NIST SPECIAL PUBLICATION 1800-7

Situational Awareness

For Electric Utilities

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

Jim McCarthy
Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP1800-7

The first draft of this publication is available free of charge from:
https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf

NIST SPECIAL PUBLICATION 1800-7

Situational Awareness for Electric Utilities

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

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Andre Thibault
John Wiltberger
The MITRE Corporation
McLean, VA

August 2019

U.S. Department of Commerce
Wilbur Ross, Secretary

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

NIST SPECIAL PUBLICATION 1800-7A

Situational Awareness

For Electric Utilities

Volume A:
Executive Summary

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani
The MITRE Corporation
McLean, VA

August 2019

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP1800-7

The first draft of this publication is available free of charge from:
https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Situational awareness, in the context of this guide, is the understanding of one's environment and the ability to predict how it might change due to various factors.

As part of their current cybersecurity efforts, some electric utilities monitor physical, operational, and information technology (IT) separately. According to energy sector stakeholders, many utilities are currently assessing a more comprehensive approach to situational awareness, which, through increased real-time or near real-time cybersecurity monitoring, can enhance the resilience of their operations.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore an example solution that can be used by energy sector companies to alert their staff to potential or actual cyber attacks directed at the grid.

The security characteristics in our situational awareness platform are informed by guidance and best practices from standards organizations, including the NIST Cybersecurity Framework and North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Version 5 standards.

This NIST Cybersecurity Practice Guide demonstrates how organizations can use commercially available products that can be integrated with an organization's existing infrastructure. The combination of these products provides a converged view of all sensor data within the utility's network systems, including IT, operational, cyber, and physical access control systems, which often exists in separate "silos."

The example solution is packaged as a "how to" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world and based on risk management. The guide may help inform electric utilities in their efforts to gain situational awareness efficiencies. Doing so may enable faster monitoring, identification, and response to incidents while also saving research and proof-of-concept costs for the sector and its ratepayers and customers.

CHALLENGE

As part of the agenda to address the U.S. critical infrastructure, the energy sector, along with healthcare, finance, transportation, water, and communications sectors, has reported significant cyber incidents. As an integral component to the energy sector, industrial control systems (ICS) are increasingly vulnerable to cybersecurity threats, whether intentional or unintentional. In December 2015, the energy sector realized the potential effect of a combined attack on an electric utility's IT and ICS. In this instance, a Ukraine power grid was attacked, resulting in an electricity disruption that left approximately 225,000 people without electric power. The malicious actors then inundated the company's customer service center with calls, which slowed the response time to the electricity outage by causing internal challenges.

The monitoring model used by some electric utilities includes separate physical, operational, and IT silos, a practice that lacks efficiency and can negatively impact response time to incidents, according to the NCCoE's energy sector stakeholders. However, a number of useful products are commercially available for monitoring enterprise networks for myriad security events; yet, these products can have limited effectiveness when considering the specific ICS infrastructure requirements. A converged network monitoring solution that is tailored to the ICS cybersecurity nuances could reduce blind spots for electric utilities, resulting in comprehensive situational awareness across enterprise business system and operational ICS environments.

SOLUTION

The NCCoE has developed *Situational Awareness for Electric Utilities* to augment existing and disparate physical, operational, and IT situational awareness efforts by using commercial and open-source products to collect and converge monitoring information across these silos. The aggregated and correlated information is analyzed, and relevant alerts are provided to each domain's monitoring capabilities, improving the situational awareness of security analysts. The converged data can facilitate a more effective, efficient, and appropriate response to an event, compared with a response that relies on isolated data.

The NCCoE sought existing technologies that provided the following capabilities:

- Security information and event management (SIEM) or log analysis software
- ICS equipment (e.g., remote terminal units, programmable logic controllers and relays) along with associated software and communications equipment (e.g., radios and encryptors)
- "bump-in-the-wire" devices for augmenting operational technology with encrypted communication and logging capabilities
- software for collecting, analyzing, visualizing, and storing operational control data (e.g., historians, outage management systems, distribution management systems, human-machine interfaces)
- products that ensure the integrity and accuracy of data collected from remote facilities

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. 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 a solution.

BENEFITS

The NCCoE's practice guide to *Situational Awareness for Electric Utilities* can help your organization:

- improve ability to detect cyber-related security breaches or anomalous behavior, likely resulting in early detection and having less impact on energy delivery, thereby lowering overall business risk while supporting enhanced resilience and reliability performance outcomes
- increase probability that investigations of attacks or anomalous system behavior will realize successful output, which in turn can inform risk management and mitigation
- improve accountability and traceability, resulting in lessons-learned use cases
- simplify regulatory compliance via automating generation and collection of disparate operational log data

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/situational-awareness . If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at energy_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

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.

Please note: Hewlett Packard Enterprise in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200

NIST SPECIAL PUBLICATION 1800-7B

Situational Awareness

For Electric Utilities

Volume B:
Approach, Architecture, and Security Characteristics

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani
The MITRE Corporation
McLean, VA

August 2019

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP1800-7

The first draft of this publication is available free of charge from:
https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-7B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-7B, 86 pages, (August 2019), 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 energy_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 IT 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 and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

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 Series 1800) 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

Through direct dialogue between NCCoE staff and members of the energy sector (composed mainly of electric power companies and those who provide equipment and/or services to them) it became clear that energy companies need to create and maintain a high level of visibility into their operating environments to ensure the security of their operational resources (operational technology [OT]), including industrial control systems (ICS), buildings, and plant equipment. However, energy companies, as well as all other utilities with similar infrastructure and situational awareness challenges, also need insight into their corporate or information technology (IT) systems and physical access control systems (PACS). The convergence of data across these three often self-contained silos (OT, IT, and PACS) can better protect power generation, transmission, and distribution.

Real-time or near real-time situational awareness is a key element in ensuring this visibility across all resources. Situational awareness, as defined in this use case, is the ability to comprehensively identify and correlate anomalous conditions pertaining to ICS, IT resources, and access to buildings, facilities, and other business mission-essential resources. For energy companies, having mechanisms to capture, transmit, view, analyze, and store real-time or near-real-time data from ICS and related networking equipment provides energy companies with the information needed to deter, identify, respond to, and mitigate cyber attacks against their assets.

With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remedy them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping demonstrate compliance with information security standards. This NCCoE project’s goal is ultimately to improve the security of OT through situational awareness.

This NIST Cybersecurity Practice Guide describes our collaborative efforts with technology providers and energy sector stakeholders to address the security challenges that energy providers face in deploying a comprehensive situational awareness capability. It offers a technical approach to meeting the challenge and also incorporates a business value mind-set by identifying the strategic considerations involved in implementing new technologies. The guide provides a modular, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how we met the challenge by using open-source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case is based on an everyday business operational scenario that provides the underlying impetus for the functionality presented in the guide. Test cases were defined with industry participation to provide multiple examples of the capabilities necessary to provide situational awareness.

While the example solution was demonstrated with a certain suite of products, the guide does not endorse these products. Instead, it presents the characteristics and capabilities that an organization’s security experts can use to identify similar standards-based products that can be integrated quickly and cost effectively with an energy provider’s existing tools and infrastructure.

KEYWORDS

correlated events; cybersecurity; energy sector; information technology; operational technology; physical access control systems; security information and event management; situational awareness

ACKNOWLEDGMENTS

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

Name	Organization
Robert Lee	Dragos
Justin Cavinee	Dragos
Jon Lavender	Dragos
Steve Roberts	Hewlett Packard Enterprise
Bruce Oehler	Hewlett Packard Enterprise
Gil Kroyzer	ICS^2
Gregory Ravikovich	ICS^2
Robert Bell	ICS^2
Fred Hintermeister	NERC
Paul J. Geraci	OSIsoft
Mark McCoy	OSIsoft
Stephen J. Sarnecki	OSIsoft
Paul Strasser	PPC
Matt McDonald	PPC
Steve Sage	PPC
T.J. Roe	Radiflow
Ayal Vogel	Radiflow

Name	Organization
Dario Lobozzo	Radiflow
Dave Barnard	RS2
Ben Smith	RSA
Tarik Williams	RSA, a Dell Technologies business
David Perodin	RSA, a Dell Technologies business
George Wrenn	Schneider Electric
Michael Pyle	Schneider Electric
AJ Nicolosi	Siemens
Jeff Foley	Siemens
Bill Johnson	TDi Technologies
Pam Johnson	TDi
Clyde Poole	TDi
Eric Chapman	University of Maryland, College Park
David S. Shaughnessy	University of Maryland, College Park
Don Hill	University of Maryland, College Park
Mary-Ann Ibeziako	University of Maryland, College Park
Damian Griffe	University of Maryland, College Park
Mark Alexander	University of Maryland, College Park
Nollaig Heffernan	Waratek

Name	Organization
James Lee	Waratek
John Matthew Holt	Waratek
Andrew Ginter	Waterfall
Courtney Schneider	Waterfall
Tim Pierce	Waterfall
Kori Fisk	The MITRE Corporation
Tania Copper	The MITRE Corporation

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	Build Involvement
Dragos	CyberLens
Hewlett Packard Enterprise*	ArcSight
ICS2	OnGuard
OSIsoft	Pi Historian
Radiflow	iSIM
RS2 Technologies	Access It!, Door Controller
RSA, a Dell Technologies business	Archer Security Operations Management
Schneider Electric	Tofino Firewall
Siemens	RUGGEDCOM CROSSBOW
TDi Technologies	ConsoleWorks
Waratek	Waratek Runtime Application Protection
Waterfall Security Solutions	Unidirectional Security Gateway, Secure Bypass

**Please note: Hewlett Packard Enterprise in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.*

The NCCoE also wishes to acknowledge the special contributions of the University of Maryland for providing us with a real-world setting for the situational awareness build; Project Performance Company for its dedication in assisting the NCCoE with the very challenging and complex integration in this build; and the NCCoE Energy Provider Community for its patience, support, and guidance throughout the life cycle of this project.

Contents

List of Figures

List of Tables

1 Summary

Situational awareness (SA) is “the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” [1]. The intent of SA is to know what is happening around you and how it might affect your activities. For electricity utilities, this means understanding what is happening in the environment that might affect delivery of electricity to customers. Traditionally, this has involved knowing the operating status of generation, transmission, and distribution systems, as well as physical challenges such as weather and readiness, to facilitate response to outages. As computers and networks have been incorporated in grid operations, awareness of the cyber situation is becoming increasingly important to ensuring that “the lights stay on.”

The National Cybersecurity Center of Excellence (NCCoE) met with energy sector stakeholders to understand key cybersecurity issues impacting operations. The feedback emphasized a more efficient means of comprehensively detecting potential cybersecurity incidents directed at their operational technology (OT) or industrial control systems (ICS), information technology (IT) or corporate networks, and their physical facilities such as substations and corporate offices.

The NCCoE’s example solution provides a converged and correlated view of OT, IT, and physical access resources. In our reference design, we collect sensor data from these resources and provide alerts to a platform that produces actionable information.

This example solution is packaged as a “how to” guide that demonstrates how to implement standards-based cybersecurity technologies in the real world based on risk analysis and regulatory requirements. The guide might help the energy industry gain efficiencies in SA while saving research and proof-of-concept costs.

1.1 The Challenge

Energy companies rely on OT to control the generation, transmission, and distribution of power. While there are a number of useful products on the market for monitoring enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of control system networks. ICS and IT devices were designed with different purposes in mind. Attempting to use IT security applications for ICS, although in many cases useful, still does not properly account for the availability requirements of ICS networks. A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots and provide real-time SA, that is, provide notification of events as they occur.

To improve overall SA, energy companies need mechanisms to capture, transmit, view, analyze, and store real-time or near-real-time data from ICS and related networking equipment. With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remedy them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time or near-real-time data from networks also helps organizations be compliance with information security standards or regulations, particularly those that require specific event log information.

There is a definite need to improve a utility's ability to detect cyber-related security breaches or anomalous behavior, in real or near real time. The ability to do this will result in earlier detection of cybersecurity incidents and potentially reduce the severity of the impact of these incidents within a utility's operational infrastructure. Energy sector stakeholders noted that a robust situational awareness solution also must be able to alert for both individual and correlated events or incidents. To address these needs, we created a scenario in which a technician dispatcher notices that a substation relay has tripped and begins to investigate the cause. The technician uses a single software interface that monitors system buses, displays an outage map, correlates operational network connections to the bus and outage maps, and indexes operational network and physical security device logs. The technician begins the investigation by querying network logs to determine whether any ICS devices received commands that might have caused the trip. If the answer is yes, then, using the same interface, the technician can automatically examine logs of the most recent commands and network traffic sent to the relevant devices. This information allows the technician to effectively extend the investigation to internal systems and users who communicated with the suspect devices.

To extend the scenario, an analyst on the IT network receives notification that a server is down. The analyst investigates across the network and is alerted of the tripped substation relay. Are the anomalies connected? Use of our SA solution could answer this question in addition to achieving the needs described above. Additional benefits of the solution are addressed in Section 1.4.

1.2 The Solution

This NIST Cybersecurity Practice Guide demonstrates how commercially available technologies can meet a utility's need to provide comprehensive real-time or near-real-time SA.

The NCCoE laboratory houses an environment that simulates the common devices and technologies found in a utility such as IT and OT systems and physical access control systems (PACS). In this guide, we show how a utility can implement a converged alerting capability to provide a comprehensive view of cyber-related events and activities across silos by using multiple commercially available products. Furthermore, we identified products and capabilities that, when linked together, provide a converged and comprehensive platform that can alert utilities to potentially malicious activity.

The guide provides:

- a detailed example solution and capabilities that address security controls
- a demonstration of the approach that uses commercially available products

- how-to instructions for implementers and security engineers with instructions on integrating and configuring the example solution into their organization's enterprise in a manner that achieves security goals with minimal impact on operational efficiency and expense

Commercial, standards-based products such as the ones we used are readily available and interoperable with existing IT infrastructure and investments. Our simulated environment is similar in breadth and diversity to the distributed networks of large organizations, which can include corporate and regional business offices, power generation plants, and substations, but not on the same scale of deployed assets as these large organizations.

This guide lists all the necessary components and provides installation, configuration, and integration information so that an energy company can replicate what we have built. The NCCoE does not endorse the suite of commercial products used in the reference design. These products were utilized after an open call to participate via the Federal Register. A utility's security expert(s) should identify the standards-based products that will best integrate with the existing tools and systems already contained in the ICS and IT infrastructure. A business can adopt this solution or one that adheres to these guidelines in whole, or this guide can be used as a starting point for tailoring and implementing parts of a solution.

1.3 Risks

This practice guide addresses risk by using current industry standards, such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) V5, as well as taking into account risk considerations at both the operational and strategic levels.

At the strategic level, one might consider the cost of mitigating these risks and the potential return on investment in implementing a product (or multiple products). One might also want to assess if a converged SA platform can help enhance the productivity of employees, minimize impacts to the operating environment, and provide the ability to investigate incidents to mitigate future occurrences. This example solution addresses imminent operational security risks and incorporates strategic risk considerations.

Operationally, the lack of a converged SA platform, especially one with the ability to collect and correlate sensor data from all the silos, can increase both the risk of malicious cyber attacks being directed at an organization, or worse, the resulting damage that might ensue should such attacks go undetected. At a fundamental level, SA provides alerts to potential malicious behavior, which includes detection, prevention, and reporting mechanisms to ensure that proper remediation and investigation take place should these events occur.

Adopting any new technology, including this example SA solution, can introduce new risks to an enterprise. However, by aggregating sensor data from all the silos (OT, PACS, and IT), a utility can increase its ability to identify a potentially malicious event that might otherwise go undetected or unreported. The lack of ability to see across the silos and correlate event data yields a potential blind spot to the safe and secure operation of utilities' most critical business assets.

1.4 Benefits

The NCCoE, in collaboration with our stakeholders in the energy sector, identified the need for a network monitoring solution specifically adapted to include ICS cybersecurity. The following are what we determined to be the key (but not exclusive) benefits of implementing this solution:

- improves a utility's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of critical incidents on energy delivery, thereby lowering overall business risk
- increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- improves accountability and traceability, leading to valuable operational lessons learned
- simplifies regulatory compliance by automating generation and collection of a variety of operational log data

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the example solution. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-7A: *Executive Summary*
- NIST SP 1800-7B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-7C: *How-To Guides* – instructions for building the example solution

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary* (NIST SP 1800-7A), which describes the following topics:

- challenges that sector organizations face in maintaining cross-silo situational awareness
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-7B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Assessing Risk Posture, provides a description of the risk analysis we performed
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary,* NIST SP 1800-7A, with your leadership team members to help them understand the importance of adopting standards-based SA for electric utilities.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, NIST SP 1800-7C, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT 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 a solution that includes PACS and OT and IT systems, and business processes. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope 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.

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 detailed definitions of terms, see the *NCCoE Glossary.*

Typeface/ Symbol	Meaning	Example
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, on-screen 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

The NCCoE initiated this project because security leaders in the energy sector told us that a lack of correlated SA information from all silos is a primary security concern to them. As we developed and refined the original problem statement, or use case, on which this project is based, we consulted with chief information officers, chief information security officers, security management personnel, and others with financial decision-making responsibility (particularly for security) in the energy sector.

Energy sector colleagues shared that they need to know when cybersecurity events occur throughout the organization. Additionally, the information generated about such events should be used to correlate data among various sources before arriving at a converged platform. Security staff need to be aware of potential or actual cybersecurity incidents in their PACS and IT and OT systems and to view these alerts on a single converged platform. Furthermore, it is essential that this platform can drill down, investigate, and subsequently fully remedy or effectively mitigate a cybersecurity incident affecting any or all of the organization.

The example solution in this guide uses commercially available capabilities designed to perform these critical functions. Though security components and tools already exist in most utilities, the value of this NCCoE build can be seen in its ability to span across all silos and correlate sensor data. Currently, utilities rely on separate and perhaps disparate systems to provide security data. It is time consuming for staff to comb through OT or IT device event logs, physical access data, and other system data to trace anomalies to their source. A real-time SA platform with a well-developed alerting mechanism can speed the process of detecting potentially malicious events, providing the information necessary to focus an investigation, making a determination regarding the potential issue, and remedying or mitigating any negative effects.

We constructed an end-to-end SA platform that includes many of the components necessary to eliminate or mitigate the impact of attacks directed at utilities. The solution employs actual grid data sent to numerous applications and devices to increase cybersecurity. The solution includes:

- asset inventorying (especially for ICS devices)
- data-in-transit encryption
- advanced security dashboard views
- configuration change alerts
- behavioral anomaly detection
- security information and event management (SIEM) capability
- unidirectional gateway functionality for ICS network protection
- single-source time stamping and log transmission capability
- Structured Query Language (SQL) injection (SQLi) detection
- intrusion detection/prevention

3.1 Audience

This guide is intended for individuals or entities who are interested in understanding the architecture of the end-to-end situational awareness platform that the NCCoE designed and implemented to enable energy sector security staff to receive correlated information on cybersecurity events that occur throughout their IT and OT systems and PACS on a single converged platform. It may also be of interest to anyone in the energy sector, industry, academia, or government who seeks general knowledge of an original design and benefits of a situational awareness security solution for energy sector organizations.

3.2 Scope

The focus of this project is to address the risk of not being able to prevent, detect, or mitigate cyber attacks against OT, IT, and PACS infrastructure in a timely manner, a topic indicated by the energy sector as a critical cybersecurity concern. In response, the NCCoE drafted a use case that identified numerous desired solution characteristics. After an open call in the Federal Register for vendors to help develop a solution, we chose participating technology collaborators on a first-come, first-served basis.

We scoped the project to produce the following high-level desired outcomes:

1. provide a real-time, converged SA capability that includes sensor data from OT, IT, and PACS networks and devices
2. provide a variety of cyber attack prevention, detection, response, reporting, and mitigation capabilities
3. correlate meaningful sensor data between silos, or between devices within individual silos, that will produce actionable alerts
4. provide a single view of this correlated alerting platform data, which can be customized to accommodate the needs of individual organizations

The objective is to perform all four capabilities and display on a single interface that can serve as the authoritative source for security analysts monitoring the security of the assets on an energy provider's facilities, networks, and systems.

3.3 Assumptions

This project is guided by the following assumptions, which should be considered when evaluating whether to implement the solution in your organization.

3.3.1 Security

The SA example solution supports data monitoring, collection, aggregation, and analysis with the goal of enabling a robust SA capability.

In the security evaluation, we assume that all potential adopters of the build or of any of its components already have in place some degree of network security. Therefore, we focus on the security protections being introduced by this reference design. The security evaluation describes vulnerabilities that may be introduced by virtue of implementing the capabilities described in this reference design and does not attempt to identify an exhaustive list of all possible vulnerabilities.

3.3.2 Existing Infrastructure

We assume that you already have some combination of the capabilities discussed in this example solution. A combination of some of the components described here, or a single component, can improve your overall security posture for OT, IT, and PACS without requiring removal or replacement of existing infrastructure. This guide provides both a complete end-to-end solution and options that can be implemented based on your needs.

This example solution is made of many commercially available components. The solution is modular in that one of the products used can be swapped for one that is suitable for your environment.

3.3.3 Technical Implementation

The guide is written from a how-to perspective. Its foremost purpose is to provide details on how to install, configure, and integrate components and how to construct correlated alerts based on the capabilities we selected. We assume that an energy provider has the technical resources to implement all or parts of the example solution or has access to integrator companies that can perform the implementation.

3.3.4 Capability Variation

We fully understand that the capabilities presented here are not the only security capabilities available to the industry. Desired security capabilities will vary considerably from one company to the next. As mentioned in the scope, our goal is to provide SA utilizing sensor data from OT, IT, and PACS. We selected what we believe to be a basic and fundamental approach to SA.

3.4 Risk Assessment

We performed two types of risk assessment: the initial analysis of the risk posed to the energy sector, which led to creation of the use case and the desired security characteristics; and an analysis to show users how to manage risk to components introduced by adoption of the solution.

NIST Special Publication (SP) 800-30, *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. Park 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, *Guide for Applying the Risk Management Framework to Federal Information Systems* — material that is available to the public [2]. 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 Assessing Risk Posture

Using the guidance in NIST’s series of special publications concerning the RMF, we performed two key activities to identify the most compelling risks encountered by energy providers. The first activity was a face-to-face meeting with members of the energy community to define the main security risks to business operations. This meeting identified a primary risk concern: the lack of a comprehensive or cross-silo SA capability, particularly one that would include sensor data from OT networks and devices. We then identified the core risk area, SA, and established the core operational risks encountered daily in this area.

We deemed the following as tactical risks:

- lack of data visualization and analysis capabilities that help dispatchers and security analysts view control system behavior, network security events, and physical security events as a cohesive whole
- lack of analysis and correlation capabilities that could help dispatchers and security analysts understand and identify security events and predict how those events might affect control system operational data from a variety of sources
- inability to aggregate and correlate logs, traffic, and operational data from a variety of sources in OT, IT, and PACS device networks
- inability to allow dispatchers and security analysts to easily automate common, repetitive investigative tasks

Our second key activity was conducting phone interviews with members of the energy sector. These interviews gave us a better understanding of the actual business risks as they relate to the potential cost and business value. NIST SP 800-39, *Managing Information Security Risk*, focuses on the business aspect of risk, namely at the enterprise level. This foundation is essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. Below is a summary of the strategic risks:

- impact on service delivery
- cost of implementation
- budget expenditures as they relate to investment in security technologies
- projected cost savings and operational efficiencies to be gained as a result of new investment in security
- compliance with existing industry standards
- high-quality reputation or public image
- risk of alternative or no action
- successful precedents

Undertaking these activities in accordance with the NIST RMF guidance yielded the necessary operational and strategic risk information, which we subsequently translated to security characteristics. We mapped these characteristics to NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, controls where applicable, along with other applicable industry and mainstream security standards.

3.4.2 Security Control Map

As explained in Section 3.4.1, we derived the security characteristics through a risk analysis process conducted in collaboration with our energy sector stakeholders. This is a critical first step in acquiring or developing the capability necessary to mitigate the risks as identified by our stakeholders. Table 3-1 presents the desired security characteristics of the use case in terms of the Subcategories of the Framework for Improving Critical Infrastructure Cybersecurity. Each Subcategory is mapped to relevant NIST standards, industry standards, controls, and best practices. We did not observe any example solution security characteristics that mapped to Respond or Recover Subcategories.

Table 3-1 Security Characteristics and Controls Mapping – NIST Cybersecurity Framework

Cybersecurity Framework Function	Cybersecurity Framework Subcategory	NIST SP 800-53 R4[a]	ISO/IEC 27001[b]	CIS CSC[c]	NERC CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried.	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-010-2
	ID.AM-2: Software platforms and applications within the organization are inventoried.	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected.	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6 CIP-007-6
	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
	PR.IP-1: A baseline configuration of information technology/industrial	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10	A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	CSC-3 CSC-10	CIP-010-2

Cybersecurity Framework Function	Cybersecurity Framework Subcategory	NIST SP 800-53 R4[a]	ISO/IEC 27001[b]	CIS CSC[c]	NERC CIP v5[d]
	control systems is created and maintained.				
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	AU family	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	CSC-6	CIP-006-6 CIP-007-6
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	AC-4, CA-3, CM-2, SI-4			CIP-010-2
	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6
	DE.AE-4: Impact of events is determined.	CP-2, IR-4, RA-3, SI-4			CIP-008-5
	DE.AE-5: Incident alert thresholds are established.	IR-4, IR-5, IR-8			CIP-008-5

Cybersecurity Framework Function	Cybersecurity Framework Subcategory	NIST SP 800-53 R4[a]	ISO/IEC 27001[b]	CIS CSC[c]	NERC CIP v5[d]
	DE.CM-1: The network is monitored to detect potential cybersecurity events.	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4			CIP-005-5 CIP-007-6
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	CA-7, PE-3, PE-6, PE-20			CIP-006-6
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	A.12.4.1		CIP-006-6
	DE.CM-4: Malicious code is detected.	SI-3	A.12.2.1	CSC-5	CIP-007-6 CIP-005-5
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4			CIP-005-5 CIP-007-6 CIP-006-6

3.5 Technologies

Table 3-2 lists all of the technologies used in this project and provides a mapping between the generic application term, the specific product used, and the security control(s) that the product provides in the example solution. Table 3-2 describes only the functions and Cybersecurity Framework Subcategories implemented in the example solution. Products may have functionality not described in the table. Refer to Table 3-1 for an explanation of the Cybersecurity Framework Subcategory codes.

Table 3-2 Products and Technologies

Component	Product	Function	Cybersecurity Framework Subcategories
SIEM	Hewlett Packard Enterprise (HPE) ArcSight *Please note: HPE in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.*	▪ aggregates all IT, Windows, OT (ICS), and physical access monitoring, event, and log data collected by the reference design ▪ acts as a data normalization and correlation point and enables queries to be developed and executed to detect potential security incidents ▪ serves as the central location at which the analyst can access all data collected	DE.AE-3, DE.AE-5 Related Subcategories: PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-7

Component	Product	Function	Cybersecurity Framework Subcategories
Network Tap	IXIA TP-CU3 Tap	▪ collects data from specific locations on the ICS network and sends it to the monitoring server via the ICS firewall ▪ The taps are passive, so if they lose power or otherwise fail, they will not adversely affect the ICS network. ▪ collects data via monitor ports that are inherently unidirectional (and so do not pose any threat of information leaking from the tap onto the ICS network)	DE.CM-1
Log Collector/ Aggregator	TDi Technologies ConsoleWorks	▪ collects and aggregates logs ▪ adds a time stamp and integrity seals the log entries ▪ Log collection in the operations facility protects against potential data loss if the communication channel between the operations and enterprise facilities fails. ▪ aggregates the log entries of all monitoring components at the operations log collector; aggregator ensures that this log data gets buffered in the operations facility and can be transferred later in the event that network connectivity to the enterprise network is lost	PR.DS-6, PR.DS-6, PR.PT-1, DE.AE-3

Component	Product	Function	Cybersecurity Framework Subcategories
ICS Asset Management System	Dragos Security CyberLens	- monitors ICS traffic and maintains a database of all ICS assets of which it is aware - This enables it to detect new ICS devices, ICS devices that disappear, and changes to known ICS devices.	ID.AM-1
Network Visualization Tool	Dragos Security CyberLens	- displays a depiction of network devices, connectivity, and traffic flows	Does not directly support a Cybersecurity Framework Subcategory. Related Subcategory: ID.AM-3
Physical Access Control System	RS2 AccessIT!	- controls user access to doors - detects and reports door open/close events and user identity	PR.AC-2
Physical Access Sensor	RS2 door controller	- senses door close/open events - generates alerts when door open and close events occur	DE.CM-2
ICS Network Intrusion Detection System (IDS)	Radiflow iSIM	- identifies monitors, and reports anomalous ICS traffic that might indicate a potential intrusion	DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-7

Component	Product	Function	Cybersecurity Framework Subcategories
Historian	OSIsoft Pi Historian	- serves as a data repository that essentially replicates the database of collected ICS values on the ICS network’s historian - can be configured to generate alerts when changes to certain ICS process values occur	Does not support a Cybersecurity Framework Subcategory in and of itself. It provides the data to be monitored by the ICS behavior monitor (next item). Related Subcategories: DE.AE-5, DE.CM-1
ICS Behavior Monitor	ICS2 On-Guard	- monitors ICS process variable values in the historian to assess application behavior, detect process anomalies, and generate alerts	DE.AE-5, DE.CM-1
Application Monitor and Protection	Waratek Runtime Protection	- monitors and protects a running application, analyzes the data it collects, and detects and reports unusual application behavior, e.g., it might generate an alert if it detects a potential SQLi attack against the SIEM	DE.AE-2, DE.AE-4, DE.AE-5, DE.CM-4
Analysis Workflow Engine	RSA NetWitness SecOps Manager	- automates workflow associated with review and analysis of data that has been collected at the SIEM - enables orchestration of various analytic engines	DE.AE-2

Component	Product	Function	Cybersecurity Framework Subcategories
Unidirectional Gateway	Waterfall unidirectional security gateway	▪ allows data to flow in only one direction	PR.AC-5, PR.PT-4
Visualization Tool	RSA SecOps	▪ provides data reduction and a dashboard capability for the data in the SIEM, as well as risk analysis	This component does not support a Cybersecurity Framework Subcategory in and of itself. Related Subcategory: ID.AM-3
Electronic Access Control and Monitoring Systems (EACMS)	TDi Technologies ConsoleWorks	▪ authenticates system managers ▪ provides role-based access control of system management functions ▪ implements a “protocol break” between the system manager and the managed assets ▪ records all system management actions	PR.AC-3, PR.AC-4, PR.MA-2, PR.PT-1, PR.PT-3, DE.CM-3
	Siemens RUGGEDCOM CROSSBOW	▪ authenticates system managers ▪ provides role-based access control of system management functions ▪ implements a “protocol break” between the system manager and the managed assets ▪ records all system management actions	PR.AC-3, PR.AC-4, PR.MA-2, PR.PT-1, PR.PT-3, DE.CM-3

Component	Product	Function	Cybersecurity Framework Subcategories
	Waterfall Secure Bypass	- provides time-limited network connectivity to perform system management functions	PR.AC-5, PR.PT-4
	Schneider Electric Tofino Firewall	- controls network connectivity for performing system management functions	PR.AC-5, PR.PT-4

3.6 Situational Awareness Test Cases

Table 3-3 provides a high-level view of the test cases used to conduct the functional evaluation of the SA use case. Details of the functional evaluation are provided in Section 6.

Table 3-3 Situational Awareness Test Cases

Test Case	Purpose	Operational Description	Events	Desired Outcome
SA-1: Event Correlation for OT and PACS	This test case focuses on the possibility of correlated events involving OT and PACS that might indicate compromised access.	This test case considers the correlation of events from two silos, which indicates a potential security issue to the SIEM. A technician entering a substation is inconsequential and expected behavior. However, if a device goes down and triggers alarms within a certain time frame, there is a possible correlation of these two events. It should not	- technician accesses sub-station/control station - OT device goes down	alert of anomalous condition that correlates to a physical and ICS network event

Test Case	Purpose	Operational Description	Events	Desired Outcome
		automatically be assumed that malicious behavior is the cause. There might be scheduled maintenance to be performed on a certain device, which would be a perfectly reasonable explanation for this test case. The key here is the correlation of the activity, which provides an indicator that could narrow possibilities and start an investigation into the activity more quickly than having an analyst looking at individual events and attempting to correlate them manually. To learn more about the data fields used to create the alert, see Section 3.2.1 of NIST SP 1800-7C, Test Cases.		
SA-2: Event Correlation — OT and IT	SQLi injection detection	This test case demonstrates how SQLi can be detected. In this instance, the baseline assumption is that applications in the IT (corporate/enterprise) network can conduct limited communication with some devices in the OT network to generate information needed by corporate operations on usage, billing, accounting, or some other type of business information. This is a common scenario — typically a specific historian would be dedicated for	detection of SQLi on IT device interconnected with OT device	alert sent to SIEM on multiple SQLi attempts

Test Case	Purpose	Operational Description	Events	Desired Outcome
		this purpose, perhaps in a network demilitarized zone. This scenario is definitely preferable, but there are too many variations in networks to account for all of them. The example we provide is focused on detecting SQLi, specifically directed at OT devices or devices connected to OT devices. To learn more about the data fields used to create the alert, see Section 3.2.1 of NIST SP 1800-7C, Test Cases.		
SA-3: Event Correlation mat OT and IT/PACS-OT	Unauthorized access attempts detected and alerts triggered based on connection requests from a device on the Supervisory Control and Data Acquisition (SCADA) network destined for an internet protocol (IP) that is outside of the SCADA IP range. This test case focuses on the possibility of a malicious actor	Unauthorized access attempts can be made in numerous ways. For test case 3, we demonstrate an alerting capability that triggers when an ICS device located on the OT network attempts to communicate with an IT device outside the authorized parameters. A key assumption here is that proper security measures have been instituted on the OT network to detect and alert for false connection requests. This scenario can also be correlated with PACS and OT, where numerous failed login attempts on a particular device trigger alerts to the SIEM. Because the connection attempt starts within the OT network, one must first investigate internally to	inbound/outbound connection attempts from devices outside authorized and known inventory	alert to SIEM showing IP of unidentified host attempting to connect or identified host attempting to connect to unidentified host

Test Case	Purpose	Operational Description	Events	Desired Outcome
	attempting to gain access to an OT device via the enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.	determine the location of the device and who had access to the location where all of this activity occurred. To learn more about the data fields used to create the alert, see Section 3.2.1 of NIST SP 1800-7C, Test Cases.		
SA-4: Data Infiltration Attempts	Examine behavior of systems; configure SIEM to alert on behavior that is outside the normal baseline. Alerts can be created emanating from OT, IT, and PACS. This test case seeks	Baselining the proper operations and communications of an OT network is essential to detecting behavioral anomalies. Inserting security capabilities to confirm the normal operation of the OT network and alert to the detection of anomalous behavior provides an essential SA capability to the operator. Anomalous behavior can include any type of security or operational issue that falls outside	anomalous behavior falling outside defined baseline	alert sent to SIEM on any event falling outside what is considered normal activity based on historical data

Test Case	Purpose	Operational Description	Events	Desired Outcome
	alerting based on behavioral anomalies rather than recognition of IP addresses, and it guards against anomalous or malicious inputs.	predefined thresholds. Here, we seek to focus specifically on anomalous behavior as it relates to data changes in the ICS protocols that could indicate a security concern, whether it is data infiltration (rogue data inputs and/or malicious data manipulation) or some other variance that falls outside what is considered to be the normal baseline. To learn more about the data fields used to create the alert, see Section 3.2.1 of NIST SP 1800-7C, Test Cases.		
SA-5: Configuration Management	Unauthorized (inadvertent or malicious) upload of an ICS network device configuration. Alert will be created to notify SIEM this has occurred. Detection method will be based primarily on inherent device capability (i.e. log files).	For this test case, we focused on unauthorized loading of a new configuration on a networking or security device in the ICS network. If a firewall, switch, or router configuration change is made, the SA solution can detect the change and send an alert to the SIEM. The SIEM provides awareness of these changes to those concerned with the security of the OT network and devices. Once those concerned have the information, they can determine whether the change was authorized. Malicious changes to the OT network or devices, if undetected, can pave the way for numerous exploits and	configuration change on Tofino FW, Cisco 2950	alert will be created to notify SIEM this has occurred

Test Case	Purpose	Operational Description	Events	Desired Outcome
		reintroduce significant risk to the OT network. To learn more about the data fields used to create the alert, see Section 3.2.1 of NIST SP 1800-7C, Test Cases.		
SA-6: Rogue Device Detection	Alerts are triggered by the introduction of any device onto the ICS network that has not been registered with the asset management capability in the build.	A primary concern of ICS owners and operators is the introduction of unauthorized devices onto the OT network. This test case focuses on the introduction of a device that has not been previously registered to the asset management tool. This test case assumes the absolute necessity of having an ICS asset management tool in place, and properly maintaining inventory throughout the life cycle of all the devices. It is essential that this be in place, as determining the difference between authorized and unauthorized devices will be extremely difficult without one. To learn more about the data fields used to create the alert, see Section 3.2.1 of NIST SP 1800-7C, Test Cases.	unidentified device appears on ICS network	alert will be created to notify SIEM that this has occurred

4 Architecture

“Cyber situational awareness involves the normalization, de-confliction, and correlation of disparate sensor data and the ability to analyze data and display the results of these analyses” [3]. This guide presents an architecture for instrumenting the ICS network of a utility’s OT silo with sensors to collect cyber events. These events are then sent to a SIEM system where they are normalized and correlated with cyber events from the IT silo and physical access events. Once collected in the SIEM, events from all three silos can be analyzed to provide a converged picture of the cyber situation. Relevant information from this converged picture can then be provided to OT, IT, and physical security personnel.

This section describes both an example solution for providing converged situational awareness across OT, IT, and physical security and a prototype implementation or “lab build” of the example solution constructed by the NCCoE to validate the example solution.

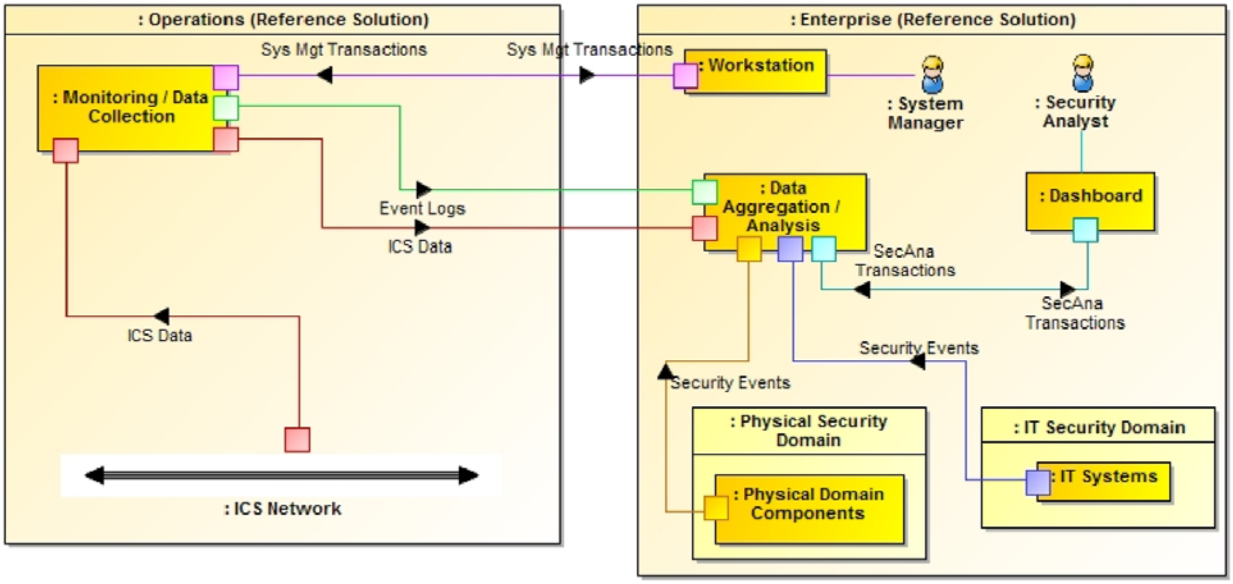
- Section 4.1, Architecture Description, describes the logical components that make up the example solution.
- Section 4.2, Example Solution Monitoring, Data Collection, and Analysis, provides details of the components used to monitor and collect data from operations, transmit the data to the enterprise services, and analyze the collected data to identify events of interest and detect potential cyber incidents.
    - Section 4.2.1, Example Solution Monitoring and Data Collection Lab Build, describes the lab prototype of the monitoring and data collection portion of the example solution.
    - Section 4.2.2, Example Solution Data Aggregation and Analysis Lab Build, describes the lab prototype of the data aggregation and analysis portion of the example solution.
- Section 4.3, Example Solution Remote Management Connection, provides details of the components that compose the on-demand limited-access remote management connection.
    - Section 4.3.1, Example Solution Operations Remote Management Lab Build, describes the lab prototype of remote management for operations facilities.
    - Section 4.3.2, Example Solution Enterprise Remote Management Lab Build, describes the lab prototype of remote management for enterprise services.

4.1 Architecture Description

A high-level view of the example solution is depicted in Figure 4-1. The solution consists of a monitoring/data collection component, which is deployed to operations facilities such as substations and generating plants; and a data aggregation/analysis component that is deployed as a single service for the enterprise. Data is collected from the ICS network by the monitoring/data collection component and sent to the data aggregation/analysis component. To protect the ICS network and the operations facility, the flow of data is restricted to be unidirectional out of operations and into the enterprise services.

At the enterprise data aggregation/analysis component, data from the ICS network is combined with data from physical security monitoring and business systems monitoring. Combining monitoring data from operations, physical security, and business systems is the basis for providing comprehensive cyber situational awareness.

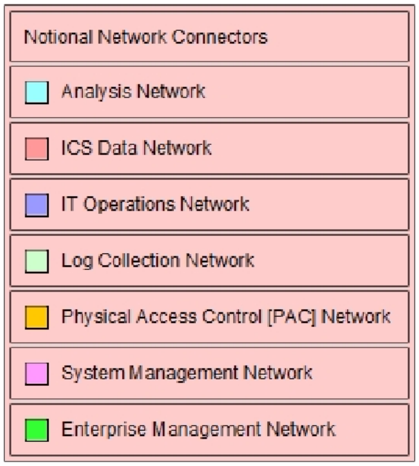
Figure 4-1 High-Level Example Solution Architecture



In addition to the unidirectional flow of monitoring data out of operations, an on-demand, limited-access bidirectional system management connection is provided from the enterprise to each operations facility. This connection provides remote access to manage the software that monitors the ICS network and operations components.

Figure 4-2 provides a color-coded legend identifying the different types of network connections portrayed in diagrams throughout Section 5.

Figure 4-2 Network Connections Color Code



Notional Network Connectors
🟦 Analysis Network
🟥 ICS Data Network
🟪 IT Operations Network
🟩 Log Collection Network
🟧 Physical Access Control [PAC] Network
🟪 System Management Network
🟩 Enterprise Management Network

- Analysis network – connects situational awareness analysis functions
- ICS Data Network – connects ICS monitoring functions
- IT Operations Network – connects IT business systems
- Log Collection Network – connects log collection and aggregation functions
- PAC Network – connects physical access control functions
- System Management Network – provides system managers with remote access to ICS monitoring functions
- Enterprise Management Network – provides vendor with remote access to the NCCoE energy sector lab

4.2 Example Solution Monitoring, Data Collection, and Analysis

Figure 4-3 depicts the monitoring and data collection components deployed in operations and the data aggregation and analysis components deployed as enterprise services. Operations has five main sources of monitoring information:

- ICS Asset Management System – monitors the ICS network to identify the devices connected to and communicating over the network. It sends an event to the enterprise SIEM system when a new device is identified on the ICS network or if a known device disappears from the network.
- ICS Network IDS – monitors ICS network traffic for traffic that matches a signature of known suspicious activity. When suspicious activity is detected, an event is sent to the enterprise SIEM.

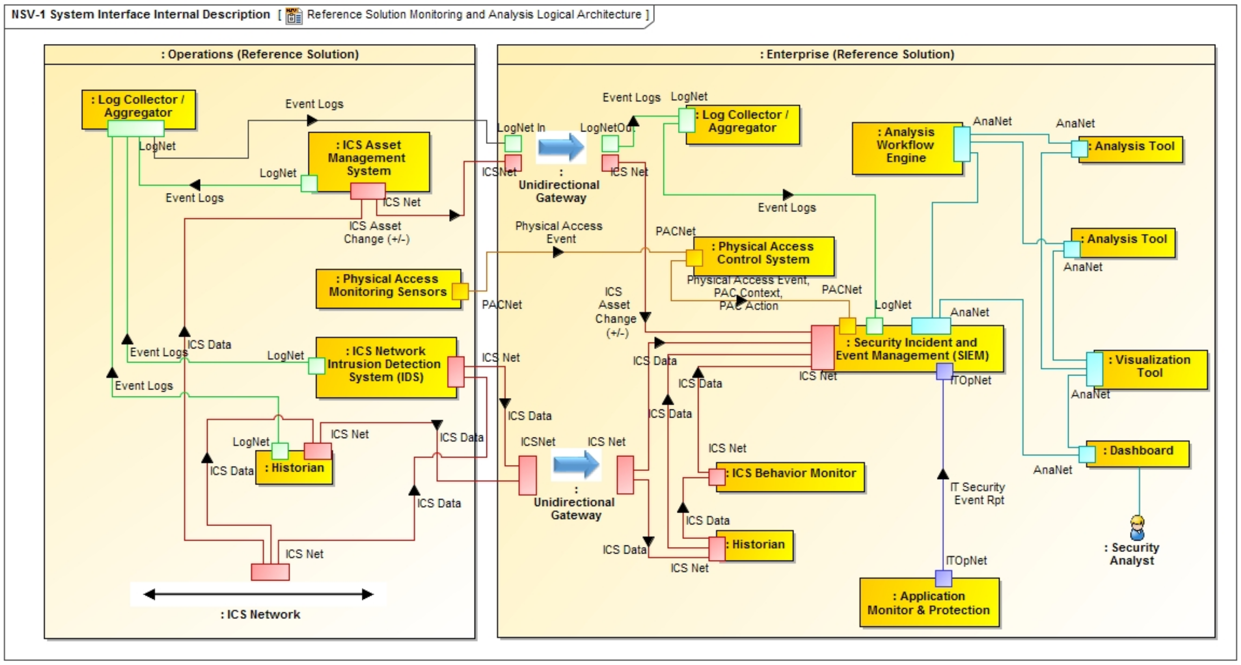
- Historian – collects parameter values from the ICSs in operations and replicates them to a second historian in enterprise. The operations historian is assumed to be an existing ICS component.
- Log Collector/Aggregator – collects log data from all of the other monitoring components in operations, stores them locally, and replicates the log data to another log collector aggregator in enterprise. Logs are captured and stored locally to prevent loss of log data should communication between operations and enterprise be disrupted.
- Physical Access Monitoring Sensors – monitor physical access to the operations facility. They detect events such as doors opening or closing and report those events to the PACS in enterprise.

A unidirectional gateway connects monitoring functions in operations to analysis functions in enterprise. This ensures that data flows in only one direction: out of operations.

Enterprise contains the following components:

- Log Collector/Aggregator – receives log data from the operations facilities and sends it to the SIEM.
- PACS – monitors physical access to all facilities and generates events to the SIEM when physical access occurs, such as doors or windows being opened and closed.

Figure 4-3 Monitoring, Data Collection, and Analysis Example Solution



- Historian –receives replicated ICS data from the operations historian.

- ICS Behavior Monitor –compares ICS data from the historian with expected values based on normal operations. It sends events to the SIEM when ICS data deviates from normal behavior on a particular ICS network.
- Application Monitor and Protection –monitors IT applications for suspicious behavior and sends events to the SIEM.
- SIEM system –receives and stores events from sensors, normalizes the data, correlates events from multiple sensors, and generates alerts.
- Analysis Workflow Engine – to the extent feasible, automates execution of courses of action related to events collected in the SIEM.
- Analysis Tools –implement algorithms that examine data from the SIEM to identify events of interest and potential cyber incidents. These components report this information to security analysts via the visualization tool.
- Visualization Tool –provides alerts and other cyber SA information to security analysts and allows them to examine the underlying data that leads to an alert.

Enterprise components serve one of two primary responsibilities: collect event data from operations into a common repository, the SIEM; or analyze data in the SIEM to detect suspicious events and potential cyber incidents.

A data diode is used to ensure that the data flows from the components in operations that monitor the ICS network are one-way data flows from operations to enterprise.

4.2.1 Example Solution Monitoring and Data Collection Lab Build

Figure 4-4 shows the products used to build an instance of the monitoring and data collection portion of the example solution. The instance was constructed at the University of Maryland's (UMD's) power cogeneration plant. As a result of this collaboration with UMD, the NCCoE was able to utilize real grid data and process it through our build collaborator's security devices and applications. Though this certainly added to the complexity of the build, we believe that using UMD's grid data provides a real-life implementation of ICS network security solutions that can be replicated at other utilities.

The NCCoE energy sector lab provides the enterprise facility described in the example solution. A virtual private network (VPN) is used in the lab build to protect data in transit between the operations facility and the enterprise facility. The VPN was established by using a Siemens RUGGEDCOM RX1501 (O1) at the cogeneration facility and a Siemens RUGGEDCOM RX1400 at the NCCoE. The RX1501 includes firewall capabilities to control which TCP ports are available to communicate with the NCCoE.

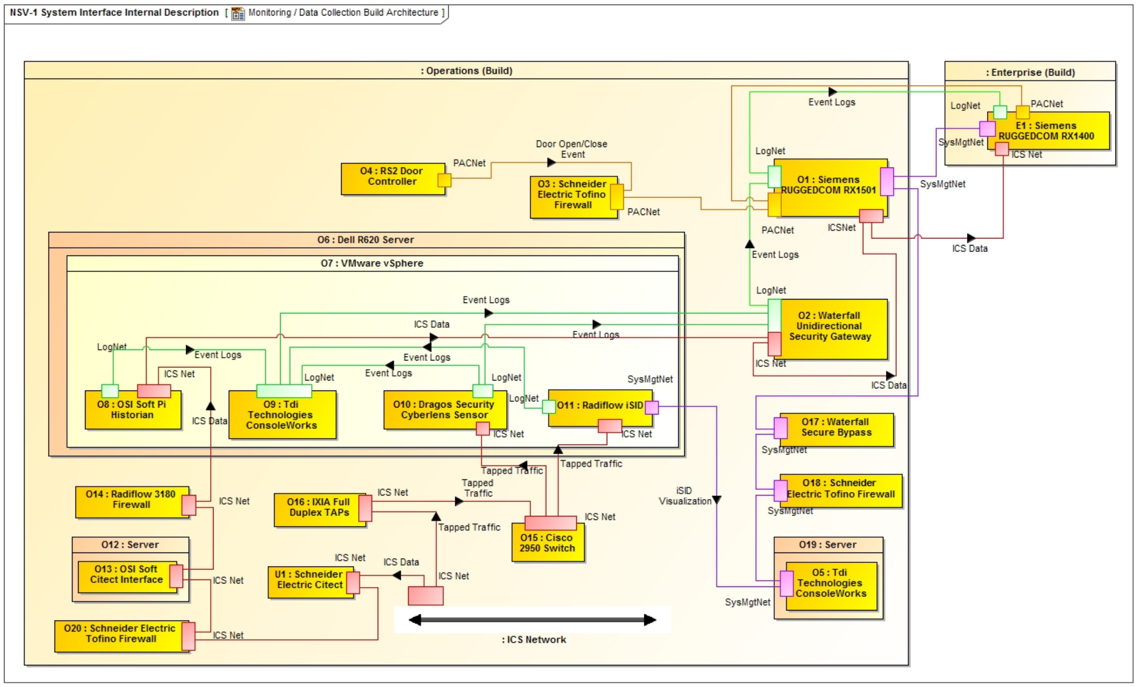
When implementing the example solution, utilities need to consider the type of network connection in place between operations and enterprise to determine what protection might be needed for data in transit.

The physical access sensor in the example solution is provided by an RS2 door controller (O4). The controller monitors a door open/close switch and sends events whenever the door at the facility is opened or closed. This information is sent over the build collaborator's enterprise network. To prevent unintended interactions between the collaborator's enterprise network and the NCCoE energy sector lab, a Schneider Electric Tofino Firewall (O3) is installed between the collaborator's enterprise network and the VPN.

A Dell R620 server (O6) running VMware (O7) was deployed to the cogeneration facility to host **monitoring and data collection software.** These are infrastructure components needed for the lab build but not considered critical to the example solution, as server types and VMware versions will vary depending on the implementation.

The historian in the example solution was implemented by an OSIsoft Pi Historian (O8) installed on the Dell server (O6). In this case, the historian was not an existing component in the facility. This facility uses a Schneider Electric Citect SCADA system to control operations. ICS data for the facility is collected and stored by this Citect SCADA system. To collect this data, the OSIsoft Citect Interface software (O13) is used to pull data from the Citect SCADA system (U1) and store it in an OSIsoft Pi Historian (O8). To ensure that data flow from the Citect SCADA system (U1) to the OSIsoft Pi Historian (O8) is unidirectional, the Citect Interface software (O13) is installed on a dedicated physical server (O12), isolated from the Citect SCADA system by a Schneider Electric Tofino Firewall (O20), and isolated from the Pi Historian (O8) by a Radiflow 3180 firewall (O14). The Pi Historian (O8) replicates data to another Pi Historian in the NCCoE energy sector lab.

Figure 4-4 Operations Monitoring and Data Collection Lab Build Architecture



The ICS Asset Management System in the example solution is implemented by Dragos Security CyberLens. CyberLens is deployed in the cogeneration facility as a sensor (O10), which monitors the ICS network, collects relevant information in files, and transfers the files to a CyberLens server in the NCCoE energy sector lab.

The ICS IDS component in the example solution is provided by Radiflow iSID (O11). Events detected by iSID (O11) are sent via syslog to the log collector/aggregator implemented by TDi Technologies ConsoleWorks (O9). In addition to log data from iSID (O11), ConsoleWorks (O9) also collects log data via syslog from CyberLens Sensor (O10) and the Pi Historian (O8). ConsoleWorks (O9) augments the syslog records with an additional time stamp and an integrity seal. These records are stored in files that are transferred to another instance of ConsoleWorks in the NCCoE energy sector lab.

Both CyberLens Sensor (O10) and iSID (O11) need ICS network data as input. To get this data without affecting the network traffic used to run the cogeneration facility, IXIA full duplex taps (O16) were installed in the ICS network at appropriate points. These taps are designed to ensure that ICS network traffic flow continues even if power to the tap is interrupted. The taps are connected to a Cisco 2950 network switch (O15). The span port of the switch is connected to both CyberLens Sensor (O10) and iSID (O11) to provide the necessary network data. Both the taps (O16) and the span port on the switch (O15) are inherently unidirectional so that ICS network data can flow only out of the ICS network to the data aggregation and analysis tools in the NCCoE energy sector lab. No data can flow back into the ICS network from the monitoring and data collection components.

Data transferred from the Pi Historian (O8), CyberLens Sensor (O10), and ConsoleWorks (O9) to the NCCoE energy sector lab is sent by using a Waterfall Security Solutions, Ltd. Unidirectional Security Gateway (O2). This gateway ensures that data can physically flow only out of the cogeneration facility to the NCCoE and is not physically able to flow back from the NCCoE to the facility.

Radiflow's iSID (O11) has a web interface that is used to both manage the system and provide security analysts with access to additional information about events reported via syslog. Access to this web interface is provided via components (O17, O18, O19, and O5) originally intended for remote management of monitoring and data collection components. These components are described in Section 4.3.1.

4.2.2 Example Solution Data Aggregation and Analysis Lab Build

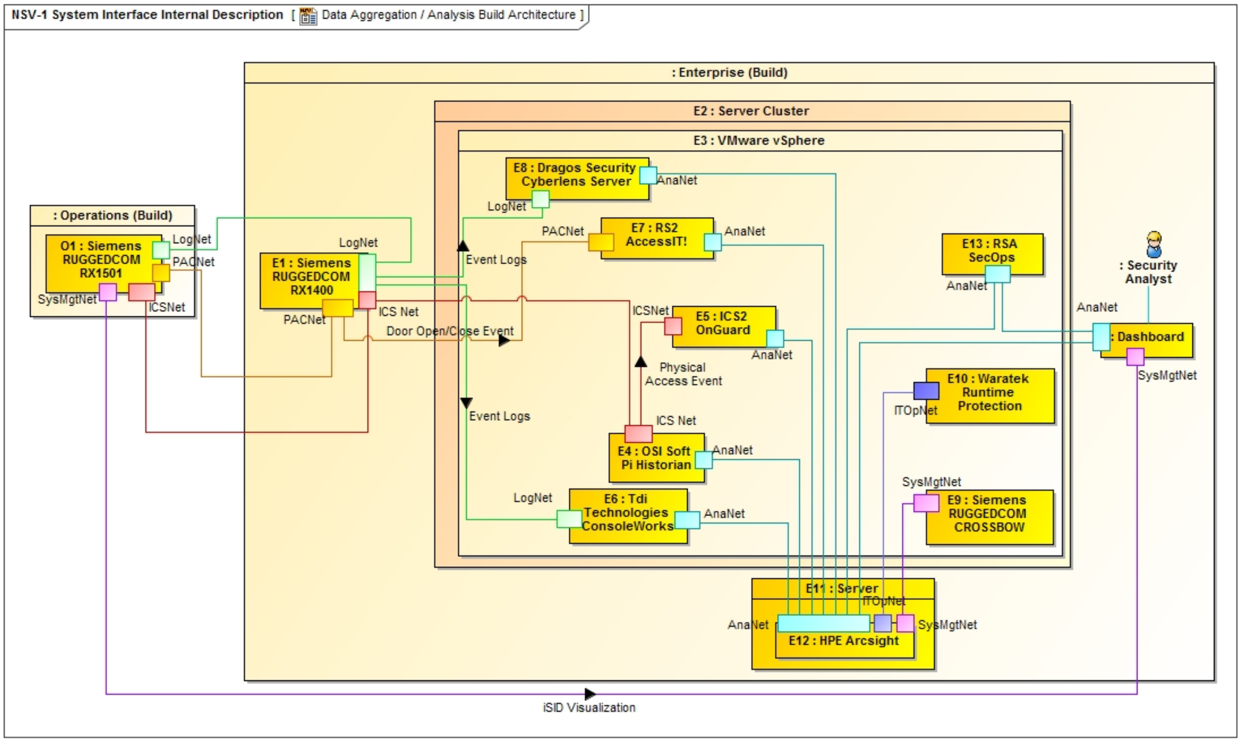
Figure 4-5 shows the products used to build an instance of the data aggregation and analysis portion of the example solution. The instance was constructed in the NCCoE energy sector lab. This lab provides the enterprise environment in the example solution. The VPN between the operations and enterprise in the example solution is provided by a Siemens RUGGEDCOM RX1400 (E1) in the lab and an RX1501 (O1) in the cogeneration facility.

A Dell server cluster (E2) running VMware (E3) is installed in the NCCoE energy sector lab to host monitoring and data aggregation and analysis software. A separate server in the lab (E11) hosts HPE ArcSight. These are infrastructure components needed for the lab build but not considered part of the example solution.

The SIEM in the example solution is provided by HPE ArcSight (E12). ArcSight is the central repository for all events generated.

Waratek Runtime Protection (E10) implements the application monitor and protection component of the example solution. Waratek Runtime Protection monitors and protects Java applications to detect potential cross-site scripting attacks. A Java application was written to access data from the enterprise OSIsoft Pi Historian (E4) database. This application is monitored by Waratek Runtime Protection (E10) and reports and blocks attempted SQL injection attacks against the historian (E4) to ArcSight (E12).

Figure 4-5 Enterprise Data Aggregation and Analysis Lab Build Architecture



The ICS Asset Management System in the operations facilities of the example solution is provided by Dragos Security CyberLens. As implemented, CyberLens is divided into two parts: a sensor (O10) in operations and a server (E8) in enterprise. The sensor (O10) sends data files to the server (E8) for analysis. When the server detects a change to the assets on the ICS network in operations, it sends an event to ArcSight (E12).

The PACS in the example solution is implemented by RS2 AccessIT! (E7). Door open/close events from the RS2 door controller (O4) in operations are sent to AccessIT! (E7) and stored in an internal database. An ArcSight database connector is used to extract these events and send them to ArcSight (E12).

The enterprise historian is provided by the OSIsoft PI Historian (E4). ICS data from the operations Pi Historian (O8) is replicated to the enterprise PI Historian (E4). This data is used by the ICS behavioral monitoring component in the example solution, implemented by ICS2 OnGuard (E5), to detect unusual ICS behavior. OnGuard (E5) reports this unusual behavior to ArcSight (E12).

The enterprise log collector/aggregator component in the example solution is provided by TDi Technologies ConsoleWorks (E6). This instance of ConsoleWorks (E6) receives files from the operations instance (O9). The files contain integrity-sealed syslog records. The enterprise instance of ConsoleWorks (E6) verifies the integrity seal on the records and sends the syslog records to ArcSight (E12).

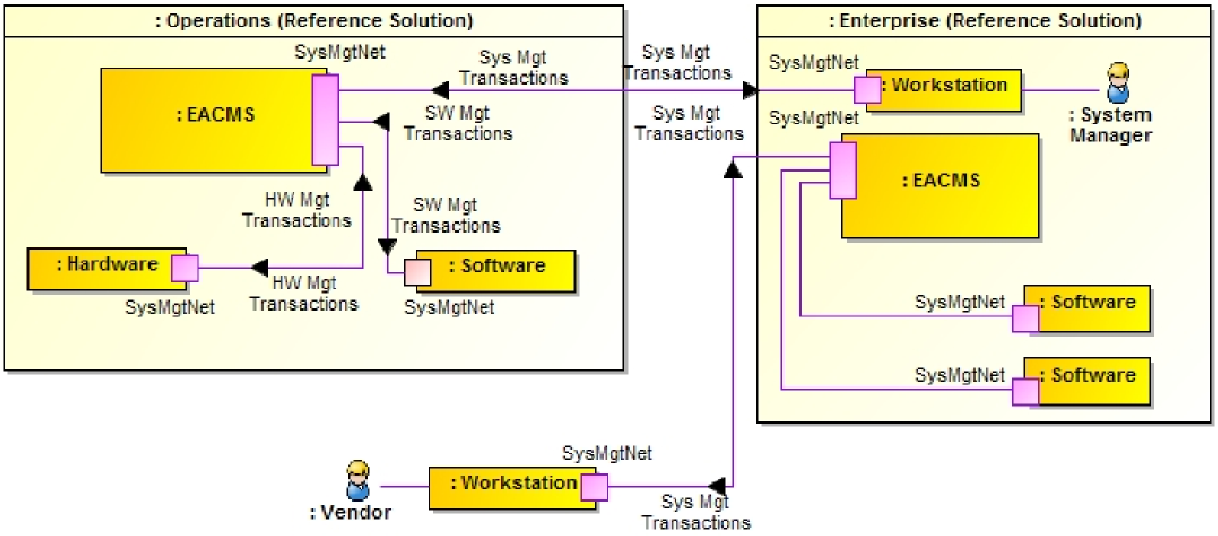
Siemens RUGGEDCOM CROSSBOW (E9), which implements part of the remote management connection described in Section 5.3, sends log information about remote management actions to ArcSight (E12).

The analysis workflow engine, analysis tools, and visualization tools in the example solution are implemented by RSA SecOps (E13). This product extracts event data from ArcSight (E12) and performs analyses to identify potential cyber incidents.

4.3 Example Solution Remote Management Connection

Because elements of the example solution are separated from the system managers who install, configure, and manage them, a remote management connection is needed from the enterprise to operations. Additionally, while not part of the example solution, the vendors who collaborated with the NCCoE to construct the lab build of the example solution need remote access to the NCCoE energy sector lab to install, configure, and integrate their products. Figure 4-6 depicts the example solution for both remote management connections. Example implementation of remote management is depicted in Figure 4-7 and Figure 4-8.

Figure 4-6 Remote Management Example Solution



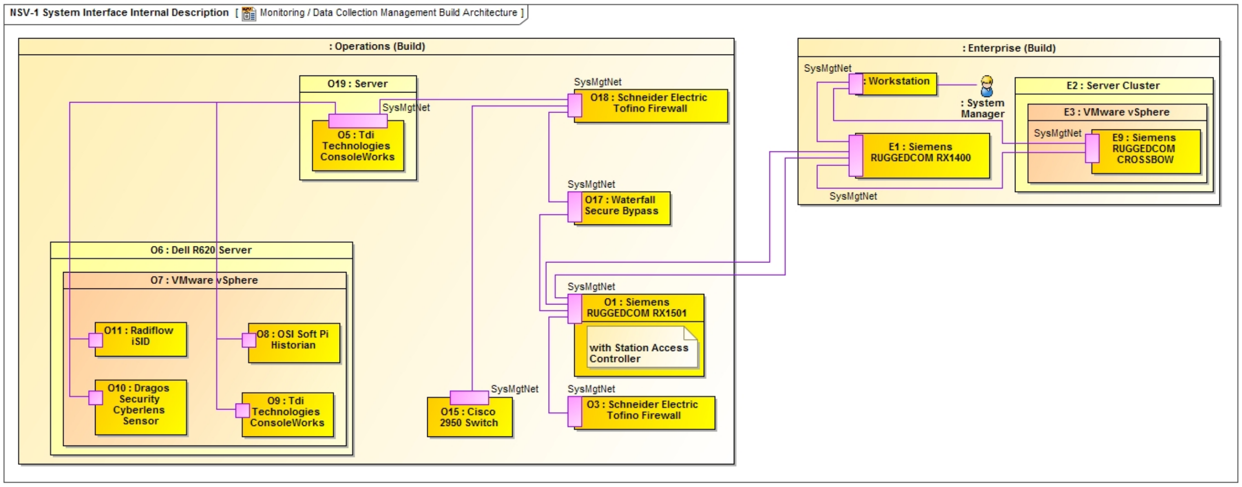
A workstation in the enterprise facility connects to the operations EACMS. The system manager authenticates to the EACMS and controls the system manager's access to hardware or software within operations, as a privileged user, to perform system management functions. A VPN is used to protect data in transit between operations and enterprise. In the lab build, the connection between operations and enterprise uses the public internet. Hence, protection for data transiting the internet is needed. When implementing the example solution, utilities need to consider the type of network connection in place between operations and enterprise to determine what protection might be needed for data in transit.

To install and manage their software in enterprise, vendors connect via VPN to an EACMS in enterprise. The vendors authenticate to the EACMS and are granted access to the software they provided.

4.3.1 Example Solution Operations Remote Management Lab Build

The lab build of operations remote management, depicted in Figure 4-7, provides two distinct implementations of the EACMS. One implementation, which provides remote management for software running on the Dell R620 server (O6), uses the Siemens RUGGEDCOM RX1501 (O1), the Waterfall Secure Bypass switch (O17), a Schneider Electric Tofino Firewall (O18), a Linux server (O19), and an instance of TDi Technologies ConsoleWorks (O5). The second implementation, which provides remote management for hardware in operations, uses Siemens RUGGEDCOM CROSSBOW (E9) and the Station Access Controller capability in the Siemens RUGGEDCOM RX1501 (O1). While the build used each implementation for a specific set of resources, either hardware or software, each implementation can manage both hardware and software.

Figure 4-7 Operations Remote Management Lab Build Architecture


NSV-1 System Interface Internal Description [Monitoring / Data Collection Management Build Architecture]
: Operations (Build)
O19 : Server
SysMgtNet
O5 : Tdi Technologies ConsoleWorks
SysMgtNet
O18 : Schneider Electric Tofino Firewall
SysMgtNet
O17 : Waterfall Secure Bypass
O6 : Dell R620 Server
O7 : VMware vSphere
O11 : Radiflow iSID
O8 : OSI Soft Pi Historian
O10 : Dragos Security Cyberlens Sensor
O9 : Tdi Technologies ConsoleWorks
SysMgtNet
O1 : Siemens RUGGEDCOM RX1501
with Station Access Controller
SysMgtNet
O15 : Cisco 2950 Switch
SysMgtNet
O3 : Schneider Electric Tofino Firewall
: Enterprise (Build)
SysMgtNet
: Workstation
: System Manager
E2 : Server Cluster
E3 : VMware vSphere
SysMgtNet
E9 : Siemens RUGGEDCOM CROSSBOW
E1 : Siemens RUGGEDCOM RX1400
SysMgtNet

The EACMS implementation for remote management of software in operations has the system manager connect to operations from enterprise over the VPN created by using the Siemens RUGGEDCOM RX1400 (E1) and RX1501 (O1). The system manager needs to connect to the operations management instance of ConsoleWorks (O5) for role-based access control, logging, auditing, and alerts. However, a Waterfall Secure Bypass (O17) is installed in the network path from the RX1501 to the ConsoleWorks (O5). The Secure Bypass (O17) is a normally open physical switch. To manage remotely, a person in the operations facility must turn a key on the Secure Bypass (O17) to close the switch. In this lab build, the collaborator's cogeneration facility representing operations is a staffed facility, so an operator is available to close the switch on the Secure Bypass (O17). Once the switch is closed, a timer is activated that automatically opens the switch after a preset time period. Remote management can be performed only if the personnel at the operations facility agree to allow access.

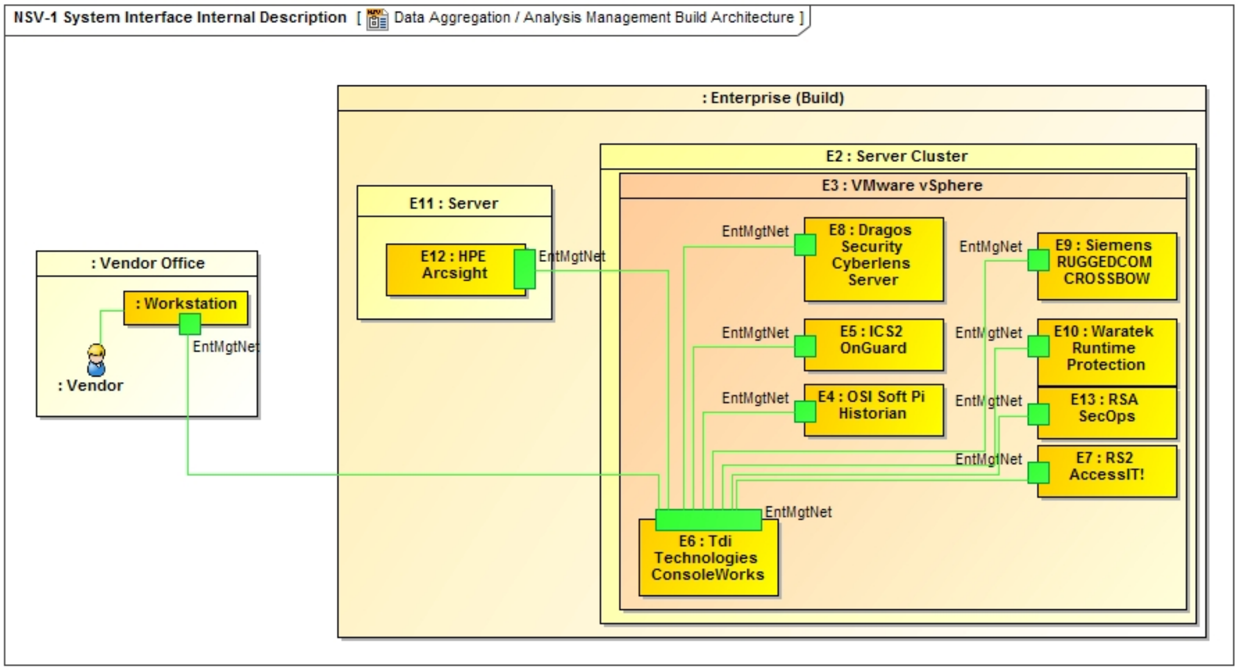
A Schneider Electric Tofino Firewall (O18) restricts the protocols that can be used to connect to the operations management instance of ConsoleWorks (O5). Once connected to O5, the system manager authenticates to ConsoleWorks, which controls privileged user access to virtual machines on the Dell server (O6). ConsoleWorks records all privileged user actions.

To remotely manage hardware in operations, the system manager authenticates to Siemens RUGGEDCOM CROSSBOW (E9) in enterprise. CROSSBOW (E9) determines the resources that the system manager is allowed to access and then makes a connection over the VPN to the resource in the RX1501 (O1). In the lab build, the Tofino Firewall (O3) isolating the door controller is connected directly to the network switch in the RX1501 (O1), and no operations personnel action is needed to manage the firewall. To manage the Cisco 2950 network switch that connects ICS network taps (O15) to CyberLens Sensor (O10) and iSID (O11), operations personnel must close the switch on the Secure Bypass (O17).

4.3.2 Example Solution Enterprise Remote Management Lab Build

Figure 4-8 depicts implementation of remote access to the NCCoE energy sector lab for vendors.

Figure 4-8 Enterprise Remote Management Lab Build Architecture


NSV-1 System Interface Internal Description [Data Aggregation / Analysis Management Build Architecture]
: Enterprise (Build)
E2 : Server Cluster
E3 : VMware vSphere
E11 : Server
E12 : HPE Arcsight
EntMgtNet
: Vendor Office
: Workstation
EntMgtNet
: Vendor
EntMgtNet
E8 : Dragos Security Cyberlens Server
EntMgNet
E9 : Siemens RUGGEDCOM CROSSBOW
EntMgtNet
E5 : ICS2 OnGuard
EntMgtNet
E10 : Waratek Runtime Protection
EntMgtNet
E4 : OSI Soft Pi Historian
EntMgtNet
E13 : RSA SecOps
EntMgtNet
E7 : RS2 AccessIT!
EntMgtNet
E6 : Tdi Technologies ConsoleWorks

The VPN providing vendor connectivity to the enterprise in the example solution is provided as core lab infrastructure by the NCCoE and is outside the scope of the lab build. Use of this VPN requires two-factor authentication.

The EACMS for vendor access in the example solution is implemented by TDi Technologies ConsoleWorks (E6). Vendors authenticate to ConsoleWorks and are allowed to connect to the virtual machines or physical server hosting their product(s). Additionally, ConsoleWorks records all the actions performed over a connection. This provides an audit trail that documents vendor activity, which can be used for accountability as well as constructing the how-to portion, volume C, of this practice guide.

5 Security Characteristic Analysis

We organized the security evaluation of the SA reference design into two parts. Section 5.1, Analysis of the Reference Design's Support for Cybersecurity Framework Subcategories, analyzes the SA reference design in terms of the specific Subcategories of the Cybersecurity Framework [4] that it supports. It identifies the security benefits provided by each of the reference design components and how the reference design supports specific cybersecurity activities, as specified in terms of Cybersecurity Framework Subcategories.

Section 5.2, Analysis of Reference Design Security, discusses potential new vulnerabilities and attack vectors that the reference design, or the infrastructure needed to manage the reference design, might introduce, as well as ways to mitigate those vulnerabilities. Overall, the purpose of the security characteristics analysis is to identify the security benefits provided by the reference design and how they map to Cybersecurity Framework Subcategories, as well as to understand the mitigating steps to secure the reference design against potential new vulnerabilities.

5.1 Analysis of the Reference Design's Support for Cybersecurity Framework Subcategories

Table 5-1, SA Reference Design Components and the Cybersecurity Framework Subcategories that They Support, lists numerous reference design components, their functions, and the Cybersecurity Framework Subcategories that they support. Although the particular products that were used to instantiate each component in the build are also listed, the focus of the security evaluation is the Cybersecurity Framework Subcategories supported by these products. This evaluation does not concern itself with specific products or their capabilities. In theory, any number of commercially available products could be substituted to provide the security capabilities of a given reference design component. Figure 5-1 and Figure 5-2 depict the monitoring/data collection and data aggregation/analysis subarchitectures of the reference design by using the generic names of each component.

Figure 5-1 Monitoring/Data Collection Subarchitecture Depicted with Generic Component Names

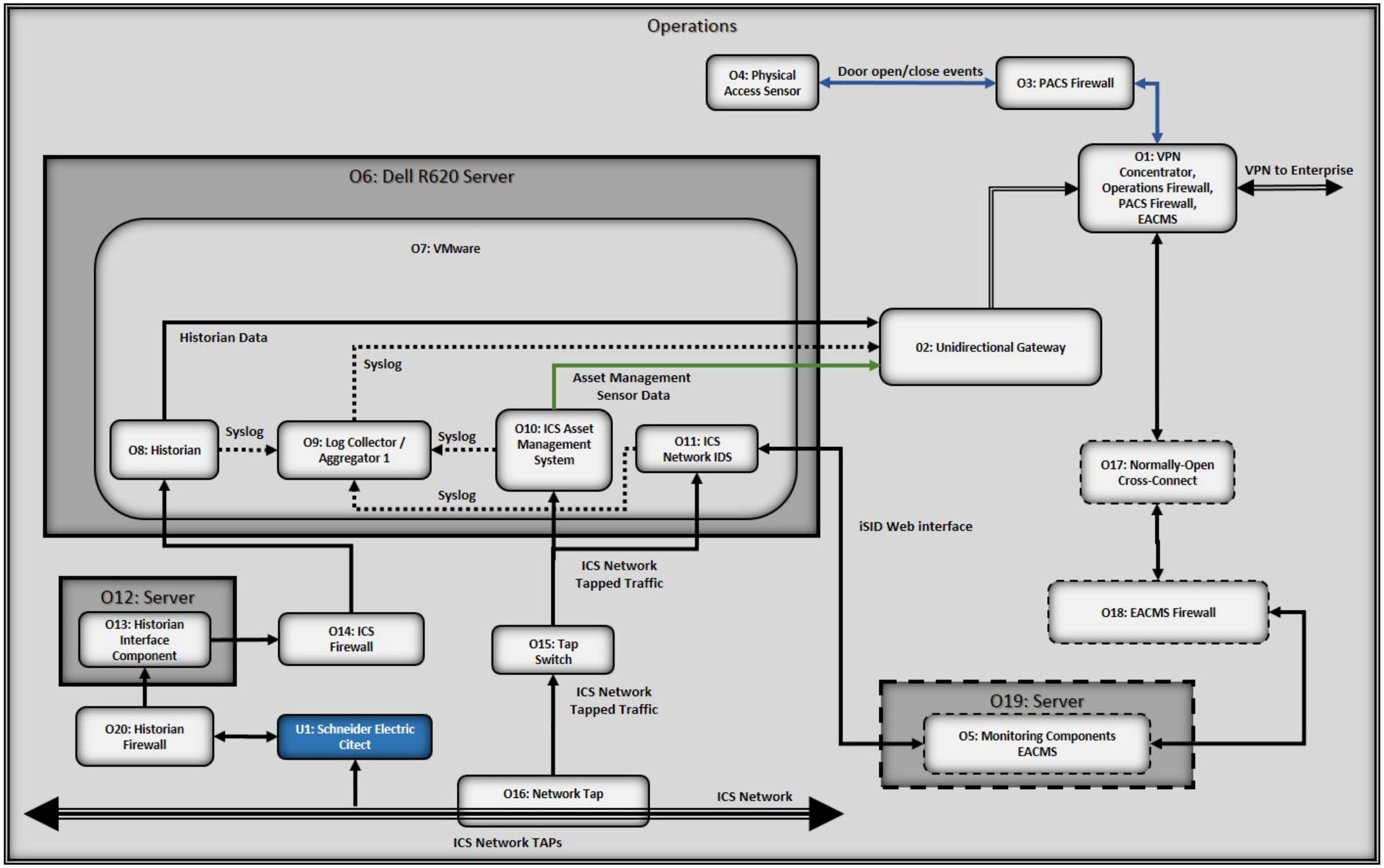

Operations
O4: Physical Access Sensor
Door open/close events
O3: PACS Firewall
O1: VPN Concentrator, Operations Firewall, PACS Firewall, EACMS
VPN to Enterprise
O6: Dell R620 Server
O7: VMware
Historian Data
Syslog
Asset Management Sensor Data
02: Unidirectional Gateway
O8: Historian
Syslog
O9: Log Collector / Aggregator 1
Syslog
O10: ICS Asset Management System
O11: ICS Network IDS
Syslog
O17: Normally-Open Cross-Connect
iSID Web interface
ICS Network Tapped Traffic
O12: Server
O13: Historian Interface Component
O14: ICS Firewall
O15: Tap Switch
O18: EACMS Firewall
ICS Network Tapped Traffic
O19: Server
O5: Monitoring Components EACMS
O20: Historian Firewall
U1: Schneider Electric Citect
O16: Network Tap
ICS Network
ICS Network TAPs

Figure 5-2 Data Aggregation/Analysis Subarchitecture Using Generic Component Names

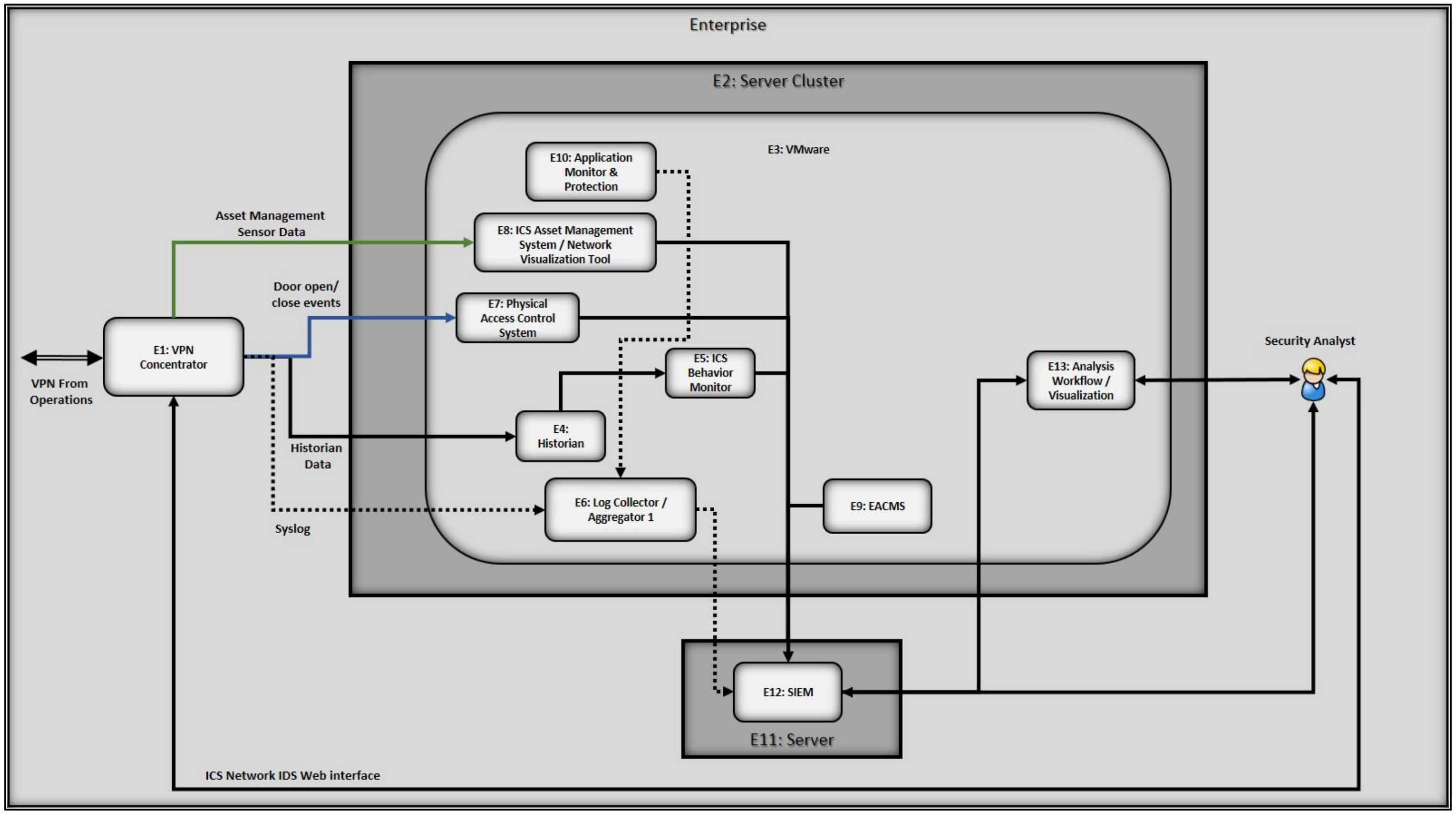

Enterprise
E2: Server Cluster
E3: VMware
E10: Application Monitor & Protection
E8: ICS Asset Management System / Network Visualization Tool
E7: Physical Access Control System
E5: ICS Behavior Monitor
E4: Historian
E6: Log Collector / Aggregator 1
E9: EACMS
E13: Analysis Workflow / Visualization
Security Analyst
E1: VPN Concentrator
VPN From Operations
Asset Management Sensor Data
Door open/ close events
Historian Data
Syslog
E12: SIEM
E11: Server
ICS Network IDS Web interface

Table 5-1 SA Reference Design Components and the Cybersecurity Framework Subcategories that They Support

Component	ID	Specific Product	Function	Cybersecurity Framework Subcategories
SIEM	E12	HPE ArcSight *Please note: HPE in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.*	Aggregates all IT, Windows, OT (ICS), and physical access monitoring, event, and log data collected by the reference design. Acts as a data normalization and correlation point and enables queries to be developed and executed to detect potential security incidents. Serves as the central location at which the analyst can access all data collected.	DE.AE-3, DE.AE-5 Related Subcategories: PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-7
Network Tap	O16	IXIA Full Duplex Tap	Collect data from specific locations on the ICS network and send it to the monitoring server via the ICS firewall. The taps are passive, so if they lose power or otherwise fail, they will not adversely affect the ICS network. Also, they collect data via monitor ports that are inherently unidirectional (and so do not pose any threat of information leaking from the tap onto the ICS network).	DE.CM-1
Log Collector/ Aggregator	O9 E6	TDi Technologies ConsoleWorks (Operations)	Log collection and aggregation; adds a time stamp and integrity seals the log entries. Log collection in the operations facility protects against potential data loss if the communication channel between the operations and enterprise facilities fails. Aggregating the log entries of all monitoring components at the operations log collector/aggregator ensures that this log data gets buffered in the operations facility and	PR.DS-6, PR.PT-1, DE.AE-3

Component	ID	Specific Product	Function	Cybersecurity Framework Subcategories
			can be transferred later if connectivity to the enterprise network is lost. *Note that two instances of the log collector/aggregator component are present in the reference design: one in the reference design's monitoring/data collection subarchitecture and another in its data aggregation/analysis subarchitecture. Integrity seals that are applied by a log collector/aggregator can be verified only at that log collector/aggregator. Therefore, the log collector/aggregator that is in the operations facility does not apply an integrity seal to its entries because these integrity seals cannot be verified in the enterprise.*	
ICS Asset Management System	O10	Dragos Security CyberLens Sensor	▪ monitors ICS traffic and maintains a database of all ICS assets of which it is aware ▪ This enables it to detect new ICS devices, ICS devices that disappear, and changes to known ICS devices.	ID.AM-1
Network Visualization Tool	E8	Dragos Security CyberLens Server	▪ displays a depiction of network devices, connectivity, and traffic flows	Does not directly support a Cybersecurity Subcategory. Related Subcategory: ID.AM-3

Component	ID	Specific Product	Function	Cybersecurity Framework Subcategories
PACS	E7	RS2 AccessIT!	▪ controls user access to doors ▪ detects and reports door open/close events and user identity	PR.AC-2
Physical Access Sensor	O4	RS2 Door Controller	▪ senses door close/open events ▪ generates alerts when door open and close events occur	DE.CM-2
ICS Network IDS	O11	Radiflow iSID	▪ identify, monitor, and report anomalous ICS traffic that might indicate a potential intrusion	DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-7
Historian	O8	OSIsoft Pi Historian	▪ serves as a data repository that essentially replicates the database of collected ICS values on the ICS network's historian ▪ can be configured to generate alerts when changes to certain ICS process values occur *Two instances of the historian component are present in the reference design: one in the monitoring/data collection subarchitecture and another in the data aggregation/analysis subarchitecture.*	Does not directly support a Cybersecurity Framework Subcategory. Provides data to be monitored by the ICS behavior monitor. Related Subcategories: DE.AE-5, DE.CM-1

Component	ID	Specific Product	Function	Cybersecurity Framework Subcategories
ICS Behavior Monitor	E5	ICS2 OnGuard	▪ monitors ICS process variable values in the historian to assess application behavior, detect process anomalies, and generate alerts	DE.AE-5, DE.CM-1
Application Monitor and Protection	E10	Waratek Runtime Protection	▪ monitors and protects a running application, analyzes the data it collects, and detects and reports unusual application behavior, e.g., it might generate an alert if it detects a potential SQL injection attack against the SIEM	DE.AE-2, DE.AE-4, DE.AE-5, DE.CM-4
Analysis Workflow Engine	E13	RSA NetWitness SecOps Manager	▪ automates workflow associated with review and analysis of data that has been collected at the SIEM ▪ enables orchestration of various analytic engines	DE.AE-2
Unidirectional Gateway	O2	Waterfall Unidirectional Security Gateway	▪ allows data to flow in only one direction	PR.AC-5, PR.PT-4
Visualization Tool	E13	RSA SecOps	▪ provides data reduction and a dashboard capability for the data in the SIEM, as well as risk analysis	Does not directly support a Cybersecurity Framework Subcategory. Related Subcategory: ID.AM-3

Component	ID	Specific Product	Function	Cybersecurity Framework Subcategories
EACMS	O5	TDi Technologies ConsoleWorks	▪ authenticates system managers ▪ provides role-based access control of system management functions ▪ implements a “protocol break” between the system manager and the managed assets ▪ records all system management actions	PR.AC-3, PR.AC-4, PR.PT-1, PR.PT-3, PR.MA-2, DE.CM-3
	E9	Siemens RUGGEDCOM CROSSBOW	▪ authenticates system managers ▪ provides role-based access control of system management functions ▪ implements a “protocol break” between the system manager and the managed assets ▪ records all system management actions	PR.AC-3, PR.AC-4, PR.PT-1, PR.PT-3, PR.MA-2, DE.CM-3
	O17	Waterfall Secure Bypass	▪ provides time-limited network connectivity to perform system management functions	PR.AC-5, PR.PT-4
	O18	Schneider Electric Tofino Firewall	▪ controls network connectivity for performing system management functions	PR.AC-5, PR.PT-4

The last column of Table 5-1 lists the Cybersecurity Framework Subcategories that each component of the reference design supports. In Section 3.4.2, Security Control Map, the Cybersecurity Framework Subcategories are mapped to specific sections of informative references that are composed of existing standards, guidelines, and best practices for that Cybersecurity Framework Subcategory. In conjunction with these references, the Cybersecurity Framework Subcategories can provide structure to the assessment of the security support provided by the SA reference design. The references provide use case validation points in that they list specific security traits that a solution that supports the desired Cybersecurity Framework Subcategories would be expected to exhibit. Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports specific security activities and provides additional confidence that the reference design addresses the SA use case security objectives. The remainder of this subsection discusses how the reference design supports each of the identified Cybersecurity Framework Subcategories.

5.1.1 Cybersecurity Framework Subcategories that Are Supported

The reference design's primary focus is the Detect function area of the Cybersecurity Framework as well as a few Subcategories within the Identify and Protect function areas. Specifically, the reference design supports:

- all five Subcategories of the Anomalies and Events Category of the Detect function area (DE.AE)
- five of the eight Subcategories of the Security Continuous Monitoring Category of the Detect function area (DE.CM)
- one activity in the Identify function area, which is in the Asset Management Category (ID.AM)
- nine activities from various Categories of the Protect function area (PR.AC-2, 3, 4, 5; PR.DS-2; PR.DS-6; PR.IP-1, and PR.PT-1, 3, 4)

We discuss these Cybersecurity Framework Subcategories in the following subsections.

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

This Cybersecurity Framework Subcategory is supported by the ICS network IDS component of the reference design. This component is a tool for identifying, monitoring, and reporting anomalous ICS traffic that might indicate a potential intrusion. This component, located in the monitoring server, sends syslog events regarding anomalous behavior that it detects to the log collector/aggregator in the monitoring server, which forwards them to the SIEM on the enterprise network, where they can be viewed by a security analyst. In addition to having the ability to send syslog events, the ICS network IDS component also has its own graphical user interface that can be accessed only by a web interface.

5.1.1.2 DE.AE-2: Detected events are analyzed to understand attack targets and methods

This Cybersecurity Framework Subcategory is supported by both the application monitor and the analysis workflow engine components, both of which are located in the data aggregation/analysis subarchitecture. The application monitor monitors a running application, analyzes the data it collects, and detects and reports unusual application behavior. In the build, the application monitor is configured to generate an alert if it detects a potential SQL injection attack against the SIEM. The analysis workflow engine, located downstream from the SIEM, automates workflows associated with review and analysis of data that has been collected at the SIEM. It consists of various analytic engines that can be orchestrated. This component enables the automated execution of well-defined courses of action that can be associated with an observable sequence of events.

In some cases, the individual monitoring components in the reference design will be able to single-handedly detect events. In other cases, the aggregation and correlation of event data from multiple sources and sensors might be needed to identify anomalies and thereby enable such detection.

Although ensuring that security analysts study, analyze, and understand attack targets and methods is outside the scope of the reference design, the objective of the reference design is to support and facilitate the ability of the analyst to perform these functions. When possible, analysis and anomaly detection procedures might be automated within various components. For events that are not detected automatically, the aggregation of all SA information at the single, centralized SIEM enables analysts to more easily correlate and visualize multiple facets of SA, facilitating their ability to analyze and understand attack targets and methods.

5.1.1.3 DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

This Cybersecurity Framework Subcategory is supported by the SIEM, which aggregates all IT, OT (ICS), and PACS data that is collected by the reference design. This includes monitoring, event, and log data. The SIEM acts as a data normalization and correlation point. It is a location at which queries can be developed and executed for detecting potential security incidents. The SIEM also serves as the central location at which the analyst can access all data collected.

Before log data is sent to the SIEM for aggregation, it is aggregated at two subcollection points, both of which also support Cybersecurity Framework Subcategory DE.AE-3. Log data are collected and aggregated at both the log collector/aggregator component in the monitoring/data collection subarchitecture and at the log collector/aggregator component in the data aggregation/analysis subarchitecture. These log collector/aggregators add time stamps to the collected log entries. The log collector/aggregator in the aggregation/analysis subarchitecture also applies an integrity seal to the log entries.

Support for this Subcategory is a main goal of the SA reference design. Aggregation and correlation of SA data from multiple sources and sensors at various analysis and anomaly detection components into a single, centralized SIEM component enables a security analyst to more easily understand attack targets and methods. All physical security, ICS network assets, network security, IT system information, reports, alerts, and other information is consolidated in a single, centralized SIEM component. In some cases, the information sent to the analysis and anomaly detection components, and the SIEM might include notifications of potential events that have already been detected. In other cases, the analysis and anomaly detection components or the analyst accessing the SIEM might be able to detect events that were not indicated by any single monitoring component. Only by combining and correlating information from a variety of sources was the event identified.

The SIEM is the normalization point for all SA data. It is a location at which queries can be developed and run to look for anomalies. The security analyst has direct access to the data collected at the SIEM. Analysis components downstream from the SIEM enable the data that has been collected at the SIEM to be analyzed. They also enable automation of the workflow that is associated with the analysis activities, enabling analytic engines to be orchestrated.

5.1.1.4 DE.AE-4: Impact of events is determined

This Cybersecurity Framework Subcategory is supported by the application monitor component, which monitors a running application, analyzes the data it collects, and detects and reports unusual application behavior (e.g., a potential SQLi attack).

5.1.1.5 DE.AE-5: Incident alert thresholds are established

Although determining incident alert threshold values is outside the scope of the reference design, various reference design components support the ability to establish such thresholds and act upon them when they are exceeded. Cybersecurity Framework Subcategory DE.AE-5 is supported by four components in the reference design: SIEM, ICS network IDS, ICS behavior monitor, and application monitor, each of which generates alerts to report some form of unusual behavior once the detected behavior exceeds established thresholds. The incident alert thresholds in the SIEM might refer to anomalies that are detected as a result of IT, OT, and PACS information correlation. The thresholds in the ICS network IDS might refer to levels of anomalous ICS traffic. ICS behavior monitor component thresholds might refer to ICS process variable anomaly levels. application monitor component thresholds are designed to detect and alert to unusual IT application behavior.

Although the historian component of the reference design does not support this Cybersecurity Framework Subcategory directly, it provides data to the ICS behavior monitor and thereby supports this Subcategory indirectly. The ICS network contains a component that acts as a historian, recording important information regarding events and variable values for various ICS components. All process values stored in this ICS historian are conveyed to the historian component of the reference design via a historian interface component. As a result, the reference design's historian component essentially replicates the ICS historian's database of values that have been collected and monitored.

The historian component's database is not a typical SQL database. It has the capability to issue an "on change" request, meaning that it can be configured to send notices when changes to certain ICS process values occur. This capability enables the reference design to avoid constant polling of historian component values and constitutes a first line of monitoring defense against potential cybersecurity events on the ICS network that might be detected when the alert thresholds are exceeded for specific ICS variable values.

5.1.1.6 DE.CM-1: The network is monitored to detect potential cybersecurity events

This Cybersecurity Framework Subcategory is supported by three components:

1. Network Tap: collects data from specific locations on the ICS network and sends it to the monitoring server
2. ICS Network IDS: monitors ICS traffic and reports anomalous ICS traffic that might indicate a potential intrusion
3. ICS Behavior Monitor: monitors ICS process variable values in the historian to assess application behavior, detect process anomalies, and generate alerts

Although the historian component does not support this Subcategory directly, it can be configured to generate alerts when ICS process variable values change. This Subcategory is also listed as being related to the SIEM due to the SIEM's role as the aggregation point for all collected information, which enables it to support network monitoring to detect potential cybersecurity events.

5.1.1.7 DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

This Cybersecurity Framework Subcategory is supported by the physical access sensor component, which senses door close/open events and generates alerts when door open and close events occur. The physical access sensor component serves as a sort of placeholder for multiple potential PACS monitoring devices that could and should be included in an operational deployment. In an operational deployment, organizations would likely include additional PACS monitoring devices, such as badge readers, to increase the amount and quality of PACS information provided as part of SA. In a real deployment, information coming out of the PACS would include not only door open/close events but also access decisions based on the identity and permissions of the individuals trying to access the doors. All such monitored PACS (and IT and OT) information is aggregated in the SIEM, which is why Cybersecurity Framework Subcategory DE.CM-2 is listed as related to the SIEM. As the aggregation point for all collected PACS data, the SIEM can therefore support monitoring of the physical environment to detect potential cybersecurity events.

5.1.1.8 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

This Cybersecurity Framework Subcategory is supported by the EACMS for system managers. All system manager actions are captured by the EACMS and can be provided to the SIEM for review and correlation with other system activity.

5.1.1.9 DE.CM-4: Malicious code is detected

This Cybersecurity Framework Subcategory is supported by the application monitor and protection component, which monitors a running application, analyzes the data it collects, and detects and reports unusual application behavior (e.g., a potential SQL injection attack). Because the reference design focuses mostly on collecting and integrating OT information and assumes that collection and integration of IT information into the SIEM is a solved problem, the application monitor component serves as a sort of placeholder for multiple potential IT monitoring devices that could and should be included in an operational deployment. In an operational deployment, organizations would likely include additional IT monitoring capabilities such as anti-virus software to increase the amount and quality of IT information provided as part of SA.

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

This Cybersecurity Framework Subcategory is supported by the ICS network IDS component, which identifies, monitors, and reports anomalous ICS traffic that might indicate a potential intrusion on the OT network. This Subcategory is also listed as related to the SIEM. The SIEM serves as the aggregation point for all collected information and can therefore support monitoring for unauthorized personnel, connections, devices, and software.

5.1.1.11 ID.AM-1: Physical devices and systems within the organization are inventoried

This Cybersecurity Framework Subcategory is supported by the ICS asset management system component, which monitors ICS traffic to sense, track, and record ICS assets, and maintains a database of all ICS assets of which it becomes aware. Such monitoring enables this component to detect and identify new devices on the ICS network, devices that disappear from the ICS network, and changes to known ICS devices. This enables it to perform data analytics and anomaly detection as well as management of the inventory of ICS assets that it senses and collects. The ICS asset management system sends logs of asset inventory events to the log collector/aggregator and feeds the ICS asset information it collects into the SIEM component.

5.1.1.12 PR.AC-2: Physical access to assets is managed and protected

This Cybersecurity Framework Subcategory is supported by the reference design’s PACS, which controls user access to doors and detects and reports door open/close events. As was stated earlier, the reference design's physical access sensor and control system components serve as placeholders for multiple potential PACS monitoring devices that could and should be included in a reference design deployment to manage and protect physical access to assets. For example, organizations would likely want to include badge readers to support access decisions based on the identity and permissions of the individuals trying to access the doors. The reference design provides the vehicle for integrating information from additional PACS devices into the SIEM.

5.1.1.13 PR.AC-3: Remote access is managed

This Cybersecurity Framework Subcategory is supported by the functions that compose the EACMS. Together, these functions allow carefully controlled and monitored remote access to manage monitoring systems deployed to operations.

5.1.1.14 PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

This Cybersecurity Framework Subcategory is supported by the functions that compose the EACMS. These functions allow definition and enforcement of role-based access permissions that incorporate least privilege and separation of duties.

5.1.1.15 PR.AC-5: Network integrity is protected, incorporating network segmentation where appropriate

This Cybersecurity Framework Subcategory is supported by using firewalls, a unidirectional gateway, and a normally open cross-connect. All of these functions segment the network to preserve integrity.

5.1.1.16 PR.DS-2: Data in transit is protected

This Cybersecurity Framework Subcategory is supported by use of a VPN, which uses encryption to protect the confidentiality and integrity of all information while it is in transit between the monitoring/data collection subarchitecture and the data aggregation/analysis subarchitecture. The reference design does not, however, protect the confidentiality or integrity of monitored data while it is in transit within either the monitoring/data collection subarchitecture or the aggregation/analysis subarchitecture.

5.1.1.17 PR.DS-6 Integrity-checking mechanisms are used to verify software, firmware, and information integrity

This Cybersecurity Framework Subcategory is supported by the log collector/aggregator that is in the aggregation/analysis subarchitecture of the reference design insofar as the log collector/aggregator integrity seals the log data that it collects. Ideally, the log collector/aggregator in the monitoring/data collection subarchitecture would also apply an integrity seal to each log entry so that this seal could be verified by the log collector/aggregator in the data aggregation/analysis subarchitecture to ensure that no log entries were modified before reaching the data aggregation/analysis subarchitecture log collector/aggregator. This integrity checking of monitoring/data collection log entries, however, is not currently provided in the build because there is currently no mechanism to enable any component other than the log collector/aggregator that applies the integrity seals to verify those seals. In an ideal world, all information sent from components in the monitoring/data collection subarchitecture to the aggregation/analysis subarchitecture would be integrity protected while both at rest and in transit.

5.1.1.18 PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained

Organizations deploying this reference design should create and maintain baseline configurations so that the reference design can use these baselines to more effectively identify potential cybersecurity threats. The ICS behavior monitor component, for example, is responsible for establishing incident alert thresholds and monitoring ICS process variable values to assess application behavior and detect process anomalies that could indicate cybersecurity events. To best establish effective thresholds and detect relevant anomalies, the ICS behavior monitor and other similar components need to have some notion of typical baseline behavior for the ICS systems. The ICS behavior monitor component itself is not expected to generate such a baseline; it builds its own model of ICS behavior based on observed values in the historian. However, it does not know if that model is correct; it knows only that the model is "normal" in the sense that the model represents what it has observed. The ICS behavior monitor and other similar components would be more effective if they were provided with a baseline configuration against which to identify anomalous behavior and unexpected thresholds. Ideally, an organization deploying the reference architecture should have a mechanism for creating, maintaining, and providing such baseline behavior information to the reference design for this purpose.

5.1.1.19 PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

This Cybersecurity Framework Subcategory is provided by both log collector/aggregators in the reference design, which aggregate logs from various devices and put time stamps on the log data. Although the SIEM does not directly support this Subcategory, PR.PT-1 is also listed as a related Subcategory for the SIEM because the SIEM can be used to review audit/log records.

Ideally, all of the monitoring/data collection components in the reference design will be capable of generating log data that contains the relevant event information and sending this log data to the log collector/aggregator component. (In the build, neither the PACS nor the physical access sensor sends log data that contains the events to the log collector/aggregator; instead, the SIEM obtains PACS event information via a PACS MySQL database.) The log collector/aggregator component's role is to aggregate all log data that it collects. In addition, when each log entry is received at the log collector/aggregator, it already contains a time stamp added by the sending device. Upon receipt of the log entry, the log collector/aggregator component puts its own time stamp on the entry to indicate the time that it was received. Discrepancies in the sent and received time stamps for a given entry can be monitored to detect suspicious activity. The log collector/aggregator in the monitoring and data collection subarchitecture then sends all logs to the log collector/aggregator in the data aggregation/analysis subarchitecture, which puts its own time stamps on the entries that it receives. It also applies an integrity seal to the entry that can be checked later to ensure that the entry has not been deliberately or inadvertently modified. This log collector/aggregator then sends its log entries to the SIEM. The SIEM consolidates these log entries along with all other SA information.

The collection of SA information in a single location (at the SIEM) enables audit and log records to be reviewed easily in accordance with policy. Furthermore, the analysis tool components into which the SIEM data feeds might facilitate automation of the review of audit and log records. Whether or not the organization performs these audit and log reviews according to policy is outside the scope of the SA reference design.

5.1.1.20 PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

This Cybersecurity Framework Subcategory is supported by the functions that compose the EACMS, and by network firewalls. The EACMS controls system manager access to systems in operations. Network firewalls control connectivity to and interaction among network assets.

5.1.1.21 PR.PT-4: Communication and controls networks are protected

This Cybersecurity Framework Subcategory is supported by a VPN, a firewall, a unidirectional gateway, and a normally open cross-connect. The VPN provides confidentiality protection for data in transit between the operations facilities and enterprise. Firewalls are placed throughout the system to control the network connections that are allowed among function within operations. A unidirectional gateway ensures that communication between operations and enterprise is one way out of operations. The normally open cross-connect allows a two-way communication path between operations and enterprise but only when physically closed at the operations side.

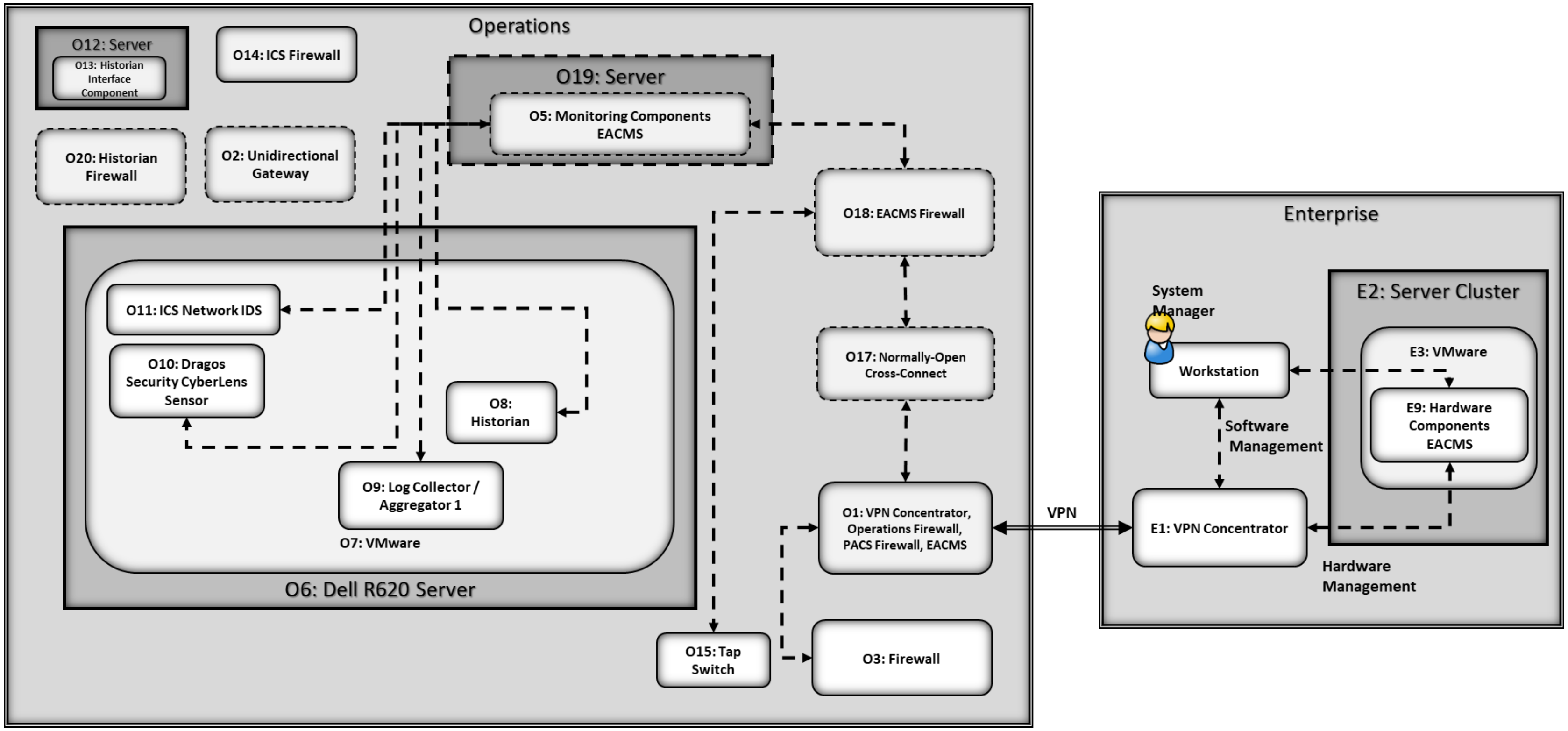
5.2 Analysis of Reference Design Security

The list of reference design components included in Table 5-1 focuses only on the components of the reference design that are needed to enable it to meet its SA objective of collecting information from the ICS network, aggregating it at a centralized location, and providing analysis capability in a manner that supports the intended Cybersecurity Framework Subcategories. Table 5-1 does not include components that are needed to manage or secure the reference design. However, the reference design itself must be managed and secured. To this end, this second part of the security evaluation focuses on the security of both the reference design itself and its management infrastructure.

Table 5-2, Components for Managing and Securing the SA Reference Design and Protecting the ICS Network, lists components that are needed to manage the reference design, secure both the reference design and the data it collects, and protect the ICS network. Table 5-2 also describes the security protections provided by each of the management and security components. As with part 1 of the security evaluation, although the products that were used to instantiate each component in the build are also listed, the security protections provided by these products are the focus of this security evaluation.

Figure 5-3 depicts the monitoring/data collection management architecture of the reference design using the generic name of each component.

Figure 5-3 Monitoring/Data Collection Management Architecture Depicted Using Generic Component Names



Note that because the NCCoE build used products from many different vendors, the NCCoE provided those vendors with access to the NCCoE lab for product installation, configuration, and maintenance. Therefore, the architecture that was actually instantiated included components for securing this vendor access path. However, this vendor access path is an artifact specific to the NCCoE build. It is not anticipated that organizations that adopt the SA architecture would enable such a vendor access path in their implementations. Therefore, this vendor access path is not included within the scope of the security evaluation.

Table 5-2 Components for Managing and Securing the SA Reference Design and Protecting the ICS Network

Component	ID	Specific Product	Security Protection Provided
EACMS	O1 O5 O18 O17	Siemens RUGGEDCOM RX1501 TDi Technologies ConsoleWorks (Operations Management) Schneider Electric Tofino Firewall Waterfall Secure Bypass	One EACMS component (Siemens RUGGEDCOM RX1501) enables remote configuration of privileged user access to the PACS firewall. This EACMS component is referred to as the PACS firewall EACMS. A second EACMS component (TDi Technologies ConsoleWorks) enables remote configuration of privileged user access to the consoles of the four components on the monitoring server (log collector/aggregator, ICS asset management system, ICS network IDS, and historian). This EACMS component is referred to as the monitoring components' EACMS. The third EACMS component (Schneider Electric Tofino Firewall) operates as the network port and protocol level to control remote management traffic exchanged between the enterprise network and the monitoring components' EACMS. It also serves as the EACMS for the taps switch. This EACMS component is referred to as the EACMS firewall. The fourth EACMS component (Waterfall Secure Bypass) is hardware that might be manually configured to enable data to be sent into the operations facility to support EACMS activities for a limited period of time. All EACMS components except for the Waterfall Secure Bypass, which is a physical cross-connect, also create an audit trail of all privileged user access to the components that they protect. They send log entries documenting this audit trail to the SIEM. None of the four components that compose the EACMS can be remotely managed.

Component	ID	Specific Product	Security Protection Provided
			Each EACMS component except for the Waterfall Secure Bypass includes the three policy subcomponents listed in the next three rows of this table.
EACMS Policy Administration Point	O1 O5 O18	Siemens RUGGEDCOM RX1501 TDi Technologies ConsoleWorks (Operations Management) Schneider Electric Tofino Firewall	The point that manages access authorization policies; it is the source of policies for the EACMS and the location at which policies might be created and edited.
EACMS Policy Decision Point (PDP)	O1 O5 O18	Siemens RUGGEDCOM RX1501 TDi Technologies ConsoleWorks (Operations Management) Schneider Electric Tofino Firewall	the point that evaluates access requests against authorization policies for the EACMS before issuing access decisions
EACMS Policy Enforcement Point (PEP)	O1 O5 O18	Siemens RUGGEDCOM RX1501 Station Access Controller TDi Technologies ConsoleWorks (Operations Management) Schneider Electric Tofino Firewall	The point that intercepts user's access request to a resource, makes a decision request to the EACMS's PDP to obtain the access decision (i.e., access to the resource is approved or rejected), and acts on the received decision. In the build, the Siemens CROSSBOW EACMS Station Access Controller is integrated into the Siemens RUGGEDCOM RX1501 component.
PACS Firewall EACMS	O1	Siemens RUGGEDCOM RX1501	enables configuration of privileged user access to the PACS firewall to be controlled remotely in a manner similar to that in which the monitoring components' EACMS enables configuration of privileged user access to the consoles on the monitoring server components to be controlled

Component	ID	Specific Product	Security Protection Provided
Monitoring Components' EACMS	O5	TDi Technologies ConsoleWorks (Operations Management)	enables configuration of privileged user access to the consoles on the monitoring server components to be controlled remotely in a manner similar to that in which the PACS firewall EACMS enables privileged user access to the PACS firewall to be controlled
EACMS Firewall	O18	Schneider Electric Tofino Firewall	Firewall that operates at the network port and protocol level to monitor all traffic received at the monitoring components' EACMS from external sources when the normally open cross connect is closed. In addition to monitoring traffic, the firewall also restricts traffic flow according to its configured rules. This firewall's purpose is to ensure that the only permitted components to which traffic can flow to and from the normally open cross-connect are the server for the monitoring component's EACMS (O19) and the taps switch (O15). It is configured to permit only three types of traffic: (1) remote management traffic exchanged between the enterprise network and the monitoring components' EACMS, which is used to control privileged user access to the consoles of the four components on the monitoring server and access to the web interface of the ICS network IDS, (2) remote management traffic exchanged between the enterprise network and the taps switch, and (3) traffic exchanged between the enterprise network and the ICS network IDS component to support the web interface that enables security analysts that are located on the enterprise network to view SA information by using the ICS network IDS component's graphical user interface. (Note that support for this last type of traffic is one way in which the reference design differs from the build because the reference design requires that the ICS network IDS component report potential IDS events by sending syslog

Component	ID	Specific Product	Security Protection Provided
			events; it does not require support for a graphical user interface to the ICS network IDS component.
PACS Firewall	O3	Schneider Electric Tofino Firewall	Monitors traffic sent between the VPN concentrator/PACS firewall EACMS component and the physical access sensor component. Configured to ensure that the only messages that are permitted to be received from the physical access sensor are door open/close, and other valid PACS events are forwarded to the VPN concentrator. The physical access sensor sits on an operational IT network that is connected to the internet. Therefore, this PACS firewall is exposed to the operational IT network and, via that network, to the internet. So configuring the PACS firewall to accept only PACS sensor messages prevents the PACS devices and the operational network on which they sit from being used as an attack vector to compromise the reference architecture. In particular, the PACS firewall prevents traffic (other than door controller traffic) from being sent from the internet to the enterprise network via the VPN.
VPN Concentrator	O1	Siemens RUGGEDCOM RX1501	The VPN concentrator supports four types of VPN traffic between the operations facility and the enterprise network: monitoring data sent from the operations facility to the enterprise network; remote management traffic used to support privileged access to the consoles of the four components on the monitoring server; remote management traffic used to support privileged user access to the console of the PACS firewall; and web interface traffic exchanged between the ICS network IDS component and a remote security analyst located on the enterprise network. The traffic exchanged on this web interface might be either traffic needed to support remote management of the ICS network IDS component by a security analyst

Component	ID	Specific Product	Security Protection Provided
			or traffic needed to support the ICS network IDS component's graphical user interface. (This graphical user interface is not part of the reference design, but it is supported in the build.)
Operations Firewall	O1	Siemens RUGGEDCOM RX1501	Firewall monitoring all traffic sent between the operations facility and external sources and restricting traffic flow according to its configured rules. This firewall is the one device on the operations facility network that is exposed to the internet at all times. Regarding traffic arriving at the operations facility from external sources, it is configured to permit (1) remote management traffic exchanged between the enterprise network and the monitoring components' EACMS, which will be further scrutinized by the EACMS firewall, (2) remote management traffic exchanged between the enterprise network and the PACS firewall EACMS, and (3) remote management traffic exchanged between the enterprise network and the taps switch.
Unidirectional Gateway	O2	Waterfall Unidirectional Security Gateway Hardware	Enforces one-way transfer between a transmitter and receiver within hardware, ensuring that data may be sent from the monitoring server to the enterprise but not in the reverse direction. The gateway also replicates industrial servers and emulates industrial devices to IT users and applications.
Normally Open Cross-Connect	O17	Waterfall Secure Bypass	Enables the data unidirectional gateway component to be bypassed so that data can be sent into the operations facility for specific management and monitoring purposes. Must be closed manually and stays closed only for a limited period of time.

Component	ID	Specific Product	Security Protection Provided
ICS Firewall	O14	Radiflow 3180 firewall	Firewall monitoring all traffic that flows from the historian interface component to the monitoring server. This firewall is configured to prevent traffic from flowing in the reverse direction, i.e., to prevent traffic from flowing from the monitoring server to the ICS network. Also, it cannot be managed remotely.
Historian Firewall	O20	Schneider Electric Tofino Firewall	Firewall monitoring all traffic that flows between the ICS historian and the historian interface component. This firewall is configured to prevent traffic from flowing from the historian interface component to the ICS network. It cannot be managed remotely.
Historian Interface Component	O13	OSIsoft Citect Interface	This component interfaces with the ICS historian that is on the ICS network. It receives data from the ICS historian and provides this to the historian component in the monitoring server of the SA reference architecture, but it does not permit data to travel in the other direction, from the monitoring server to the ICS historian.
Tap Switch	O15	Cisco 2950 (Aggregator)	This switch aggregates data received from all ICS taps and forwards this data to the monitoring server. It is configured to permit only one-way data flow from the tap interfaces toward the monitoring server interface. No data is permitted to travel out of the tap interfaces toward the taps.

5.2.1 Protecting the ICS Network

A main security requirement of the SA use case is to ensure that the ICS network is not impacted by the monitoring to which it is subjected. In particular, it is crucial to ensure that, although data can flow from the ICS network to the reference design, a minimal amount of very strictly restricted data is allowed to flow from the reference design onto the ICS network. There are two paths on which data flows from the ICS network to the monitoring server: from the ICS network taps, and from the ICS historian.

These taps are inherently unidirectional. By design, they permit data to flow only from the ICS network to the monitoring server. They are not able to allow data to flow from the monitoring server to the ICS network. These taps are also passive, meaning that if they were to lose power or otherwise fail, they would not disrupt the flow of data on the ICS network.

This unidirectional transmission path is enforced by the historian firewall (O20) (i.e., a Schneider Electric Tofino Firewall in the build), the historian interface component (O13), the server on which it resides, and the ICS firewall (O14) (i.e., the Radiflow 3180 firewall in the build), all of which sit between the ICS historian (i.e., Schneider Electric Citect in the build) and the monitoring server. These components are critical for ensuring that only a small amount of strictly restricted data is permitted to travel into the ICS network from the monitoring server.

In the build, the historian interface component (O13) pulls data from the ICS historian (Schneider Electric Citect, U1) and pushes this information to the historian component in the monitoring server (O8). This means that the historian interface component (O13) needs to send a message to the ICS historian (U1) that sits on the ICS to cause it to send the historian data to the historian interface component. Therefore, the historian firewall (O20) between the historian interface component and the ICS historian has to be configured to permit requests for data to flow from the historian interface component to the ICS historian. It also must be configured to allow historian data to flow in the opposite direction, i.e. from the ICS historian to the historian interface component.

The fact that requests for data pulled from the ICS historian must be permitted to be sent from the operations network to the ICS network is not ideal. To protect the ICS network, it would be preferable to prevent all data flow from the operations network to the ICS network. To ensure that requests for historian data are the only type of data that is permitted to be sent from the operations network to the ICS network, it is essential that the historian firewall (O20) that sits between these two components be configured to limit the data that is sent to the ICS network to the necessary requests for historian data and nothing more. It is also essential that this historian firewall (O20) cannot be configured remotely. This ensures that only an insider who has physical access to this firewall (O20) would be able to modify its rules to permit additional traffic to enter the ICS network from the operations network.

Once it has the historian data, the historian interface component pushes this data to the historian component (O8) on the monitoring server. This means that the firewall (O14) that sits between the historian interface component and the historian component can (and must) be configured not to permit any data to flow in the direction from the monitoring server to the historian interface component. It is also essential not to allow this firewall (O14) to be configured remotely.

In short, the reference design balances two competing goals:

1. protecting the ICS network as fully as possible from receipt of potentially harmful data from the reference design itself
2. enabling the ICS historian to receive requests for data from the reference design

It achieves these goals by isolating the historian interface component on both sides by firewalls, ensuring that these firewalls are configured correctly, and ensuring that neither these firewalls, the historian interface component, nor the server that the historian interface component sits on is remotely configurable. It should also be noted that the historian interface component is running on a server that is distinct from the monitoring server. This separation ensures that the reference design does not depend solely on VMware's ability to separate applications running on it to ensure that no data is permitted to travel from the monitoring server to the historian interface component. As discussed, none of the components located between the ICS historian and the monitoring server may be managed remotely. Creating additional means to configure these components from outside the operations facility is considered a greater risk than being unable to monitor changes to these firewalls from outside the facility; therefore, only technicians physically on site at the operations facility may change the configuration of these components.

5.2.2 Protecting the Reference Design from Outside Attack

Measures implemented to protect the monitoring and data collection subarchitecture itself from outside attack include …

- The PACS firewall situated between the physical access sensors and the VPN concentrator/PACS firewall EACMS is configured to permit only door open/close events and other valid notifications to be sent from the physical access sensors to the monitoring and data collection subarchitecture. The physical access sensors sit on the facility's operational network, which exposes them to the internet. The PACS firewall plays a crucial role in preventing external attacks to the monitoring network. It prevents the PACS devices and the operational network on which they sit from being used as an attack vector to compromise the monitoring and data collection subarchitecture.
- Data should be allowed to flow only from the enterprise network into the monitoring server under carefully controlled circumstances and with limited restrictions. The architecture's unidirectional gateway component (i.e., the Waterfall Unidirectional Security Gateway Hardware component in the build) that sits between the monitoring server and the VPN concentrator component (i.e., the Siemens RUGGEDCOM RX1501) is designed to enforce this in a unidirectional manner. This unidirectional gateway is a combination of hardware and

software. The hardware physically permits only one-way transfer across an optical connection between a hardware transmitter and a hardware receiver. The hardware ensures that monitored data may be sent from the monitoring server to the enterprise, but no data may be sent in the reverse direction on this connection into the monitoring server. Unidirectional gateway software replicates industrial servers and emulates industrial devices from the protected operations network to the enterprise network.

5.2.3 Protecting the Remote Management Paths

In the example solution presented, for the purpose of monitoring, the SA architecture design assumed that the data aggregation/analysis activity would be performed at a physically separate location from the data monitoring/collection activity. This scenario was used to reflect real-world operations; its risk is greater than the scenario in which the monitoring/data collection subarchitecture and the data aggregation/analysis subarchitecture are physically co-located in the same secure facility. Therefore, mechanisms for protecting the data and management path between the two parts of the architecture that support these activities are integral to the reference design.

For the purpose of monitoring, data should flow in a unidirectional manner from the operations facility to the enterprise network. For management purposes, however, there is a need for traffic to be able to flow into the operations facility from the enterprise network. In particular, incoming traffic is required to enable remote management of the following components:

- the PACS firewall (one of the Schneider Electric Tofino Firewalls in the build), which sits between the VPN concentrator and the physical access sensor
- the four data collection components in the monitoring server at the operations facility
- the tap switch, which sits between the ICS taps and the monitoring server
- the PACS firewall EACMS/operations firewall

Remote management traffic destined for the monitoring server or the taps switch must instead bypass the unidirectional gateway to reach its destination. This remote management traffic can be used to monitor and configure the PACS firewall.

Remote management traffic destined for the monitoring server or the taps switch must instead bypass the data diode to reach its destination. To enable this bypass, we used the normally open cross-connect component (the Waterfall Secure Bypass component in the build). Closing this normally open cross-connect enables traffic to flow back and forth between the enterprise network and the monitoring server for limited time periods.

These remote management access paths contain numerous components and features designed to secure them. These components are as follows:

- VPN concentrator – is directly exposed to the internet. This component is situated on its own network in the operations facility.
- Operations firewall – monitors all traffic sent between the operations facility and external sources and restricts traffic flow according to its configured rules. It is exposed to the internet at all times.

  This component contains a PEP for the PACS firewall (the Schneider Electric Tofino Firewall between the RS2 Door Controller and the RUGGEDCOM RX1501 in the build). This PEP is the "station access controller" shown within the RUGGEDCOM RX1501 build diagram. It enables administrative access to the console of the PACS firewall to be managed and monitored remotely.
- Normally open cross-connect – enables the unidirectional gateway to be bypassed, enabling traffic to flow into the operations facility monitoring architecture. As mentioned earlier, the unidirectional gateway sits on a path between the monitoring server and the operations firewall/VPN concentrator (RUGGEDCOM RX1500) to ensure that information can flow only in a unidirectional manner from the monitoring server to the enterprise network.

  This component is a physical switch that is normally open, ensuring that no data can be transmitted across it. This switch must be closed manually with a physical key by an operator who is located on site at the operations facility to enable remote traffic to enter the monitoring/data collection portion of the architecture from the enterprise. Once closed, it will remain closed for a limited, configurable amount of time (e.g., 30 minutes), and then it will automatically open (unless explicitly opened before this time period expires). The connection cannot be enabled remotely.
- EACMS firewall –is instantiated by using the Schneider Electric Tofino Firewall in the build. After passing through the VPN concentrator, the operations firewall, and the normally open cross-connect, traffic received from the enterprise flows to the EACMS firewall. Because of its placement behind the VPN concentrator, the operations firewall, and the normally open cross-connect, this component is not by default exposed to any traffic from outside the operations facility except for those periods of time when the normally open cross-connect has been explicitly closed, and traffic sent to the facility on a VPN meets the requirements for entry that are enforced by the operations firewall.

  When such a connection into the operations facility from outside is established, the EACMS firewall is needed to monitor traffic being exchanged between the operations facility and the outside. This firewall operates at the network port and protocol level to monitor and control remote management traffic exchanged between the enterprise network and both the taps switch and the monitoring components' EACMS. Three types of traffic are permitted by the EACMS firewall:

1. remote management traffic exchanged between the enterprise network and the monitoring components' EACMS (TDi Technologies ConsoleWorks), which is used to manage privileged access to each of the components on the monitoring server
2. web interface traffic exchanged between the ICS network IDS component on the monitoring server and a remote security analyst located on the enterprise network. The traffic exchanged on this web interface might be needed either to support remote management of the ICS network IDS component or to enable the security analyst to view SA data via the ICS network IDS component's graphical user interface.
3. remote management traffic exchanged between the hardware component EACMS (Siemens RUGGEDCOM CROSSBOW) on the enterprise network and the taps switch, which is used to administer the taps switch

- Monitoring components' EACMS – this component is instantiated by using TDi Technologies ConsoleWorks in the build. Remote management traffic coming through the EACMS firewall to the operations facility that is destined for one of the four monitoring server components may reach those components only via the monitoring components' EACMS. This is a component that administrators must use to configure user privileges or to access the consoles of the four components on the monitoring server. This component is connected to the consoles of each of the four applications running on the monitoring server so it can control access to these consoles and permit only those users with administrator privileges to access each console. It also records all activities that are performed on these consoles. The monitoring components' EACMS enables the monitoring server components to be configured remotely, but the tool itself cannot be configured remotely. Web interface traffic that is sent between the ICS network IDS component (O11) and a security analyst on the enterprise network must also be sent through the monitoring components' EACMS. This web interface traffic includes both SA monitoring data accessed via the ICS network IDS graphical user interface and traffic needed to remotely manage the ICS network IDS.

  The monitoring components' EACMS runs on a server that is separate and distinct from the monitoring server. This separation is necessary to ensure that the architecture does not depend solely on VMware's ability to separate applications running on it, which would be the case if the monitoring components' EACMS were on the same VMware server as the monitoring server and its components. The server on which the monitoring components' EACMS server is running cannot be remotely managed.

- PACS firewall EACMS (O1) – is instantiated in the build by using the Siemens RUGGEDCOM RX1501 component that sits on the enterprise network. It enables monitoring and configuration of user privileges on the PACS firewall (O3) in a manner similar to the monitoring components' EACMS (O19). The PACS firewall EACMS is used to remotely configure and manage the PACS firewall, i.e., the firewall that sits between the VPN concentrator (O1) and the physical access sensors (O4).

To further protect the remote management path, the reference design does not permit any components that are in the remote management path to be remotely configurable. The only way that components and software that are in the remote management path can be administered and configured is in person.

5.2.4 Protecting the Remote Path to the IDS Web Interface

As mentioned earlier, the ICS network IDS component has a web interface that facilitates remote management and access to its graphical user interface. Because a security analyst using the web interface to view SA data is expected to be located on the enterprise network rather than at the operations center, SA traffic will flow between the ICS network IDS and the enterprise network via this web interface. Security mechanisms are needed to monitor and restrict this traffic flowing into the operations center. The web interface traffic uses the same path as traffic remotely managing the monitoring server components; it relies on the same security mechanisms as those that protect the remote management path, namely the operations firewall (O1), the normally open cross-connect (O17), the EACMS firewall (O18), and the monitoring components' EACMS (O19).

5.2.5 Protecting the SIEM

The SIEM component enables information collected at the reference design's disparate sensors and monitoring components to be combined, correlated, and analyzed in a way that would not be possible when using the data from a single SA component in isolation. Aggregation of SA information in the SIEM provides enormous potential in terms of anomaly detection and increased SA. Ironically, the main strength of the reference design might serve as its vulnerability unless properly protected. If a malicious actor can penetrate the SIEM to modify or delete information, alter the processes used to analyze or visualize asset information, or alter information while in transit to the SIEM, then the very system that was designed to increase SA and make a wide variety of asset information centrally available to security analysts could be used as an attack vector. It is imperative that access to the SIEM be strictly limited to a small number of authorized users. Ideally, the integrity of the monitored information will also be protected from the points at which it is collected until it reaches the SIEM component. Ensuring the integrity and completeness of all data sent to and stored in the SIEM is essential to securing the reference design solution. If the components used to implement the reference design do not inherently provide data integrity for monitored information that is sent to the SIEM, then security will rely on enforcement of strict physical access control to ensure that attackers are not given the opportunity to access and modify/delete data that is in the SIEM or in transit to the SIEM.

It is worth noting that the absence of an SIEM does not mean that an energy organization does not have this SA information stored on its networks. Access to the SA information resides instead at disparate locations on the network. Energy services organizations still need to safeguard this SA information in the various locations where it is generated and stored, and while in transit.

5.2.5.1 Controlling access to the SIEM

Only highly privileged users should be permitted to log into the SIEM. No users should be permitted to modify SA data that is being stored on this component. Monitoring, logging, and auditing of all console activity performed on this component is essential to ensuring that authorized users are not performing unauthorized activities on this component. Periodic reports should be generated, listing all users who logged into the SIEM component and activities performed.

5.2.5.2 SIEM data verification

Mechanisms are needed to help ensure that information collected or generated at a collection component is sent to and received by the SIEM, i.e., that the SIEM receives all of the monitored information that it should. If a malicious actor were to disable a sensor without the reference design being alerted, serious harm could result. Mechanisms are needed to ensure that if a monitoring or collection system is disabled or otherwise unable to send information to the SIEM, or if monitored information is deleted before reaching the SIEM, the absence of this information will be detected so that the situation can be remedied. Ideally, liveness checks for each of the devices on the enterprise network that report directly to the SIEM can be built into the SIEM, so that if heartbeat messages or other expected updates are not received at the expected intervals, alerts will be generated.

To the extent possible, these checks may be configured and implemented with the reference design components themselves. For example, ArcSight, the SIEM used in the build, can be configured to generate alerts when it does not receive data. However, this mechanism is not foolproof. Configuration of the SIEM requires that ArcSight alerts be tuned by using a baseline of received data. Accuracy of the alerts depends on the extent to which the data that is sent mimics the baseline used to tune the SIEM. There is no guarantee that every item of information that is dropped would be detected. If monitoring devices are generating heartbeat messages, the SIEM could be equipped with a script to enable it to detect missing messages and thereby infer that either a monitoring device or its communication channel to the SIEM is not operational.

The SIEM cannot be expected to detect failure of monitoring devices that do not report directly to it. If a sensor reports to an intermediate system rather than directly to the SIEM itself, the intermediate system must be involved in detecting the potential failure of the sensor. There needs to be a way for the SIEM and all intermediate components in the reference design to know if the sensors that report to them are alive and well. Having sensors send heartbeats is one example of how such a liveness detection mechanism could be implemented. Mechanisms should be designed for each sensor type so that the sensor’s liveness can be validated and an alert can be generated when the sensor fails. For example, if the ICS access management system on the enterprise network does not receive an update from the ICS access management system on the operations network, it should generate an alert. Similarly, if the log collector/aggregator in the monitoring server detects that it has not received a log message that was sent to it by one of the monitoring components, it should be configured to generate an alert.

The ability to detect sensor failure is complicated by the unidirectional nature of the data transfer from the operations network to the enterprise network. This one-way transfer of information prevents components on the enterprise network from trying to ping sensors on the operational network. Given this constraint, it might make most sense to have a designated application in the operations network that is responsible for tracking the health of all monitoring devices and periodically sending a status report regarding sensor health to the enterprise network. Given that it is already receiving information from all monitoring components on the operational network, the log collector/aggregator component is a good candidate location for implementing such a centralized sensor health tracking service in the operations network.

5.2.5.3 Information integrity protection

If SA information were to be deleted, modified, or falsified, whether in transit or at rest, the result could be catastrophic. Access to each reference design component and especially the SIEM must be protected to prevent modification or deletion of collected SA information. Although end-to-end integrity protection for data at rest and for data in transit is desirable, such comprehensive protection is not a component of this reference design.

As a compensating mechanism, a malicious actor must be local to the operations network to compromise the integrity of monitored information that is on the operations network because monitoring data is not permitted to enter the operations network from outside; all data paths for monitoring data are outbound. (Note that the build’s support of a web interface for monitoring ICS network IDS data via a graphical user interface violates this principle.) While this leaves the potential for malicious activity by an actor who is an authorized user on the operations network, this approach greatly reduces component threat exposure. The reference design’s use of a VPN protects data integrity and confidentiality while data is in route between the operations facility and the enterprise facility.

Within the enterprise network, all data in transit to the SIEM can have its integrity protected by using ArcSight connectors that have integrity checking (and/or encryption) enabled. Such use of integrity-checking connectors between all components and ArcSight might take care of integrity protection for data in transit within the enterprise network. However, there does not seem to be an equivalent general solution for protecting data in transit within the operations network. If ArcSight connectors were to be used to send syslog, historian, or other monitored data to the SIEM from the operations network, the integrity of the received data could be validated at the SIEM. However, because of the unidirectional nature of the one-way transfer between the operations network and the enterprise network, there would be no way for the SIEM to become aware that it has lost its connection to the source if the communication network should fail.

In much the same way that mechanisms are needed for each sensor type to ensure that the sensor’s liveness can be validated, mechanisms for ensuring the integrity of each type of monitored data are also needed. Each data transfer in the reference design should be protected with integrity mechanisms to ensure that any loss or modification of data that occurs during the transfer will be detected: the integrity of historian data sent from the operations historian component to the enterprise historian component, the integrity of information sent from the ICS asset management system sensor on the operations network to the ICS asset management system server and network visualization tool on the enterprise network, the integrity of door open and close events sent from the physical access sensor on the operations network to the PACS on the enterprise network, and the integrity of syslog data sent from the log collector/aggregator on the operations network to the log collector/aggregator on the enterprise network.

Syslog data can, in theory, be encrypted to ensure the integrity of the log data, assuming the individual products used to implement the reference design support syslog encryption. However, relying on syslog encryption to protect the integrity of data sent from monitoring devices to the SIEM suffers from the same drawback as would relying on ArcSight encryptors: If the communication network between the operations network and the enterprise network fails, the SIEM would not have any way to be alerted to this failure, and log data that is in transit between the two networks would be dropped. Instead, the proposed solution for the reference design is for the log collector/aggregator on the operations network to collect all syslog data sent from other monitoring components and apply an integrity seal to this syslog information. The integrity seal is applied not only to the syslog record but also to the entire log file up to that point, so it protects the record's place in the file in addition to protecting the content of the record. The operations network instance of the log collector/aggregator sends syslog records to the enterprise network instance of the log collector/aggregator. The enterprise instance of the log collector/aggregator applies equivalent integrity seals to the received records. Should a question arise about the integrity of syslog records, both the operations and enterprise log collector/aggregators can validate the integrity of the records they hold. Further, a comparison could be made between operations and enterprise records. Because the log records are stored in a log collector/aggregator on the operations network instead of sent directly to the enterprise network from each of the monitoring devices that generate them, these log records will not be dropped or lost if the communication channel between the operations and enterprise networks fails.

5.3 Securing an Operational Deployment

When deploying the SA reference design in a live, operational environment, it is essential that organizations follow security best practices to address potential vulnerabilities, ensure that all assumptions that the solution relies upon are valid, and minimize any risk to the operational ICS network. Note that the laboratory instantiation of the reference architecture builds did not implement every security recommendation. The following list of best practices recommendations are designed to reduce this risk but should not be considered comprehensive. Merely following this list will not guarantee a secure environment:

- Test individual components to ensure that they provide the expected Cybersecurity Framework Subcategory support and that they do not introduce potential vulnerabilities. For example, the taps deployed should be tested to verify that they are passive, i.e., that when power is turned off to them, they do not disrupt the flow of traffic on the network on which they are deployed. They should also be tested to validate that they permit data to flow in only one direction, ensuring that they cannot be used as an entry point for malicious traffic to enter the network that is being monitored by the taps.

- Harden all components: All components should be deployed on securely configured operating systems that use long and complex passwords and are configured according to best practices.
- Scan operating systems for vulnerabilities.
- Keep operating systems up-to-date on patching, version control, and monitoring indicators of compromise by performing, for example, virus and malware detection.
- Maintain all components in terms of ensuring that all patches are promptly applied, anti-virus signatures are kept up-to-date, indicators of compromise are monitored, etc. (patches should be tested before they are applied).
- Change the default password when installing software.
- Identify and understand what predefined administrative and other accounts each component comes with by default to eliminate any inadvertent back doors into these components. These accounts must be disabled and, even though they are disabled, their default passwords must also be changed to complex passwords.
- On key devices that protect the ICS network (e.g., the ICS firewall and the historian firewall) and that are on the remote management path, the number of accounts on these devices should be limited, ideally, to one specific administrator and a backup account. As is the case in the reference design, all components on the remote access path should be configurable only in person.
- Implement mechanisms to monitor the ICS and historian firewalls.
- Organizations leveraging the reference design solution should conduct their own evaluations of their implementation of the solution.
- All reference design components that are designed to detect anomalies and identify potential areas of concern with the use of analysis tools should be equipped with as comprehensive a set of rules as possible to take full advantage of the analysis and anomaly detection capabilities of each component. The rules that are implemented must be consistent across components, and they must enforce the organization’s security policies as fully and accurately as possible. The SIEM should be configured with rules indicating the ICS systems, software, applications, connections, devices, values, and activities that are authorized to enable it to ensure that only authorized personnel, connections, devices, and software are on the ICS network.
- Identity and access management and IT asset management security infrastructures should be put into place that will protect the reference design solution (namely, control access to each

reference design component and especially to the SIEM component) and help ensure that the information fed into the SIEM component is complete and unmodified.

- The access control policies for the SIEM component should be designed to enforce best security practices such as the principles of least privilege and separation of duties, and these policies should be devised so that they can detect anomalous behavior or information that could indicate a security breach. Access to this component should require authentication and use of long and complex passwords. SA data stored in this component should be read-only with any attempt to modify or delete information generating security alerts and log entries.
- Firewall configurations should be verified to ensure that data transmission is limited to those interactions that are needed to support sending information from various data-gathering components to the SIEM component and to analysis components as explicitly indicated in the reference design flow diagram. In addition, the intercomponent connections that are permitted should be restricted to specific IP address and port combinations.
- Physical access to both the operations and the enterprise networks should be strongly controlled.
- If possible, SA information sent from the monitoring components to the SIEM component should have integrity-checking mechanisms applied to enable detection of tampering. Integrity mechanisms should conform to most recent industry best practices.
- All components of the reference design solution should be installed, configured, and used according to the guidance provided by the component vendor.
- Only a very few users (superadministrators) should be designated to have the ability to control (initiate, modify, or stop) the types of information that each monitoring component collects and sends to the SIEM. Any changes made to the types of information to be monitored by or sent from any given collection component or device should, by policy, require approval of more than one individual, and these changes must themselves be reported to the SIEM component.
- Whenever a superadministrator logs into or out of a collection component, these events must be reported to and logged at a “monitor of monitors” system as well as to the SIEM component. Upon logging in and logging out, a list of the types of information that the midtier device will report to the SIEM component should be sent so that any permanent changes that the superadministrator has made to this list can be detected.
- Ideally, it should not be possible for anyone, including superadministrators, to modify the logging policies on any collection component so that a change to the list of information reported to the SIEM component would not itself be reported. However, this might not be how collection components are implemented. Therefore, it is imperative that a configuration management component that is part of a monitor-of-monitors system be configured to frequently validate and enforce such reporting at all collection devices. Furthermore, access to the configuration management component must be strictly controlled to ensure that its configuration is not changed so that it will not enforce reporting of configuration changes at all other midtier devices.

- Superadministrator access to the configuration management component should, by policy, require more than two individuals. All changes made during superadministrator access to the configuration management component should be reviewed by more than two individuals.

5.4 Security Evaluation Summary

The SA reference design's integration, consolidation, and display of the SA information enables converged, efficient, and quick access to the variety of SA information that is collected, enabling better SA. In addition, consolidation of disparate types of PACS, IT, and OT information in a single location (the SIEM) enables the organization to correlate and analyze different types of monitored information in a way that is not possible when analyzing different categories of information in isolation, enabling security incidents to be detected and responded to in a timely and prioritized fashion. This consolidation, combined with the ability to apply rules-based analysis to the information, makes it possible for the SA system to automatically detect anomalous situations that might indicate a security breach that would otherwise have been impossible to detect by any single component of the system working in isolation.

6 Functional Evaluation

We conducted a functional evaluation of the SA example solution to verify that several common key provisioning functions of the example solution, as implemented in our laboratory build, worked as expected. The SA workflow capability demonstrated the ability to:

- implement a converged alerting capability to provide a comprehensive view of cyber-related events and activities
- utilize commercially available products to achieve the comprehensive view
- provide a converged and comprehensive platform that can alert utilities to potentially malicious activity

Section 6.1 explains the functional test plan in more detail and lists the procedures used for each of the functional tests.

6.1 SA Functional Test Plan

This test plan includes the test cases necessary to conduct the functional evaluation of the SA use case. The SA implementation is currently in a split deployment setup, with part of the lab at the NCCoE (enterprise side) and the other at the University of Maryland (operations side). Section 5 describes the test environment. Each test case consists of fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 6-1 provides a template of a test case, including a description of each field in the test case.

Table 6-1 Functional Test Plan

Test Case Field	Description
Parent requirement	identifies the top-level requirement or series of top-level requirements leading to the testable requirement
Testable requirement	drives the definition of the remainder of the test case fields; specifies the capability to be evaluated
Cybersecurity Framework Categories	associated Subcategories from the NIST SP 800-53 rev 4 Cybersecurity Framework controls addressed by the test case
Description	describes the objective of the test case
Associated test cases	A test case might be based on the outcome of another test case(s), e.g., analysis-based test cases produce a result that is verifiable through various means such as log entries, reports, and alerts.
Preconditions	indicates various starting-state items, such as a specific capability configuration or a specific protocol and content
Procedure	actions required to implement the test case, e.g., a single sequence of steps or sequences of steps (with delineation) to indicate variations in the test procedure
Expected results	the specific expected results for each variation in the test procedure
Actual results	the actual observed results compared with the expected results
Overall result	the overall result of the test as a pass/fail. In some instances, determination of the overall result might be more involved, such as determining pass/fail based on a percentage of errors identified.

6.2 SA Use Case Requirements

This section identifies the SA functional evaluation requirements that are addressed by using this test plan. Table 6-2 lists those requirements and associated test cases.

Table 6-2 Functional Evaluation Requirements

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 1	The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk.		
CR 1.a		IT	SA-2, SA-3, SA-4, SA-6
CR 1.b		OT	SA-1, SA-3, SA-4, SA-5, SA-6
CR 1.c		PACS	SA-1, SA-3
CR 2	The SA system shall include an SA workflow capability that increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions.		
CR 2.a		IT	SA-2
CR 2.b		OT	
CR 2.c		PACS	
CR 3	The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned.		
CR 3.a		IT	SA-1, SA-5, SA-6
CR 3.b		OT	SA-6

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 3.c		PACS	SA-1
CR 4	The SA system shall include an SA workflow capability that simplifies regulatory compliance by automating generation and collection of a variety of operational log data.		
CR 4.a		IT	SA-5
CR 4.b		OT	
CR 4.c		PACS	

6.3 Test Case: SA-1

Table 6-3 Test Case ID: SA-1

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS (CR 3) The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned. (CR 3.a) IT, (CR 3.c) PACS
Testable Requirement	(CR 1.b) OT, (CR 1.c) PACS, (CR 3.a) IT, (CR 3.c) PACS
Description	Show that the SA solution can monitor for door access and correlate to badge used. Show that the SA solution recognizes OT device going offline and alert IT network to anomalous condition. Show that the SA solution can correlate time frame between door access and OT device going offline.

Associated Test Cases	Event Correlation — OT and PACS: Technician accesses substation/control station, and OT device goes down. Alert of anomalous condition and subsequently correlate to PACS to see who accessed facility.
Cybersecurity Framework Categories	DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-2, PR.AC-2
Preconditions	▪ SA solution is implemented and operational in both operations and enterprise network. ▪ Ensure door controllers are properly installed and configured.
Procedure	1. At operations network, open door leading to lab network to create door open event. 2. Once inside, unplug a connection from one of the network taps to the aggregating switch (this is to simulate an ICS device being disconnected). 3. Monitor SIEM for correlation activity.
Expected Results (pass)	1. CyberLens system recognizes missing device(s) and notifies SIEM. 2. AccessIt! updates SIEM of door activity. 3. SIEM correlates timing between door activity and device(s) missing. 4. SIEM generates alert accordingly.
Actual Results	1. CyberLens system is alerted to a device offline. 2. AccesIt! is alerted to door open event. 3. SIEM shows each individual alert, along with timing between the alerts.
Overall Result	PASS

6.4 Test Case: SA-2

Table 6-4 Test Case ID: SA-2

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT (CR 2) The SA system shall include an SA workflow capability that increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions. (CR 2.a) IT
Testable Requirement	(CR 1.a) IT, (CR 2.a) IT
Description	Show that the SA solution can monitor user input for validity. Show that the SA solution can actively defend against software-based attacks. Show that the SA solution can alert IT to potential attacks.
Associated Test Cases	Event Correlation — OT and IT: Enterprise (IT) Java application communication with OT device (historian) and used as a vector for SQLi
Cybersecurity Framework Categories	DE.AE-1, DE.AE-2, DE.CM-1, DE.CM-4
Preconditions	▪ Web application running Java is installed. ▪ Web application is connected to a database. ▪ Web application server is installed and used to run Java-based web application.
Procedure	1. Connect to web application to query database. 2. Attempt a normal query for data. 3. Attempt a malicious query for data exfiltration.

Expected Results (pass)	1. The database should return normal results when a normal query is initiated. 2. The web application should return no results when a malicious query is initiated. 3. SIEM should be alerted by Waratek upon receipt of a malicious query.
Actual Results	1. Normal queries yielded normal results as expected. 2. Malicious queries yielded warnings and no results from web interface. 3. SIEM was alerted of malicious queries by Waratek and displayed malicious queries in dashboard.
Overall Result	PASS

6.5 Test Case: SA-3

Table 6-5 Test Case ID: SA-3

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Testable Requirement	(CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Description	Show that the SA solution can monitor network traffic inside the operations network. Show that the SA solution can alert to IP addresses not in expected ranges. Show that the SA solution can alert on failed logins above a given threshold. Show that the SA solution can correlate aforementioned anomalous behavior and alert analyst accordingly.
Associated Test Cases	Event Correlation — OT and IT/PACS-OT: Unauthorized access attempts detected and alerts triggered based on connection requests from a device on the SCADA network destined for an IP that is outside the SCADA IP range. This test case focuses on the possibility of a malicious actor attempting to gain access to an OT device via the enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.

Cybersecurity Framework Categories	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-7
Preconditions	▪ Waterfall Unidirectional Security Gateway is configured to replicate traffic one way out of the operations network. ▪ ConsoleWorks is configured with authorized user access requirements.
Procedure	1. Attempt authorized login to operations device. 2. Attempt unauthorized login to operations device. 3. Connect laptop to Powerconnect 7024 switch and attempt communication on network.
Expected Results (pass)	1. Allows connection to operations device from authorized users. 2. Alerts on threshold of unauthorized logins/failed login attempts to operations device. 3. Alerts to new device found on network. 4. Blocks attempts of communication from new device to other network devices.
Actual Results	1. ConsoleWorks connections are allowed from authorized users to OT devices. 2. OT devices alert on failed login attempts. 3. SIEM alerts are shown in dashboard for failed login attempts.
Overall Result	PASS

6.6 Test Case: SA-4

Table 6-6 Test Case ID: SA-4

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company’s ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS

Testable Requirement	(CR 1.a) IT, (CR 1.b) OT, (CR 1.c) PACS
Description	Show that the SA solution can utilize behavioral patterns to recognize anomalous events inside respective networks. Show that the SA solution can alert analysts to behavioral anomalies within respective networks.
Associated Test Cases	Data Exfiltration Attempts: Examine behavior of systems; configure SIEM to alert on behavior that is outside the normal baseline. Alerts can be created emanating from OT, IT, and PACS. This test case seeks alerting based on behavioral anomalies rather than recognition of IP addresses.
Cybersecurity Framework Categories	DE.AE-1, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-7
Preconditions	▪ established baselines in operations network ▪ Ensure continued monitoring of modeled behavior in operations network.
Procedure	1. Inject new IP addresses into established baseline sensor for operations network. 2. Inject anomalous network traffic (previously unreported protocols) into baseline sensor. 3. Manipulate enterprise historian to show anomalous data/tags being stored. 4. Replicate network traffic to show higher volume than normal in baseline.
Expected Results (pass)	1. CyberLens acknowledges unknown IP address and/or protocols and reports to SIEM. 2. ICS2 recognizes changes within historian to detect anomalous industrial control behavior and alerts SIEM. 3. ICS2 recognizes uptick in historian activity and alerts SIEM. 4. CyberLens recognizes uptick in network activity and alerts SIEM. 5. SIEM aggregates alerts and notifies analyst.

Actual Results	1. CyberLens alerts to both unknown new IP address as well as new protocols. 2. unable to manipulate enterprise historian with current setup 3. CyberLens alerted to changes in network traffic. 4. SIEM aggregated alerts and showed alerts on dashboard.
Overall Result	PARTIAL PASS

6.7 Test Case: SA-5

Table 6-7 Test Case ID: SA-5

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.b) OT (CR 3) The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned. (CR 3.a) IT, (CR 3.b) OT (CR 4) The SA system shall include an SA workflow capability that simplifies regulatory compliance by automating generation and collection of a variety of operational log data. (CR 4.a) IT, (CR 4.b) OT
Testable Requirement	(CR 1.b) OT, (CR 3.a) IT, (CR 3.b) OT, (CR 4.a) IT
Description	Show that the SA solution can detect when anomalous types of network traffic communicate with devices.
Associated Test Cases	Configuration Management: unauthorized (inadvertent or malicious) uploading of an ICS network device configuration. Alert will be created to notify SIEM that this has occurred. Detection method will be based primarily on inherent device capability (i.e., log files).
Cybersecurity Framework Categories	DE.AE-1, DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-7, ID.AM-2

Preconditions	Baseline established for operations network
Procedure	1. Connect through VPN to operations monitoring network. 2. Inject file into network traffic to mimic unauthorized/unseen protocols between monitored components.
Expected Results (pass)	1. iSID recognizes anomalous network traffic and alerts SIEM. 2. SIEM aggregates alerts and notifies analyst.
Actual Results	1. iSID shows alert for injected data. 2. SIEM aggregated alerts from iSID and displayed on dashboard.
Overall Result	PASS

6.8 Test Case: SA-6

Table 6-8 Test Case ID: SA-6

Parent Requirement	(CR 1) The SA system shall include an SA workflow capability that improves a company's ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk. (CR 1.a) IT, (CR 1.b) OT (CR 3) The SA system shall include an SA workflow capability that improves accountability and traceability, leading to valuable operational lessons learned. (CR 3.a) IT, (CR 3.b) OT
Testable Requirement	(CR 1.a) IT, (CR 1.b) OT, (CR 3.a) IT, (CR 3.b) OT
Description	Show that the SA solution can detect and notify on introduction of an unknown device to ICS network. Show that the SA solution can notify analyst of unknown device.
Associated Test Cases	Rogue Device Detection: Alerts are triggered by introduction of any device onto the ICS network that has not been registered with the asset management capability in the build.

Cybersecurity Framework Categories	DE.AE-1, DE.AE-3, DE.CM-2, DE.CM-7, ID.AM-1, PR.AC-2
Preconditions	Baseline established for operations network.
Procedure	1. Connect previously unknown device to network tap aggregation switch. 2. Create IP address on unknown device within known IP address range. 3. Send spoofed traffic to monitor.
Expected Results (pass)	1. CyberLens recognizes anomalous network device and alerts SIEM. 2. SIEM aggregates alerts and notifies analyst.
Actual Results	1. CyberLens recognized new device on network and alerted SIEM. 2. SIEM aggregated alerts from CyberLens in dashboard and notified analyst.
Overall Result	PASS

Appendix A List of Acronyms

CR	Capability Requirement
CRADA	Cooperative Research and Development Agreement
DE.AE	Anomalies and Events Category of the Detect Function Area
DE.CM	Security Continuous Monitoring Category of the Detect Function Area
E1	Siemens RUGGEDCOM RX1400
E2	Dell Server Cluster
E3	VMware
E4	OSIsoft Pi Historian
E5	OnGuard
E6	ConsoleWorks
E7	RS2 AccessIT!
E8	CyberLens Server
E9	Siemens RUGGEDCOM CROSSBOW
E10	Waratek Runtime Protection
E11	Separate Server in the Lab, Gosting HPE ArcSight (E12)
E12	HPE ArcSight
E13	RSA SecOps
EACMS	Electronic Access Control and Monitoring System
HPE	Hewlett Packard Enterprise
ICS	Industrial Control System
ID.AM	Asset Management Category of the Cybersecurity Framework Identify Function Area
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
NCCoE	National Cybersecurity Center of Excellence
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
O1	Siemens RUGGEDCOM RX1501
O2	Waterfall Security Solutions, Ltd. Unidirectional Security Gateway
O3	Schneider Electric Tofino Firewall

O4	RS2 Door Controller
O5	TDi Technologies ConsoleWorks
O6	Dell R620 Server
O7	VMware
O8	OSIsoft Pi Historian
O9	TDi Technologies ConsoleWorks
O10	CyberLens Sensor
O11	Radiflow iSID
O12	Dedicated Physical Server Isolated from the Citect SCADA system (U1)
O13	OSIsoft Citect Interface Software
O14	Radiflow 3180 Firewall
O15	Cisco 2950 Network Switch
O16	IXIA Full duplex Taps
O17	Waterfall Secure Bypass Switch
O18	Schneider Electric Tofino Firewall
O19	Linux Server
O20	Schneider Electric Tofino Firewall (Historian Firewall)
OT	Operational Technology
PAC	Physical Access Control
PACS	Physical Access Control Systems
PDP	Policy Decision Point
PEP	Policy Enforcement Point
RMF	Risk Management Framework
SA	Situational Awareness
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SP	Special Publication
SQL	Structured Query Language
SQLi	Structured Query Language Injection
U1	Citect SCADA system
UMD	University of Maryland
VPN	Virtual Private Network

Appendix B References

[1] M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” *Human Factors*, vol. 37, no. 1, pp. 32–64, March 1995.

[2] *Risk Management Framework (RMF) – Frequently Asked Questions, Roles and Responsibilities,* and *Quick Start Guides*, National Institute of Standards and Technology (NIST): Computer Security Resource Center, Gaithersburg, Md. Available: http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/.

[3] The IT Law Wiki: FANDOM Powered by Wikia. *Cyber situational awareness*. Available: http://itlaw.wikia.com/wiki/Cyber_situational_awareness.

[4] NIST. Cybersecurity Framework — Standards, guidelines, and best practices to promote the protection of critical infrastructure. Available: http://www.nist.gov/itl/cyberframework.cfm.

NIST SPECIAL PUBLICATION 1800-7C

Situational Awareness

For Electric Utilities

Volume C:
How-to Guides

Jim McCarthy
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Otis Alexander
Sallie Edwards
Don Faatz
Chris Peloquin
Susan Symington
Andre Thibault
John Wiltberger
Karen Viani
The MITRE Corporation
McLean, VA

August 2019

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP1800-7

The first draft of this publication is available free of charge from:
https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-7C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-7C, 173 pages, (August 2019), 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 energy_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 IT 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 and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

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 Series 1800) 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

Through direct dialogue between NCCoE staff and members of the energy sector (composed mainly of electric power companies and those who provide equipment and/or services to them) it became clear that energy companies need to create and maintain a high level of visibility into their operating environments to ensure the security of their operational resources (operational technology [OT]), including industrial control systems (ICS), buildings, and plant equipment. However, energy companies, as well as all other utilities with similar infrastructure and situational awareness challenges, also need insight into their corporate or information technology (IT) systems and physical access control systems (PACS). The convergence of data across these three often self-contained silos (OT, IT, and PACS) can better protect power generation, transmission, and distribution.

Real-time or near-real-time situational awareness is a key element in ensuring this visibility across all resources. Situational awareness, as defined in this use case, is the ability to comprehensively identify and correlate anomalous conditions pertaining to ICS, IT resources, and access to buildings, facilities, and other business mission-essential resources. For energy companies, having mechanisms to capture, transmit, view, analyze, and store real-time or near-real-time data from ICS and related networking equipment provides energy companies with the information needed to deter, identify, respond to, and mitigate cyber attacks against their assets.

With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remedy them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping demonstrate compliance with information security standards. This NCCoE project's goal is ultimately to improve the security of operational technology through situational awareness.

This NIST Cybersecurity Practice Guide describes our collaborative efforts with technology providers and energy sector stakeholders to address the security challenges that energy providers face in deploying a comprehensive situational awareness capability. It offers a technical approach to meeting the challenge and also incorporates a business value mind-set by identifying the strategic considerations involved in implementing new technologies. The guide provides a modular, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how we met the challenge by using open-source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case is based on an everyday business operational scenario that provides the underlying impetus for the functionality presented in the guide. Test cases were defined with industry participation to provide multiple examples of the capabilities necessary to provide situational awareness.

While the example solution was demonstrated with a certain suite of products, the guide does not endorse these products. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost effectively with an energy provider's existing tools and infrastructure.

KEYWORDS

correlated events; cybersecurity; energy sector; information technology; operational technology; physical access control systems; security information and event management; situational awareness

ACKNOWLEDGMENTS

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

Name	Organization
Pam Johnson	TDi
Clyde Poole	TDi
Eric Chapman	University of Maryland, College Park
David S. Shaughnessy	University of Maryland, College Park
Don Hill	University of Maryland, College Park
Mary-Ann Ibeziako	University of Maryland, College Park
Damian Griffe	University of Maryland, College Park
Mark Alexander	University of Maryland, College Park
Nollaig Heffernan	Waratek
James Lee	Waratek
John Matthew Holt	Waratek
Andrew Ginter	Waterfall
Courtney Schneider	Waterfall
Tim Pierce	Waterfall
Kori Fisk	The MITRE Corporation
Tania Copper	The MITRE Corporation

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	Build Involvement
Dragos	CyberLens
Hewlett Packard Enterprise (HPE)*	ArcSight
ICS2	OnGuard
OSIsoft	PI Historian
Radiflow	iSIM
RS2 Technologies	Access It!, Door Controller
RSA, a Dell Technologies business	Archer Security Operations Management
Schneider Electric	Tofino Firewall
Siemens	RUGGEDCOM CROSSBOW
TDi Technologies	ConsoleWorks
Waratek	Waratek Runtime Application Protection
Waterfall Security Solutions	Unidirectional Security Gateway, Secure Bypass

**Please note: HPE in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.*

The NCCoE also wishes to acknowledge the special contributions of the University of Maryland for providing us with a real-world setting for the situational awareness build; Project Performance Company for its dedication in assisting the NCCoE with the very challenging and complex integration in this build; and the NCCoE Energy Provider Community for its patience, support, and guidance throughout the life cycle of this project.

Contents

List of Figures

List of Tables

1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not recreate the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to situational awareness. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-7A: *Executive Summary*
- NIST SP 1800-7B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-7C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary* (NIST SP 1800-7A), which describes the following topics:

- challenges enterprises face in maintaining cross-silo situational awareness
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-7B, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Risk, provides a description of the risk analysis we performed.
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary,* NIST SP 1800-7A, with your leadership team members to help them understand the importance of adopting a standards-based situational awareness solution.

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use the How-To portion of the guide, NIST SP 1800-7C, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT 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 a solution that includes physical access control systems (PACS) operational technology (OT), IT systems, and business processes. 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. Volume B, Section 3.5, Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

1.2 Build Overview

Energy sector colleagues shared that they need to know when cybersecurity events occur throughout the organization. Additionally, the information about such events must correlate data among various sources before arriving at a converged platform. Security staff need to be aware of potential or actual cybersecurity incidents in their IT and OT systems and PACS and to view these alerts on a single converged platform. Furthermore, the ability to drill down, investigate, and subsequently fully remedy or effectively mitigate a cybersecurity incident affecting any or all of the organization is essential.

1.3 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 detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, on-screen 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.

1.4 Logical Architecture Summary

NIST Special Publication (SP) 1800-7B describes an example solution consisting of a monitoring/data collection component, which is deployed to operations facilities such as substations and generating plants; and a data aggregation/analysis component that is deployed as a single service for the enterprise. Data is collected from the industrial control systems (ICS) network by the monitoring/data collection component and sent to the data aggregation/analysis component. NIST SP 1800-7B also presents an architecture for building an instance of the example solution by using commercial products. That architecture is depicted in Figure 1-1 and Figure 1-2 below.

Figure 1-1 Monitoring and Data Collection Lab Build Architecture

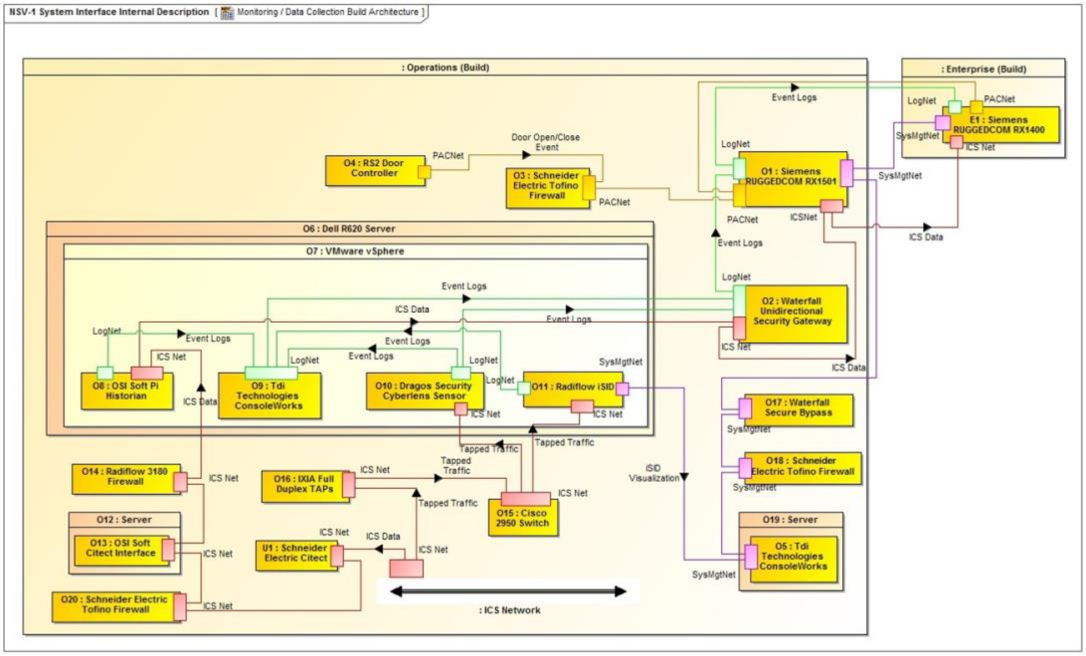
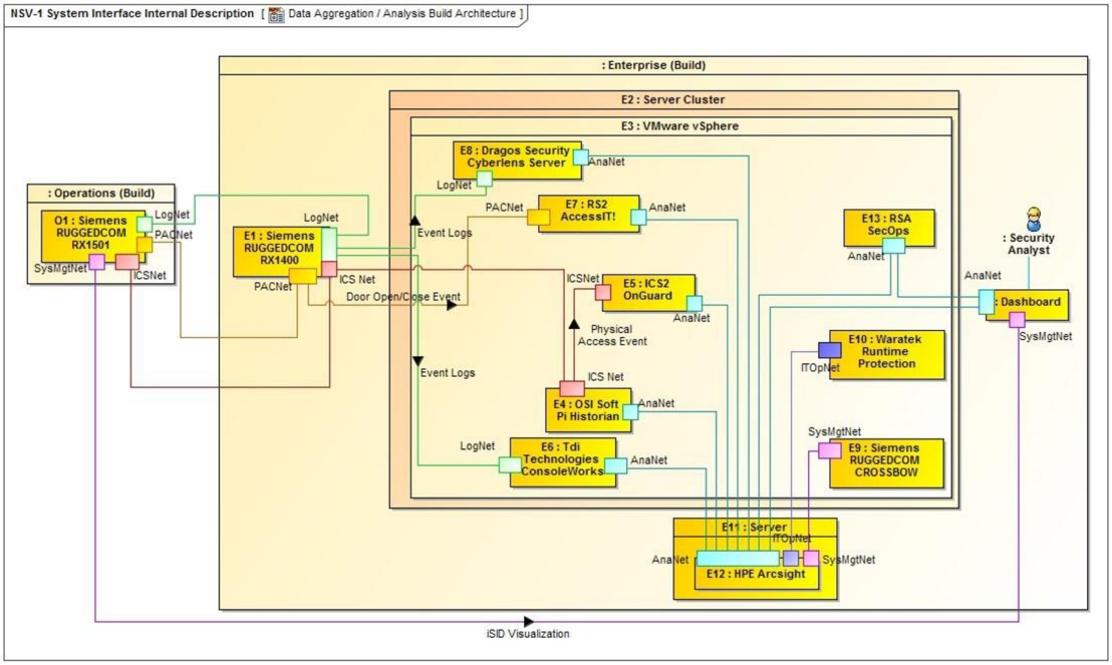


Figure 1-2 Data Aggregation and Analysis Lab Build Architecture



This practice guide provides detailed instructions on installing, configuring, and integrating the products used to build an instance of the example solution. The role of each product in the example solution is described in NIST SP 1800-7B, Section 4, Architecture.

1.5 Wiring Diagrams

The architecture diagrams in the previous section present the logical connections needed among the products used to build an instance of the example solution. This section describes the physical wiring that implements those logical connections.

Figure 1-3 Enterprise Lab Wiring Diagram

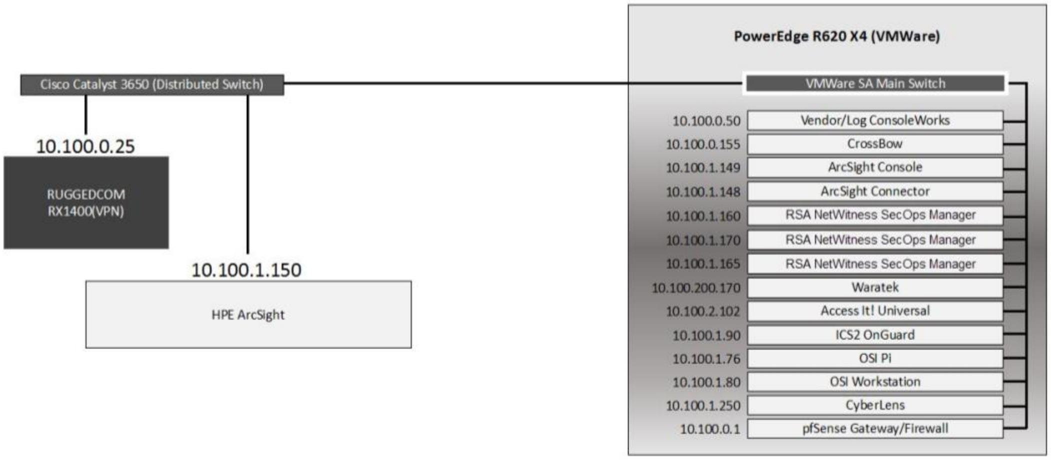
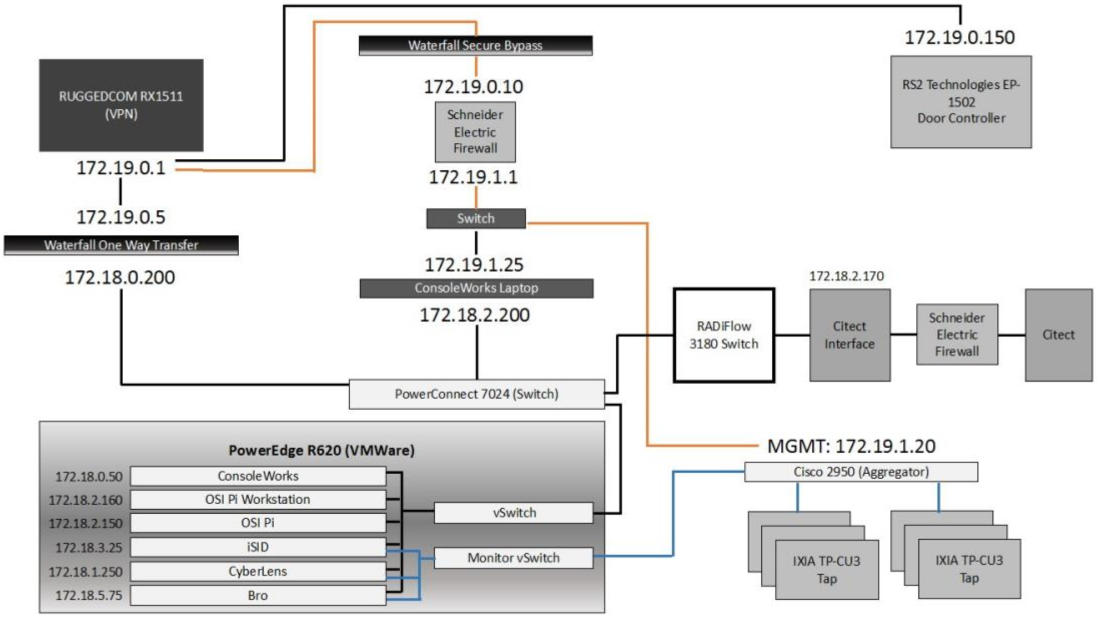

Cisco Catalyst 3650 (Distributed Switch)
10.100.0.25
RUGGEDCOM RX1400(VPN)
10.100.1.150
HPE ArcSight
PowerEdge R620 X4 (VMWare)
VMWare SA Main Switch
10.100.0.50 Vendor/Log ConsoleWorks
10.100.0.155 CrossBow
10.100.1.149 ArcSight Console
10.100.1.148 ArcSight Connector
10.100.1.160 RSA NetWitness SecOps Manager
10.100.1.170 RSA NetWitness SecOps Manager
10.100.1.165 RSA NetWitness SecOps Manager
10.100.200.170 Waratek
10.100.2.102 Access It! Universal
10.100.1.90 ICS2 OnGuard
10.100.1.76 OSI Pi
10.100.1.80 OSI Workstation
10.100.1.250 CyberLens
10.100.0.1 pfSense Gateway/Firewall

Figure 1-4 Cogeneration Facility Lab Network Diagram



2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all of the products used to build an instance of the example solution. Product installation information is organized alphabetically by vendor with one section for each instance of the product. The section heading includes the unique product instance identifier used in the example solution architecture diagrams. Those identifiers have the form “Ln” where L is a letter and n is a number. Three different letters are used in the example solution architecture diagrams:

- **En** identifies a product instance installed in the enterprise portion of the build constructed in the NCCoE energy sector lab. For example, **E1** is the Siemens RUGGEDCOM RX1400 installed in the NCCoE lab.
- **On** identifies a product instance installed in the operations portion of the build constructed in the build partner’s cogeneration facility. For example, **O1** is the Siemens RUGGEDCOM RX1501 installed in the build partner’s cogeneration facility.
- **Un** identifies a product instance that is an existing part of the build partner’s cogeneration facility. For example, **U1** is the Citect supervisory control and data acquisition (SCADA) controller that is part of the build partner’s cogeneration facility control system.

If the build contains multiple instances of the same product installed in nominally the same way, the full installation instructions are presented for one instance. Only the differences in installation and configuration are presented for the additional instances. For example, the build includes three instances of TDi Technologies ConsoleWorks (O5, O9, E6). Full installation instructions are provided for the E6 instance of TDi Technologies ConsoleWorks. The instructions provided for the O5 and O9 instances describe only the differences between those instances and the E6 instance.

2.1 Cisco 2950 (O15)

The Cisco 2950 switch is used to aggregate the IXIA network taps (O16). The configuration file is presented in the following subsection.

2.1.1 Cisco 2950 (O15) Installation Guide

```
Using 1904 out of 32768 bytes

!

version 12.1

no service pad

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname aggregator

!

aaa new-model

enable secret 5 $1(s*tC$RHcpvnJts/adF.ONLSK32.

enable password C1sc0

!

username admin privilege 15 secret 5 $1*.1Gz$nHZ.CVIlq28oMB46m2X8k/

ip subnet-zero

!

ip domain-name lab-mgmt

ip ssh time-out 120

ip ssh authentication-retries 3

ip ssh version 2

!

spanning-tree mode pvst

no spanning-tree optimize bpdu transmission

spanning-tree extend system-id

!
```

```
!
!
!
interface FastEthernet0/1
no keepalive
speed 100
!
interface FastEthernet0/2
no keepalive
speed 100
!
interface FastEthernet0/3
no keepalive
!
interface FastEthernet0/4
no keepalive
!
interface FastEthernet0/5
no keepalive
!
interface FastEthernet0/6
no keepalive
!
interface FastEthernet0/7
no keepalive
!
interface FastEthernet0/8
no keepalive
!
interface FastEthernet0/9
no keepalive
!
interface FastEthernet0/10
no keepalive
!
```

```
interface FastEthernet0/11
no keepalive
!
interface FastEthernet0/12
no keepalive
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
switchport mode trunk
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport access vlan 1000
switchport mode access
!
interface FastEthernet0/25
!
```

```
interface FastEthernet0/26
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan1000
ip address 172.19.1.20 255.255.254.0
no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
password -1pqla,zMXKSOW)@
transport input ssh
line vty 5 15
password -1pqla,zMXKSOW)@
transport input ssh
!
!
!
monitor session 1 source interface Fa0/1 - 12 rx
monitor session 1 destination interface Fa0/23
end
```

2.2 Dragos Security CyberLens (E8, O10)

Dragos Security CyberLens software utilizes sensors placed within critical networks to identify assets and networks, building topologies and alerting on anomalies.

2.2.1 Dragos Security CyberLens Server (E8) Environment Setup

The system that was set up to run this application was a fully updated (as of 5/20/2016) Ubuntu 14.04 long-term support (LTS) operating system with the following hardware specifications:

- 4-core processor
- 8 gigabytes (GB) random access memory (RAM)

- 40 GB hard disk drive (HDD)

Other Requirements:

- Sudo or root privileges
- CyberLens installer (cyberlens-<version>-linux-<architecture>-installer.run)
- valid CyberLens license file

2.2.2 Dragos Security CyberLens Server (E8) Installation and Configuration Guide

1. As root:
    a. `./cyberlens-<version>-linux-<architecture>-installer.run`

    b. Accept the agreement and select **Forward.**

    c. Select **Forward** for a randomly generated password for root on the MySQL Server. A custom password can be specified if desired.

    d. Select **Forward** for a randomly generated password for CyberLens on the MySQL Server. As in the previous step, a custom password can be specified if desired.

    e. Select **Forward** to accept the installation configuration.

    f. Choose a **Username, Password** (and Confirm Password), and **Email Address** for the CyberLens login, then select **Forward.**

    g. Select **Localhost Access Only** (the files will be transferred across the Waterfall Security Gateway), then select **Forward.**

    h. Select **Forward.** Do not check the box for Block Outbound Traffic.

    i. Click the **folder icon** to select the CyberLens license file, then select **Forward.**

    j. Select **Forward** to begin installation.

2. Configure:
    a. Open a browser and navigate to *http://localhost/*

    b. On the menu bar on the left, select **Server Console.**

    c. Click the **drop-down arrow** next to **Options,** and check the box for **Use Sensor Files.**

    d. Click **Start** to start the server.

3. Set up file transfer protocol (FTP) for transferring files across the Waterfall Security Gateway:
    a. First, set up the user login. We used the username “waterfall.”

b. `adduser waterfall`

c. Specify password.

d. Add additional information if desired.

e. Type **y** to accept information.

f. `apt-get install vsftpd`

g. Edit `/etc/vsftpd.conf`

h. Ensure anonymous_enable=NO

i. Ensure local_enable=YES

j. Set write_enable=YES

k. `service vsftpd restart`

l. `ln -s /var/www/html/cyberlens/lib/file_link/ /home/waterfall/`

4. Permissions error: When files are copied over, the permissions default to **waterfall:waterfall.** Use the following steps to change the default to **www-data:www-data.**

   a. `sudo apt-get install incrontab`

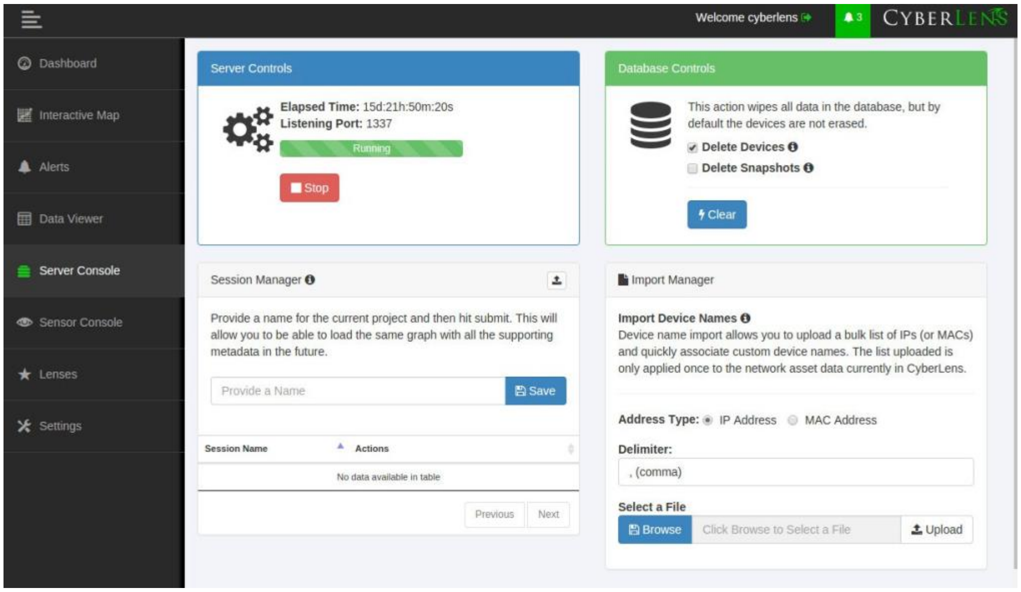
   b. `sudo vi /etc/incron.allow`

      i. Add `root` to file, then save and exit.

   c. `sudo incrontab -u root -e`

      i. Add `/var/www/html/cyberlens/lib/file_link IN_CREATE /bin/chown -R www-data:www-data /var/www/html/cyberlens/lib/file_link` then save and exit.

New files created in the directory should now automatically change permissions and be ingested.



Elapsed Time: 15d:21h:50m:20s
Listening Port: 1337

This action wipes all data in the database, but by default the devices are not erased.

☑ Delete Devices
☐ Delete Snapshots

Provide a name for the current project and then hit submit. This will allow you to be able to load the same graph with all the supporting metadata in the future.

Provide a Name

Session Name	Actions
No data available in table	

Import Device Names

Device name import allows you to upload a bulk list of IPs (or MACs) and quickly associate custom device names. The list uploaded is only applied once to the network asset data currently in CyberLens.

Address Type: ● IP Address ○ MAC Address

Delimiter: , (comma)

Select a File: Click Browse to Select a File

2.2.3 Dragos Security CyberLens Sensor (O10) Installation Guide

For Dragos Security CyberLens Sensor, follow the steps in Section 2.2.1 and Section 2.2.2 for Dragos Security CyberLens Server. There is no need to fix the permissions error.

2.3 Hewlett Packard Enterprise (HPE) ArcSight (E12)

HPE ArcSight is used as a central security information and event management (SIEM) platform, collecting alerts from across the build and aggregating them in one central location.
(Please note: HPE in this project is now Micro Focus Government Solutions, which acquired the suite of products and solutions used by the NCCoE in this build.)

2.3.1 HPE ArcSight (E12) Installation Guide

2.3.1.1 ArcSight Enterprise Security Manager (ESM) Manager Server Environment Setup

The following configuration matched requirements for the product relative to the use in the situational awareness use case.

1. The base operating system is CentOS 7. The following partition scheme was used for the installation.

Table 2-1 CentOS Partitioning Scheme for ArcSight ESM Manager Server

Name	Size	Type
/	50 GB	ext4
/boot	1 GB	ext4
/home	22 GB	ext4
/tmp	40 GB	tmpfs
/opt	2126 GB	ext4[a]

a. It is recommended to use XFS for/opt in lieu of ext4.

2. Ensure /tmp is larger than 3 GB; otherwise, ESM will fail to install.

3. Ensure the installation of X Windows and "compatibility libraries" are installed as well; ESM requires them.

4. Modification of user process limit may be required to ensure efficient thread usage:

   a. If there is not already a file /etc/security/limits.d/90-nproc.conf, create it (and the limits.d directory, if necessary).

   b. If the file already exists, delete all entries in the file.

   c. Add the following lines:

   ```
   * soft nproc 10240
   * hard nproc 10240
   ```

5. Adjust networking items:

   a. Set **internet protocol (IP) address** to 10.100.1.150.

   b. Set **Gateway** to 10.100.0.1.

   c. Set S**ubnet mask** to 255.255.0.0.

   d. Add DNS server in **/etc/resolv.conf.**

   ```
   10.97.74.8
   ```

   e. Add host name in **/etc/hosts** as follows (or add to DNS):

   ```
   10.100.1.150 arcsight.es-sa-b1.test arcsight
   ```

   f. Set host name in **/etc/sysconfig/**network.

   g. Set **ONBOOT** to **yes** in **/etc/sysconfig/network-scripts/ifcfg-eth0.**

6. Ensure ports **8443, 9443,** and **9000** are open on server firewall (e.g., check via iptables -S or iptables -L -n). If needed, add the following (as root). Adjust 0.0.0.0/0 statements as needed.

```
iptables -I INPUT -p tcp --dport 8443 -s 0.0.0.0/0 -j ACCEPT

iptables -I INPUT -p tcp --dport 9443 -s 0.0.0.0/0 -j ACCEPT

iptables -I INPUT -p tcp --dport 9000 -s 0.0.0.0/0 -j ACCEPT
```

   If using a SuperConnector/Forwarder (e.g., to RSA Archer), add the following (adjust for user datagram protocol (UDP) or transmission control protocol (TCP) as needed):

```
iptables -I OUTPUT -p tcp -d 0.0.0.0/0 --dport 514 -j ACCEPT
```

7. Save the rules:

```
/sbin/service iptables save
```

8. Set Selinux to **permissive mode** (may set back to enforcing mode upon completion of installation).

9. `adduser arcsight`

10. `mkdir /opt/arcsight/`

11. `chown arcsight:arcsight /opt/arcsight/`

12. Modify files to imitate Red Hat Enterprise Linux (RHEL) 6.5 (for CentOS and newer Red Hat versions):

    a. Edit `/etc/system-release`

    ```
    CentOS release 6.5 (Final)
    ```

    b. Edit `/etc/system-release-cpe`

    ```
    cpe:/o:centos:linux:6:GA
    ```

13. Ensure the time zone (tzdata) package is version 2014F or later. To install, use …

```
rpm -Uvh tzdata
```

or

```
yum update
```

14. Reboot.

2.3.2 ArcSight ESM Manager Server Operating System Installation

1. Copy the ESM installation tar file (do not untar) to `/home/arcsight/Desktop/ArcSight` (create folder if it does not exist).

2. Copy the ESM zipped license file (do not unzip) into the folder from the previous step.
3. `cd /home/arcsight/Desktop/ArcSight` (su arcsight if not currently arcsight user)
4. `chown arcsight:arcsight <ESM Install File>`
5. `tar xvf <ESM Install File>`
6. `./ArcSightESMSuite.bin -i console`

   Note: *Stop xwindows first if doing the installation with the -i console switch. This switch runs the installation from the command line rather than from a graphical user interface (GUI). The command line installation eases troubleshooting.*

7. As user “arcsight” run the configuration wizard:

   ```
   /opt/arcsight/manager/bin/arcsight firstbootsetup -boxster -soft -i console
   ```

8. Settings in the wizard:
   a. CORR-Engine (DB) password = ___________
   b. System storage size = 301 GB
   c. Event storage size = 361 GB
   d. Online event archive size = 200 GB (~1/6 minus 10% of total space; system reserves 10% of space)
   e. Retention period (days) = 30
   f. Manager host name = arcsight.es-sa-b1.test
   g. Administrator username = admin
   h. Administrator password = ___________
9. As user “root” run the following to install the ArcSight services onto the operating system:
10. Open a browser and navigate to ArcSight Command Center (*https://arcsight.es-sa-b1.test:8443*). Set the manager Java heap to 12288 (or another value based on available RAM).

2.3.3 ArcSight Console Environment Setup

1. Microsoft Windows 7 64-bit with the following settings:
   a. 1 virtual central processing unit (vCPU)
   b. 4 GB RAM

   c. 150 GB storage

2. The guest operating system (OS) IP information was set as follows:

   a. IP address: 10.100.1.149

   b. Gateway: 10.100.0.1?

   c. Subnet mask: 255.255.0.0?

   d. DNS: 10.97.74.8, 8.8.8.8, 8.8.4.4

3. Installed virtual machine (VM) Tools on guest OS to resolve missing mouse cursor issue.

4. Created OS user: arcsight, with password: __________

2.3.4 ArcSight Console Installation

1. Download ArcSight Console installation file (for Windows).

2. Run ArcSight Console installation file?

3. Add ArcSight Manager IP address to Windows OS host file (or add to DNS) at:

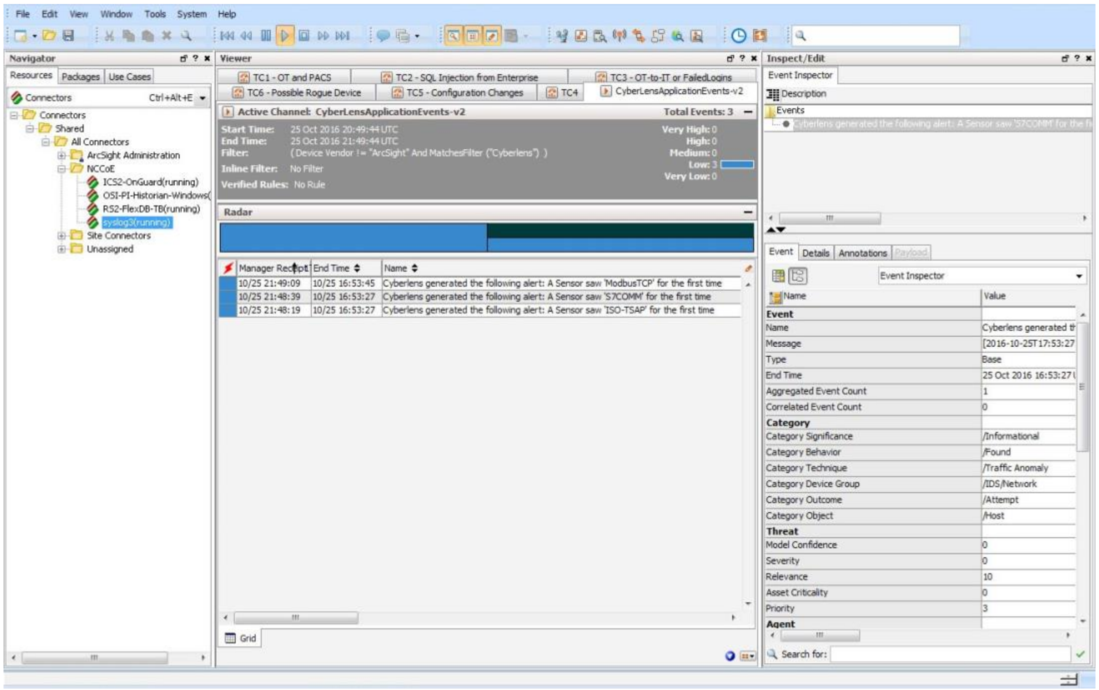
   C:\windows\system32\drivers\etc\hosts (edit this file as Administrator) by adding the following line:

   ```
   10.100.1.150 arcsight.es-sa-b1.test arcsight
   ```

4. Open ArcSight Console.

5. Log in to ArcSight Console with **user: arcsight, password:** __________, and in the **Manager** drop-down selection box type or select the server name: `arcsight.es-sa-b1.test`

6. At certificate-related pop-up, click **Accept.**



Active Channel: CyberLensApplicationEvents-v2 Total Events: 3

Start Time: 25 Oct 2016 20:49:44 UTC
End Time: 25 Oct 2016 21:49:44 UTC
Filter: (Device Vendor != "ArcSight" And MatchesFilter ("Cyberlens"))
Inline Filter: No Filter
Verified Rules: No Rule

Very High: 0
High: 0
Medium: 0
Low: 3
Very Low: 0

Manager Receipt	End Time	Name
10/25 21:49:09	10/25 16:53:45	Cyberlens generated the following alert: A Sensor saw 'ModbusTCP' for the first time
10/25 21:48:39	10/25 16:53:27	Cyberlens generated the following alert: A Sensor saw 'S7COMM' for the first time
10/25 21:48:19	10/25 16:53:27	Cyberlens generated the following alert: A Sensor saw 'ISO-TSAP' for the first time

Events
- Cyberlens generated the following alert: A Sensor saw 'S7COMM' for the fi

Name	Value
Event	
Name	Cyberlens generated th
Message	[2016-10-25T17:53:27
Type	Base
End Time	25 Oct 2016 16:53:27 U
Aggregated Event Count	1
Correlated Event Count	0
Category	
Category Significance	/Informational
Category Behavior	/Found
Category Technique	/Traffic Anomaly
Category Device Group	/IDS/Network
Category Outcome	/Attempt
Category Object	/Host
Threat	
Model Confidence	0
Severity	0
Relevance	10
Asset Criticality	0
Priority	3
Agent	

2.3.4.1 ArcSight Connector Server Preparation

1. CentOS 7 host with the following VM settings:
    a. 1 vCPU
    b. 12 GB RAM
    c. 140 GB provisioned
2. Install CentOS using the following options:
    a. Server with GUI Xwindows libraries are required in accordance with ArcSight guide.
    b. File and Storage (in case file-based log collection will be used)
    c. Compatibility libraries
    d. Development tools
3. Set guest host name as follows: `arcconn.es-sa-b1.test`
4. Install VM Tools on guest OS.
5. Set guest OS IP information as follows:
    a. IP address: 10.100.1.148

   b. Gateway: 10.100.0.1

   c. Subnet mask: 255.255.0.0

   d. DNS: 10.97.74.8, 8.8.8.8

6. Add host names in /etc/ hosts as follows (or add to DNS):

   10.100.1.148 arcconn.es-sa-b1.test arcconn

7. 10.100.1.150 arcsight.es-sa-b1.test arcsight adduser arcsight

8. `mkdir /opt/arcsight/`

9. chown -r arcsight:arcsight /opt/arcsight/

10. As user arcsight, `mkdir /opt/arsight/connectors/syslog1`

11. Ensure UDP port 514 is open inbound on server firewall and also that connector is allowed outbound on port 8443. For example: …

    a. As root:

    ```
    iptables -I INPUT -p udp --dport 514 -s 0.0.0.0/0 -j ACCEPT
    iptables -I OUTPUT -p tcp -d 0.0.0.0/0 --dport 8443 -j ACCEPT
    ```

    b. Save the rules:

    ```
    /sbin/service iptables save
    ```

12. Disable firewall:

    a. systememct1 disable firewall

    b. systemct1 mask firewalld expressions

13. Disable OS native syslog service:

    systemctl disable rsyslog.service

2.4 ICS2 OnGuard (E5)

ICS2 OnGuard is used for behavioral analysis based on an extended model of historical historian information. Utilizing this information, OnGuard alerts to changes in historian activity based on deviations to original model.

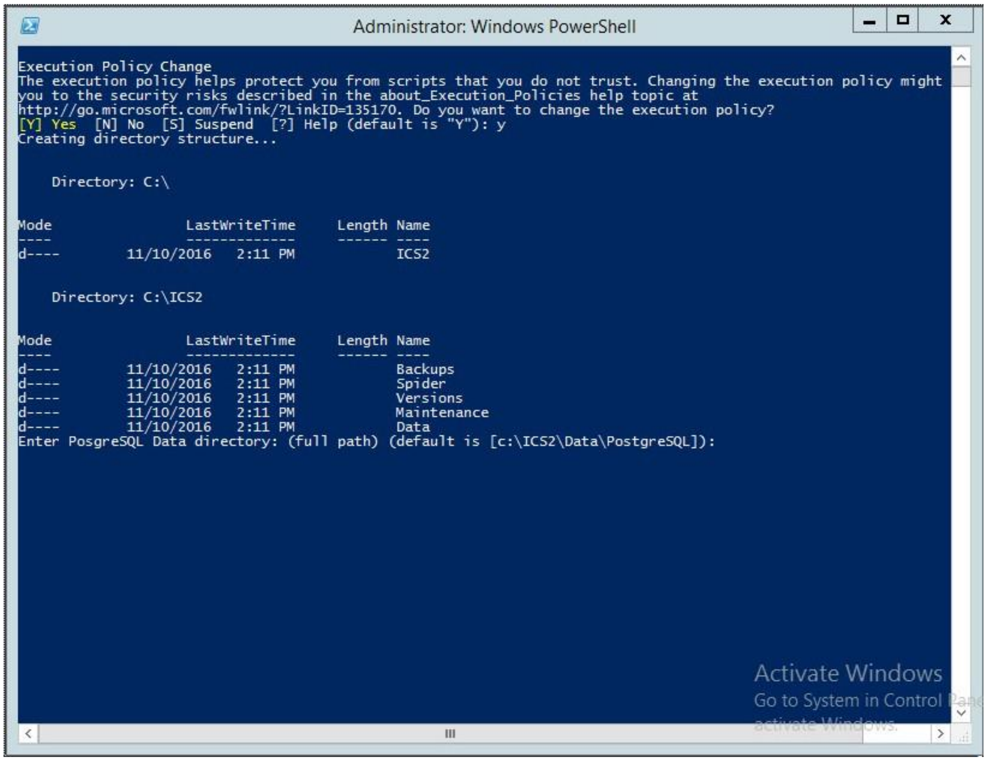
2.4.1 Environment Setup

The following configuration matched requirements for the product relative to the use in the situational awareness build:

- Microsoft Windows Server 2012 R2
- VM with CPU Quad Core 2.199 gigahertz (GHz)
- VM with 16,384 MB of memory
- virtual hard disk
- OSIsoft PI OLE DB Driver
- ICS2_Installation_<version>.zip

2.4.2 Install Vendor Software

1. Open and extract the provided ***ICS2_Installation_<version>.zip*** file.
2. Open the **ICS2 Installation folder** created by extracting the .zip file.
3. Right-click the ***ServerDeploy.PS1*** **file** and select **Run with PowerShell.**
4. Press **Y** to change the execution policy.
5. Once the directory structure has been created, press **Enter** for the default PostgreSQL directory.

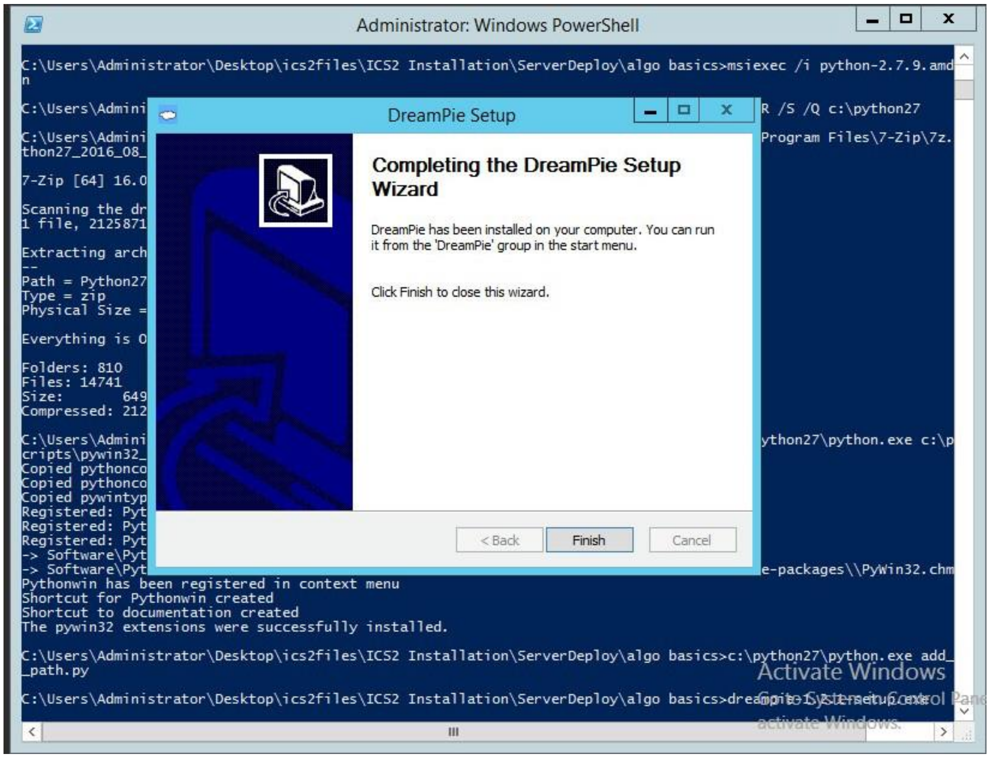

Administrator: Windows PowerShell
Activate Windows
Go to System in Control Panel to activate Windows.

```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
Creating directory structure...


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        11/10/2016   2:11 PM            ICS2


    Directory: C:\ICS2


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        11/10/2016   2:11 PM            Backups
d----        11/10/2016   2:11 PM            Spider
d----        11/10/2016   2:11 PM            Versions
d----        11/10/2016   2:11 PM            Maintenance
d----        11/10/2016   2:11 PM            Data
Enter PosgreSQL Data directory: (full path) (default is [c:\ICS2\Data\PostgreSQL]):
```

6. Press **Enter** for the default SQLServer directory.

   The installer will install multiple products, including Google Chrome and Notepad++.

7. When the DreamPie installer pops up, click **Next.**
8. Select **Install for anyone using this computer** and click **Next.**
9. Keep the default destination folder and click **Install.**
10. When the installation is complete, click **Next.**
11. Close the installer by clicking **Finish.**



```
C:\Users\Administrator\Desktop\ics2files\ICS2 Installation\ServerDeploy\algo basics>msiexec /i python-2.7.9.amd
n

C:\Users\Admini                                                                  R /S /Q c:\python27

C:\Users\Admini                                                                  Program Files\7-Zip\7z.
thon27_2016_08_

7-Zip [64] 16.0

Scanning the dr
1 file, 2125871

Extracting arch
--
Path = Python27
Type = zip
Physical Size =

Everything is O

Folders: 810
Files: 14741
Size:       649
Compressed: 212

C:\Users\Admini                                                                  ython27\python.exe c:\p
cripts\pywin32_
Copied pythonco
Copied pythonco
Copied pywintyp
Registered: Pyt
Registered: Pyt
Registered: Pyt
-> Software\Pyt
-> Software\Pyt                                                                  e-packages\\PyWin32.chm
Pythonwin has been registered in context menu
Shortcut for Pythonwin created
Shortcut to documentation created
The pywin32 extensions were successfully installed.

C:\Users\Administrator\Desktop\ics2files\ICS2 Installation\ServerDeploy\algo basics>c:\python27\python.exe add_
_path.py

C:\Users\Administrator\Desktop\ics2files\ICS2 Installation\ServerDeploy\algo basics>dre
```

Completing the DreamPie Setup Wizard

DreamPie has been installed on your computer. You can run it from the 'DreamPie' group in the start menu.

Click Finish to close this wizard.

12. Once completed, PowerShell will close.

2.4.3 Install OnGuard System

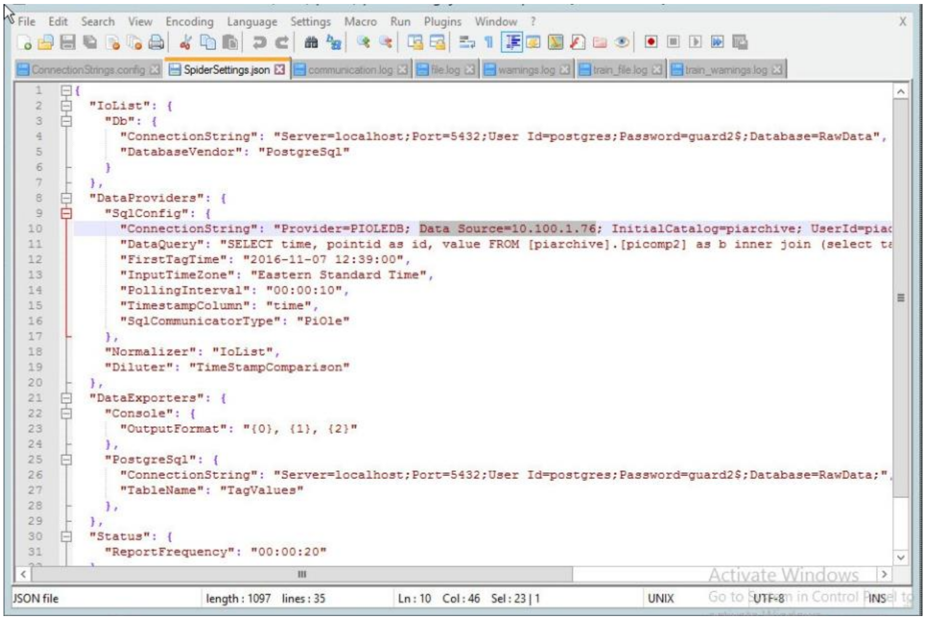
1. Open the **Deploy OnGuard <version>** folder.

2. Double-click the **DeployOnGuard** Windows Batch File.

3. Verify that **ApplicationSettings.config, ConnectionStrings.config**, and **SpiderSettings.json** have been created.

    a. If necessary, change the historian IP address (OSIsoft PI) in **SpiderSettings.json** to the appropriate IP address (the key is **DataProviders.SqlConfig.ConnectionString).**

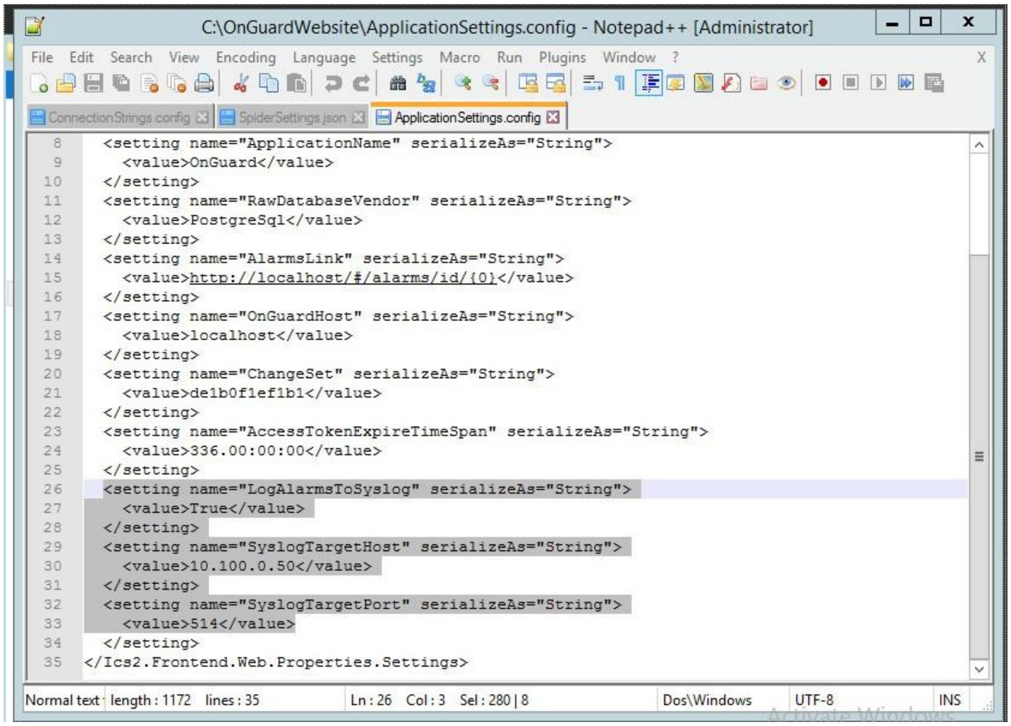
Figure 2-1 OSIsoft PI Historian Connection



```
{
  "IoList": {
    "Db": {
      "ConnectionString": "Server=localhost;Port=5432;User Id=postgres;Password=guard2$;Database=RawData",
      "DatabaseVendor": "PostgreSql"
    }
  },
  "DataProviders": {
    "SqlConfig": {
      "ConnectionString": "Provider=PIOLEDB; Data Source=10.100.1.76; InitialCatalog=piarchive; UserId=pia
      "DataQuery": "SELECT time, pointid as id, value FROM [piarchive].[picomp2] as b inner join (select ta
      "FirstTagTime": "2016-11-07 12:39:00",
      "InputTimeZone": "Eastern Standard Time",
      "PollingInterval": "00:00:10",
      "TimestampColumn": "time",
      "SqlCommunicatorType": "PiOle"
    },
    "Normalizer": "IoList",
    "Diluter": "TimeStampComparison"
  },
  "DataExporters": {
    "Console": {
      "OutputFormat": "{0}, {1}, {2}"
    },
    "PostgreSql": {
      "ConnectionString": "Server=localhost;Port=5432;User Id=postgres;Password=guard2$;Database=RawData;",
      "TableName": "TagValues"
    },
  },
  "Status": {
    "ReportFrequency": "00:00:20"
```

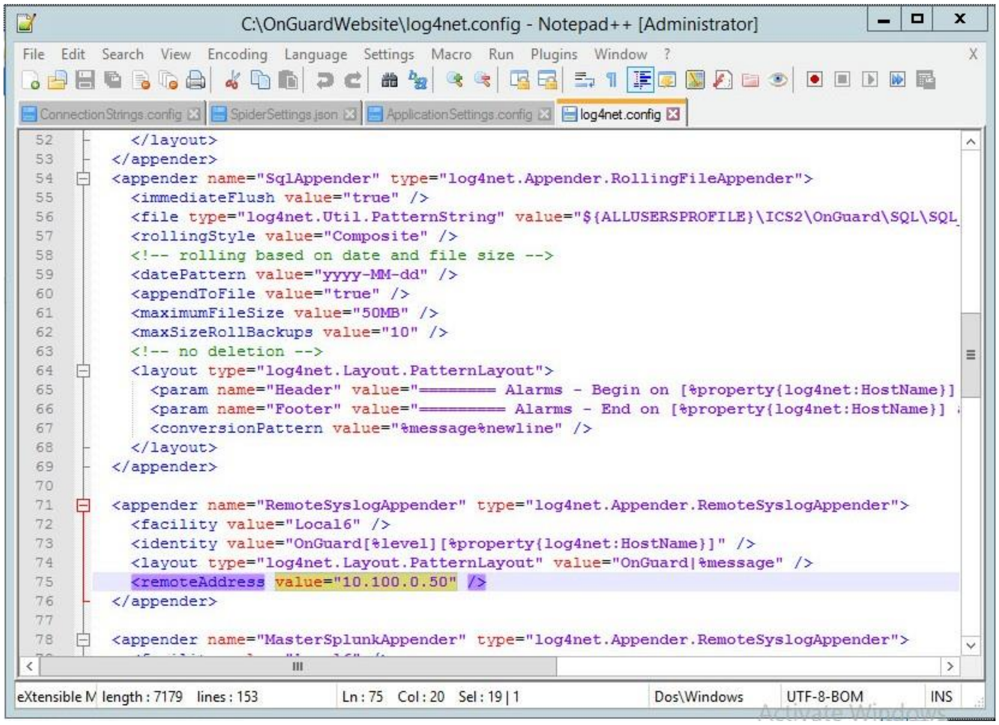
b. In ApplicationSettings.config, verify that settings LogAlarmsToSyslog is True, SyslogTargetHost is set to the syslog server IP (10.100.0.50), and the SyslogTargetPort is set to 514 (or whatever port syslog is listening on).

Figure 2-2 ApplicationSettings Syslog Configuration


C:\OnGuardWebsite\ApplicationSettings.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
ConnectionStrings.config
SpiderSettings.json
ApplicationSettings.config
Normal text file
length : 1172 lines : 35
Ln : 26 Col : 3 Sel : 280 | 8
Dos\Windows
UTF-8
INS

```
  <setting name="ApplicationName" serializeAs="String">
    <value>OnGuard</value>
  </setting>
  <setting name="RawDatabaseVendor" serializeAs="String">
    <value>PostgreSql</value>
  </setting>
  <setting name="AlarmsLink" serializeAs="String">
    <value>http://localhost/#/alarms/id/{0}</value>
  </setting>
  <setting name="OnGuardHost" serializeAs="String">
    <value>localhost</value>
  </setting>
  <setting name="ChangeSet" serializeAs="String">
    <value>de1b0f1ef1b1</value>
  </setting>
  <setting name="AccessTokenExpireTimeSpan" serializeAs="String">
    <value>336.00:00:00</value>
  </setting>
  <setting name="LogAlarmsToSyslog" serializeAs="String">
    <value>True</value>
  </setting>
  <setting name="SyslogTargetHost" serializeAs="String">
    <value>10.100.0.50</value>
  </setting>
  <setting name="SyslogTargetPort" serializeAs="String">
    <value>514</value>
  </setting>
</Ics2.Frontend.Web.Properties.Settings>
```

c. Open **C:\OnGuardWebsite\log4net.config** in Notepad++ and verify that the appender **RemoteSyslogAppender** has a **remoteAddress** value of the syslog server IP (10.100.0.50).



C:\OnGuardWebsite\log4net.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
ConnectionStrings.config
SpiderSettings.json
ApplicationSettings.config
log4net.config
eXtensible M length : 7179 lines : 153 Ln : 75 Col : 20 Sel : 19 | 1 Dos\Windows UTF-8-BOM INS

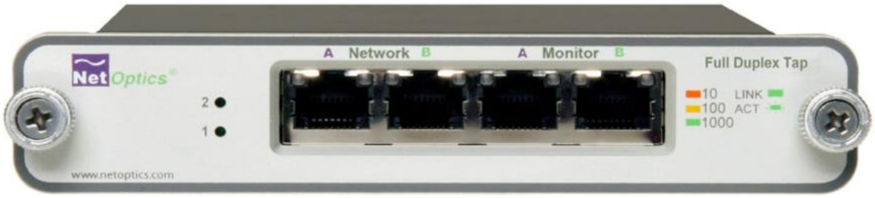
```
      </layout>
    </appender>
    <appender name="SqlAppender" type="log4net.Appender.RollingFileAppender">
      <immediateFlush value="true" />
      <file type="log4net.Util.PatternString" value="${ALLUSERSPROFILE}\ICS2\OnGuard\SQL\SQL_
      <rollingStyle value="Composite" />
      <!-- rolling based on date and file size -->
      <datePattern value="yyyy-MM-dd" />
      <appendToFile value="true" />
      <maximumFileSize value="50MB" />
      <maxSizeRollBackups value="10" />
      <!-- no deletion -->
      <layout type="log4net.Layout.PatternLayout">
        <param name="Header" value="========= Alarms - Begin on [%property{log4net:HostName}]
        <param name="Footer" value="========= Alarms - End on [%property{log4net:HostName}]
        <conversionPattern value="%message%newline" />
      </layout>
    </appender>

    <appender name="RemoteSyslogAppender" type="log4net.Appender.RemoteSyslogAppender">
      <facility value="Local6" />
      <identity value="OnGuard[%level][%property{log4net:HostName}]" />
      <layout type="log4net.Layout.PatternLayout" value="OnGuard|%message" />
      <remoteAddress value="10.100.0.50" />
    </appender>

    <appender name="MasterSplunkAppender" type="log4net.Appender.RemoteSyslogAppender">
```

4. Close Notepad++ and open Google Chrome to *http://localhost/* for the login screen.

2.5 IXIA Full-Duplex Tap (O16)

The following is the installation for the IXIA TP-CU3 taps used in the lab.

Figure 2-3 IXIA TP-CU3 Network Tap



1. Mount the tap to the rack.

2. Utilize the supplied power cord to connect an outlet to the power jacks located on the rear of the tap.

3. To connect to the network …

    a. Connect **Network Port A** to the Ethernet cable coming in from the control system network.

    b. Connect **Network Port B** to an Ethernet cable going out to the destination port of the original Ethernet cable used in the previous step.

    c. Verify that the link LEDs illuminate.

    d. Connect **Monitor Port A** to the monitoring port of the device used to monitor the ingress of **Network Port A.**

    e. Connect **Monitor Port B** to the monitoring port of the device used to monitor the ingress of **Network Port B.**

4. The tap installation and setup are complete.

2.6 OSIsoft PI Historian (E4, O8)

OSIsoft PI Historian is the primary historian type utilized in the build. The two instances serve as the main mirror of the control system's historian as well as a secondary historian located in the enterprise network. The secondary historian feeds the anomaly detection platform in the enterprise network.

For further information, visit http://www.osisoft.com/federal/.

2.6.1 OSIsoft PI Historian (E4) Installation Guide

The following are the installation and configuration for the OSIsoft PI Historian located within the enterprise network.

2.6.1.1 Environment Setup

- Microsoft Windows Server 2012 R2
- 2.2 GHz processor
- 8 GB RAM
- 250 GB storage
- Structured Query Language (SQL) Server Express

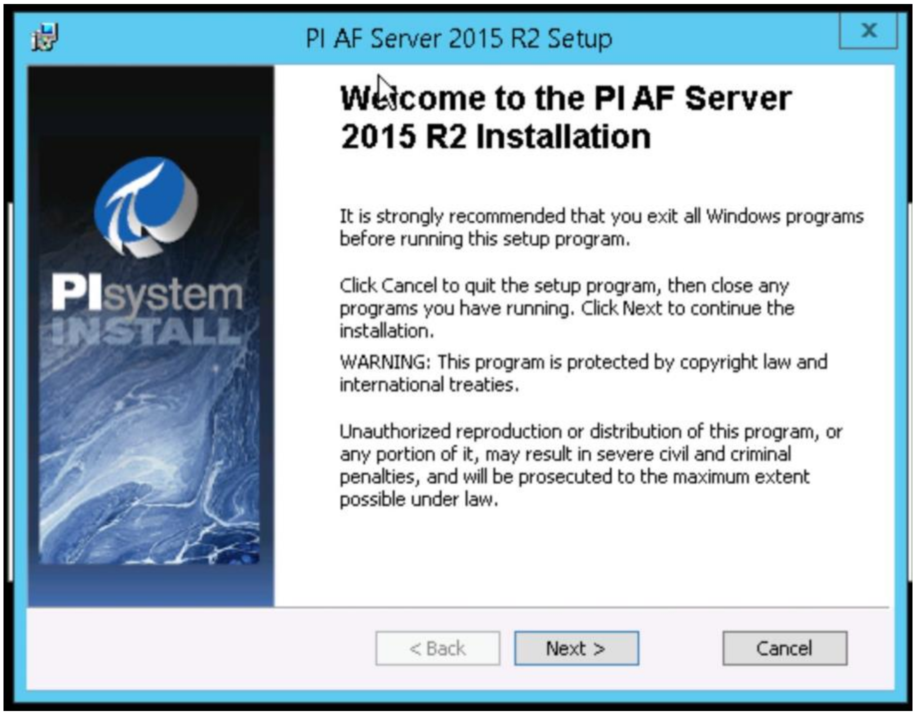
2.6.1.2 Installation Instructions

1. Create admin user in windows: **Piadmin**

2. Create admin user in windows: **Afadmin**

3. Create standard user in windows: **Piuser**
4. Create new folder **C:\Download**
5. Install SQL Server 2014.
    a. Create instance:
        i. Name: **PIAFSQL**
        ii. Instance ID: **PIAF**
    b. SQL Server Configuration Manager:
        i. Enable SWL Server Network Configuration -> Protocols for PIAFSQL -> {Shared Memory, Named Pipes, TCP/IP}
6. Copy **PI-AF-Server_2015-R2_** to **C:\Download** and self-extract setup (run as administrator).
    a. A reboot will be required.
    b. After reboot, the Microsoft Visual C++ 2013 install window will appear.

Figure 2-4 PI AF Server 2015 R2 Setup



PI AF Server 2015 R2 Setup

Welcome to the PI AF Server 2015 R2 Installation

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

c. On the “Welcome to the PI AF Server 2015 R2 Installation” screen …

   i. Click **Next.**

   ii. Click **Next** to select default install directory.

   iii. Click **Next** for default features.

   iv. Select **Virtual User Account.**

   v. Under SQL Server Connection, select **<hostname>\PIAFSQL** and click **Next.**

   vi. Click **Install.**

7. Open **Open Database Connectivity (ODBC) Data Sources (64-bit).**

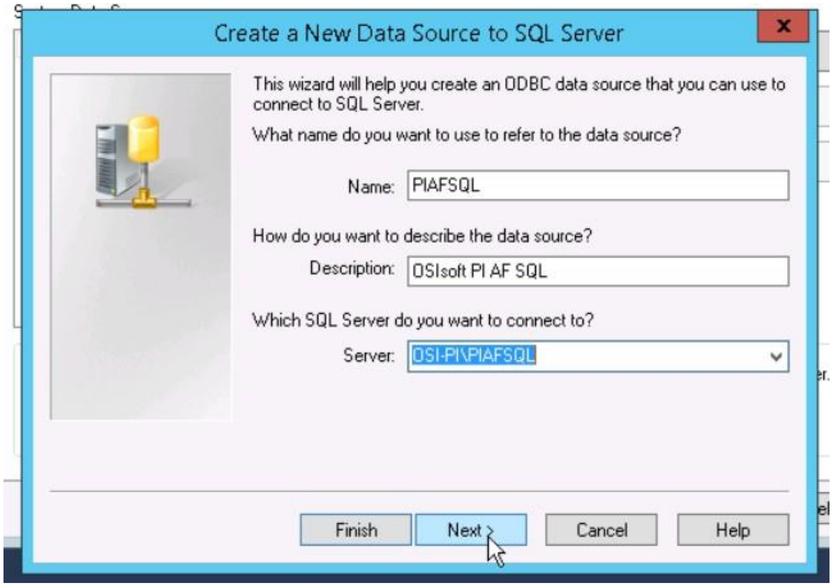
   a. Under System DSN, click **Add.**

      i. Name: **PIAFSQL**

      ii. Description: **OSIsoft PI AF SQL**

      iii. Server: **<hostname>\PIAFSQL**

Figure 2-5 Create New Data Source for SQL



Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: PIAFSQL

How do you want to describe the data source?

Description: OSIsoft PI AF SQL

Which SQL Server do you want to connect to?

Server: OSI-PI\PIAFSQL

   b. Click **Next.**

c. Click **Next.**

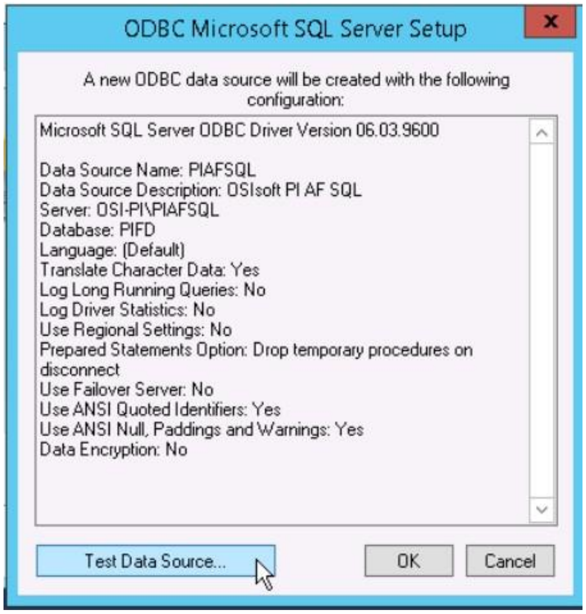
d. Check the **Change the default database to: and select PIFD.**

e. Click **Next.**

f. Click **Finish.**

g. Click **Test Data Source…**

Figure 2-6 Testing SQL Setup



A new ODBC data source will be created with the following configuration:

```
Microsoft SQL Server ODBC Driver Version 06.03.9600

Data Source Name: PIAFSQL
Data Source Description: OSIsoft PI AF SQL
Server: OSI-PI\PIAFSQL
Database: PIFD
Language: (Default)
Translate Character Data: Yes
Log Long Running Queries: No
Log Driver Statistics: No
Use Regional Settings: No
Prepared Statements Option: Drop temporary procedures on
disconnect
Use Failover Server: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
Data Encryption: No
```

h. After a successful pass, click **OK** three times to close ODBC Data Sources.

8. Open Microsoft SQL Server Management Studio (as Administrator).

   a. Ensure the settings are correct and click **Connect.**

   b. In the left tab, select **<hostname>\PIAFSQL > Databases > PFID > Tables** and ensure tables are listed.

   c. Close Microsoft SQL Server Management Studio.

9. Copy **PISDK_2014_** and **PISMT_2015_R2_** to *C:\Downloads.*

10. Copy **PI-AF-Client_2015-R2_** to *C:\Download* and run as administrator.

a. Change the Extraction path to **.**

b. When the PI AF Client 2015 R2 installation screen starts up, click **OK.**

c. In the Default Data server input, type `piafsql` and click **Next.**

d. Click **Next** for the default PIHOME directory.

e. Wait for the installation to finish and click **Next.**

f. Select whether to participate in the Customer Experience Improvement and click **Next.**

g. Click **Next** for default features, then click **Install.**

h. Verify that the Service Status screen shows all services started successfully, and click **Next.**

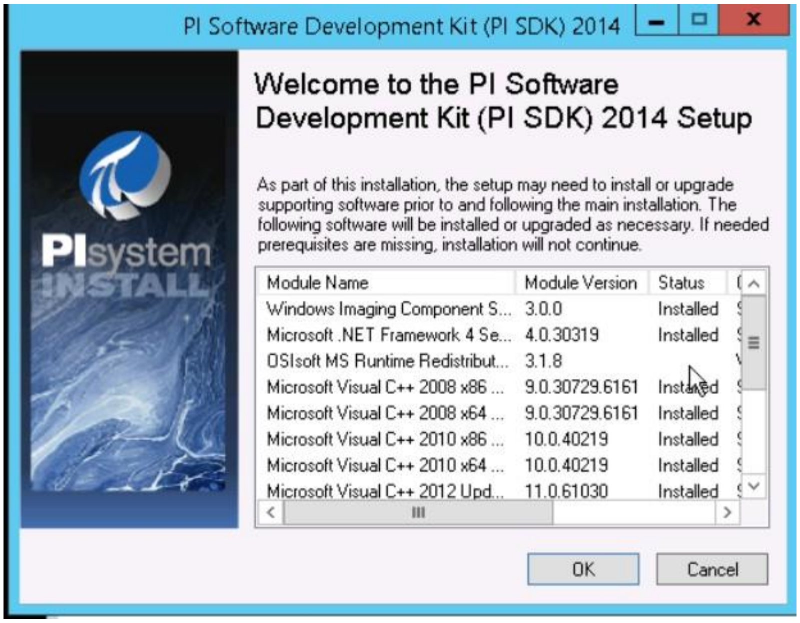
i. Click **Close.**

11. Run **PISDK_2014_** as administrator.

a. Change the Extraction path to **.**

b. When the PI Software Development Kit installation screen starts up, click **OK.**

Figure 2-7 PI SDK Setup



PI Software Development Kit (PI SDK) 2014

Welcome to the PI Software Development Kit (PI SDK) 2014 Setup

As part of this installation, the setup may need to install or upgrade supporting software prior to and following the main installation. The following software will be installed or upgraded as necessary. If needed prerequisites are missing, installation will not continue.

Module Name	Module Version	Status
Windows Imaging Component S...	3.0.0	Installed
Microsoft .NET Framework 4 Se...	4.0.30319	Installed
OSIsoft MS Runtime Redistribut...	3.1.8	
Microsoft Visual C++ 2008 x86 ...	9.0.30729.6161	Installed
Microsoft Visual C++ 2008 x64 ...	9.0.30729.6161	Installed
Microsoft Visual C++ 2010 x86 ...	10.0.40219	Installed
Microsoft Visual C++ 2010 x64 ...	10.0.40219	Installed
Microsoft Visual C++ 2012 Upd...	11.0.61030	Installed

c. On the screen listing services that will be stopped, click **OK.**

d. Verify that the Service Status screen shows all services started successfully, and click **Next.**

e. Click **Close.**

12. Run **PISMT_2015_R2_** as administrator.

a. Change the Extraction path to **.**

b. When the installation screen starts up, click **Next** twice.

c. On User Information, change the **Full Name** field to **PIadmin** and fill in **Organization.**

d. Click **Next.**

e. Click **Install.**

f. Click **Close.**

13. Run the **MSRuntimes** and **MSRuntimes_x64** applications to install the proper DLLs.

14. Run **OSIprerequisites-standalone_2.0.0.10_** as administrator.

a. Click **OK.**

b. Change Unzip folder to **.** and select **Unzip.**

c. When completed, click **Close.**

15. Run **OSIprerequisites-Patch_2.1.1_**

a. Change Unzip folder to **.** and select **Unzip.**

b. When completed, click **Close.**

16. Reboot the machine.

17. Create the following folders:

a. *C:\PI*

b. *C:\PI\Bin*

c. *C:\PI\Dat*

d. *C:\PI\License*

e. *C:\PI\Queue*

    f. *C:\PI\Archive*

18. Copy a generated license file into *C:\PI\License* and name `pilicense.dat`.

19. Copy *PIServer_2012SP_x64_* to *C:\Downloads.*

20. Run *PIServer_2012SP_x64_* as Administrator.

    a. Change the Unzip folder to **.** and click **Unzip.**

    b. When the PI Server 2012 SP1 64-bit installation screen starts up, click **OK.**

    c. When it is showing what is installed, click **Close.**

    d. On the welcome screen, click **Next.**

    e. On licensing, click **Browse** and select **C:\PI\License,** then **Next**.

    f. Verify that the AF Server is the host name, then click **Next.**

    g. Ensure that **No** is selected for **enabling PI Module Database,** and click **Next.**

    h. For PI Server Binaries, click **Browse** and select **C:\PI\Bin.**

    i. For Event Queues, click **Browse** and select **C:\PI\Dat.**

    j. For Archives, click **Browse** and select **C:\PI\Archive.**

    k. Click **Next.**

    l. Click **Next** to start installation.

    m. When complete, click **Close.**

21. Open **PI System Management Tools.**

    a. Under Servers on the left, select the **piafsql server**.

    b. Close **PI System Management Tools.**

22. Reboot system.

23. Copy **C:\PI\Bin\admin\pisrvstart.bat** and **C:\PI\Bin\admin\pisrvstop.bat** to the **Desktop.**

24. Open **PISDKUtility.**

    a. Under Tools, select **Add Server.**

        i. Network Path/fully qualified domain name (FQDN): **<hostname>**

        ii. Click **OK.**

b. Under Default User Name for the new server, type **piadmin.**

c. Under Connections, select **Options.**

    i. Set the Connection time-out to **30 seconds.**

    ii. For Default Server, select **<hostname>.**

    iii. Ensure the **Protocol Order** is …

        1. **PI Trust**

        2. **Default User**

        3. **Windows Security**

    iv. Click **OK.**

d. Under Connections, select **Aliases.**

    i. Click **Add…**

    ii. Under Alias, type the machine's **IP Address.**

    iii. Click **OK.**

    iv. Click **Close.**

e. Click **Save.**

2.6.2 OSIsoft PI Historian (O8) Installation Guide

Follow the installation guide for OSIsoft PI Historian in Section 2.6.1.

2.7 OSIsoft Citect Interface (O13)

The OSIsoft Citect Interface creates a connection for the OSIsoft PI Historian to interface with the SCADA server for aggregating historian data.

2.7.1 OSIsoft Citect Interface (O13) Installation Guide

1. Open the **pipc.ini** file located in **C:\Windows** (or the **%windir%** directory).

2. The file should contain the following info. If the file does not exist, create it and add the following lines:

```
[PIPC]

PIHOME=C:\Program Files (x86)\PIPC
```

3. Start the installation executable **(Citect_#.#.#.#_.exe).**

4. This will install files in **PIHOME\Interfaces\Citect\.**

5. Copy the following files from the Citect machine's **Bin** directory into the **PIHOME\Interfaces\Citect\** directory.

    a. **CtApi.dll**

    b. **Ct_ipc.dll**

    c. **CtEng32.dll**

    d. **CtRes32.dll**

    e. **CtUtil32.dll**

    f. **CiDebugHelp.dll**

6. To install the connector as a service, run **PI_Citect.exe /install /auto /depend tcpip.** Test the connection between the interface node and the Citect node by using the **PI_CitectTest.exe** connection tester.

7. Run the **interface configuration utility (ICU),** and configure a new instance of this interface.

8. Define digital states.

9. **Cit_Bad_Conn** indicates communication problems with the Citect node.

10. Build input tags and, if desired, output tags for this interface by using the point builder utility **PICitect_PointBuilder.exe.** Important point attributes and their purposes are:

a.	Location1 (interface instance ID):	1
b.	Location2 (input/output parameter):	0 (input)
c.	Location3 (not used):	0
d.	Location4 (scan class):	1
e.	Location5 (not used):	0
f.	ExDesc (optional, event-driven scans):	-
g.	InstrumentTag:	[Citect point name]

11. Start the interface interactively, and confirm its successful connection to the PI Server without buffering.

12. Confirm that the interface collects data successfully.

13. Stop the interface, and configure a buffering application (either Bufserv or PIBufss). When configuring buffering, use the ICU menu item **Tools > Buffering… > Buffering Settings** to make a change to the default value (32678) for the Primary and Secondary Memory Buffer Size (Bytes) to **2000000.** This will optimize the throughput for buffering and is recommended by OSIsoft.

14. Start the buffering application and the interface. Confirm that the interface works together with the buffering application by stopping the PI Server.

15. Configure the interface to run as an automatic service that depends on the PI Update Manager and PI Network Manager services.

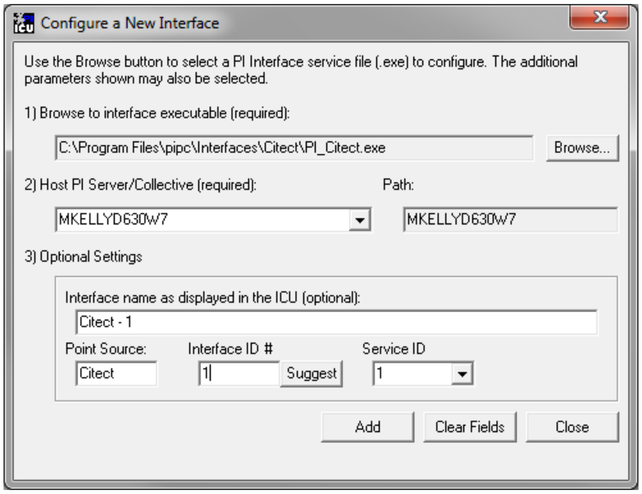
16. Restart the interface node, and confirm that the interface and the buffering application restart.

2.7.2 Configuration

The PI Interface Configuration Utility provides a graphical user interface for configuring PI interfaces. If the interface is configured by the PI ICU, the batch file of the interface (PI_Citect.bat) will be maintained by the PI ICU, and all configuration changes will be kept in that file and the module database. The procedure below describes the necessary steps for using PI ICU to configure the PI Citect interface.

1. From the PI ICU menu, select **Interface,** then **New Windows Interface Instance** from EXE..., and then **Browse** to the **PI_Citect.exe** executable file. Then, enter values for **Host PI System, Point Source,** and **Interface ID#.** A window such as the following results:

Figure 2-8 Configure New Interface



Use the Browse button to select a PI Interface service file (.exe) to configure. The additional parameters shown may also be selected.

1) Browse to interface executable (required): C:\Program Files\pipc\Interfaces\Citect\PI_Citect.exe

2) Host PI Server/Collective (required): MKELLYD630W7 Path: MKELLYD630W7

3) Optional Settings

Interface name as displayed in the ICU (optional): Citect - 1

Point Source: Citect Interface ID #: 1 Service ID: 1

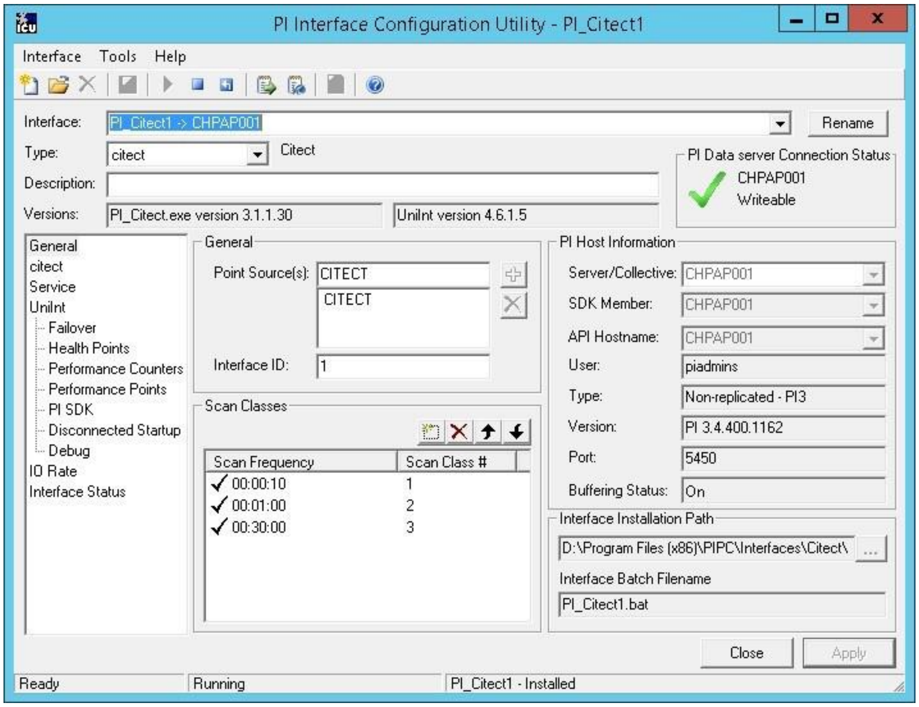
2. **Interface name as displayed in the ICU (optional)** will have PI- pre-pended to this name, and it will be the display name in the services menu.

3. Click **Add.**

4. Once the interface is added to PI ICU, near the top of the main PI ICU screen, the interface **Type** should be **Citect.** If not, use the drop-down box to change the interface Type to be Citect.

5. Click on **Apply** to enable the PI ICU to manage this instance of the PI Citect interface.

Figure 2-9 ICU — General Configuration



Interface: PI_Citect1 -> CHPAP001

Type: citect Citect

Description:

Versions: PI_Citect.exe version 3.1.1.30 UniInt version 4.6.1.5

PI Data server Connection Status: CHPAP001 Writeable

General
citect
Service
UniInt
- Failover
- Health Points
- Performance Counters
- Performance Points
- PI SDK
- Disconnected Startup
- Debug
IO Rate
Interface Status

General

Point Source(s): CITECT
CITECT

Interface ID: 1

Scan Classes

Scan Frequency	Scan Class #
✓ 00:00:10	1
✓ 00:01:00	2
✓ 00:30:00	3

PI Host Information

Server/Collective: CHPAP001

SDK Member: CHPAP001

API Hostname: CHPAP001

User: piadmins

Type: Non-replicated - PI3

Version: PI 3.4.400.1162

Port: 5450

Buffering Status: On

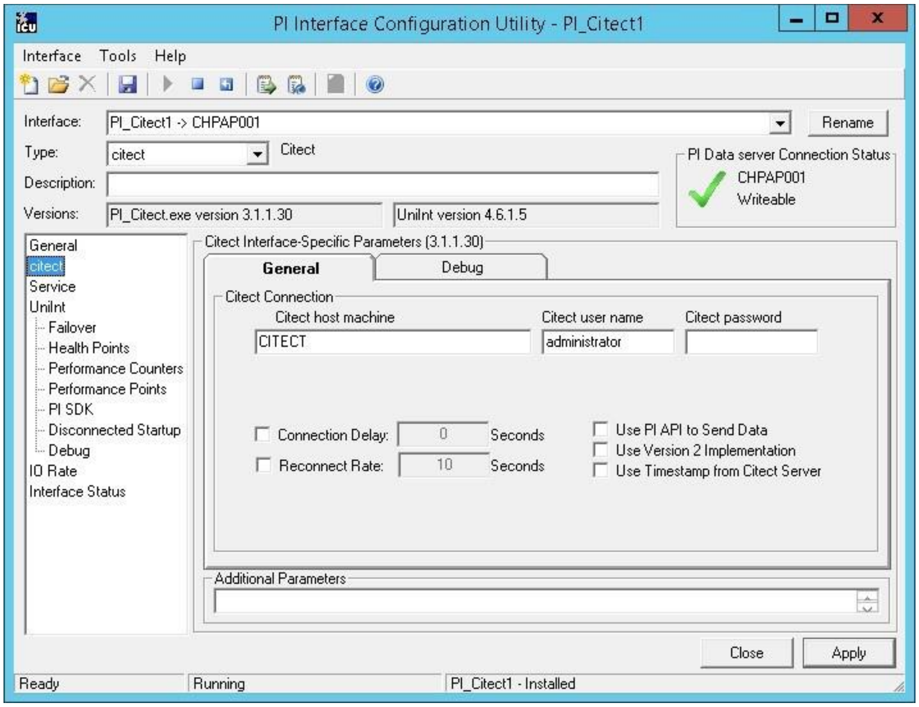
Interface Installation Path: D:\Program Files (x86)\PIPC\Interfaces\Citect\

Interface Batch Filename: PI_Citect1.bat

Ready | Running | PI_Citect1 - Installed

6. Because the start-up file of the PI Citect interface is maintained automatically by the PI ICU, use the Citect page to configure the start-up parameters, and do not make changes in the file manually.

Figure 2-10 ICU — Citect ICU Control



Interface: PI_Citect1 -> CHPAP001

Type: citect Citect

Description:

Versions: PI_Citect.exe version 3.1.1.30 UniInt version 4.6.1.5

PI Data server Connection Status
CHPAP001
Writeable

Citect Interface-Specific Parameters (3.1.1.30)

Citect Connection

Citect host machine: CITECT

Citect user name: administrator

Citect password:

□ Connection Delay: 0 Seconds

□ Reconnect Rate: 10 Seconds

□ Use PI API to Send Data

□ Use Version 2 Implementation

□ Use Timestamp from Citect Server

Additional Parameters

Ready | Running | PI_Citect1 - Installed

7. Supply values for the fields in the Citect **General** tab as follows:

   a. Citect host machine — **CITECT**

   b. Citect username — **administrator**

   c. Citect password — **<enter password here>**

   d. Connection Delay — **none (unchecked)**

   e. Reconnect Rate — **none (unchecked)**

   f. Use PI API data to Send Data — **(unchecked)**

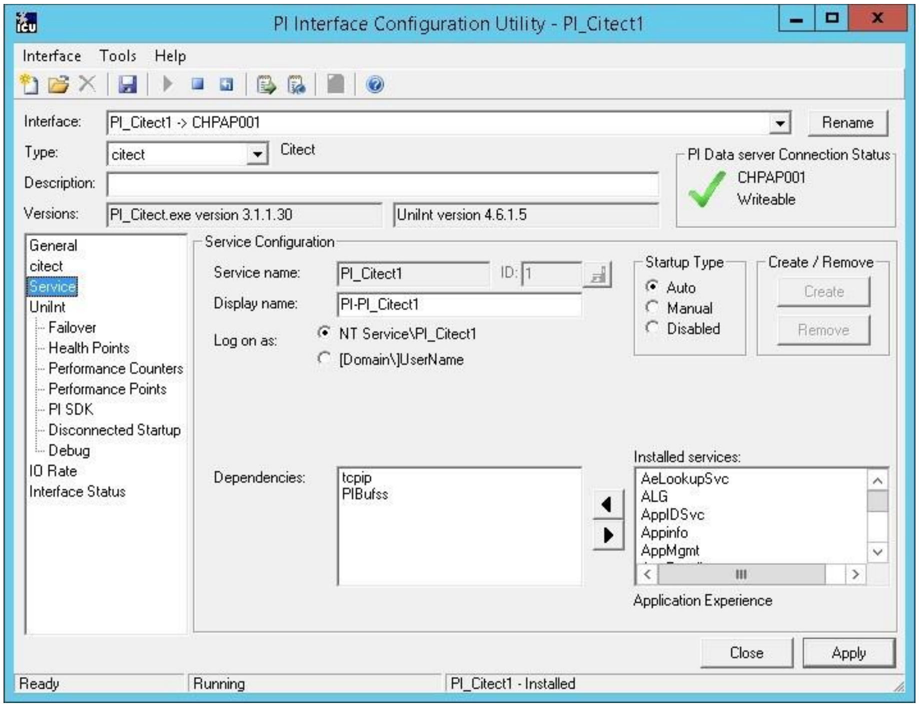
   g. Use Version 2 Implementation — **(unchecked)**

   h. Use Timestamp from Citect Server — **(unchecked)**

8. Keep the defaults on the Citect **Debug** tab.

9. To set up the interface as a Windows Service, use the **Service** page. This page allows configuration of the interface to run as a service as well as starting and stopping the interface service. Keep the default values, as shown below.

Figure 2-11 ICU — Windows Service Setup



PI Interface Configuration Utility - PI_Citect1

Interface: PI_Citect1 -> CHPAP001

Type: citect Citect

Description:

Versions: PI_Citect.exe version 3.1.1.30 | UniInt version 4.6.1.5

PI Data server Connection Status: CHPAP001 Writeable

Service Configuration

Service name: PI_Citect1 ID: 1

Display name: PI-PI_Citect1

Log on as: ● NT Service\PI_Citect1 ○ [Domain\]UserName

Startup Type: ● Auto ○ Manual ○ Disabled

Dependencies: tcpip PIBufss

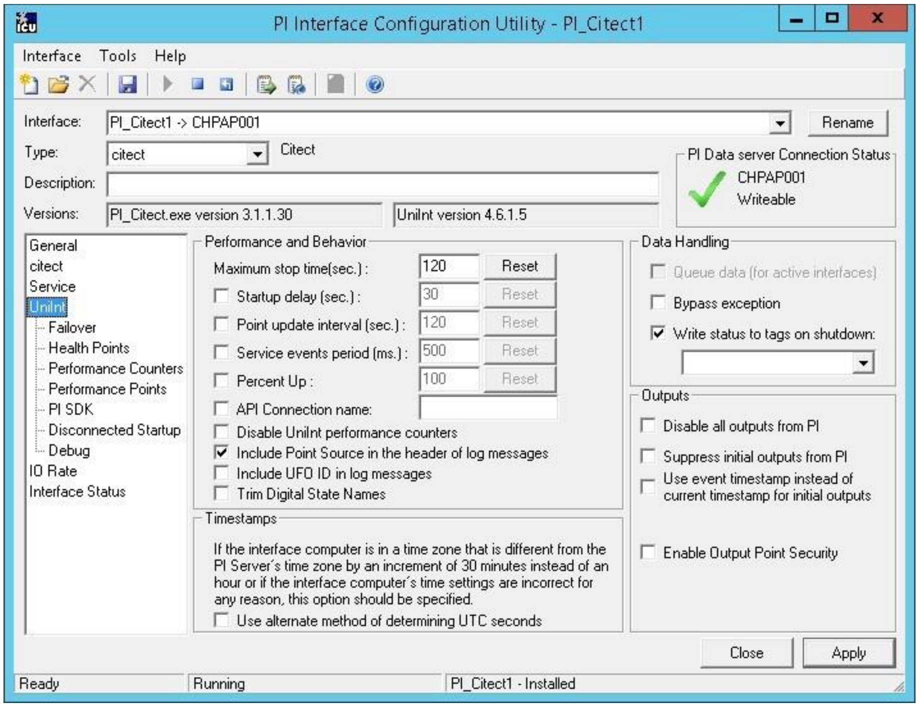
Installed services: AeLookupSvc ALG AppIDSvc Appinfo AppMgmt

Application Experience

Ready | Running | PI_Citect1 - Installed

10. Because the PI Citect interface is a UniInt-based interface, the UniInt page allows the user to access UniInt features through the PI ICU and to make changes to the behavior of the interface.

Figure 2-12 ICU — UniInt Configuration



Interface: PI_Citect1 -> CHPAP001

Type: citect Citect

Description:

Versions: PI_Citect.exe version 3.1.1.30 UniInt version 4.6.1.5

PI Data server Connection Status
✓ CHPAP001
Writeable

General
citect
Service
UniInt
- Failover
- Health Points
- Performance Counters
- Performance Points
- PI SDK
- Disconnected Startup
- Debug
IO Rate
Interface Status

Performance and Behavior
Maximum stop time(sec.) : 120
□ Startup delay (sec.) : 30
□ Point update interval (sec.) : 120
□ Service events period (ms.) : 500
□ Percent Up : 100
□ API Connection name:
□ Disable UniInt performance counters
☑ Include Point Source in the header of log messages
□ Include UFO ID in log messages
□ Trim Digital State Names

Timestamps
If the interface computer is in a time zone that is different from the PI Server's time zone by an increment of 30 minutes instead of an hour or if the interface computer's time settings are incorrect for any reason, this option should be specified.
□ Use alternate method of determining UTC seconds

Data Handling
□ Queue data (for active interfaces)
□ Bypass exception
☑ Write status to tags on shutdown:

Outputs
□ Disable all outputs from PI
□ Suppress initial outputs from PI
□ Use event timestamp instead of current timestamp for initial outputs
□ Enable Output Point Security

Ready | Running | PI_Citect1 - Installed

11. Keep the default values, but check the following boxes:

    a. **Include Point Source in the header log of messages**

    b. **Write status to tags on shutdown**

12. Uncheck the following box:

    Suppress initial outputs from PI

2.8 RS2 Technologies Access It! Universal.NET (E7)

RS2 Technologies Access It! Universal.NET pairs with the RS2 Door Controller to monitor access into the lab utilized in the build. The software then alerts the SIEM for any access into the facility, allowing the SIEM to correlate network events with physical access events.

2.8.1 Environment Setup

The following configuration matched requirements for the product relative to the use in the example solution:

- Microsoft Windows Server 2012 R2
- VM with CPU Quad Core 2.199 GHz
- VM with 8,192 MB of memory
- virtual hard disk containing 240 GB of storage
- .NET Framework 3.5

2.8.1.1 Product Installation

1. Start the provided **AIUniversalNET51044CD.exe.**
2. Follow the prompts for installation:
    a. Select **Stand-Alone/Server Installation.**
    b. Select **I do not have a SQL Server Installed.**
    c. When prompted to install SQL Server 2008 R2 Express Edition, select **Yes.**
    d. Select **Install Access It! Universal.NET.**
    e. When prompted to install a Stand-Alone Server version of Access It! Universal.NET, select **OK.**
    f. Select **Next >.**
    g. Read the license agreement and select **Next >** if the terms of the agreement are agreeable.
    h. Use the default installation folder **C:\Program Files(x86)\RS2 Technologies\Access It! Universal.NET\,** then select **Next >.**
3. When the installer is ready, select **Next >** to continue.
4. Select **Close** to exit the installer.

2.8.2 Post-Installation and Configuration

Post-installation and configuration are partially dependent on installation and configuration of the RS2 Technologies Door Controller (O4). If that is not complete, please follow that guide first before attempting to complete the post-installation of Access It! Universal.NET (E7).

1. Launch Access It! Universal.NET by selecting it from the **Start** menu.

2. Log in with the default username **Admin.** Leave password blank.

2.8.2.1 Connecting Access It! Universal.NET

1. Select **Hardware** under the Navigation pane, then select the **Channels** pane.
2. Select the **green + sign** in the top left corner to create a new channel.
3. For Channel Type, select **IP server.**
4. Ensure Protocol Type is secure copy protocol (**SCP).**
5. Ensure **Channel Enabled** is checked.
6. Select **Save.**
7. Select **SCPs** under the Navigation pane on the left.
8. Select the **green + sign** in the top left corner to create a new SCP.
9. Under the **General** tab …
    a. Select **EP-1502** for Model.
    b. Ensure **Device installed** is checked.
    c. Set **SCP time zone** to the local time zone of the door controller.
10. Under the **Comm.** tab …
    a. Ensure that the channel created in the previous steps is listed.
    b. Set the IP address to **10.100.2.150.**
    c. Ensure the port number is set to **3001.**
    d. Ensure the Encryption Settings is set to **None.**
11. Select **Save.**

2.8.2.2 Enable TCP/IP for Local SQL 2008 R2 Express Edition Server

1. Launch **Microsoft SQL Server Configuration Manager.**
2. Expand **SQL Server Network Configuration (32-bit).**
3. Select **Protocols** for **AIUNIVERSAL.**
4. Right-click on **TCP/IP,** then select **Properties.**

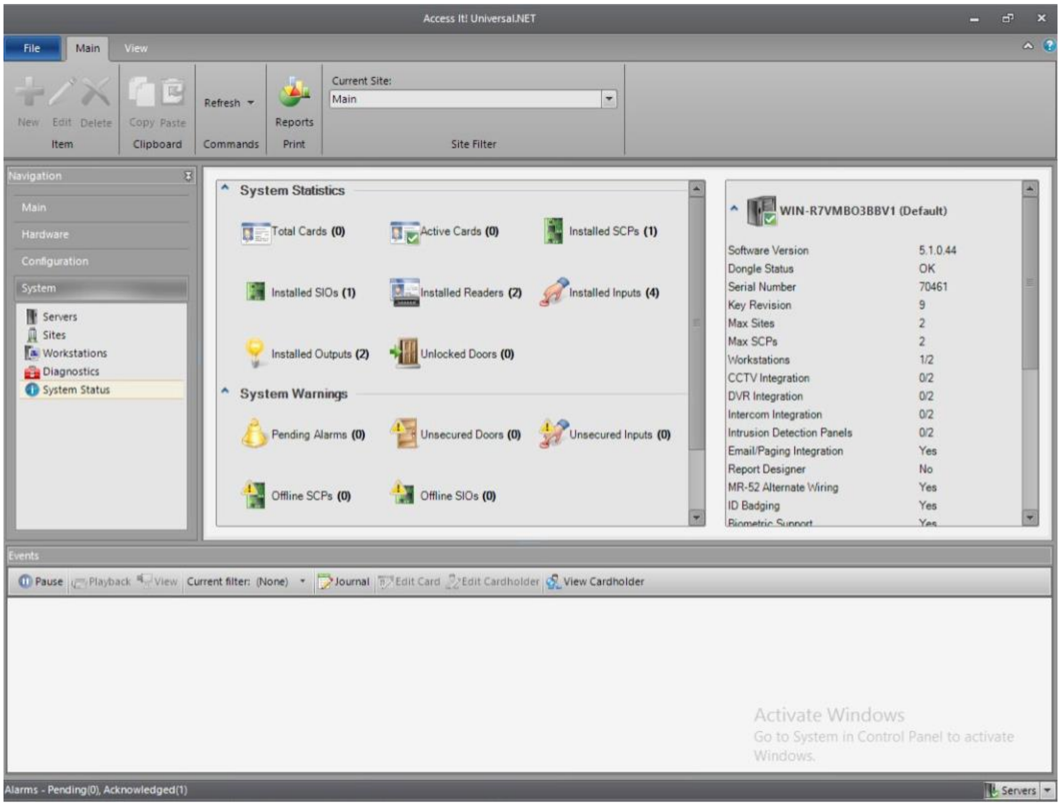
5. Select the **IP Addresses** tab.

6. Under **IP1,** ensure that **IP Address** is set to **0.0.0.0,** and **TCP Port** is set to **1433.**

7. Under **IPALL,** ensure that **TCP Dynamic Ports** is set to **52839,** and **TCP Port** is set to **1433.**

8. Restart the SQL Server. Select **SQL Server Services,** then right-click on **SQL Server (AIUNIVERSAL)** and select **Restart.**

Figure 2-13 System Status



System Statistics

Total Cards **(0)**
Active Cards **(0)**
Installed SCPs **(1)**
Installed SIOs **(1)**
Installed Readers **(2)**
Installed Inputs **(4)**
Installed Outputs **(2)**
Unlocked Doors **(0)**

System Warnings

Pending Alarms **(0)**
Unsecured Doors **(0)**
Unsecured Inputs **(0)**
Offline SCPs **(0)**
Offline SIOs **(0)**

WIN-R7VMBO3BBV1 (Default)

Software Version	5.1.0.44
Dongle Status	OK
Serial Number	70461
Key Revision	9
Max Sites	2
Max SCPs	2
Workstations	1/2
CCTV Integration	0/2
DVR Integration	0/2
Intercom Integration	0/2
Intrusion Detection Panels	0/2
Email/Paging Integration	Yes
Report Designer	No
MR-52 Alternate Wiring	Yes
ID Badging	Yes
Biometric Support	Yes

Alarms - Pending(0), Acknowledged(1)

2.9 RS2 Technologies Door Controller (O4)

The RS2 Technologies Door Controller is the physical piece to the Access It! Universal.NET product. This piece connects to the door itself, alerting the software to any access to the location.

2.9.1 Hardware Installation

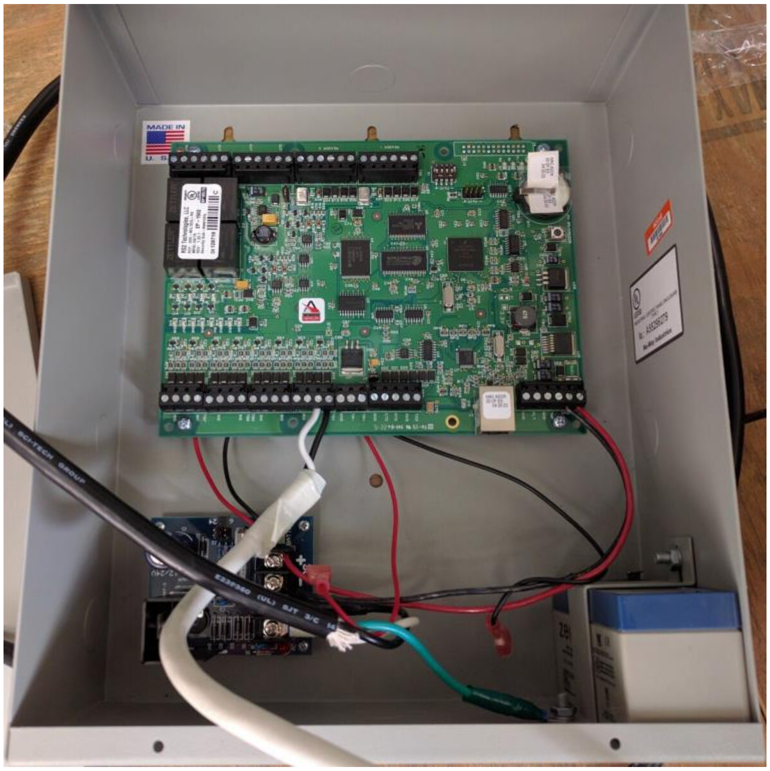
The following instructions detail the hardware installation for the door controller:

1. The fully assembled and closed case:

Figure 2-14 RS2 Door Controller Case

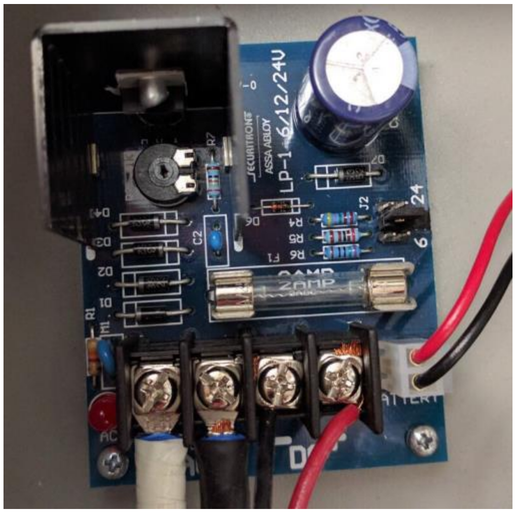
2. The interior modules:

Figure 2-15 Inside of RS2 Door Controller Case



3. The battery is pictured in the lower right corner of the case. The smaller board (AC/DC inverter) is pictured below:

Figure 2-16 AC/DC Inverter



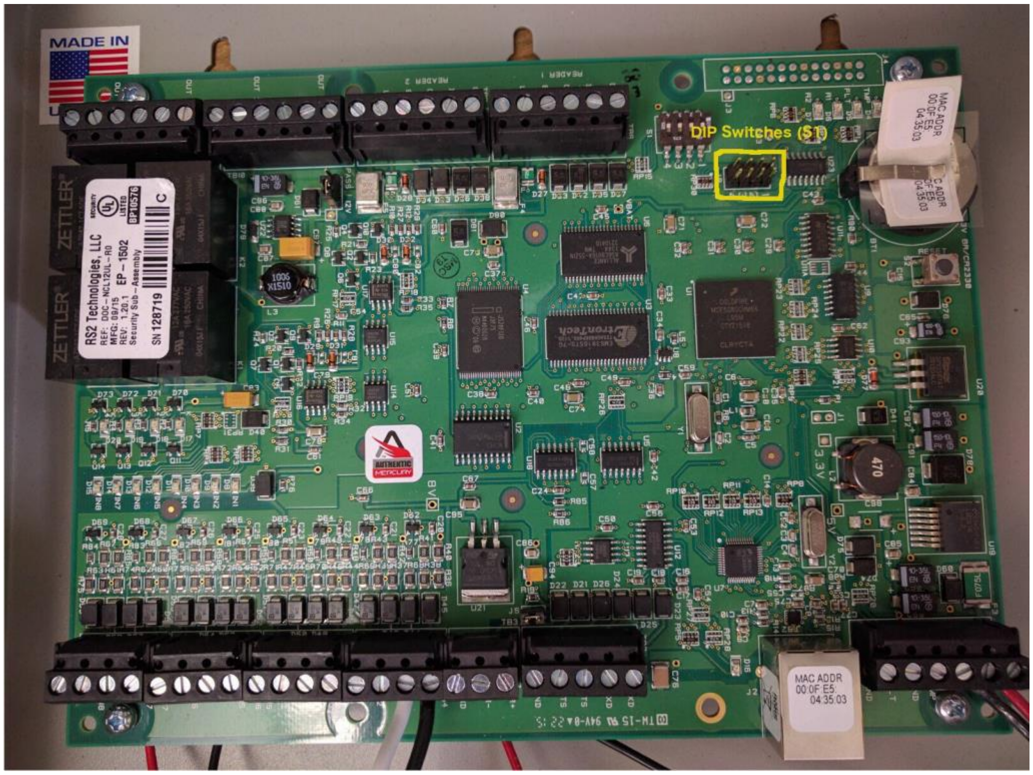
4. The two cables to the left are for positive and neutral input from a low voltage AC power supply. The ground (green) cable from the AC power supply attaches to a grounding nut on the case (pictured in the previous figure).

   The black and red cables to the left of AC are the DC outputs. These supply power directly to the door controller EP-1502 board.

   The other two black and red wires, connected to a harness, sit in the BATTERY port of the smaller board. These provide a trickle charge to the battery, which can be used in the event of a power outage.

   The larger EP-1502 board is pictured below:

Figure 2-17 EP-1502 Door Controller Board



5. The white and black wires on the bottom center of the figure go into **Door Contact 1 - IN1,** and these connect to the physical door-monitoring devices.

6. Power is supplied to the board via the bottom right corner posts, for 12 to 24 VDC (max 500 mA).

2.9.2 Connecting Hardware to Access It! Universal.NET

Conduct the following steps to connect the EP-1502 Door Controller Board to the Access It! Universal.NET software. The DIP switches referenced in these steps apply to those highlighted in yellow in the figure above.

1. Ensure that DIP Switch **DIP 2** is **ON** and **1, 3,** and **4** are **OFF.**

2. Power on the EP-1502.

3. Manually configure a computer to **192.168.0.100.**

4. Using a crossover cable, connect the computer to the EP-1502 board.

5. Open a web browser, and navigate to *http://192.168.0.251.*

6. Set DIP Switch **DIP 1** to **ON.**

7. Select Click Here to Login.

8. Select **Continue to this website (not recommended)**.

9. Log in with username **admin** and password **password.**

10. Select **Network** on the left-hand menu.

11. Select **Use Static IP configuration.**

    a. IP Address: **172.18.3.50**

    b. Subnet Mask: **172.18.0.0/16**

    c. Default Gateway: **172.18.0.1**

12. Click **OK.**

13. Click **Apply Setting.**

14. Click **Apply, Reboot.**

15. Wait 60 seconds for the EP-1502 to reboot.

16. Remove power from the EP-1502.

17. Set **all DIP switches** to **OFF.**

18. Remove the crossover cable, and connect to the network.

19. Apply power to the EP-1502 and follow the instructions in Section 2.8.2, Post-Installation and Configuration.

2.10 Radiflow 3180 (O14)

Radiflow's 3180 is a secure, ruggedized router used to handle connections between the OSIsoft Citect Interface and the OSIsoft PI Historian. This device ensures that proper communication is allowed while stopping any traffic that is not required.

2.10.1 Radiflow 3180 (O14) Installation Guide

1. Log in with the **su** user with the provided username and password.

2. Enter the following commands:

    a. `config terminal`

    b. `ip access-list extended 1001`

c. `permit tcp host 172.16.2.170 eq 5450 host 172.18.2.150 eq 5450 priority 1`

d. `exit`

e. `interface fastethernet 0/1`

f. `ip access-group 1001 in`

g. `exit`

h. `ip access-list extended 1002`

i. `permit tcp host 172.16.2.150 eq 5450 host 172.18.2.170 eq 5450 priority 2`

j. `exit`

k. `interface fastethernet 0/2`

l. `ip access-group 1002 in`

m. `exit`

n. `ip access-list extended 2001`

o. `deny ip any any priority 51`

p. `exit`

q. `interface fastethernet 0/1`

r. `ip access-group 2001 in`

s. `exit`

t. `ip access-list extended 2002`

u. `deny ip any any priority 52`

v. `exit`

w. `interface fastethernet 0/2`

x. `ip access-group 2002 in`

y. `exit`

z. `write start`

aa. `reload`

2.11 Radiflow iSID (O11)

Radiflow's iSID product is a software industrial intrusion detection system that monitors for anomalies within the control systems network and builds a network topology model.

2.11.1 Environment Setup

Radiflow supplies an open virtual appliance (OVA) to be deployed to a virtualized environment, so environment setup should be minimal.

2.11.2 Product Installation

1. After deploying the vendor-provided OVA on a virtualized platform, navigate to **/home/radiflow/isid.**

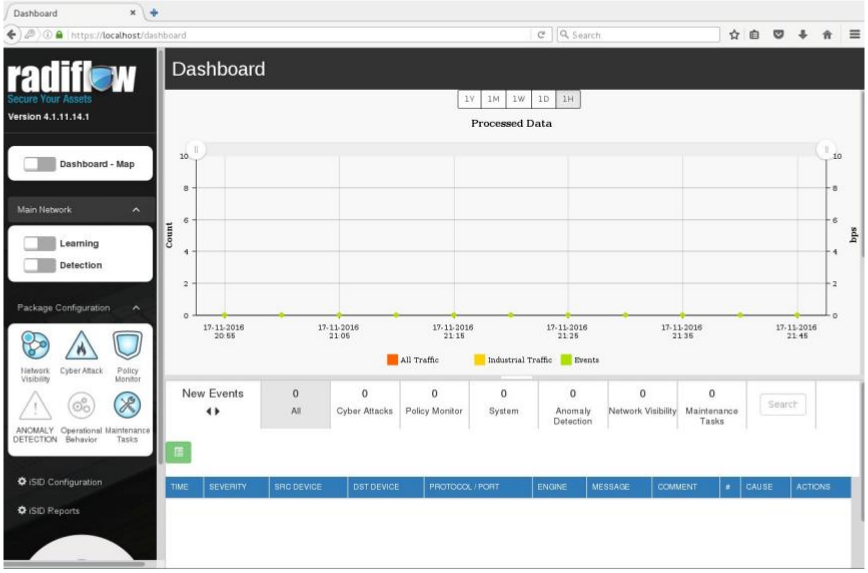
2. Modify the **server.conf** file to reflect the IP address of the syslog server:

```
rfids_remote_syslog_server=172.18.0.50

poco_source_dir=/home/radiflow/tools/poco
```

3. Run **sudo ./build_install_all.sh stop start install config bridge**.

4. Open a web browser, and navigate to *https://localhost/dashboard.*

Figure 2-18 Radiflow iSID Web Dashboard



5. Toggle the **Learning** switch on the left bar under Main Network.

Allow learning to take place for **5 to 7 days.**

6. Toggle the **Detection** switch on the left bar under Main Network.
7. Setup and configuration are now complete.

2.12 RSA Archer Security Operations Management (E13)

Governance, risk, and compliance (GRC) platforms allow an organization to link strategy and risk, adjusting strategy when risk changes, while remaining in compliance with laws, regulations, and security policies. RSA Archer Security Operations Management, based in part on the RSA Archer GRC platform, was used to perform the task of the Analysis Workflow Engine and Security Incident Response and Management.

For more information, visit …

- https://www.rsa.com/en-us/resources/rsa-netwitness-secops-manager
- https://www.rsa.com/en-us/products/threat-detection-and-response/rsa-netwitness-secops-manager
- https://www.rsa.com/en-us/products/threat-detection-and-response/network-monitoring-and-forensics

2.12.1 System Requirements

This build installed a multihost RSA Archer GRC platform node on a VMware VM with the Microsoft Windows Server 2012R2 operating system to provide the Security Incident Response Management environment needed.

Note: *All components, features, and configurations presented in this guide reflect what we used based on vendors' best practices and requirements. Please refer to vendors' official documentation for complete instructions for other options.*

2.12.2 Preinstallation

We chose the multihost deployment option for installing and configuring the GRC platform on multiple VMs under the Microsoft Windows Server 2012R2 Operating System. The web application and services are running on one server, instance database/Microsoft SQL Server is running on one server, and integration components for Security Incident Response are running on a third server. Below are the preinstallation tasks that we performed prior the RSA Archer installation:

- Operating System: Windows Server 2012R2 Enterprise
- Database: Microsoft SQL Server 2012 Enterprise (x64)

Follow Microsoft's installation guidelines and steps to install the SQL Server Database Engine and SQL Server Management tools. Refer to https://msdn.microsoft.com/en-us/library/bb500395(v=sql.110).aspx for additional details.

We used the following configuration settings during the installation and configuration process. We also created the required database instances and users for the RSA Archer installation. Test the database instances by using different users to verify the login permissions on all database instances and configuration databases to ensure that database owners have sufficient privileges and correct user mappings.

Table 2-2 RSA Archer Configuration Settings

Setting	Value
Collation settings set to case insensitive for instance database	SQL_Latin1_general_CP1_CI_AS
SQL compatibility level set appropriately	SQL Server 2012 - 110
Locale set	English (United States)
Database server time zone	EST
Platform language	English
Create both the instance and configuration databases within a single SQL Server instance. For migration, create only the configuration database.	Database names: *grc-content* *grc-config*
User Account set to Database Owner role	*grc-content-archeruser* *grc-config-archeruser*
Recovery Model	Simple (configuration and instance databases)
Auto Shrink	False (configuration database)
Auto-Growth	Set it for (instance database)
Max Degree of Parallelism	1 (configuration and instance databases)

Web and Services

- Microsoft Internet Information Services (IIS) 8
- Microsoft .NET Framework 4.5

Use Server Manager for installing IIS and .NET Framework, referring to http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012 for detailed steps and corresponding screenshots.

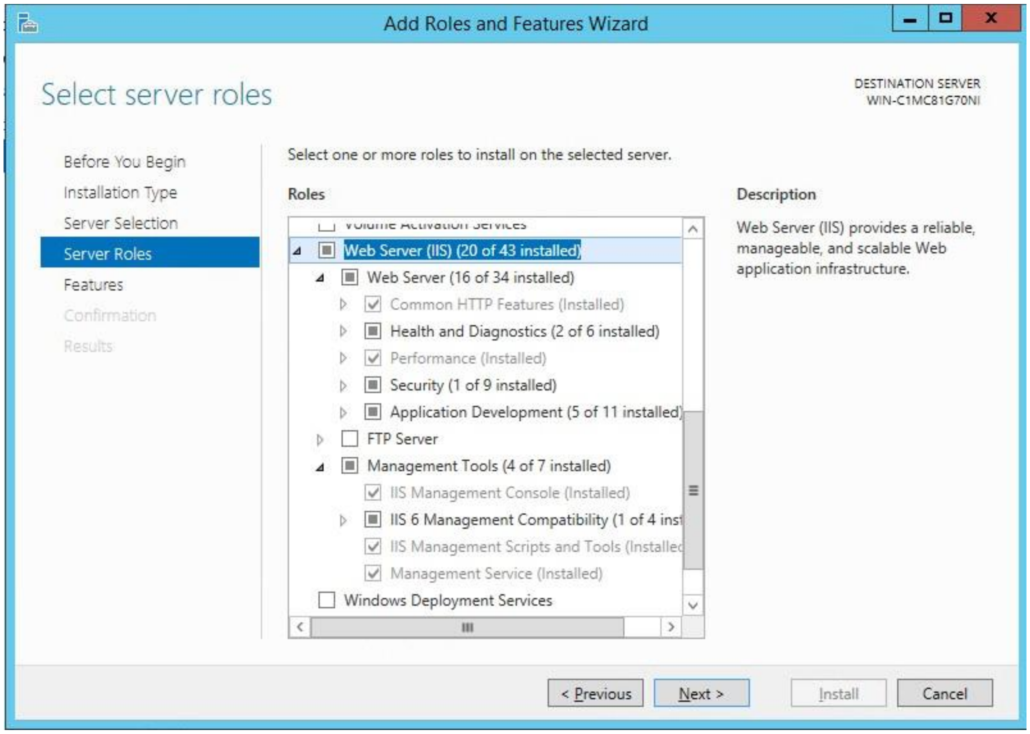
First install IIS and then install the .NET Framework.

Table 2-3 below summarizes the required IIS components and .NET Framework features followed by the screenshots.

Table 2-3 IIS Components and .NET Framework

Required Option	Value
IIS	
Common (http) Features	Default Document Directory Browsing http Errors Static Content
Health and Diagnostics	http Logging
Application Development	.NET Extensibility 4.5 Active Server Pages (ASP) .NET 4.5 Internet Server Application Programming Interface (ISAPI) Extensions ISAPI Filters
Security	Request Filtering
Management Tools	IIS Management Console
.NET Framework	
.NET Framework 4.5 Features	.NET Framework 4.5 ASP.NET 4.5
WCF Services	http Activation TCP Port Sharing

Figure 2-19 Web Server (IIS) Components Section



Select server roles

DESTINATION SERVER
WIN-C1MC81G70NI

Select one or more roles to install on the selected server.

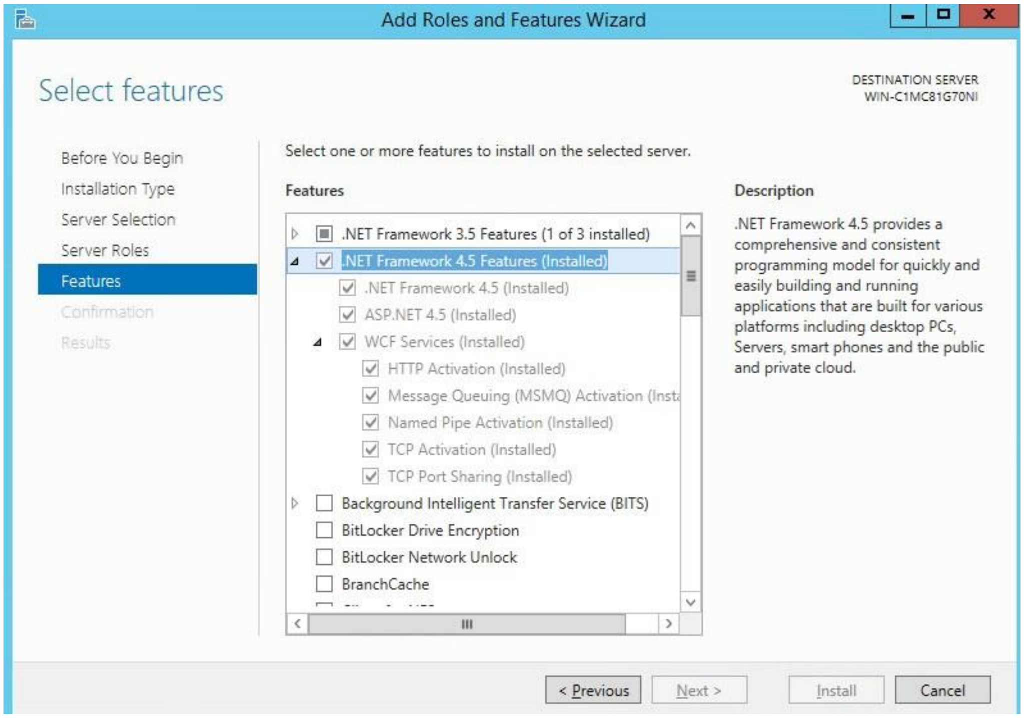
Roles

- □ Volume Activation Services
- ■ Web Server (IIS) (20 of 43 installed)
  - ■ Web Server (16 of 34 installed)
    - ☑ Common HTTP Features (Installed)
    - ■ Health and Diagnostics (2 of 6 installed)
    - ☑ Performance (Installed)
    - ■ Security (1 of 9 installed)
    - ■ Application Development (5 of 11 installed)
  - □ FTP Server
  - ■ Management Tools (4 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - ■ IIS 6 Management Compatibility (1 of 4 inst
    - ☑ IIS Management Scripts and Tools (Installec
    - ☑ Management Service (Installed)
- □ Windows Deployment Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 2-20 .NET Framework 4.5 Features Selection



Select one or more features to install on the selected server.

Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ☑ .NET Framework 4.5 Features (Installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5 (Installed)
  - ☑ WCF Services (Installed)
    - ☑ HTTP Activation (Installed)
    - ☑ Message Queuing (MSMQ) Activation (Insta
    - ☑ Named Pipe Activation (Installed)
    - ☑ TCP Activation (Installed)
    - ☑ TCP Port Sharing (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache

Description

.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

Microsoft Office 2013 Filter Pack

Download it from Microsoft website http://www.microsoft.com/en-us/download/details.aspx?id=40229 and install it.

Java Runtime Environment (JRE) 8

Download and install JRE 8. Refer to http://www.oracle.com/technetwork/java/javase/install-windows-64-142952.html for details.

Note: *All preinstallation software must be installed and configured before installing RSA Archer.*

2.12.3 Installation

1. Create folders **C:\ArcherFiles\Indexes** and **C:\ArcherFiles\Logging** (will be used later).
2. Obtain/Download the installer package from RSA; extract the installation package.
3. Run installer.
   a. Open installation folder; right-click on **ArcherInstall.exe.**

b. Select **Run as Administrator.**

c. Click **OK** to run the installer.

d. Follow the prompts from the installer for each step, set the value, and click **Next.**

e. Select all components (Web Application, Services, Instance Database) for installation, then click **Next.**

f. Specify the X.509 Certification by selecting it from the checklist (create new cert or use existing cert). We created a new cert.

g. Set the Configuration Database options with the following properties:

SQL Server:	<ip address of SQL Server>
Login Name:	######
Password:	######
Database:	grc-config (This is the configuration database we created during the preinstallation process.)

h. Set the Configuration Web Application options with the following properties:

Website:	Default Website
Destination Directory:	Select Install in an IIS application option with RSAarcher as the value

i. Set Configuration of the Service Credentials.

Select **Use the Local System Account to Run All** from the checklist.

j. Set the Services and Application Files paths with the following properties:

i. Services: use the default value **C:\Program Files\RSA Archer\Services\.**

ii. Application Files: use the default value **C:\Program Files\RSA Archer\.**

k. Set the Log File Path to **C:\ArcherFiles\Logging.**

l. Perform the installation by clicking **Install,** wait for the installer to complete installing all components, then click **Finish.** The RSA Archer Control Panel opens.

2.12.4 Post-Installation

2.12.4.1 Configure the Installation Settings

Verify and set the configurations for the following by clicking on **RSA Archer Control Panel > Installation Settings,** then select corresponding sections:

1. Logging Section
    a. Path: **Archer Files\Logging**
    b. Level: **Error**
2. Locale and Time Zone Section
    a. Locale: **English (United States)**
    b. Time Zone: **(UTC-05:00) Eastern Time (US & Canada)**
3. On the Toolbar, click **Save.**
4. Create the Default GRC Platform Instance.
    a. Start the RSA Archer Queuing Service by doing the following steps:
        i. Go to **Start.**
        ii. Open **Server Manager.**
        iii. Locate **RSA Archer Queuing** in the list under the **SERVICES** section.
        iv. Right-click **RSA Archer Queuing,** and click **Start.**
    b. Add a new instance by doing the following steps:
        i. Open the **RSA Archer Control Panel.**
        ii. In **Instance Management,** double-click **Add New Instance.**
        iii. Enter **SituationalAwareness** as the **Instance Name,** then click **Go.**
        iv. Complete the properties as needed.
    c. Configure the Database Connection Properties by doing the following steps:
        i. Open the RSA Archer Control Panel.
        ii. In the **Database** tab, go to the **Connection Properties** section.
        iii. In **Instance Management,** double-click the **SituationalAwareness** instance.

    d. In the **Database** tab, set up the following:

        i. SQL Server: **<ip address of SQL Server>**

        ii. Login name: **xxxxxx**

        iii. Password: **xxxxxx**

        iv. Database: **grc-content**

5. Click on the **Test Connection** link to make sure the **Success** message appears.

6. Configure the **General Properties** by doing the following steps:

    a. Open **RSA Archer Control Panel.**

    b. Go to **Instance Management.**

    c. Under **All Instances,** click on **SituationalAwareness.**

    d. In the **General** tab, set up the following:

        i. **File Repository** section — Path **C:\ArcherFiles\Indexes**.

        ii. **Search Index** section — **Content Indexing:** Check on Index design language only; Path: **C:\ArcherFiles\Indexes\SituationalAwareness**

7. Configure the **Web Properties** by doing the following steps:

    a. Open the **RSA Archer Control Panel.**

    b. Go to **Instance Management.**

    c. Under **All Instances,** click on **SituationalAwareness.**

    d. In the **Web** tab, set up the following:

        i. Base uniform resource locator (URL): *http://localhost/RSAArcher/*

        ii. Authentication URL: **default.aspx**

8. Change **SysAdmin** and **Service Account** passwords by doing the following steps:

    a. Open the **RSA Archer Control Panel.**

    b. Go to **Instance Management.**

    c. Under **All Instances,** click on **SituationalAwareness.**

    d. Select the **Accounts** tab.

    e. Change the password on the page by using a strong password.
    f. Complete the Default GRC Platform Instance Creation by clicking **Save** on the toolbar.

9. Register the Instance by doing the following steps:
    a. Open the **RSA Archer Control Panel.**
    b. Go to **Instance Management.**
    c. Under **All Instances,** right-click on **SituationalAwareness.**
    d. Select **Update Licensing,** enter the following information, then click on **Active:**
        i. **Serial Number** (obtained from RSA)
        ii. **Contact Info** (First Name, Last Name, Company, etc.)
        iii. **Activation Method** (select Automated)
10. Activate the Archer Instance by doing the following steps:
    a. Start the **RSA Archer Services.**
    b. On **Server Manager,** go to **Local Services** or **All Services.**
    c. Locate the following services, right-click on each service, and click **Start.**
        i. **RSA Archer Configuration**
        ii. **RSA Archer Job Engine**
        iii. **RSA Archer Lightweight Directory Access Protocol (LDAP) Synchronization**
    d. Restart the **RSA Archer Queuing Service.**
        i. Open **Server Manager.**
        ii. Go to **Local Services** or **All Services.**
        iii. Locate the **RSA Archer Queuing.**
        iv. Right-click on **RSA Archer Queuing,** and click **Restart.**
    e. Rebuild the Archer Search Index.
        i. Open **RSA Archer Control Panel.**
        ii. Go to **Instance Management.**

iii. Under **All Instances,** right-click on **SituationalAwareness,** then click on **Rebuild Search Index.**

11. Configure and activate the Web Role (IIS).

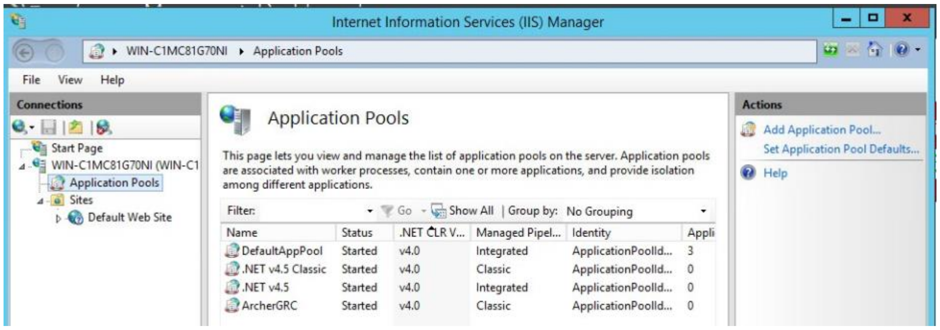
    a. Set up **Application Pools** as shown in the screenshot.

        i. Open **Server Manager.**

        ii. Navigate to **Tools > IIS Manager > Application Pools** (in the left side bar).

        iii. Right-click to add applications (.NET, ArcherGRC, etc.); example screenshot is below.

Figure 2-21 Application Pools



Application Pools

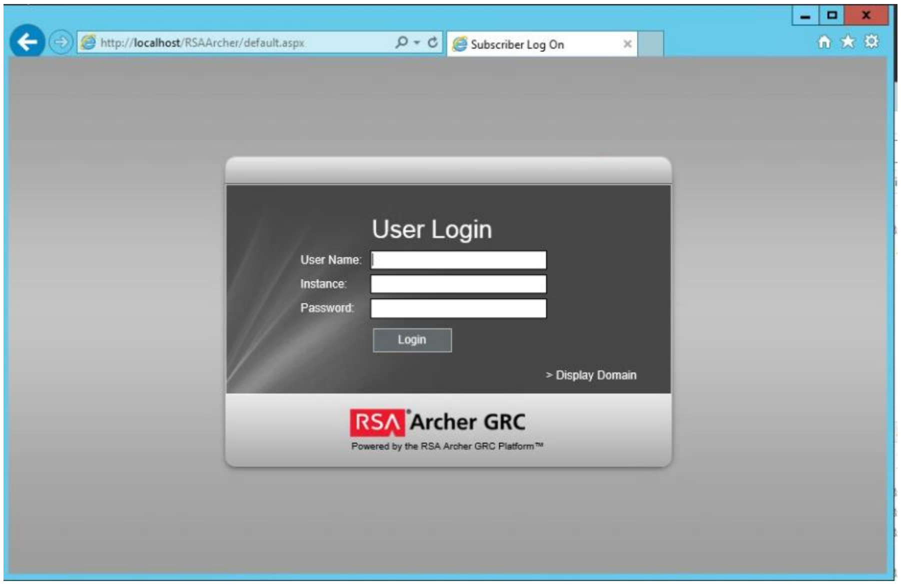
This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Appli
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	3
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
ArcherGRC	Started	v4.0	Classic	ApplicationPoolId...	0

    b. Restart IIS.

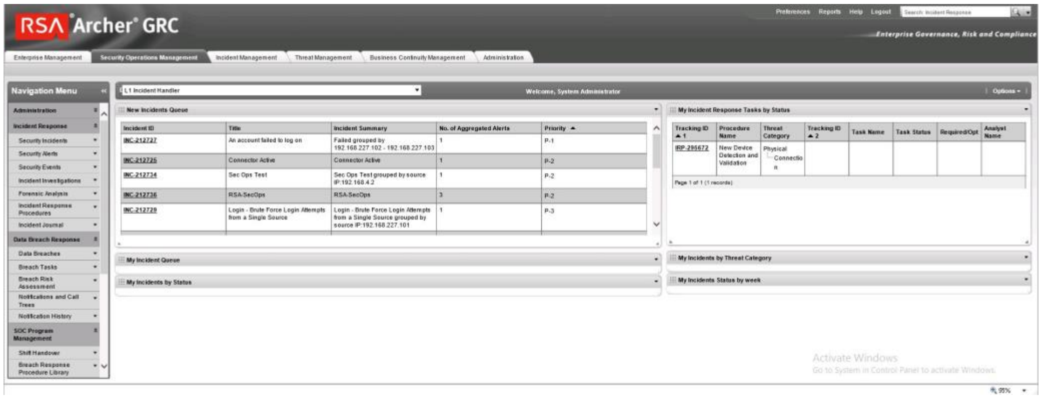
12. Verify that RSA Archer GRC is accessible by opening a browser and inserting the **Base** and **Authentication URL** from the Web tab of the RSA Archer Control Panel. The RSA Archer GRC Login screen appears as shown below.

Figure 2-22 RSA Archer User Login



13. Log in to **SituationalAwareness** Instance.

Figure 2-23 Security Operations Management Tab



New Incidents Queue

Incident ID	Title	Incident Summary	No. of Aggregated Alerts	Priority ▲
INC-212727	An account failed to log on	Failed grouped by 192.168.227.102 - 192.168.227.103	1	P-1
INC-212725	Connector Active	Connector Active	1	P-2
INC-212734	Sec Ops Test	Sec Ops Test grouped by source IP:192.168.4.2	1	P-2
INC-212736	RSA-SecOps	RSA-SecOps	3	P-2
INC-212729	Login - Brute Force Login Attempts from a Single Source	Login - Brute Force Login Attempts from a Single Source grouped by source IP:192.168.227.101	1	P-3

My Incident Response Tasks by Status

Tracking ID ▲ 1	Procedure Name	Threat Category	Tracking ID ▲ 2	Task Name	Task Status	Required/Opt	Analyst Name
IRP-295672	New Device Detection and Validation	Physical Connection					

Page 1 of 1 (1 records)

2.12.5 Configuration of ArcSight ESM to RSA Archer Security Operations Management

After a base installation of RSA Archer and the associated RSA Archer Security Operations Management functionality, an additional configuration is required to connect the Security Incident Response use case to external data providers, such as ArcSight ESM. In this environment, this required an installation and configuration of the RSA Archer Unified Collector Framework on the third Windows Server in the Archer multihost setup. For full details, please consult the installation and configuration guide for the RSA Collector Framework.

1. Create user within RSA Archer framework for the Collector Framework Web Services access. For testing, this user was granted appropriate privileges to read and write data for Security Alert Data originating from ArcSight.
2. Execute Archer Unified Collector Framework installer. When prompted, provide the Archer Collector Framework Web Services username and password created in step 1.
3. When prompted, follow the instructions for importing the Data Feed for the Unified Collector Framework (UCF).

2.12.6 Additional ArcSight Integration Configuration

Additional details for the ArcSight installation can be found in the RSA Archer Security Operations Management Implementation Guide from RSA. Below are the steps that were followed specifically for this environment to enable the connection to ArcSight.

1. Create ArcSight Forwarding Connector User.
    a. From **ArcSight ESM Console**:
        i. Create a new group under custom user groups and name as follows: **FwdConnector**
        ii. Create a new user under that group and name as follows: **FwdConnectorUser**
        iii. Set the user type to **Forwarding Connector.**
        iv. For additional detail, see pages 7 – 9 of FwdConn_ConfigGuide_7.0.7.7286.0.pdf.
2. Install **SuperConnector** (also known as Forwarding Connector).
    a. From the **ArcSight ESM Manager command line** …
        i. Su to **arcsight** user
        ii. Find the install file **ArcSight-7.0.7.7286.0-Superconnector.bin,** and run the following command (to allow the installation to execute):

```
chmod + x ArcSight-7.0.7.7286.0-Superconnector.bin
```

        iii. Make a folder for the connector:

e.g., `mkdir /opt/arsight/superconnector`

iv. As **arcsight** user, execute the installation file:

   ./ArcSight-7.0.7.7286.0-Superconnector.bin

v. Choose to install to the folder that was just made:

   e.g., **/opt/arcsight/superconnector**

vi. Accept defaults.

vii. Choose **Don't Create Links.**

viii. **Install.**

ix. **Next.**

x. Enter the ArcSight ESM Manager name: **[hostname]**

xi. Enter the ArcSight ESM Manager port: **8443**

xii. Enter the name of the user that was just created: **FwdConnectorUser**

xiii. Enter the ArcSight Manager password: ____________

xiv. Import the manager certificate.

xv. Select **CEF Syslog.**

xvi. Enter the IP address of the RSA Archer UCF IP, Port: **514**, **TCP** (not UDP)

xvii. Select **Next** twice, **Exit, Done.**

xviii. As user **root,** install the service as follows:

```
/opt/arcsight/superconnector/current/bin/arcsight agentsvc -i
-u arcsight
```

xix. Start the service as follows:

```
./etc/init.d/arc_superagent_ng start
```

Note: *If another forwarding destination needs to be added, see page 32 of FwdConn_ConfigGuide_7.0.7.7286.0.pdf.*

2.12.7 Sample Use Case Demonstration

For the use of the Security Incident Response use case and integration with ArcSight, the following sample use case was simulated:

1. Event 1

    An individual enters a substation, an event that is detected by a door controller. This door reader is able to log its data or a SIEM, such as ArcSight, including identifying information (such as a badge ID or user).

2. Event 2

    A new device appears on the substation network, detected by a tool (for example, CyberLens). This data is reported via a log event to a SIEM such as ArcSight.

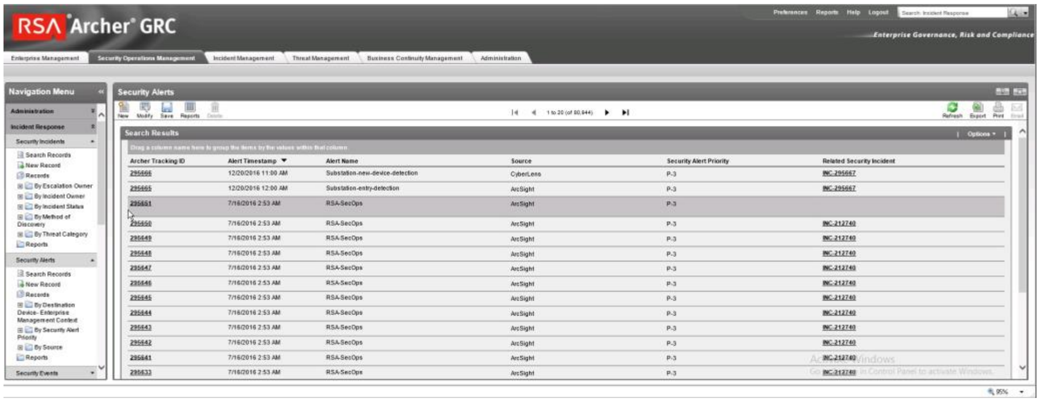
3. Action 1

    An Alert/Correlation Rule appropriate for these events fires in ArcSight, triggering message delivery to RSA Archer Security Incident Response for review and possible action.

Below are screenshots and narratives of this sample use case within the RSA Archer Security Operations Management Use Case.

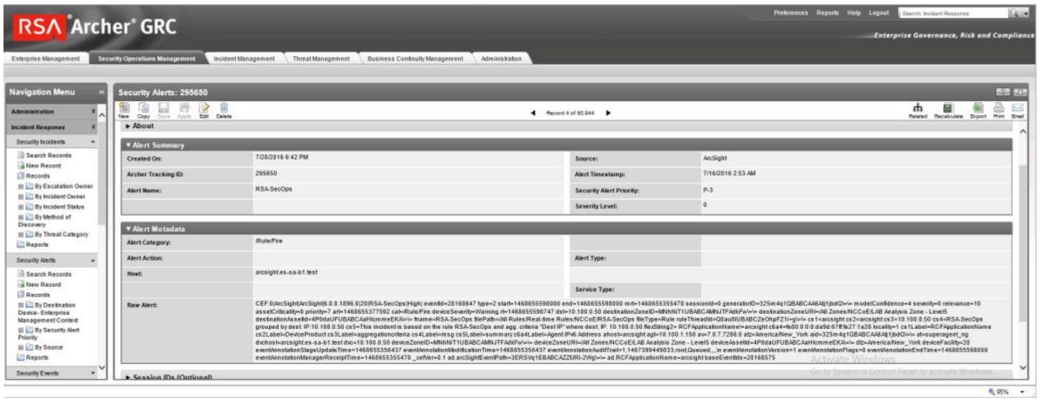
1. User is logged into the Archer Interface and is examining the Security Alerts that have been delivered for review.

Figure 2-24 Multiple Security Alerts within the RSA Archer Console



Archer Tracking ID	Alert Timestamp	Alert Name	Source	Security Alert Priority	Related Security Incident
295666	12/20/2016 11:00 AM	Substation-new-device-detection	CyberLens	P-3	INC-295667
295665	12/20/2016 12:00 AM	Substation-entry-detection	ArcSight	P-3	INC-295667
295651	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	
295650	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295649	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295648	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295647	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295646	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295645	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295644	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295643	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295642	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295641	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740
295633	7/16/2016 2:53 AM	RSA-SecOps	ArcSight	P-3	INC-212740

Figure 2-25 Sample Message from ArcSight, Showing Raw Log Message/Alert and Parsing with Normalization


RSA Archer GRC
Preferences Reports Help Logout
Enterprise Governance, Risk and Compliance
Enterprise Management
Security Operations Management
Incident Management
Threat Management
Business Continuity Management
Administration
Navigation Menu
New Copy Save Apply Edit Delete
Record 4 of 80,944
Related Recalculate Export Print Email
95%

Security Alerts: 295650

▸ About

▾ Alert Summary

Created On:	7/28/2016 6:42 PM	Source:	ArcSight
Archer Tracking ID:	295650	Alert Timestamp:	7/16/2016 2:53 AM
Alert Name:	RSA-SecOps	Security Alert Priority:	P-3
		Severity Level:	0

▾ Alert Metadata

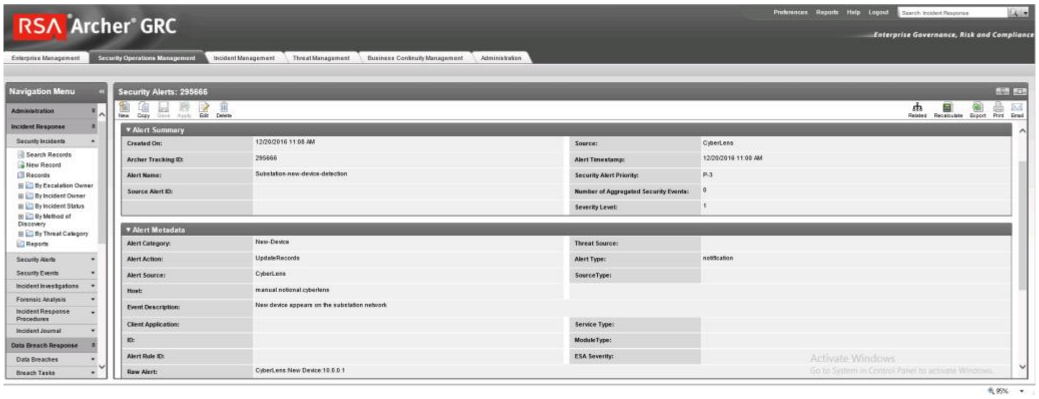
Alert Category:	/Rule/Fire		
Alert Action:		Alert Type:	
Host:	arcsight.es-sa-b1.test		
		Service Type:	

Raw Alert:

```
CEF:0|ArcSight|ArcSight|6.8.0.1896.0|20|RSA-SecOps|High| eventId=28168647 type=2 start=1468655598000 end=1468655598000 mrt=1468655355478 sessionId=0 generatorID=325m4q1QBABCAA6Aj1jbdQ\=\= modelConfidence=4 severity=0 relevance=10
assetCriticality=0 priority=7 art=1468655377592 cat=/Rule/Fire deviceSeverity=Warning rt=1468655598747 dst=10.100.0.50 destinationZoneID=MNhNiT1UBABCAMNJTFAdkFw\=\= destinationZoneURI=/All Zones/NCCoE/LAB Analysis Zone - Level5
destinationAssetId=4P0daUFUBABCAaHlcmmeEKA\=\= fname=RSA-SecOps filePath=/All Rules/Real-time Rules/NCCoE/RSA-SecOps fileType=Rule ruleThreadId=Q0au8IUBABCZeOhpFZ1i+g\=\= cs1=arcsight cs2=arcsight cs3=10.100.0.50 cs4=RSA-SecOps
grouped by dest. IP:10.100.0.50 cs5=This incident is based on the rule RSA-SecOps and agg. criteria "Dest IP" where dest. IP: 10.100.0.50 flexString2= RCFApplicationName\=arcsight c6a4=fe80:0:0:0:da9d:67ff:fe27:1a28 locality=1 cs1Label=RCFApplicationName
cs2Label=DeviceProduct cs3Label=aggregationcriteria cs4Label=msg cs5Label=summary c6a4Label=Agent IPv6 Address ahost=arcsight agt=10.100.1.150 av=7.0.7.7286.0 atz=America/New_York aid=325m4q1QBABCAA6Aj1jbdQ\=\= at=superagent_ng
dvchost=arcsight.es-sa-b1.test dvc=10.100.0.50 deviceZoneID=MNhNiT1UBABCAMNJTFAdkFw\=\= deviceZoneURI=/All Zones/NCCoE/LAB Analysis Zone - Level5 deviceAssetId=4P0daUFUBABCAaHlcmmeEKA\=\= dtz=America/New_York deviceFacility=20
eventAnnotationStageUpdateTime=1468655356437 eventAnnotationModificationTime=1468655356437 eventAnnotationAuditTrail=1,1467399449833,root,Queued,,,\n eventAnnotationVersion=1 eventAnnotationFlags=0 eventAnnotationEndTime=1468655598000
eventAnnotationManagerReceiptTime=1468655355478 _cefVer=0.1 ad.arcSightEventPath=3ERSVq1EBABCAZZ8URI-2Wg\=\= ad.RCFApplicationName=arcsight baseEventIds=28168575
```

▸ Session IDs (Optional)

Figure 2-26 Sample Message Showing Alert Indicating New Device Detected at Substation


RSA Archer GRC
Preferences Reports Help Logout
Enterprise Governance, Risk and Compliance
Enterprise Management
Security Operations Management
Incident Management
Threat Management
Business Continuity Management
Administration
Navigation Menu
New Copy Save Apply Edit Delete
Related Recalculate Export Print Email
95%

Security Alerts: 295666

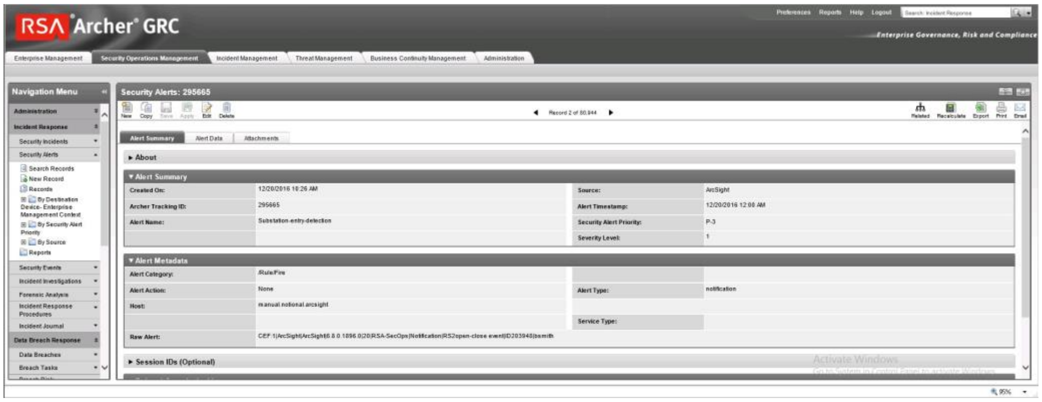
▾ Alert Summary

Created On:	12/20/2016 11:08 AM	Source:	CyberLens
Archer Tracking ID:	295666	Alert Timestamp:	12/20/2016 11:00 AM
Alert Name:	Substation-new-device-detection	Security Alert Priority:	P-3
Source Alert ID:		Number of Aggregated Security Events:	0
		Severity Level:	1

▾ Alert Metadata

Alert Category:	New-Device	Threat Source:	
Alert Action:	UpdateRecords	Alert Type:	notification
Alert Source:	CyberLens	SourceType:	
Host:	manual.notional.cyberlens		
Event Description:	New device appears on the substation network		
Client Application:		Service Type:	
ID:		ModuleType:	
Alert Rule ID:		ESA Severity:	
Raw Alert:	CyberLens New Device:10.0.0.1		

Figure 2-27 Sample Message Showing an Alert Indicating Badged Entry Detected at Substation



Security Alerts: 295665

Record 2 of 80,844

Alert Summary

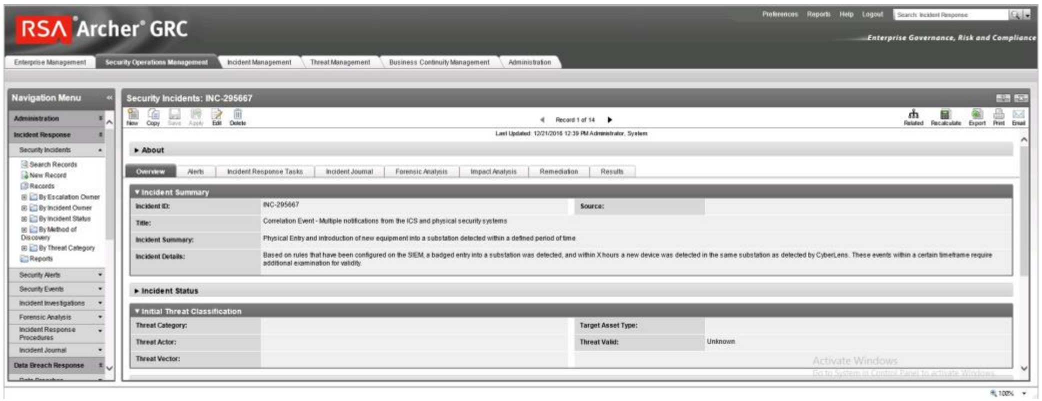
Created On:	12/20/2016 10:26 AM	Source:	ArcSight
Archer Tracking ID:	295665	Alert Timestamp:	12/20/2016 12:00 AM
Alert Name:	Substation-entry-detection	Security Alert Priority:	P-3
		Severity Level:	1

Alert Metadata

Alert Category:	/Rule/Fire		
Alert Action:	None	Alert Type:	notification
Host:	manual.notional.arcsight		
		Service Type:	
Raw Alert:	CEF:1|ArcSight|ArcSight|6.8.0.1896.0|20|RSA-SecOps|Notification|RS2open-close event|ID203948|bsmith		

2. Based on rule or physical examination, these alerts are deemed Incident Investigation material and instantiate a full Incident Response Workflow.

Figure 2-28 New Incident Response Workflow Record Started, Documented with Title, Summary, Details



Security Incidents: INC-295667

Record 1 of 14

Last Updated: 12/21/2016 12:39 PM Administrator, System

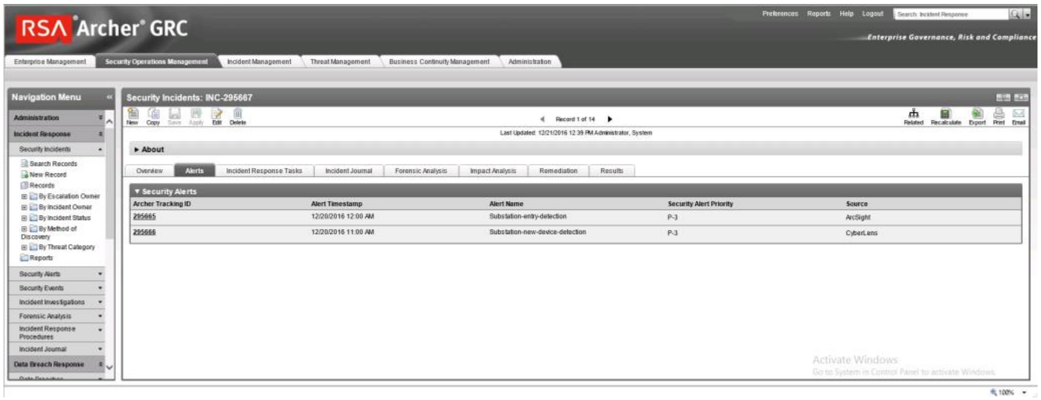
Incident Summary

Incident ID:	INC-295667	Source:	
Title:	Correlation Event - Multiple notifications from the ICS and physical security systems		
Incident Summary:	Physical Entry and introduction of new equipment into a substation detected within a defined period of time		
Incident Details:	Based on rules that have been configured on the SIEM, a badged entry into a substation was detected, and within X hours a new device was detected in the same substation as detected by CyberLens. These events within a certain timeframe require additional examination for validity.		

Initial Threat Classification

Threat Category:		Target Asset Type:	
Threat Actor:		Threat Valid:	Unknown
Threat Vector:			

Figure 2-29 Incident Record Alerts Tab, Showing the Association of Two Events Attached to This Incident Response Investigation Record



Security Incidents: INC-295667

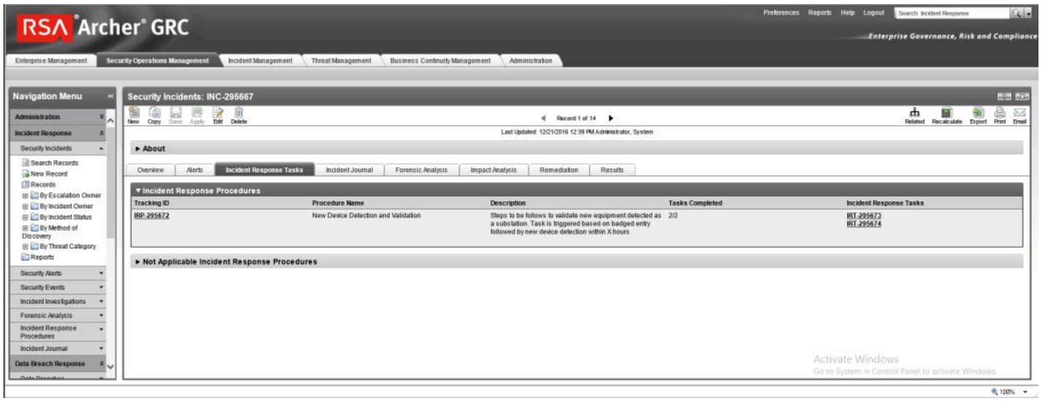
Last Updated: 12/21/2016 12:39 PM Administrator, System

Security Alerts

Archer Tracking ID	Alert Timestamp	Alert Name	Security Alert Priority	Source
295665	12/20/2016 12:00 AM	Substation-entry-detection	P-3	ArcSight
295666	12/20/2016 11:00 AM	Substation-new-device-detection	P-3	CyberLens

3. Based on Incident type, Appropriate Incident Response Procedure(s) and related tasks are assigned to the Record for completion. This directly represents the defined policy and procedure(s) outlines and maintained by an organization's security policy program and response.

Figure 2-30 Incident Response Procedure with Two Related Tasks Assigned to the Incident Response Record



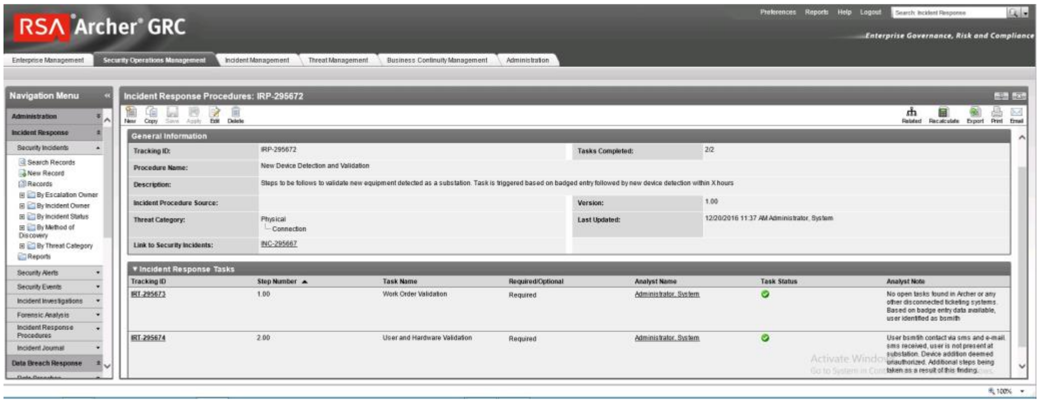
Security Incidents: INC-295667

Last Updated: 12/21/2016 12:39 PM Administrator, System

Incident Response Procedures

Tracking ID	Procedure Name	Description	Tasks Completed	Incident Response Tasks
IRP-295672	New Device Detection and Validation	Steps to be follows to validate new equipment detected as a substation. Task is triggered based on badged entry followed by new device detection within X hours	2/2	IRT-295673 IRT-295674

Figure 2-31 Incident Response Tasks with Status, Details, and Completion Status



Incident Response Procedures: IRP-295672

General Information

Tracking ID:	IRP-295672	Tasks Completed:	2/2
Procedure Name:	New Device Detection and Validation		
Description:	Steps to be follows to validate new equipment detected as a substation. Task is triggered based on badged entry followed by new device detection within X hours		
Incident Procedure Source:		Version:	1.00
Threat Category:	Physical Connection	Last Updated:	12/20/2016 11:37 AM Administrator, System
Link to Security Incidents:	INC-295667		

Incident Response Tasks

Tracking ID	Step Number	Task Name	Required/Optional	Analyst Name	Task Status	Analyst Note
IRT-295673	1.00	Work Order Validation	Required	Administrator, System	✓	No open tasks found in Archer or any other disconnected ticketing systems. Based on badge entry data available, user identified as bsmith
IRT-295674	2.00	User and Hardware Validation	Required	Administrator, System	✓	User bsmith contact via sms and e-mail. sms received, user is not present at substation. Device addition deemed unauthorized. Additional steps being taken as a result of this finding.

2.13 Schneider Electric Tofino Firewall (O3, O18, O20)

Schneider Electric Tofino Firewalls are used in multiple points throughout the build, supplying the necessary protection for network devices, including the door controller, the TDi ConsoleWorks operations management instance, and the connection between the OSIsoft Citect connector and the SCADA server.

2.13.1 Schneider Electric Tofino Firewall (O3) Installation Guide

1. Log in to the web interface:

    a. Open a browser and navigate to the IP address assigned to device.

    b. Enter the username **admin** and password **private.**

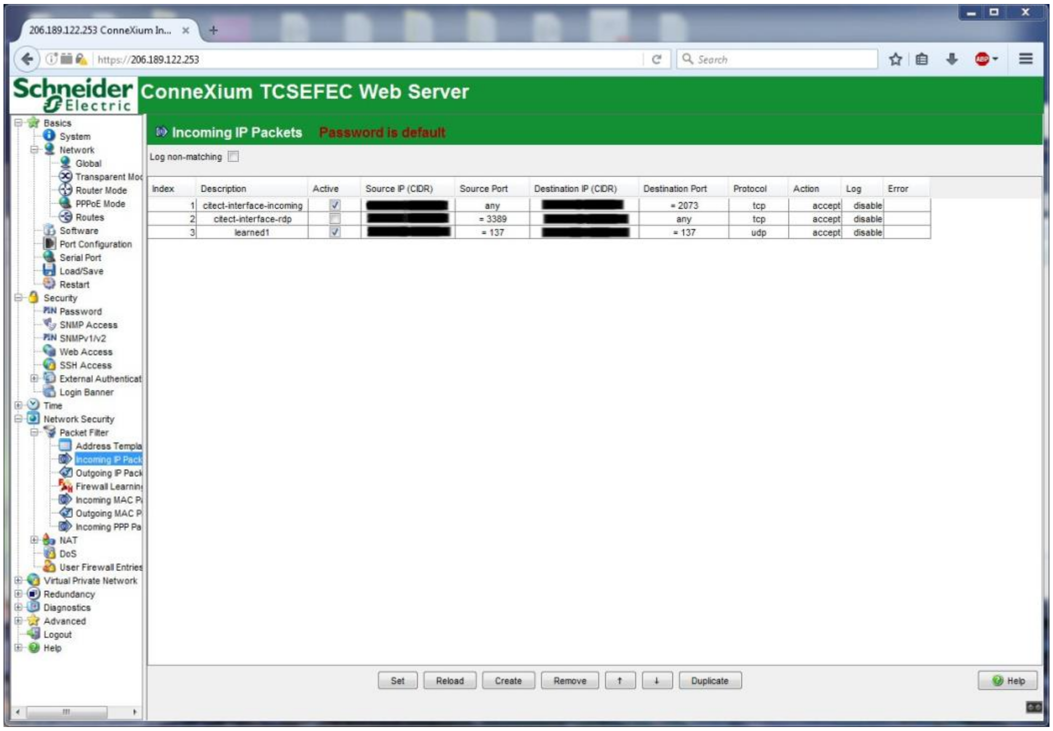
2. For Login-Type, select **Administration,** then select **OK.**

3. From the menu on the left, select **Network Security -> Packet Filter -> Incoming IP Packets.** This is where the firewall rules will be created.

4. Click the **Create** button on the bottom of the main window.

5. Fill in the text fields for Description, Source IP (CIDR), Source Port, Destination IP (CIDR), Destination Port, Protocol, Action Log, and Error according to the rules needed for incoming packets.

Figure 2-32 Incoming Packet Configuration



ConneXium TCSEFEC Web Server

Incoming IP Packets Password is default

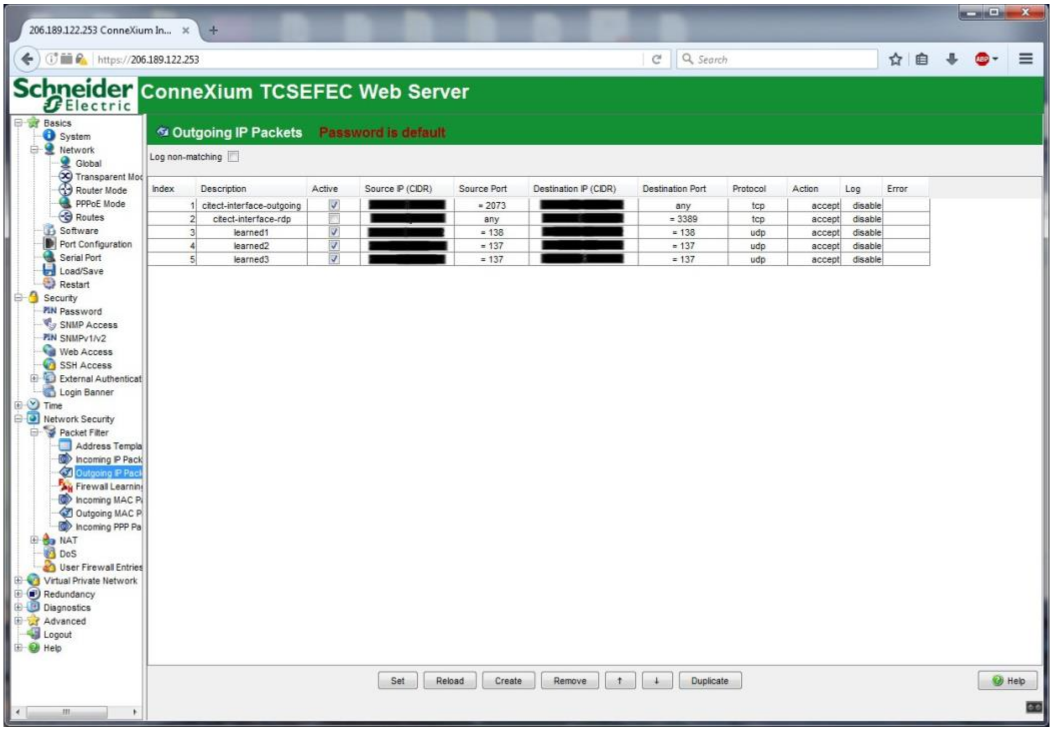
Log non-matching □

Index	Description	Active	Source IP (CIDR)	Source Port	Destination IP (CIDR)	Destination Port	Protocol	Action	Log	Error
1	citect-interface-incoming	☑	[redacted]	any	[redacted]	= 2073	tcp	accept	disable	
2	citect-interface-rdp	□	[redacted]	= 3389	[redacted]	any	tcp	accept	disable	
3	learned1	☑	[redacted]	= 137	[redacted]	= 137	udp	accept	disable	

6. From the menu on the left, select **Network Security -> Packet Filter -> Outgoing IP Packets.**

7. Follow the previous steps to create outgoing firewall rules.

Figure 2-33 Outgoing Packet Configuration



Outgoing IP Packets Password is default

Log non-matching ☐

Index	Description	Active	Source IP (CIDR)	Source Port	Destination IP (CIDR)	Destination Port	Protocol	Action	Log	Error
1	citect-interface-outgoing	☑	[redacted]	= 2073	[redacted]	any	tcp	accept	disable	
2	citect-interface-rdp	☐	[redacted]	any	[redacted]	= 3389	tcp	accept	disable	
3	learned1	☑	[redacted]	= 138	[redacted]	= 138	udp	accept	disable	
4	learned2	☑	[redacted]	= 137	[redacted]	= 137	udp	accept	disable	
5	learned3	☑	[redacted]	= 137	[redacted]	= 137	udp	accept	disable	

8. If necessary, configure the interface IP addresses from the menu on the left by selecting **Basics -> Network -> Transparent Mode.**

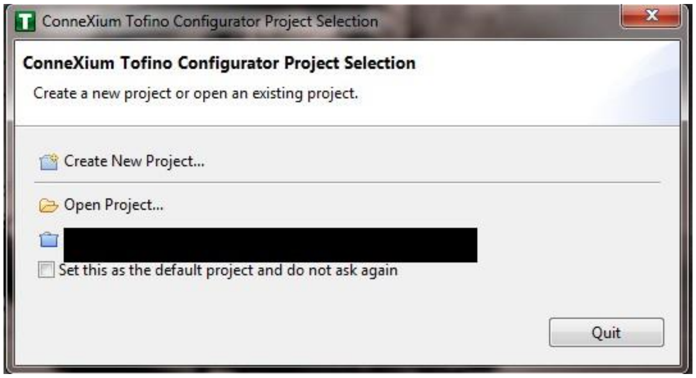
2.13.2 Schneider Electric Tofino Firewall (O18) Installation Guide

Install and Configure the Schneider Tofino Firewall:

1. Download the ConneXium software from the Schneider site as stated in the instructions accompanying the firewall, then start the ConneXium Tofino Configurator.

2. In the start-up screen, click **Create New Project…**

Figure 2-34 Create New Project



ConneXium Tofino Configurator Project Selection

Create a new project or open an existing project.

Create New Project...

Open Project...

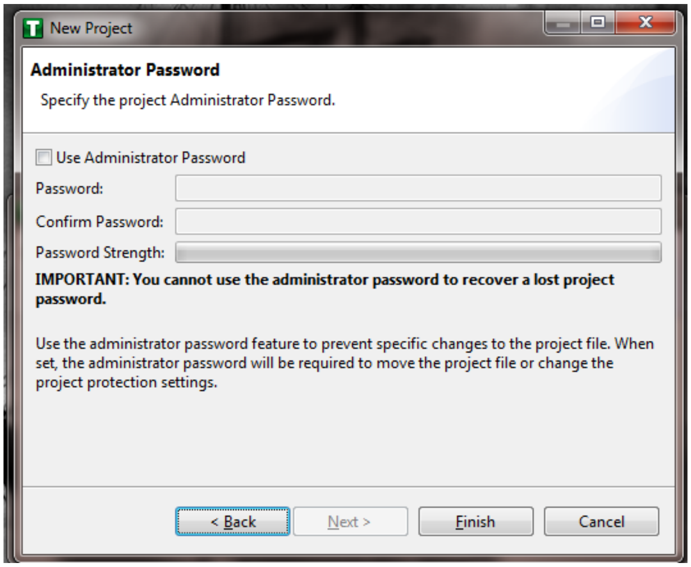
[redacted]

□ Set this as the default project and do not ask again

3. Enter the name for the project in the **Project name** field, the company name in the **Company** field, then click **Next.**

4. In the Project Protection screen, choose a password to protect the project, then click **Next.**

Figure 2-35 Administrator Password



Administrator Password

Specify the project Administrator Password.

□ Use Administrator Password

Password:

Confirm Password:

Password Strength:

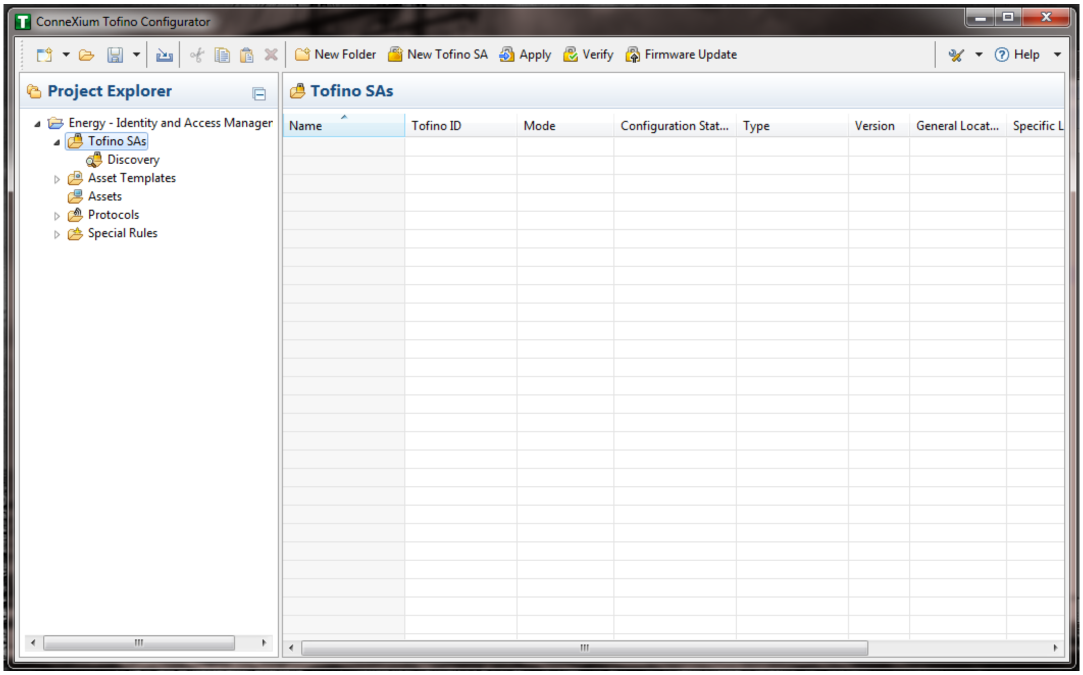
IMPORTANT: You cannot use the administrator password to recover a lost project password.

Use the administrator password feature to prevent specific changes to the project file. When set, the administrator password will be required to move the project file or change the project protection settings.

5. In the Administrator Password screen, choose the administrator password, then click **Finish.**

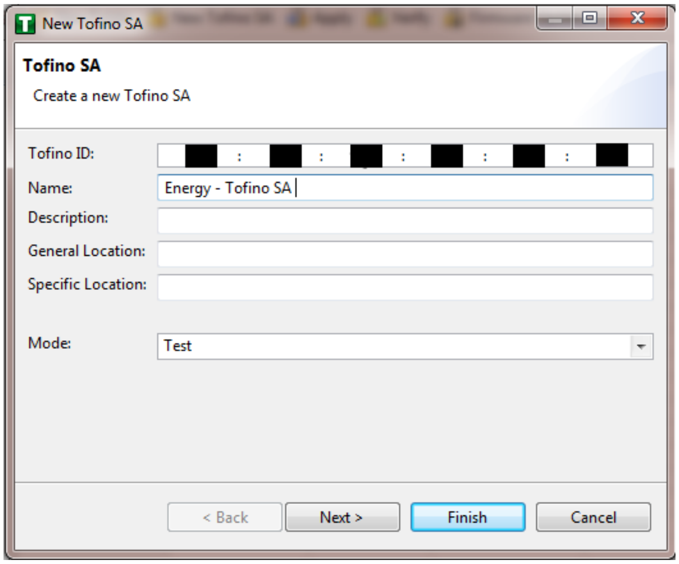
6. In the Project Explorer window, right-click **Tofino SAs,** and select **New Tofino SA.** A folder can also be created for the SAs to help organize multiple areas.

Figure 2-36 Project Explorer Window



7. In the **Tofino ID** field, enter the MAC address listed on the firewall hardware sticker. Fill out the rest of the fields as necessary, then click **Finish.**

Figure 2-37 Tofino SA/MAC Address



Tofino ID: [redacted] : [redacted] : [redacted] : [redacted] : [redacted] : [redacted]

Name: Energy - Tofino SA

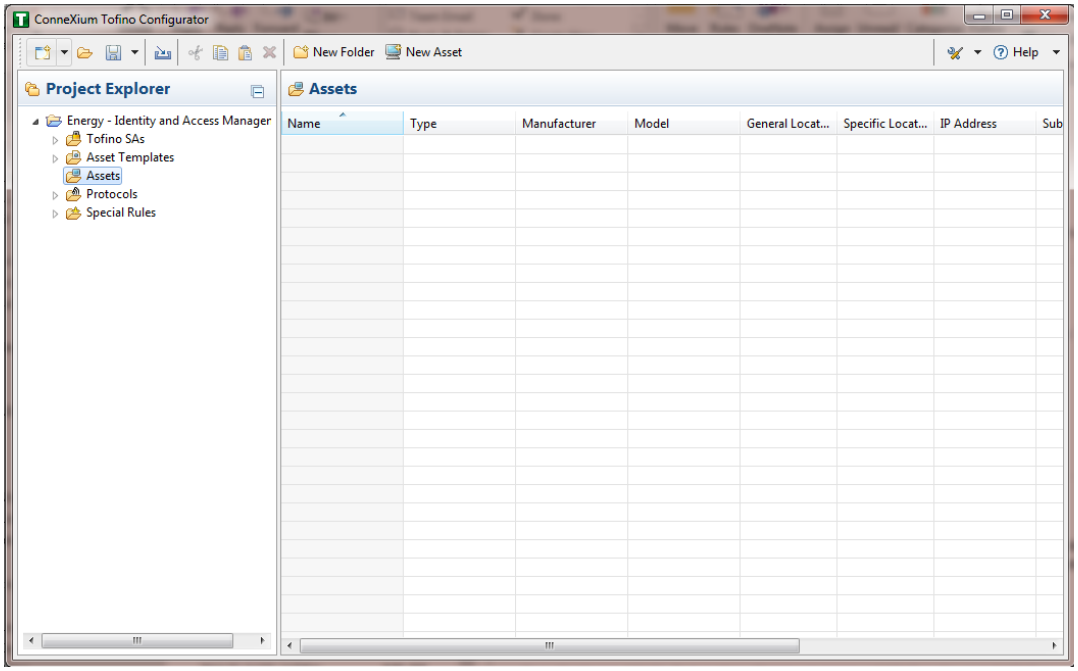
Description:

General Location:

Specific Location:

Mode: Test

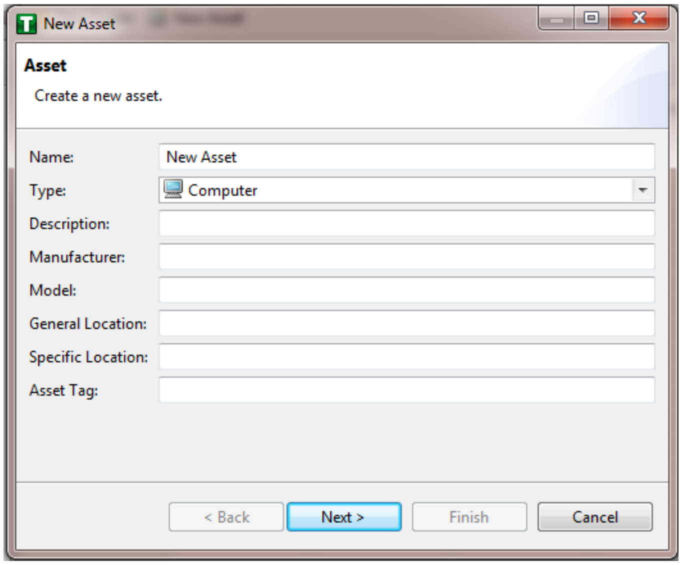
Figure 2-38 Project Explorer



8. Right-click on the **Assets** icon in the Project Explorer frame, then click **New Asset.**

9. In the New Asset window, set the name and type of the device and all other fields as necessary, then click **Next.**

Figure 2-39 New Asset



New Asset

Asset

Create a new asset.

Name: New Asset

Type: Computer

Description:

Manufacturer:

Model:

General Location:

Specific Location:

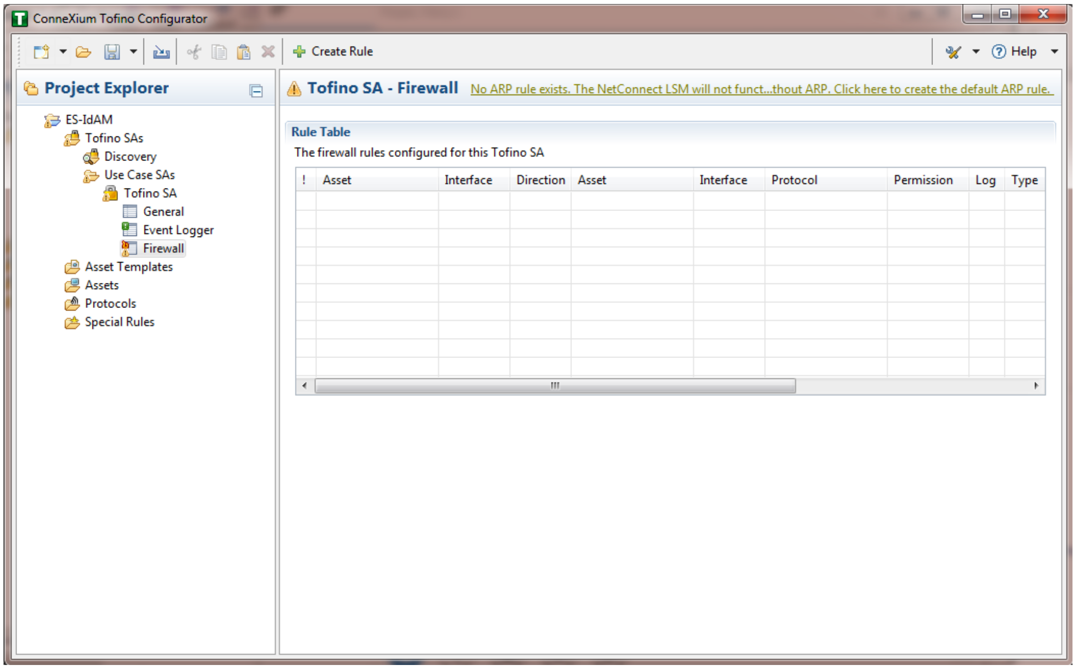
Asset Tag:

10. Fill in the **IP address** and/or the **MAC address** fields, then click **Finish.**

11. Repeat for all devices on the network. When they are configured, click on the **Assets** icon in the Project Explorer frame (if it is not already selected). There should be a list of all configured assets.

12. Under the Project Explorer frame, click the **drop-down arrow** next to Tofino SAs, then choose the SA created earlier. From there, click **Firewall** in the Project Explorer frame to display current firewall rules. This should currently be empty.

Figure 2-40 Project Explorer Tofino SA Icon



Tofino SA - Firewall No ARP rule exists. The NetConnect LSM will not funct...thout ARP. Click here to create the default ARP rule.

Rule Table

The firewall rules configured for this Tofino SA

!	Asset	Interface	Direction	Asset	Interface	Protocol	Permission	Log	Type

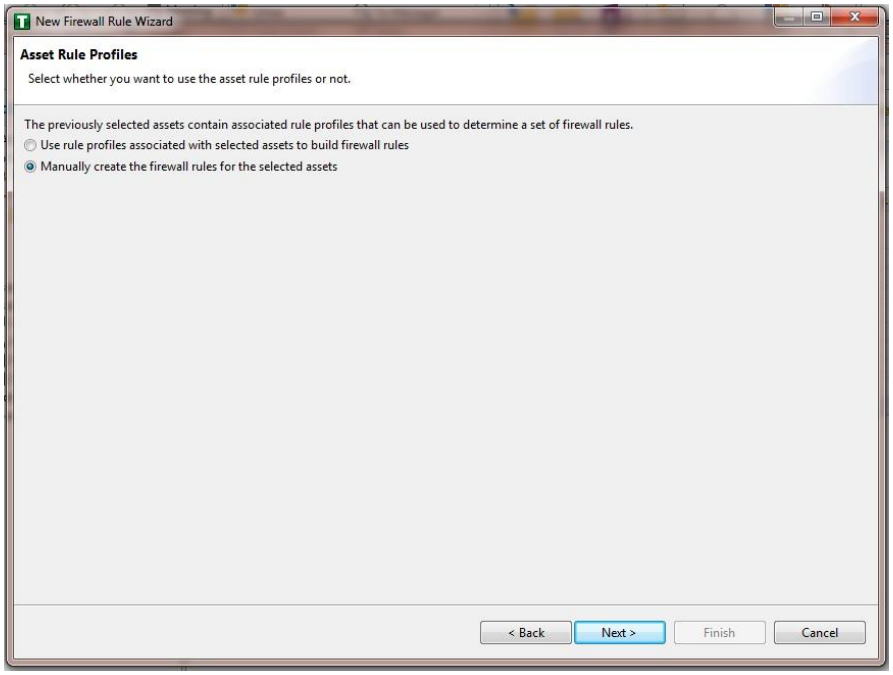
13. To create the first rule, click the **+ Create Rule** button above the Tofino SA-Firewall title. Then, ensure the **Standard rule** radio button is selected, and click **Next.**

14. On the next screen, choose the interface for **Asset 1.** This is where traffic originates before going into the device.

    Select a source asset and a destination asset from the radio buttons below. Set the direction of the traffic by using the arrow buttons in the middle. When finished, select **Next.**

15. In the Asset Rule Profiles window, select the **Manually create the firewall rules for the selected assets** radio button, then click **Next.**

Figure 2-41 Asset Rule Profiles



New Firewall Rule Wizard

Asset Rule Profiles

Select whether you want to use the asset rule profiles or not.

The previously selected assets contain associated rule profiles that can be used to determine a set of firewall rules.

○ Use rule profiles associated with selected assets to build firewall rules

● Manually create the firewall rules for the selected assets

16. On the Protocol screen, choose the protocol to be checked against. Then choose the **Permission** on the right side of the screen, as well as whether to log, then click **Finish.**

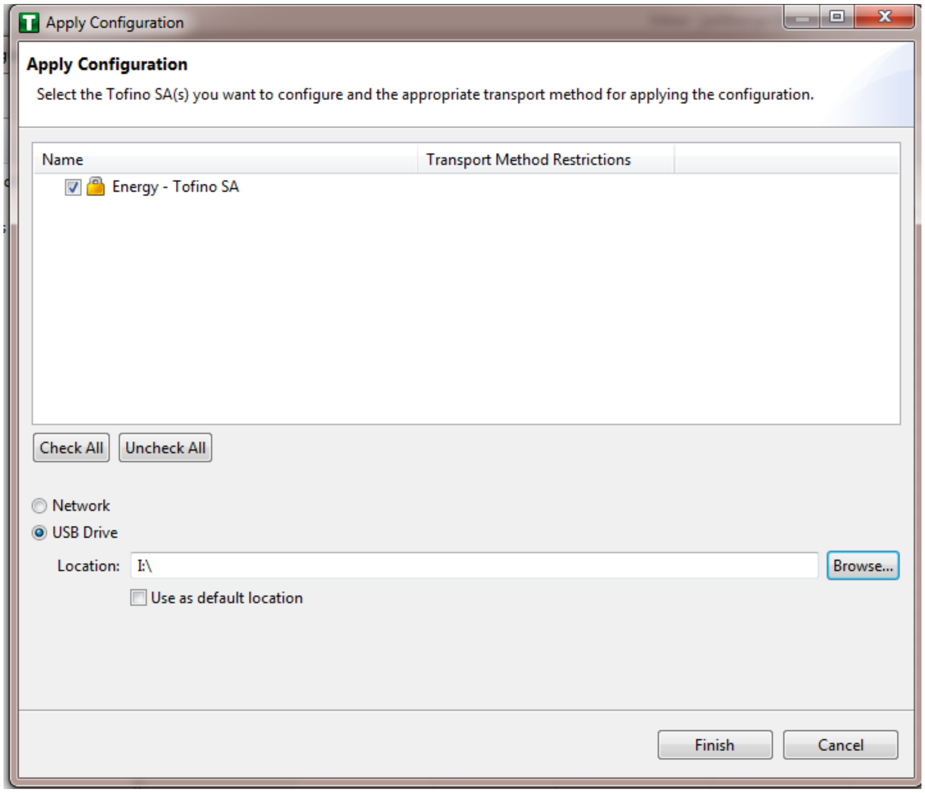
17. After these steps are completed, the firewall rule should be listed in the **Rule Table.**

18. Repeat steps for the remainder of the rules needed.

19. Finally, click the **Save** button on the menu bar.

20. Place a FAT/FAT32 formatted Universal Serial Bus (USB) device into the computer running the ConneXium Tofino Configurator, then right-click **Tofino SAs** in the Project Explorer pane and select **Apply.** If the project asks that it be saved, click **OK.**

Figure 2-42 Apply Configuration Pane



Apply Configuration

Select the Tofino SA(s) you want to configure and the appropriate transport method for applying the configuration.

Name	Transport Method Restrictions
☑ Energy - Tofino SA	

○ Network

● USB Drive

Location: I:\

□ Use as default location

21. In the Apply Configuration pane, ensure that the appropriate SA is selected in the table at the top and that the **USB Drive** radio button is selected. Browse to the top-level directory of the USB drive, then click **Finish.**

22. A pop-up will announce successful completion.

23. Ensure that the firewall has been powered on and has been running for at least one minute, then plug the USB device used to copy the Tofino configuration into the USB port on the back of the firewall.

24. Press the **Save/Load/Reset** button twice, setting it to the **Load** setting. (Pressing once should turn the indicator light to green pressing it again will change it from green to amber.) After a few seconds, the device will begin displaying lights that move from right to left across the LEDs on the back, indicating the configuration is being loaded.

25. Once the lights stop moving right to left, wait a few seconds to ensure that the **Fault** LED does not light up. Then remove the USB drive and place it back into the computer running the ConneXium Tofino Configurator software.

26. Right-click **Tofino SAs** in the Project Explorer pane and select **Verify.**

27. At the Verify Loaded Configuration window, select the **Tofino SA** in the table, and select the **USB Drive** radio button. Then select the USB drive by using the **Browse** button. Finally, click **Finish.**

28. A pop-up will announce successful verification, and configuration is complete.

2.13.3 Schneider Electric Tofino Firewall (O20) Installation Guide

Refer to the guide in Section 2.13.2 on installing the Schneider Electric Tofino Firewall (O18).

2.14 Siemens RUGGEDCOM CROSSBOW (E9)

Siemens RUGGEDCOM CROSSBOW is a platform that allows remote connections and controls from the enterprise side of the lab to the control systems network lab. The product does require the Waterfall Secure Bypass to be in the closed position, however CROSSBOW also monitors the IXIA Network TAP aggregator Cisco switch for any configuration changes, which then prompts an alert to the centralized SIEM.

2.14.1 Environment Setup

- Microsoft Windows Server 2012 (64-bit)
- 4 GB RAM
- 4 cores
- 200 GB HDD
- Software:
  - Microsoft SQL Server 2012 (version 11.0.2100.60)

2.14.2 Installation Procedure

The following sections detail the installation procedure for the Siemens RUGGEDCOM CROSSBOW used in the build.

2.14.2.1 Installing CROSSBOW Database

1. On the RUGGEDCOM CROSSBOW Server, extract the contents of **SQLScripts.zip** to RUGGEDCOMCROSSBOW install directory (e.g. **C:\ProgramFiles\RuggedCom\CrossBow).**

2. On a Microsoft SQL Server, launch **SQL Server Management Studio,** and connect to the SQL Server as a System Administrator (SA) or administrator.

3. In **Object Explorer,** expand the SQL Server.
4. Right-click **Databases,** and then click **New Database.** The New Database screen will appear.
5. In the **Database name** field, type the name of the new database (e.g. **CROSSBOW).**
6. Click **….** and the **Select Database Owner** dialogue box will appear.
7. Select a user to be the RUGGEDCOM CROSSBOW database owner in the SQL Server. This grants the RUGGEDCOM CROSSBOW Server full access to the RUGGEDCOM CROSSBOW database.
8. If the desired account is unavailable, add a Windows domain user account for authenticating against the database. This account must be added to the database as an authorized user.
9. Click **OK.**
10. Optional: Further configure the database (such as the recovery model) as required based on the chosen database backup strategy. For more information, contact the local Database Administrator (if available) or visit the Microsoft Developer Network website (https://msdn.microsoft.com/en-us/library/bb545450).
11. Click **OK.**
12. In Object Explorer, expand the **Security** folder, followed by **Logins.**
13. Right-click the desired Windows domain account, and then click **Properties.** The **Login Properties** dialogue box will appear.
14. Under **Default database,** select the **CROSSBOW** database, then click **OK.**
15. Execute the following scripts in order:
    a. Crossbow_db_create.sql
    b. Crossbow_db_functions.sql
    c. Crossbow_db_initial_data.sql
    d. Crossbow_db_scripts.sql
    e. Crossbow_db_client_queries.sql

2.14.2.2 Installing CROSSBOW Server and Services

1. Contact Siemens Customer Support, and obtain a compressed zip file containing the latest CROSSBOW Server installer for RUGGEDCOM CROSSBOW v4.4.

2. Open the compressed zip file, and double-click **Server Strong Setup.msi.** The CROSSBOW Server with Strong Authentication Setup installation wizard will appear.

3. Follow the onscreen instructions to install CROSSBOW Server.

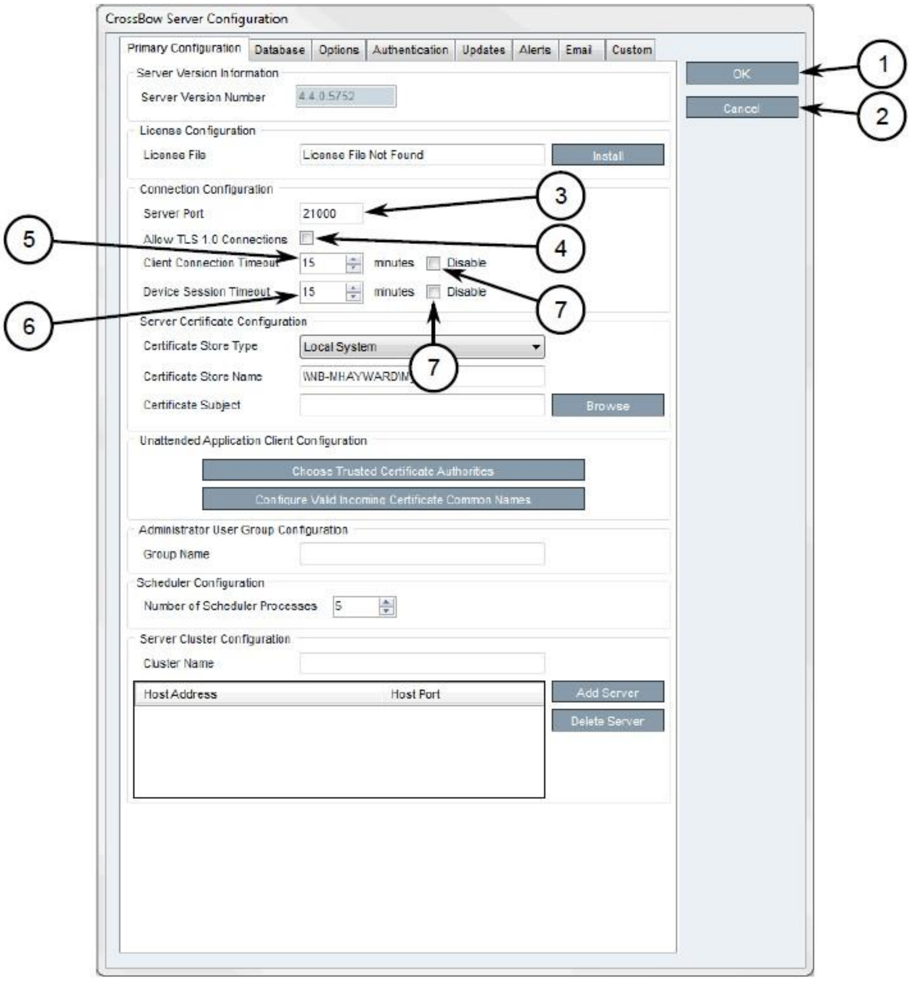
2.14.2.3 Configuring Server Host Connection

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.

2. Make sure the **CROSSBOW Main Server** service is **stopped.**

3. Under **CrossBow Main Server,** click **Configure.** The CrossBow Server Configuration dialogue box will appear.

Figure 2-43 CrossBow Server Configuration



CrossBow Server Configuration

Server Version Information
Server Version Number: 4.4.0.5752

License Configuration
License File: License File Not Found

Connection Configuration
Server Port: 21000
Allow TLS 1.0 Connections: □
Client Connection Timeout: 15 minutes □ Disable
Device Session Timeout: 15 minutes □ Disable

Server Certificate Configuration
Certificate Store Type: Local System
Certificate Store Name: \\WB-MHAYWARD\M
Certificate Subject:

Unattended Application Client Configuration

Administrator User Group Configuration
Group Name:

Scheduler Configuration
Number of Scheduler Processes: 5

Server Cluster Configuration
Cluster Name:

Host Address	Host Port

1. *OK Button*
2. *Cancel Button*
3. *Server Port Box*
4. *Allow Transport Layer Security 1.0 Connections Check Box*
5. *Client Connection Timeout Box*
6. *Device Session Timeout Box*
7. *Disable Check Box*

4. On the Primary Configuration tab, under **Connection Configuration,** type the TCP port number that the CROSSBOW Client application will use to connect to the CROSSBOW Server in the **Server Port** field. The default port number is 21000 but can be changed as needed.

5. In the **Client Connection Timeout** field, type or select the maximum amount of time (in minutes) for the server to wait before disconnecting an inactive client. To disable this feature, select **Disable.**

6. In the **Device Session Timeout** field, type or select the maximum amount of time (in minutes) for the server to wait before disconnecting an inactive remote device. To disable this feature, select **Disable.**

7. Click **OK** to save changes.

8. Start the CROSSBOW Main Server service.

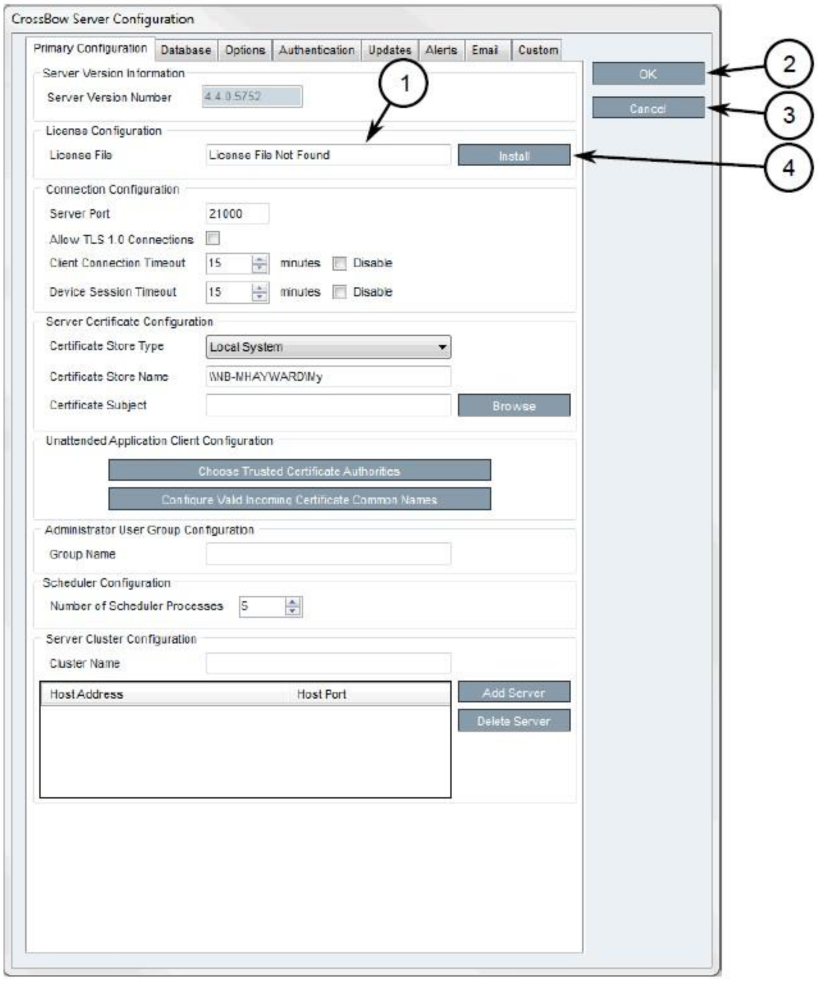
2.14.2.4 Installing a License File

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.

2. Make sure the **CROSSBOW Main Server** service is **stopped.**

3. Under **CrossBow Main Server,** click **Configure.** The CrossBow Server Configuration dialogue box will appear.

Figure 2-44 CrossBow Server Configuration



Server Version Information

Server Version Number: 4.4.0.5752

License Configuration

License File: License File Not Found

Connection Configuration

Server Port: 21000

Allow TLS 1.0 Connections □

Client Connection Timeout: 15 minutes □ Disable

Device Session Timeout: 15 minutes □ Disable

Server Certificate Configuration

Certificate Store Type: Local System

Certificate Store Name: \\NB-MHAYWARD\My

Certificate Subject:

Unattended Application Client Configuration

Administrator User Group Configuration

Group Name:

Scheduler Configuration

Number of Scheduler Processes: 5

Server Cluster Configuration

Cluster Name:

Host Address	Host Port

1. *License File Box*
2. *OK Button*
3. *Cancel Button*
4. *Install Button*

4. On the **Primary Configuration** tab, under **License Configuration,** either type the name of the license file (including the system path) or click **Install** and select the desired file.

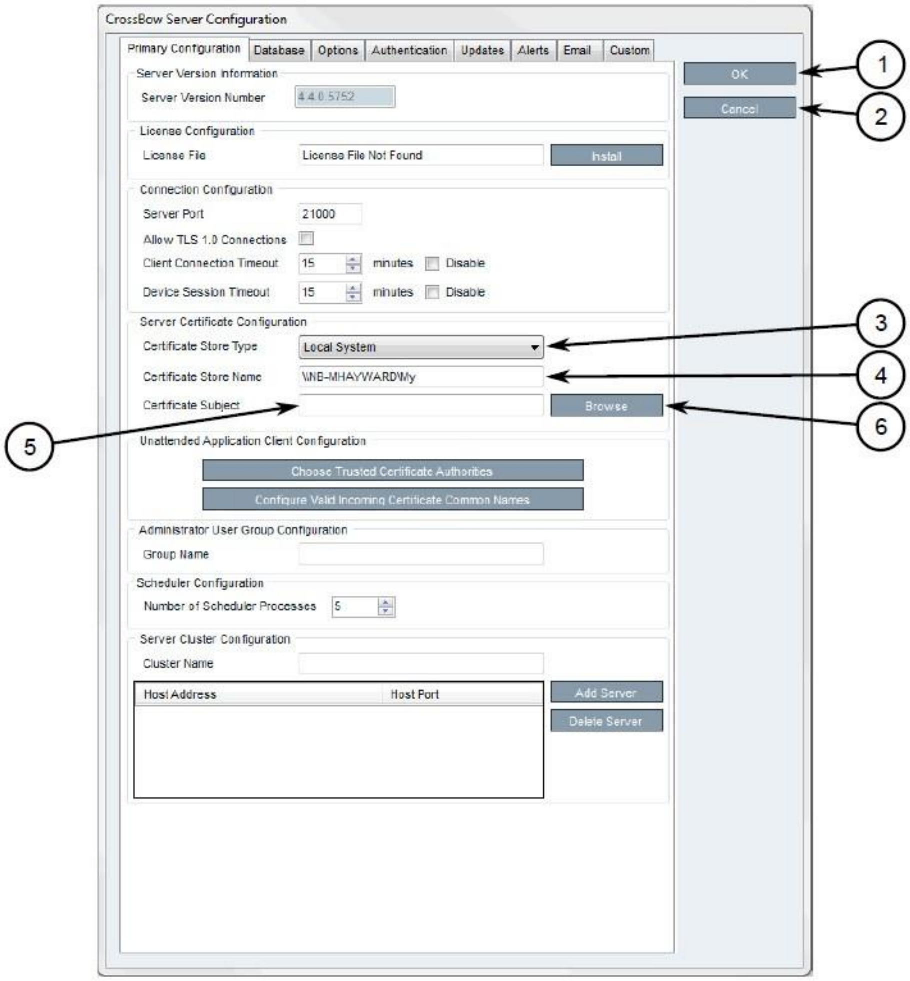
5. Click **OK** to save changes.

6. Start the CROSSBOW Main Server service.

2.14.2.5 Selecting/Installing the CROSSBOW Server Certificate

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.
2. Make sure the **CROSSBOW Main Server** service is **stopped.**
3. Under **CrossBow Main Server,** click **Configure.** The CrossBow Server Configuration dialogue box will appear.

Figure 2-45 CrossBow Server Configuration



Server Version Information
Server Version Number: 4.4.0.5752

License Configuration
License File: License File Not Found

Connection Configuration
Server Port: 21000
Allow TLS 1.0 Connections ☐
Client Connection Timeout: 15 minutes ☐ Disable
Device Session Timeout: 15 minutes ☐ Disable

Server Certificate Configuration
Certificate Store Type: Local System
Certificate Store Name: \\NE-MHAYWARD\My
Certificate Subject:

Unattended Application Client Configuration

Administrator User Group Configuration
Group Name:

Scheduler Configuration
Number of Scheduler Processes: 5

Server Cluster Configuration
Cluster Name:

Host Address	Host Port

1. *OK Button*
2. *Cancel Button*
3. *Certificate Store Type List*

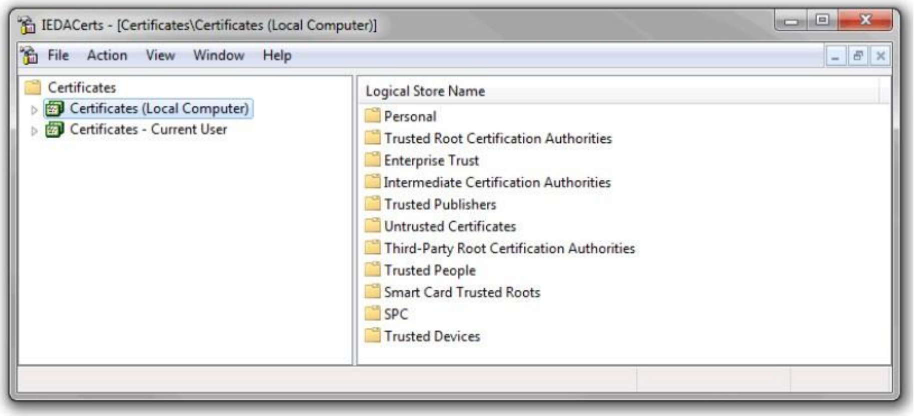
    4. *Certificate Store Name Box*
    5. *Certificate Subject Box*
    6. *Browse Button*

4. On the Primary Configuration tab, under **Server Certificate Configuration,** click **Browse.** The Select Server Certificate dialogue box will appear.

5. Click **Import.** A confirmation dialogue box will appear.

6. Click **Yes.** A confirmation dialogue box will appear, as well as the Microsoft Management Console (MMC) snap-in.

Figure 2-46 MMC Snap-In



Certificates
- Certificates (Local Computer)
- Certificates - Current User

Logical Store Name
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Smart Card Trusted Roots
- SPC
- Trusted Devices

7. Expand **Certificates (Local Computer).**

8. Right-click either **Personal** or **Trusted Root Certification Authorities,** point to **All Tasks,** then click **Import.** The Certificate Import Wizard will appear.

9. Follow the onscreen instructions to import the certificate.

10. Close the Microsoft Management Console snap-in.

11. Once the certificate is imported, click **OK** to close the dialogue box.

12. On the Select Server Certificate dialogue box, select the certificate from the list, and click **OK**. The certificate name appears in the **Certificate Subject** field.

13. Click **OK** to save changes.

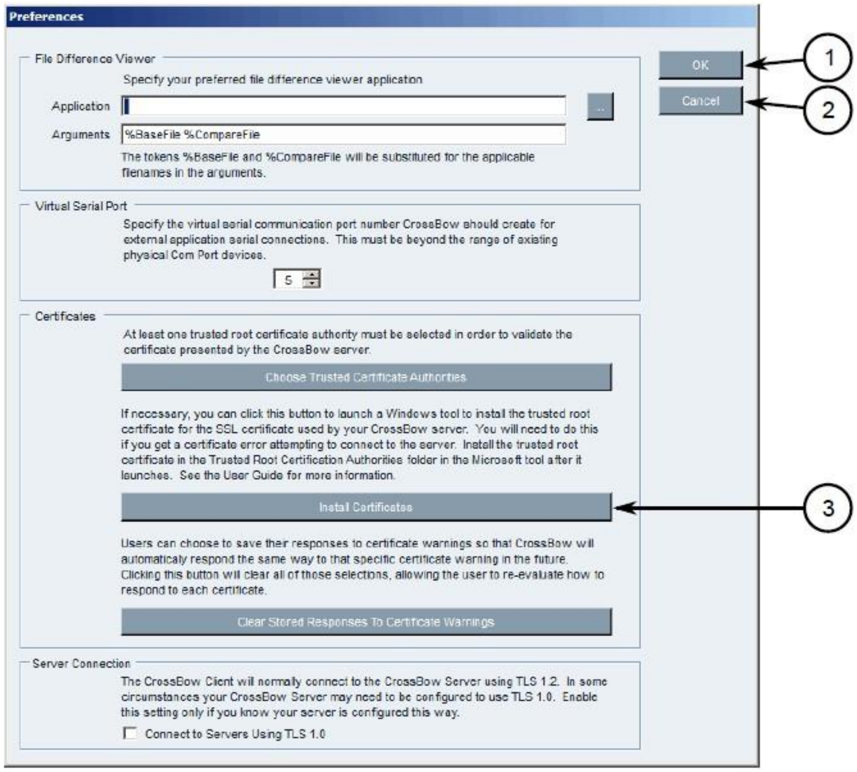
14. Start the CROSSBOW Main Server service.

2.14.2.6 Verifying/Installing the CROSSBOW Client Certification Authority (CA) Certificate

1. Launch CROSSBOW Client, but do not connect to the RUGGEDCOM CROSSBOW Server.

2. On the toolbar, click **File,** then click **Preferences.** The Preferences dialogue box will appear.

Figure 2-47 Preferences Dialogue Box



File Difference Viewer

Specify your preferred file difference viewer applicaton

Application

Arguments %BaseFile %CompareFile

The tokens %BaseFile and %CompareFile will be substituted for the applicable filenames in the arguments.

Virtual Serial Port

Specify the virtual serial communication port number CrossBow should create for external application serial connections. This must be beyond the range of existing physical Com Port devices.

5

Certificates

At least one trusted root certificate authority must be selected in order to validate the certificate presented by the CrossBow server.

Choose Trusted Certificate Authorties

If necessary, you can click this button to launch a Windows tool to install the trusted root certificate for the SSL certificate used by your CrossBow server. You will need to do this if you get a certificate error attempting to connect to the server. Install the trusted root certificate in the Trusted Root Certification Authorities folder in the Microsoft tool after it launches. See the User Guide for more information.

Install Certificates

Users can choose to save their responses to certificate warnings so that CrossBow will automaticaly respond the same way to that specific certificate warning in the future. Clicking this button will clear all of those selections, allowing the user to re-evaluate how to respond to each certificate.

Clear Stored Responses To Certificate Warnings

Server Connection

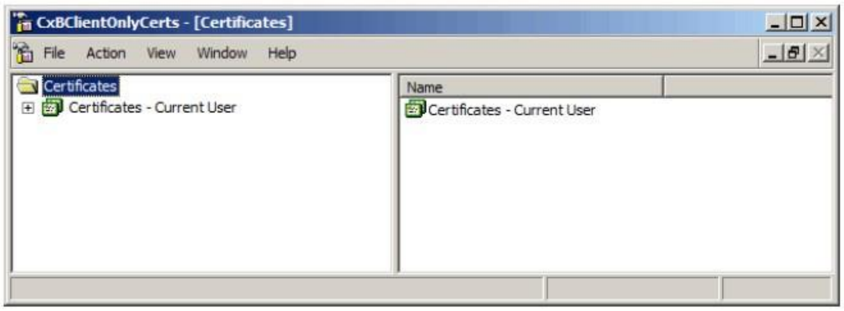
The CrossBow Client will normally connect to the CrossBow Server using TLS 1.2. In some circumstances your CrossBow Server may need to be configured to use TLS 1.0. Enable this setting only if you know your server is configured this way.

☐ Connect to Servers Using TLS 1.0

1. *OK Button*
2. *Cancel Button*
3. *Install Certificates Button*

3. Click **Install Certificates.** The CxBClientOnlyCerts snap-in will appear.

Figure 2-48 CxBClientOnlyCerts Snap-In


CxBClientOnlyCerts - [Certificates]
File
Action
View
Window
Help
Certificates
Certificates - Current User
Name
Certificates - Current User

4. In the left pane, navigate to **Certificates — Current User ->Trusted Root Certification Authorities -> Certificates.**

5. Verify the appropriate CA certificate is listed in the right pane.

6. If the certificate is not listed, proceed to the next step.

7. Right-click **Trusted Root Certification Authorities,** point to **All Tasks,** then click **Import.** The Certificate Import Wizard will appear.

8. Follow the onscreen instructions to import a new CA certificate.

9. Close the snap-in.

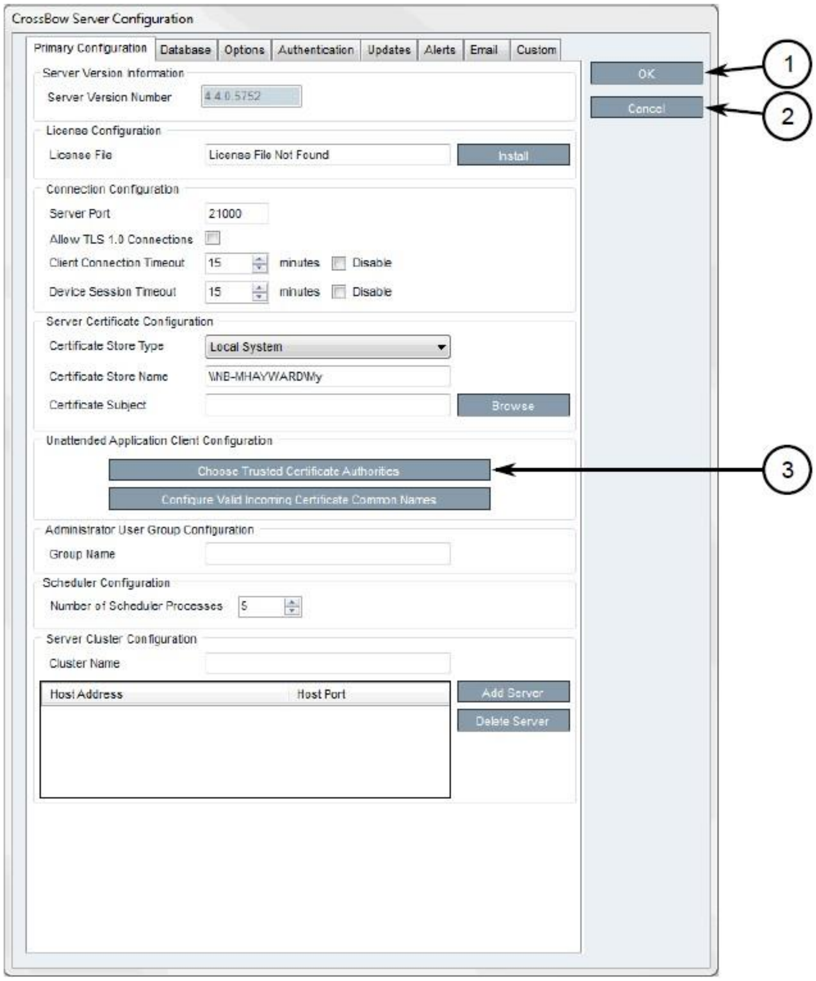
2.14.2.7 Select a Trusted CA for the CROSSBOW Server

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.

2. Make sure the **CROSSBOW Main Server** service is **stopped.**

3. Under **CrossBow Main Server,** click **Configure.** The CrossBow Server Configuration dialogue box will appear.

Figure 2-49 CrossBow Server Configuration



CrossBow Server Configuration

Server Version Information

Server Version Number: 4.4.0.5752

License Configuration

License File: License File Not Found

Connection Configuration

Server Port: 21000

Allow TLS 1.0 Connections ☐

Client Connection Timeout: 15 minutes ☐ Disable

Device Session Timeout: 15 minutes ☐ Disable

Server Certificate Configuration

Certificate Store Type: Local System

Certificate Store Name: \\NB-MHAYWARD\My

Certificate Subject:

Unattended Application Client Configuration

Administrator User Group Configuration

Group Name:

Scheduler Configuration

Number of Scheduler Processes: 5

Server Cluster Configuration

Cluster Name:

Host Address	Host Port

1. *OK Button*
2. *Cancel Button*
3. *Choose Trusted Certificate Authorities Button*

4. Click **Choose Trusted Certificate Authorities.** A dialogue box will appear.

5. Optional: Filter the list of CAs by selecting **Show Root Certificate Authorities, Show Intermediate Certificate Authorities,** and/or **Show Third Party Certificate Authorities.**

6. Select one or more CAs from the list, or select **Specify a certificate authority** and define the CA in the box below.

7. Click **OK** to save changes.

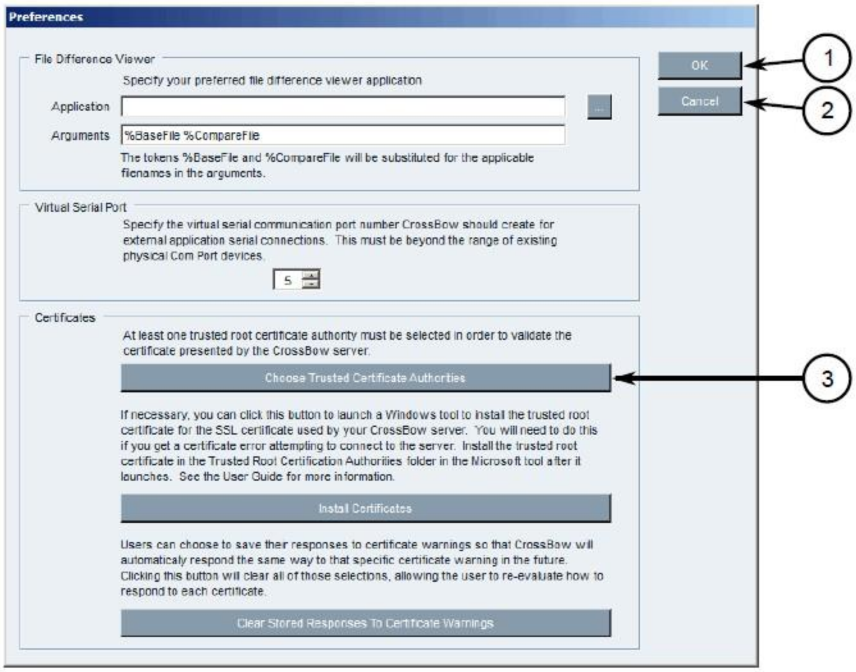
8. Start the CROSSBOW Main Server service.

2.14.2.8 Selecting a Trusted CA for a CROSSBOW Client

1. Launch CROSSBOW Client, but do not connect to the RUGGEDCOM CROSSBOW Server.

2. On the toolbar, select **File,** then click **Preferences.** The Preferences dialogue box will appear.

Figure 2-50 Preference Dialogue Box



Specify your preferred file difference viewer application

Arguments: %BaseFile %CompareFile

The tokens %BaseFile and %CompareFile will be substituted for the applicable filenames in the arguments.

Specify the virtual serial communication port number CrossBow should create for external application serial connections. This must be beyond the range of existing physical Com Port devices.

5

At least one trusted root certificate authority must be selected in order to validate the certificate presented by the CrossBow server.

If necessary, you can click this button to launch a Windows tool to install the trusted root certificate for the SSL certificate used by your CrossBow server. You will need to do this if you get a certificate error attempting to connect to the server. Install the trusted root certificate in the Trusted Root Certification Authorities folder in the Microsoft tool after it launches. See the User Guide for more information.

Users can choose to save their responses to certificate warnings so that CrossBow will automaticaly respond the same way to that specific certificate warning in the future. Clicking this button will clear all of those selections, allowing the user to re-evaluate how to respond to each certificate.

1. *OK Button*
2. *Cancel Button*
3. *Choose Trusted Certificate Authorities Button*

3. Click **Choose Trusted Certificate Authorities.** A dialogue box will appear.

4. Optional: Filter the list of CAs by selecting **Show Root Certificate Authorities, Show Intermediate Certificate Authorities,** and/or **Show Third Party Certificate Authorities.**

5. Select one or more CAs from the list, or select **Specify a certificate authority** and define the CA in the box below.

6. Click **OK** to save changes.

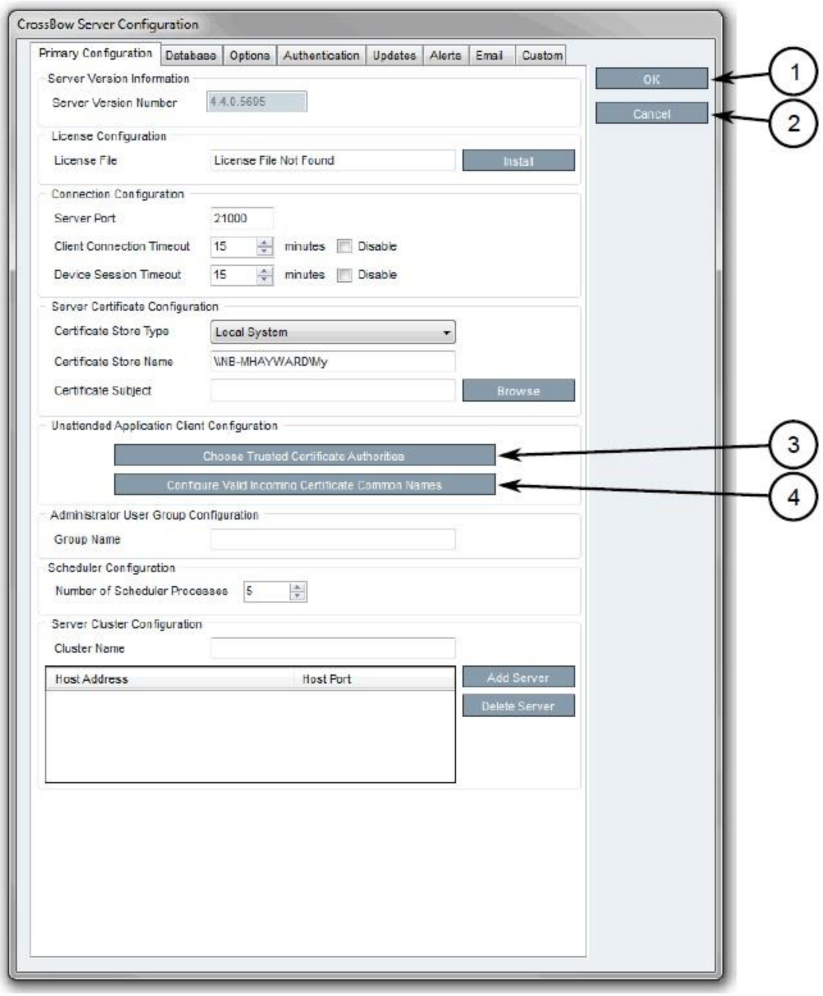
2.14.2.9 Adding a Common Name

1. Access the RUGGEDCOM CROSSBOW Server, and launch CROSSBOW Server.

2. Make sure the **CROSSBOW Main Server** service is **stopped.**

3. Under **CrossBow Main Server,** click **Configure.** The CrossBow Server Configuration dialogue box will appear.

Figure 2-51 CrossBow Server Configuration



Server Version Information
Server Version Number: 4.4.0.5605

License Configuration
License File: License File Not Found

Connection Configuration
Server Port: 21000
Client Connection Timeout: 15 minutes □ Disable
Device Session Timeout: 15 minutes □ Disable

Server Certificate Configuration
Certificate Store Type: Local System
Certificate Store Name: \\NB-MHAYWARD\My
Certificate Subject:

Unattended Application Client Configuration

Administrator User Group Configuration
Group Name:

Scheduler Configuration
Number of Scheduler Processes: 5

Server Cluster Configuration
Cluster Name:

Host Address	Host Port

1. *OK Button*
2. *Cancel Button*

    3. *Choose Trusted Certificate Authorities Button*
    4. *Configure Valid Incoming Certificate Common Names Button*

4. On the **Primary Configuration** tab, under **Unattended Application Client Configuration,** click **Configure Valid Incoming Certificate Common Names.** The Incoming Certificate Common Name dialogue box will appear.

5. Click **Add Name.** The Common Name dialogue box will appear.

6. In the **Common Name** box, type the common name, then click **OK** to close the dialogue box.

7. Click **OK.**

8. Start the CROSSBOW Main Server service.

2.14.2.10 Managing the RUGGEDCOM CROSSBOW Certificates and Keys

The following references the RUGGEDCOM RX1400 and RX1511 web interface:

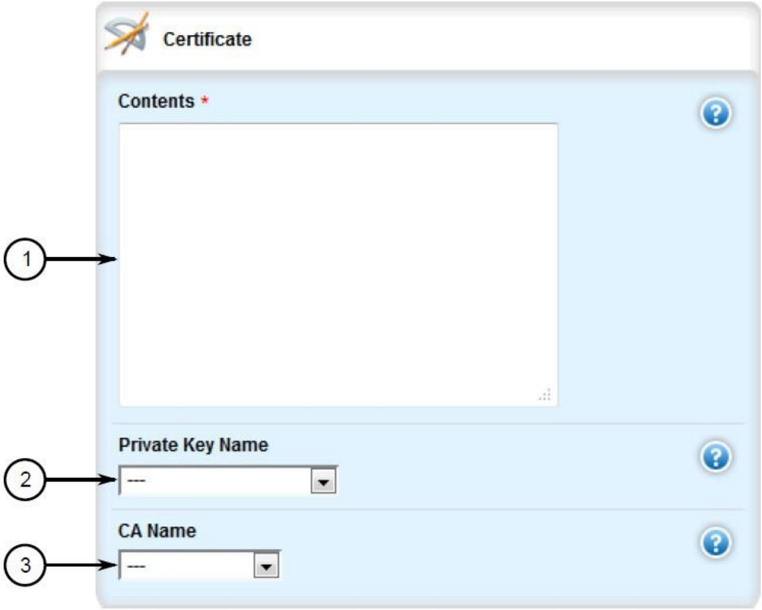
1. Navigate to **security -> crypto -> ca** and click **<Add ca>.** The Key Settings form will appear.

2. Configure the following parameter as required:

    a. name

3. Click **Add.** The CA form will appear.

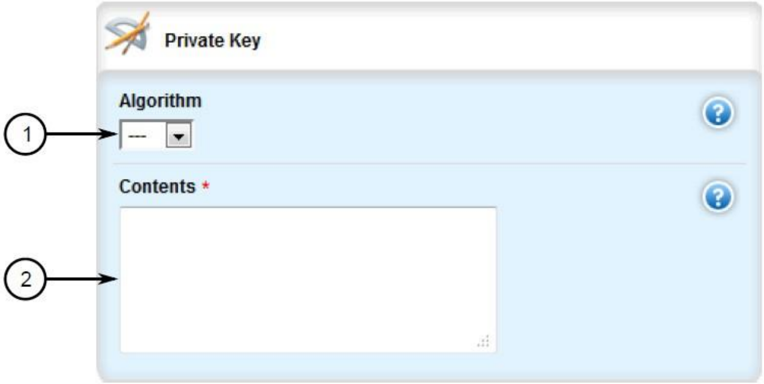
Figure 2-52 Virtual Private Network (VPN) Certificate Form



1. *Contents Box*
2. *Private Key Name List*
3. *CA Certificate Name List*

4. Copy the contents of the CA certificate into the **Key Cert Sign Certificate** field.
5. Add the associated Certificate Revocation List.
6. Navigate to **security -> crypto -> private-key** and click **<Add private-key>.** The Key Settings form will appear.
7. In the Key Settings form, configure the following parameter as required:
   a. name
8. Click **Add** to create the new private key. The Private Key form will appear.

Figure 2-53 VPN Private Key Form



1. *Algorithm List*
2. *Contents Box*

9. In the Private Key form, configure the following parameters as required:

    a. Algorithm

    b. Contents

2.14.2.11 Managing the RUGGEDCOM CROSSBOW Application on RX1501

To enable or disable communication with a RUGGEDCOM CROSSBOW system, do the following:

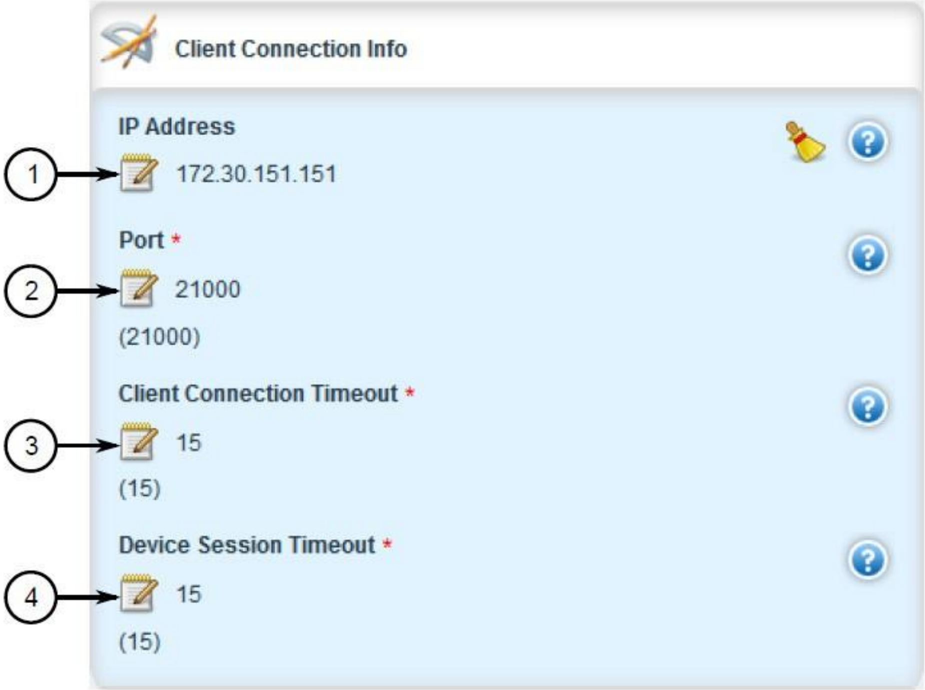
1. Change the mode to **Edit Private** or **Edit Exclusive.**

2. Navigate to **apps -> crossbow**. The CROSSBOW form will appear.

3. Ensure that the **Enabled** check box is selected.

4. Navigate to **apps -> crossbow -> client-connection.** The Client Connection Info form will appear.

Figure 2-54 Client Connection Info



Client Connection Info

IP Address

172.30.151.151

Port *

21000

(21000)

Client Connection Timeout *

15

(15)

Device Session Timeout *

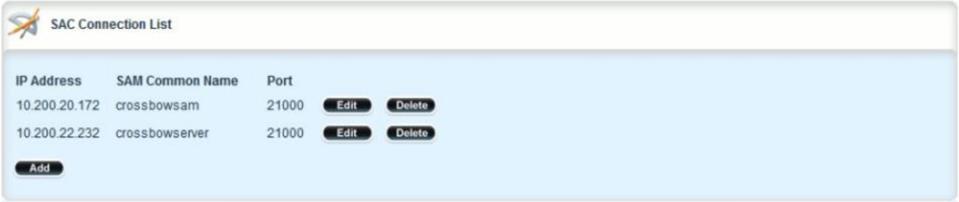
15

(15)

1. *IP Address Box*
2. *Port Box*
3. *(Keep default)*
4. *(Keep default)*

5. Configure the following parameters as required:
    a. ipaddr
    b. port
6. Navigate to **apps -> crossbow -> sac-connection.** The station access controller (SAC) Connection List will appear.

Figure 2-55 SAC Connection List



SAC Connection List

IP Address	SAM Common Name	Port		
10.200.20.172	crossbowsam	21000	Edit	Delete
10.200.22.232	crossbowserver	21000	Edit	Delete

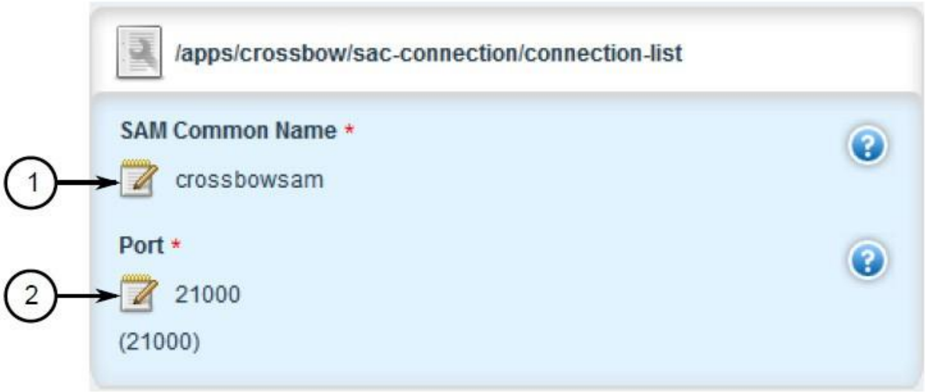
7. Navigate to **apps -> crossbow -> sac-connection -> Add connection-list.** The Key Settings form will appear.

8. Configure the following parameter(s) as required:

    a. sam-ipaddr

9. Click **Add.** The Connection List form will appear.

Figure 2-56 Connection List



/apps/crossbow/sac-connection/connection-list

SAM Common Name *
crossbowsam

Port *
21000
(21000)

1. SAM Common Name Box
2. Port Box

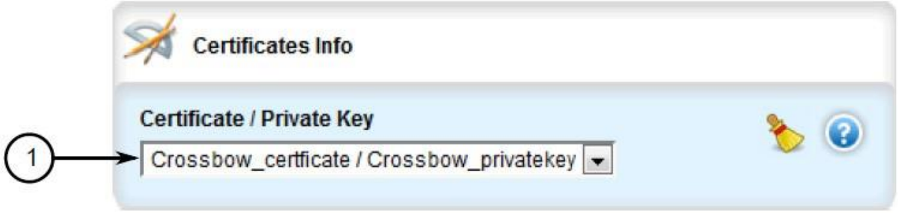
10. Configure the following parameters as required:

    a. sam-name

    b. sam-port

11. Navigate to **apps -> crossbow -> certificate.** The Certificates Info forms will appear.

Figure 2-57 Certificates Info



Certificate / Private Key

Crossbow_certficate / Crossbow_privatekey

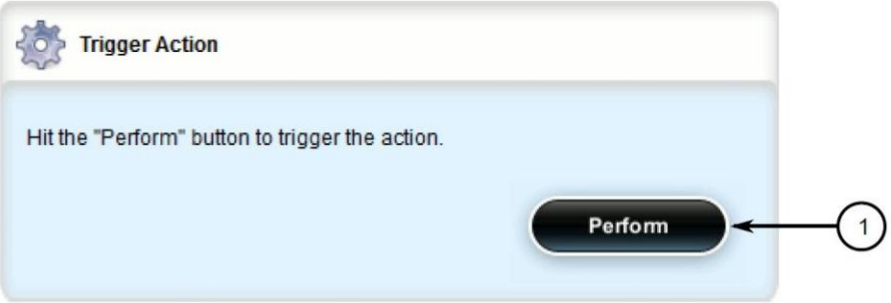
1. *Certificate/Private Key List*

12. Configure the following parameters as required:
    a. cert
    b. cert-private-key
13. Navigate to **apps -> crossbow -> certificate -> ca-cert-list** and click **<Add ca-cert-list>.** The Key Settings form will appear.
14. Configure the following parameter as required:
    a. name
15. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialogue box will appear. Click **OK** to proceed.
16. Click **Exit Transaction,** or continue making changes.

2.14.2.12 Viewing the RUGGEDCOM CROSSBOW Log

1. Navigate to **apps -> crossbow -> status** and click **log** in the menu. The Trigger Action form will appear.

Figure 2-58 Trigger Action

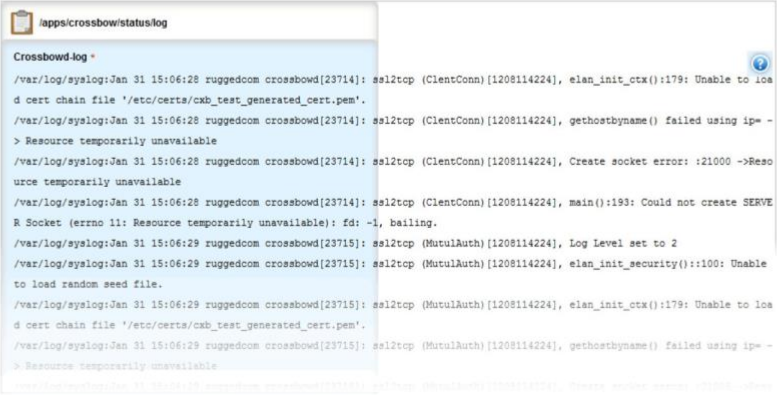


Hit the "Perform" button to trigger the action.

1. *Perform Button*

2. Click **Perform.** The Log form will appear.

Figure 2-59 Status Log



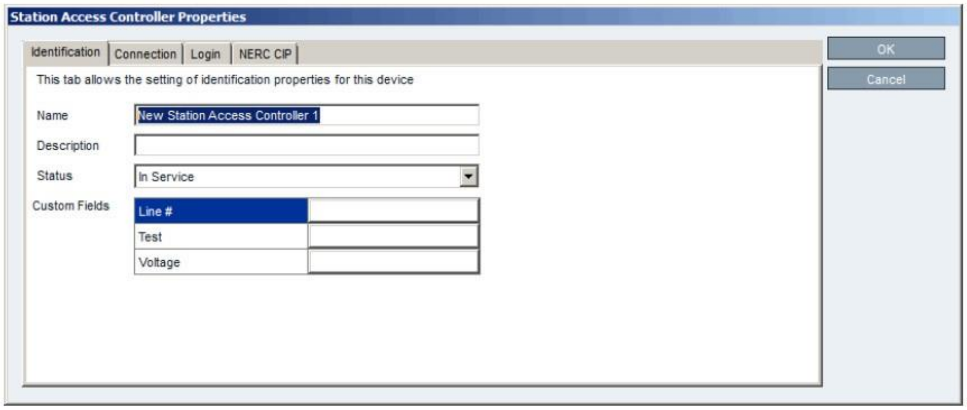
```
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClentConn)[1208114224], elan_init_ctx():179: Unable to loa
d cert chain file '/etc/certs/cxb_test_generated_cert.pem'.
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClentConn)[1208114224], gethostbyname() failed using ip= -
> Resource temporarily unavailable
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClentConn)[1208114224], Create socket error: :21000 ->Reso
urce temporarily unavailable
/var/log/syslog:Jan 31 15:06:28 ruggedcom crossbowd[23714]: ssl2tcp (ClentConn)[1208114224], main():193: Could not create SERVE
R Socket (errno 11: Resource temporarily unavailable): fd: -1, bailing.
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutulAuth)[1208114224], Log Level set to 2
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutulAuth)[1208114224], elan_init_security()::100: Unable
to load random seed file.
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutulAuth)[1208114224], elan_init_ctx():179: Unable to loa
d cert chain file '/etc/certs/cxb_test_generated_cert.pem'.
/var/log/syslog:Jan 31 15:06:29 ruggedcom crossbowd[23715]: ssl2tcp (MutulAuth)[1208114224], gethostbyname() failed using ip= -
> Resource temporarily unavailable
```

2.14.2.13 Managing SACs

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges. The Field Layout tab appears by default.

2. In the right pane, right-click the associated facility or gateway, and click **Add Station Access Controller.** The Station Access Controller Properties dialogue box will appear.

Figure 2-60 Station Access Controller Properties



Station Access Controller Properties

This tab allows the setting of identification properties for this device

Name: New Station Access Controller 1

Description:

Status: In Service

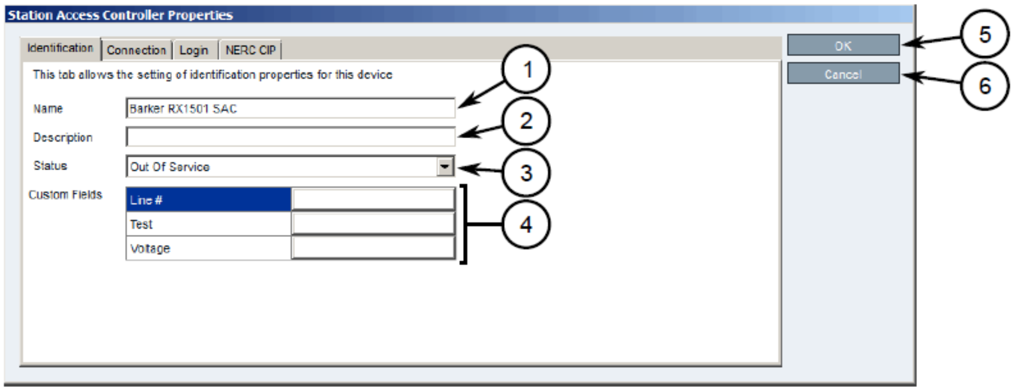
Custom Fields:

Line #	
Test	
Voltage	

1. *Name Box*
2. *Description Box*
3. *Status List*
4. *Custom Fields*
5. *OK Button*
6. *Cancel Button*

3. Configure the identification properties (e.g., name, description) for the SAC.

Figure 2-61 SAC Property Configuration — Identification



Station Access Controller Properties

This tab allows the setting of identification properties for this device

Name: Barker RX1501 SAC

Description:

Status: Out Of Service

Custom Fields:

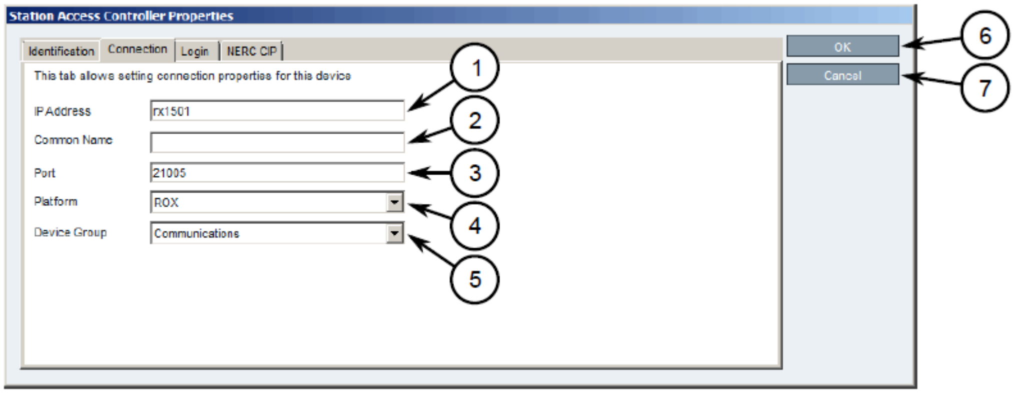
Line #	
Test	
Voltage	

1. *Name Box*
2. *Description Box*
3. *Status List*
4. *Custom Fields*

5. *OK Button*
6. *Cancel Button*

4. Configure the connection properties (e.g., IP address, port, platform) for the SAC.

Figure 2-62 SAC Property Configuration — Connection



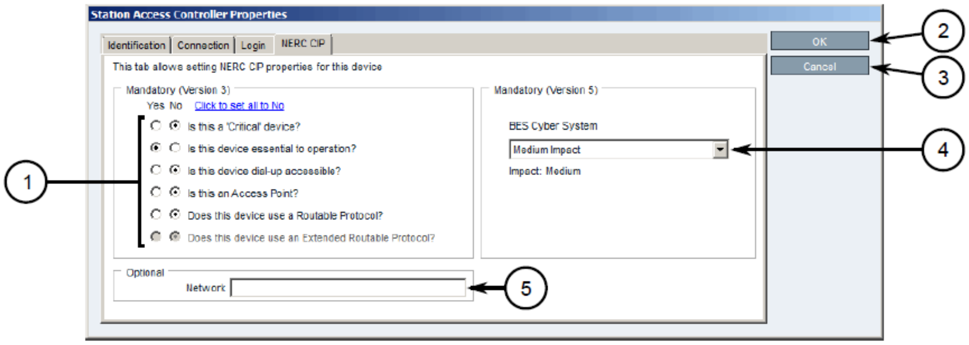
This tab allows setting connection properties for this device

IP Address: rx1501
Common Name:
Port: 21005
Platform: ROX
Device Group: Communications

1. *IP Address Box*
2. *Common Name Box*
3. *Port Box*
4. *Platform List*
5. *Device Group*
6. *OK Button*
7. *Cancel Button*

5. Configure the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) properties for the SAC.

Figure 2-63 SAC Property Configuration — NERC CIP



This tab allows setting NERC CIP properties for this device

Mandatory (Version 3)

Yes	No	
○	●	Is this a 'Critical' device?
●	○	Is this device essential to operation?
○	●	Is this device dial-up accessible?
○	●	Is this an Access Point?
○	●	Does this device use a Routable Protocol?
○	●	Does this device use an Extended Routable Protocol?

Mandatory (Version 5)

BES Cyber System: Medium Impact

Impact: Medium

Optional

Network:

1. *Questions*
2. *Network Box*
3. *OK Button*
4. *Cancel Button*
5. *BES Cyber System List*

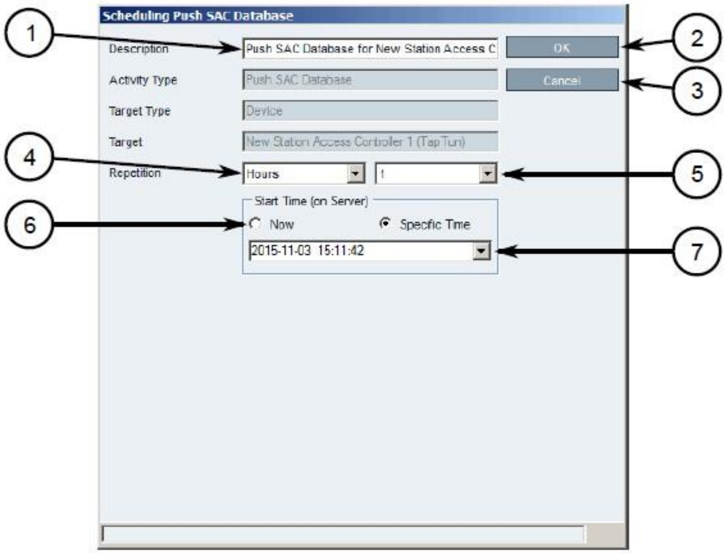
2.14.2.14 Updating the SAC Database

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges. Make sure to enter the host name and port number for the SAC during the login process.

2. Search for the SAC's device family on the **Devices** tab.

3. Right-click the **Station Access Controller** device family, point to **Special Operations,** then click **Push SAC Database.** The Scheduling Push SAC Database dialogue box will appear.

Figure 2-64 Scheduling Push SAC Database



Scheduling Push SAC Database

Description: Push SAC Database for New Station Access C

Activity Type: Push SAC Database

Target Type: Device

Target: New Station Access Controller 1 (Tap Tun)

Repetition: Hours 1

Start Time (on Server)

○ Now ● Specific Time

2015-11-03 15:11:42

1. *Description Box*
2. *OK Button*
3. *Cancel Button*
4. *Repetition Lists*
5. *Start Time Options*
6. *Start Time Box*

4. Optional: Under **Description,** type a description for the operation. Include details such as the affected target, the purpose of the operation, etc. This description will appear in the list of scheduled operations.
5. Under **Repetition,** select the interval and value (if applicable).
6. Under **Start Time (On Server),** select **Now** or **Specific Time.**
7. Click **OK** to save changes. The operation will commence at the selected time.

2.14.2.15 Managing Devices and Gateways

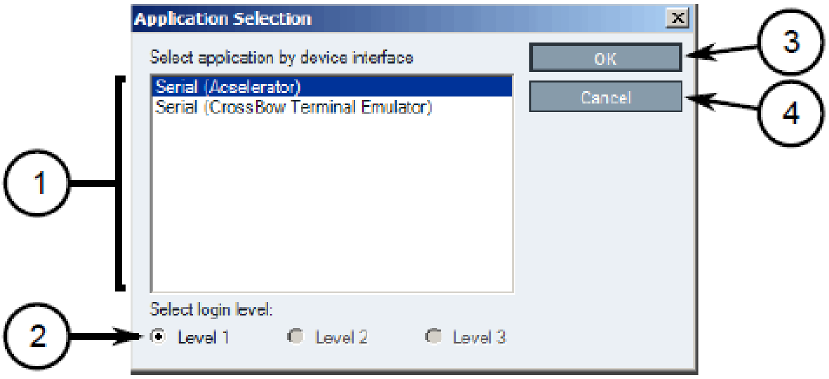
1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges.
2. On the **Field Layout** tab, right-click the desired facility or gateway, and click **Add Device, Add Gateway,** or **Add Subordinate Gateway (gateways only).** The Device Properties or Gateway Properties dialogue box will appear.
3. Configure the identification properties (e.g., name, description) for the device/gateway.
4. Configure the connection properties (e.g., host name, user names, passwords) for the device/gateway.
5. Configure the interfaces available for the device/gateway.
6. Enable or disable the applications available for the device/gateway.
7. Configure the NERC CIP properties for the device/gateway.
8. Configure any advanced parameters associated with the device/gateway.
9. Click **OK** to save changes.

2.14.2.16 Connecting to a Device/Gateway

1. Access the RUGGEDCOM CROSSBOW client workstation, launch CROSSBOW Client, and log in as a user with the necessary administrative privileges.
2. If connecting to the device/gateway via a Station Access Controller, make sure to enter the host name and port number for the SAC during the login process. Otherwise, provide the host name and port number for the RUGGEDCOM CROSSBOW Server.
3. Search for the desired device/gateway on the **Field Layout** or **Devices** tab by either facility or device type.

4. Right-click the device/gateway, and then click either **Connect (devices)** or **Connect to Gateway (gateways).** The Application Selection dialogue box will appear.

Figure 2-65 Application Selection Dialogue



Application Selection

Select application by device interface

Serial (Acselerator)
Serial (CrossBow Terminal Emulator)

Select login level:

● Level 1 ○ Level 2 ○ Level 3

1. *Available Applications*
2. *Select Login Level Options*
3. *OK Button*
4. *Cancel Button*

5. Select an application to connect to the device's interface.

6. Under **Select login level,** select the login level to use when connecting to the device.

7. Click **OK.** RUGGEDCOM CROSSBOW will attempt to connect to the device. Review the Messages pane for details.

8. Once connected, the device/gateway and the connection status are displayed in the **Device Connection History** pane.

9. When the application launches, if required, enter the local host IP address or the real IP address of the end-device or gateway, followed by the port number.

2.15 Siemens RUGGEDCOM RX1400 (E1)

The Siemens RUGGEDCOM RX1400 device is used on the enterprise side of the lab and creates an always-on VPN connection to the Siemens RUGGEDCOM RX1501, located on the boundary of the control network lab.

2.15.1 Environment Setup

Requirements for installation:

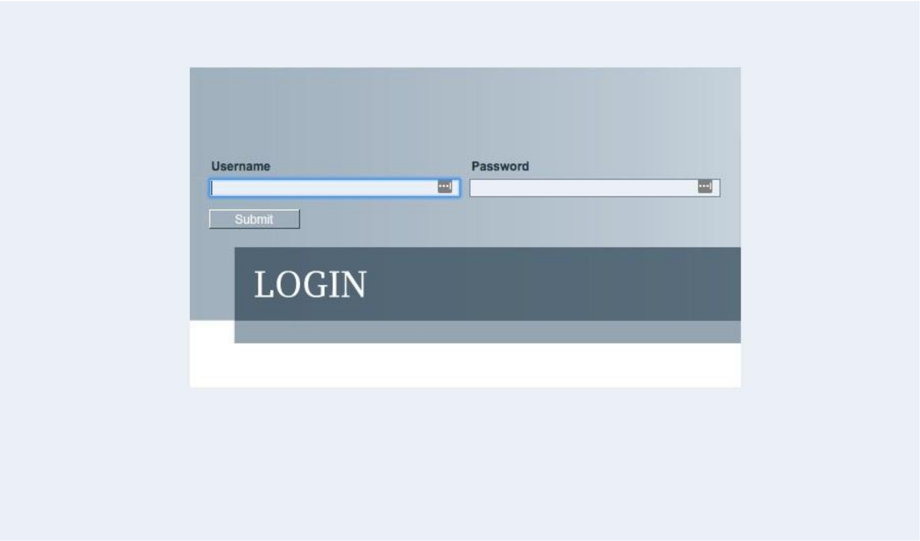
- personal computer/laptop with Ethernet port
- CAT5 or higher Ethernet cables
- RUGGEDCOM VPN device
- any type of terminal emulator
- web browser
- When connecting the device to the network, the NCCoE used switch.0001 as the wide area network (WAN) port and switch.0010 as the local area network port connected to the local network.

2.15.2 Installation Procedure

1. After powering on the device, connect to the IP address that the device supplies itself via a web browser. The connection will most likely require an interim switch for connecting, but this varies between cases.

2. The following screen should appear:

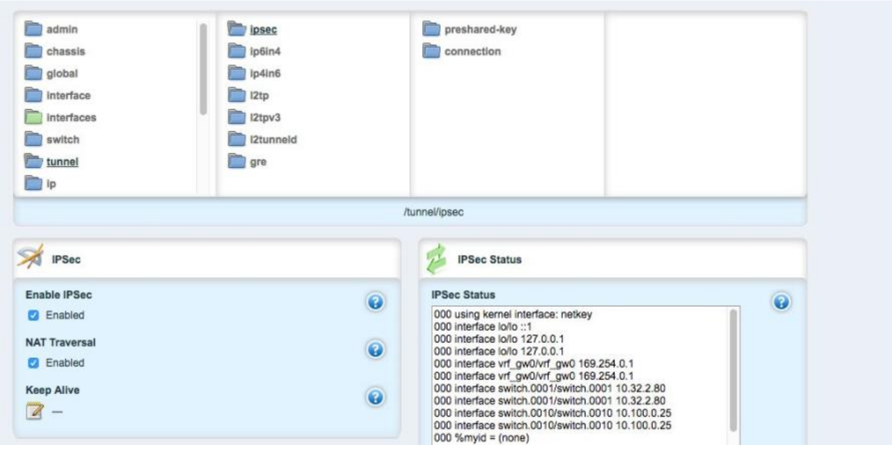
Figure 2-66 RUGGEDCOM Web Login



3. Once logged in, click the link for **Edit Private** to go into Edit mode.

4. Navigate to **tunnel -> ipsec,** and check the boxes for **Enable IP security (IPSec)** and network address translator (**NAT) Traversal.**

Figure 2-67 Enable IPSec and NAT Traversal



Enable IPSec
☑ Enabled

NAT Traversal
☑ Enabled

Keep Alive
—

IPSec Status

```
000 using kernel interface: netkey
000 interface lo/lo ::1
000 interface lo/lo 127.0.0.1
000 interface lo/lo 127.0.0.1
000 interface vrf_gw0/vrf_gw0 169.254.0.1
000 interface vrf_gw0/vrf_gw0 169.254.0.1
000 interface switch.0001/switch.0001 10.32.2.80
000 interface switch.0001/switch.0001 10.32.2.80
000 interface switch.0010/switch.0010 10.100.0.25
000 interface switch.0010/switch.0010 10.100.0.25
000 %myid = (none)
```

5. Click **preshared-key,** then **<Add preshared-key>.**
6. In the **Remote Address** field, type the remote IP address (the cogeneration plant's IP address).
7. In the **Local Address** field, type the local IP address (the enterprise network).
8. Click **Add.**
9. Click the newly created entry under the preshared-key folder.
10. Under **Secret Key,** create a new secret key that will be shared between devices.
11. Under **ipsec->connection,** click **<Add connection>** to create a new connection.
12. Fill in a name for **Connection Name,** then click **Add.**
13. Click on the new connection, and click the **Enable** check box for **Dead Peer Detect.**
14. Ensure that the settings under **Dead Peer Detect** are:
    a. Interval: **30**
    b. Timeout: **120**
    c. Action: **Restart**
15. Under **Connection**, set the following parameters:

    a. Startup Operation: **start**
    b. Authenticate By: **secret**
    c. Connection Type: **tunnel**
    d. Address-family: **ipv4**
    e. Perfect Forward Secrecy: **yes**
    f. SA Lifetime: **default**
    g. IKE Lifetime: **default**
    h. L2TP: **Unchecked (disabled)**
    i. Monitor Interface: **switch.0001**

16. In the top window row, select the folder **ike,** and click **<Add algorithm>.**
17. Under **Key settings,** ensure the following parameters and click **Add:**
    a. Cipher Algorithm: **aes256**
    b. Hash Method: **sha2**
    c. Modpgroup: **modp8192**
18. Going back to the top window row, select the **esp** folder directly underneath **ike,** then select **algorithm** and click **<Add algorithm>.**
19. Under **Key settings,** ensure the following parameters and click **Add:**
    a. Cipher Algorithm: **aes256**
    b. Hash Method: **sha2**
20. Going back to the top window row, select **left** under **esp.**
21. Under **Public IP Address,** ensure **Type** is **address,** then type the IP address into the **Hostname** or **IP Address** field.
22. Going back to the top window row, select **subnet,** and click **<Add subnet>.**
23. Under **Key Settings,** in the **Subnet Address** field, type the local subnet on the inside of the RX1400 in the box (lab used 10.100.0.0/16) and click **Add.**
24. Going back to the top window row, select **right** under **left.**

25. Under **Public IP Address,** ensure **Type** is **address,** then type the remote VPN IP Address into the **Hostname** or **IP Address** field.

26. Under the **Right** heading, for **NAT Traversal Negotiation Method,** select **rfc-3947.**

27. Going back to the top window row, select **subnet,** then click **<Add subnet>.**

28. Under **Key Settings,** in the **Subnet Address** field, type the remote subnet on the inside of the remote VPN in the box (lab used 172.19.0.0/16) and click **Add.**

29. Going back to the beginning of the top row, ensure that **interfaces->ip->switch.0001->ipv4** contains a folder named after the externally facing network IP address.

30. Ensure that **interface->ip->switch.0010->ipv4** contains a folder named after the internal network (lab used 10.100.0.0/16).

2.16 Siemens RUGGEDCOM RX1501 (O1)

The Siemens RUGGEDCOM RX1501 device is used on the boundary of the control network lab and creates an always-on VPN connection to the Siemens RUGGEDCOM RX1400, located on the inside of the enterprise network lab.

2.16.1 Siemens RUGGEDCOM RX1501 (O1) Installation Guide

The instructions for installation of the RUGGEDCOM RX1501 are very similar to those in Section 2.15, with the following additional information:

1. Ensure that the shared key used in this installation is the same as the one used in the previous installation.

2. The remote IPs and local IPs will be different for this installation as they are relative to the device.

3. **NAT Traversal Negotiation Method** will be on the **left** menu option (as opposed to the **right** listed earlier) and must be the same value (e.g., rfc-3947).

2.17 TDi Technologies ConsoleWorks (E6, O5, O9)

TDi Technologies ConsoleWorks creates multiple consoles (both GUI- and terminal-based) that allow connections through a web interface to internal devices, utilizing a protocol break to separate connections. ConsoleWorks is also utilized to normalize syslogs from the control network before sending them to the SIEM.

2.17.1 System Environment

The system that was set up to run this application was a fully updated (as of 4/20/2016) CentOS 7 Operating System with the following hardware specifications:

- 4 GB RAM
- 500 GB HDD
- 2 network interface controllers (NICs)
- This installation required a preconfigured network where one NIC was located on the WAN side (connected to the Waterfall Secure Bypass) and the other was connected to the Dell R620 ESXi server.

Other requirements:

- ConsoleWorks install media (a CD was used in the build)
    - ConsoleWorksSSL-<version>.rpm
    - ConsoleWorks_gui_gateway-<version>.rpm
- ConsoleWorks license keys (TDI_Licenses.tar.gz)
- software installation command:

```
yum install uuid libbpng12 libvncserver
```

2.17.2 Installation

As Root:

1. Place ConsoleWorks Media into the system (assuming from here on that the media is in the form of a CD).
2. `mount /dev/sr0 /mnt/cdrom`
3. `mkdir /tmp/consoleworks`
4. `cp /mnt/cdrom/consolew.rpm /tmp/consoleworks/consolew.rpm`
5. `rpm -ivh /tmp/consoleworks/ConsoleWorksSSL-<version>.rpm`
6. `mkdir /tmp/consoleworkskeys/`
7. Copy ConsoleWorks keys to `/tmp/consoleworkskeys/`
8. `cd /tmp/consoleworkskeys/`
9. `tar xzf TDI_Licenses.tar.gz`
10. `cp /tmp/consoleworkskeys* /etc/TDI_licenses/`

11. `/opt/ConsoleWorks/bin/cw_add_invo`

12. **Accept** the License Terms.

13. Press **Enter** to continue.

14. Name the instance of ConsoleWorks.

15. Press **Enter** to accept default port (5176).

16. Press **N** to deny SYSLOG listening.

17. Press **Enter** to accept parameters entered.

18. Press **Enter** to return to /opt/ConsoleWorks/bin/cw_add_invo.

19. `rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm`

20. `/opt/gui_gateway/install_local.sh`

21. `/opt/ConsoleWorks/bin/cw_start <invocation name created early>`

22. `service gui_gatewayd start`

2.17.3 Usage

1. Open a browser and navigate to *https://<ConsoleWorksIP>:5176*.

2. Log in with Username **console_manager,** Password **Setup.**

3. Change the default password.

4. Choose **Register Now.**

2.17.3.1 Initial Configuration

All instructions below start with a menu on the sidebar.

1. Tags

   Security > Tags > Add

   i. Set **Name.**

   ii. Click **Save.**

2. Profiles

   Users > Profiles > Add

   i. Set **Name.**

ii. Select **Tag.**

iii. Click **Save.**

3. Users

Users->Add

i. Set **Name.**

ii. Set **Password.**

iii. Set **Profile.**

iv. Set **Tag.**

v. Click **Save.**

2.17.3.2 Graphical Connections

Use the following steps to set up graphical connections (specifically virtual network computing (VNC)):

1. Graphical Gateway:

   a. **Graphical->Gateways->Add**

   b. Set a name, then set Host as **Localhost** and port as **5172.**

   c. Check the **Enabled** check box and click **Save.**

   d. Verify that it works by clicking **Test** in the top left corner.

2. Add a graphical connection (We will use VNC.):

   a. **Graphical->Add**

   b. Set **Name.**

   c. Set the **Type** (VNC/remote desktop protocol (RDP)).

   d. Set the **Hostname/IP.**

   e. If recordings are desired, set **Directory** and **Recordings.**

   f. Set the **Authentication.**

   g. Add **Graphical Gateway.**

   h. Add **Tags.**

3. Access Controls

    a. **Security->Access Control->Add**

    b. Set **Name.**

    c. Check **Enabled.**

    d. Set **Priority.**

    e. Set **ALLOW.**

    f. Set **Component Type** to **Graphical Connection.**

    g. The following will appear under **Profile Selection**:

        i. `Property Profile Equals *Profile Name* <join>`

        ii. The correct profile should appear in the box on right.

    h. The following will appear under **Resource Selection**:

        i. `Associate With a Tag that`

        ii. `Property Tag Equals *Tag name* <join>`

        iii. The correct Graphical Console should appear in the box on right.

    i. Under **Privileges**, check …

        i. **Aware**

        ii. **View**

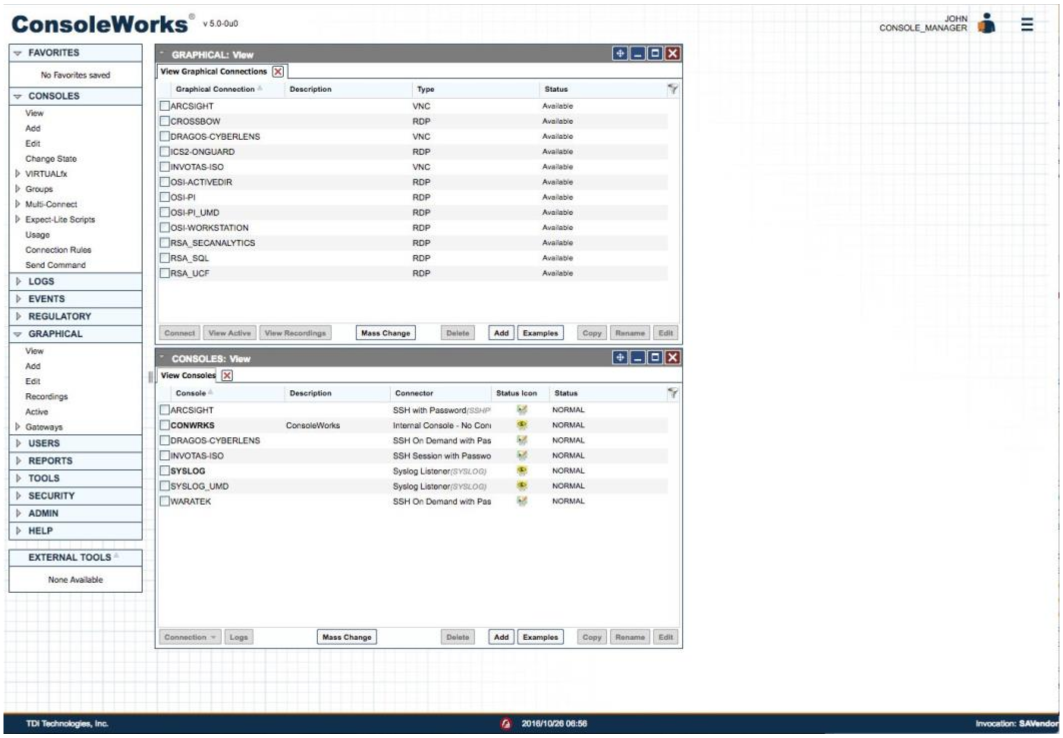
        iii. **Connect**

        iv. **Enable**

        v. **Monitor**

    j. Click **Save.**

Figure 2-68 Binding to Syslog



Graphical Connection	Description	Type	Status
☐ARCSIGHT		VNC	Available
☐CROSSBOW		RDP	Available
☐DRAGOS-CYBERLENS		VNC	Available
☐ICS2-ONGUARD		RDP	Available
☐INVOTAS-ISO		VNC	Available
☐OSI-ACTIVEDIR		RDP	Available
☐OSI-PI		RDP	Available
☐OSI-PI_UMD		RDP	Available
☐OSI-WORKSTATION		RDP	Available
☐RSA_SECANALYTICS		RDP	Available
☐RSA_SQL		RDP	Available
☐RSA_UCF		RDP	Available

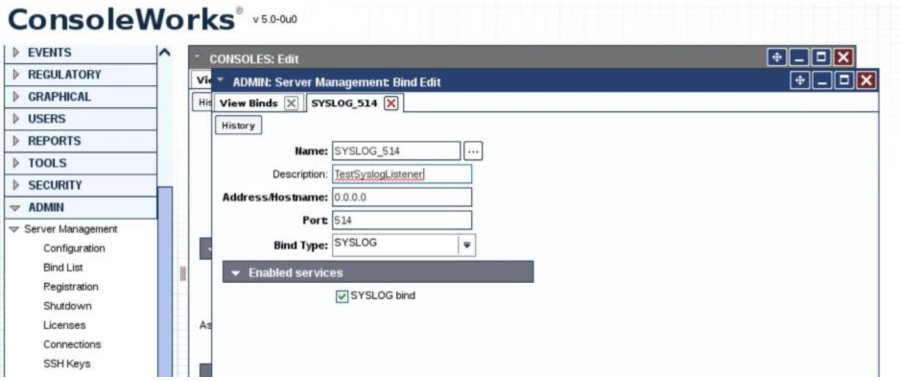
Console	Description	Connector	Status Icon	Status
☐ARCSIGHT		SSH with Password(SSHP	✓	NORMAL
☐**CONWRKS**	ConsoleWorks	Internal Console - No Con	●	NORMAL
☐DRAGOS-CYBERLENS		SSH On Demand with Pas	✓	NORMAL
☐INVOTAS-ISO		SSH Session with Passwo	✓	NORMAL
☐**SYSLOG**		Syslog Listener(SYSLOG)	●	NORMAL
☐SYSLOG_UMD		Syslog Listener(SYSLOG)	●	NORMAL
☐WARATEK		SSH On Demand with Pas	✓	NORMAL

2.17.4 TDi Technologies ConsoleWorks (E6) Installation Guide

Follow the guide above on installing ConsoleWorks instance (O5), however, do not follow Section 2.17.3.1, Initial Configuration; or Section 2.17.3.2, Graphical Connections.

1. Navigate to **Server Management > Bind List > Add.**
2. Enter a name for **Binding** (e.g. SYSLOG_514).
3. Leave **Address** as default (0.0.0.0).
4. Set **Port** to **514.**
5. Set Bind type to **SYSLOG** and **Enable.**

Figure 2-69 Server Management Bind Edit



Name: SYSLOG_514
Description: TestSyslogListener
Address/Hostname: 0.0.0.0
Port: 514
Bind Type: SYSLOG
Enabled services
☑ SYSLOG bind

6. Navigate to **Consoles > Add.**

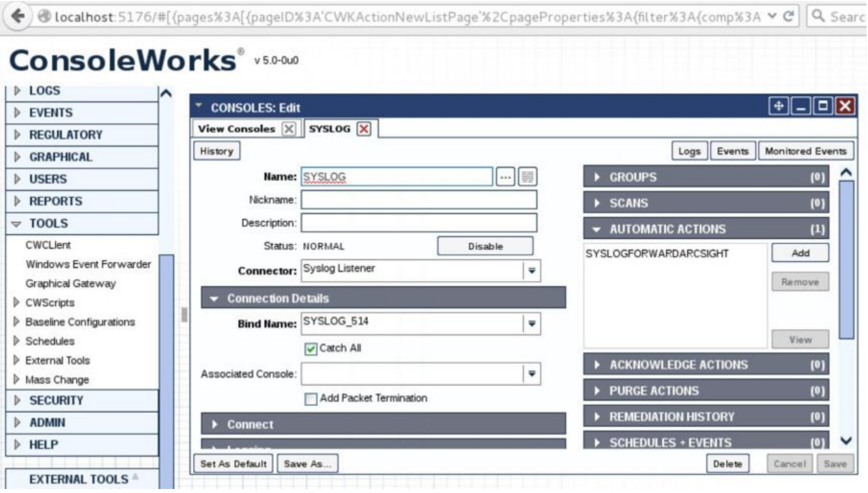
7. Add **Console** and set a name (e.g., SYSLOG).

8. In the **Connector** field, click the drop-down menu, and select **Syslog Listener.**

9. Under **Connection Details,** click the drop-down menu, and select the **Binding** that was created above (e.g., SYSLOG_514).

10. Check the **Catch All** check box.

Figure 2-70 Adding SYSLOG Console

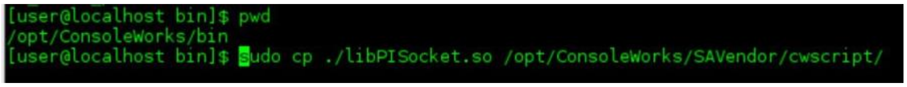


Name: SYSLOG
Nickname:
Description:
Status: NORMAL
Connector: Syslog Listener
Connection Details
Bind Name: SYSLOG_514
☑ Catch All
Associated Console:
☐ Add Packet Termination

SYSLOGFORWARDARCSIGHT

11. Copy the socket plug-in to the **cwscript** directory under the ConsoleWorks instance directory.

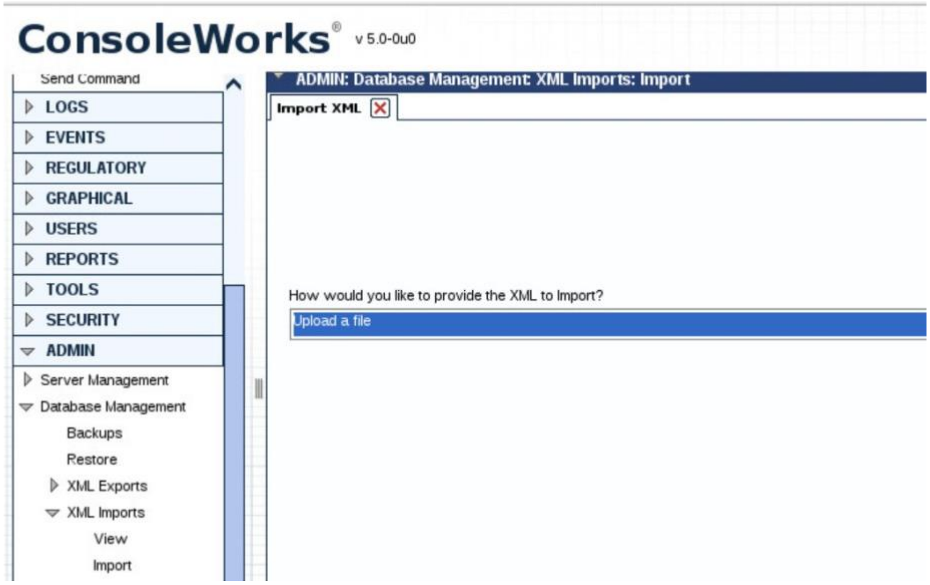
Figure 2-71 Copying Plug-In to CWScript Directory



```
[user@localhost bin]$ pwd
/opt/ConsoleWorks/bin
[user@localhost bin]$ sudo cp ./libPISocket.so /opt/ConsoleWorks/SAVendor/cwscript/
```

12. Navigate to **Admin > Database Management > XML Imports > Import > Upload a file,** then click **Next.**

Figure 2-72 CWScript Upload

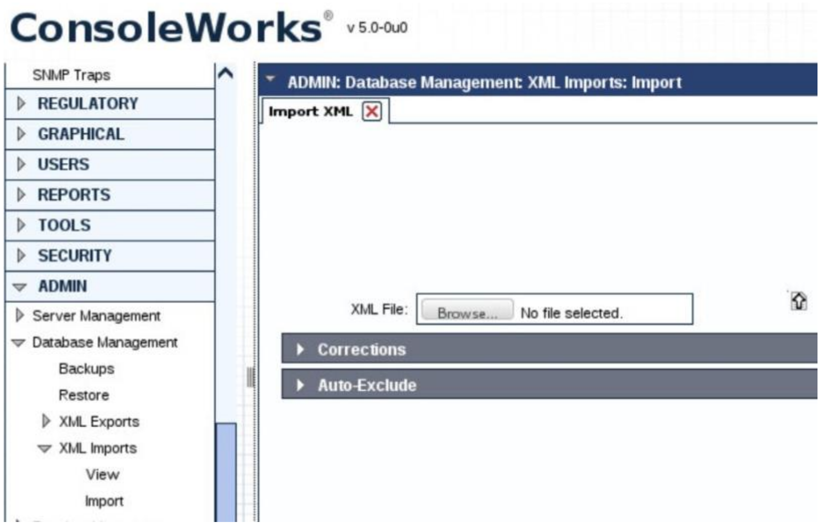


How would you like to provide the XML to Import?

Upload a file

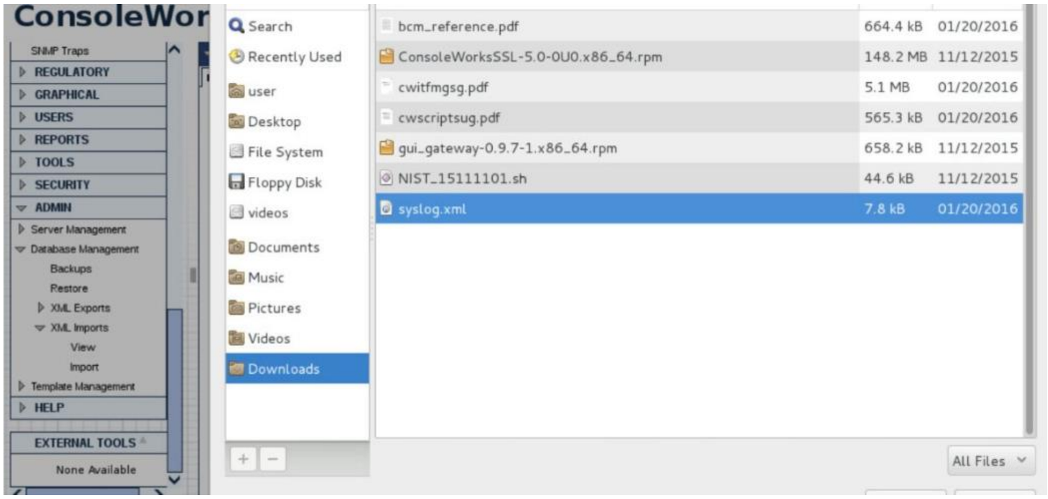
13. Click **Browse.**

Figure 2-73 Browse for CWScript



14. Select the **syslog.xml** file, then click **Next.**

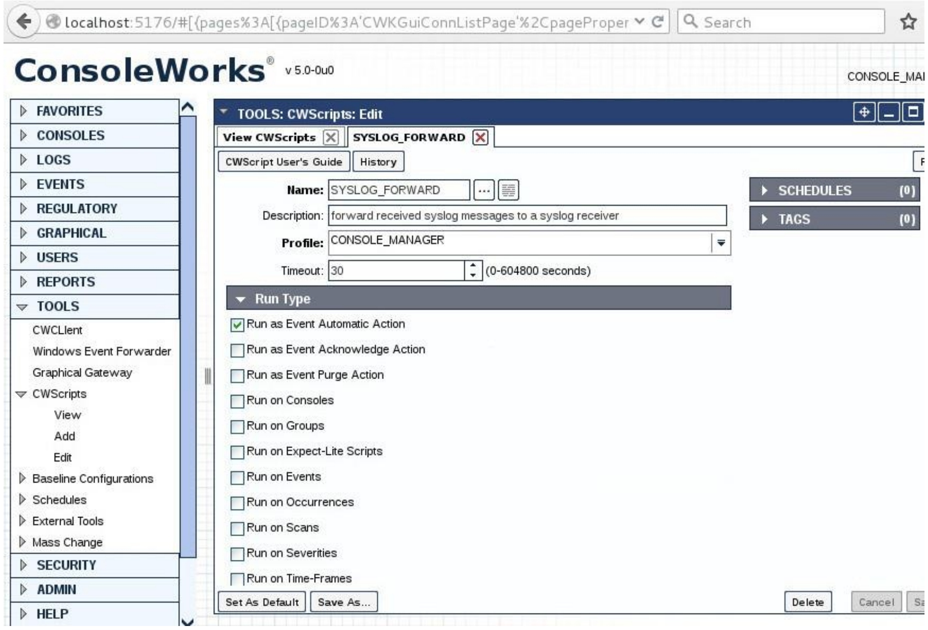
Figure 2-74 Select CWScript XML



bcm_reference.pdf	664.4 kB	01/20/2016
ConsoleWorksSSL-5.0-0U0.x86_64.rpm	148.2 MB	11/12/2015
cwitfmgsg.pdf	5.1 MB	01/20/2016
cwscriptsug.pdf	565.3 kB	01/20/2016
gui_gateway-0.9.7-1.x86_64.rpm	658.2 kB	11/12/2015
NIST_15111101.sh	44.6 kB	11/12/2015
syslog.xml	7.8 kB	01/20/2016

15. Navigate to **Tools > CWScripts > Select SYSLOG_FORWARD > Review Settings.**

Figure 2-75 Review CWScript Settings



Name: SYSLOG_FORWARD

Description: forward received syslog messages to a syslog receiver

Profile: CONSOLE_MANAGER

Timeout: 30 (0-604800 seconds)

Run Type

☑ Run as Event Automatic Action
☐ Run as Event Acknowledge Action
☐ Run as Event Purge Action
☐ Run on Consoles
☐ Run on Groups
☐ Run on Expect-Lite Scripts
☐ Run on Events
☐ Run on Occurrences
☐ Run on Scans
☐ Run on Severities
☐ Run on Time-Frames

16. Navigate to **Actions > Automatic > Add.**

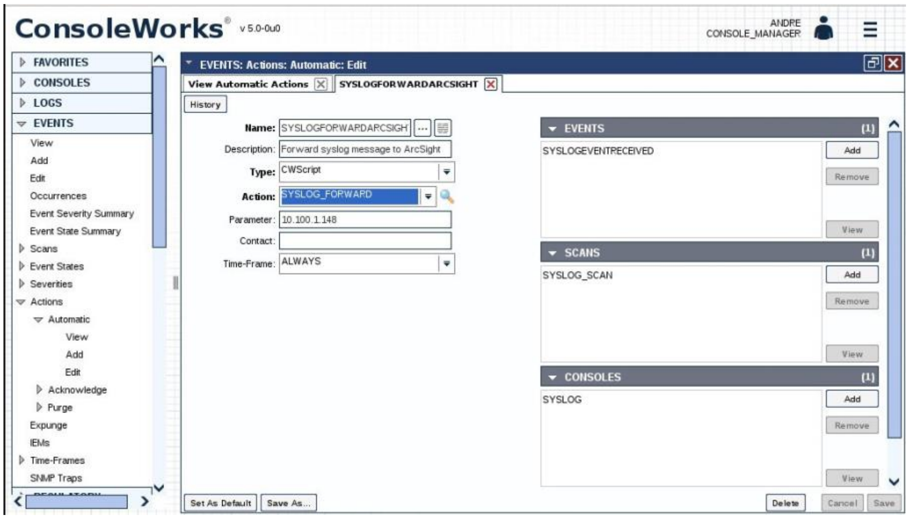
17. Set **Name.**

18. Set Type to **CWScript.**

19. In the **Action** field, click the drop-down menu, and select **SYSLOG_FORWARD.**

20. In the **Parameter** field, enter the IP address (or FQDN) of the Syslog target.

Figure 2-76 Modify Action and Parameter for CWScript



Name: SYSLOGFORWARDARCSIGH

Description: Forward syslog message to ArcSight

Type: CWScript

Action: SYSLOG_FORWARD

Parameter: 10.100.1.148

Contact:

Time-Frame: ALWAYS

EVENTS (1): SYSLOGEVENTRECEIVED

SCANS (1): SYSLOG_SCAN

CONSOLES (1): SYSLOG

21. Navigate to **Scans,** then select **Add.**

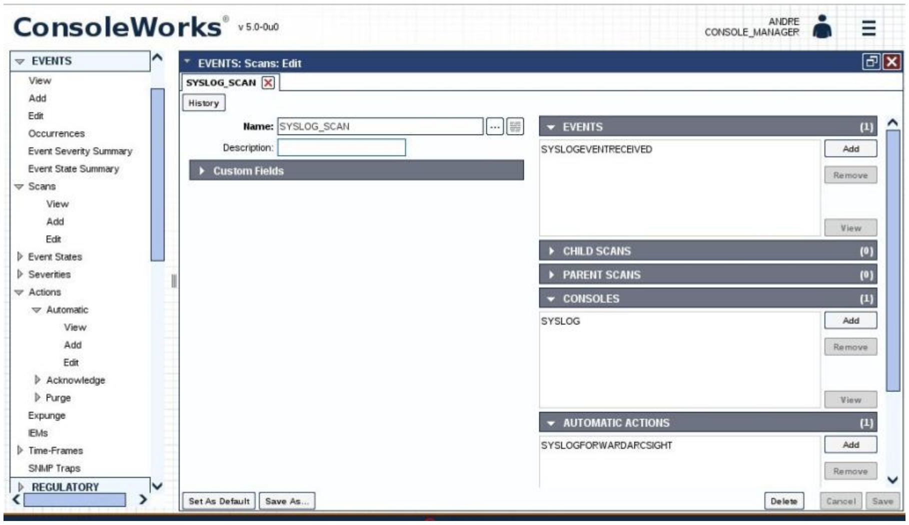
22. Set **Name.**

23. In the **Consoles** field, add/select the Console defined in the previous steps.

24. In the **Automatic Action** field, add/select the Action defined in the previous steps.

    Note: *The Events field will be updated later*.

Figure 2-77 Add New Scan



Name: SYSLOG_SCAN

Description:

EVENTS (1)

SYSLOGEVENTRECEIVED

CONSOLES (1)

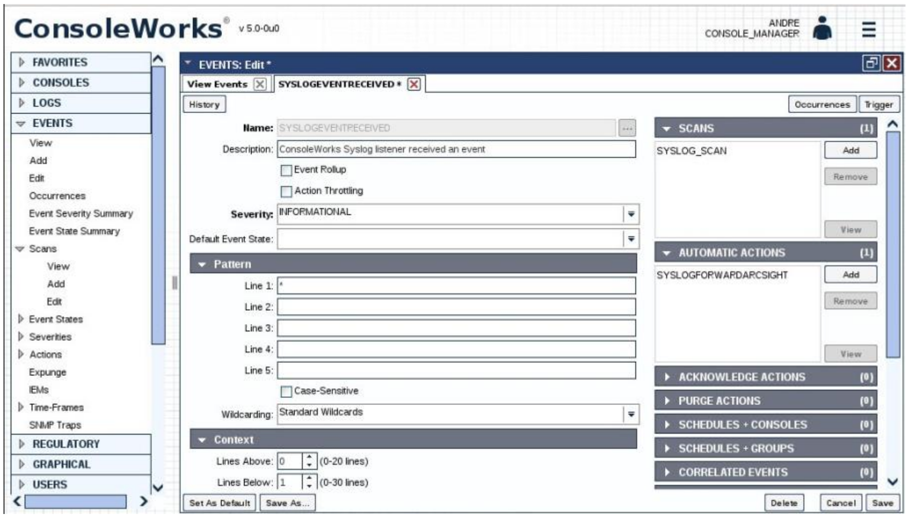
SYSLOG

AUTOMATIC ACTIONS (1)

SYSLOGFORWARDARCSIGHT

25. Navigate to **Events,** then select **Add.**
26. **Name** the Event.
27. Set the **Severity** level.
28. In the **Pattern** fields, line 1, type in a character pattern that matches the syslog data. Set **Wildcarding** to **Standard Wildcards.**
29. In the context **Lines Below** field, enter **1.**
30. In the **Scans** field, click **Add,** then select the name of the Scan that was defined in the previous steps.
31. In the **Automatic Actions** field, click **Add,** then select the name of the Action that was defined in the previous steps.

Figure 2-78 Add New Event



Name: SYSLOGEVENTRECEIVED

Description: ConsoleWorks Syslog listener received an event

☐ Event Rollup

☐ Action Throttling

Severity: INFORMATIONAL

Default Event State:

Line 1: *

Line 2:

Line 3:

Line 4:

Line 5:

☐ Case-Sensitive

Wildcarding: Standard Wildcards

Lines Above: 0 (0-20 lines)

Lines Below: 1 (0-30 lines)

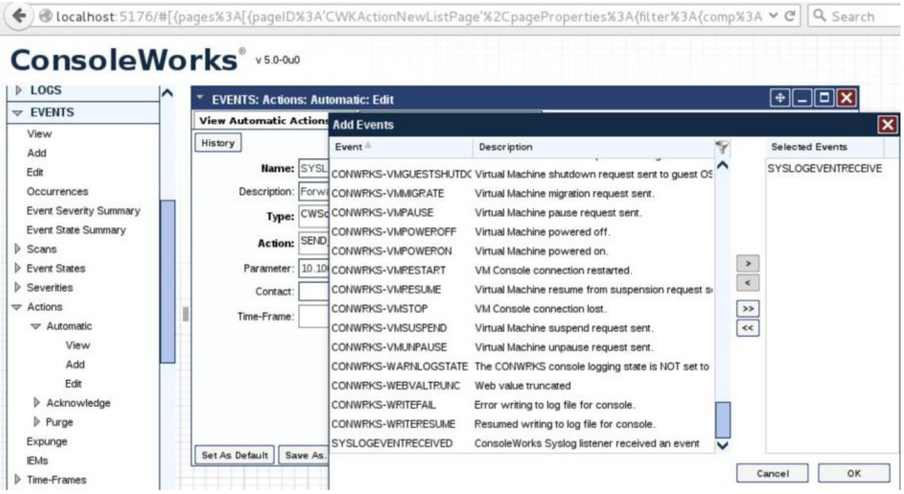
SCANS: SYSLOG_SCAN

AUTOMATIC ACTIONS: SYSLOGFORWARDARCSIGHT

32. Navigate back to **Actions > Automatic,** then edit the Action defined in the previous steps.

33. In the **Event** field, confirm that the Event that was just created is selected.

Figure 2-79 Syslog Forwarding Action Config



Name: SYSL

Description: Forw

Type: CWSc

Action: SEND

Parameter: 10.10

Contact:

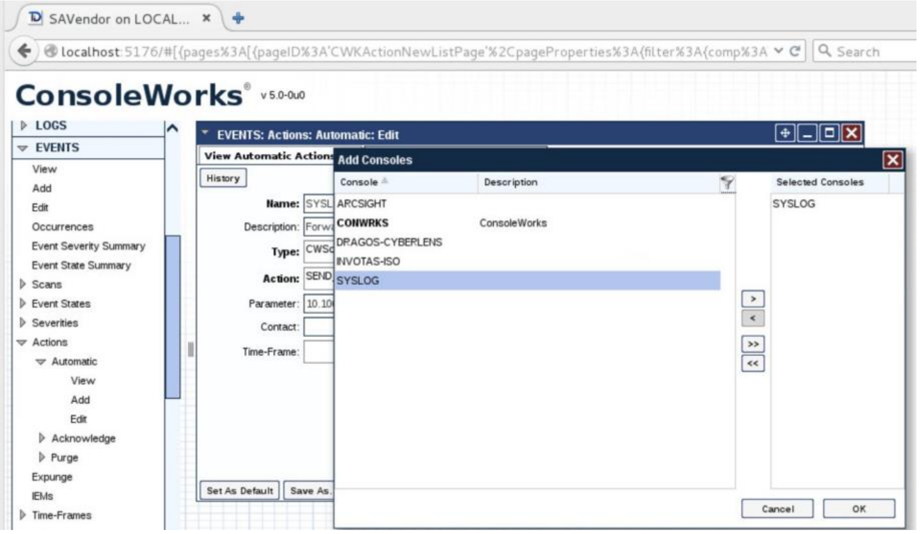
Time-Frame:

Event	Description
CONWRKS-VMGUESTSHUTDC	Virtual Machine shutdown request sent to guest OS
CONWRKS-VMMIGRATE	Virtual Machine migration request sent.
CONWRKS-VMPAUSE	Virtual Machine pause request sent.
CONWRKS-VMPOWEROFF	Virtual Machine powered off.
CONWRKS-VMPOWERON	Virtual Machine powered on.
CONWRKS-VMRESTART	VM Console connection restarted.
CONWRKS-VMRESUME	Virtual Machine resume from suspension request s
CONWRKS-VMSTOP	VM Console connection lost.
CONWRKS-VMSUSPEND	Virtual Machine suspend request sent.
CONWRKS-VMUNPAUSE	Virtual Machine unpause request sent.
CONWRKS-WARNLOGSTATE	The CONWRKS console logging state is NOT set to
CONWRKS-WEBVALTRUNC	Web value truncated
CONWRKS-WRITEFAIL	Error writing to log file for console.
CONWRKS-WRITERESUME	Resumed writing to log file for console.
SYSLOGEVENTRECEIVED	ConsoleWorks Syslog listener received an event

Selected Events: SYSLOGEVENTRECEIVE

34. In the **Console** field, select the Syslog Console that was defined in previous steps.

Figure 2-80 Add Console to Syslog Forwarding Action Config

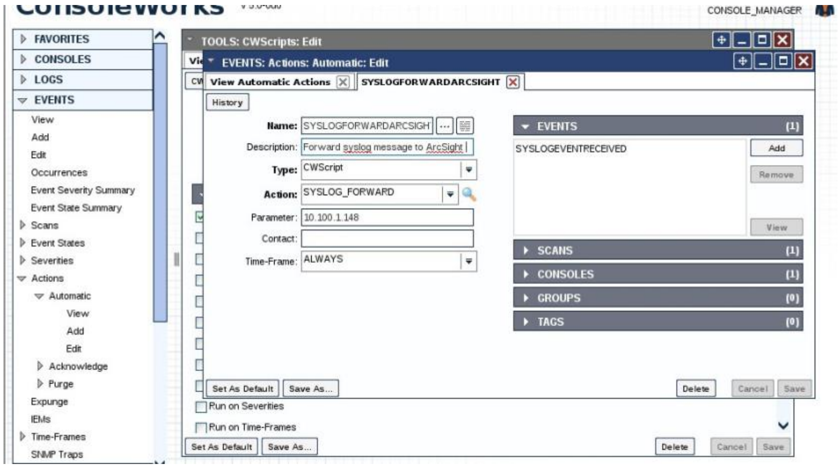


Console	Description
ARCSIGHT	
CONWRKS	ConsoleWorks
DRAGOS-CYBERLENS	
INVOTAS-ISO	
SYSLOG	

Selected Consoles: SYSLOG

35. Review settings.

Figure 2-81 Review Event Settings



Name: SYSLOGFORWARDARCSIGH
Description: Forward syslog message to ArcSight
Type: CWScript
Action: SYSLOG_FORWARD
Parameter: 10.100.1.148
Contact:
Time-Frame: ALWAYS

EVENTS (1): SYSLOGEVENTRECEIVED
SCANS (1)
CONSOLES (1)
GROUPS (0)
TAGS (0)

36. Add rules to ConsoleWorks host OS firewall:

```
iptables -I INPUT -p udp --dport 514 -s 0.0.0.0/0 -j ACCEPT iptables -I
OUTPUT -p udp -s 0.0.0.0/0 --dport 514 -j ACCEPT
```

37. Save the rules:

```
/sbin/service iptables save
```

2.17.5 TDi Technologies ConsoleWorks (O9) Installation Guide

Follow the guide for ConsoleWorks (E6) in Section 2.17.4.

2.18 Waterfall Technologies Unidirectional Security Gateway (O2)

Waterfall's Unidirectional Security Gateway delivers a security gateway solution for replicating servers and emulating devices from the control system lab to the enterprise system lab. The replication occurs through hardware that is physically able to transmit information in only one direction and physically unable to transmit any information or attack in the reverse connection. The Unidirectional Gateway's combination of hardware and software supports many kinds of replications, including process historians, many open platform communication (OPC) variants, syslog, FTP, and others.

2.18.1 Waterfall Technologies Unidirectional Security Gateway (O2) Installation Guide

The Unidirectional Security Gateway was shipped to the NCCoE as an appliance in a 1U server chassis. The chassis contains two Host Modules, each running Microsoft Windows 8. The chassis also contains a Transmit (TX) Module and a Receive (RX) Module, linked by a short fiber-optic cable. The TX Module is physically able to send information/light to the fiber but is unable to receive any signal from the fiber. Conversely, the RX Module is able to receive information from the fiber but has no transmitter and so is physically unable to send any information to the fiber. In this guide, we will refer to the Windows Host Module connected to the TX Module as the Tx host, and the Windows Host Module connected to the RX Module as the Rx host.

2.18.1.1 Rx Configuration

1. Open the **Waterfall RX Configuration** utility located in the **Start** menu.

2.18.1.1.1 FTP Stream

1. Expand **wfStreamRx** from the left sidebar.
2. Expand **Files.**
3. From the sidebar, select **Local Folder.**
4. Under **Channels,** select **Add.** Ensure that the **Active** check box is checked.
5. Fill out the **Channel Name** field, and make a note of the **Channel ID** in parenthesis.
6. From the sidebar, select **NCFTP.**
7. Under **Channels,** select **Add.** Ensure that the **Active** check box is checked.

8. Select the **Automatically Bind to Local Folder with ID** radio button. Ensure that the ID for the Local Folder is selected by using the same ID that was automatically generated for the Local Folder that was just created.
9. Fill out the correct values for the following form fields:
    a. FTP folder: **/file_link**
    b. FTP host: **10.100.1.250**
    c. FTP port: **21**
    d. Username: **waterfall**
    e. Password: **<insert password here>**
10. For **Transfer mode,** select the **Passive** radio button.
11. For **Transfer type,** select the **Binary** radio button.
12. Ensure that the **Enable recursive transfer** check box is checked.
13. Ensure that the **File pattern** check box is checked and that the form field contains this value: *****.

2.18.1.1.2 OSI Pi Streams

1. Digital
    a. Expand **wfStreamRxPI_D** from the left sidebar.
    b. Expand **SME** from the left sidebar.
    c. Expand **PiPoint** from the left sidebar.
    d. Ensure that the **Active** check box is checked.
    e. Fill out the correct values for the following form fields:
        i. Channel name: **PiPt Digital**
        ii. Server IP: **10.100.1.76**
        iii. Points type: **Digital**
        iv. Snapshots/Sec limit: **5000**
        v. Snapshots/Sec warning: **500**
2. Numeric
    a. Expand **wfStreamRxPI_N** from the left sidebar.

b. Expand **SME** from the left sidebar.

c. Expand **PiPoint** from the left sidebar.

d. Ensure that the **Active** check box is checked.

e. Fill out the correct values for the following form fields:

i. Channel name: **PiPt Numeric**

ii. Server IP: **10.100.1.76**

iii. Points type: **Numeric**

iv. Snapshots/Sec limit: **5000**

v. Snapshots/Sec warning: **5000**

3. String

a. Expand **wfStreamRxPI_S** from the left sidebar.

b. Expand **SME** from the left sidebar.

c. Expand **PiPoint** from the left sidebar.

d. Ensure that the **Active** check box is checked.

e. Fill out the correct values for the following form fields:

i. Channel name: **PiPt String**

ii. Server IP: **10.100.1.76**

iii. Points type: **String**

iv. Snapshots/Sec limit: **5000**

v. Snapshots/Sec warning: **5000**

2.18.1.1.3 Syslog Streams

1. Expand **wfStreamRx** from the left sidebar.

2. Expand I**T Monitoring** from the left sidebar.

3. Select **Syslog UDP** from the left sidebar.

4. Under **Channels,** select **Add.** Ensure that the **Active** check box is checked.

5. Fill out the correct values for the following form fields:

Channel name: **Syslog 1**

Send report every: **500**

6. Under T**arget Addresses,** select **Add,** and set the IP address to **10.100.0.50** and port to **514.**

2.18.1.2 TX Configuration

Open the **Waterfall TX Configuration** utility located in the **Start** menu.

2.18.1.2.1 FTP Stream

1. Expand **wfStreamTx** from the left sidebar.
2. Expand **Files.**
3. From the sidebar, select **Local Folder.**
4. Under **Channels,** select **Add.** Ensure that the **Active** check box is checked.
5. Fill out the **Channel name** field, and make a note of the **Channel ID** in parenthesis.
6. From the sidebar, select **NCFTP.**
7. Under **Channels,** select **Add.** Ensure that the **Active** check box is checked.
8. Select the **Automatically Bind to Local Folder with ID** radio button. Select the ID that was automatically generated for the Local Folder created in the previous steps.
9. Fill out the correct values for the following form fields:
    a. FTP folder: **/file_link**
    b. FTP host: **172.18.1.250**
    c. FTP port: **21**
    d. Username: **root**
    e. Password: **<insert password here>**
10. For **Transfer mode,** select the **Passive** radio button.
11. For **Transfer type,** select the **Binary** radio button.
12. Ensure that the **Enable recursive transfer** check box is checked.
13. Ensure that the **File pattern** check box is checked and that the field contains this value: *****.

2.18.1.2.2 OSI Pi Streams

1. Digital
    a. Expand **wfStreamTxPI_D** from the left sidebar.
    b. Expand **SME** from the left sidebar.
    c. Expand **PiPoint** from the left sidebar.
    d. Ensure that the **Active** check box is checked.
    e. Fill out the correct values for the following form fields:
        i. Channel name: **PiPt Digital**
        ii. Server IP: **172.18.2.150**
        iii. Points type: **Digital**
        iv. Snapshots/Sec limit: **5000**
        v. Snapshots/Sec warning: **5000**
        vi. APS port: **3010**
2. Numeric
    a. Expand **wfStreamTxPI_N** from the left sidebar.
    b. Expand **SME** from the left sidebar.
    c. Expand **PiPoint** from the left sidebar.
    d. Ensure that the **Active** check box is checked.
    e. Fill out the correct values for the following form fields:
        i. Channel name: **PiPt Numeric**
        ii. Server IP: **172.18.2.150**
        iii. Points type: **Numeric**
        iv. Snapshots/Sec limit: **5000**
        v. Snapshots/Sec warning: **5000**
        vi. APS port: **3000**

3. String
    a. Expand **wfStreamTxPI_S** from the left sidebar.
    b. Expand **SME** from the left sidebar.
    c. Expand **PiPoint** from the left sidebar.
    d. Ensure that the **Active** check box is checked.
    e. Fill out the correct values for the following form fields:
        i. Channel name: **PiPt String**
        ii. Server IP: **172.18.2.150**
        iii. Points type: **String**
        iv. Snapshots/Sec limit: **5000**
        v. Snapshots/Sec warning: **5000**
        vi. APS port: **3020**

2.18.1.2.3 Syslog Streams

1. Expand **wfStreamTx** from the left sidebar.
2. Expand **IT Monitoring** from the left sidebar.
3. Select **Syslog UDP** from the left sidebar.
4. Under **Channels,** select **Add.** Ensure that the **Active** check box is checked.
5. Fill out the correct values for the following form fields:
    a. Channel name: **Syslog 1**
    b. Send report every: **500**
    c. Port: **514**
    d. IP (Listening): **0.0.0.0**
6. Under **target addresses,** select **Add.** Set the IP address to **10.100.0.50** and port to **514.**

2.19 Waterfall Secure Bypass (O17)

Waterfall Secure Bypass is used as a secure connection solution that allows bidirectional communication into the product lab at the control system. It is solely dependent on a person turning a physical key, and it has an automated time-out of two hours.

2.19.1 Waterfall Secure Bypass (O17) Installation Guide

The Waterfall Secure Bypass Solution is installed directly between the Siemens RUGGEDCOM RX1501 (O1) and a Schneider Electric Tofino Firewall (O18).

1. Connect an Ethernet cable from the RX1501 to the **Ext** interface of the Secure Bypass.

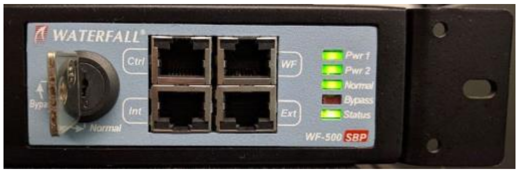
2. Connect an Ethernet cable from the WAN interface of the Tofino to the **Int** interface of the Secure Bypass.

3. When the key is fully turned clockwise, the Secure Bypass will allow bidirectional traffic between the Tofino and the RX1501.

4. When the key is fully turned counterclockwise, the Secure Bypass will block all traffic between the Tofino and the RX1501.

5. If the key is left fully turned clockwise for more than two hours (time was configured at Waterfall location prior to receiving the device), the Secure Bypass will block all traffic between the Tofino and the RX1501. To allow for traffic to pass again, the user must fully turn the key counterclockwise and then clockwise again.

Figure 2-82 Waterfall Secure Bypass Interface



2.20 Waratek Runtime Application Protection (E10)

Waratek Runtime Application Protection is a software agent plug-in for monitoring and protecting user interactions with enterprise applications. In the build, Waratek is monitoring a database application for any attempts the user may undertake to pull unauthorized data from the database (mainly through SQL injection).

For further information, see http://www.waratek.com/solutions/ or http://www.waratek.com/runtime-application-self-protection-rasp/.

2.20.1 System Environment

A CentOS 7 Operating System (fully updated as of 4/20/2016) was set up to run this application. Other requirements:

Web application that demonstrates protection capabilities (this build used Spiracle, Waratek's demo application: https://github.com/waratek/spiracle).

- web application server (This build used Apache Tomcat 9.)
- SQL database (can be MSSQL, MySQL, or Oracle. In the build, we used MySQL.)

2.20.2 Waratek Runtime Application Protection (E10) for Java Installation

1. Download JDK 8 from the Oracle site, and unzip in **/opt** directory (e.g. /opt/jdk1.8.0_121).
2. To configure for apache tomcat (or other web server), in `$CATALINA_HOME/bin/Catalina.sh`, point `JAVA_HOME` to `/opt/<jdk version>`
3. Add the following line to Catalina.sh:

   ```
   JAVA_OPTS="-javaagent:/opt/waratek/waratek.jar

   -Dcom.waratekContainerHome=/opt/<jdk version>"
   ```

4. Change directories to **/opt,** and untar the **waratek_home.tar.gz** package.
5. `cd waratek_home`
6. Create the **Rules** directory in the current directory.
7. Move the provided **LICENSE_KEY** file from Waratek to **/var/lib/javad/.**
8. Create a rules file: **/opt/waratek-home/Rules/global.rules**

   ```
   VERSION 1.0

   # SQL Injection Blocking sqli:database:mysql:deny:warn
   file:read:/opt/tomcat/*:allow:trace
   ```

9. Create a logging XML file: **/opt/waratek/mylogProps.xml**

   ```
   <logProps-array>

   <logProps>

           <logMode>BOTH</logMode>

           <logFile>SECURITYLOG</logFile>

           <fileName>/opt/waratek/alerts.log</fileName>

           <remoteHost>**INSERT REMOTE SYSLOG HERE (i.e.
           10.100.100.10:514)**</remoteHost>
   ```

```
                <patternLayout>%m</patternLayout>
                <priorityLevel>WARN</priorityLevel>
        </logProps>
        </logProps-array>
```

10. Edit the **/opt/waratek_home/setenv.sh** file as follows:

```
export WARATEK_OPTS="-Dcom.waratek.jvm.name=tomcat7
-Dcom.waratek.rules.local=/opt/waratek_home/Rules/jvc.rules
-Dcom.waratek.log.properties=/opt/waratek_home/logProps.xml
-Dcom.waratek.jmxh
```

2.20.3 Usage

To utilize the Runtime Protection for Java product, start the web application mentioned in Section 2.20.1, System Environment. The web application server (Tomcat 9 in our case) should load the Runtime Protection JDK that was configured.

2.21 ArcSight Connector Guides

The following detail the custom configuration for the ArcSight connectors to individual monitoring and alerting products.

2.21.1 Dragos CyberLens Connector

2.21.1.1 Configure Source Product

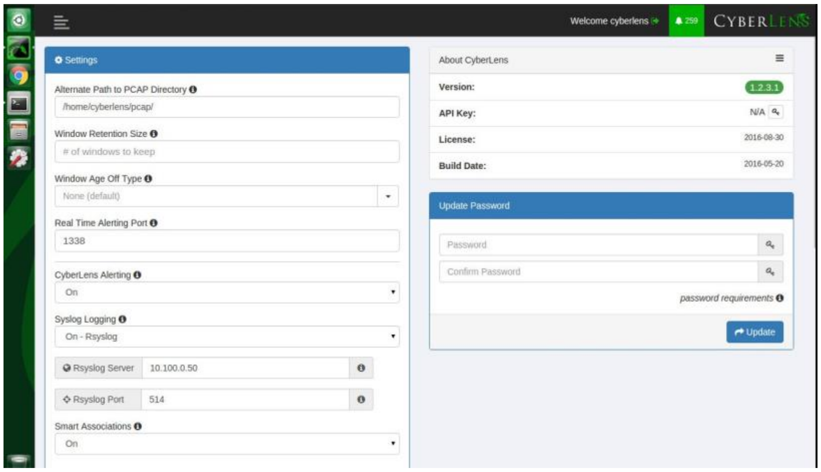
1. Connect to the CyberLens console.
2. In the CyberLens application, go to **Settings.**
3. In the **CyberLens Alerting** drop-down, select **On.**
4. In the **Syslog Logging** section …
    a. Select the drop-down for **On - Rsyslog.**
    b. Enter the **IP address** of the syslog server, e.g.:

       ```
       172.18.0.50
       ```

    c. Enter the **port** of the syslog server, e.g.:

       ```
       514
       ```

Figure 2-83 Set Up Syslog on CyberLens



Alternate Path to PCAP Directory: /home/cyberlens/pcap/

Window Retention Size: # of windows to keep

Window Age Off Type: None (default)

Real Time Alerting Port: 1338

CyberLens Alerting: On

Syslog Logging: On - Rsyslog

Rsyslog Server: 10.100.0.50

Rsyslog Port: 514

Smart Associations: On

Version: 1.2.3.1

API Key: N/A

License: 2016-08-30

Build Date: 2016-05-20

Password

Confirm Password

5. From the command line, using the **cybersudo** account, check the OS firewall to see if it allows the syslog traffic by running **sudo ufw status. Add** and **save** the rule if needed.

Note: *Upon upgrading CyberLens software, the rsyslog settings may be lost. Be sure to check and update these settings as needed after any upgrades*.

2.21.1.2 Install/Configure Custom ArcSight FlexConnector

1. Follow ArcSight's instructions for installing a Linux-based syslog SmartConnector [1].
2. Copy the custom FlexConnector configuration files to the appropriate locations.
3. Start the Connector service:

```
/etc/init.d/arc_<connectorName> start
```

2.21.1.3 Custom Parser — ArcSight FlexConnector Parser

1. Create a file containing the text below, and copy this file to **/opt/arcsight/connectors/<connector directory>/current/user/agent/flexagent/cyberlens.subagent.sdkrfilereader.properties**

```
#:::::::::::::::::::::::::::::::::::::::::::::::

# Syslog custom subagent regex properties file: for CyberLens rsyslog

#

# raw syslog example:

# "Sep 6 16:04:48 ubuntu CyberLensApp: I, [2016-09-06T16:04:48.839937

#65401]       INFO -- : Cyberlens generated the following alert: A Sensor
saw 'S7COMM' for the first time"
```

```
#
#::::::::::::::::::::::::::::::::::::::::::::::

# without double slashes
# regex=(CyberLensApp):\sI, (\[\d+-\d\d-\d\d\S\d\d:\d\d:\d\d.\d+
#\d+]) (\D+) -- : (.*)\n?Source IP: (\d+.\d+.\d+.\d+)\n?(.*)
# with double slashes and newline
regex=(CyberLensApp):\\sI,
(\\[\\d+-\\d\\d-\\d\\d\\S\\d\\d:\\d\\d:\\d\\d.\\d+ #\\d+]) (\\D+) -- :
(.*)\\n?Source IP: (\\d+.\\d+.\\d+.\\d+)\\n?(.*)

token.count=6 token[0].name=Application
token[1].name=Message
token[2].name=Severity
token[3].name=Name
token[4].name=SourceIP
token[4].type=IPAddress
token[5].name=CatchAnyDoubledLines

event.name=Name
event.deviceProduct= stringConstant("CyberLens")
event.deviceVendor= stringConstant("DragosSecurity")
event.deviceSeverity=Severity
event.message=Message event.deviceProcessName=Application
event.deviceAddress=SourceIP
event.deviceCustomString1=CatchAnyDoubledLines

severity.map.veryhigh.if.deviceSeverity=1,2
severity.map.high.if.deviceSeverity=3,4
severity.map.medium.if.deviceSeverity=5,6
severity.map.low.if.deviceSeverity=INFO
```

2.21.1.4 ArcSight agent.properties File

1. Modify the agent.properties file settings as needed based on the example below:

   /opt/arcsight/connectors/<connector directory>/current/user/agent/agent.properties

2. Modify the **customsubagent** list as needed for the environment.

3. Replace the **IP address** to suit the environment.

```
#ArcSight Properties File

#Fri Mar 18 17:37:10 GMT 2016

agents.maxAgents=1

agents[0].aggregationcachesize=1000

agents[0].customsubagentlist=cyberlens.subagent.sdkrfilereader.propert
ies_syslog|cyberlensPREFIX.subagent.sdkrfilereader.properties_syslog|s
ourcefire_syslog|ciscovpnios_syslog|apache_syslog|ciscovpnnoios_syslog

|ciscorouter_syslog|pf_syslog|nagios_syslog|cef_syslog|ciscorouter_non
ios_syslog|catos_syslog|symantecnetworksecurity_syslog|snare_syslog|mc
afeesig_syslog|symantecendpointprotection_syslog|citrix_syslog|linux_a
uditd_syslog|vmwareesx_syslog|citrixnetscaler_syslog|vmwareesx_4_1_sys
log||pulseconnectsecure_syslog|pulseconnectsecure_keyvalue_syslog|flex
agent_syslog|generic_syslog

#agents[0].customsubagentlist=sourcefire_syslog|ciscorouter_syslog|pf_
syslog|cef_syslog|ciscorouter_nonios_syslog|catos_syslog|symantecnetwo
rksecurity_syslog|symantecendpointprotection_syslog|linux_auditd_syslo
g|vmwareesx_syslog|vmwareesx_4_1_syslog|flexagent_syslog|generic_syslo   g

agents[0].destination.count=1

agents[0].destination[0].agentid=3R9bQilMBABCIy6NStvvaDA\=\=

agents[0].destination[0].failover.count=0

agents[0].destination[0].params=<?xml version\="1.0" encoding\="UTF-
8"?>\n<ParameterValues>\n

<Parameter Name\="aupmaster" Value\="false"/>\n

<Parameter Name\="port" Value\="8443"/>\n

<Parameter Name\="fipsciphers" Value\="fipsDefault"/>\n

<Parameter Name\="host"

Value\="arcsight.es-sa-b1.test"/>\n

<Parameter Name\="filterevents"

Value\="false"/>\n</ParameterValues>\n

agents[0].destination[0].type=http

agents[0].deviceconnectionalertinterval=60000

agents[0].enabled=true

agents[0].entityid=0WbNilMBABCAAoBJrJmUOw\=\=

agents[0].fcp.version=0

agents[0].filequeuemaxfilecount=100

agents[0].filequeuemaxfilesize=10000000

agents[0].forwarder=false agents[0].forwardmode=true

agents[0].id=3R9bQilMBABCIy6NStvvaDA\=\=
agents[0].ipaddress=10.100.1.148

agents[0].overwriterawevent=false

agents[0].persistenceinterval=0

agents[0].port=514 agents[0].protocol=UDP

agents[0].rawloginterval=-1

agents[0].rawlogmaxsize=-1

agents[0].tcpbindretrytime=5000

agents[0].tcpbuffersize=10240

agents[0].tcpcleanupdelay=-1

agents[0].tcpmaxbuffersize=1048576

agents[0].tcpmaxidletime=-1

agents[0].tcpmaxsockets=1000

agents[0].tcppeerclosedchecktimeout=-1

agents[0].tcpsetsocketlinger=false

agents[0].tcpsleeptime=50

agents[0].type=syslog

agents[0].unparsedevents.log.enabled=true

agents[0].usecustomsubagentlist=true

agents[0].usefilequeue=true

remote.management.ssl.organizational.unit=HzjHilMBABCAAWiR1ATijw
```

2.21.1.5 Map File

1. Create a file containing the text below, and copy this file to **/opt/arcsight/<connector directory>/current/user/agent/map/map.1.properties**

   Note: *If an existing* map.1.properties *file exists, increment the suffix as needed (e.g.,* map.2.properties*).*

   ```
   !Flags,CaseSens-,Overwrite
   regex.event.name,set.event.deviceVendor,set.event.deviceProduct

   .*Cyberlens.*,DragosSecurity,CyberLens
   ```

2.21.1.6 Categorization File

1. Create a .csv file containing the text below, and copy this file to **/opt/arcsight/<connector directory>/current/user/agent/acp/categorizer/current/<deviceproduct>/deviceproduct.csv**

event.deviceProduct	set.event.categoryObject	set.event.categoryBehavior	set.event.categoryTechnique	set.event.categoryDeviceGroup	set.event.categorySignificance	set.event.categoryOutcome

CyberLens	/Host	/Found	/Traffic Anomaly	/IDS/Network	/Informational	/attempt

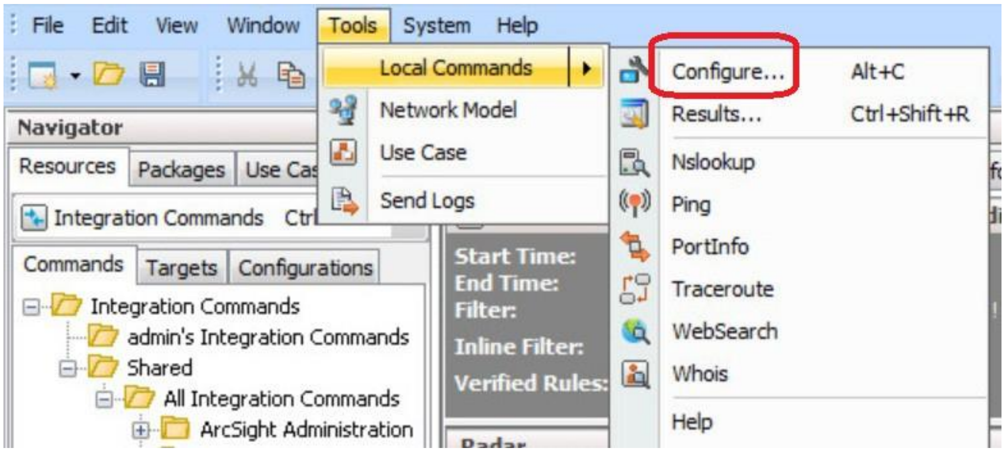
2.21.2 ICS2 OnGuard

2.21.2.1 Integration Setup

This will allow a user to right-click on a URL in an event to spawn OnGuard with the URL passed as a parameter.

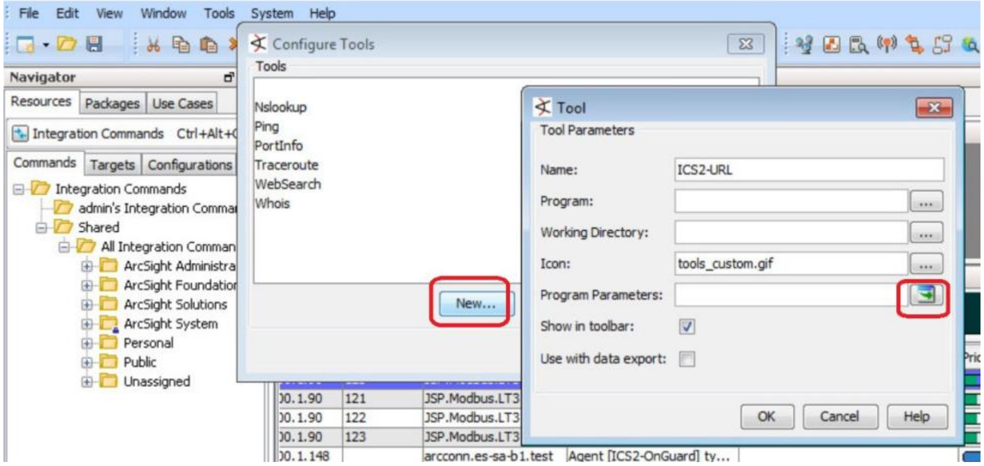
1. Select **Tools > Local Commands > Configure.**

Figure 2-84 ArcSight Configure



2. In the **name** field, type I**CS2-URL,** then select the **Program Parameters** browse button.

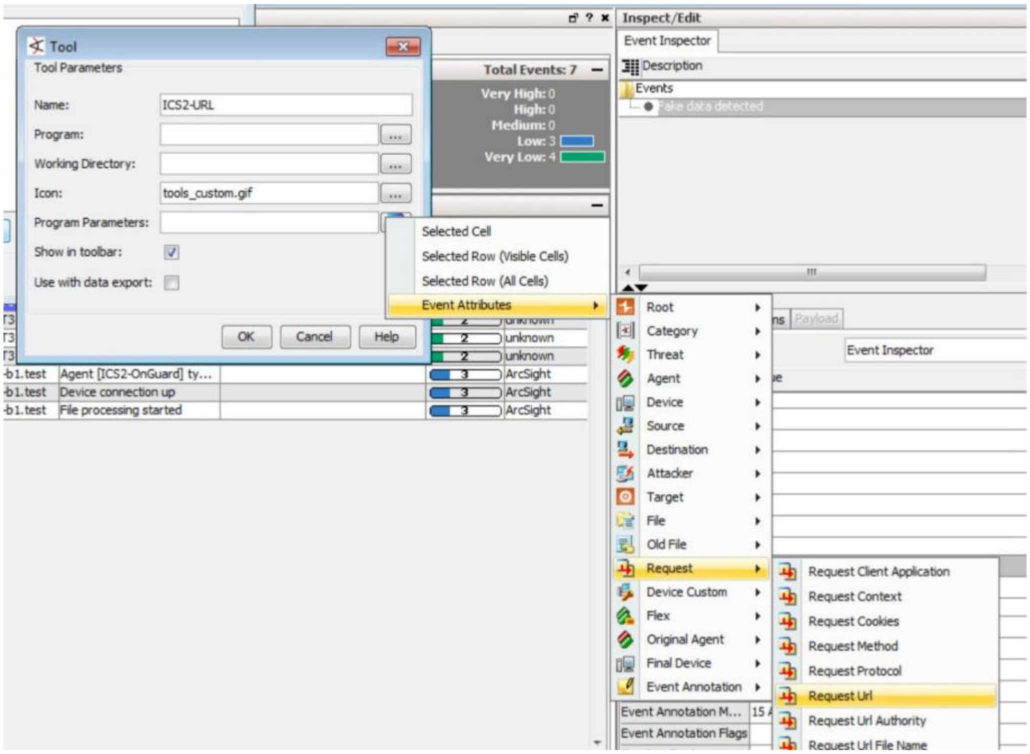
Figure 2-85 Program Parameters Setup



Name: ICS2-URL
Program:
Working Directory:
Icon: tools_custom.gif
Program Parameters:
Show in toolbar: ☑
Use with data export: □

3. Select **Event Attributes > Request > Request URL**.

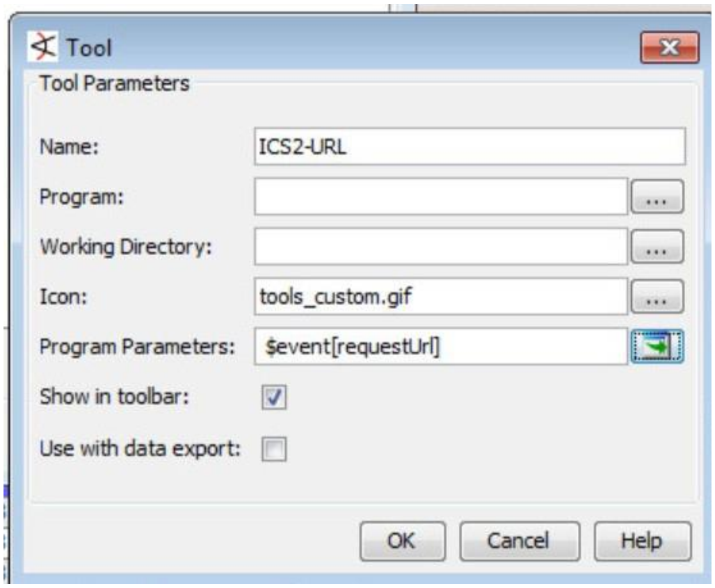
Figure 2-86 Request URL Configuration



Name: ICS2-URL
Program:
Working Directory:
Icon: tools_custom.gif
Program Parameters:
Show in toolbar: ☑
Use with data export: □

4. Select **OK.**

Figure 2-87 Tool URL Verification



Tool Parameters

Name: ICS2-URL

Program:

Working Directory:

Icon: tools_custom.gif

Program Parameters: $event[requestUrl]

Show in toolbar: ☑

Use with data export: □

5. Right-click on a **URL** in an event, select **Tools,** and verify that the **ICS2-URL tool** appears in the menu.

2.21.2.2 Install/Configure Custom ArcSight FlexConnector

1. Follow ArcSight's instructions for installing a Linux-based syslog SmartConnector.

2. Copy the custom FlexConnector configuration files to the appropriate locations.

    a. See Sections 6-8 of cyberlens-syslog-configuration-v2_3.docx.

3. Start the Connector service:

```
/etc/init.d/arc_[connectorName] start
```

2.21.2.3 Custom Parser — ArcSight FlexConnector Parser

1. Create a file containing the text below, and copy the file to **/opt/arcsight/connectors/[connector-directory]/current/user/agent/flexagent/onguard.s dkrfilereader.properties**

```
#::::::::::::::::::::::::::::::::::::::::::::::
# Syslog custom regex properties file
# for ICS^2 OnGuard CEF syslog
```

```
delimiter=| text.qualifier="
comments.start.with=\#
trim.tokens=true
contains.empty.tokens=true


token.count=8


token[0].name=Token0 token[0].type=String
token[1].name=Token1 token[1].type=String
token[2].name=Token2 token[2].type=Integer
token[3].name=Token3 token[3].type=String
token[4].name=Token4 token[4].type=String
token[5].name=Token5
token[5].type=TimeStamp
token[5].format=yyyy-MM-dd HH\:mm\:ssz
token[6].name=Token6
token[6].type=TimeStamp
token[6].format=yyyy-MM-dd HH\:mm\:ssz
token[7].name=Token7 token[7].type=String
# mappings
event.deviceCustomString1=Token0
event.deviceHostName=Token1
event.externalId=Token2
event.name=Token3 event.message=Token4
event.startTime=Token5
event.endTime=Token6
event.requestUrl=Token7
event.deviceVendor= stringConstant("ICS2")
event.deviceProduct= stringConstant("OnGuard")


#severity.map.veryhigh.if.deviceSeverity=1,2
severity.map.high.if.deviceSeverity=HIGH
severity.map.medium.if.deviceSeverity=MEDIUM
severity.map.low.if.deviceSeverity=LOW
severity.map.verylow.if.deviceSeverity=INFO
```

2.21.2.4 ArcSight agent.properties File

Example, from the following directory: **/opt/arcsight/connectors/[connector directory]/current/user/agent/agent.properties**

```
#ArcSight Properties File

#Fri Apr 08 22:28:12 BST 2016

agents.maxAgents=1

agents[0].AgentSequenceNumber=0

agents[0].configfile=onguard

agents[0].destination.count=1

agents[0].destination[0].agentid=3dfzD91MBABDtvfjvZeFjZw\=\=

agents[0].destination[0].failover.count=0

agents[0].destination[0].params=<?xml version\="1.0"

encoding\="UTF-8"?>\n<ParameterValues>\n      <Parameter Name\="host"

Value\="arcsight.es-sa-b1.test"/>\n     <Parameter Name\="aupmaster"

Value\="false"/>\n  <Parameter Name\="filterevents"
Value\="false"/>\n<Parameter

Name\="port" Value\="8443"/>\n

<Parameter Name\="fipsciphers"

Value\="fipsDefault"/>\n</ParameterValues>\n

agents[0].destination[0].type=http

agents[0].deviceconnectionalertinterval=60000

agents[0].enabled=true

agents[0].entityid=3dfzD91MBABDtvfjvZeFjZw\=\=

agents[0].extractfieldnames=

agents[0].extractregex=

agents[0].extractsource=File Name

agents[0].fcp.version=0

agents[0].fixedlinelength=-1

agents[0].followexternalrotation=true

agents[0].id=3dfzD91MBABDtvfjvZeFjZw\=\=

agents[0].internalevent.filecount.duration=-1

agents[0].internalevent.filecount.enable=false

agents[0].internalevent.filecount.minfilecount=-1

agents[0].internalevent.filecount.timer.delay=60

agents[0].internalevent.fileend.enable=true
```

```
agents[0].internalevent.filestart.enable=true

agents[0].logfilename=/opt/arcsight/connectors/syslogfiledata/OnGuardS
yslogExample.txt

agents[0].maxfilesize=-1

agents[0].onrotation=RenameFileInTheSameDirectory

agents[0].onrotationoptions=processed

agents[0].persistenceinterval=0

agents[0].preservedstatecount=10

agents[0].preservedstateinterval=30000

agents[0].preservestate=false

agents[0].roationonlywheneventexists=false

agents[0].rotationdelay=30

agents[0].rotationscheme=None

agents[0].rotationsleeptime=10

agents[0].startatend=false

agents[0].type=sdkfilereader

agents[0].unparsedevents.log.enabled=true

agents[0].usealternaterotationdetection=false

agents[0].usefieldextractor=false

agents[0].usenonlockingwindowsfilereader=false

remote.management.second.listener.port=10051

remote.management.ssl.organizational.unit=vRTB91MBABCAASNGV81kQQ

server.base.url=https\://arcsight.es-sa-b1.test\:8443

server.registration.host=arcsight.es-sa-b1.test
```

2.21.2.5 *Additional Configuration Files*

2.21.2.5.1 Map File

Create a file containing the text below, and copy this file to **/opt/arcsight/connector directory]/current/user/agent/map/map.1.properties**

> Note: *If an existing map.1.properties file exists, increment the suffix as needed (e.g.,* map.2.properties*).*

```
!Flags,CaseSens-,Overwrite
regex.event.name,set.event.deviceVendor,set.event.deviceProduct

.*On-Guard.*,ICS2,OnGuard

.*OnGuard.*,ICS2,OnGuard
```

2.21.2.5.2 Categorization File

Create a .csv file containing the text below, and copy this file to **/opt/arcsight/connector directory]/current/user/agent/acp/categorizer/current/[deviceproduct]/ deviceproduct.csv**

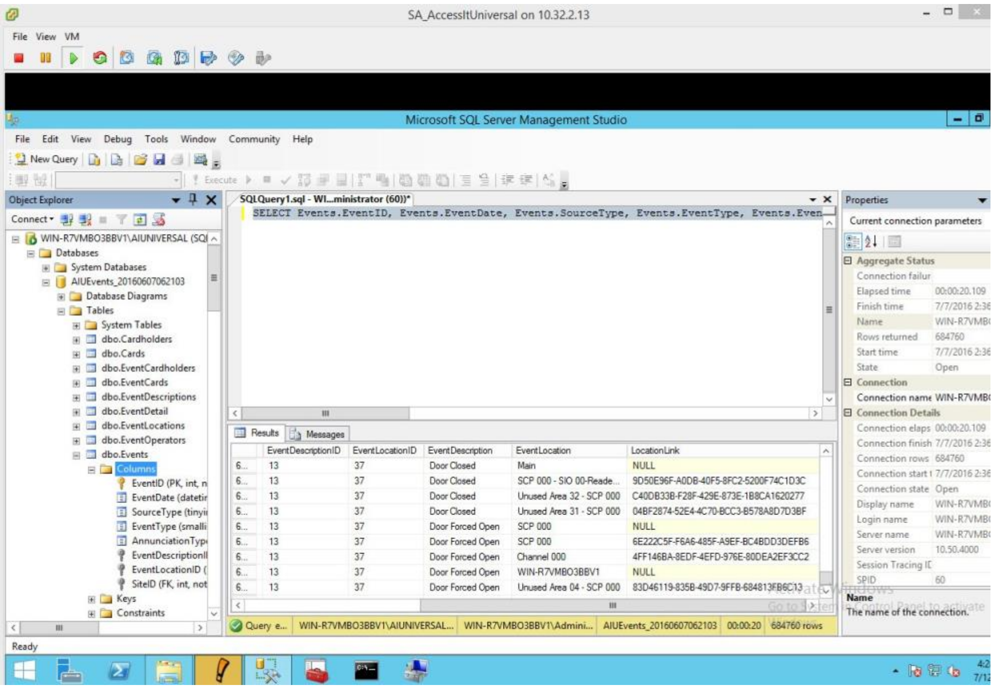
event. device Product	set.event. category Object	set.event. category Behavior	set.event. category Technique	set.event. category DeviceGroup	set.event. category Significance	set.event. category Outcome
OnGuard	/Host	/Found	/Traffic Anomaly	/IDS/Network	/Informational	/Attempt

2.21.3 RS2 Access It! Universal.NET

2.21.3.1 Review Data Source

1. Review the relevant fields in Access It!'s Microsoft SQL Server Management Studio.

Figure 2-88 Access It! SQL Table



```
SELECT Events.EventID, Events.EventDate, Events.SourceType, Events.EventType, Events.Even
```

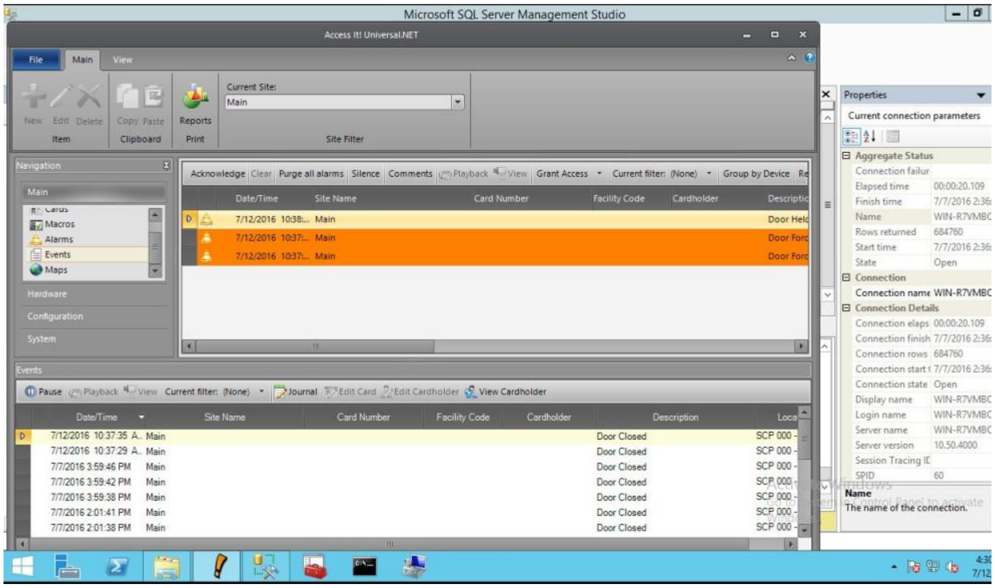
	EventDescriptionID	EventLocationID	EventDescription	EventLocation	LocationLink
6...	13	37	Door Closed	Main	NULL
6...	13	37	Door Closed	SCP 000 - SIO 00-Reade...	9D50E96F-A0DB-40F5-8FC2-5200F74C1D3C
6...	13	37	Door Closed	Unused Area 32 - SCP 000	C40DB33B-F28F-429E-873E-1B8CA1620277
6...	13	37	Door Closed	Unused Area 31 - SCP 000	04BF2874-52E4-4C70-BCC3-B578A8D7D3BF
6...	13	37	Door Forced Open	SCP 000	NULL
6...	13	37	Door Forced Open	SCP 000	6E222C5F-F6A6-485F-A9EF-BC4BDD3DEFB6
6...	13	37	Door Forced Open	Channel 000	4FF146BA-8EDF-4EFD-976E-80DEA2EF3CC2
6...	13	37	Door Forced Open	WIN-R7VMBO3BBV1	NULL
6...	13	37	Door Forced Open	Unused Area 04 - SCP 000	83D46119-835B-49D7-9FFB-684813FB6C13

Query e... | WIN-R7VMBO3BBV1\AIUNIVERSAL... | WIN-R7VMBO3BBV1\Admini... | AIUEvents_20160607062103 | 00:00:20 | 684760 rows

Aggregate Status	
Connection failur	
Elapsed time	00:00:20.109
Finish time	7/7/2016 2:36
Name	WIN-R7VMB(
Rows returned	684760
Start time	7/7/2016 2:36
State	Open
Connection	
Connection name	WIN-R7VMB(
Connection Details	
Connection elaps	00:00:20.109
Connection finish	7/7/2016 2:36
Connection rows	684760
Connection start t	7/7/2016 2:36
Connection state	Open
Display name	WIN-R7VMB(
Login name	WIN-R7VMB(
Server name	WIN-R7VMB(
Server version	10.50.4000
Session Tracing ID	
SPID	60

2. Review the data in RS2's Access It! application.

Figure 2-89 Access It! Application Window



Current Site: Main

Current filter: (None)

Date/Time	Site Name	Card Number	Facility Code	Cardholder	Descriptic
7/12/2016 10:38:...	Main				Door Held
7/12/2016 10:37:...	Main				Door Forc
7/12/2016 10:37:...	Main				Door Forc

Current filter: (None)

Date/Time	Site Name	Card Number	Facility Code	Cardholder	Description	Loca
7/12/2016 10:37:35 A..	Main				Door Closed	SCP 000 -
7/12/2016 10:37:29 A..	Main				Door Closed	SCP 000 -
7/7/2016 3:59:46 PM	Main				Door Closed	SCP 000 -
7/7/2016 3:59:42 PM	Main				Door Closed	SCP 000 -
7/7/2016 3:59:38 PM	Main				Door Closed	SCP 000 -
7/7/2016 2:01:41 PM	Main				Door Closed	SCP 000 -
7/7/2016 2:01:38 PM	Main				Door Closed	SCP 000 -

Aggregate Status	
Connection failur	
Elapsed time	00:00:20.109
Finish time	7/7/2016 2:36
Name	WIN-R7VMBC
Rows returned	684760
Start time	7/7/2016 2:36
State	Open
Connection	
Connection name	WIN-R7VMBC
Connection Details	
Connection elaps	00:00:20.109
Connection finish	7/7/2016 2:36
Connection rows	684760
Connection start t	7/7/2016 2:36
Connection state	Open
Display name	WIN-R7VMBC
Login name	WIN-R7VMBC
Server name	WIN-R7VMBC
Server version	10.50.4000
Session Tracing ID	
SPID	60

Name
The name of the connection.

2.21.3.2 Install/Configure Custom ArcSight FlexConnector

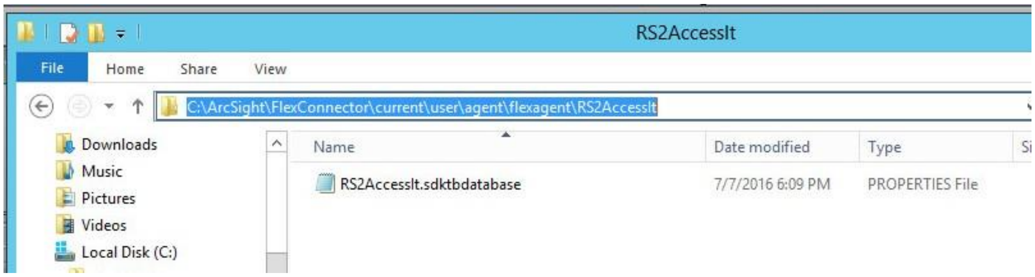
1. On the Access It! server, follow ArcSight's instructions for installing a Microsoft Windows-based Flex Connector, and specify the **Time Based Database** option [1].
2. Copy the custom FlexConnector configuration files to the appropriate locations. See Sections 6-8 of cyberlens-syslog-configuration-v2_3.docx.
3. Start the Connector service via the **Windows Administrative Tools > Services** control panel item.

2.21.3.3 Custom Parser — ArcSight FlexConnector Parser

This parser will allow ArcSight to query the RS2 Access It! SQL database for door controller event data.

1. Create a file containing the text below, and copy this file to the connector installation directory.
2. Example location: **C:\ArcSight\FlexConnector\user\agent\flexagent\RS2AccessIt**

Figure 2-90 Example Location



C:\ArcSight\FlexConnector\current\user\agent\flexagent\RS2AccessIt

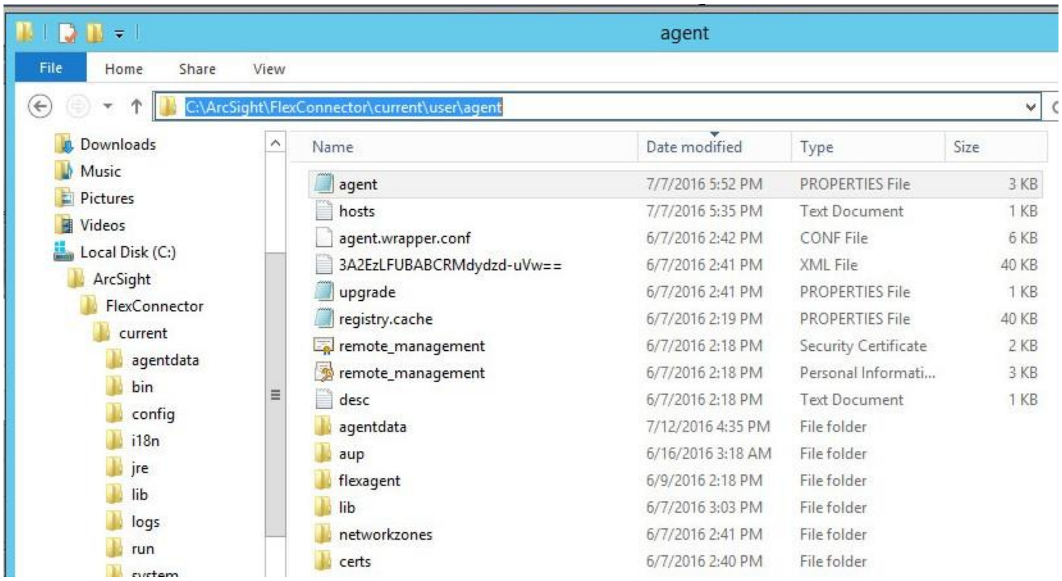
Name	Date modified	Type
RS2AccessIt.sdktbdatabase	7/7/2016 6:09 PM	PROPERTIES File

```
# Flex Connector for RS2 AccessIt Door Controller MS SQL Database
version.id=1.0

version.order=0

version.query=SELECT Max(EventDate) FROM Events


# Pull events from which time period lastdate.query=SELECT
Max(EventDate) FROM Events


additionaldata.enabled=true


# Database Query

query= SELECT Events.EventID, Events.EventDate, Events.SourceType,
Events.EventType, Events.EventDescriptionID, Events.EventLocationID,
EventDescriptions.EventDescription \

    FROM Events \

    LEFT OUTER JOIN EventDescriptions ON Events.EventDescriptionID =
    EventDescriptions.EventDescriptionID \

    WHERE Events.EventDate > ? \ ORDER
    BY Events.EventDate


# gets all the day's events once, and no new events

#timestamp.field=Events.EventDate

# gets events every time a new event occurs timestamp.field=EventDate
uniqueid.fields=EventDescription,EventLocation,LocationLink


# DB Column Mapping

event.deviceEventClassId= concatenate(EventDescription,":",EventID)

event.externalId=EventID
event.endTime=EventDate
event.name=EventDescription
#event.message=EventLocation
event.deviceCustomString1=SourceType
event.deviceCustomString2=EventType
event.deviceCustomString3=EventDescriptionID
event.deviceCustomString4=EventLocationID
#event.deviceCustomString5=LocationLink

# Constants Mapping
event.deviceVendor=  stringConstant(RS2) event.deviceProduct=
stringConstant(AccessIt) event.deviceCustomString1Label=
stringConstant(SourceType) event.deviceCustomString2Label=
stringConstant(EventType)
event.deviceCustomString3Label= stringConstant(EventDescriptionID)
event.deviceCustomString4Label= stringConstant(EventLocationID)
#event.deviceCustomString5Label= stringConstant(LocationLink)

# Severity Mapping event.deviceSeverity=EventDescription
severity.map.veryhigh.if.deviceSeverity=Door Forced Open,Door Held Open
severity.map.high.if.deviceSeverity=Power Loss,Comm Fail,Shutdown
severity.map.medium.if.deviceSeverity=Door Closed,Door Open,Startup
#severity.map.low.if.deviceSeverity=Low
```

2.21.3.4 ArcSight agent.properties File

1. Modify the **agent.properties** file settings as needed based on the example below.
2. Replace the Database connection **string/url** (in bold below) to suit the environment (refer to section above).

Figure 2-91 Example String/URL



C:\ArcSight\FlexConnector\current\user\agent

Name	Date modified	Type	Size
agent	7/7/2016 5:52 PM	PROPERTIES File	3 KB
hosts	7/7/2016 5:35 PM	Text Document	1 KB
agent.wrapper.conf	6/7/2016 2:42 PM	CONF File	6 KB
3A2EzLFUBABCRMdydzd-uVw==	6/7/2016 2:41 PM	XML File	40 KB
upgrade	6/7/2016 2:41 PM	PROPERTIES File	1 KB
registry.cache	6/7/2016 2:19 PM	PROPERTIES File	40 KB
remote_management	6/7/2016 2:18 PM	Security Certificate	2 KB
remote_management	6/7/2016 2:18 PM	Personal Informati...	3 KB
desc	6/7/2016 2:18 PM	Text Document	1 KB
agentdata	7/12/2016 4:35 PM	File folder	
aup	6/16/2016 3:18 AM	File folder	
flexagent	6/9/2016 2:18 PM	File folder	
lib	6/7/2016 3:03 PM	File folder	
networkzones	6/7/2016 2:41 PM	File folder	
certs	6/7/2016 2:40 PM	File folder	

```
#ArcSight Properties File

#Thu Jul 28 17:02:44 EDT 2016

agents.maxAgents=1

agents[0].AgentSequenceNumber=0

agents[0].JDBCDriver=com.microsoft.sqlserver.jdbc.SQLServerDriver

agents[0].configfolder=RS2AccessIt

agents[0].database=Default

agents[0].dbcpcachestatements=false

agents[0].dbcpcheckouttimeout=600

agents[0].dbcpidletimeout=300

agents[0].dbcpmaxcheckout=-1

agents[0].dbcpmaxconn=5

agents[0].dbcpreap=300

agents[0].dbcprowprefetch=-1

agents[0].destination.count=1
```

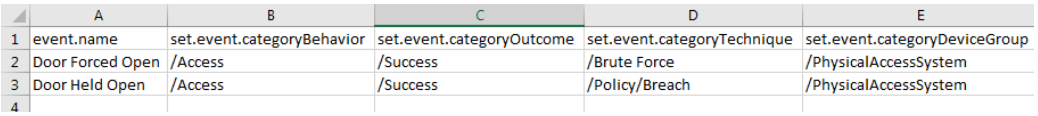
```
agents[0].destination[0].agentid=3B+tGM1YBABDj2XjY9XWuyg\=\=

agents[0].destination[0].failover.count=0

agents[0].destination[0].params=<?xml version\="1.0" encoding\="UTF-
8"?>\n<ParameterValues>\n

<Parameter Name\="aupmaster"

Value\="false"/>\n

<Parameter Name\="port"

Value\="8443"/>\n

<Parameter Name\="fipsciphers"

Value\="fipsDefault"/>\n

<Parameter Name\="host"

Value\="arcsight.es-sa-b1.test"/>\n

<Parameter Name\="filterevents"

Value\="false"/>\n</ParameterValues>\n

agents[0].destination[0].type=http

agents[0].deviceconnectionalertinterval=60000

agents[0].enabled=true

agents[0].entityid=YdZKM1YBABCAAwkPuy5kNg\=\=

agents[0].fcp.version=0 agents[0].frequency=45

agents[0].id=3B+tGM1YBABDj2XjY9XWuyg\=\=

agents[0].initretrysleeptime=60000

agents[0].jdbcquerytimeout=-1

agents[0].jdbctimeout=240000

agents[0].loopingenabled=false

agents[0].password=OBFUSCATE.4.8.1\:tN7+FHyJvO5qkdFrnyHeng\=\=

agents[0].passwordchangeingcharactersets=UPPERCASE\=ABCDEFGHIJKLMNOPQR
STUVWXYZ,LOWERCASE\=abcdefghijklmnopqrstuvwxyz,NUMBER\=01234567890,SPECIAL\=+-
\!@\#$%&*()

agents[0].passwordchangingcharactersetdelimiter=,

agents[0].passwordchangingenabled=false
```

```
agents[0].passwordchanginginterval=86400

agents[0].passwordchanginglength=16

agents[0].passwordchangingtemplate=UPPERCASE,NUMBER,SPECIAL,UPPERCASE|
LOWERCASE|NUMBER,UPPERCASE|LOWERCASE|NUMBER|SPECIAL

agents[0].persistenceinterval=1

agents[0].preservedstatecount=10

agents[0].preservedstateinterval=30000

agents[0].preservestate=true

agents[0].rotationtimeout=30000

agents[0].startatend=true

agents[0].type=sdktbdatabase

agents[0].unparsedevents.log.enabled=false

agents[0].url=jdbc\:sqlserver\://10.100.2.102\:1433;databasename\=AIUE
vents_20160607062103

agents[0].useconnectionpool=true

agents[0].user=OBFUSCATE.4.8.1\:LkwoJdKuWx8CDMiRZv4Qpg\=\=

remote.management.second.listener.port=10050

remote.management.ssl.organizational.unit=rE09M1YBABCAAQkPuy5kNg
```

2.21.3.5 Categorization File

1. Create a .csv file containing the fields below, and copy this file to the appropriate folder: **C:\ArcSight\<connector directory>\current\user\agent\acp\categorizer\current\rs2accessit\rs2accessit.csv**

Figure 2-92 Categorization File Fields



	A	B	C	D	E
1	event.name	set.event.categoryBehavior	set.event.categoryOutcome	set.event.categoryTechnique	set.event.categoryDeviceGroup
2	Door Forced Open	/Access	/Success	/Brute Force	/PhysicalAccessSystem
3	Door Held Open	/Access	/Success	/Policy/Breach	/PhysicalAccessSystem
4					

2.21.4 Additional References

1. HPE ArcSight SmartConnector User Guide https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-SmartConnector-User-Guide-7-12-0/ta-p/1586784

2. Syslog Guide https://community.microfocus.com/t5/ArcSight-Connectors/SmartConnector-for-Raw-Syslog-Daemon/ta-p/1589006

3. SmartConnector Quick Reference https://community.microfocus.com/t5/ArcSight-User-Discussions/SmartConnector-Quick-Reference/td-p/1598927

4. HPE ArcSight FlexConnector Developer's Guide https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-FlexConnector-Developer-s-Guide/ta-p/1584874

5. FlexConnector Quick Reference https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-FlexConnector-Developer-s-Guide/ta-p/1584874

3 Test Cases/Alert Configurations

This section shows filters used in ArcSight for the test cases as well as descriptions of test case alerts.

3.1 ArcSight Filters

The following sections describe the creation of filters and what filters were used in the build.

3.1.1 Filter Creation

ArcSight content is composed of many parts. A primary component in all content is the ArcSight filter. Use the following steps to create a filter:

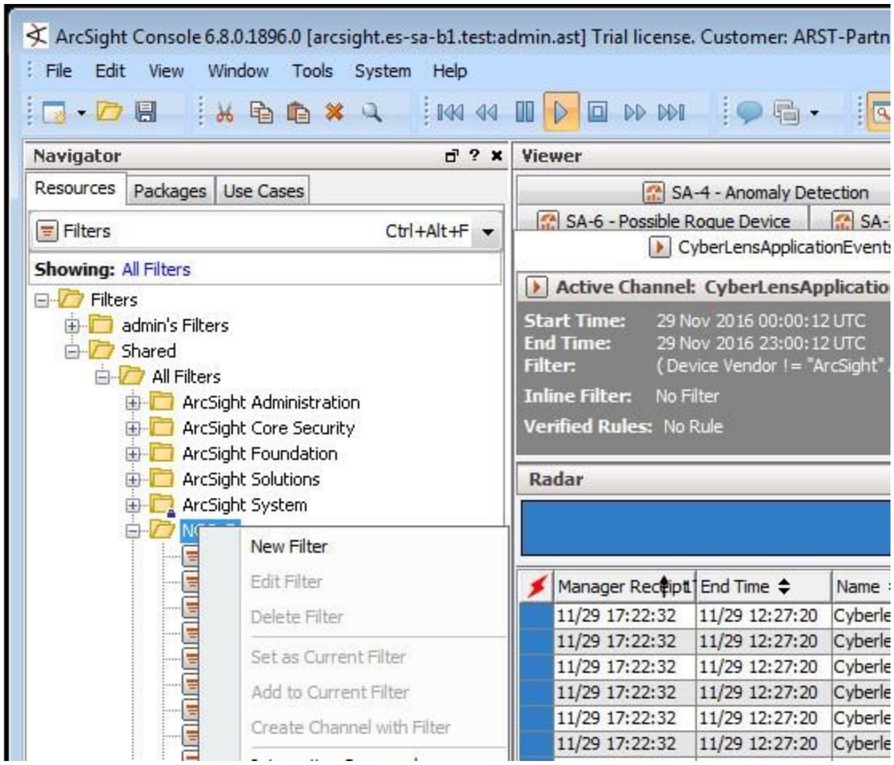
1. Go to the ArcSight navigation pane on the left.

2. Select **Filters** from the drop-down menu.

3. Right-click on a folder location.

4. Select **New Filter** from the pop-up menu.

Figure 3-1 Create New Filter



Showing: All Filters

Active Channel: CyberLensApplicatio

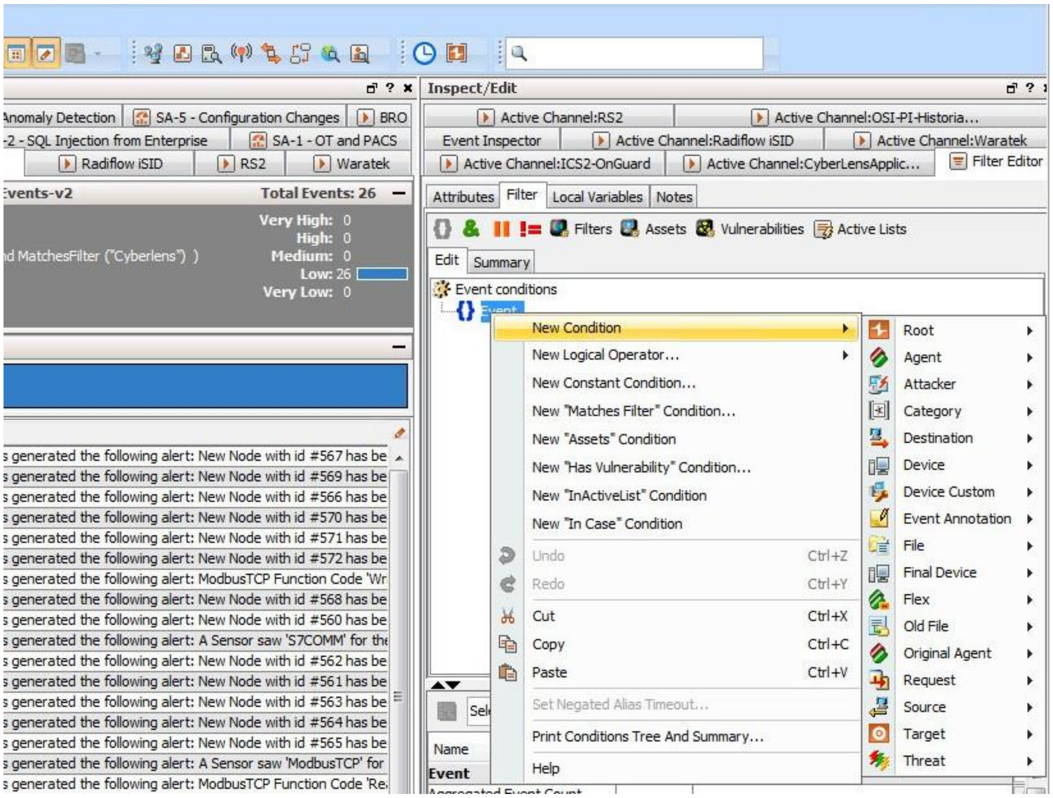
Start Time: 29 Nov 2016 00:00:12 UTC
End Time: 29 Nov 2016 23:00:12 UTC
Filter: (Device Vendor != "ArcSight"
Inline Filter: No Filter
Verified Rules: No Rule

Manager Receipt	End Time	Name
11/29 17:22:32	11/29 12:27:20	Cyberle
11/29 17:22:32	11/29 12:27:20	Cyberle
11/29 17:22:32	11/29 12:27:20	Cyberle
11/29 17:22:32	11/29 12:27:20	Cyberle
11/29 17:22:32	11/29 12:27:20	Cyberle
11/29 17:22:32	11/29 12:27:20	Cyberle

5. Right-click **Event** in the right pane of the Edit Window.

6. Select **New Condition** from the pop-up menu.

Figure 3-2 Create Conditions (Logic)



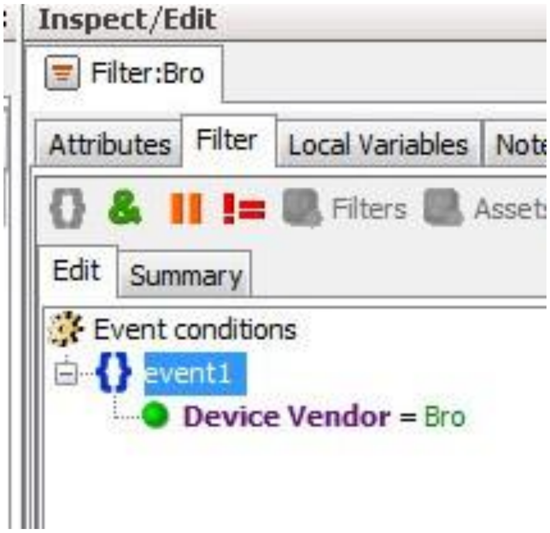
s generated the following alert: New Node with id #567 has be
s generated the following alert: New Node with id #569 has be
s generated the following alert: New Node with id #566 has be
s generated the following alert: New Node with id #570 has be
s generated the following alert: New Node with id #571 has be
s generated the following alert: New Node with id #572 has be
s generated the following alert: ModbusTCP Function Code 'Wr
s generated the following alert: New Node with id #568 has be
s generated the following alert: New Node with id #560 has be
s generated the following alert: A Sensor saw 'S7COMM' for the
s generated the following alert: New Node with id #562 has be
s generated the following alert: New Node with id #561 has be
s generated the following alert: New Node with id #563 has be
s generated the following alert: New Node with id #564 has be
s generated the following alert: New Node with id #565 has be
s generated the following alert: A Sensor saw 'ModbusTCP' for
s generated the following alert: ModbusTCP Function Code 'Re

7. Next, begin constructing the conditions for which to query the ArcSight database.

Note: *It is customary to create a central folder to house ArcSight content and allow it to be shared by groups of users. Once content (such as filters) has been tested, it can then be copied or moved to the group (shared) folder. Permissions can be set on the folder to control access as needed.*

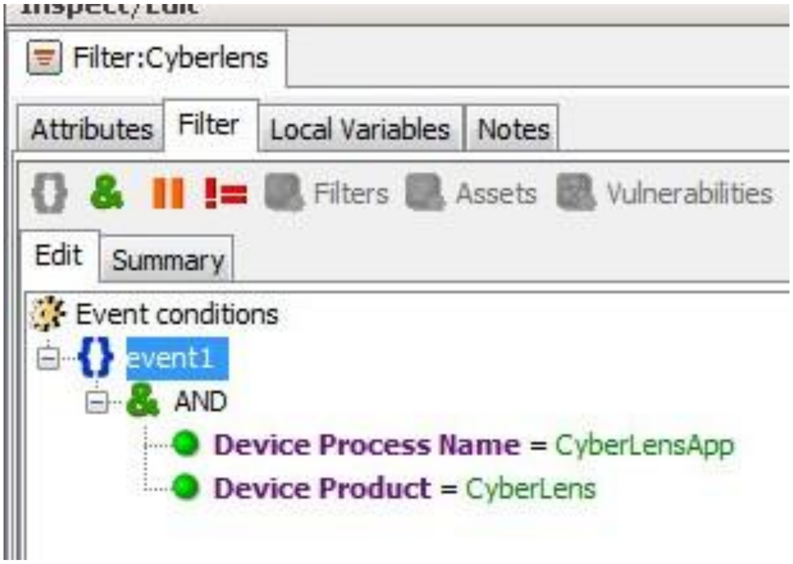
Shown below are ArcSight Filters that were created to support the Situational Awareness Test Cases.

Figure 3-3 Bro Filter



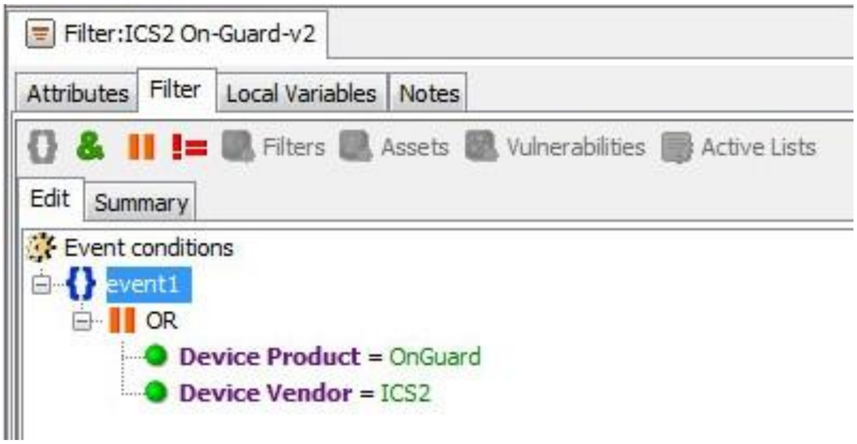
Event conditions
event1
Device Vendor = Bro

Figure 3-4 Dragos CyberLens Filter



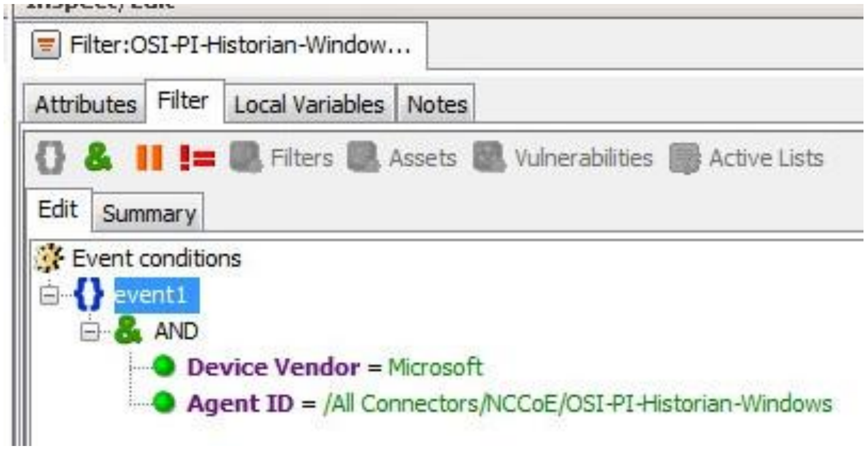
Event conditions
event1
AND
Device Process Name = CyberLensApp
Device Product = CyberLens

Figure 3-5 ICS2 On-Guard Filter



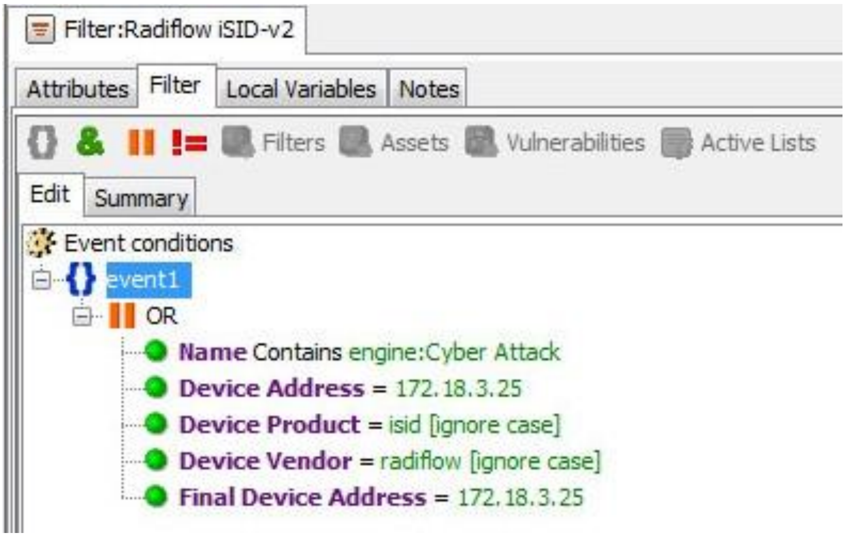
Event conditions
- event1
  - OR
    - Device Product = OnGuard
    - Device Vendor = ICS2

Figure 3-6 Windows Log Filter for OSI PI Historian



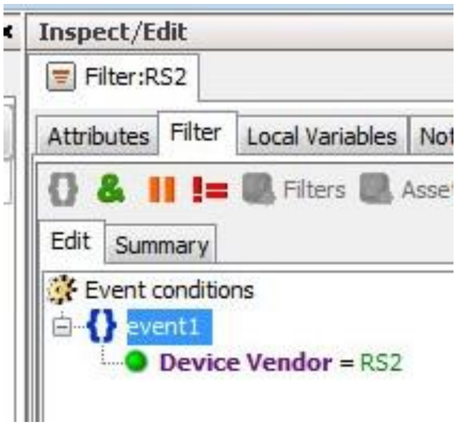
Event conditions
- event1
  - AND
    - Device Vendor = Microsoft
    - Agent ID = /All Connectors/NCCoE/OSI-PI-Historian-Windows

Figure 3-7 Radiflow iSID Filter



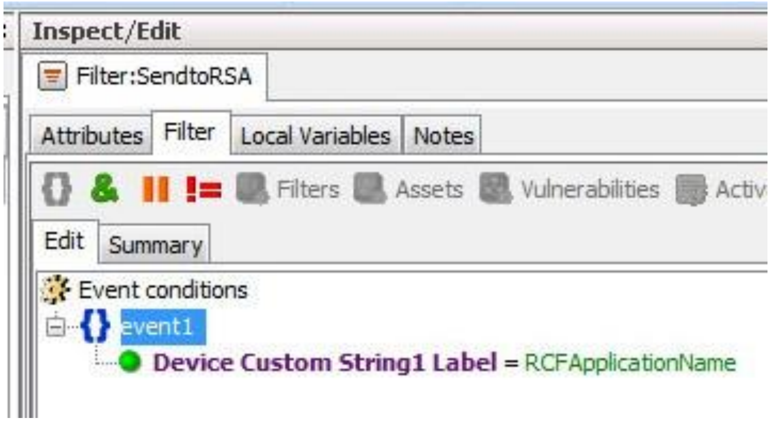
Event conditions
event1
OR
Name Contains engine:Cyber Attack
Device Address = 172.18.3.25
Device Product = isid [ignore case]
Device Vendor = radiflow [ignore case]
Final Device Address = 172.18.3.25

Figure 3-8 RS2 Access It! Filter



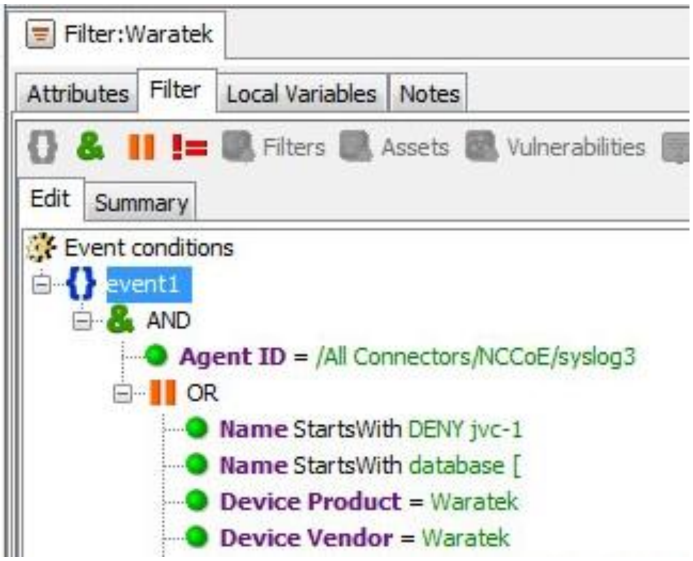
Event conditions
event1
Device Vendor = RS2

Figure 3-9 RSA Archer Filter



Event conditions
event1
Device Custom String1 Label = RCFApplicationName

Figure 3-10 Waratek Filter

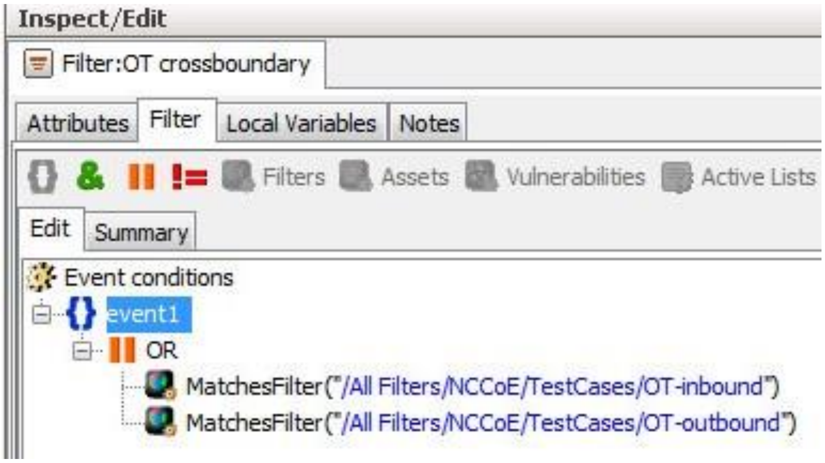


Event conditions
event1
AND
Agent ID = /All Connectors/NCCoE/syslog3
OR
Name StartsWith DENY jvc-1
Name StartsWith database [
Device Product = Waratek
Device Vendor = Waratek

Below are filters that were created to match against conditions based on …

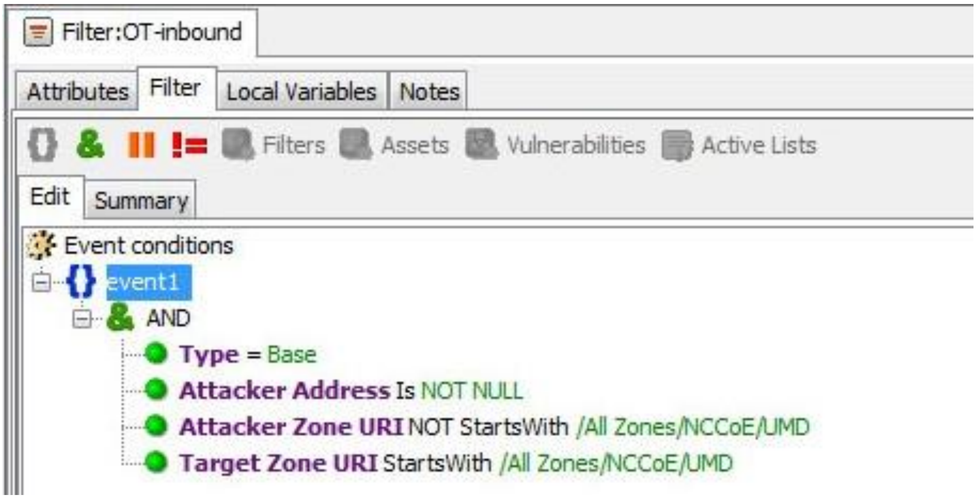
- direction of network activity
- awareness of Security Zones (OT versus non - OT)

Figure 3-11 OT Cross-Boundary Filter



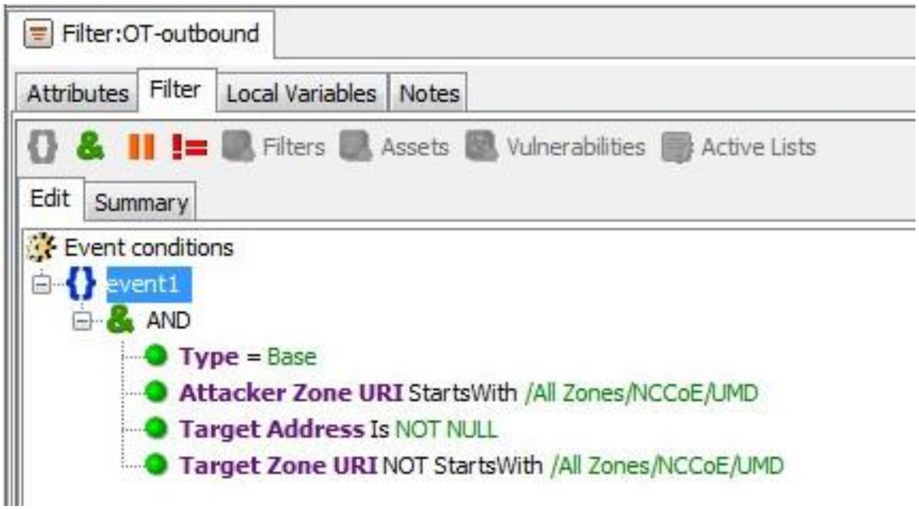
Event conditions
event1
OR
MatchesFilter("/All Filters/NCCoE/TestCases/OT-inbound")
MatchesFilter("/All Filters/NCCoE/TestCases/OT-outbound")

Figure 3-12 OT Inbound Filter



Event conditions
event1
AND
Type = Base
Attacker Address Is NOT NULL
Attacker Zone URI NOT StartsWith /All Zones/NCCoE/UMD
Target Zone URI StartsWith /All Zones/NCCoE/UMD

Figure 3-13 OT Outbound Filter

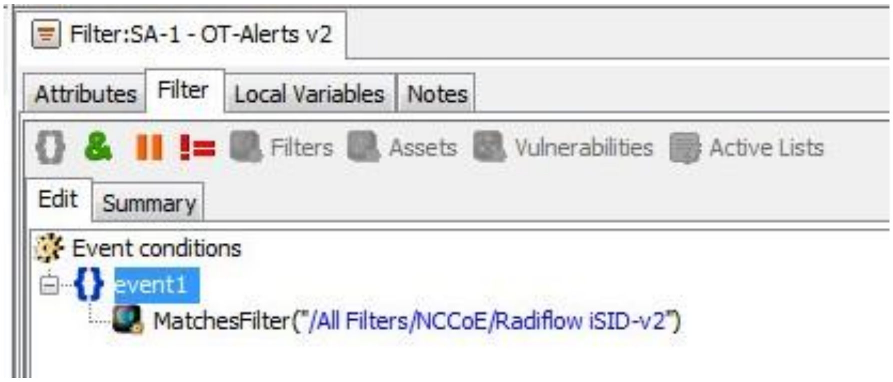


Event conditions
- event1
  - AND
    - Type = Base
    - Attacker Zone URI StartsWith /All Zones/NCCoE/UMD
    - Target Address Is NOT NULL
    - Target Zone URI NOT StartsWith /All Zones/NCCoE/UMD

3.1.2 ArcSight Test Cases

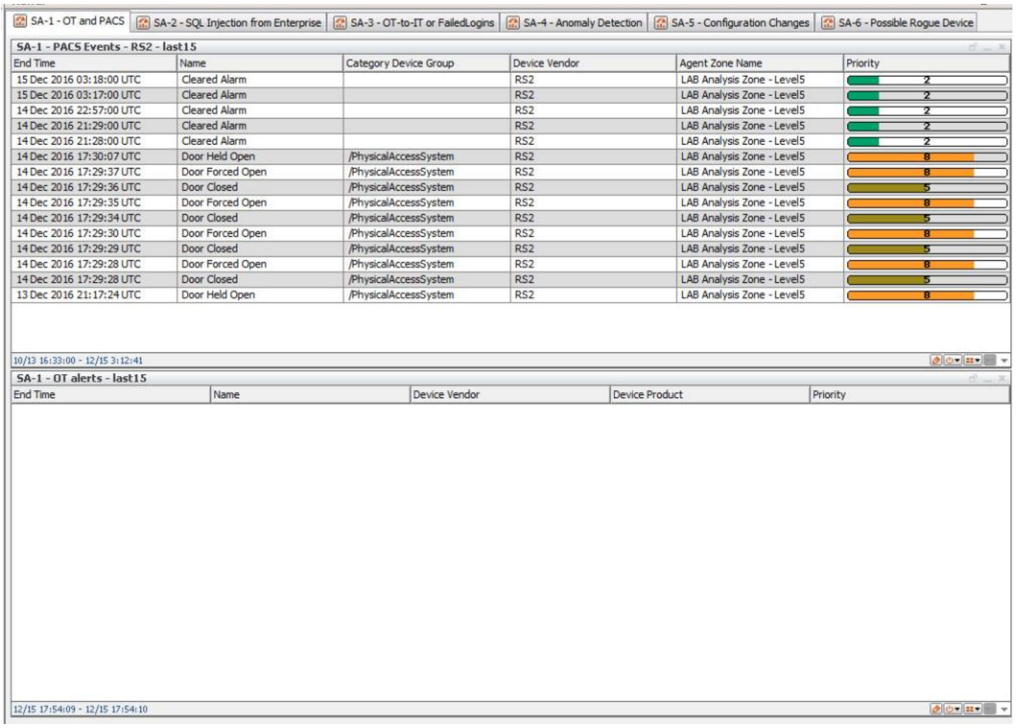
Shown below are additional filters that were built to support the SA Test Cases. Also shown are examples of Dashboards and Data Monitors that use these filters.

Figure 3-14 SA-1 - OT-Alerts Filter



Event conditions
- event1
  - MatchesFilter("/All Filters/NCCoE/Radiflow iSID-v2")

Figure 3-15 SA-1 - OT and PACS Dashboard


SA-1 - OT and PACS
SA-2 - SQL Injection from Enterprise
SA-3 - OT-to-IT or FailedLogins
SA-4 - Anomaly Detection
SA-5 - Configuration Changes
SA-6 - Possible Rogue Device

SA-1 - PACS Events - RS2 - last15

End Time	Name	Category Device Group	Device Vendor	Agent Zone Name	Priority
15 Dec 2016 03:18:00 UTC	Cleared Alarm		RS2	LAB Analysis Zone - Level5	2
15 Dec 2016 03:17:00 UTC	Cleared Alarm		RS2	LAB Analysis Zone - Level5	2
14 Dec 2016 22:57:00 UTC	Cleared Alarm		RS2	LAB Analysis Zone - Level5	2
14 Dec 2016 21:29:00 UTC	Cleared Alarm		RS2	LAB Analysis Zone - Level5	2
14 Dec 2016 21:28:00 UTC	Cleared Alarm		RS2	LAB Analysis Zone - Level5	2
14 Dec 2016 17:30:07 UTC	Door Held Open	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	8
14 Dec 2016 17:29:37 UTC	Door Forced Open	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	8
14 Dec 2016 17:29:36 UTC	Door Closed	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	5
14 Dec 2016 17:29:35 UTC	Door Forced Open	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	8
14 Dec 2016 17:29:34 UTC	Door Closed	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	5
14 Dec 2016 17:29:30 UTC	Door Forced Open	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	8
14 Dec 2016 17:29:29 UTC	Door Closed	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	5
14 Dec 2016 17:29:28 UTC	Door Forced Open	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	8
14 Dec 2016 17:29:28 UTC	Door Closed	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	5
13 Dec 2016 21:17:24 UTC	Door Held Open	/PhysicalAccessSystem	RS2	LAB Analysis Zone - Level5	8

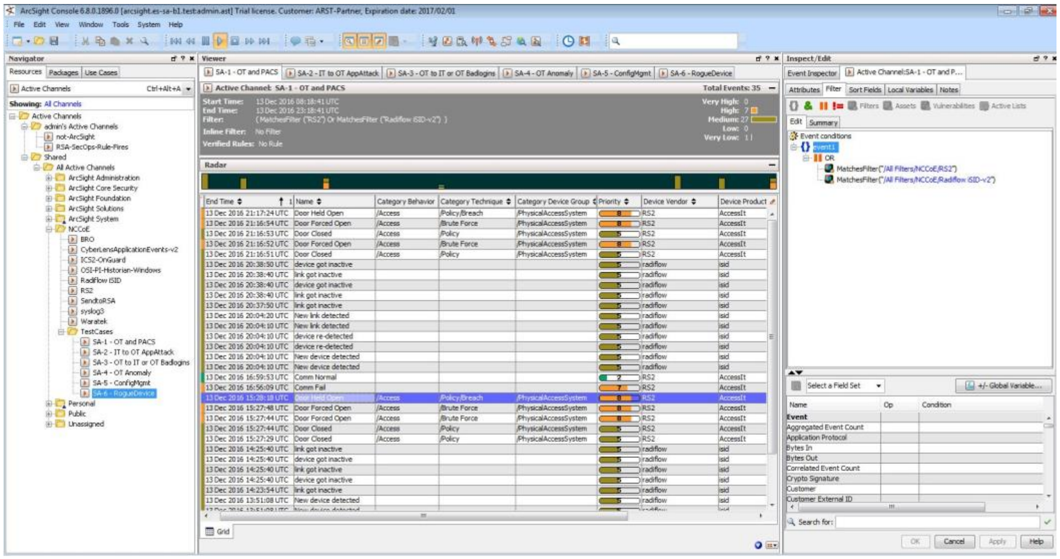
10/13 16:33:00 - 12/15 3:12:41

SA-1 - OT alerts - last15

End Time	Name	Device Vendor	Device Product	Priority

12/15 17:54:09 - 12/15 17:54:10

Figure 3-16 SA-1 OT and PACS Active Channel



Active Channel: SA-1 - OT and PACS Total Events: 35

Start Time: 13 Dec 2016 08:18:41 UTC
End Time: 13 Dec 2016 23:18:41 UTC
Filter: (MatchesFilter ("RS2") Or MatchesFilter ("Radiflow iSID-v2"))
Inline Filter: No Filter
Verified Rules: No Rule

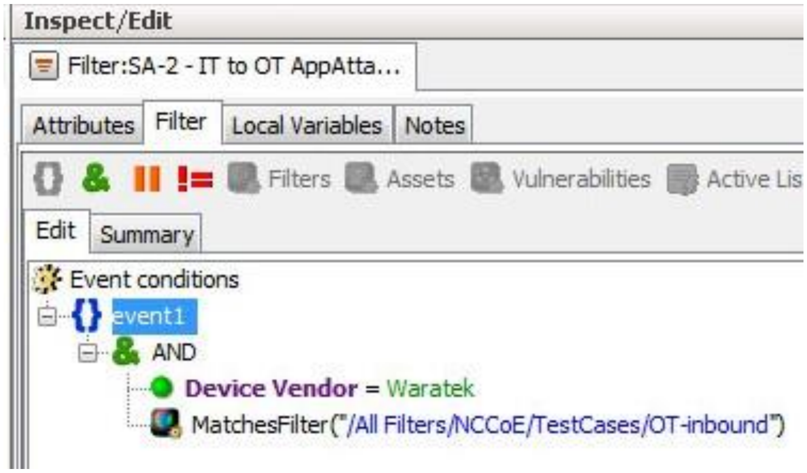
Very High: 0
High: 7
Medium: 27
Low: 0
Very Low: 1

End Time	Name	Category Behavior	Category Technique	Category Device Group	Priority	Device Vendor	Device Product
13 Dec 2016 21:17:24 UTC	Door Held Open	/Access	/Policy/Breach	/PhysicalAccessSystem	8	RS2	AccessIt
13 Dec 2016 21:16:54 UTC	Door Forced Open	/Access	/Brute Force	/PhysicalAccessSystem	8	RS2	AccessIt
13 Dec 2016 21:16:53 UTC	Door Closed	/Access	/Policy	/PhysicalAccessSystem	5	RS2	AccessIt
13 Dec 2016 21:16:52 UTC	Door Forced Open	/Access	/Brute Force	/PhysicalAccessSystem	8	RS2	AccessIt
13 Dec 2016 21:16:51 UTC	Door Closed	/Access	/Policy	/PhysicalAccessSystem	5	RS2	AccessIt
13 Dec 2016 20:38:50 UTC	device got inactive				5	radiflow	isid
13 Dec 2016 20:38:40 UTC	link got inactive				5	radiflow	isid
13 Dec 2016 20:38:40 UTC	device got inactive				5	radiflow	isid
13 Dec 2016 20:38:40 UTC	link got inactive				5	radiflow	isid
13 Dec 2016 20:37:50 UTC	link got inactive				5	radiflow	isid
13 Dec 2016 20:04:20 UTC	New link detected				5	radiflow	isid
13 Dec 2016 20:04:10 UTC	New link detected				5	radiflow	isid
13 Dec 2016 20:04:10 UTC	device re-detected				5	radiflow	isid
13 Dec 2016 20:04:10 UTC	device re-detected				5	radiflow	isid
13 Dec 2016 20:04:10 UTC	New device detected				5	radiflow	isid
13 Dec 2016 20:04:10 UTC	New device detected				5	radiflow	isid
13 Dec 2016 16:59:53 UTC	Comm Normal				2	RS2	AccessIt
13 Dec 2016 16:56:09 UTC	Comm Fail				7	RS2	AccessIt
13 Dec 2016 15:28:18 UTC	Door Held Open	/Access	/Policy/Breach	/PhysicalAccessSystem	8	RS2	AccessIt
13 Dec 2016 15:27:48 UTC	Door Forced Open	/Access	/Brute Force	/PhysicalAccessSystem	8	RS2	AccessIt
13 Dec 2016 15:27:44 UTC	Door Forced Open	/Access	/Brute Force	/PhysicalAccessSystem	8	RS2	AccessIt
13 Dec 2016 15:27:44 UTC	Door Closed	/Access	/Policy	/PhysicalAccessSystem	5	RS2	AccessIt
13 Dec 2016 15:27:29 UTC	Door Closed	/Access	/Policy	/PhysicalAccessSystem	5	RS2	AccessIt
13 Dec 2016 14:25:40 UTC	link got inactive				5	radiflow	isid
13 Dec 2016 14:25:40 UTC	device got inactive				5	radiflow	isid
13 Dec 2016 14:25:40 UTC	link got inactive				5	radiflow	isid
13 Dec 2016 14:25:40 UTC	device got inactive				5	radiflow	isid
13 Dec 2016 14:23:54 UTC	link got inactive				5	radiflow	isid
13 Dec 2016 13:51:08 UTC	New device detected				5	radiflow	isid

Event conditions
event1
OR
MatchesFilter("/All Filters/NCCoE/RS2")
MatchesFilter("/All Filters/NCCoE/Radiflow iSID-v2")

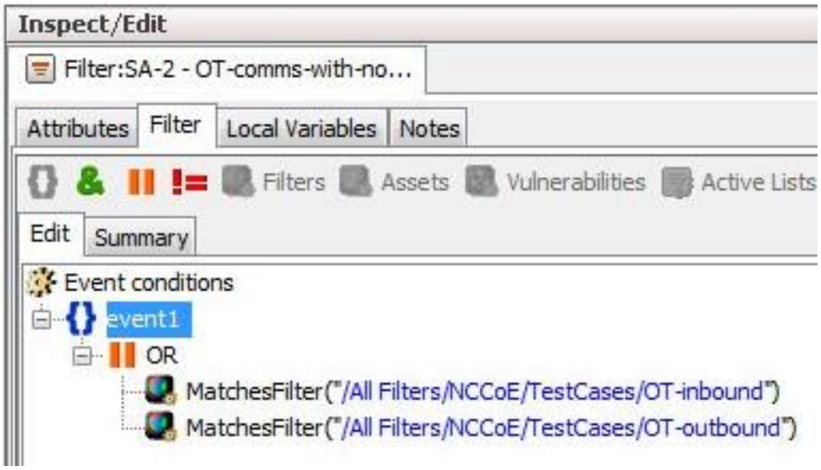
Name	Op	Condition
Event		
Aggregated Event Count		
Application Protocol		
Bytes In		
Bytes Out		
Correlated Event Count		
Crypto Signature		
Customer		
Customer External ID		

Figure 3-17 SA-2 - IT to OT AppAttack Filter



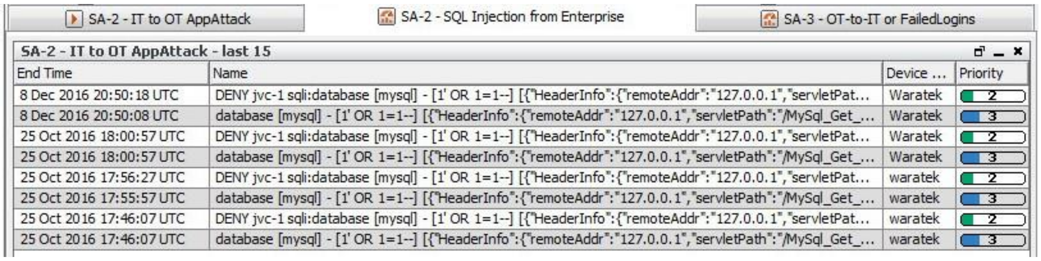
```
Event conditions
  event1
    AND
      Device Vendor = Waratek
      MatchesFilter("/All Filters/NCCoE/TestCases/OT-inbound")
```

Figure 3-18 SA-2 OT-comms-with-non-OT Filter



```
Event conditions
  event1
    OR
      MatchesFilter("/All Filters/NCCoE/TestCases/OT-inbound")
      MatchesFilter("/All Filters/NCCoE/TestCases/OT-outbound")
```

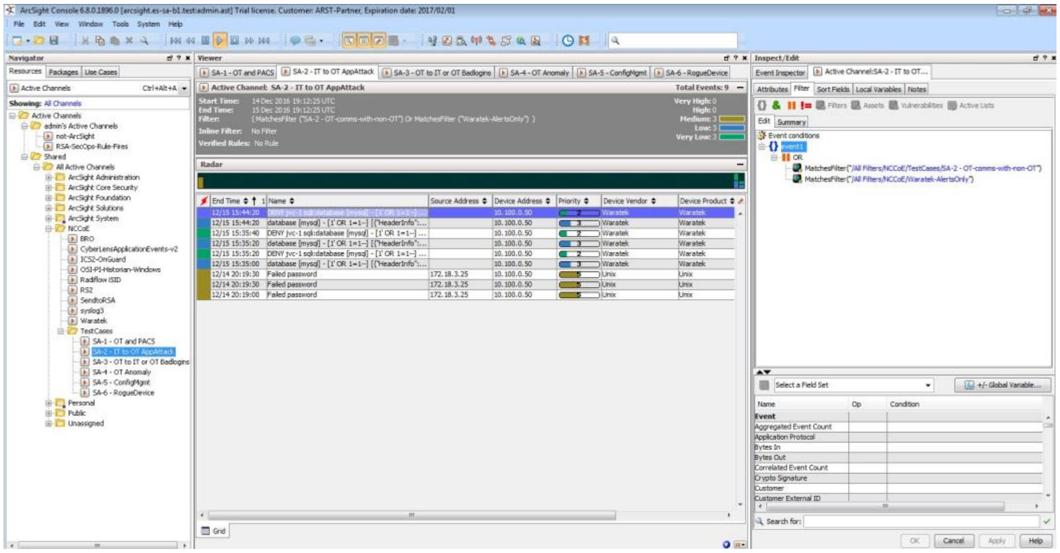
Figure 3-19 SA-2 SQL Injection Dashboard


SA-2 - IT to OT AppAttack
SA-2 - SQL Injection from Enterprise
SA-3 - OT-to-IT or FailedLogins

SA-2 - IT to OT AppAttack - last 15

End Time	Name	Device ...	Priority
8 Dec 2016 20:50:18 UTC	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat...	Waratek	2
8 Dec 2016 20:50:08 UTC	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySql_Get_...	Waratek	3
25 Oct 2016 18:00:57 UTC	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat...	Waratek	2
25 Oct 2016 18:00:57 UTC	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySql_Get_...	Waratek	3
25 Oct 2016 17:56:27 UTC	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat...	waratek	2
25 Oct 2016 17:55:57 UTC	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySql_Get_...	waratek	3
25 Oct 2016 17:46:07 UTC	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPat...	waratek	2
25 Oct 2016 17:46:07 UTC	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":{"remoteAddr":"127.0.0.1","servletPath":"/MySql_Get_...	waratek	3

Figure 3-20 SA-2 SQL Injection Active Channel



ArcSight Console 6.8.0.1896.0 [arcsight.es-sa-b1.test:admin.ast] Trial license. Customer: ARST-Partner, Expiration date: 2017/02/01

Active Channel: SA-2 - IT to OT AppAttack — Total Events: 9

Start Time: 14 Dec 2016 19:12:25 UTC
End Time: 15 Dec 2016 19:12:25 UTC
Filter: (MatchesFilter ("SA-2 - OT-comms-with-non-OT") Or MatchesFilter ("Waratek-AlertsOnly"))
Inline Filter: No Filter
Verified Rules: No Rule

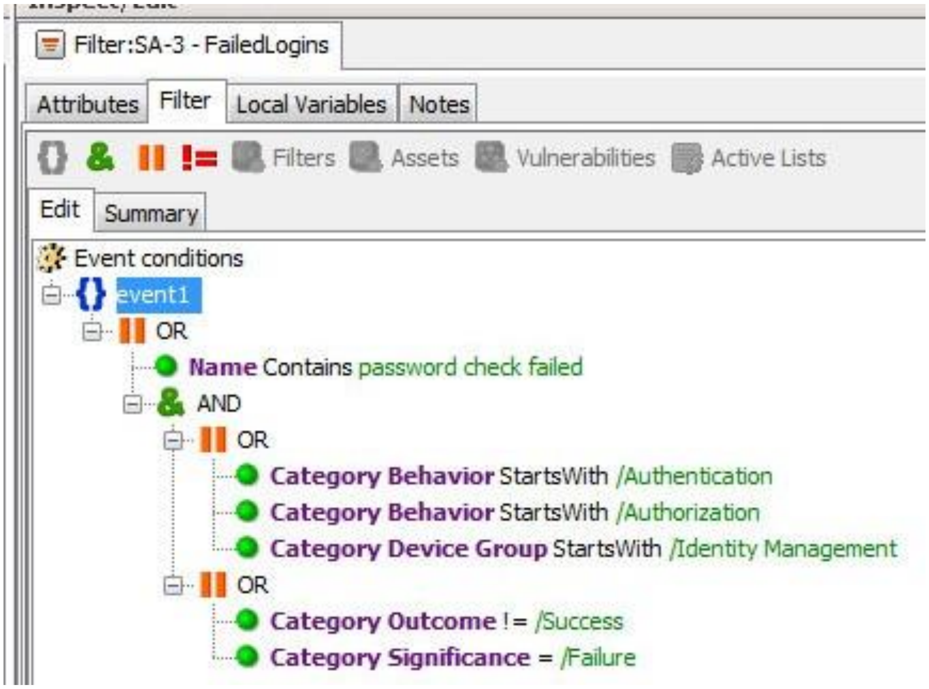
Very High: 0
High: 0
Medium: 3
Low: 3
Very Low: 3

End Time	Name	Source Address	Device Address	Priority	Device Vendor	Device Product
12/15 15:44:20	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] ...		10.100.0.50	2	Waratek	Waratek
12/15 15:44:20	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":...		10.100.0.50	3	Waratek	Waratek
12/15 15:35:40	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] ...		10.100.0.50	2	Waratek	Waratek
12/15 15:35:20	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":...		10.100.0.50	3	Waratek	Waratek
12/15 15:35:20	DENY jvc-1 sqli:database [mysql] - [1' OR 1=1--] ...		10.100.0.50	2	Waratek	Waratek
12/15 15:35:00	database [mysql] - [1' OR 1=1--] [{"HeaderInfo":...		10.100.0.50	3	Waratek	Waratek
12/14 20:19:30	Failed password	172.18.3.25	10.100.0.50	5	Unix	Unix
12/14 20:19:30	Failed password	172.18.3.25	10.100.0.50	5	Unix	Unix
12/14 20:19:00	Failed password	172.18.3.25	10.100.0.50	5	Unix	Unix

```
Event conditions
  event1
    OR
      MatchesFilter("/All Filters/NCCoE/TestCases/SA-2 - OT-comms-with-non-OT")
      MatchesFilter("/All Filters/NCCoE/Waratek-AlertsOnly")
```

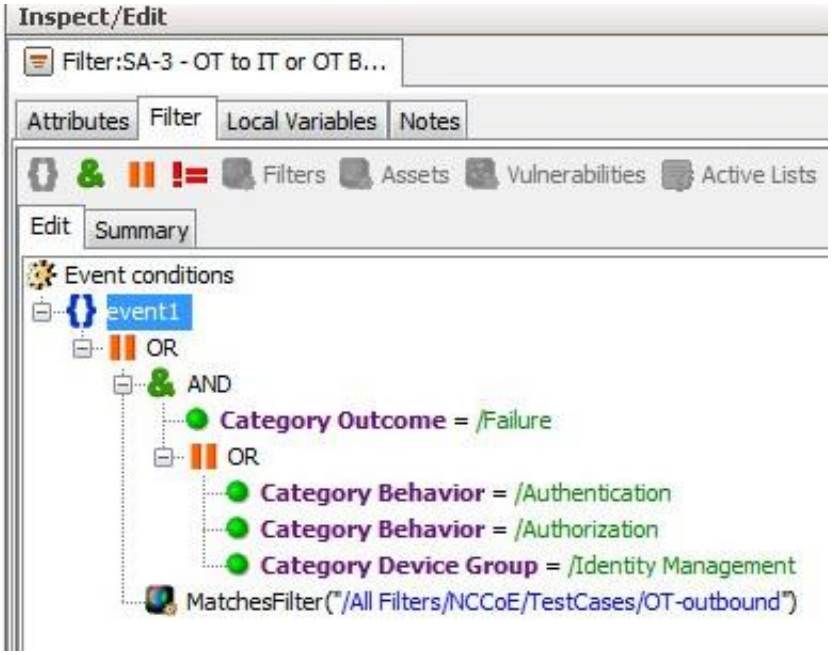
Name	Op	Condition
Event		
Aggregated Event Count		
Application Protocol		
Bytes In		
Bytes Out		
Correlated Event Count		
Crypto Signature		
Customer		
Customer External ID		

Figure 3-21 SA-3 - FailedLogins Filter



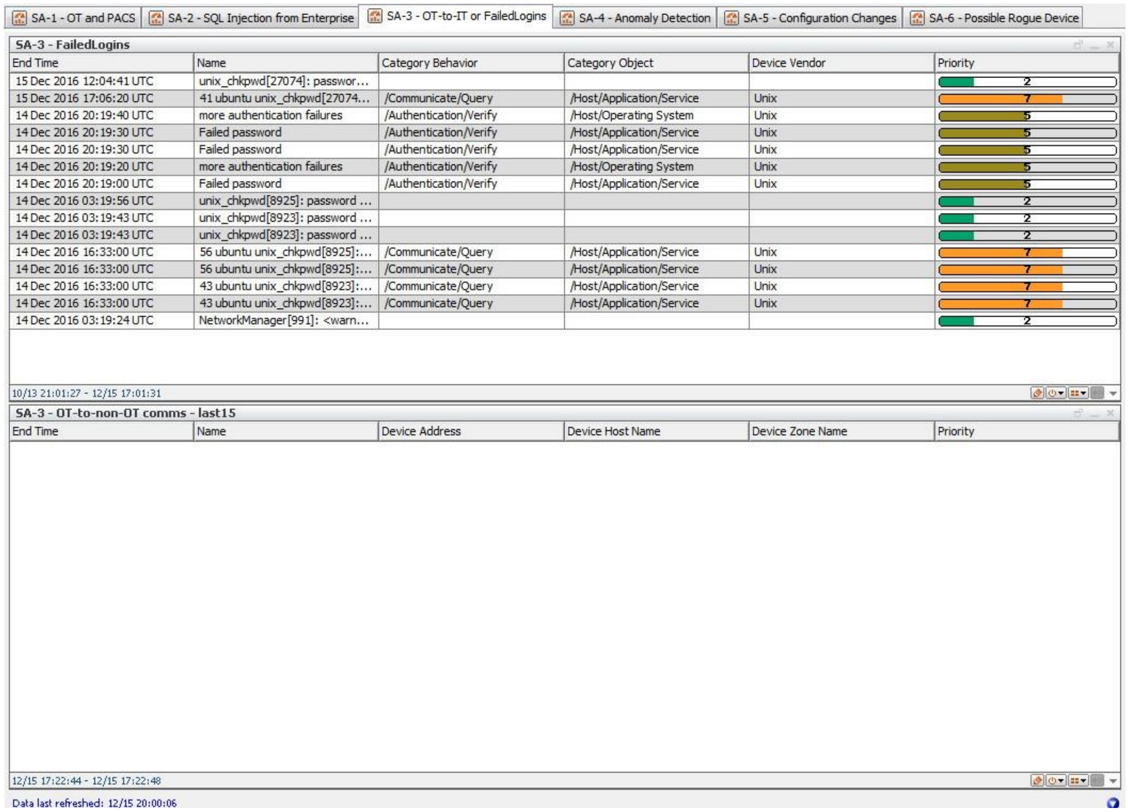
```
Event conditions
  event1
    OR
      Name Contains password check failed
      AND
        OR
          Category Behavior StartsWith /Authentication
          Category Behavior StartsWith /Authorization
          Category Device Group StartsWith /Identity Management
        OR
          Category Outcome != /Success
          Category Significance = /Failure
```

Figure 3-22 SA-3 OT to IT or OT BadLogins Filter



```
Event conditions
{} event1
   OR
      AND
         Category Outcome = /Failure
         OR
            Category Behavior = /Authentication
            Category Behavior = /Authorization
            Category Device Group = /Identity Management
      MatchesFilter("/All Filters/NCCoE/TestCases/OT-outbound")
```

Figure 3-23 SA-3 OT-to-IT or FailedLogins Dashboard



SA-1 - OT and PACS
SA-2 - SQL Injection from Enterprise
SA-3 - OT-to-IT or FailedLogins
SA-4 - Anomaly Detection
SA-5 - Configuration Changes
SA-6 - Possible Rogue Device

SA-3 - FailedLogins

End Time	Name	Category Behavior	Category Object	Device Vendor	Priority
15 Dec 2016 12:04:41 UTC	unix_chkpwd[27074]: passwor...				2
15 Dec 2016 17:06:20 UTC	41 ubuntu unix_chkpwd[27074...	/Communicate/Query	/Host/Application/Service	Unix	7
14 Dec 2016 20:19:40 UTC	more authentication failures	/Authentication/Verify	/Host/Operating System	Unix	5
14 Dec 2016 20:19:30 UTC	Failed password	/Authentication/Verify	/Host/Application/Service	Unix	5
14 Dec 2016 20:19:30 UTC	Failed password	/Authentication/Verify	/Host/Application/Service	Unix	5
14 Dec 2016 20:19:20 UTC	more authentication failures	/Authentication/Verify	/Host/Operating System	Unix	5
14 Dec 2016 20:19:00 UTC	Failed password	/Authentication/Verify	/Host/Application/Service	Unix	5
14 Dec 2016 03:19:56 UTC	unix_chkpwd[8925]: password ...				2
14 Dec 2016 03:19:43 UTC	unix_chkpwd[8923]: password ...				2
14 Dec 2016 03:19:43 UTC	unix_chkpwd[8923]: password ...				2
14 Dec 2016 16:33:00 UTC	56 ubuntu unix_chkpwd[8925]:...	/Communicate/Query	/Host/Application/Service	Unix	7
14 Dec 2016 16:33:00 UTC	56 ubuntu unix_chkpwd[8925]:...	/Communicate/Query	/Host/Application/Service	Unix	7
14 Dec 2016 16:33:00 UTC	43 ubuntu unix_chkpwd[8923]:...	/Communicate/Query	/Host/Application/Service	Unix	7
14 Dec 2016 16:33:00 UTC	43 ubuntu unix_chkpwd[8923]:...	/Communicate/Query	/Host/Application/Service	Unix	7
14 Dec 2016 03:19:24 UTC	NetworkManager[991]: <warn...				2

10/13 21:01:27 - 12/15 17:01:31

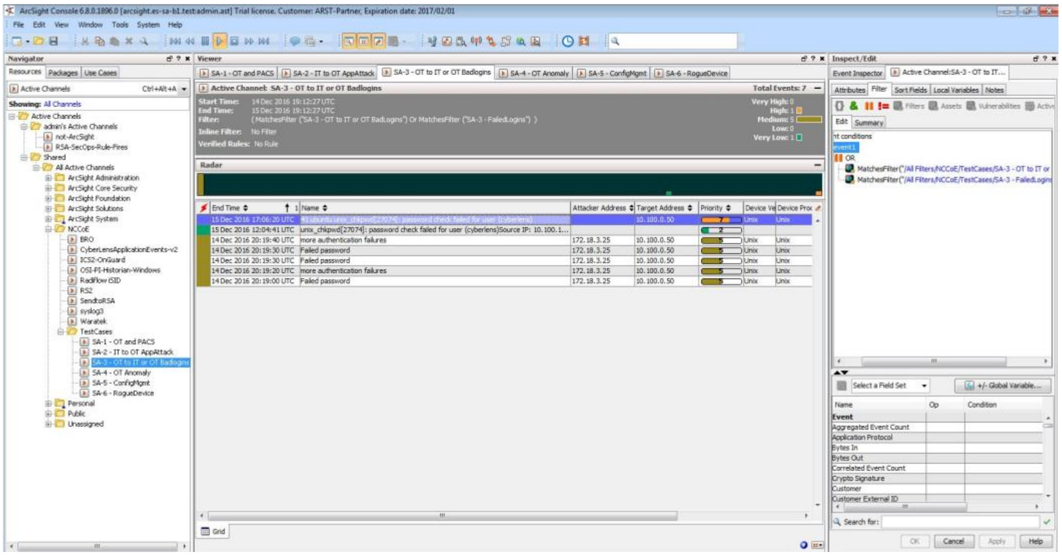
SA-3 - OT-to-non-OT comms - last15

End Time	Name	Device Address	Device Host Name	Device Zone Name	Priority

12/15 17:22:44 - 12/15 17:22:48

Data last refreshed: 12/15 20:00:06

Figure 3-24 SA-3 OT-to-IT or FailedLogins Active Channel



ArcSight Console 6.8.0.1896.0 [arcsight.es-sa-b1.test:admin.ast] Trial license. Customer: ARST-Partner, Expiration date: 2017/02/01

Active Channel: SA-3 - OT to IT or OT Badlogins — Total Events: 7

Start Time: 14 Dec 2016 19:12:27 UTC
End Time: 15 Dec 2016 19:12:27 UTC
Filter: (MatchesFilter ("SA-3 - OT to IT or OT BadLogins") Or MatchesFilter ("SA-3 - FailedLogins"))
Inline Filter: No Filter
Verified Rules: No Rule

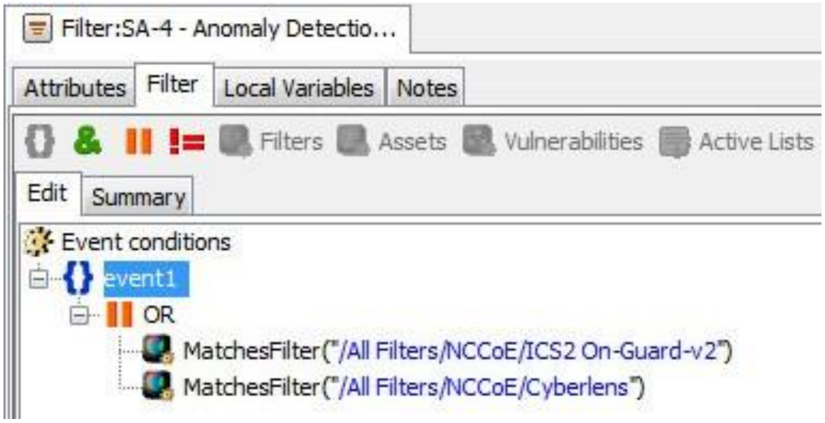
Very High: 0
High: 1
Medium: 5
Low: 0
Very Low: 1

End Time	Name	Attacker Address	Target Address	Priority	Device Ve	Device Proc
15 Dec 2016 17:06:20 UTC	41:ubuntu unix_chkpwd[27074]: password check failed for user (cyberlens)		10.100.0.50	7	Unix	Unix
15 Dec 2016 12:04:41 UTC	unix_chkpwd[27074]: password check failed for user (cyberlens)Source IP: 10.100.1...			2		
14 Dec 2016 20:19:40 UTC	more authentication failures	172.18.3.25	10.100.0.50	5	Unix	Unix
14 Dec 2016 20:19:30 UTC	Failed password	172.18.3.25	10.100.0.50	5	Unix	Unix
14 Dec 2016 20:19:30 UTC	Failed password	172.18.3.25	10.100.0.50	5	Unix	Unix
14 Dec 2016 20:19:20 UTC	more authentication failures	172.18.3.25	10.100.0.50	5	Unix	Unix
14 Dec 2016 20:19:00 UTC	Failed password	172.18.3.25	10.100.0.50	5	Unix	Unix

Inspect/Edit — Active Channel:SA-3 - OT to IT...

nt conditions
event1
OR
MatchesFilter("/All Filters/NCCoE/TestCases/SA-3 - OT to IT or
MatchesFilter("/All Filters/NCCoE/TestCases/SA-3 - FailedLogins

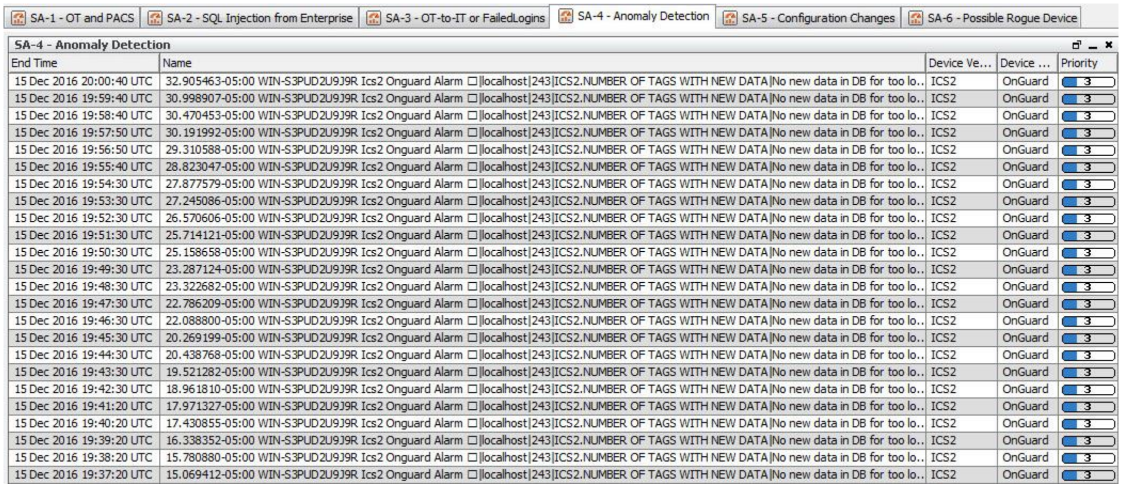
Figure 3-25 SA-4 Anomaly Detection Filter



Filter:SA-4 - Anomaly Detectio...

Event conditions
event1
OR
MatchesFilter("/All Filters/NCCoE/ICS2 On-Guard-v2")
MatchesFilter("/All Filters/NCCoE/Cyberlens")

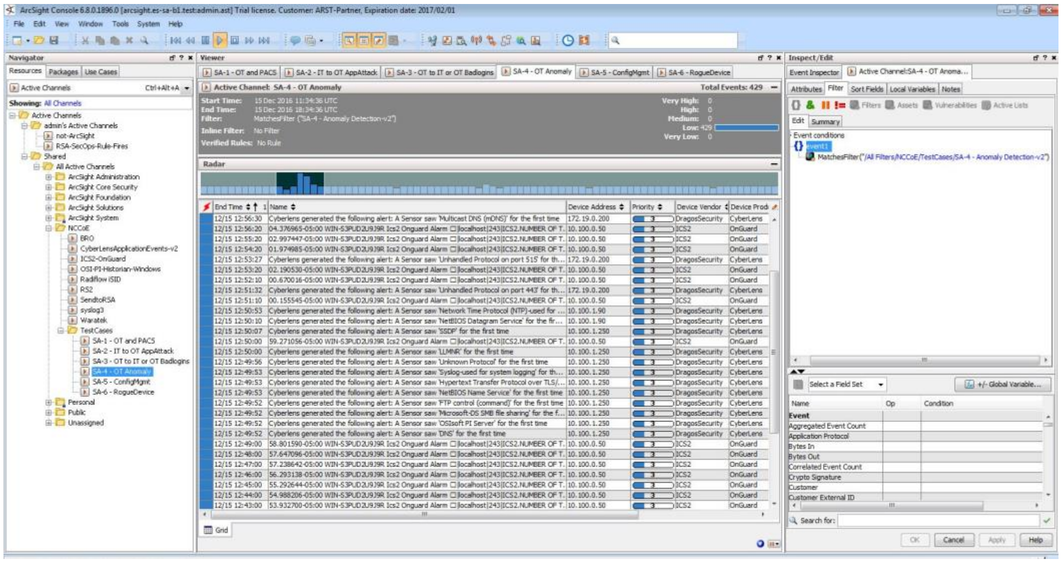
Figure 3-26 SA-4 Anomaly Detection Dashboard


SA-1 - OT and PACS
SA-2 - SQL Injection from Enterprise
SA-3 - OT-to-IT or FailedLogins
SA-4 - Anomaly Detection
SA-5 - Configuration Changes
SA-6 - Possible Rogue Device

SA-4 - Anomaly Detection

End Time	Name	Device Ve...	Device ...	Priority
15 Dec 2016 20:00:40 UTC	32.905463-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:59:40 UTC	30.998907-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:58:40 UTC	30.470453-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:57:50 UTC	30.191992-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:56:50 UTC	29.310588-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:55:40 UTC	28.823047-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:54:30 UTC	27.877579-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:53:30 UTC	27.245086-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:52:30 UTC	26.570606-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:51:30 UTC	25.714121-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:50:30 UTC	25.158658-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:49:30 UTC	23.287124-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:48:30 UTC	23.322682-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:47:30 UTC	22.786209-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:46:30 UTC	22.088800-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:45:30 UTC	20.269199-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:44:30 UTC	20.438768-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:43:30 UTC	19.521282-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:42:30 UTC	18.961810-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:41:20 UTC	17.971327-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:40:20 UTC	17.430855-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:39:20 UTC	16.338352-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:38:20 UTC	15.780880-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3
15 Dec 2016 19:37:20 UTC	15.069412-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF TAGS WITH NEW DATA|No new data in DB for too lo..	ICS2	OnGuard	3

Figure 3-27 Anomaly Detection Active Channel



ArcSight Console 6.8.0.1896.0 [arcsight.es-sa-b1.test:admin.ast] Trial license. Customer: ARST-Partner, Expiration date: 2017/02/01

Showing: All Channels

- Active Channels
  - admin's Active Channels
    - not-ArcSight
    - RSA-SecOps-Rule-Fires
  - Shared
    - All Active Channels
      - ArcSight Administration
      - ArcSight Core Security
      - ArcSight Foundation
      - ArcSight Solutions
      - ArcSight System
      - NCCoE
        - BRO
        - CyberLensApplicationEvents-v2
        - ICS2-OnGuard
        - OSI-PI-Historian-Windows
        - Radiflow iSID
        - RS2
        - SendtoRSA
        - syslog3
        - Waratek
        - TestCases
          - SA-1 - OT and PACS
          - SA-2 - IT to OT AppAttack
          - SA-3 - OT to IT or OT Badlogins
          - SA-4 - OT Anomaly
          - SA-5 - ConfigMgmt
          - SA-6 - RogueDevice
      - Personal
      - Public
      - Unassigned

Active Channel: SA-4 - OT Anomaly — Total Events: 429

Start Time: 15 Dec 2016 11:34:36 UTC
End Time: 15 Dec 2016 18:34:36 UTC
Filter: MatchesFilter ("SA-4 - Anomaly Detection-v2")
Inline Filter: No Filter
Verified Rules: No Rule

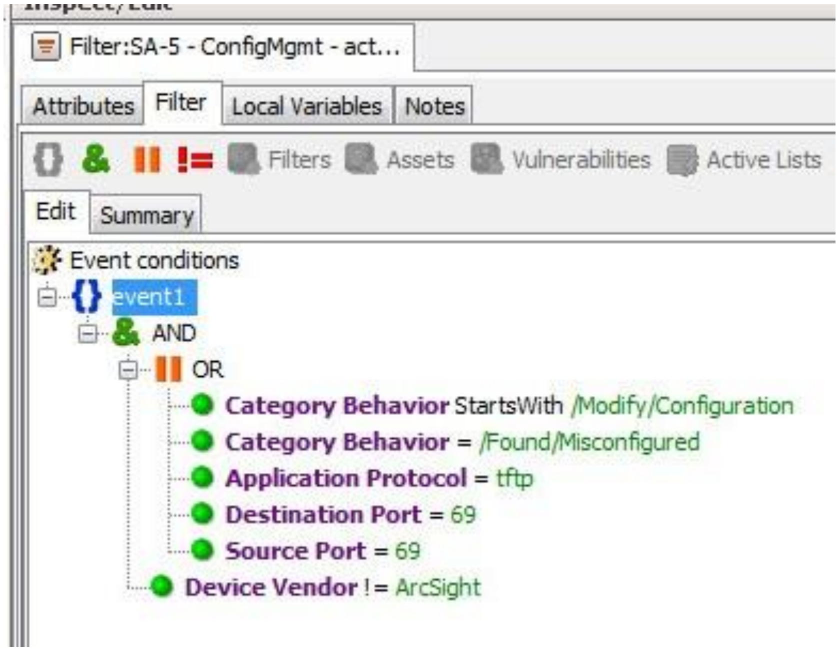
Very High: 0
High: 0
Medium: 0
Low: 429
Very Low: 0

End Time	Name	Device Address	Priority	Device Vendor	Device Prod
12/15 12:56:30	Cyberlens generated the following alert: A Sensor saw 'Multicast DNS (mDNS)' for the first time	172.19.0.200	3	DragosSecurity	CyberLens
12/15 12:56:20	04.376965-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:55:20	02.997447-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:54:20	01.974985-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:53:27	Cyberlens generated the following alert: A Sensor saw 'Unhandled Protocol on port 515' for th...	172.19.0.200	3	DragosSecurity	CyberLens
12/15 12:53:20	02.190530-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:52:10	00.670016-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:51:32	Cyberlens generated the following alert: A Sensor saw 'Unhandled Protocol on port 443' for th...	172.19.0.200	3	DragosSecurity	CyberLens
12/15 12:51:10	00.155545-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:50:53	Cyberlens generated the following alert: A Sensor saw 'Network Time Protocol (NTP)-used for ...	10.100.1.90	3	DragosSecurity	CyberLens
12/15 12:50:10	Cyberlens generated the following alert: A Sensor saw 'NetBIOS Datagram Service' for the fir...	10.100.1.90	3	DragosSecurity	CyberLens
12/15 12:50:07	Cyberlens generated the following alert: A Sensor saw 'SSDP' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:50:00	59.271056-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:50:00	Cyberlens generated the following alert: A Sensor saw 'LLMNR' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:56	Cyberlens generated the following alert: A Sensor saw 'Unknown Protocol' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:53	Cyberlens generated the following alert: A Sensor saw 'Syslog-used for system logging' for th...	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:53	Cyberlens generated the following alert: A Sensor saw 'Hypertext Transfer Protocol over TLS/...	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:53	Cyberlens generated the following alert: A Sensor saw 'NetBIOS Name Service' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:52	Cyberlens generated the following alert: A Sensor saw 'FTP control (command)' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:52	Cyberlens generated the following alert: A Sensor saw 'Microsoft-DS SMB file sharing' for the f...	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:52	Cyberlens generated the following alert: A Sensor saw 'OSIsoft PI Server' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:52	Cyberlens generated the following alert: A Sensor saw 'DNS' for the first time	10.100.1.250	3	DragosSecurity	CyberLens
12/15 12:49:00	58.801590-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:48:00	57.647096-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:47:00	57.238642-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:46:00	56.293138-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:45:00	55.292644-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:44:00	54.988206-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard
12/15 12:43:00	53.932700-05:00 WIN-S3PUD2U9J9R Ics2 Onguard Alarm □|localhost|243|ICS2.NUMBER OF T.	10.100.0.50	3	ICS2	OnGuard

Event conditions
- event1
  - MatchesFilter("/All Filters/NCCoE/TestCases/SA-4 - Anomaly Detection-v2")

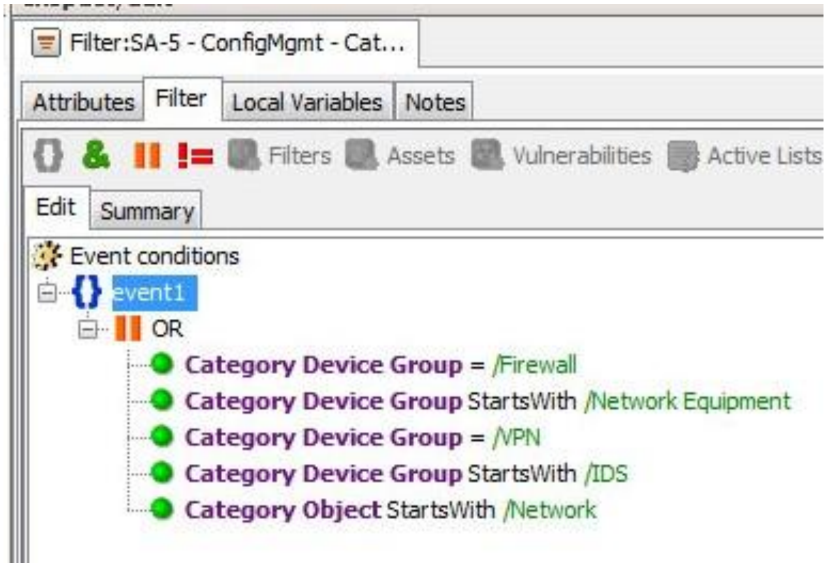
Name	Op	Condition
Event		
Aggregated Event Count		
Application Protocol		
Bytes In		
Bytes Out		
Correlated Event Count		
Crypto Signature		
Customer		
Customer External ID		

Figure 3-28 SA-5 ConfigMgnt Filter



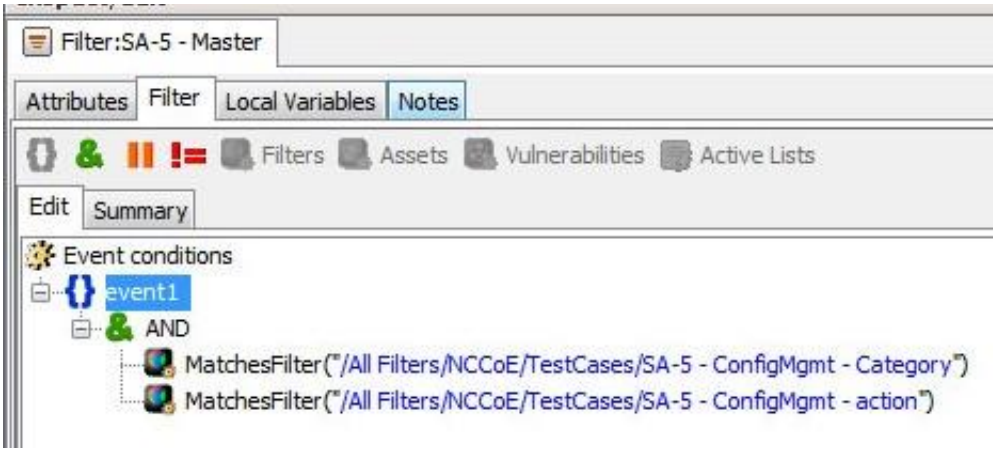
```
Event conditions
{} event1
  & AND
    || OR
      ● Category Behavior StartsWith /Modify/Configuration
      ● Category Behavior = /Found/Misconfigured
      ● Application Protocol = tftp
      ● Destination Port = 69
      ● Source Port = 69
    ● Device Vendor != ArcSight
```

Figure 3-29 SA-5 ConfigMgmt Filter



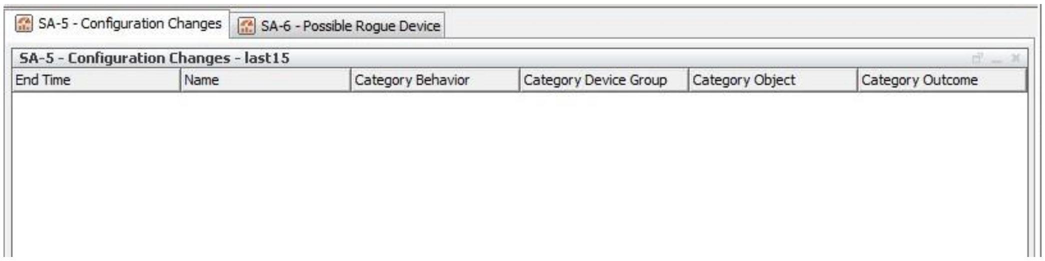
```
Event conditions
{} event1
  || OR
    ● Category Device Group = /Firewall
    ● Category Device Group StartsWith /Network Equipment
    ● Category Device Group = /VPN
    ● Category Device Group StartsWith /IDS
    ● Category Object StartsWith /Network
```

Figure 3-30 SA-5 Master Filter



```
Event conditions
  event1
    AND
      MatchesFilter("/All Filters/NCCoE/TestCases/SA-5 - ConfigMgmt - Category")
      MatchesFilter("/All Filters/NCCoE/TestCases/SA-5 - ConfigMgmt - action")
```

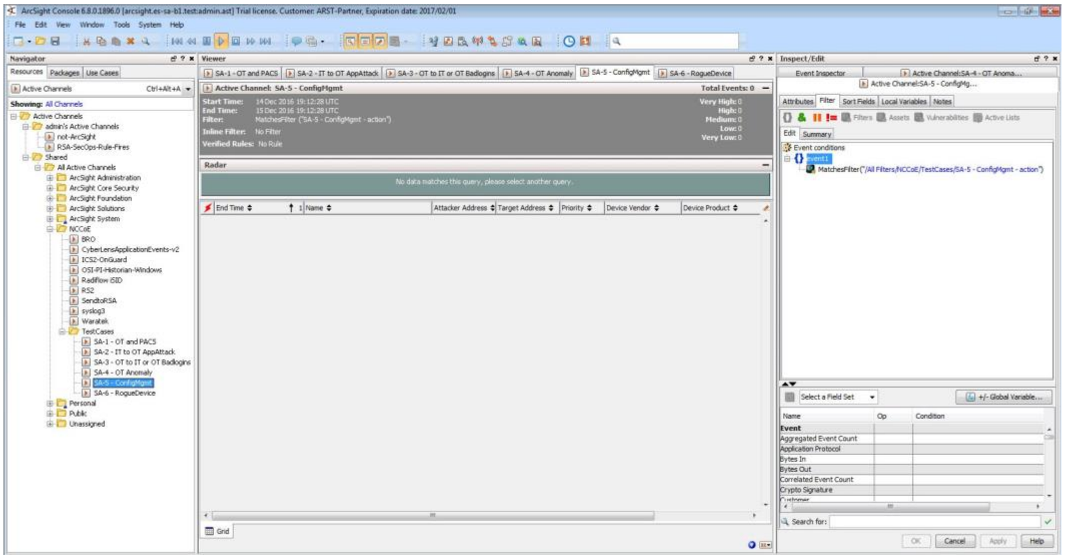
Figure 3-31 SA-5 Configuration Changes Dashboard



SA-5 - Configuration Changes - last15

End Time	Name	Category Behavior	Category Device Group	Category Object	Category Outcome

Figure 3-32 SA-5 Configuration Changes Active Channel



ArcSight Console 6.8.0.1896.0 [arcsight.es-sa-b1.test:admin.ast] Trial license. Customer: ARST-Partner, Expiration date: 2017/02/01

Active Channel: SA-5 - ConfigMgmt   Total Events: 0

Start Time: 14 Dec 2016 19:12:28 UTC
End Time: 15 Dec 2016 19:12:28 UTC
Filter: MatchesFilter ("SA-5 - ConfigMgmt - action")
Inline Filter: No Filter
Verified Rules: No Rule

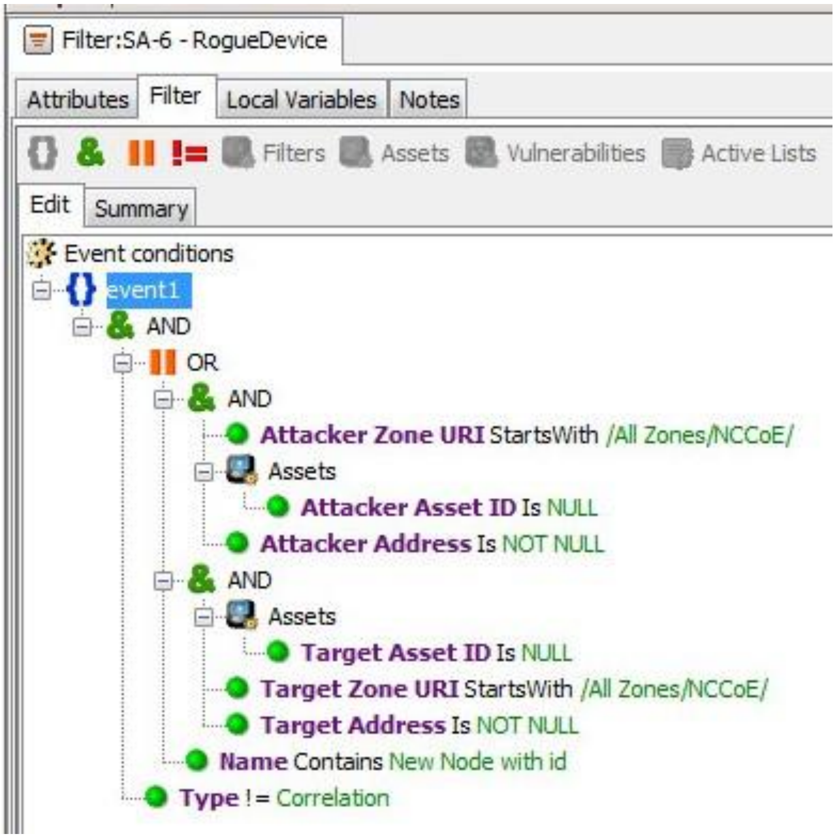
Very High: 0
High: 0
Medium: 0
Low: 0
Very Low: 0

Radar

No data matches this query, please select another query.

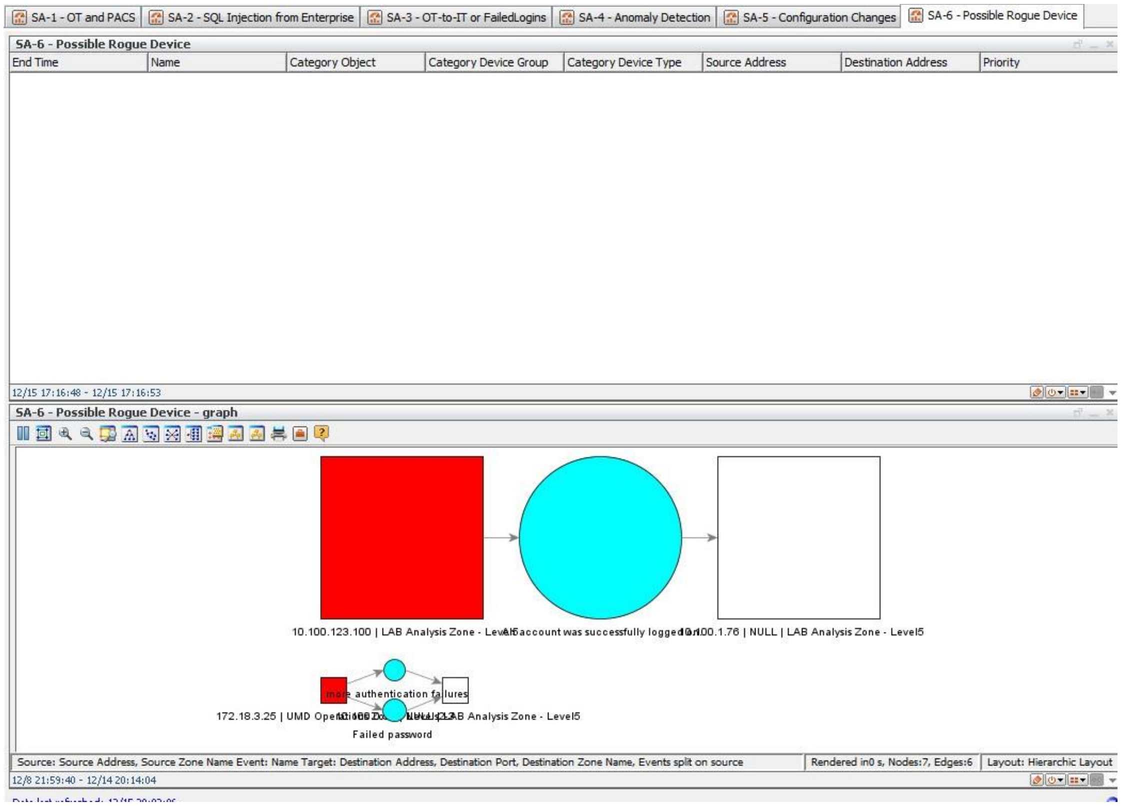
Event conditions
event1
MatchesFilter("/All Filters/NCCoE/TestCases/SA-5 - ConfigMgmt - action")

Figure 3-33 SA-6 RogueDevice Filter



```
Event conditions
{} event1
   AND
      OR
         AND
            Attacker Zone URI StartsWith /All Zones/NCCoE/
            Assets
               Attacker Asset ID Is NULL
            Attacker Address Is NOT NULL
         AND
            Assets
               Target Asset ID Is NULL
            Target Zone URI StartsWith /All Zones/NCCoE/
            Target Address Is NOT NULL
         Name Contains New Node with id
      Type != Correlation
```

Figure 3-34 SA-6 Rogue Device Dashboard



SA-1 - OT and PACS | SA-2 - SQL Injection from Enterprise | SA-3 - OT-to-IT or FailedLogins | SA-4 - Anomaly Detection | SA-5 - Configuration Changes | SA-6 - Possible Rogue Device

SA-6 - Possible Rogue Device

End Time	Name	Category Object	Category Device Group	Category Device Type	Source Address	Destination Address	Priority

12/15 17:16:48 - 12/15 17:16:53

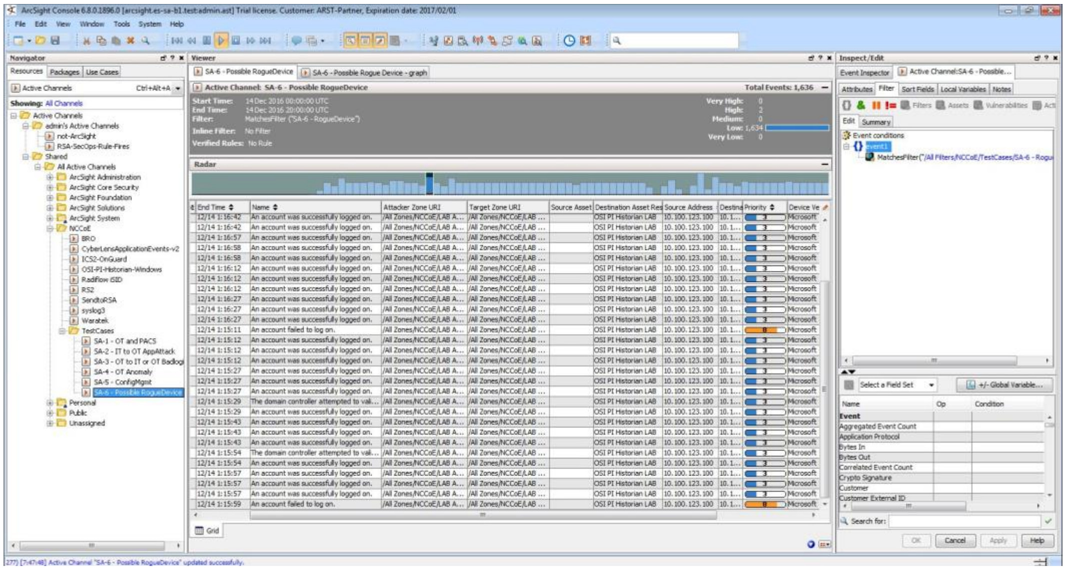
SA-6 - Possible Rogue Device - graph

10.100.123.100 | LAB Analysis Zone - Level5
An account was successfully logged on
10.100.1.76 | NULL | LAB Analysis Zone - Level5
more authentication failures
172.18.3.25 | UMD Operations Zone
NULL | LAB Analysis Zone - Level5
Failed password

Source: Source Address, Source Zone Name Event: Name Target: Destination Address, Destination Port, Destination Zone Name, Events split on source | Rendered in0 s, Nodes:7, Edges:6 | Layout: Hierarchic Layout

12/8 21:59:40 - 12/14 20:14:04

Figure 3-35 SA-6 Rogue Device Active Channel



Active Channel: SA-6 - Possible RogueDevice   Total Events: 1,636

Start Time: 14 Dec 2016 00:00:00 UTC
End Time: 14 Dec 2016 20:00:00 UTC
Filter: MatchesFilter ("SA-6 - RogueDevice")
Inline Filter: No Filter
Verified Rules: No Rule

Very High: 0
High: 2
Medium: 0
Low: 1,634
Very Low: 0

End Time	Name	Attacker Zone URI	Target Zone URI	Source Asset	Destination Asset Res	Source Address	Destina	Priority	Device Ve
12/14 1:16:42	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:42	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:57	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:58	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:58	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:12	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:12	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:12	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:27	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:27	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:16:27	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:11	An account failed to log on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	8	Microsoft
12/14 1:15:12	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:12	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:12	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:27	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:27	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:27	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:29	The domain controller attempted to vali...	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:29	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:43	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:43	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:43	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:54	The domain controller attempted to vali...	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:54	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:57	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:57	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:57	An account was successfully logged on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	3	Microsoft
12/14 1:15:59	An account failed to log on.	/All Zones/NCCoE/LAB A...	/All Zones/NCCoE/LAB ...		OSI PI Historian LAB	10.100.123.100	10.1...	8	Microsoft

Event conditions
event1
MatchesFilter("/All Filters/NCCoE/TestCases/SA-6 - Rogu

Name	Op	Condition
Event		
Aggregated Event Count		
Application Protocol		
Bytes In		
Bytes Out		
Correlated Event Count		
Crypto Signature		
Customer		
Customer External ID		

277) [7:47:48] Active Channel "SA-6 - Possible RogueDevice" updated successfully.

3.2 Test Cases

Below are descriptions of test cases as matched to Section 3.6, Situational Awareness Test Cases, of NIST SP 1800-7B.

3.2.1 SA-1 Event Correlation for OT and PACS

This test case focuses on the possibility of correlated events occurring that involve OT and PACS and that might indicate compromised access.

3.2.1.1 Events

1. Technician accesses substation/control station.
2. OT device goes down.

3.2.1.2 Desired Outcome

Alert of anomalous condition and subsequent correlation to PACS to see who accessed facility

3.2.1.3 ArcSight Content

1. OT network Zones
2. Filter for OT network Zones.

3. filters for OT/IT inbound, outbound, cross-boundary communications
4. filter for RS2 Door Controller events
5. filter for CyberLens or iSID events
6. Active List for RS2 Door Controller events with time threshold
7. rule to add RS2 Door Controller filter events to Active List
8. Data Monitor and Dashboard to display results of the above

3.2.2 SA-2 Event Correlation for OT and IT

The enterprise (IT) Java application communication with an OT device (historian) is used as a vector for SQL injection (SQLi), which also includes data exfiltration attempts.

3.2.2.1 Events

Detection of SQLi attack on IT device interconnected with OT device

3.2.2.2 Desired Outcome

Alert sent to SIEM on multiple SQLi attempts

3.2.2.3 ArcSight Content

1. filter for Waratek events (intended to monitor for SQLi against the OSIsoft PI Historian)
2. filter to combine Waratek and OT/IT inbound communications filters
3. Data Monitor and Dashboard to display results of the above

3.2.3 SA-3 Event Correlation for OT and IT/PACS and OT

Unauthorized access attempts are detected, and alerts are triggered based on connection requests from a device on the SCADA network destined for an IP that is outside the SCADA IP range. This test case focuses on the possibility of a malicious actor attempting to gain access to an OT device via the enterprise (IT) network. This test case is also relevant in a PACS-OT scenario, in which someone has physical access to an OT device but lacks the necessary access to perform changes to the device, and alerts are sent based on numerous failed login attempts.

3.2.3.1 Events

Inbound/outbound connection attempts from devices outside authorized and known inventory

3.2.3.2 Desired Outcome

Alert to SIEM showing IP of unidentified host attempting to connect, or of identified host attempting to connect to unidentified host

3.2.3.3 ArcSight Content

1. Use OT network Zones (as defined in SA-1 content).
2. Use filter for OT network Zones (as defined in SA-1 content).
3. Filter for events from OT network Zone to/from a different Zone
4. Filters for authorization, authentication failures
5. Filter for authorization, authentication failures, or outbound events
6. Data Monitor and Dashboard to display results of the above

3.2.4 SA-4 Data Infiltration Attempts

Examine the behavior of systems, and configure the SIEM to alert on behavior that is outside the normal baseline. Alerts can be created emanating from OT, IT, and PACS. This test case seeks alerting based on behavioral anomalies rather than recognition of IP addresses, and guards against anomalous or malicious inputs.

3.2.4.1 Events

Anomalous behavior falling outside defined baseline

3.2.4.2 Desired Outcome

Alert sent to SIEM on any event falling outside of what is considered normal activity based on historical data

3.2.4.3 ArcSight Content

1. Use OT network Zones.
2. Use Filter for OT network Zones.
3. Filter for ICS2 OnGuard events or events with a Category of Traffic Anomaly (e.g., as defined in Dragos Security CyberLens ArcSight FlexConnector/Categorizer files).
4. Data Monitor and Dashboard to display results of the above

3.2.5 SA-5 Configuration Management

An alert will be created to notify the SIEM of unauthorized (inadvertent or malicious) uploading of an ICS network device configuration. The detection method will be primarily based on inherent device capability (i.e., log files).

3.2.5.1 Events

Configuration change on Tofino FW, Cisco 2950

3.2.5.2 Desired Outcome

Alert will be created to notify SIEM that this has occurred.

3.2.5.3 ArcSight Content

1. Filter for any of the following:
    a. ArcSight Category events:
        i. /Modify/Configuration
        ii. /Found/Misconfigured
        iii. tftp protocol
        iv. tftp port
2. Filter for following ArcSight Category Device Groups:
    a. /Firewall
    b. /Network Equipment
    c. /VPN
    d. /IDS
    e. or Category Object:
        i. /Network
3. Data Monitor and Dashboard to display results of the above

3.2.6 SA-6 Rogue Device Detection

Alerts are triggered by the introduction of any device onto the ICS network that has not been registered with the asset management capability in the build.

3.2.6.1 Events

Unidentified device appears on ICS network.

3.2.6.2 Desired Outcome

Alert will be created to notify the SIEM that this has occurred.

3.2.6.3 ArcSight Content

1. Specific Asset definitions for all known ICS devices (grouped by OT Zones)
2. Filter to detect presence of any “non-ICS” devices (not in Asset lists).
3. Filter for CyberLens events alerting on “new” hosts.
4. Data Monitor and Dashboard to display results of the above

Appendix A List of Acronyms

ASP	Active Server Pages
CA	Certificate Authority
CRADA	Cooperative Research and Development Agreement
E1	Siemens RUGGEDCOM RX1400
E4	OSIsoft Pi Historian
E5	OnGuard
E6	ConsoleWorks
E7	RS2 Access IT!
E8	CyberLens Server
E9	Siemens RUGGEDCOM CROSSBOW
E10	Waratek Runtime Protection
E12	Hewlett Packard Enterprise ArcSight
E13	RSA SecOps
EACMS	Electronic Access Control and Monitoring System
ESM	Enterprise Security Manager
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HDD	Hard Disk Drive
HPE	Hewlett Packard Enterprise
ICS	Industrial Control System(s)
ICU	Interface Configuration Utility
IDS	Intrusion Detection System
IIS	Internet Information Services
IP	Internet Protocol
IPSec	IP Security

ISAPI	Internet Server Application Programming Interface
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LTS	Long-Term Support
NAT	Network Address Translator
NCCoE	The National Cybersecurity Center of Excellence
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
O1	Siemens RUGGEDCOM RX1501
O2	Waterfall Security Solutions, Ltd. Unidirectional Security Gateway
O3	Schneider Electric Tofino Firewall
O4	RS2 Door Controller
O5	TDi Technologies ConsoleWorks
O8	OSIsoft Pi Historian
O9	TDi Technologies ConsoleWorks
O10	CyberLens Sensor
O11	Radiflow iSID
O13	OSIsoft Citect Interface software
O14	Radiflow 3180 Firewall
O15	Cisco 2950 Network Switch
O16	IXIA Full Duplex Taps
O17	Waterfall Secure Bypass Switch
O18	Schneider Electric Tofino Firewall
O20	Schneider Electric Tofino Firewall
ODBC	Open Database Connectivity

OPC	Open Platform Communication
OT	Operational Technology
OVA	Open Virtual Appliance
PAC	Physical Access Control
PACS	Physical Access Control Systems
PDP	Policy Decision Point
PEP	Policy Enforcement Point
RDP	Remote Desktop Protocol
RHEL	Red Hat Enterprise Linux
RMF	Risk Management Framework
SA	Situational Awareness
SAC	Station Access Controller
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protocol
SIEM	Security Information and Event Management
SP	Special Publication
SQL	Structured Query Language
SQLi	Structured Query Language Injection
U1	Citect SCADA System
UDP	User Datagram Protocol
UMD	University of Maryland
vCPU	Virtual Central Processing Unit
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B References

[1] Micro Focus. *HPE ArcSight SmartConnector User Guide – Hewlett Packard Software Community*. Available: https://www.protect724.hpe.com/docs/DOC-2279.