Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	N/A	▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.	AC-4 CA-3 CM-2 SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	N/A	▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.	AU-6 CA-7 IR-4 SI-4
DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing	▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.	AU-6 AU-12 CA-7 IR-4 IR-5 SI-4

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
	information can be checked to allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time.		
DE.CM-1: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	▪ Ability to monitor specific actions based on the IoT device identity. ▪ Ability to access information about the IoT device's cybersecurity state and other necessary data. ▪ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor communications traffic.	▪ Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information. ▪ Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing how to perform monitoring activities.	AU-12 CA-7 CM-3 SC-7 SI-4
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	N/A	N/A	AC-2 AU-12 CA-7 CM-3 SC-5 SC-7

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	NIST SP 800-53 Rev. 5
			SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.	AC-2 AU-12 AU-13 CA-7 CM-10 CM-11

E.2 Device Capabilities Supporting Functional Test Scenarios

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

Table E-2 builds on the functional test scenarios included in Section 5 of this document. The table lists both **device cybersecurity capabilities** and **nontechnical supporting capabilities** that map to relevant *Cybersecurity Framework* Subcategories for each of the functional test scenarios. If IoT devices are

integrated into future efforts or a production ICS environment, selecting devices and/or third parties that provide these capabilities can help achieve the respective functional requirements.

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

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

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

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
Scenario 1: Protect Host from Mal-ware via USB: This test will demon-strate blocking the introduction of malware through physical access to a workstation within the manufacturing system. **PR.DS-6** **PR.MA-2** **DE.AE-2**	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures,	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities. ▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.
Scenario 2: Protect Host from Mal-ware via Network Vector This test will demonstrate the	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures.	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
detection of mal-ware introduction from the network. **PR.DS-6** **PR.MA-1** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3** **DE.CM-7**	▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications)	▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when	operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
Scenario 3: Protect Host from Malware via Remote Access Connections: This test will demonstrate blocking malware attempting to infect manufacturing system through authorized remote access connections.	▪ Ability to uniquely identify the IoT device logically. ▪ Ability to uniquely identify a remote IoT device. ▪ Ability for the device to support a unique device ID. ▪ Ability to configure IoT device access control policies using IoT device identity. ▪ Ability to verify the identity of an IoT device.	▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
PR.AC-1 **PR.AC-3** **PR.AC-4** **PR.AC-7** **PR.MA-1** **PR.MA-2** **DE.CM-3** **DE.CM-7**	▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access. ▪ Ability to set and change authentication configurations, policies, and limitations settings for the IoT device. ▪ Ability to revoke access to the device. ▪ Ability to create unique IoT device user accounts. ▪ Ability to identify unique IoT device user accounts. ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to configure IoT device access control policies using IoT device identity. ▪ Ability to authenticate external users and systems.	▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device. ▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces, such as for specific support, updates, ongoing maintenance, and other purposes. ▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems. ▪ Providing education explaining how to enforce authorized access at the system level. ▪ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication. ▪ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques. ▪ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to securely interact with authorized external, third-party systems. ▪ Ability to identify when an external system meets the required security requirements for a connection. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks. ▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface. ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to prevent external access to the IoT device management interface. ▪ Ability to assign roles to IoT device user accounts.	▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles. ▪ Ability to apply least privilege to user accounts. ▪ Ability to enable automation and reporting of account management activities. ▪ Ability for the IoT device to require authentication prior to connecting to the device. ▪ Ability for the IoT device to support a second, or more, authentication method(s). ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors.	

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	
Scenario 4: Protect Host from Unauthorized Application Installation: This test will demonstrate blocking the installation and execution of unauthorized applications on workstation in the manufacturing system. **PR.DS-6** **PR.MA-1** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3** **DE.CM-7**	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting).	▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
Scenario 5: Protect from Unauthorized Addition of a Device: This test will demonstrate the detection of an unauthorized device connecting to the manufacturing system. **PR.DS-6** **PR.MA-1** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3** **DE.CM-7**	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation).	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings.	▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
Scenario 6: Detect Unauthorized Device-to-Device Communications: This test will demonstrate the detection of unau-	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures.	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
thorized communi-cations between devices. **PR.DS-6** **PR.MA-1** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3** **DE.CM-7**	▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications)	controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when	▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
Scenario 7: Protect from Unauthorized Modification and Deletion of Files: This test will demonstrate protection of files from unauthorized deletion both locally and on network file share. **PR.DS-1** **PR.DS-6** **PR.IP-4** **PR.MA-1** **DE.AE-2**	▪ Ability to execute cryptographic mechanisms of appropriate strength and performance. ▪ Ability to obtain and validate certificates. ▪ Ability to change keys securely. ▪ Ability to generate key pairs. ▪ Ability to store encryption keys securely. ▪ Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.	▪ Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data, associated systems data, and data output from the IoT device. ▪ Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements. ▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to support data encryption and signing to prevent data from being altered in device storage. ▪ Ability to secure data stored locally on the device. ▪ Ability to secure data stored in remote storage areas (e.g., cloud, server). ▪ Ability to utilize separate storage partitions for system and user data. ▪ Ability to protect the audit information through mechanisms such as: ▪ encryption ▪ digitally signing audit files ▪ securely sending audit files to another device ▪ other protections created by the device manufacturer ▪ Ability to identify software loaded on the IoT device based on IoT device identity.	▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary. ▪ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored. ▪ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it.	webinar) for various aspects involved with backing up the IoT device data. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.
Scenario 8: Detect Unauthorized Modification of PLC Logic: This test will demonstrate the detection of PLC logic modification. **PR.AC-3** **PR.AC-7** **PR.DS-6** **PR.MA-1** **PR.MA-2** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3** **DE.CM-7**	▪ Ability to configure IoT device access control policies using IoT device identity. ▪ Ability to authenticate external users and systems. ▪ Ability to securely interact with authorized external, third-party systems. ▪ Ability to identify when an external system meets the required security requirements for a connection. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks. ▪ Ability to establish requirements for remote	▪ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication. ▪ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques. ▪ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device. ▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	access to the IoT device and/or IoT device interface. ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to prevent external access to the IoT device management interface. ▪ Ability for the IoT device to require authentication prior to connecting to the device. ▪ Ability for the IoT device to support a second, or more, authentication method(s). ▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms.	▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use.	▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities. ▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a	▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	Universal Serial Bus [USB] port is present).	
Scenario 9: Protect from Modification of Historian Data: This test will demonstrate the blocking of modification of historian archive data. **PR.DS-6** **PR.MA-1** **DE.AE-2**	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures,	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.
Scenario 10: Detect Sensor Data Manipulation: This test will demonstrate detection of atypical data reported to the historian. **PR.IP-4** **PR.DS-6** **PR.MA-1** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3** **DE.CM-7**	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective	▪ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary. ▪ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored. ▪ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data. ▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities.	▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
Scenario 11: Detect Unauthorized Firmware Modification: This test will demonstrate the detection of device firmware modification **PR.DS-6** **PR.MA-1** **DE.AE-1** **DE.AE-2** **DE.AE-3** **DE.CM-1** **DE.CM-3**	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
DE.CM-7	unauthorized access and modification. ▪ Ability to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it. ▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory). ▪ Ability to provide a physical indicator of sensor use. ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to	explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.

Scenario ID and Description with *Cybersecurity Framework* Sub-categories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	allow for review, analysis, and reporting). ▪ Ability to keep an accurate internal system time. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of sensors. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems. ▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched. ▪ Providing documentation describing the types of usage and environmental systems data that can be collected from the IoT device. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.