

**NIST SPECIAL PUBLICATION 1800-23**

---

# Energy Sector Asset Management

## For Electric Utilities, Oil & Gas Industry

---

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

**James McCarthy**  
**Lauren Acierto**  
**Glen Joy**  
**Jason Kuruvilla**  
**Titilayo Ogunyale**  
**Nikolas Urlaub**  
**John Wiltberger**  
**Devin Wynne**

DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management>



NIST SPECIAL PUBLICATION 1800-23

# Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry

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

James McCarthy  
Glen Joy  
*National Cybersecurity Center of Excellence  
Information Technology Laboratory*

Lauren Acierto  
Jason Kuruvilla  
Titilayo Ogunyale  
Nikolas Urlaub  
John Wiltberger  
*Devin Wynne  
The MITRE Corporation  
McLean, Virginia*

DRAFT

September 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 1800-23A**

---

# Energy Sector Asset Management

## For Electric Utilities, Oil & Gas Industry

---

**Volume A:  
Executive Summary**

**James McCarthy  
Glen Joy**

National Cybersecurity Center of Excellence  
Information Technology Laboratory

**Lauren Acierto  
Jason Kuruville  
Titilayo Ogunyale  
Nikolas Urlaub  
John Wiltberger  
Devin Wynne**

The MITRE Corporation  
McLean, Virginia

September 2019

DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management>

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



# 1 Executive Summary

- 2       ▪ The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards  
3       and Technology (NIST) built a laboratory environment to demonstrate how energy organizations  
4       can strengthen their operational technology (OT) asset management practices by leveraging  
5       capabilities that may already exist within their operating environment or by implementing new  
6       capabilities.
- 7       ▪ As electric utilities and the oil and gas industry are some of the nation's [critical infrastructures](#),  
8       the incapacitation or destruction of assets, systems, and networks in the energy sector could  
9       have serious negative effects on the economy, public health, and safety.
- 10      ▪ As industrial control systems (ICS) in the energy sector become more interconnected,  
11      vulnerabilities within OT assets and processes are targets for malicious actors.
- 12      ▪ A challenge for energy organizations is maintaining an updated asset inventory. It is difficult to  
13      protect what cannot be seen or is not known. Without an effective asset management solution,  
14      organizations that are unaware of any assets in their infrastructure may be unnecessarily  
15      exposed to cybersecurity risks.
- 16      ▪ This NIST Cybersecurity Practice Guide provides detailed steps on how energy organizations can  
17      identify and manage OT assets and detect cybersecurity risks associated with them.

## 18 CHALLENGE

19 Energy organizations may be a prime target of growing and evolving cybersecurity threats, given the  
20 criticality of their infrastructure to our nation. A cyber attack that disrupts OT processes or equipment  
21 can result in safety issues and the loss of power, as well as in significant productivity costs. Currently,  
22 many energy organizations rely on manual processes to manage their OT assets, which makes it  
23 challenging to quickly identify and respond to potential threats. Existing asset inventories may be static,  
24 one-time, or point-in-time snapshots of auditing activities conducted previously without a way to see  
25 the current status of those assets. As OT systems become interconnected and integrated with other  
26 information technology (IT) systems, organizations seeking to modernize OT processes will have to  
27 identify automated methods to strengthen their OT asset management capabilities.

## 28 SOLUTION

29 The NCCoE, in collaboration with experts from the energy sector and technology vendors, developed an  
30 asset management example solution that includes managing, monitoring, and baselining OT assets to  
31 reduce the risk of cybersecurity incidents. This practice guide outlines practical steps on how  
32 organizations can implement new asset management capabilities or leverage existing asset  
33 management capabilities, to enhance the security of OT assets.

34 The NCCoE sought existing technologies that provided the following capabilities:

- 35       ▪ OT/ICS asset inventory (including devices using serial connections)
- 36       ▪ high-speed communication mechanisms for remote asset management
- 37       ▪ reliable/secure/encrypted communications

- 38       ▪ continuous asset monitoring
- 39       ▪ log analysis and correlation
- 40       ▪ cybersecurity event/attack detection
- 41       ▪ patch-level information
- 42       ▪ vulnerability awareness

43 While the NCCoE used a suite of commercial products to address this challenge, this guide does not  
44 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your  
45 organization’s information security experts should identify the products that will best integrate with  
46 your existing tools and IT/OT infrastructure. Your organization can adopt this solution or one that  
47 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
48 implementing parts of a solution.

## 49 **BENEFITS**

50 The NCCoE’s practice guide on Energy Sector Asset Management can help your energy organization:

- 51       ▪ reduce cybersecurity risk and potentially reduce the impact of safety and operational risks such  
52       as power disruption
- 53       ▪ develop and execute a strategy that provides continuous OT asset management and monitoring
- 54       ▪ respond faster to security alerts through automated cybersecurity-event capabilities
- 55       ▪ implement current cybersecurity standards and best practices, while maintaining the  
56       performance of energy infrastructures

## 57 **SHARE YOUR FEEDBACK**

58 You can view or download the guide at [https://www.nccoe.nist.gov/projects/use-cases/energy-](https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management)  
59 [sector/asset-management](https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management). Help the NCCoE make this guide better by sharing your thoughts with us as  
60 you read the guide. If you adopt this solution for your own organization, please share your experience  
61 and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our  
62 solution, so we encourage organizations to share lessons learned and best practices for transforming the  
63 processes associated with implementing this guide.

64 To provide comments or to learn more by arranging a demonstration of this example implementation,  
65 contact the NCCoE at [energy\\_nccoe@nist.gov](mailto:energy_nccoe@nist.gov).

66

---

## 67 **TECHNOLOGY PARTNERS/COLLABORATORS**

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



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

---

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](mailto:nccoe@nist.gov)  
301-975-0200

**NIST SPECIAL PUBLICATION 1800-23B**

---

# Energy Sector Asset Management

## For Electric Utilities, Oil & Gas Industry

---

**Volume B:**  
**Approach, Architecture, and Security Characteristics**

**James McCarthy**

**Glen Joy**

National Cybersecurity Center of Excellence  
Information Technology Laboratory

**Lauren Acierto**

**Jason Kuruville**

**Titilayo Ogunyale**

**Nikolas Urlaub**

**John Wiltberger**

**Devin Wynne**

The MITRE Corporation  
McLean, Virginia

September 2019

DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management>



DRAFT

## DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-23B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-23B, 47 pages, (September 2019), CODEN: NSPUE2

## FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Public comment period: September 23, 2019 through November 25, 2019

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

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



## 1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 17 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 27 **ABSTRACT**

28 Industrial control systems (ICS) compose a core part of our nation's critical infrastructure. Energy sector  
29 companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine, and  
30 transport oil and natural gas. Given the wide variety of ICS assets, such as programmable logic  
31 controllers and intelligent electronic devices, that provide command and control information on  
32 operational technology (OT) networks, it is essential to protect these devices to maintain continuity of  
33 operations. These assets must be monitored and managed to reduce the risk of a cyber attack on ICS-  
34 networked environments. Having an accurate OT asset inventory is a critical component of an overall  
35 cybersecurity strategy.

36 The NCCoE at NIST is responding to the energy sector’s request for an automated OT asset management  
 37 solution. To remain fully operational, energy sector entities should be able to effectively identify,  
 38 control, and monitor their OT assets. This document provides guidance on how to enhance OT asset  
 39 management practices by leveraging capabilities that may already exist in an energy organization’s  
 40 operating environment as well as implementing new capabilities.

41 **KEYWORDS**

42 *energy sector asset management; ESAM; ICS; industrial control system; malicious actor; monitoring;*  
 43 *operational technology; OT; SCADA; supervisory control and data acquisition*

44 **ACKNOWLEDGMENTS**

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

Name	Organization
Matt Cowell	Dragos, Inc.
Tom VanNorman	Dragos, Inc.
Andrew Dunham	Forescout Technologies, Inc.
Tim Jones	Forescout Technologies, Inc.
John Norsworthy	Forescout Technologies, Inc.
Lindsey Hale	FoxGuard Solutions, Inc.
Steve Boyd	KORE Wireless, Inc.
Brian Hicks	KORE Wireless, Inc.
Adam Cohn	Splunk Inc.
Bill Wright	Splunk Inc.
Ray Erlinger	TDi Technologies, Inc.
Bill Johnson	TDi Technologies, Inc.

Name	Organization
Samantha Pelletier	TDi Technologies, Inc.
Gabe Authier	Tripwire, Inc.
Steven Sletten	Tripwire, Inc.
Jim Wachhaus	Tripwire, Inc.

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

Technology Partner/Collaborator	Build Involvement
<a href="#">Dragos, Inc.</a>	Dragos Platform v1.5
<a href="#">ForeScout Technologies, Inc.</a>	ForeScout CounterACT v8.0.1
<a href="#">FoxGuard Solutions, Inc.</a>	FoxGuard Solutions Patch and Update Management Program v1
<a href="#">KORE Wireless Group, Inc.</a>	KORE Wireless Cellular Connectivity with Cellular Gateway v2.0
<a href="#">Splunk, Inc.</a>	Splunk Enterprise v7.1.3
<a href="#">TDi Technologies, Inc.</a>	TDi Technologies ConsoleWorks v5.2-0u1
<a href="#">Tripwire, Inc.</a>	Tripwire Industrial Visibility v3.2.1

50 **Contents**

51 **1 Summary..... 1**

52 1.1 Challenge..... 2

53 1.2 Solution..... 2

54 1.2.1 Relevant Standards and Guidance..... 3

55 1.3 Benefits..... 5

56 **2 How to Use This Guide ..... 5**

57 2.1 Typographic Conventions..... 6

58 **3 Approach ..... 7**

59 3.1 Audience..... 8

60 3.2 Scope ..... 8

61 3.3 Assumptions ..... 9

62 3.4 Risk Assessment ..... 10

63 3.4.1 Threats ..... 11

64 3.4.2 Vulnerabilities ..... 11

65 3.4.3 Risk ..... 12

66 3.4.4 Security Control Map ..... 13

67 3.4.5 National Initiative for Cybersecurity Education Workforce Framework ..... 18

68 3.5 Technologies..... 21

69 **4 Architecture ..... 23**

70 4.1 Architecture Description ..... 23

71 4.1.1 High-Level Architecture ..... 23

72 4.1.2 Reference Architecture..... 25

73 4.2 Example Solution..... 27

74 4.2.1 UMD Site Topology ..... 27

75 4.2.2 Plano Site Topology..... 28

76 4.2.3 Enterprise Location Topology ..... 29

77            4.2.4    Asset Management Dashboard .....30

78    **5    Functional Test Plan ..... 33**

79            5.1    Test Cases ..... 33

80            5.1.1    ESAM-1: New Device Attached .....33

81            5.1.2    ESAM-2: Vulnerability Notification .....35

82            5.1.3    ESAM-3: Device Goes Offline .....36

83            5.1.4    ESAM-4: Anomalous Device Communication .....37

84            5.1.5    ESAM-5: Remote Devices with Cellular Connectivity .....38

85    **6    Security Characteristic Analysis ..... 39**

86            6.1    Assumptions and Limitations ..... 40

87            6.2    Analysis of the Reference Design’s Support for Cybersecurity Framework

88               Subcategories ..... 40

89            6.2.1    ID.AM-1: Physical Devices and Systems Within the Organization Are Inventoried....40

90            6.2.2    ID.RA-2: Threat and Vulnerability Information Is Received from Information-Sharing

91               Forums and Sources.....41

92            6.2.3    PR.DS-2: Data in Transit Is Protected.....41

93            6.2.4    PR.MA-1: Maintenance and Repair of Organizational Assets Are Performed and

94               Logged in a Timely Manner with Approved and Controlled Tools .....41

95            6.2.5    PR.MA-2: Remote Maintenance of Organizational Assets Is Approved, Logged, and

96               Performed in a Manner that Prevents Unauthorized Access .....41

97            6.2.6    PR.PT-4: Communications and Control Networks Are Protected.....42

98            6.2.7    DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users and

99               Systems Is Established and Managed .....42

100           6.2.8    DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and Methods

101                  42

102           6.3    Lessons Learned ..... 42

103    **7    Future Build Considerations ..... 43**

104    **Appendix A    List of Acronyms ..... 44**

105    **Appendix B    References ..... 46**

106 **List of Figures**

107 **Figure 3-1 High-Level Topology** .....8

108 **Figure 3-2 Asset Management Characteristics** .....9

109 **Figure 4-1 High-Level Architecture** .....24

110 **Figure 4-2 Reference Architecture** .....25

111 **Figure 4-3 UMD In-Depth Topology**.....27

112 **Figure 4-4 Plano In-Depth Topology**.....28

113 **Figure 4-5 Enterprise In-Depth Topology**.....29

114 **Figure 4-6 Asset Dashboard: Asset Characteristics**.....30

115 **Figure 4-7 Asset Dashboard: Asset Communications** .....31

116 **Figure 4-8 Asset Dashboard: Asset Details, UMD**.....32

117 **Figure 4-9 Asset Dashboard: Asset Details, Plano** .....33

118 **List of Tables**

119 **Table 3-1 Security Control Map** .....13

120 **Table 3-2 NIST NICE Work Roles Mapped to the Cybersecurity Framework: ESAM** .....18

121 **Table 3-3 Products and Technologies** .....21

## 122 1 Summary

123 Industrial control systems (ICS) compose a core part of our nation’s critical infrastructure [1]. Energy-  
124 sector companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine,  
125 and transport oil and natural gas. Given the wide variety of ICS assets, such as programmable logic  
126 controllers (PLCs) and intelligent electronic devices (IEDs), which provide command and control  
127 information on operational technology (OT) networks, it is essential to protect these devices to maintain  
128 continuity of operations. Having an accurate OT asset inventory is a critical component of an overall  
129 cybersecurity strategy.

130 Energy companies own, operate, and maintain critical OT assets that possess unique requirements for  
131 availability and reliability. These assets must be monitored and managed to reduce the risk of cyber  
132 attacks on ICS-networked environments. Key factors in strengthening OT asset management capabilities  
133 are determining which tools can collect asset information and what type of communications  
134 infrastructure is required to transmit this information.

135 The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and  
136 Technology (NIST) is responding to the energy sector’s request for an automated OT asset management  
137 solution. To remain fully operational, energy sector entities should be able to effectively identify,  
138 control, and monitor all of their OT assets. This document provides guidance on how to enhance OT  
139 asset management practices, by leveraging capabilities that may already exist in an energy  
140 organization’s operating environment as well as implementing new capabilities.

141 The capabilities demonstrated in this guide were selected to address several key tenets of asset  
142 management: 1) establish a baseline of known assets, 2) establish a dynamic asset management  
143 platform that can alert operators to changes in the baseline, and 3) capture as many attributes about  
144 the assets as possible via the automated capabilities implemented.

145 In addition to these key tenets, this practice guide offers methods of asset management that address  
146 particular challenges in an OT environment, including the need to 1) account for geographically  
147 dispersed and remote assets, 2) have a consolidated view of the sum total of OT assets, and 3) be able  
148 to readily identify an asset’s disposition, or level of criticality, in the overall operational environment.

149 The capabilities showcased in this guide may provide energy-sector entities with the means to establish  
150 a comprehensive OT asset management baseline that can be monitored over the life of the asset.  
151 Implementation of these capabilities provides an automated inventory that can be viewed in near real  
152 time and can alert designated personnel to changes to the inventory. This will prove useful from both a  
153 cybersecurity and operational perspective, as it can otherwise be difficult to quickly identify any  
154 anomalies due to a cyber attack or operational issues. This document concerns itself primarily with  
155 cybersecurity; however, it is possible that other operational benefits may be realized.

## 156 1.1 Challenge

157 Many energy-sector companies face challenges in managing their assets, particularly when those assets  
158 are remote and geographically dispersed. Organizations may not have the tools to provide a current  
159 account of their assets or may not be leveraging existing capabilities required to produce an adequate  
160 inventory. Existing asset inventories may be static, onetime, or point-in-time snapshots of auditing  
161 activities conducted previously without a way to see the current status of those assets. Adding to the  
162 challenge, asset inventories may be kept in documents or spreadsheets that may be difficult to manually  
163 maintain and update, especially considering that inventories can change frequently. Without an  
164 effective asset management solution, organizations that are unaware of any assets in their  
165 infrastructure may be unnecessarily exposed to cybersecurity risks. It is difficult to protect what cannot  
166 be seen or is not known.

## 167 1.2 Solution

168 This NCCoE Cybersecurity Practice Guide demonstrates how energy organizations can use commercially  
169 available technologies that are consistent with cybersecurity standards, to address the challenge of  
170 establishing, enhancing, and automating their OT asset management.

171 This project demonstrates an OT asset management solution that consists of the following  
172 characteristics:

- 173     ▪ the ability to discover assets connected to a network
- 174     ▪ the ability to identify and capture as many asset attributes as possible to baseline assets, such as  
175 manufacturer, model, operating system (OS), internet protocol (IP) addresses, media access  
176 control (MAC) addresses, protocols, patch-level information, and firmware versions, along with  
177 physical and logical locations of the assets
- 178     ▪ continuous identification, monitoring, and alerting of newly connected devices, disconnected  
179 devices, and their connections to other devices (IP based and serial)
- 180     ▪ the ability to determine disposition of an asset, including the level of criticality (high, medium, or  
181 low) and its relation and communication to other assets within the OT network
- 182     ▪ the ability to alert on deviations from the expected operation of assets

183 Furthermore, this practice guide:

- 184     ▪ maps security characteristics to standards, regulations, and best practices from NIST and other  
185 standards organizations
- 186     ▪ provides a detailed architecture and capabilities that address asset management
- 187     ▪ describes best practices and lessons learned
- 188     ▪ provides instructions for implementers and security engineers to re-create the reference design



- 189       ▪ is modular and uses products that are readily available and interoperable with existing energy  
190       infrastructures

### 191   1.2.1 Relevant Standards and Guidance

192   In developing our example implementation, we were influenced by standards and guidance from the  
193   following sources, which can also provide an organization with relevant standards and best practices:

- 194       ▪ American National Standards Institute (ANSI)/International Society of Automation (ISA)-  
195       TR62443-2-3-2015, *Security for industrial automation and control systems Part 2-3: Patch*  
196       *management in the IACS environment*, 2015. [https://www.isa.org/store/isa-tr62443-2-3-2015,-](https://www.isa.org/store/isa-tr62443-2-3-2015,-security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-iacs-environment/40228386)  
197       [security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-](https://www.isa.org/store/isa-tr62443-2-3-2015,-security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-iacs-environment/40228386)  
198       [iacs-environment/40228386](https://www.isa.org/store/isa-tr62443-2-3-2015,-security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-iacs-environment/40228386)
- 199       ▪ ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for industrial automation and control systems Part*  
200       *3-3: System security requirements and security levels*, 2013. [https://www.isa.org/store/ansi/isa-](https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785)  
201       [62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-](https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785)  
202       [system-security-requirements-and-security-levels/116785](https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785)
- 203       ▪ ISA-62443-2-1-2009, *Security for Industrial Automation and Control Systems: Establishing an*  
204       *Industrial Automation and Control Systems Security Program*.  
205       [https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-](https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731)  
206       [for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-](https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731)  
207       [control-systems-security-program-/116731](https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731)
- 208       ▪ Center for Internet Security (CIS), *Critical Security Controls V6.0*. <https://cisecurity.org/controls>
- 209       ▪ Information Systems Audit and Control Association (ISACA), *Control Objectives for Information*  
210       *and Related Technology 5*, <https://www.isaca.org/cobit/pages/default.aspx>
- 211       ▪ NIST, *Cryptographic Standards and Guidelines*. [https://csrc.nist.gov/Projects/Cryptographic-](https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines)  
212       [Standards-and-Guidelines](https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines)
- 213       ▪ Department of Energy, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2),*  
214       *Version 1.1*, February 2014. [https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-](https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf)  
215       [Feb2014.pdf](https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf)
- 216       ▪ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12,  
217       2014. [https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)  
218       [framework-021214.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)
- 219       ▪ Internet Engineering Task Force (IETF) Request for Comments (RFC) 4254, *The Secure Shell (SSH)*  
220       *Connection Protocol*, January 2006. <https://www.ietf.org/rfc/rfc4254.txt>
- 221       ▪ IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008.  
222       <https://tools.ietf.org/html/rfc5246>
- 223       ▪ International Organization for Standardization (ISO) 55000:2014, *Asset Management—*  
224       *Overview, Principles and Terminology*, January 2014. <https://www.iso.org/standard/55088.html>

- 225       ▪ ISO 55001:2014, *Asset Management—Management Systems—Requirements*, January 2014.  
226       <https://www.iso.org/standard/55089.html>
- 227       ▪ ISO 55002:2014, *Asset Management—Management Systems—Guidelines for the Application of*  
228       *ISO 55001*, January 2014. <https://www.iso.org/standard/55090.html>
- 229       ▪ ISO/International Electrotechnical Commission (IEC) 19770-1:2017, *Information Technology—IT*  
230       *Asset Management—Part 1: IT Asset Management Systems—Requirements*, December 2017.  
231       <https://www.iso.org/standard/68531.html>
- 232       ▪ ISO/IEC 19770-5:2015, *Information Technology—IT Asset Management—Part 5: Overview and*  
233       *Vocabulary*, August 2015. <https://www.iso.org/standard/68291.html>
- 234       ▪ ISO/IEC 27001:2013, *Information Technology—Security Techniques—Information Security*  
235       *Management Systems—Requirements*, October 2013.  
236       <https://www.iso.org/standard/54534.html>
- 237       ▪ ISO/IEC 27019:2017, *Information Technology—Security Techniques—Information Security*  
238       *Controls for the Energy Utility Industry*, October 2017.  
239       <https://www.iso.org/standard/68091.html>
- 240       ▪ NIST Special Publication (SP) 800-40 Revision 3, *Guide to Enterprise Patch Management*  
241       *Technologies*, July 2013. <https://doi.org/10.6028/NIST.SP.800-40r3>
- 242       ▪ NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport*  
243       *Layer Security (TLS) Implementations*, April 2014. <https://doi.org/10.6028/NIST.SP.800-52r1>
- 244       ▪ NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and*  
245       *Organizations*, April 2013. <https://doi.org/10.6028/NIST.SP.800-53r4>
- 246       ▪ NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015.  
247       <https://doi.org/10.6028/NIST.SP.800-82r2>
- 248       ▪ NIST SP 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary*  
249       *Approach in the Engineering of Trustworthy Secure Systems*, November 2016.  
250       <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf>
- 251       ▪ NIST SP 1800-5 (DRAFT), *IT Asset Management*, 2014. [https://nccoe.nist.gov/library/it-asset-](https://nccoe.nist.gov/library/it-asset-management-nist-sp-1800-5-practice-guide)  
252       [management-nist-sp-1800-5-practice-guide](https://nccoe.nist.gov/library/it-asset-management-nist-sp-1800-5-practice-guide)
- 253       ▪ NIST SP 1800-7 (DRAFT), *Situational Awareness for Electric Utilities*, 2017.  
254       [https://nccoe.nist.gov/library/situational-awareness-electric-utilities-nist-sp-1800-7-practice-](https://nccoe.nist.gov/library/situational-awareness-electric-utilities-nist-sp-1800-7-practice-guide)  
255       [guide](https://nccoe.nist.gov/library/situational-awareness-electric-utilities-nist-sp-1800-7-practice-guide)
- 256       ▪ North American Electric Reliability Corporation (NERC), *Reliability Standards for the Bulk Electric*  
257       *Systems of North America*, last updated June 5, 2019.  
258       [http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.](http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf)  
259       [pdf](http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf)

## 260 1.3 Benefits

261 This NCCoE practice guide can help your organization:

- 262       ▪ reduce cybersecurity risk and potentially reduce the impact of safety and operational risks such  
263       as power disruption
- 264       ▪ develop and execute a strategy that provides continuous OT asset management and monitoring
- 265       ▪ respond faster to security alerts through automated cybersecurity event capabilities
- 266       ▪ implement current cybersecurity standards and best practices, while maintaining the  
267       performance of energy infrastructures
- 268       ▪ strengthen awareness of remote and geographically dispersed OT assets

269 Other potential benefits include:

- 270       ▪ additional data for organizations to address business needs such as budget planning and  
271       technology updates
- 272       ▪ improved situational awareness and strengthened cybersecurity posture

## 273 2 How to Use This Guide

274 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides  
275 users with the information they need to replicate the energy sector asset management (ESAM) solution  
276 that focuses on OT assets and does not include software inventory. This reference design is modular and  
277 can be deployed in whole or in part.

278 This guide contains three volumes:

- 279       ▪ NIST SP 1800-23A: *Executive Summary*
- 280       ▪ NIST SP 1800-23B: *Approach, Architecture, and Security Characteristics* – what we built and why  
281       **(you are here)**
- 282       ▪ NIST SP 1800-23C: *How-To Guides* – instructions for building the example solution

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

284 **Senior information technology (IT) executives, including chief information security and technology**  
285 **officers**, will be interested in the *Executive Summary*, NIST SP 1800-23A, which describes the following  
286 topics:

- 287       ▪ challenges that enterprises face in OT asset management
- 288       ▪ example solution built at the NCCoE
- 289       ▪ benefits of adopting the example solution

290 **Technology or security program managers** who are concerned with how to identify, understand, assess,  
291 and mitigate risk will be interested in this part of the guide, NIST SP 1800-23B, which describes what we  
292 did and why. The following sections will be of particular interest:

- 293       ▪ Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- 294       ▪ Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to  
295       cybersecurity standards and best practices.

296 You might share the *Executive Summary*, NIST SP 1800-23A, with your leadership team members to help  
297 them understand the importance of adopting a standards-based solution to strengthen their OT asset  
298 management practices by leveraging capabilities that may already exist within their operating  
299 environment or by implementing new capabilities.

300 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.  
301 You can use the how-to portion of the guide, NIST SP 1800-23C, to replicate all or parts of the build  
302 created in our lab. The how-to portion of the guide provides specific product installation, configuration,  
303 and integration instructions for implementing the example solution. We do not re-create the product  
304 manufacturers’ documentation, which is generally widely available. Rather, we show how we integrated  
305 the products together in our environment to create an example solution.

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

314 A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a  
315 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and  
316 success stories will improve subsequent versions of this guide. Please contribute your thoughts to  
317 [energy\\_nccoe@nist.gov](mailto:energy_nccoe@nist.gov)

## 318 **2.1 Typographic Conventions**

319 The following table presents typographic conventions used in this volume. Acronyms used in figures can  
320 be found in Appendix A.

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

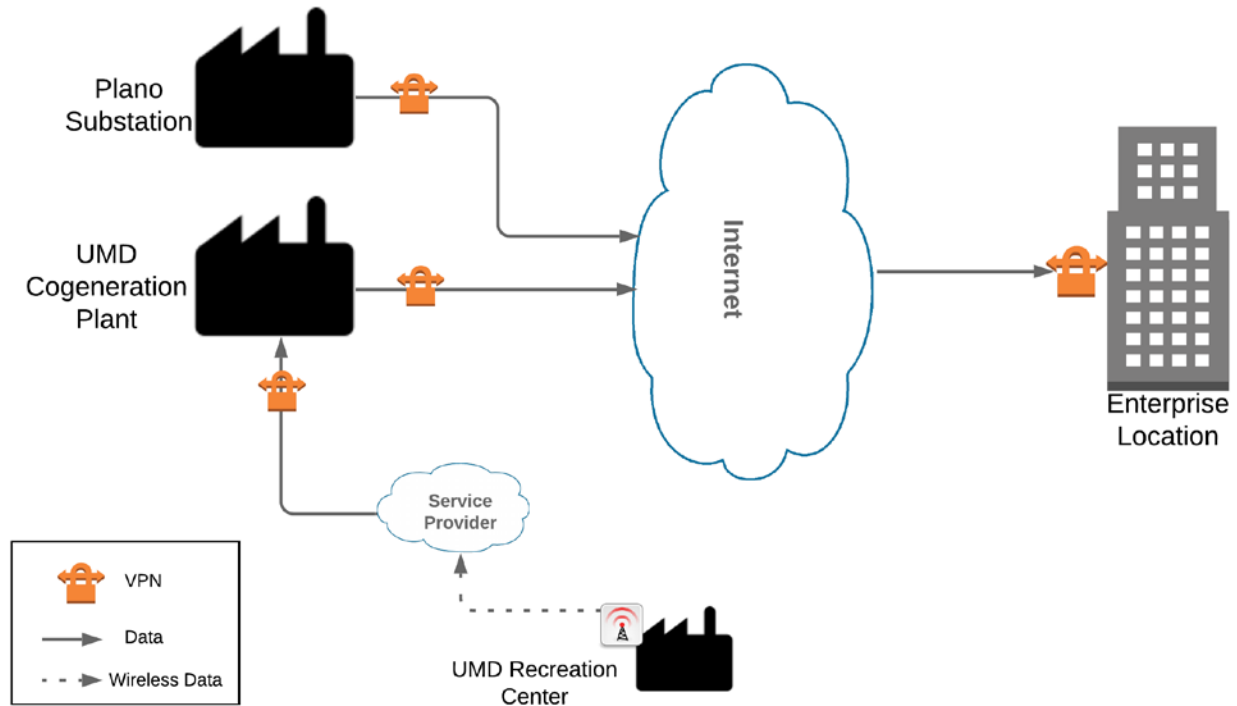
### 321 **3 Approach**

322 This practice guide highlights the approach the NCCoE used to develop the example implementation.  
 323 The approach includes a risk assessment and analysis, logical design, example build development,  
 324 testing, and security control mapping.

325 Based on discussions with cybersecurity practitioners in the energy sector, the NCCoE pursued the ESAM  
 326 Project to illustrate the broad set of capabilities available to manage OT assets. ICS infrastructures  
 327 consist of both IT and OT assets; however, this guide focuses primarily on OT devices due to their unique  
 328 challenges.

329 The NCCoE collaborated with its Community of Interest members and participating vendors to produce  
 330 an example architecture and example implementation. Vendors provided technologies that met project  
 331 requirements and assisted in installing and configuring those technologies. This practice guide highlights  
 332 the example architecture and example implementation, including supporting elements such as a  
 333 functional test plan, security characteristic analysis, lessons learned, and future build considerations.

334 To reasonably replicate a live ICS environment, the project consists of three distinct geographic  
 335 locations: 1) Plano, Texas; 2) College Park, Maryland; and 3) Rockville, Maryland. The Plano site is TDi  
 336 Technology's lab and represents a substation. The College Park site is the University of Maryland's  
 337 (UMD's) cogeneration plant. The Rockville site is the NCCoE's energy lab and represents the enterprise  
 338 location. The diagram in Figure 3-1 below visually represents the physical layout of the project.

339 **Figure 3-1 High-Level Topology**

340 Both the Plano substation and the UMD cogeneration plant are connected through the internet to the  
 341 NCCoE energy lab as the enterprise location. Each site is connected via a multipoint, always-on virtual  
 342 private network (VPN). This allows the NCCoE to aggregate data from multiple sites into a single  
 343 location, emulating multisite deployments found within the energy sector. The UMD site also consists of  
 344 a remote site connected via wireless technology. Each site is described in more detail in Section 4.  
 345

### 346 **3.1 Audience**

347 This guide is intended for individuals or entities responsible for cybersecurity of ICS and for those  
 348 interested in understanding an example architecture demonstrating asset management capabilities for  
 349 OT. It may also be of interest to anyone in industry, academia, or government who seeks general  
 350 knowledge of an OT asset management solution for energy-sector organizations.

### 351 **3.2 Scope**

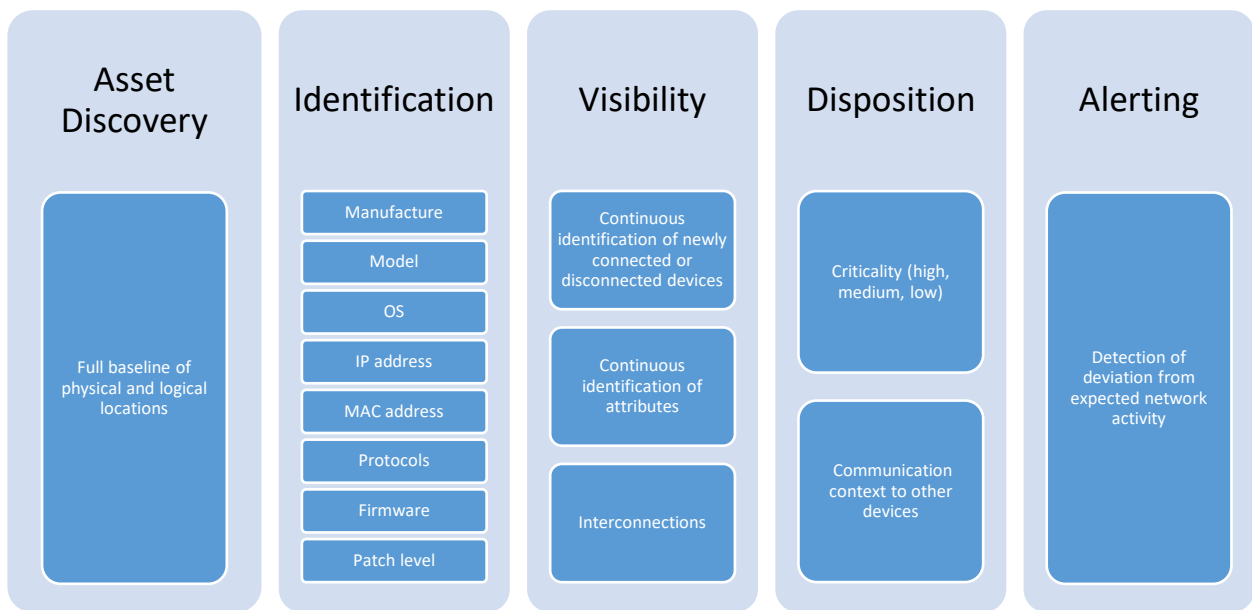
352 This document focuses on OT asset management, namely devices used to control, monitor, and  
 353 maintain generation, transmission, and distribution of various forms of energy. These devices include  
 354 PLCs, IEDs, engineering workstations, historians, and human-machine interfaces (HMIs). This document  
 355 does not consider software inventories or other physical assets that may be used to support energy  
 356 operations, such as buildings, trucks, and physical access control systems. The solution is designed to

357 deliver an automated OT asset inventory that provides asset information in real or near real time and  
358 can alert personnel of any changes to the inventory. Additionally, we focus on OT asset management  
359 from a cybersecurity perspective. Although operational benefits can be obtained from implementation  
360 of one or more of the components of this guide, we propose OT asset management as a fundamental  
361 and core aspect of properly maintaining an adequate cybersecurity posture.

362 This project addresses the following characteristics of asset management:

- 363     ▪ **Asset Discovery:** establishment of a full baseline of physical and logical locations of assets
- 364     ▪ **Asset Identification:** capture of asset attributes, such as manufacturer, model, OS, IP addresses,  
365       MAC addresses, protocols, patch-level information, and firmware versions
- 366     ▪ **Asset Visibility:** continuous identification of newly connected or disconnected devices and IP  
367       (routable and non-routable) and serial connections to other devices
- 368     ▪ **Asset Disposition:** the level of criticality (high, medium, or low) of a particular asset, its relation  
369       to other assets within the OT network, and its communication (including serial) with other  
370       devices
- 371     ▪ **Alerting Capabilities:** detection of a deviation from the expected operation of assets

372 **Figure 3-2 Asset Management Characteristics**



373

### 374 3.3 Assumptions

375 This project makes the following assumptions:

- 376       ▪ The solution will scale to real-world operating environments.
- 377       ▪ Some level of an asset management capability already exists within an organization.
- 378       ▪ Although we differentiate between IT and OT asset inventories, there may be some overlap.
- 379       ▪ All OT assets within an organization’s infrastructure, especially those considered critical, need to  
380 be identified, tracked, and managed.
- 381       ▪ OT networks are composed of numerous ICS devices (e.g., PLCs and IEDs) in addition to other  
382 vital components (e.g., engineering workstations, historians, and HMIs) that are typically  
383 installed on a Windows and/or Linux OS.

### 384 3.4 Risk Assessment

385 [NIST SP 800-30 Revision 1, \*Guide for Conducting Risk Assessments\*](#), states that risk is “a measure of the  
386 extent to which an entity is threatened by a potential circumstance or event, and typically a function of:  
387 (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of  
388 occurrence” [2]. The guide further defines risk assessment as “the process of identifying, estimating, and  
389 prioritizing risks to organizational operations (including mission, functions, image, reputation),  
390 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of  
391 an information system. Part of risk management incorporates threat and vulnerability analyses, and  
392 considers mitigations provided by security controls planned or in place.”

393 The NCCoE recommends that any discussion of risk management, particularly at the enterprise-level,  
394 begins with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for  
395 Information Systems and Organizations*—publicly-available material [3]. The Risk Management  
396 Framework guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from  
397 which we developed the project, the security characteristics of the build, and this guide [4].

398 The basis for our assessment of the risks associated with the challenges in asset management for OT is  
399 derived from [NIST SP 800-82 Revision 2, \*Guide to Industrial Control Systems \(ICS\) Security\*, Section 3](#).  
400 There are certain risks inherent in OT that are not found or that occur rarely in traditional IT  
401 environments, for example:

- 402       ▪ the physical impact a cybersecurity incident could cause to an energy organization’s OT assets  
403 and to the larger energy grid
- 404       ▪ the risk associated with non-digital control components within an OT environment and their lack  
405 of visibility within the organization

406 The NIST Cybersecurity Framework control mapping and related security controls found in this guide are  
407 based on these underlying risk concerns.



### 408 3.4.1 Threats

409 A threat is “any circumstance or event with the potential to adversely impact organizational operations”  
410 [5]. If an organization is not aware of its deployed OT assets, it is difficult to protect them and any other  
411 assets that may contain known or unknown vulnerabilities. Such lack of awareness increases the risk of  
412 exploitation of other networks, devices, and protocol-level vulnerabilities.

413 The Cybersecurity and Infrastructure Security Agency (CISA) ICS-Computer Emergency Readiness Team  
414 (CERT) defines cyber-threat sources to ICS as “persons who attempt unauthorized access to a control  
415 system device and/or network using a data communications pathway” [6]. Specifically, CISA ICS-CERT  
416 alongside NIST SP 800-82, *Guide to Industrial Control Systems Security* [1], identifies various malicious  
417 actors who may pose threats to ICS infrastructure [6]. These include:

- 418       ▪ foreign intelligence services—national government organizations whose intelligence-gathering  
419       and espionage activities seek to harm U.S. interests
- 420       ▪ criminal groups—such as organized crime groups that seek to attack for monetary gain
- 421       ▪ hackers—regarded as the most widely publicized; however, they often possess very little  
422       tradecraft to produce large-duration attacks
- 423       ▪ terrorists—adversaries of the U.S. who are less equipped in their cyber capabilities and therefore  
424       pose only a limited cyber threat

425 At the asset level, CISA ICS-CERT provides alerts and advisories when vulnerabilities for various OT assets  
426 are discovered that may pose a threat, if exploited, to ICS infrastructure [7].

427 The vulnerabilities are enumerated in the Common Vulnerabilities and Exposures vulnerability naming  
428 standard from the MITRE Corporation [8] and are organized according to severity by high, medium, and  
429 low, determined by the Common Vulnerability Scoring System standard from NIST. Common examples  
430 of such vulnerabilities include hard-coded credentials, unchanged default passwords, and encryption  
431 anomalies [9].

### 432 3.4.2 Vulnerabilities

433 CISA ICS-CERT defines a vulnerability as a defect that may allow a malicious actor to gain unauthorized  
434 access or interfere with normal operations of systems [10]. A vulnerability may exist inherently within a  
435 device or within the design, operation, and architecture of a system. This project does not address  
436 securing specific asset-based vulnerabilities at the device level. The key vulnerability addressed then in  
437 this guide is an organization not having visibility over its deployed assets.

438 NIST SP 800-82 categorizes ICS vulnerabilities into the following categories with examples [1]:

- 439       ▪ Policy and Procedure—incomplete, inappropriate, or nonexistent security policy, including its  
440       documentation, implementation guides (e.g., procedures), and enforcement

- 441       ▪ Architecture and Design—design flaws, development flaws, poor administration, and connections  
442       with other systems and networks
- 443       ▪ Configuration and Maintenance—misconfiguration and poor maintenance
- 444       ▪ Physical—lack of or improper access control, malfunctioning equipment
- 445       ▪ Software Development—improper data validation, security capabilities not enabled, inadequate  
446       authentication privileges
- 447       ▪ Communication and Network—nonexistent authentication, insecure protocols, improper firewall  
448       configuration

449 Knowledge of deployed assets is paramount in securing an organization’s ICS infrastructure and  
450 mitigating risks associated with asset-based vulnerabilities. The knowledge of an asset’s location and  
451 baselining of its behavior enable detection of anomalous behavior via network monitoring that may be  
452 the result of a successfully exploited vulnerability. The ability to reliably detect changes in asset behavior  
453 and knowing an asset’s attributes are key in responding to potential cybersecurity incidents.

### 454 3.4.3 Risk

455 Information-system-related security risks are those risks that arise from loss of confidentiality, integrity,  
456 or availability of information or information systems and that reflect potential adverse impacts to  
457 organizational operations (including mission, functions, image, or reputation), organizational assets,  
458 individuals, other organizations, and the nation. For the energy sector, a primary risk concern to OT is a  
459 lack of awareness of the devices running on the infrastructure. If OT assets cannot be properly  
460 accounted for, they cannot be protected. The following are tactical risks associated with lack of an OT  
461 asset management solution:

- 462       ▪ lack of knowledge of an existing asset
- 463       ▪ lack of knowledge of the asset’s physical and logical location
- 464       ▪ lack of a near-real-time comprehensive asset inventory
- 465       ▪ lack of knowledge of asset vulnerabilities and available patches
- 466       ▪ lack of data visualization and analysis capabilities that help dispatchers and a security analyst  
467       view device security events

468 **3.4.4 Security Control Map**

469 The NIST Cybersecurity Framework security Functions, Categories, and Subcategories that the reference design supports were  
 470 identified through a risk analysis [11]. Table 3-1 below maps NIST SP 800-53 Rev. 4 Security and Privacy Controls [12], along with  
 471 industry security references, to the NIST Cybersecurity Framework Subcategories addressed in this practice guide.

472 **Table 3-1 Security Control Map**

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
IDENTIFY (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried.	1	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8 PM-5	CIP-002-5.1a:R1, R2 CIP-010-2:R1, R2

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	<b>ID.RA-2:</b> Threat and vulnerability information is received from information-sharing forums and sources.	4	4.2.3, 4.2.3.9, 4.2.3.12	A.6.14	A.6.1.4	SI-5, PM-15, PM-16	n/a
PROTECT (PR)	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	<b>PR.DS-2:</b> Data-in-transit is protected.	13, 14	n/a	SR 3.1, SR 3.8, SR 4.1, SR 4.2	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8, SC-11, SC-12	CIP-005-5:R2 Part 2.2 CIP-011-2:R1 Part 1.2
		<b>PR.DS-6:</b> Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	2,3	n/a	SR 3.1, SR 3.3, SR 3.4, SR 3.8	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	SC-16, SI-7	CIP-010-2:R1, R2, R3

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	<b>Maintenance (PR.MA):</b> Maintenance and repair of industrial control and information system components are performed consistent with policies and procedures.	<b>PR.MA-1:</b> Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools.	n/a	4.3.3.3.7	n/a	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6	MA-2, MA-3, MA-5, MA-6	CIP-10-2:R1
		<b>PR.MA-2:</b> Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	3, 5	4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8	n/a	A.11.2.4, A.15.1.1, A.15.2.1	MA-4	CIP-010-2:R1

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443-2-1:2009	ISA 62443-3-3:2013	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	<b>PR.PT-4:</b> Communications and control networks are protected.	8, 12, 15	n/a	SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	A.13.1.1, A.13.2.1, A.14.1.3	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	CIP-005-5:R1 Part 1.2
<b>DETECT (DE)</b>	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected in a timely manner, and the	<b>DE.AE-1:</b> A baseline of network operations and expected data flows for users and systems is	1, 4, 6, 12, 13, 15, 16	4.4.3.3	n/a	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	AC-4, CA-3, CM-2, SI-4	CIP-010-2:R1

Informative References								
Function	Category	Subcategory	CIS CSC 2016	ISA 62443- 2-1:2009	ISA 62443- 3- 3:2013	ISO/IEC 27001: 2013	NIST SP 800-53 Rev. 4	NERC CIP Standards
	potential impact of events is understood.	established and managed.						
		<b>DE.AE-3:</b> Event data is aggregated and correlated from multiple sources and sensors.	1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16	n/a	SR 6.1	A.12.4.1, A.16.1.7	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	CIP-008-5:R1.4 CIP-010-2:R1

### 473 3.4.5 National Initiative for Cybersecurity Education Workforce Framework

474 This guide details the work roles needed to perform the tasks necessary to implement the cybersecurity  
 475 Functions and Subcategories detailed in the reference design. The work roles are based on the [National  
 476 Initiative for Cybersecurity Education](#) (NICE) Workforce Framework [13].

477 Table 3-2 maps the Cybersecurity Framework Categories implemented in the reference design to the  
 478 NICE work roles. Note that the work roles defined may apply to more than one NIST Cybersecurity  
 479 Framework Category.

480 For more information about NICE and other work roles, the NIST SP 800-181, *NICE Cybersecurity  
 481 Workforce Framework*, is available at [https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-  
 482 181.pdf](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf).

483 **Table 3-2 NIST NICE Work Roles Mapped to the Cybersecurity Framework: ESAM**

Work Role ID	Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
OM-STS-001	Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).	Operate and Maintain	Customer Service and Technical Support	ID.AM-1
PR-VAM-001	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.	Protect and Defend	Vulnerability Assessment Management	ID.RA-2
OM-DTA-002	Information Systems	Examines data from multiple disparate sources, with the goal of providing security and privacy	Operate and Maintain	Data Administration	PR.DS-2



Work Role ID	Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
	Security Developer	insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.			
PR-CDA-001	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments, to mitigate threats.	Protect and Defend	Cyber Defense Analysis	PR.DS-2
OM-DTA-001	Database Administrator	Administers databases and data management systems that allow secure storage, query, protection, and utilization of data.	Operate and Maintain	Data Administration	PR.DS-6
OM-ADM-001	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g., installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).	Operate and Maintain	Systems Administration	PR.MA-1
SP-TRD-001	Research & Develop-	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated.	Securely Provision	Technology R&D	PR.MA-2

Work Role ID	Work Role	Work Role Description	Category	Specialty Area	Cybersecurity Framework Subcategory Mapping
	ment Specialist	Conducts comprehensive technology research to evaluate potential vulnerabilities in cyber space systems.			
SP-ARC-002	Security Architect	Ensures stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.	Securely Provision	Systems Architecture	PR.PT-4
SP-ARC-001	Enterprise Architect	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.	Securely Provision	Systems Architecture	DE.AE-1
CO-OPS-001	Cyber Operator	Conducts collection, processing, and geo-location of systems to exploit, locate, and track targets of interest. Performs network navigation and tactical forensic analysis and, when directed, executes on-net operations.	Collect and Operate	Cyber Operations	DE.AE-3

484 **3.5 Technologies**

485 Table 3-3 lists all of the technologies and their role in this project and provides a mapping among the  
 486 generic application term, the specific product used, and the security control(s) that the product  
 487 provides. Refer to Table 3-1 for an explanation of the NIST Cybersecurity Framework Subcategory codes.

488 **Table 3-3 Products and Technologies**

Capability	Product	Project Role	Cybersecurity Framework Subcategories
Asset discovery and monitoring	Dragos Platform v1.5	Passive asset discovery, threat detection, and incident response for ICS networks	ID.AM-1, DE.AE-1, DE.AE-2
Data collection and inventory tool	ForeScout CounterACT v8.0.1	CounterACT appliance collects data from one location and reports back to the CounterACT Enterprise Manager on the enterprise network.	ID.AM-1, DE.AE-1, DE.AE-2
Asset identification, analysis, and baselining	FoxGuard Solutions Patch and Update Management Program v1	Patch availability reporting is an ICS security patch management report that consolidates patch sources into one source.	ID.RA-2
		Vulnerability Notification Report is curated specific to your asset list, putting critical security vulnerability data at your fingertips for your assets.	

Capability	Product	Project Role	Cybersecurity Framework Subcategories
		ICS Update Tool consumes monthly security-patch-availability reports and translates them into a dashboard of business analytics. This visualization of patch data provides near-real-time decision-making.	
Secure remote access	KORE Wireless, Inc. Cellular Connectivity with Cellular Gateway v2.0	Provide a secure bridge from remote devices via one or more long-term evolution (LTE) networks to the application server on the ICS network that gathers the data from the remote asset.	PR.DS-2, PR.MA-1
Analyzing and visualizing machine data	Splunk Enterprise v7.1.3	Provides capabilities for data collection, indexing, searching, reporting, analysis, alerting, monitoring, and visualization.	DE.AE-1, DE.AE-2
Data Collection, monitoring, and analysis	TDi Technologies, Inc. ConsoleWorks v5.2-0u1	Provides data collection and interfacing with serial conversion devices. Also provides analysis and reporting.	ID.AM-1, PR.DS-2
Anomaly detection	Tripwire Industrial Visibility v3.2.1	Passively scans the industrial control environments at two locations. Tripwire Industrial Visibility builds a baseline of assets and network traffic between those assets then alerts on anomalous traffic.	ID.AM-1, DE.AE-1, DE.AE-2

## 489 **4 Architecture**

490 The project architecture focuses on the key capabilities of asset management: asset discovery,  
491 identification, visibility, disposition, and alerting capabilities. When combined, these capabilities allow  
492 an organization to have a more robust understanding, not only of its device inventory and architecture  
493 but also of the current state of its devices and automated alerts for anomalous behavior of its assets.

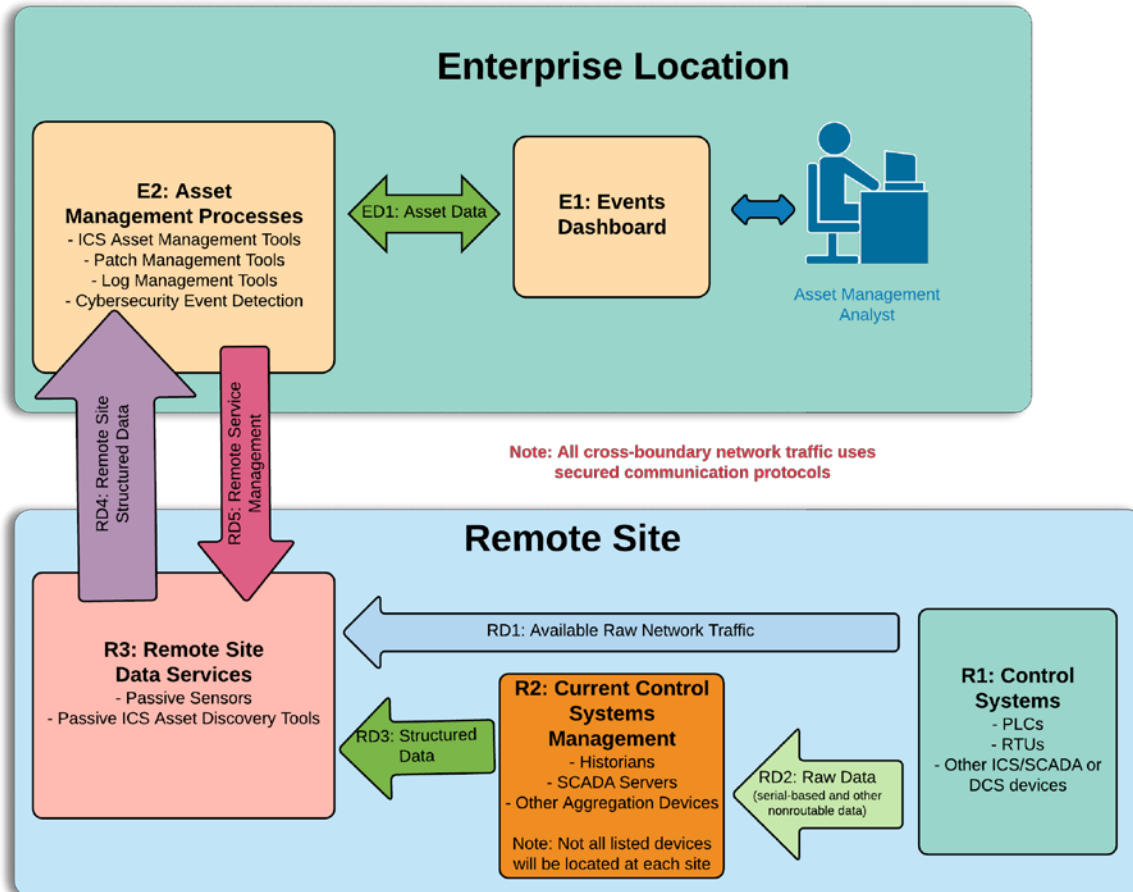
494 This section presents a high-level architecture, a reference design, detailed topologies, and a  
495 visualization dashboard for implementing such a solution. The high-level architecture is a generic  
496 representation of the reference design. The reference design includes a broad set of capabilities  
497 available in the marketplace, to illustrate the ESAM capabilities noted above, that an organization may  
498 implement. Each topology depicts the physical architecture of the example solution. The asset  
499 management dashboard displays the network connectivity between devices and a list of known assets  
500 within the network. The NCCoE understands that an organization may not need all of the capabilities. An  
501 organization may choose to implement a subset of the capabilities, depending on its risk management  
502 decisions.

### 503 **4.1 Architecture Description**

#### 504 **4.1.1 High-Level Architecture**

505 The ESAM solution is designed to address the Cybersecurity Framework Functions, Categories, and  
506 Subcategories described in Table 3-1 and is depicted in Figure 3-1.

507 Figure 4-1 High-Level Architecture



508

509 Figure 4-1 depicts the high-level architecture for monitoring ICS assets, including those located in  
 510 remote sites. While one remote site is depicted, the architecture allows inclusion of multiple remote  
 511 sites. This allows a repeatable and standard framework of deployment and strategy for multiple remotes  
 512 sites, which can be tailored to individual site needs.

513 The high-level architecture (Figure 4-1) above is best described starting at the remote site control  
 514 systems. Information at this level appears as raw ICS-based data (including serial communications), ICS-  
 515 based network traffic (Distributed Network Protocol 3, Modbus, EtherIP, etc.), or raw networking data  
 516 (Transmission Control Protocol [TCP]/User Datagram Protocol, internet control message protocol  
 517 [ICMP], address resolution protocol [ARP], etc.). Serial communications are encapsulated in network  
 518 protocols. All of this data is collected and stored by the remote site data servers (R3) object. These  
 519 sensors are collecting ICS network traffic and raw IP networking data from the control systems (R1) and  
 520 current control systems management (R2). Data collected by the remote site data servers (R3) is sent

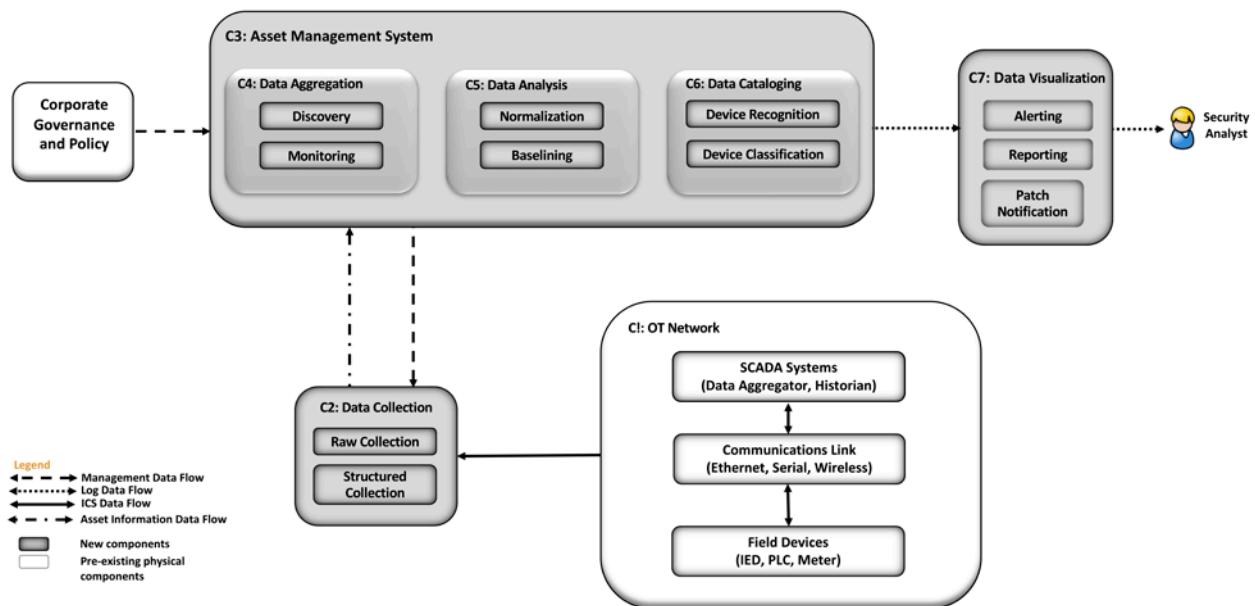
521 through a VPN tunnel to listening servers in the enterprise location. Once data arrives from the remote  
 522 site at the enterprise-data-collection server, it is ingested into the assets management processes (E2).  
 523 These tools aggregate the remote site structured data (RD4) from multiple sites, to build a holistic  
 524 picture of the health and setup of the network. Next, both events and asset data from the asset  
 525 management processes (E2) tools are sent directly to the events dashboard (E1). In the events  
 526 dashboard (E1), events are displayed in an easily digestible format for an analyst.

527 In the event of needed configuration of remote site data servers (R3), remote service management  
 528 connections can be established between the asset management processes (E2) and the remote site data  
 529 servers (R3). This traffic is routed through the aforementioned VPN tunnel and is terminated inside the  
 530 remote site data servers (R3). This allows configuration solely in the remote site data servers (R3),  
 531 utilizing the established VPN tunnel for security, without allowing access to either the current control  
 532 systems management (R2) or control systems (R3) devices.

### 533 4.1.2 Reference Architecture

534 The reference architecture shown in Figure 4-2 depicts the detailed ESAM design, including relationships  
 535 among the included capabilities.

536 **Figure 4-2 Reference Architecture**



537 As indicated by the legend, different lines represent different types of data flowing into the various  
 538 components. ICS data is depicted with solid lines. Management data flow is depicted with the dashed  
 539 line. Asset information is depicted with a dot-dash line. Log data is depicted with a dotted line. Each of  
 540 the clear shapes represents a preexisting or optional component. The OT network consists of devices  
 541

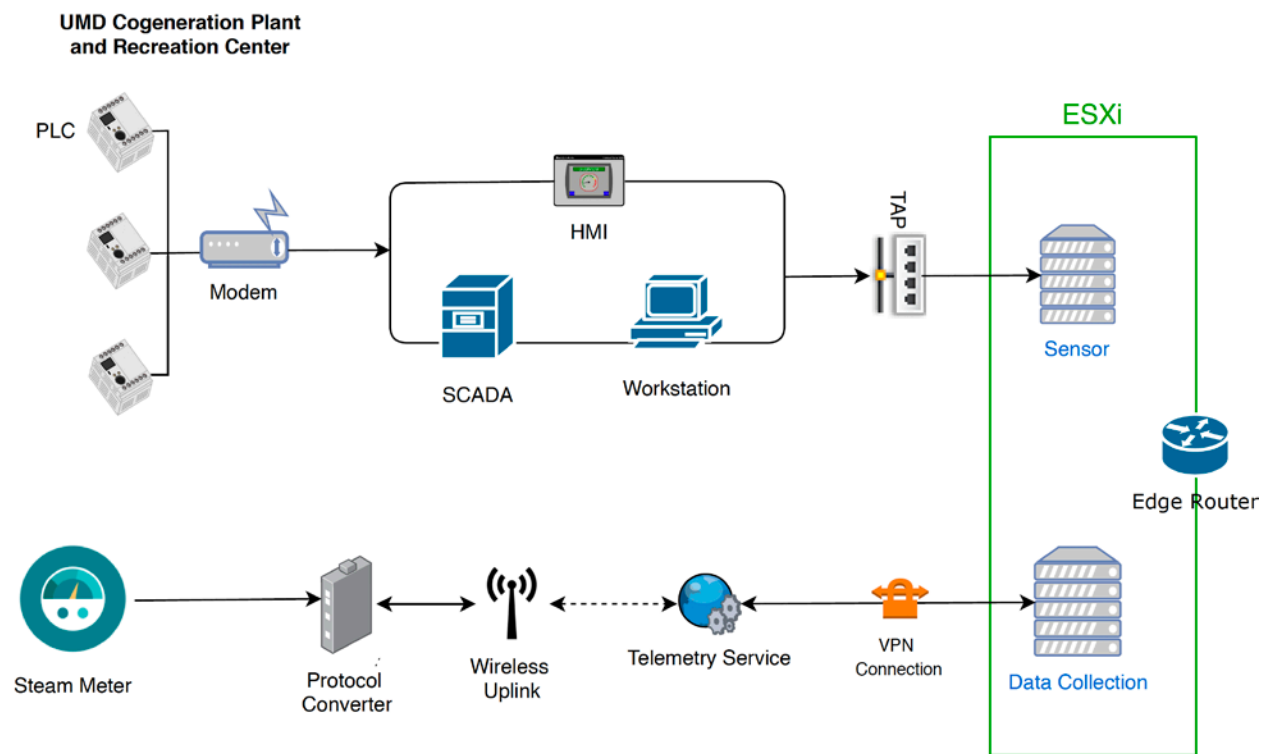
542 composed of ICS-based data, ICS network traffic, or raw networking data. The example implementation  
543 includes the ICS devices in both the UMD cogeneration plant as well as TDi's lab in Plano, Texas, in the  
544 Reference Design OT Network categorization group.

545 Another component that utilizes the ESAM solution is corporate governance and policy. Corporate  
546 governance and policy may guide different aspects of the ESAM solution, such as how long records will  
547 be maintained, how to classify devices, and how often reports are run. Each organization's governance  
548 and policy will be determined by organizational risk tolerance and management decisions.

549 The components of the ESAM reference design, Figure 4-2, come together to form the asset  
550 management system. Each capability is described below:

- 551       ▪ The data collection capability captures the data from the in-place OT network. Data can be  
552       collected in raw packet capture form as well as any structured form that may come from tools  
553       or devices within the OT network. This capability can be configured through normal remote  
554       management channels, to ensure the most precise and policy-informed data ingestion needed  
555       for the organization.
- 556       ▪ The data aggregation component ingests data from the data collection capability and utilizes  
557       both the discovery capability and monitoring capability. The monitoring capability tracks  
558       network activity collected from the OT network. After a training period, the discovery capability  
559       identifies new devices when new IP addresses and MAC addresses are communicating on the  
560       network.
- 561       ▪ The data analysis capability utilizes both a normalization capability to bring in traffic from  
562       multiple sites into a single picture and a baselining capability to establish an informed standard  
563       of how an asset's network traffic should behave under normal operations.
- 564       ▪ The device cataloging capability simultaneously uses information from the data collection  
565       component. The device recognition capability identifies different types of devices within the  
566       system. Devices are identified by MAC address to determine the manufacturer or by deep-  
567       packet inspection to determine the model, serial number, or both of a device if the raw ICS  
568       protocol contains such information. Figure 4-4 below depicts the option for determining the  
569       serial and model number of a device, when scanning is technically feasible. The organization  
570       should verify compliance with relevant regulations before deploying this aspect of the solution.  
571       Next, the device classification capability can determine the level of criticality for devices, both  
572       automatically as well as manually if requested.
- 573       ▪ The data visualization capability displays data from components of the asset management  
574       system. Here, the alerting capability notifies analysts of incidents, including deviations to normal  
575       behaviors. This component also includes the reporting capability to generate timely reports  
576       needed in operations of the organization. One key feature of the reporting capability is the  
577       ability to report when a cybersecurity patch is available.



578 **4.2 Example Solution**579 **4.2.1 UMD Site Topology**580 **Figure 4-3 UMD In-Depth Topology**

581

582 UMD's cogeneration plant was utilized as one of the remote sites for the project. At the site, the control  
 583 system network consists of PLCs, networking equipment, operator workstations, HMIs, and Supervisory  
 584 Control and Data Acquisition (SCADA) servers. The control system network is fitted with network test  
 585 access points (TAPs) to collect network traffic from the ICS network. This traffic feeds into a port on the  
 586 ESXi server that is mapped to a virtual Switched Port Analyzer (SPAN) switch. Each sensor monitors  
 587 traffic on the SPAN switch. The sensor collects the raw data, processes network packets, performs deep-  
 588 packet inspection, and forwards structured data through the edge router to an asset management  
 589 server, as shown above in Figure 4-3.

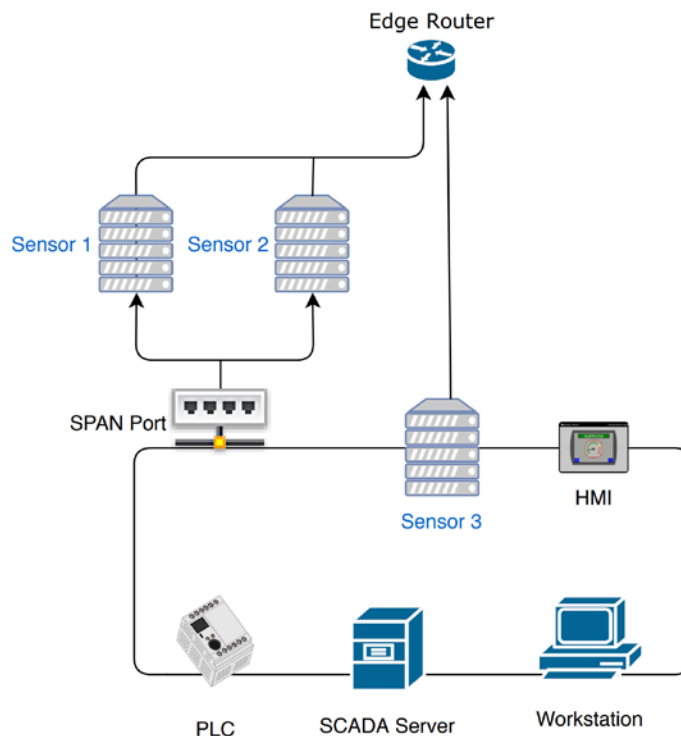
590 The UMD site topology also consists of a steam-meter asset in the solution. The steam meter utilizes  
 591 highway addressable remote transducer (HART) communication protocol and is in a building separate  
 592 from the cogeneration plant. The steam meter is wired to a protocol converter that converts HART  
 593 communications to Ethernet. The wireless uplink is a cellular connection device providing wireless

594 connectivity to the telemetry service provider. A VPN connection links the data collection server to the  
 595 telemetry service provider, which allows data to be read from the steam meter.

596 Following collection of data from both the control system network and the steam meter to the VMware  
 597 ESXi servers, the data is then sent through a VPN tunnel out of the edge router to the enterprise  
 598 location. A description of the enterprise location is found in Section 4.2.3

## 599 4.2.2 Plano Site Topology

600 **Figure 4-4 Plano In-Depth Topology**

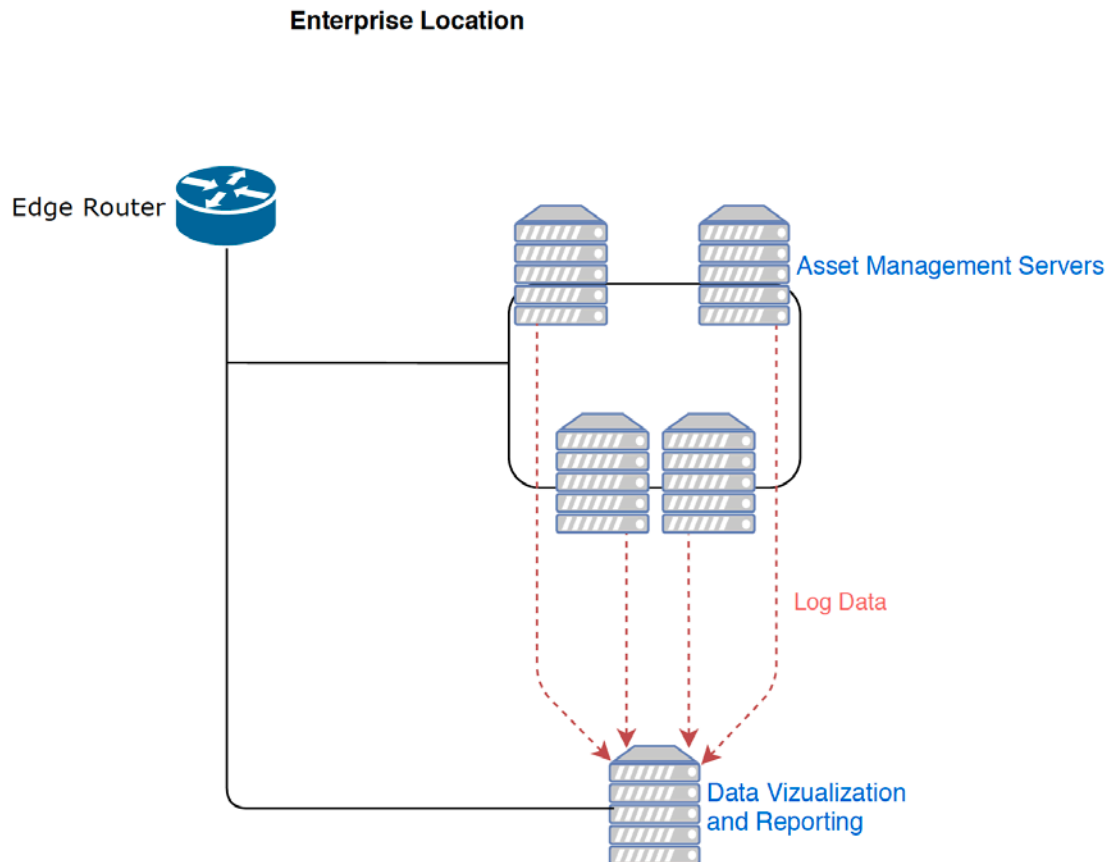


601

602 The lab in Plano, Texas, depicted in Figure 4-4, represents a second site and is set up to collect  
 603 information from a variety of devices communicating on a network. The Plano site consist of PLCs, HMIs,  
 604 SCADA servers, and workstations. Sensor 1 and Sensor 2 passively monitor devices via a SPAN port. Both  
 605 sensors are collecting data. Sensor 3 has a network interface located on the control network, to  
 606 demonstrate the ability to actively scan devices if desired. Actively scanning devices requires scripts to  
 607 interrogate devices by using a method supported by the device. Methods may include using login  
 608 credentials or combinations of commands to retrieve data from the device. Typically, similar devices  
 609 from the same manufacturer can utilize similar scripts. Otherwise, most device types require unique  
 610 scripts. Most devices can be scanned to retrieve the model number, serial number, and more. All three  
 611 sensors transfer their data, via the edge router, through a VPN to the enterprise location.

## 612 4.2.3 Enterprise Location Topology

613 Figure 4-5 Enterprise In-Depth Topology



614

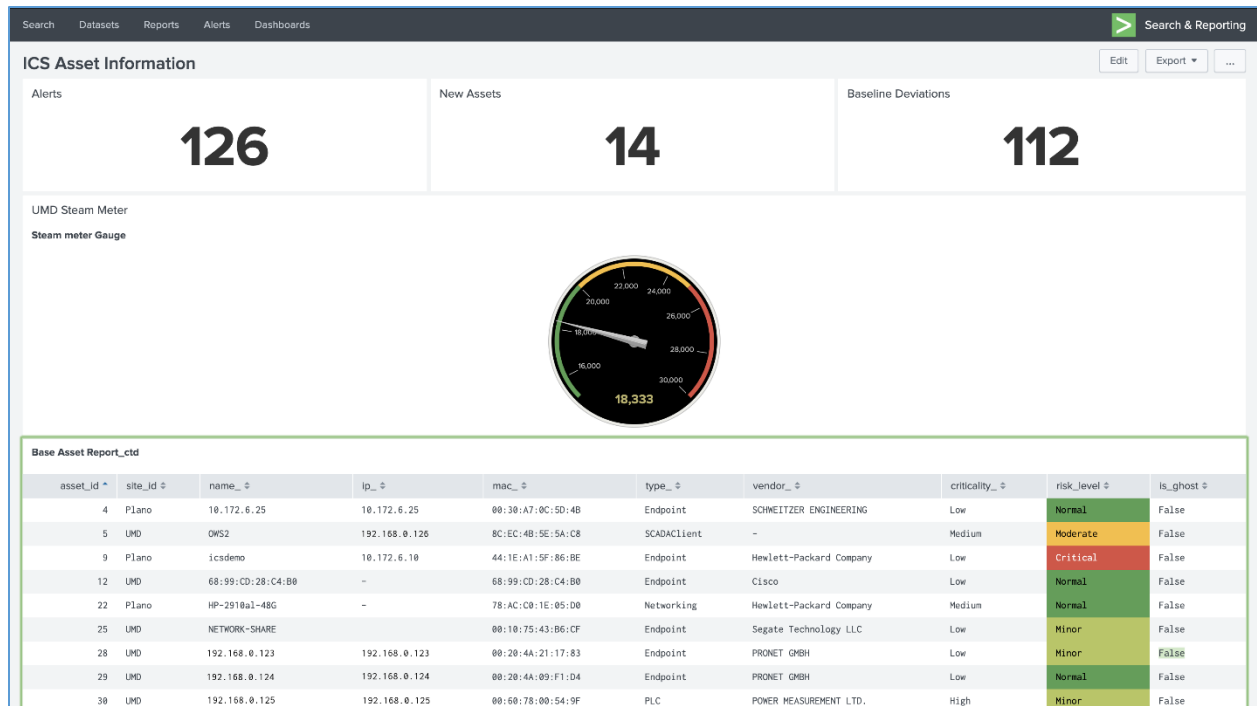
615 The enterprise location in the NCCoE Lab (Rockville, Maryland), depicted in Figure 4-5, represents a  
 616 central operations center for an organization. Data from both the Plano and UMD sites is sent to the  
 617 enterprise location, for processing through the asset management servers.

618 The asset management servers aggregate the data, analyze the data, and catalog the details about the  
 619 assets currently on the network, incorporating both remote sites. Portions of this data are logged and  
 620 forwarded to the data visualization and reporting server. First, alerts on new baselines and baseline  
 621 deviations are forwarded via syslog. Alerts on asset changes, including new assets, changes in IP and  
 622 MAC addresses, and offline assets, are forwarded via syslog along with identified threats to those assets.  
 623 Last, a comma-separated value (CSV) asset report is automatically forwarded on a regular basis to  
 624 maintain an updated and near-real-time asset inventory.

625 **4.2.4 Asset Management Dashboard**

626 Note: IP addresses shown in the figures below have been sanitized.

627 **Figure 4-6 Asset Dashboard: Asset Characteristics**



628

629 Figure 4-6 showcases how the asset management dashboard displays a list of known assets within the

630 network. At the top of the dashboard, the total amount of alerts, number of new assets, and number of

631 baseline deviations detected from both the Plano and UMD locations are listed. The gauge displays the

632 meter reading from the Yokogawa steam meter at UMD. Information collected on each asset (including

633 IP address, MAC address, asset type, criticality, and risk level) is displayed in the table.

634 Figure 4-7 Asset Dashboard: Asset Communications

UMD communications

first table from tiv baseline data

from Apr 1 through Jun 1, 2019

46,344 events (4/1/19 12:00:00.000 AM to 6/2/19 12:00:00.000 AM)

46,344 results 100 per page

shost	src	smac	dhost	dst	dmac	Type	Port	Comms	msg
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	N/A	Broadcast / Multicast	UDP / 3702	Other	UDP from any port to port 3702
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	N/A	Broadcast / Multicast	UDP / 3702	Other	UDP from any port to port 3702
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	00:20:4a:21:19:30	Endpoint: Other	None	Network	ARP : Request for ipv4 address 192.168.0.123
N/A	192.168.0.124	00:20:4a:21:19:30	CITECT	192.168.0.123	54:bf:64:7b:02:3a	SCADA Server: CITECT,GE,Modbus,Rockwell	None	Network	ARP : Response for ipv4 address 192.168.0.123 with mac address 00:20:4a:21:19:30
CITECT	192.168.0.123	54:bf:64:7b:02:3a	N/A	192.168.0.124	N/A	Broadcast / Multicast	UDP / 3702	Other	UDP from any port to port 3702

635

636 Figure 4-7 showcases the asset management dashboard visualization of network connectivity among  
637 devices. The visualization shows the interconnection among known assets, listing types of  
638 communications and messages.

639 Figure 4-8 Asset Dashboard: Asset Details, UMD

asset_id	site_id	name	ip	mac	type	vendor	criticality	risk_level	is_ghost	Device	Platform
31	5	192.168.0.123	192.168.0.123	00:60:78:00:54:9E	PLC	POWER MEASUREMENT LTD.	High	Minor	False	CHP GT1 Meter Gas Turbine 1	GE 90-70 (firmware unknown)
30	5	192.168.0.124	192.168.0.124	00:60:78:00:54:9F	PLC	POWER MEASUREMENT LTD.	High	Minor	False	CHP BPSTG Meter Back Presure Steam Turbine	Potentially Woodward ProTech 203, not 100%
29	5	192.168.0.125	192.168.0.125	00:20:4A:09:F1:D4	Endpoint	PRONET GMBH	Low	Normal	False	Mowatt Substation Ethernet to RS-485	Lantronix Converter
28	5	192.168.0.126	192.168.0.126	00:20:4A:21:17:83	Endpoint	PRONET GMBH	Low	Minor	False	CHP Ethernet to RS-485 Converter	Lantronix Converter
25	5	NETWORK-SHARE	192.168.0.127	00:10:75:43:B6:CF	Endpoint	Segate Technology LLC	Low	Minor	False	Network Accessible Storage, not 100%	Windows ME
5	5	OWS2	192.168.0.128	8C:EC:4B:5E:5A:C8	SCADAClient	-	Medium	Moderate	False	CHP Station 2 Center	Windows 7
33	5	192.168.0.130	192.168.0.130	00:20:4A:21:18:C9	Endpoint	PRONET GMBH	Low	Normal	False	Mowatt Substation Ethernet to RS-485	Lantronix Converter

640

641 Figure 4-8 showcases more detailed information about assets at the UMD location. The asset  
 642 information is supplemented with known data about the devices.

643 Figure 4-9 Asset Dashboard: Asset Details, Plano

Search Datasets Reports Alerts Dashboards Search & Reporting

Plano Detailed report for Patch info

outputs to /opt/splunk/var/run/splunk/csv

Year to date

✓ 33 events (1/1/19 12:00:00.000 AM to 9/12/19 11:24:06.000 AM)

12 results 100 per page

Asset Id	IP	Mac	Vendor	Operating System	Serial_Number	Version
75	10.0.0.11	00:60:2E:00:40:FF	CYCLADES CORPORATION	-	SG1131R0BH	W.15.14.0014
61	10.0.0.12	68:05:CA:36:38:65	Intel Corporate	Windows 10		10.0.17134
59	10.0.0.13	00:30:A7:0A:54:79	SCHWEITZER ENGINEERING	-	1141920246	SEL-3622-R204-V2-Z010006-D20170510
77	10.0.0.14	00:04:BF:B1:7B:D2	VersaLogic Corp.	-	14291	2.0.34
81	10.0.0.15	00:30:A7:0A:57:22	SCHWEITZER ENGINEERING	-	1141920245	SEL-3620-R204-V2-Z010006-D20170510
107	10.0.0.16	00:0A:DC:14:42:60,00:0A:DC:14:42:62	RuggedCom Inc.	-		4.1.1
93	10.0.0.17	00:D0:4F:00:18:15	BITRONICS, INC.	-	924455	02.15.1
108	10.0.0.18	00:0A:DC:3A:69:80,00:0A:DC:3A:69:82	RuggedCom Inc.	-		v2.15.1
109	10.0.0.19	00:30:A7:17:49:69	SCHWEITZER ENGINEERING	-	1173460197	SEL-451-5-R321-V0-Z024012-D20171008
57	10.0.0.20	00:30:A7:12:DF:95	SCHWEITZER ENGINEERING	-	1163641270	SEL-3530-4-R136-V1-Z001001-D20161026
40	10.0.0.21	00:30:A7:12:BC:FB	SCHWEITZER ENGINEERING	-		SEL-700G-R110-V0-Z005002-D20160831
69	10.0.0.22	00:30:A7:17:38:27	SCHWEITZER ENGINEERING	-	1173400079	SEL-3610-R205-V0-Z011006-D20171026

644

645 Figure 4-9 showcases more detailed information about assets at the Plano location. The asset

646 information is supplemented via automated scripts and manual entry. This report is normalized and

647 then analyzed for patch notifications.

## 648 5 Functional Test Plan

### 649 5.1 Test Cases

650 The below test cases demonstrate integration of capabilities for use in the project. For reference,

651 components of Figure 4-1 High-Level Architecture and Figure 4-2 Reference Architecture are included

652 with their corresponding identifier tags in parenthesis.

#### 653 5.1.1 ESAM-1: New Device Attached

Description
<ul style="list-style-type: none"> <li>▪ Device attached to the network that has not appeared previously.</li> <li>▪ ESAM solution will identify and alert on the new device.</li> </ul>

<b>Procedure</b>	<ul style="list-style-type: none"> <li>▪ Connect laptop to UMD-based Remote Site Data Server (R3) network.</li> <li>▪ Request Dynamic Host Configuration Protocol for device, and generate minimal network traffic.</li> <li>▪ Monitor Events Dashboard (E1) for identification of new device.</li> </ul>
<b>Architectural Requirements</b>	<ul style="list-style-type: none"> <li>▪ Raw network traffic appears on network at remote site.</li> <li>▪ New device generates known network traffic with new connection (ARP/Reverse Address Resolution Protocol [RARP]), High-bandwidth Digital Content Protection, TCP connections, etc.).</li> <li>▪ Network traffic is captured by sensors at Remote Site Data Servers (R3).</li> <li>▪ Servers pass alerted data to enterprise location Asset Management Processes (E2).</li> <li>▪ Alerts are aggregated and displayed to user in the Events Dashboard (E1).</li> </ul>
<b>Capabilities Requirements</b>	<ul style="list-style-type: none"> <li>▪ Network data collection via TAPs and SPAN ports on network device.</li> <li>▪ Routing of network data through Asset Management (C3) sensors.</li> <li>▪ Data Collection (C2) utilizing discovery and normalization processes for remote site asset information data flow.</li> <li>▪ Alerting and analytics based on asset information data flow structured by the data collection capability presented to the analyst.</li> </ul>
<b>Expected Results</b>	Events Dashboard (E1) will notify analyst via alerts for new devices.
<b>Actual Results</b>	<ul style="list-style-type: none"> <li>▪ New device is created on network.</li> <li>▪ Baseline monitoring system recognizes new device on network.</li> <li>▪ Alert is created on Events Dashboard (E1).</li> </ul>
<b>Overall Result</b>	PASS



## 654 5.1.2 ESAM-2: Vulnerability Notification

<b>Description</b>	<ul style="list-style-type: none"> <li>▪ New vulnerability is released, affecting devices within the Control Systems (R1).</li> <li>▪ ESAM solution can recognize affected devices and alert analysts to: <ul style="list-style-type: none"> <li>• potential vulnerable devices</li> <li>• current status of devices</li> <li>• any potential patching for devices</li> </ul> </li> </ul>
<b>Procedure</b>	<ul style="list-style-type: none"> <li>▪ Utilizing established asset list contained within the Asset Management Process (E2), create sanitized device list.</li> <li>▪ Import device list to the Patch Management Tools inside the Asset Management Process (E2) for structuring.</li> <li>▪ Submit structured device list to the Patch Management service.</li> <li>▪ Ingest returned Patch Management report to Events Dashboard (E1) for alerting a reporting to analyst.</li> </ul>
<b>Architectural Requirements</b>	<ul style="list-style-type: none"> <li>▪ Assets cataloged within the Asset Management Process (E2), including vendor, device type, firmware version, and other pertinent information.</li> <li>▪ Deliver device list with above information to the Patch Management tools.</li> <li>▪ Deliver structured device list to the Patch Management service.</li> <li>▪ Ingest report from the Patch Management service to Events Dashboard (E1).</li> </ul>
<b>Capabilities Requirements</b>	<ul style="list-style-type: none"> <li>▪ Data Cataloging (C6) components track asset-specific information.</li> <li>▪ Vulnerability reports are compared with data included in submitted structured reports based on Data Cataloging (C6) information.</li> </ul>
<b>Expected Results</b>	Analyst will receive reported information in Events Dashboard and will be able to identify potentially vulnerable devices.

<b>Actual Results</b>	<ul style="list-style-type: none"> <li>▪ Device list is created and normalized.</li> <li>▪ List is delivered to vendor for analysis.</li> <li>▪ Vendor-delivered results added to dashboard.</li> <li>▪ Events Dashboard notifies analyst of potentially vulnerable devices.</li> </ul>
<b>Overall Result</b>	PASS

655 **5.1.3 ESAM-3: Device Goes Offline**

<b>Description</b>	<ul style="list-style-type: none"> <li>▪ Device previously attached to the network no longer appears on the network.</li> <li>▪ ESAM solution will identify and alert on the loss of device.</li> </ul>
<b>Procedure</b>	<ul style="list-style-type: none"> <li>▪ Option 1:             <ul style="list-style-type: none"> <li>• Determine control system device on Plano lab network that we can disconnect for test purposes.</li> <li>• Disconnect device from network.</li> <li>• Monitor Events Dashboard (E1) for changes and alerts.</li> </ul> </li> <li>▪ Option 2:             <ul style="list-style-type: none"> <li>• Determine which network TAP to disconnect from UMD network to the Remote Site Data Server (R3) network.</li> <li>• Disconnect selected TAP from network.</li> <li>• Monitor Events Dashboard (E1) for changes and alerts.</li> </ul> </li> </ul>
<b>Architectural Requirements</b>	<ul style="list-style-type: none"> <li>▪ Established baselines generated from network and control system monitoring determine normalized system behavior.</li> <li>▪ Lack of communication from a device triggers an anomaly in the Asset Management Process (E2).</li> <li>▪ Events Dashboard (E1) is notified of anomalous activity and notifies analyst via an alert.</li> </ul>
<b>Capabilities Requirements</b>	<ul style="list-style-type: none"> <li>▪ Network and Serial TAPs capture data from OT Network (C1).</li> </ul>

	<ul style="list-style-type: none"> <li>Asset Management System (C3) sensors monitor data to feed Data Collection (C2) capability.</li> <li>Security incident and event management (SIEM) utilizes alerts from anomalous activity being transferred from data collection capabilities and presents them to the analyst.</li> </ul>
<b>Expected Results</b>	Events Dashboard (E1) will notify analyst via alerts for loss of connection to device(s).
<b>Actual Results</b>	<ul style="list-style-type: none"> <li>Device is taken offline on control network.</li> <li>Baseline monitoring system recognizes device is no longer online.</li> <li>Alert is created on Events Dashboard.</li> </ul>
<b>Overall Result</b>	PASS

656 **5.1.4 ESAM-4: Anomalous Device Communication**

<b>Description</b>	<ul style="list-style-type: none"> <li>Device begins communicating in ways that are not established in known baselines.</li> <li>ESAM solution alerts to newly formed traffic patterns or device behaviors that do not correlate to determined device interaction baselines.</li> </ul>
<b>Procedure</b>	<ul style="list-style-type: none"> <li>Utilizing devices within Plano network, begin communication with a device outside the established baseline.</li> <li>Monitor Events Dashboard (E1) for newly created alerts signifying the departure from established baseline traffic and activity.</li> </ul>
<b>Architectural Requirements</b>	<ul style="list-style-type: none"> <li>Established baselines generated from network and control system monitoring determine normalized system behavior.</li> <li>Recognition of network anomaly and non-normal ICS activity (function codes, configuration changes, timing of commands, etc.) generate alerts in the Asset Management Processes (E2).</li> <li>The Events Dashboard (E1) is notified of anomalous activity and notifies analyst via an alert.</li> </ul>
<b>Capabilities Requirements</b>	<ul style="list-style-type: none"> <li>Network data collection via TAPs and SPAN ports on network device.</li> </ul>

	<ul style="list-style-type: none"> <li>Routing of network data through Asset Management (C3) sensors.</li> <li>Data Collection (C2) utilizing discovery and normalization processes for remote site asset information data flow.</li> <li>Alerting and analytics based on asset information data flow structured by the data collection capability presented to the analyst.</li> </ul>
<b>Expected Results</b>	Events Dashboard (E1) will notify analyst via alerts for anomalous device activity.
<b>Actual Results</b>	<ul style="list-style-type: none"> <li>Two devices start communicating in a way unseen before.</li> <li>Monitoring picks up new device communications, creates an alert.</li> <li>Events Dashboard delivers alert to analyst.</li> </ul>
<b>Overall Result</b>	PASS

657 **5.1.5 ESAM-5: Remote Devices with Cellular Connectivity**

<b>Description</b>	<ul style="list-style-type: none"> <li>Devices located in areas without access to Ethernet-based networking for connection to outside internet.</li> <li>Utilizing cellular networks, these devices gain connectivity through specialized cellular modems not requiring a physical networking infrastructure.</li> </ul>
<b>Procedure</b>	<ul style="list-style-type: none"> <li>Selected location will not be connected to main build network via normal Ethernet-based connections.</li> <li>Utilizing cellular-based networking, devices will connect to a VPN that has an upstream gateway connected through a cellular modem.</li> <li>These devices will be ingested into the build at the UMD Remote Site Data Servers (R3) then further cataloged through standard channels into the Events Dashboard (E1).</li> </ul>
<b>Architectural Requirements</b>	<ul style="list-style-type: none"> <li>Cellular-based modem inside a subset of the Remote Site Data Servers (R3) that can be used to capture both Raw Network Traffic (RD1) and Structured Data (RD3).</li> </ul>

	<ul style="list-style-type: none"> <li>▪ VPN connectivity through cellular-based modem to a VPN concentrator, delivering data to the on-site Remote Site Data Servers (R3).</li> <li>▪ The previous test cases apply once data from remote sites reach Remote Site Data Servers (R3).</li> </ul>
<b>Capabilities Requirements</b>	<ul style="list-style-type: none"> <li>▪ Communication links over cellular connections for the TAP capabilities.</li> <li>▪ Routing of network data through Asset Management System (C3) sensors.</li> <li>▪ Data Collection (C2) utilizing discovery and normalization processes for remote site asset information data flow.</li> <li>▪ Alerting and analytics based on asset information data flow structured by the data collection capability presented to the analyst.</li> </ul>
<b>Expected Results</b>	Devices in cellular-based remote sites will also show in the Events Dashboard (E1).
<b>Actual Results</b>	<ul style="list-style-type: none"> <li>▪ Devices in location devoid of direct internet connection are connected to cellular-based modem.</li> <li>▪ Cellular modem carries device communications to Asset Management servers.</li> <li>▪ Device monitoring appears in Events Dashboard.</li> </ul>
<b>Overall Result</b>	PASS

## 658 **6 Security Characteristic Analysis**

659 The purpose of the security characteristic analysis is to understand the extent to which the project  
660 meets its objective of demonstrating asset management for OT. A key aspect of our security evaluation  
661 involved assessing how well the reference design addresses the security characteristics it was intended  
662 to support. The Cybersecurity Framework Subcategories were used to provide structure to the security  
663 assessment, by consulting the specific sections of each standard cited in reference to a Subcategory [14].  
664 The cited sections provide validation points that the example solution would be expected to exhibit.  
665 Using the Cybersecurity Framework Subcategories as a basis for organizing our analysis allowed us to  
666 systematically consider how well the reference design supports the intended security characteristics.

## 667 **6.1 Assumptions and Limitations**

668 The security characteristic analysis has the following limitations:

- 669     ▪ It is neither a comprehensive test of all security components nor a red-team exercise.
- 670     ▪ It cannot identify all weaknesses.
- 671     ▪ It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these  
672 devices would reveal only weaknesses in implementation that would not be relevant to those  
673 adopting this reference architecture.

## 674 **6.2 Analysis of the Reference Design's Support for Cybersecurity** 675 **Framework Subcategories**

676 This section analyzes the example implementation in terms of the specific Subcategories of the  
677 Cybersecurity Framework that they support. This enables an understanding of how the example  
678 implementation achieved the goals of the design when compared against a standardized framework.

679 This section identifies the security benefits provided by each component of the example implementation  
680 and how those components support specific cybersecurity activities, as specified in terms of  
681 Cybersecurity Framework Subcategories.

### 682 **6.2.1 ID.AM-1: Physical Devices and Systems Within the Organization Are** 683 **Inventoried**

684 The ESAM reference design employs multiple applications that keep inventory of devices. Using passive  
685 analysis of network communications as well as device polling, the design captures relevant data about  
686 each asset within the scope of the build, to give an asset owner insight into what devices are deployed.

687 The reference design notifies on device installation, updates, and removals, helping maintain an up-to-  
688 date, complete, accurate, and readily available inventory of system components. These processes are  
689 automated, allowing an organization to have a central repository for inventory of assets as well as for  
690 specifying roles played by those assets.

691 Some devices may prove difficult to inventory. If a device utilizes communications not initially monitored  
692 by the ESAM reference design, the device will not be captured in the inventory. The ESAM reference  
693 design employs an optional active scanning process that can resolve this situation.

### 6.2.2 ID.RA-2: Threat and Vulnerability Information Is Received from Information-Sharing Forums and Sources

The ESAM reference design implements a patch and vulnerability intelligence solution through vendor-provided reporting. Utilizing asset lists described above, patch and vulnerability information is provided by the vendor product, to relay system security alerts and advisories to analysts.

The reference design allows an organization to be aware of potential vulnerabilities that may be applicable in the network and to the organization's assets. The design informs an organization whether assets within its inventory have updates available, if any assets have vulnerabilities, and the criticality of those patches or vulnerabilities. This information is broken out into a per-device format, helping form a more informed decision on updates.

### 6.2.3 PR.DS-2: Data in Transit Is Protected

The ESAM reference design has multiple remote connections stemming from multiple remote sites. Data is constantly being transmitted across these connections, so protection of these connections is vital. The reference design utilizes VPN connections for all connections going out of an edge-network device.

The VPN connecting the three physically remote sites—namely the enterprise site; UMD; and Plano, Texas—utilizes an always-on, multipoint VPN connection. This connection is using TLS 1.2 and certificate authentication to ensure maximum security as well as maximum reliability.

### 6.2.4 PR.MA-1: Maintenance and Repair of Organizational Assets Are Performed and Logged in a Timely Manner with Approved and Controlled Tools

The ESAM reference design does not specifically track maintenance scheduling or approvals; however, predictive and preventive maintenance is supported by elements contained in the design. Patch and vulnerability information provided by vendors, combined with information from other sources, can be used by the organization to make informed cybersecurity-maintenance decisions.

This information supports any process that builds maintenance scheduling, allowing an organization to determine what assets should be included in preventive or predictive maintenance times. Although mainly software focused, asset information may include model numbers for devices, allowing an organization to locate and replace specific devices if needed.

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

The ESAM reference design utilizes connections within the project to allow authenticated remote access to a system. This authentication is predicated on access to the enterprise network, forcing a potential

725 user to first gain access to the asset management network before being able to remotely manage  
726 devices.

727 These connections are then wrapped within the established VPN tunnel, protecting systems from replay  
728 attacks or other attacks that require open, repeatable authentication techniques to gain access to a  
729 system. This allows a more secure remote management path for devices when manual configuration is  
730 required.

### 731 6.2.6 PR.PT-4: Communications and Control Networks Are Protected

732 The ESAM reference design is designed to protect critical devices located within the OT network. For the  
733 architecture, any connection pulling data from the control networks utilizes a one-way data connection  
734 (currently in the form of a SPAN port or a network TAP) to ensure no externally routable connectivity.

735 The active scanning device listed within the architecture is an optional aspect of the design and would  
736 require an organization to verify compliance with relevant regulations, before deploying this aspect of  
737 the solution.

### 738 6.2.7 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for 739 Users and Systems Is Established and Managed

740 The ESAM reference design utilizes passive and active scanning tools to scan the industrial control  
741 environments at the two remote locations. These tools build a baseline of assets and network traffic  
742 between those assets using machine learning, alerting to any anomalous behavior.

### 743 6.2.8 DE.AE-2: Detected Events Are Analyzed to Understand Attack Targets and 744 Methods

745 The ESAM reference design utilizes discovery and monitoring tools to detect malicious activity from an  
746 established baseline of network activity. Any deviation from established baselines will notify  
747 organizational analysts to activity not recognized as normal behavior. The analyst will be informed what  
748 triggered the alert, allowing them to better respond to the incident.

749 Along with anomaly detection capabilities, the reference design employs alerting and reporting  
750 capabilities based on known attack tactics and techniques. Recognition of these threats also elicits an  
751 alert that is reported to the analyst.

## 752 6.3 Lessons Learned

753 Identifying and replicating the infrastructure(s) likely found in an OT operating environment is a  
754 challenge. The NCCoE ESAM Team did not limit this build to a lab environment. The team was able to  
755 demonstrate effective OT asset management in existing, real-world energy-sector environments with  
756 the support of collaborators who offered their infrastructure, resources, personnel, and assets.



757 While numerous automated capabilities are used to capture and maintain asset information, a  
758 significant manual effort will likely be needed to identify assets, especially those that are remote and  
759 not connected to an existing network infrastructure. Further, given the variety of assets deployed, we  
760 experienced instances where serial communication devices required conversion to IP-based  
761 communication protocols. It is critical to establish the necessary communication infrastructure to ensure  
762 these devices become part of the main, automated inventory that this project showcases.

763 While the technology we used is not complex, working through coordination and deployment of the  
764 supporting infrastructure and asset management technologies will be a rather large undertaking for any  
765 company looking to adopt this solution or any component of it. We highly recommend that executive  
766 management support be in place, whether the OT asset management solution is deployed to a specific  
767 site or across the entire enterprise.

## 768 **7 Future Build Considerations**

769 The Industrial Internet of Things, or IIoT, refers to the application of instrumentation and connected  
770 sensors and other devices to machinery and vehicles in the transport, energy, and industrial sectors. For  
771 the energy sector in particular, distributed energy resources (DERs), such as solar photovoltaic panels  
772 and wind turbines, introduce information exchanges between a utility's distribution control system and  
773 the DERs, to manage the flow of energy in the distribution grid. Moreover, the rate at which these IIoT  
774 devices are deployed in the energy sector is projected to increase and could introduce asset  
775 management and cybersecurity challenges for the sector. Expanding the architecture to include IIoT  
776 devices and using IIoT-generated data for near-real-time asset management could ensure secure  
777 deployment of these assets and may be explored in a future project.

## 778 **Appendix A** **List of Acronyms**

<b>ANSI</b>	American National Standards Institute
<b>ARP</b>	Address Resolution Protocol
<b>CERT</b>	Computer Emergency Readiness Team
<b>CIS</b>	Center for Internet Security
<b>CISA</b>	Cybersecurity and Infrastructure Security Agency
<b>CSV</b>	Comma-Separated Value
<b>DER</b>	Distributed Energy Resource(s)
<b>ESAM</b>	Energy Sector Asset Management
<b>HART</b>	Highway Addressable Remote Transducer
<b>HMI</b>	Human-Machine Interface
<b>ICMP</b>	Internet Control Message Protocol
<b>ICS</b>	Industrial Control System(s)
<b>IEC</b>	International Electrotechnical Commission
<b>IED</b>	Intelligent Electronic Device
<b>IETF</b>	Internet Engineering Task Force
<b>IIoT</b>	Industrial Internet of Things
<b>IP</b>	Internet Protocol
<b>ISA</b>	International Society of Automation
<b>ISACA</b>	Information Systems Audit and Control Association
<b>ISO</b>	International Organization for Standardization
<b>LTE</b>	Long-Term Evolution
<b>MAC</b>	Media Access Control
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NICE</b>	National Initiative for Cybersecurity Education
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>OT</b>	Operational Technology
<b>PLC</b>	Programmable Logic Controller
<b>RARP</b>	Reverse Address Resolution Protocol
<b>RFC</b>	Request for Comments
<b>SCADA</b>	Supervisory Control and Data Acquisition

DRAFT

<b>SIEM</b>	Security Information and Event Management
<b>SP</b>	Special Publication
<b>SPAN</b>	Switched Port Analyzer
<b>TAP</b>	Test Access Points
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>UDP</b>	User Datagram Protocol
<b>UMD</b>	University of Maryland
<b>VPN</b>	Virtual Private Network

## 779 Appendix B References

- 780 [1] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, National Institute of  
781 Standards and Technology (NIST) Special Publication (SP) 800-82 Revision 2, NIST, Gaithersburg,  
782 Md., May 2015. Available: <https://doi.org/10.6028/NIST.SP.800-82r2>.
- 783 [2] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-  
784 30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available:  
785 <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- 786 [3] Joint Task Force, *Risk Management Framework for Information Systems and Organizations*, NIST  
787 SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available:  
788 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>.
- 789 [4] NIST. *Risk Management Framework: Quick Start Guides*. [Online]. Available:  
790 [https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-](https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides)  
791 [guides](https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides).
- 792 [5] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-  
793 30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available:  
794 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- 795 [6] Cybersecurity and Infrastructure Security Agency (CISA) Industrial Control Systems Cyber  
796 Emergency Response Team (ICS-CERT). Cyber Threat Source Descriptions. [Online]. Available:  
797 <https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions>.
- 798 [7] CISA ICS-CERT. National Cyber Awareness System. Alerts. [Online]. Available: [https://www.us-](https://www.us-cert.gov/ncas/alerts)  
799 [cert.gov/ncas/alerts](https://www.us-cert.gov/ncas/alerts).
- 800 [8] MITRE. Common Vulnerabilities and Exposures. [Online]. Available: <https://cve.mitre.org/>.
- 801 [9] NIST. National Vulnerability Database. Common Vulnerability Scoring System. [Online].  
802 Available: <https://nvd.nist.gov/vuln-metrics/cvss>.
- 803 [10] CISA ICS-CERT. National Cyber Awareness System. Report Incidents, Phishing, Malware, or  
804 Vulnerabilities. [Online]. Available: <https://www.us-cert.gov/report>.
- 805 [11] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Apr. 16, 2018.  
806 Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- 807 [12] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information*  
808 *Systems and Organizations* NIST SP 800-53 Revision 4, NIST, Gaithersburg, Md., Apr. 2013.  
809 Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

- 810 [13] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity*  
811 *Workforce Framework*, NIST SP 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available:  
812 <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf>.
- 813 [14] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, Apr. 16, 2018.  
814 Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

**NIST SPECIAL PUBLICATION 1800-23C**

---

# Energy Sector Asset Management

## For Electric Utilities, Oil & Gas Industry

---

**Volume C:  
How-To Guides**

**James McCarthy  
Glen Joy**

National Cybersecurity Center of Excellence  
Information Technology Laboratory

**Lauren Acierto  
Jason Kuruville  
Titilayo Ogunyale  
Nikolas Urlaub  
John Wiltberger  
Devin Wynne**

The MITRE Corporation  
McLean, Virginia

September 2019

DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management>



DRAFT

## DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-23C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-23C, 76 pages, (September 2019), CODEN: NSPUE2

## FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Public comment period: September 23, 2019 through November 25, 2019

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

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

## 1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 17 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 27 **ABSTRACT**

28 Industrial control systems (ICS) compose a core part of our nation's critical infrastructure. Energy sector  
29 companies rely on ICS to generate, transmit, and distribute power and to drill, produce, refine, and  
30 transport oil and natural gas. Given the wide variety of ICS assets, such as programmable logic  
31 controllers and intelligent electronic devices, that provide command and control information on  
32 operational technology (OT) networks, it is essential to protect these devices to maintain continuity of  
33 operations. These assets must be monitored and managed to reduce the risk of a cyber attack on  
34 ICS-networked environments. Having an accurate OT asset inventory is a critical component of an  
35 overall cybersecurity strategy.



36 The NCCoE at NIST is responding to the energy sector’s request for an automated OT asset management  
 37 solution. To remain fully operational, energy sector entities should be able to effectively identify,  
 38 control, and monitor their OT assets. This document provides guidance on how to enhance OT asset  
 39 management practices, by leveraging capabilities that may already exist in an energy organization’s  
 40 operating environment as well as by implementing new capabilities.

#### 41 **KEYWORDS**

42 *energy sector asset management; ESAM; ICS; industrial control system; malicious actor; monitoring;*  
 43 *operational technology; OT; SCADA; supervisory control and data acquisition*

#### 44 **ACKNOWLEDGMENTS**

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

Name	Organization
Matt Cowell	Dragos, Inc.
Tom VanNorman	Dragos, Inc.
Andrew Dunham	Forescout Technologies, Inc.
Tim Jones	Forescout Technologies, Inc.
John Norsworthy	Forescout Technologies, Inc.
Lindsey Hale	FoxGuard Solutions, Inc.
Steve Boyd	KORE Wireless, Inc.
Brian Hicks	KORE Wireless, Inc.
Adam Cohn	Splunk Inc.
Bill Wright	Splunk Inc.
Ray Erlinger	TDi Technologies, Inc.
Bill Johnson	TDi Technologies, Inc.

Name	Organization
Samantha Pelletier	TDi Technologies, Inc.
Gabe Authier	Tripwire, Inc.
Steven Sletten	Tripwire, Inc.
Jim Wachhaus	Tripwire, Inc.

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

Technology Partner/Collaborator	Build Involvement
<a href="#">Dragos, Inc.</a>	Dragos Platform v1.5
<a href="#">ForeScout Technologies, Inc.</a>	ForeScout CounterACT v8.0.1
<a href="#">FoxGuard Solutions, Inc.</a>	FoxGuard Solutions Patch and Update Management Program v1
<a href="#">KORE Wireless Group, Inc.</a>	KORE Wireless Cellular Connectivity with Cellular Gateway v2.0
<a href="#">Splunk, Inc.</a>	Splunk Enterprise v7.1.3
<a href="#">TDi Technologies, Inc.</a>	TDi Technologies ConsoleWorks v5.2-0u1
<a href="#">Tripwire, Inc.</a>	Tripwire Industrial Visibility v3.2.1

50 **Contents**

51 **1 Introduction ..... 1**

52 1.1 Practice Guide Structure ..... 1

53 1.2 Build Overview ..... 2

54 1.3 Typographic Conventions ..... 4

55 1.4 Logical Architecture Summary ..... 4

56 **2 Product Installation Guides ..... 4**

57 2.1 ConsoleWorks ..... 4

58 2.1.1 ConsoleWorks Configurations at the NCCoE ..... 5

59 2.2 Forescout CounterACT ..... 30

60 2.2.1 CounterACT Enterprise Manager Configuration ..... 31

61 2.2.2 CounterACT Appliance Configuration ..... 42

62 2.3 Dragos Platform ..... 43

63 2.3.1 Dragos Sitestore Configuration ..... 43

64 2.3.2 Dragos Midpoint Sensor ..... 45

65 2.3.3 Dragos Splunk Integration ..... 45

66 2.4 FoxGuard Patch and Update Management Program ..... 47

67 2.4.1 Patch Report ..... 47

68 2.5 Kore Wireless ..... 54

69 2.5.1 Bridge Configuration ..... 55

70 2.5.2 Virtual Private Network Configuration ..... 56

71 2.6 pfSense VPN ..... 58

72 2.6.1 Plano and UMD VPN Configuration ..... 58

73 2.7 Splunk ..... 58

74 2.7.1 Splunk Enterprise Configuration ..... 59

75 2.8 Tripwire Industrial Visibility ..... 61

76 2.8.1 Tripwire Industrial Visibility Configuration UMD ..... 62

77 2.8.2 Tripwire Industrial Visibility Configuration Plano ..... 68

78	2.8.3	Tripwire Industrial Visibility Configuration National Cybersecurity Center of	
79		Excellence .....	69
80	<b>Appendix A</b>	<b>List of Acronyms .....</b>	<b>76</b>
81		<b>List of Figures</b>	
82		<b>Figure 1-1 High-Level Topology .....</b>	<b>3</b>
83		<b>Figure 2-1 Update Availability Summary .....</b>	<b>48</b>
84		<b>Figure 2-2 Device Update Availability Details-1 .....</b>	<b>49</b>
85		<b>Figure 2-3 Device Update Availability Details-2 .....</b>	<b>50</b>
86		<b>Figure 2-4 Device Update Availability Details-3 .....</b>	<b>51</b>
87		<b>Figure 2-5 Device Update Availability Details-4 .....</b>	<b>52</b>
88		<b>Figure 2-6 Device Update Availability Details-5 .....</b>	<b>53</b>
89		<b>Figure 2-7 Patch Evidence Documentation .....</b>	<b>54</b>
90		<b>List of Tables</b>	
91		<b>Table 2-1 Dragos Required Files.....</b>	<b>44</b>

## 92 1 Introduction

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

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

### 100 1.1 Practice Guide Structure

101 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a  
102 standards-based reference design and provides users with the information they need to replicate this  
103 asset management solution in the energy sector. This reference design is modular and can be deployed  
104 in whole or in part.

105 This guide contains three volumes:

- 106     ▪ NIST SP 1800-23A: *Executive Summary*
- 107     ▪ NIST SP 1800-23B: *Approach, Architecture, and Security Characteristics* – what we built and why
- 108     ▪ NIST SP 1800-23C: *How-To Guides* – instructions for building the example solution (**you are**  
109         **here**)

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

111 **Senior IT executives, including chief information security and technology officers**, will be interested in  
112 the *Executive Summary, NIST SP 1800-23A*, which describes the following topics:

- 113     ▪ challenges that enterprises face in operational technology (OT) asset management
- 114     ▪ example solution built at the NCCoE
- 115     ▪ benefits of adopting the example solution

116 **Technology or security program managers** who are concerned with how to identify, understand, assess,  
117 and mitigate risk will be interested in NIST SP 1800-23B, which describes what we did and why. The  
118 following sections will be of particular interest:

- 119     ▪ Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- 120     ▪ Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to  
121 cybersecurity standards and best practices.

122 You might share the *Executive Summary*, NIST SP 1800-23A, with your leadership team members to help  
123 them understand the importance of adopting a standards-based solution to strengthen their OT asset  
124 management practices, by leveraging capabilities that may already exist within their operating  
125 environment or by implementing new capabilities.

126 **IT professionals** who want to implement an approach like this will find this whole practice guide useful.  
127 You can use this How-To portion of the guide, NIST SP 1800-23C, to replicate all or parts of the build  
128 created in our lab. This How-To portion of the guide provides specific product installation, configuration,  
129 and integration instructions for implementing the example solution. We do not recreate the product  
130 manufacturers' documentation, which is generally widely available. Rather, we show how we  
131 incorporated the products together in our environment to create an example solution.

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

141 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a  
142 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and  
143 success stories will improve subsequent versions of this guide. Please contribute your thoughts to  
144 [energy\\_nccoe@nist.gov](mailto:energy_nccoe@nist.gov).

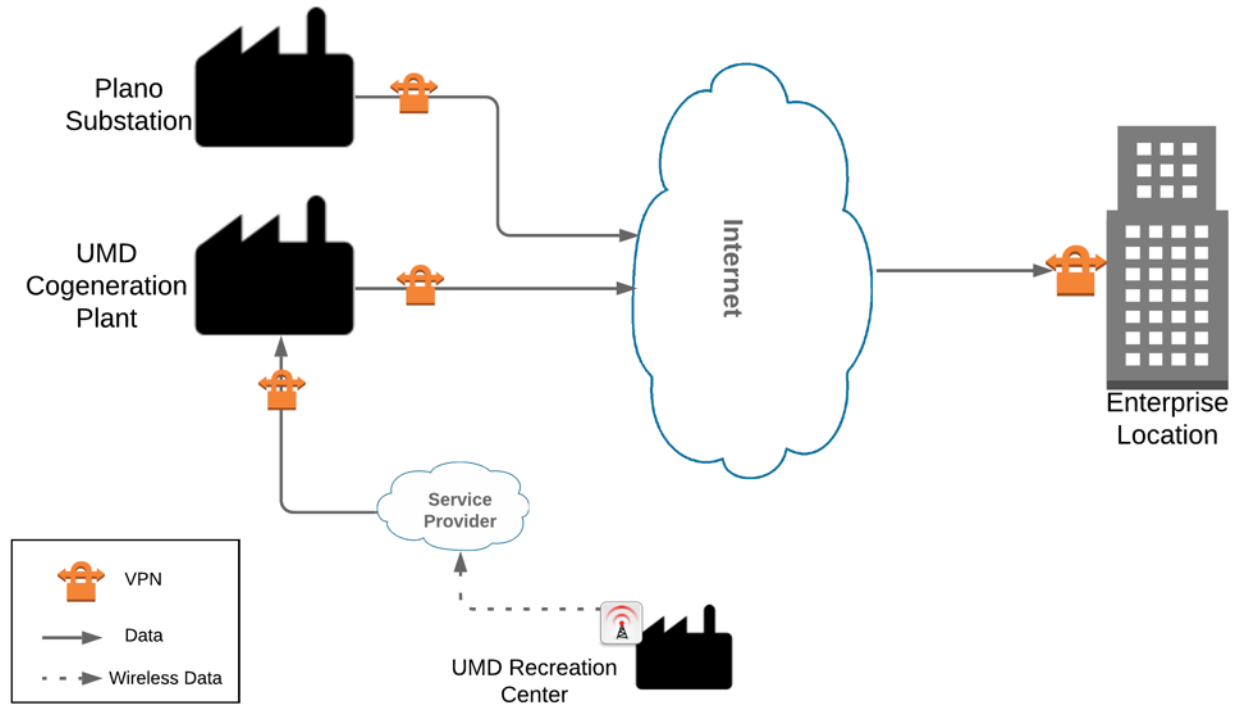
145 Acronyms used in figures can be found in the List of Acronyms appendix.

## 146 **1.2 Build Overview**

147 The example solution fulfills the need for an automated asset inventory. This example solution allows  
148 devices to be identified in multiple ways, depending on the needs of the organization. The architecture  
149 is intended as one solution.

150 The example solution makes use of two "remote" sites, while the National Cybersecurity Center of  
151 Excellence (NCCoE) serves as the enterprise location as shown in Figure 1-1 below. Having a central  
152 enterprise location provides flexibility to add multiple sites as well as the ability to collect all data in one  
153 place.

154 **Figure 1-1 High-Level Topology**



155

156 Different components in the build are installed at each location. However, some components preexist,  
157 including the OT assets, networks, routers, and protocol converters. This guide will describe the  
158 installation and configuration details of the components installed at each site but not preexisting  
159 components. A detailed topology and description of each site can be found in Volume B, Section 4.2,  
160 Example Solution.

## 161 1.3 Typographic Conventions

162 The following table presents typographic conventions used in this volume.

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

## 163 1.4 Logical Architecture Summary

164 A logical architecture summary can be found in Volume B of this practice guide, Section 4.1, Architecture  
165 Description.

## 166 2 Product Installation Guides

167 This section of the practice guide contains detailed instructions for installing and configuring all of the  
168 products, where applicable, used to build an instance of the example solution.

### 169 2.1 ConsoleWorks

170 ConsoleWorks performs as a data collection server and a data analysis server. The data collection server  
171 is located at the University of Maryland (UMD) and reads data from a steam meter via protocol  
172 converters. The data analysis server resides at the NCCoE and normalizes data collected from security  
173 information and event management (SIEM) software, for processing by the patch analysis and reporting  
174 tool.



## 175 2.1.1 ConsoleWorks Configurations at the NCCoE

176 The following subsections document the software, hardware/virtual machine (VM), and network  
177 configurations for the ConsoleWorks server at the NCCoE.

### 178 2.1.1.1 VM Configuration

179 The ConsoleWorks VM is given the following resources:

- 180     ▪ CentOS 7.5
- 181     ▪ Central processing unit (CPU) cores
- 182     ▪ 100 gigabyte (GB) hard disk
- 183     ▪ 10 GB random access memory (RAM)
- 184     ▪ 1 network interface controller/card (NIC)

### 185 2.1.1.2 Network Configuration

- 186     ▪ Dynamic Host Configuration Protocol (DHCP): disabled
- 187     ▪ Internet protocol version (IPv6): ignore
- 188     ▪ IPv4: Manual
- 189     ▪ IPv4 address: 10.100.100.6
- 190     ▪ Netmask: 255.255.255.0

### 191 2.1.1.3 Installation

- 192 1. Download the installation kit from the <http://support.tditechnologies.com> website. A username and  
193 password are required, so contact TDi Support at [support@tditechnologies.com](mailto:support@tditechnologies.com) to request them.
- 194 2. Create a directory to contain the ConsoleWorks installation files: `#mkdir temp/conworks`
- 195 3. Run the following command: `# yum local install consoleworksssl-<version>_x86_64.rpm`
- 196 4. Extract the provided compressed license script to `/tmp/conworks`.
- 197 5. Run the script from the extracted zip file.
- 198 6. Start ConsoleWorks with the following command: `# /opt/ConsoleWorks/bin/cw_start default`

- 199 7. Connect to the Console at *https://10.100.100.6:5176*. Log in using the default credentials.

ADMIN: Server Management: Registration

Registration

### ConsoleWorks Registration

[Complete My Offline Registration](#)

Contact Name:

Contact Email:

Telephone:

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Seneca Highway

Address Line 2:

City: Rockville

State/Province: MD

Zip/Postal Code: 20850

Country: US

View current registration status of all licenses

Register Online Register Offline

Cancel Save

PROXY DETAILS

ADVANCED OPTIONS

200

- 201 8. Fill in the details for Registration. Click **Register Online**. Click **Save**.

ADMIN: Server Management: Registration

Registration

### ConsoleWorks Registration

[Complete My Offline Registration](#)

Contact Name:

Contact Email:

Telephone:

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Seneca Highway

Address Line 2:

City: Rockville

State/Province: MD

Zip/Postal Code: 20850

Country: US

View current registration status of all licenses

Register Online Register Offline

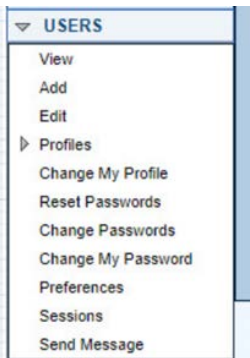
Cancel Save

PROXY DETAILS

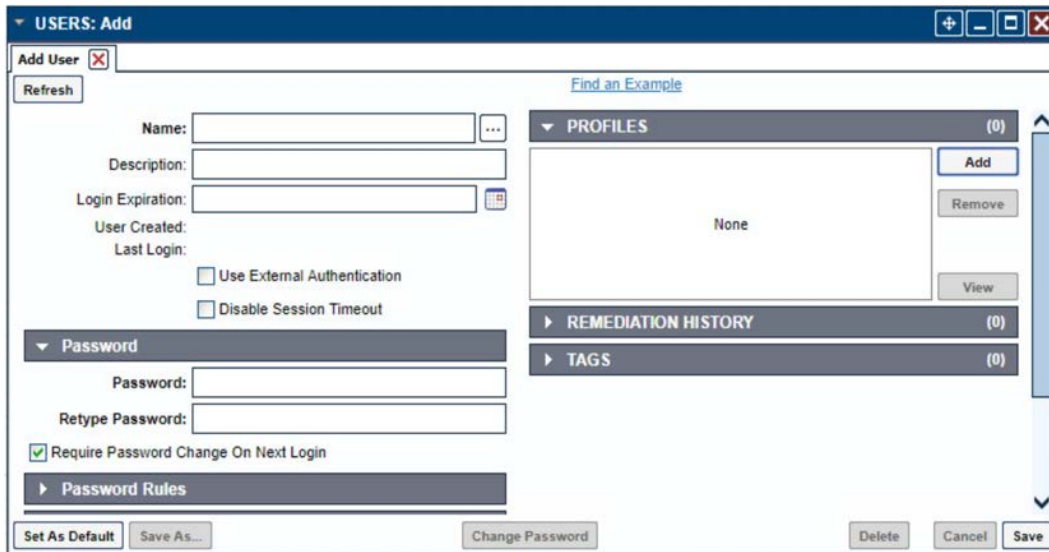
ADVANCED OPTIONS

202

203 9. Create a new user. Navigate on the left to **Users > Add**.

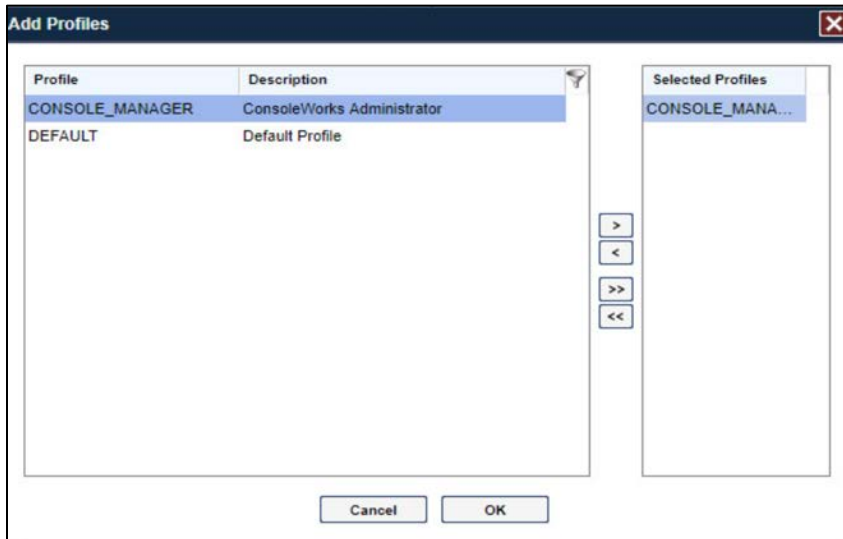


204  
205 10. Enter the **Name** and **Password**. Select **Add**.



206

207 11. Add **CONSOLE\_MANAGER** as a selected profile, as shown in the screenshot below. Select **OK**.



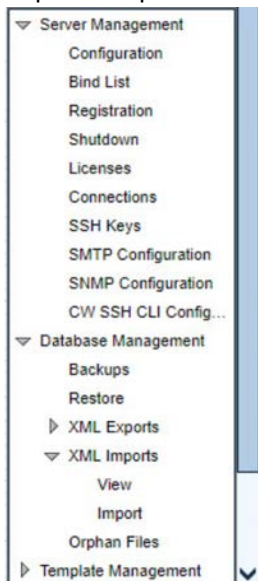
208

209 12. Click **Save**.

#### 210 *2.1.1.4 Configuration*

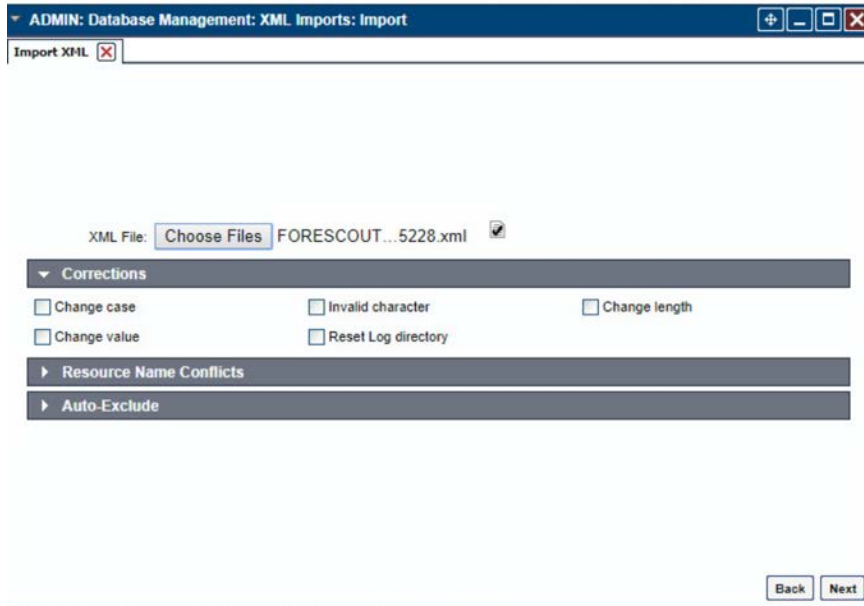
211 ConsoleWorks provides the scripts to normalize data, for processing by FoxGuard Patch and Update  
212 Management Program (PUMP). The script provided is in extensible markup language (XML) format.

213 1. Import the provided XML file at **Admin > Database Management > XML Imports > Import**.



214

215 2. Click **Choose Files**. Locate the provided XML file. Select **Next**.



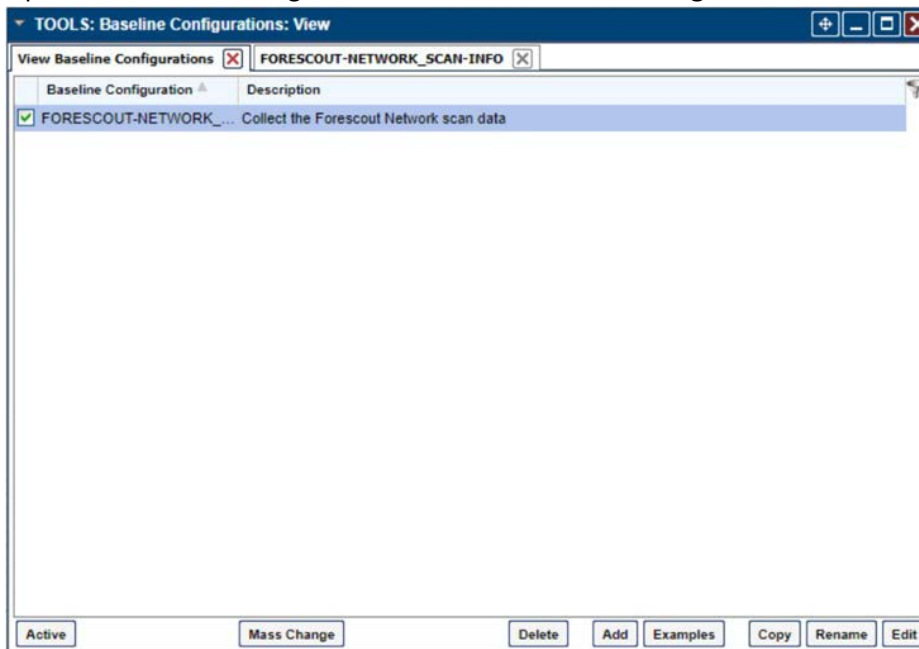
216

217 3. Select **Next**. The import is complete.



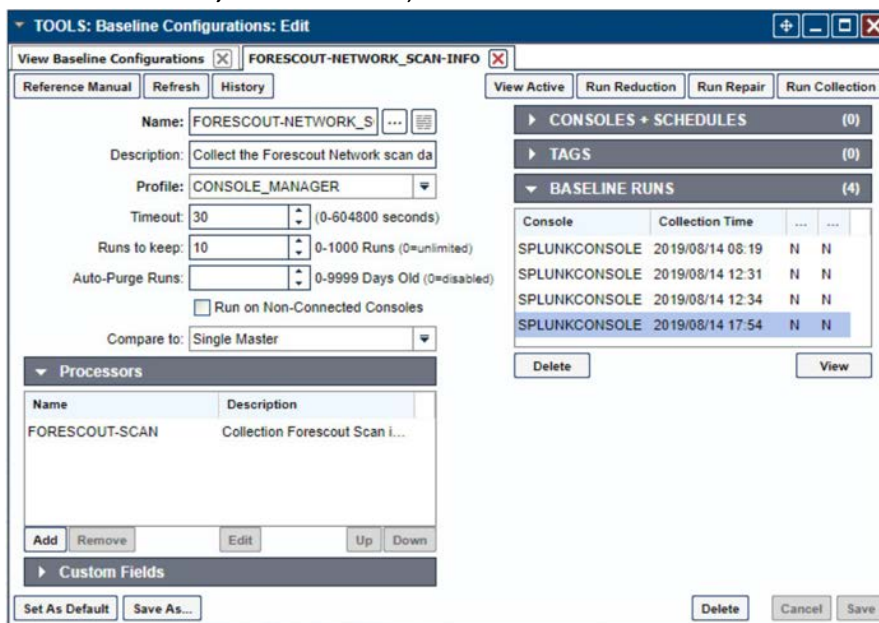
218

219 4. Open the baseline configuration at **Tools > Baseline Configurations > View**. Select **Edit**.



220

221 5. Under **Processors**, select the scan, and click **Edit**.

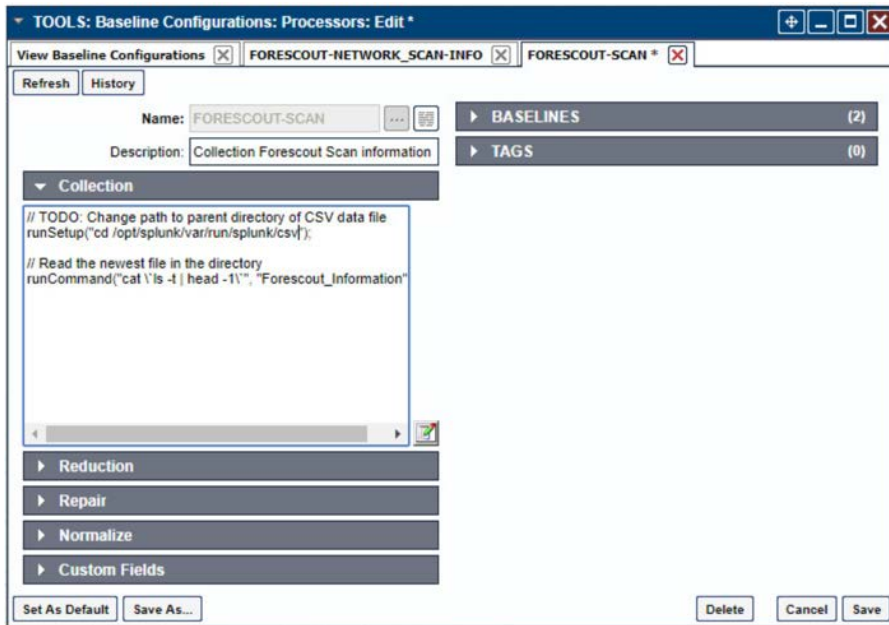


222

223 6. Under **Collection**, update the path to match where Splunk saves the inventory, as shown in the  
224 screenshot.

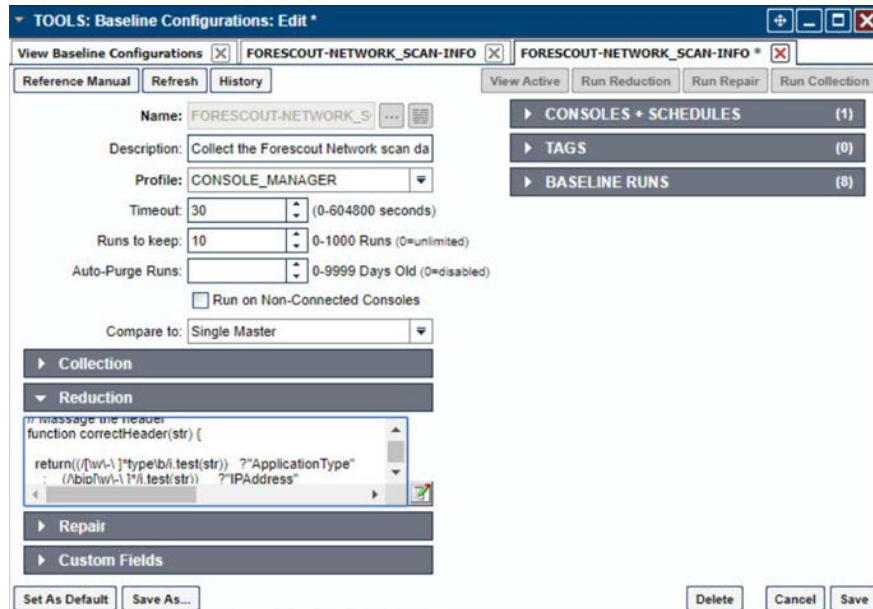
225 // TODO: Change path to parent directory of CSV data file

```
226 runSetup("cd /opt/splunk/var/run/splunk/csv");  
227 // Read the newest file in the directory  
228 runCommand("cat `ls -t | head -1`", "Forescout_Information", 5);
```



229

230 7. Under **Reduction**, enter the following script, as shown in the screenshot below.



231

```

232     include("UTIL");
233     include("UTIL_CUSTOM_FILE");
234     include("UTIL_JSON");
235     ///////////////////////////////////////////////////////////////////
236     ///////////////////////////////////////////////////////////////////
237     // Massage the header
238     function correctHeader(str) {
239     return((/[w\-\ ]*type\b/i.test(str)) ?"ApplicationType"
240         :    (/bip[ w\-\ ]*/i.test(str))    ?"IPAddress"
241         :    (/bmac[ w\-\ ]*/i.test(str))    ?"MACAddress"
242         :    (/bmodel[ w\-\ ]*/i.test(str))  ?"ModelNumber"
243         :    (/bpart[ w\-\ ]*/i.test(str))   ?"PartNumber"
244         :    (/basset.?id\b/i.test(str))     ?"PK"
245         :    (/bproduct[ w\-\ ]*/i.test(str))?"ProductName"
246         :    (/bserial[ w\-\ ]*/i.test(str)) ?"SerialNumber"
247         :    (/bvendor/i.test(String(str)))  ?"VendorName"
248         :    (/version/i.test(String(str)))  ?"VersionName"
249         :                                     String(str).replace(/[W\_]+/g, "
250 ").camelSpaced().toCapCase().replace(/\/ +/g, " "));
251     }
252     ///////////////////////////////////////////////////////////////////
253     ///////////////////////////////////////////////////////////////////
254     // ref: http://stackoverflow.com/a/1293163/2343
255     function CSVToArray(strData, strDelimiter) {
256         // Check to see if the delimiter is defined. If not, then default to comma.
257         strDelimiter=(typeof strDelimiter!='undefined')?strDelimiter:",";
258         // Create a regular expression to parse the CSV values.
259         //                                     Delimiters           Quoted fields
260     Standard fields.
261         var objPattern=new
262     RegExp(("(\\\"+strDelimiter+|\\r?\\n|\\r|^)(?:\"([^\"])*(?:\"\\\"[^\"]*)*\")\"|([^\
263     \\\"+strDelimiter+\\r\\n]*)\"), "gi");
264         // Create an array to hold our data. Give the array a default empty first row.

```



```
265     var arrData=[];
266     // Create an array to hold our individual pattern matching groups.
267     var arrMatches=null;
268     // Keep looping over the regular expression matches until we can no longer
269     find a match.
270     while(arrMatches=objPattern.exec(strData)) {
271         // Get the delimiter that was found.
272         var strMatchedDelimiter=arrMatches[1];
273         // Check to see if the given delimiter has a length (is not the start of
274         string) and if it matches field delimiter.
275         // If it does not, then we know that this delimiter is a row delimiter.
276         if(strMatchedDelimiter.length && strMatchedDelimiter!==strDelimiter) {
277             // Since we have reached a new row of data, add an empty row to our data
278             array.
279             arrData.push([]);
280         }
281         var strMatchedValue;
282         // Now that we have our delimiter out of the way, let's check to see which
283         kind of value we captured (quoted or unquoted).
284         if(arrMatches[2]) {
285             // We found a quoted value. When we capture this value, unescape any
286             double quotes.
287             //strMatchedValue=arrMatches[2].replace(new RegExp( "\\\"\\\"", "g" ), "\\");
288             strMatchedValue=arrMatches[2].replace(/\\"{2}/g, '');
289         } else {
290             // We found a non-quoted value.
291             strMatchedValue=arrMatches[3];
292         }
293         // Now that we have our value string, let's add it to the data array.
294         arrData[arrData.length-1].push(strMatchedValue);
295     }
296     // Return the parsed data.
```

```

297     return(arrData);
298 }
299 ///////////////////////////////////////////////////////////////////
300 ///////////////////////////////////////////////////////////////////
301 function procCSV(csv) {
302     // Convert string to YYYYMMDD_HHMMSS for readability
303     var outputDir="/FOXGUARD/"+(now.slice(0,8));
304     var outputFile=""+outputDir+"/"+(now.slice(8,14));
305     var result=[];
306     // Default of negative feedback
307     var tracker=false;
308     if(typeof csv!='undefined' && csv.length>0) {
309         try {
310             var lines=CSVToArray(csv);
311             lines.shift();
312             if(lines.length>1) {
313                 try {
314                     // Header names
315                     var props=lines[0];
316                     if(props.length>0) {
317                         // Massage header names
318                         for(var k=0;k<props.length;k++) {
319                             if(props[k].length>0) {
320                                 props[k]=correctHeader(props[k]);
321                             }
322                         }
323                         for(i=1;i<lines.length;i++) {
324                             var j=lines[i];
325                             if(j.length>0) {
326                                 var obj={
327                                     "ApplicationType": "Firmware",

```

```
328         "ModelNumber": "unspecified",
329         "PartNumber": "unspecified",
330         "PK": "unspecified",
331         "ProductName": "unspecified",
332         "SerialNumber": "unspecified",
333         "VendorName": "unspecified",
334         "VersionName": "unspecified"
335     };
336
337     if(String(ServerConfig.getList()[0].conwrksinvo).split("/")[3]!="default") {
338
339         obj.Site=String(ServerConfig.getList()[0].conwrksinvo).split("/")[3];
340     }
341     for(var k=0;k<props.length;k++) {
342         if(Boolean(j[k]) && j[k]!="-") {
343             switch(props[k]) {
344                 case "IPAddress":
345
346                 //obj.IPAddress=(rEIPv4.test(j[k]))?j[k].match(rEIPv4)[1]:(rEIPv6.test(j[k]))?j[k].
347                 match(rEIPv6)[1]:"unspecified";
348
349                 break;
350                 case "MACAddress":
351
352                 //obj.MACAddress=(rEMAC.test(j[k]))?j[k].match(rEMAC)[1]:"unspecified";
353
354                 break;
355                 case "OperatingSystem":
356
357                 obj.ApplicationType="Operating System";
358                 obj.OperatingSystem=j[k];
359                 obj.ProductName=j[k];
360
361                 break;
362                 case "VendorName":
363
364                 if(obj.VendorName=="unspecified") {
```

```
360         obj.VendorName=j[k];
361     }
362     break;
363     case "VersionName":
364         obj.VersionName=j[k];
365         if(rESEL.test(j[k])) {
366             obj.ModelNumber=j[k].match(rESEL)[1];
367             obj.VendorName="Schweitzer";
368         }
369         break;
370     default:
371         obj[props[k]]=j[k];
372         break;
373     }
374 }
375 }
376 if(obj.hasOwnProperty('OperatingSystem')) {
377     obj.OperatingSystemVersion=obj.VersionName;
378     //delete obj.VersionName;
379 }
380 for(var p in obj) {
381     // These are required properties
382     if(["ProductName", "VendorName", "VersionName"].indexOf(p)<0) {
383         // Not a required property, and no useful data, get rid of it!
384         if(Boolean(obj[p])===false || obj[p]=="unspecified") {
385             delete obj[p];
386         }
387     }
388 }
389 result.push({
```

```
390         "AssetIdentifiers": obj,
391         "FUI": null
392     });
393 }
394 }
395 try {
396     setReduction("Forescout_Information", JSON.stringify(result, null, 2));
397     makeDirectory(""+outputDir);
398     // File for FoxGuard
399     setCustomFileContents(""+outputFile+".txt", JSON.stringify(result,
400 null, 2));
401     // Copy of original input
402     //setCustomFileContents(""+outputFile+".csv", csv);
403     // If everything goes great, return with positive feedback
404     tracker=true;
405 } catch(ex) {
406     print("ERROR: "+ex);
407 }
408 } else {
409     print("ERROR: Missing header data");
410 }
411 } catch(ex) {
412     print("ERROR: "+ex);
413 }
414 } else {
415     print("ERROR: Going to need more data than this");
416 }
417 } catch(ex) {
418     print("ERROR: "+ex);
419 }
420 } else {
```

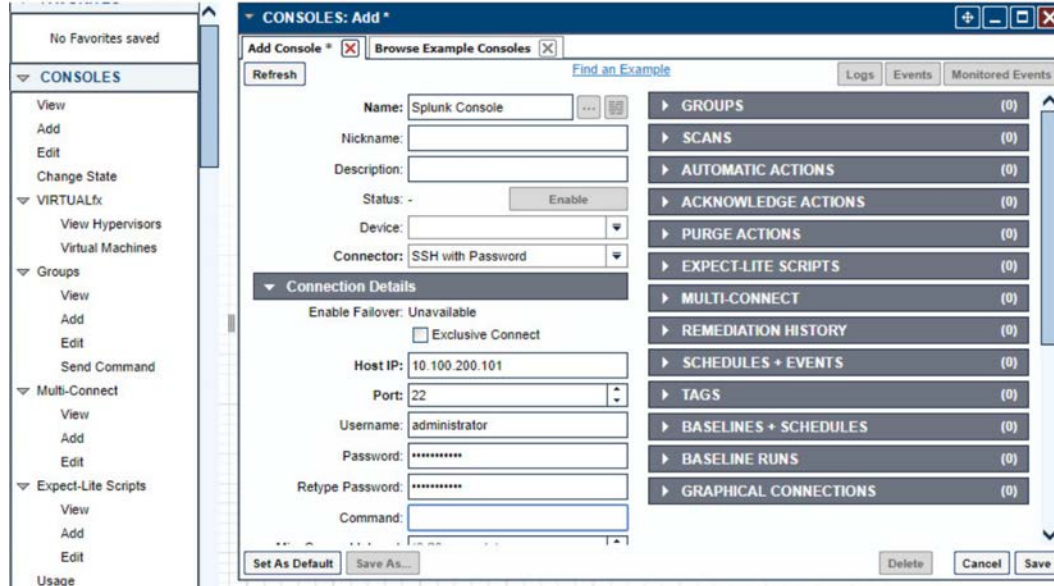
```

421     print("ERROR: We got nothing!");
422     }
423     return(tracker);
424     }
425     ///////////////////////////////////////////////////////////////////
426     ///////////////////////////////////////////////////////////////////
427     // value for TZ offset
428     var d=0;
429     try {
430         d=new Date().getTimezoneOffset();
431     } catch(ex) {
432         print("ERROR: "+ex);
433     }
434     // Create string of YYYYMMDDHHMMSS
435     var now=String(new Date(Date.now()-(d*60000)).toJSON()).replace(/\D/g,
436     "").slice(0,14);
437     // IPv4
438     var rEIPv4=/\b(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])\.\.){3}(?:25[0-
439     5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])\b/;
440     // IPv6
441     var rEIPv6=/\b([\da-fA-F]{1,4}(:[\da-fA-F]{0,4}){2,6}[\da-fA-F]{1,4})\b/;
442     // MAC
443     var rEMAC=/\b(?:[\da-fA-F]{2}\:){5}[\da-fA-F]{2}\b/;
444     // SEL
445     var rESEL=/\b(SEL-.\+)-R/;
446     try {
447         procCSV(getOutput("Forescout_Information"));
448     } catch(ex) {
449         print("ERROR: "+ex);
450     }
451     8. Select Save.

```

452 9. Navigate to **Consoles > Add**.

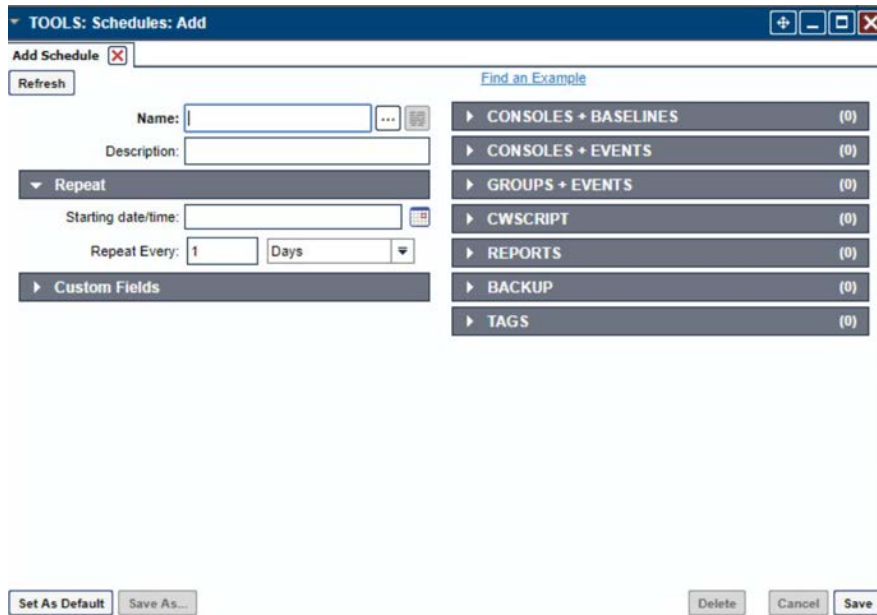
453 10. Enter a name and connection details for the Splunk server. Select **Save**.



454

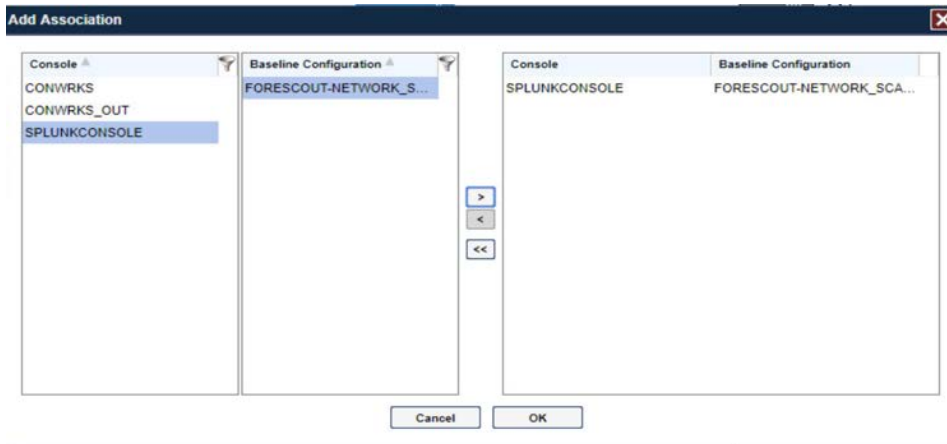
455 11. Navigate to **Tools > Schedule**. Click **Add**.

456 12. Name the schedule. Set the time to run at an acceptable interval (this build set the interval to  
457 repeat daily). Under **CONSOLES + BASELINES**, click **Add**.

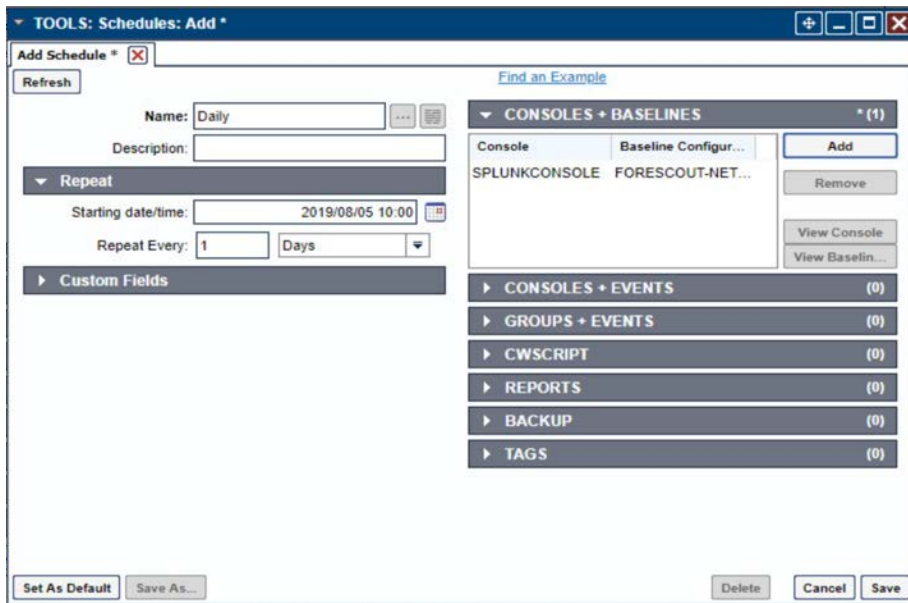


458

- 459 13. Select the previously created Splunk console and the imported baseline configuration. Click the  
460 arrow. Click **OK**.



- 461 14. Click **Save**.  
462



463  
464 **2.1.1.5 ConsoleWorks Configurations UMD**

465 The following subsections document the software, hardware/VM, and network configurations for the  
466 ConsoleWorks server at UMD.

467 **2.1.1.6 VM Configuration**

468 The UMD ConsoleWorks VM is given the following resources:

- 469  Windows Server 2016



- 470       ▪ 2 CPU cores
- 471       ▪ 100 GB hard Disks
- 472       ▪ 12 GB RAM
- 473       ▪ 2 NIC

#### 474    2.1.1.7 *Network Configuration*

475    Network Configuration (Interface 1):

- 476       ▪ DHCP: disabled
- 477       ▪ IPv6: ignore
- 478       ▪ IPv4: Manual
- 479       ▪ IPv4 address: 10.100.1.6
- 480       ▪ Netmask: 255.255.255.0

481    Network Configuration (Interface 2):

- 482       ▪ DHCP: disabled
- 483       ▪ IPv6: ignore
- 484       ▪ IPv4: Manual
- 485       ▪ IPv4 address: 172.16.2.82
- 486       ▪ Netmask: 255.255.255.248

#### 487    2.1.1.8 *Installation*

- 488    1. Download the installation kit from the <http://support.tditechnologies.com> website. A username and  
489       password are required, so contact TDi Support at [support@tditechnologies.com](mailto:support@tditechnologies.com) to request them.
- 490    2. Run the installer `cw_server_<version>.exe`.
- 491    3. Download the Splunk universal forwarder installer from the  
492       [https://www.splunk.com/en\\_us/download/universal-forwarder.html](https://www.splunk.com/en_us/download/universal-forwarder.html) website. A username and  
493       password are required. An account can be created on the Splunk website.
- 494    4. Use the `splunkforwarder-<version>-x64-release.msi` installer to install the Splunk Universal  
495       Forwarder on the machine running the ConsoleWorks.

- 496 5. Connect to the Console at *https://10.100.1.6:5176*. Log in using the default credentials.

ADMIN: Server Management: Registration

Registration

ConsoleWorks Registration [Complete My Offline Registration](#)

Contact Name:

Contact Email:

Telephone:

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Seneca Highway

Address Line 2:

City: Rockville

State/Province: MD

Zip/Postal Code: 20850

Country: US

[PROXY DETAILS](#)

[ADVANCED OPTIONS](#)

View current registration status of all licenses

Register Online Register Offline Cancel Save

- 497 6. Fill in the details for **Registration**. Click **Register Online**. Click **Save**.
- 498

ADMIN: Server Management: Registration

Registration

ConsoleWorks Registration [Complete My Offline Registration](#)

Contact Name:

Contact Email:

Telephone:

Facility (Site) Name: NCCoE

Address Line 1: 9700 Great Seneca Highway

Address Line 2:

City: Rockville

State/Province: MD

Zip/Postal Code: 20850

Country: US

[PROXY DETAILS](#)

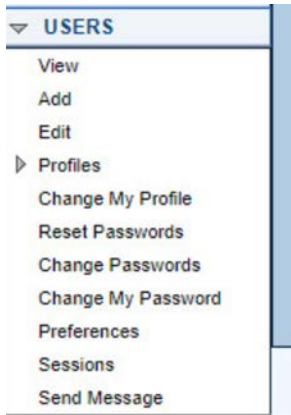
[ADVANCED OPTIONS](#)

View current registration status of all licenses

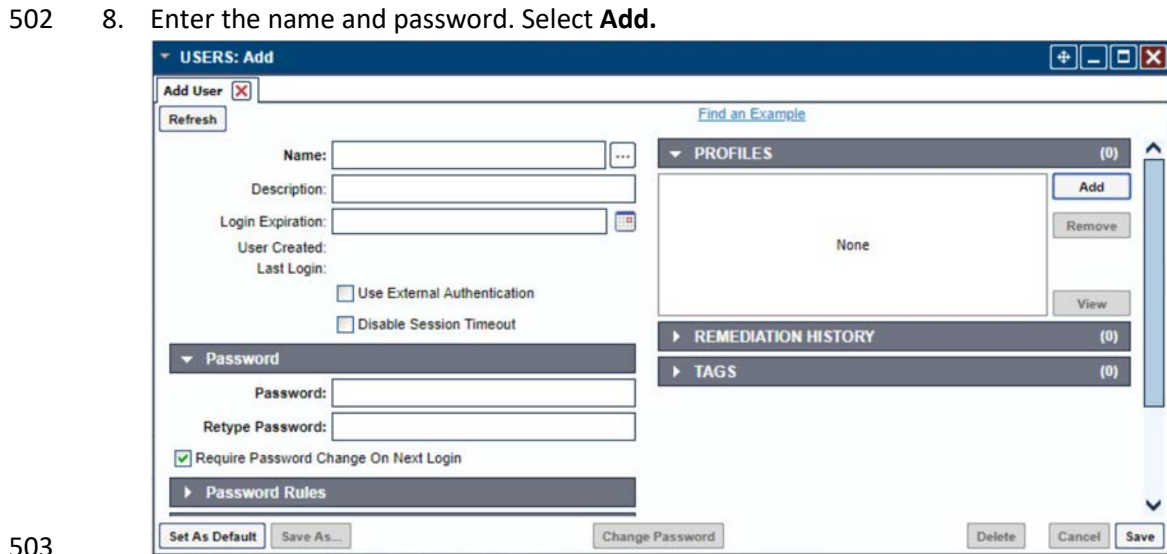
Register Online Register Offline Cancel Save

499

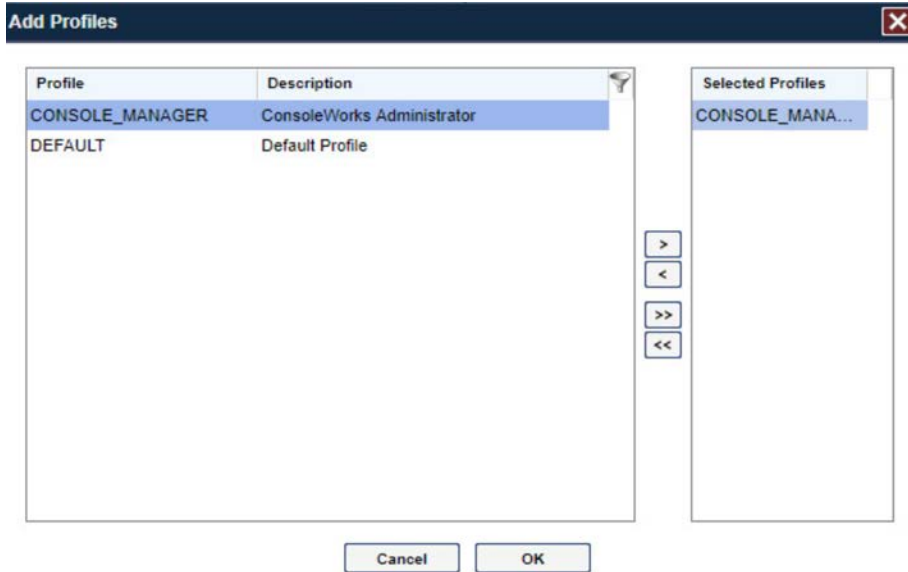
- 500 7. Create a new user. Navigate on left to **Users > Add**.



- 501 8. Enter the name and password. Select **Add**.



504 9. Add **CONSOLE\_MANAGER** as a selected profile, as shown in the screenshot below. Select **OK**.

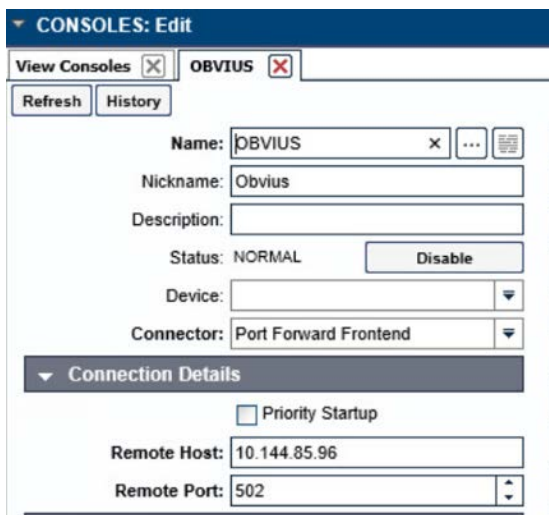


505  
506 10. Click **Save**.

507 *2.1.1.9 Configuration*

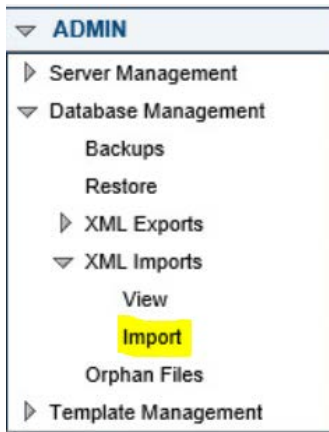
508 ConsoleWorks provides the scripts to query the Modbus server. The script provided is in XML format.

- 509 1. Navigate to **Consoles > Add**.
- 510 2. Enter a name and connection details that will be used to connect to the Obvius data acquisition
- 511 server. Select **Save**.



512

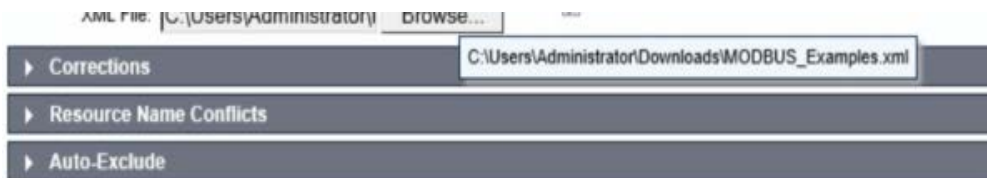
- 513 3. Navigate to **Admin > Database Management > XML Imports > Import**.



- 514
- 515 4. Select **Upload a file**, then click **Next**.



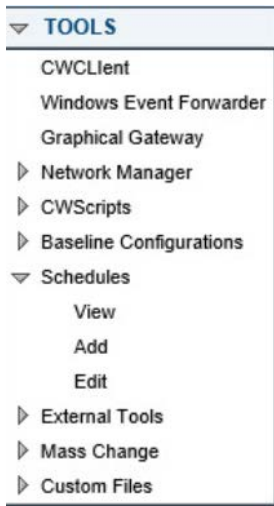
- 516
- 517 5. Click **Browse**, then find the XML file.



- 518
- 519 6. Click **Next**. ConsoleWorks will import the two CWScripts: *UTIL\_MODBUS* and *UTIL\_MODBUS\_GE*.

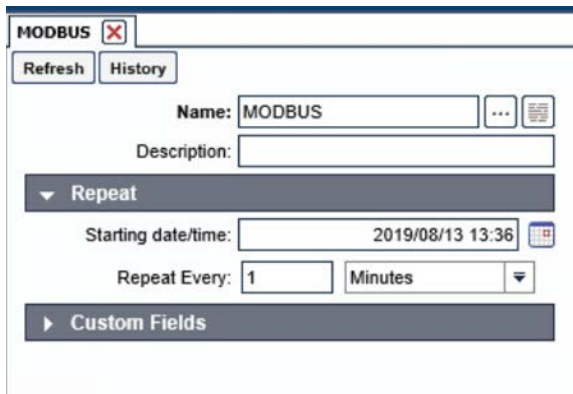


- 520
- 521 7. Navigate to **Tools > Schedule**. Click **Add**.



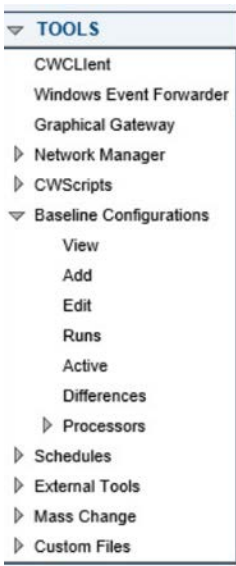
522

523 8. Name the schedule. Set the time to run at an acceptable interval, then **save**.



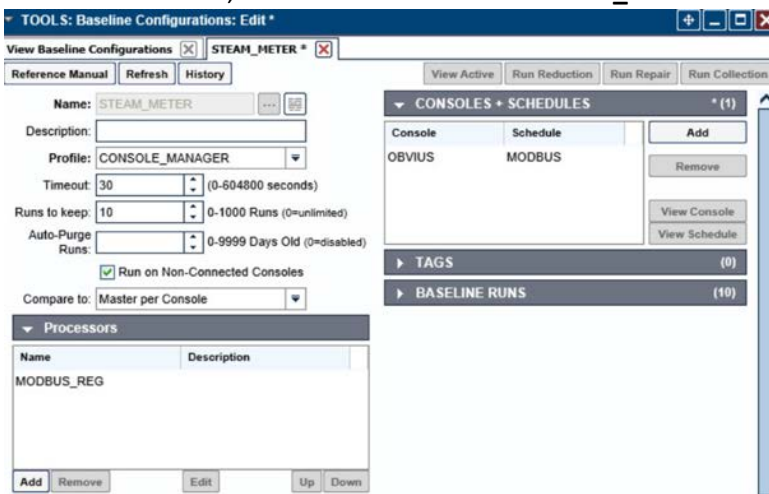
524

525 9. Navigate to **Tools > Baseline Configurations > Add.**



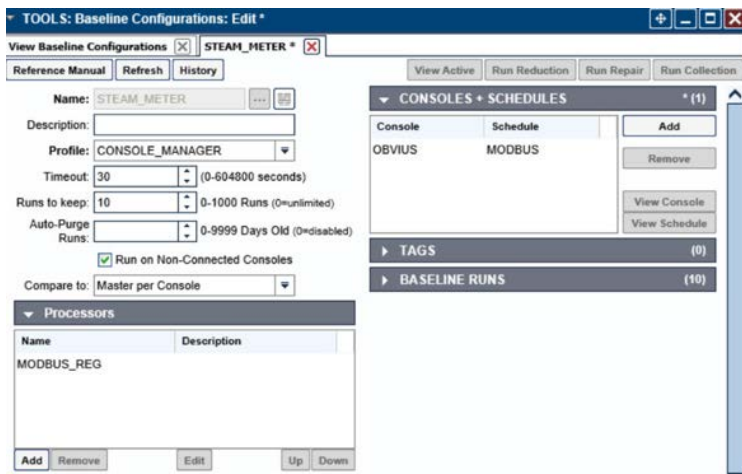
526

527 10. Name the baseline, and set the Profile to **CONSOLE\_MANAGER**.



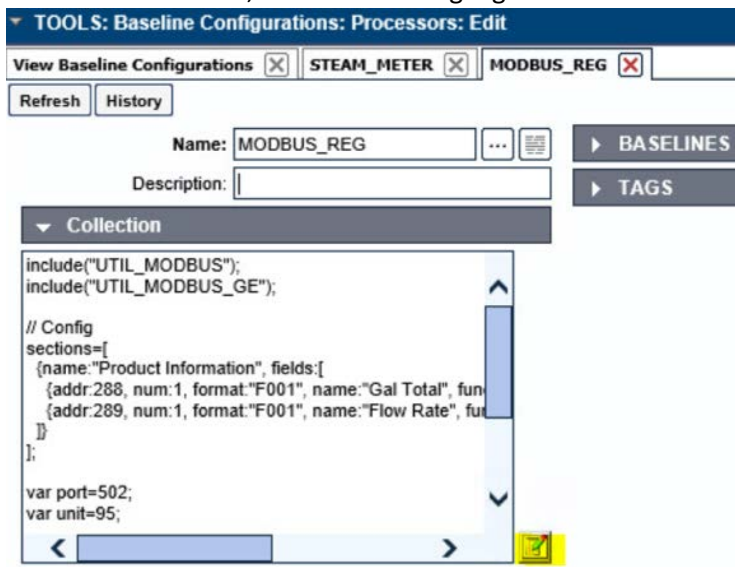
528

529 11. Create a Processor to collect the information from the OBVIUS server. Click **Add** under **Processors**.



530

531 12. Name the Processor, then click the highlighted button. Enter the text that follows, then click **Save**.



532

533 include("UTIL\_MODBUS");  
534 include("UTIL\_MODBUS\_GE");

535 // Config  
536 sections=[  
537 {name:"Product Information", fields:[  
538 {addr:288, num:1, format:"F001", name:"Gal Total", functionName:  
539 readHoldingRegisters},  
540 {addr:289, num:1, format:"F001", name:"Flow Rate", functionName:  
541 readHoldingRegisters},  
542 ]}  
543 ];



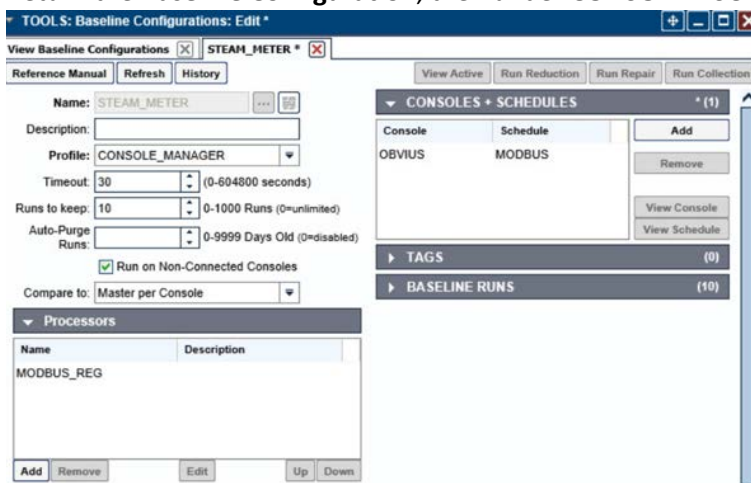
DRAFT

```
544 var port=502;
545 var unit=95;

546 // Execute
547 var server=console.port;

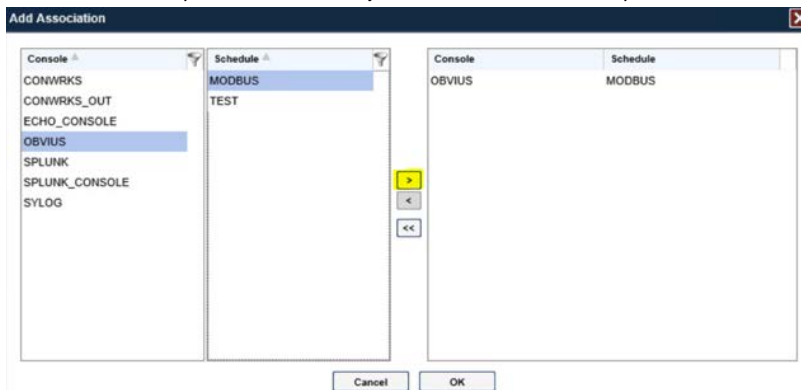
548 for(var s=0;s<sections.length;s++) {
549     setOutput(sections[s].name, formatGEOOutput(modbusConnection(server, port, unit,
550     sections[s].fields)));
551     log("SPLUNK",formatGEOOutput(modbusConnection(server, port, unit,
552     sections[s].fields)));
553 }
```

554 13. Return the **Baseline Configuration**, then under **CONSOLE + SCHEDULES**, select **Add**.



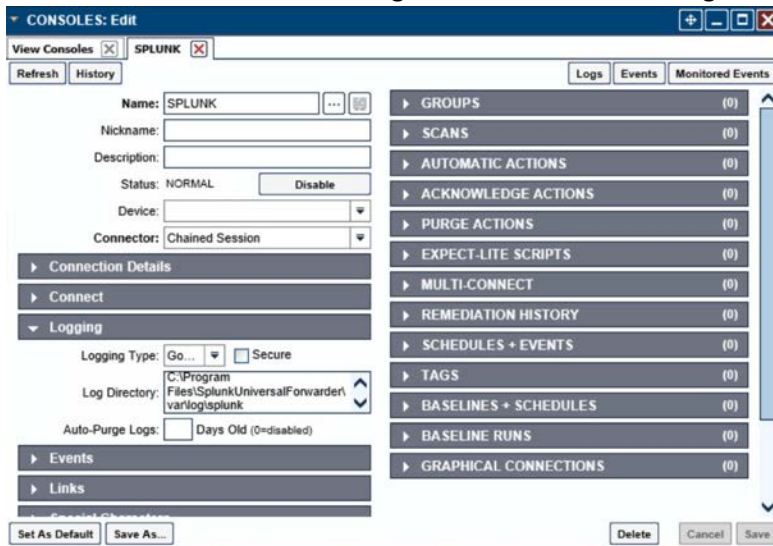
555

556 14. Under **Console**, select **OBVIUS**, and select **MODBUS**, then click **>**.



557

- 558 15. Create the SPLUNK console to log the collected Modbus registers at **Console > Add**.



- 559
- 560 16. Name the **Console**, and set the connector to **Chain Session**, the log type to **Governed**, and the Log
- 561 Directory to the below location:

562 `C:\Program Files\SplunkUniversalForwarder\log\splunk`

- 563 17. Navigate to `C:\Program Files\SplunkUniversalForwarder\etc\system\local\`

- 564 18. Add the following lines to the `outputs.conf` file:

565 `[tcpout:default-autolb-group]`

566 `server = 10.100.200.101:9997`

567 `[tcpout-server://10.100.200.101:9997]`

- 568 19. Add the following lines to the `inputs.conf` file:

569 `[monitor://$SPLUNK_HOME\var\log\splunk\SPLUNK.LOG*]`

570 `index = modbus`

## 571 2.2 Forescout CounterACT

572 Forescout CounterACT is used as a data collection and inventory tool. The CounterACT appliance actively

573 collects data from the ICS lab in Plano, Texas. The appliance reports back to the CounterACT Enterprise

574 Manager on the enterprise network in Rockville, Maryland. Once installed, the appliance is configured

575 and managed through the enterprise manager.

576 Forescout CounterACT can be deployed on virtual or physical appliances. For virtualized environments,  
577 VMware ESXi, Microsoft Hyper-V, and KVM hypervisors are supported. Large networks that require  
578 multiple physical or virtual appliances can be centrally managed by the Enterprise Manager.

579 <https://www.forescout.com/platform/specifications/#virtual-appliance>

580 Note: Some network-related information has been redacted.

## 581 2.2.1 CounterACT Enterprise Manager Configuration

### 582 2.2.1.1 VM Configuration

583 The CounterACT Enterprise Manager is configured as follows:

- 584     ▪ Red Hat Enterprise Linux 7
- 585     ▪ CPU cores
- 586     ▪ 16 GB of RAM
- 587     ▪ 200 GB of storage
- 588     ▪ 1 NIC

### 589 2.2.1.2 Network

590 Network Configuration (Interface 1):

- 591     ▪ IPv4: Manual
- 592     ▪ IPv6: disabled
- 593     ▪ IPv4 address: 10.100.100.33
- 594     ▪ Netmask: 255.255.255.0
- 595     ▪ Gateway: 10.100.100.1

### 596 2.2.1.3 Installation

597 To install CounterACT Enterprise Manager, refer to the installation guide available at

598 <https://www.forescout.com/company/resources/forescout-installation-guide-8-1/>.

### 599 2.2.1.4 Configuration

600 The following steps contain configuration instructions for scanning devices at the Plano location. For  
601 additional CounterACT configuration details, refer to the administration guide at

602 <https://www.forescout.com/wp-content/uploads/2018/11/counteract-administration-guide-8.0.1.pdf>.

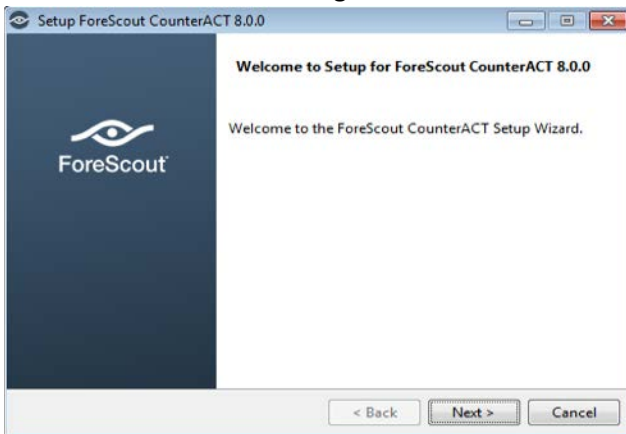
603 The CounterACT Enterprise Manager and CounterACT Appliance can be managed through the  
604 CounterACT console. Complete the following steps to install the console on a Windows desktop:

- 605 1. Download the executable from a Forescout portal.  
606 2. Select the CounterACT Console Setup file. The CounterACT Console software download screen  
607 opens.



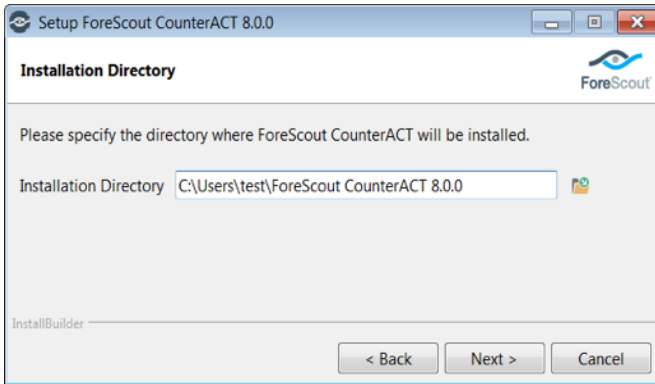
- 608  
609 3. Select the download link required, and save the EXE file.

- 610 4. Select and run the file to begin the installation. The **Setup Wizard** opens. Select **Next**.



611

- 612 5. Use the default installation directory. Click **Next**.



613

- 614 6. Click **Next**.

- 615 7. The installation begins. When completed, click **Finish**.

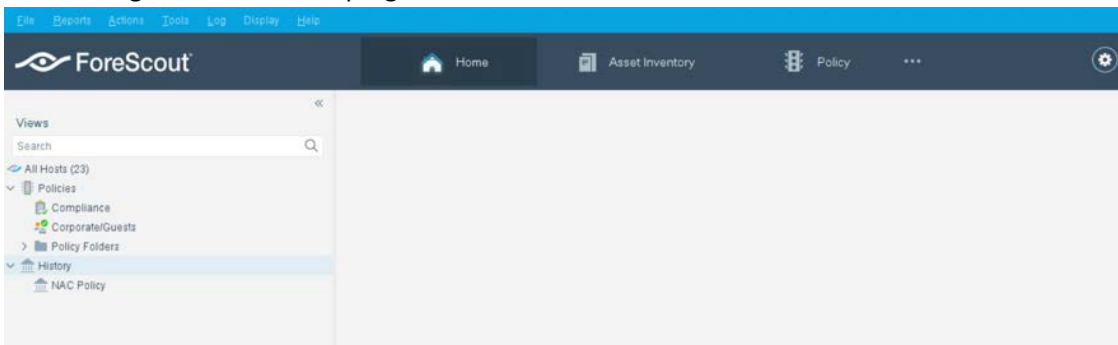


616

- 617 8. Connect to the Enterprise Manager with the Console and the password used during the CounterACT  
618 Enterprise Manager installation.

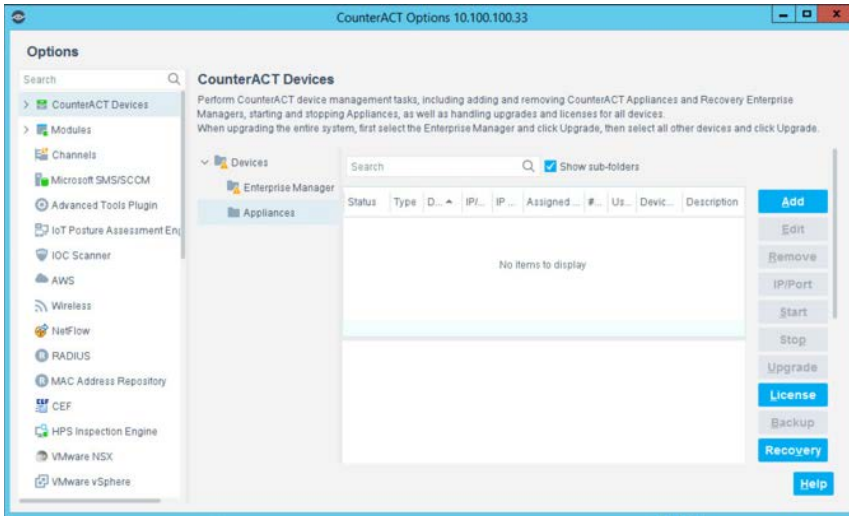


- 619  
620 9. Select the gear icon in the top right of console.

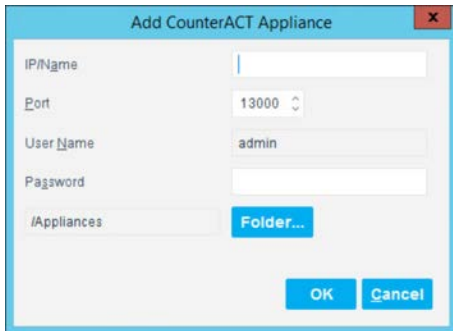


621

622 10. Select **Add**.

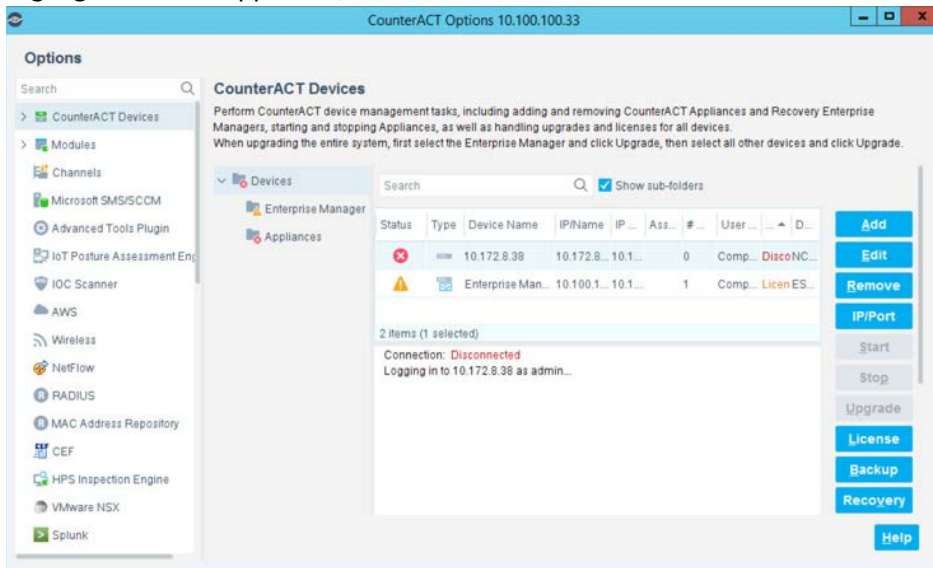


623  
624 11. Enter the internet protocol (IP) address of the appliance, and the admin password used in setup.  
625 12. Select **OK**.



626

627 13. Highlight the new appliance, and select **License**.



628

629 14. Enter the required information. Select **Submit**.

The screenshot shows a 'License Request Form' dialog box. It contains the following fields and options:

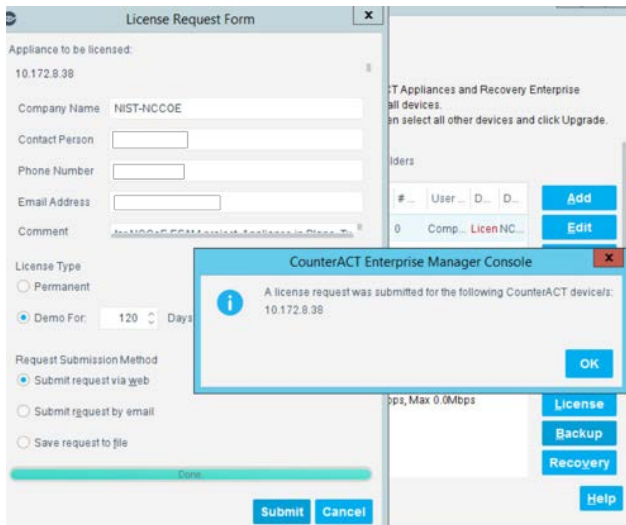
- Appliance to be licensed: 10.172.8.38
- Company Name: NIST-NCCOE
- Contact Person: [Empty field]
- Phone Number: [Empty field]
- Email Address: [Empty field]
- Comment: Inr NCCoF FSAM project Appliance in Plano, Tx
- License Type:
  - Permanent
  - Demo For: 120 Days
- Request Submission Method:
  - Submit request via web
  - Submit request by email
  - Save request to file

At the bottom right, there are 'Submit' and 'Cancel' buttons.

630



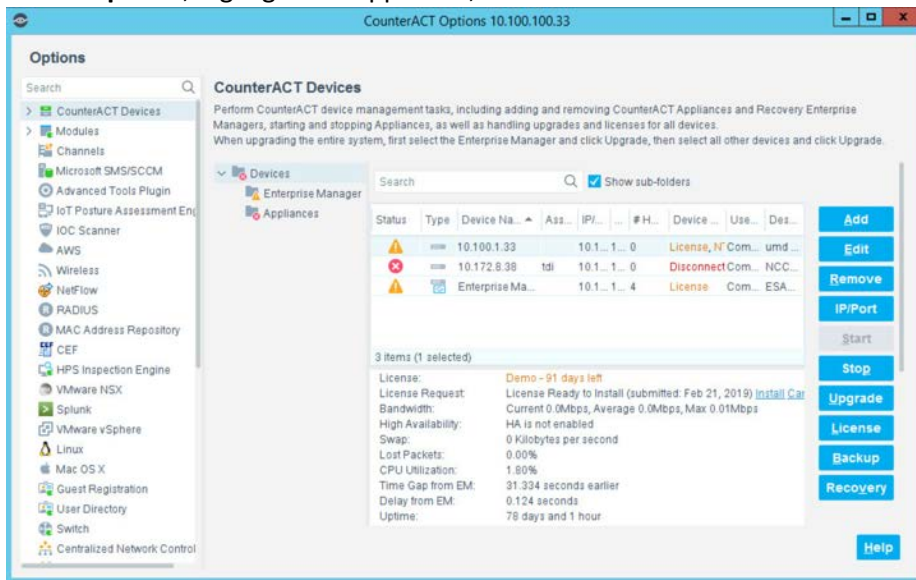
631 15. Select **OK**.



632

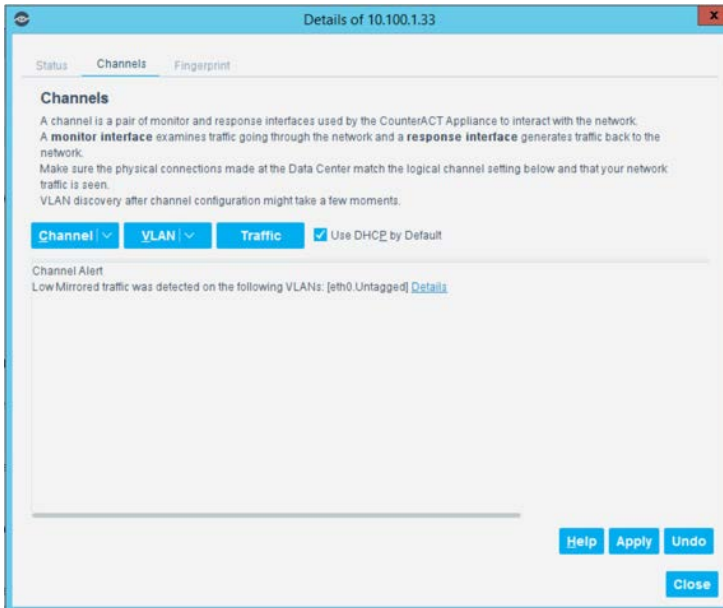
633 2.2.1.4.1 Appliance Interfaces Configurations

634 1. Under **Options**, highlight the appliance, and select **Edit**.



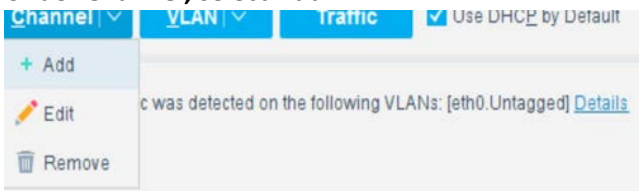
635

636 2. Select the **Channels** tab.



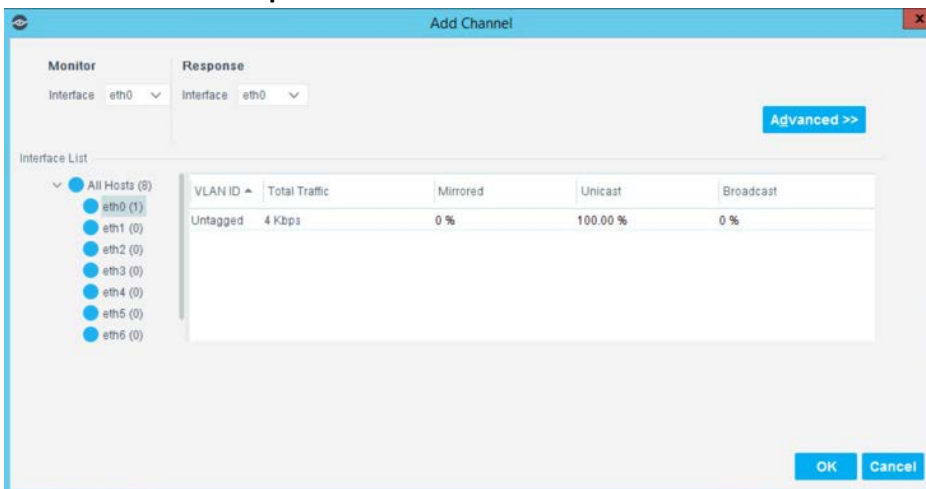
637

638 3. Under **Channel**, select **Add**.



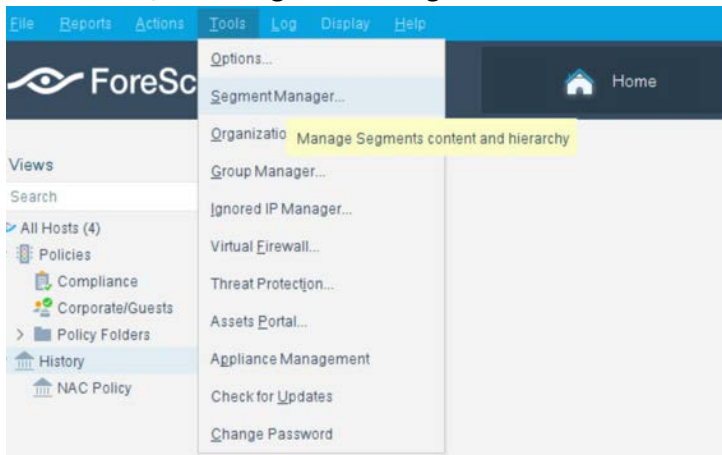
639

640 4. Use the drop-down to select the interface listening on a switched port analyzer (SPAN) switch for  
641 both **Monitor** and **Response**. Select **OK**.



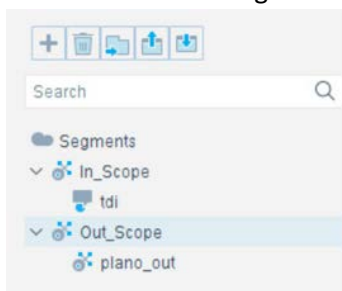
642

- 643 5. Under **Tools**, select **Segment Manager**.



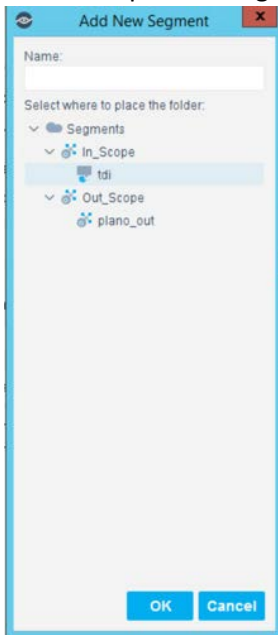
644

- 645 6. Select the + to add and name two segments called *In\_Scope* and *Out\_Scope*. Click **OK**. These will  
646 indicate which IP range should be scanned and which should not be scanned.



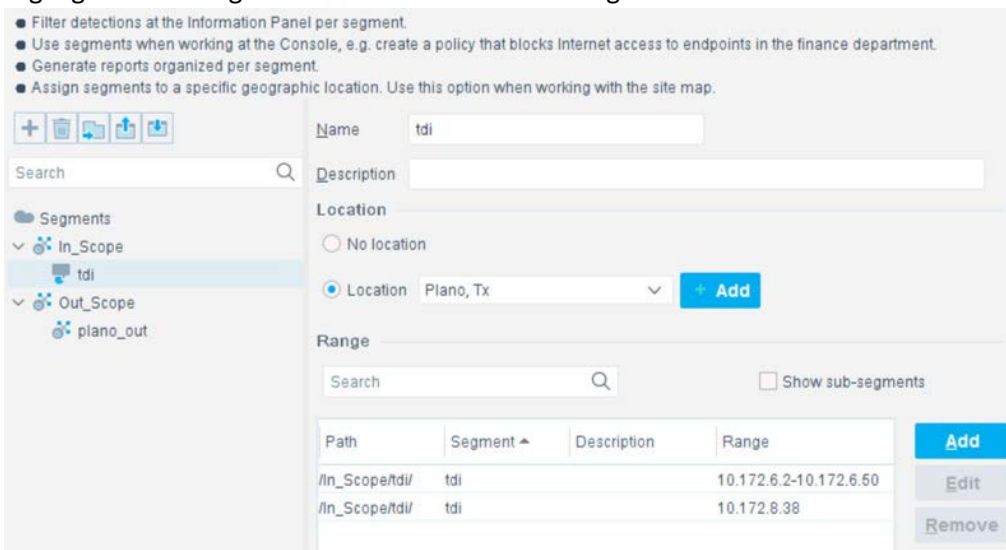
647

648 7. Select the plus icon again to add two subsegments shown in the screenshot below. Click **OK**.



649

650 8. Highlight the *tdi* segment. Click **Add** to add the range of IP addresses to scan. Click **OK**.



651

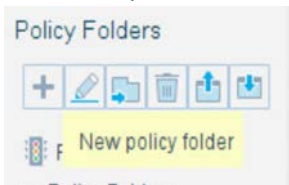
652 9. Repeat for the *plano\_out* segment for IP address to not scan. Click **OK**.

653 2.2.1.4.2 Upload Network Scan Policies

654 Forescout network scan policies are prewritten and delivered as an XML file.

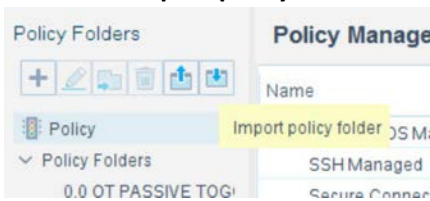
655 1. First, create a folder to house the polices. From the **Enterprise Manager** Console, select the **Policy**  
656 tab.

657 2. Select the plus icon to create a new folder.

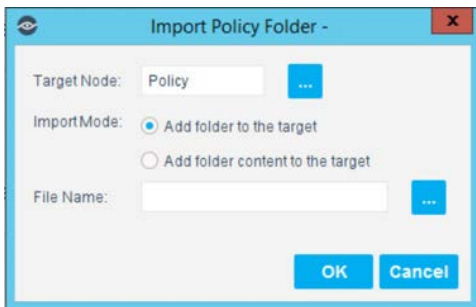


658  
659 3. Name the folder. Click **OK**.

660 4. Select the **import policy** icon.



661  
662 5. Select ... to locate the XML file.



663  
664 6. Select the XML file.

665 7. Select **OK**.

666 8. Repeat Steps 27–30 for each XML policy file.

667 9. Select **Start**. Select **Apply** to start and apply the changes.

#### 668 2.2.1.4.3 Splunk Integration

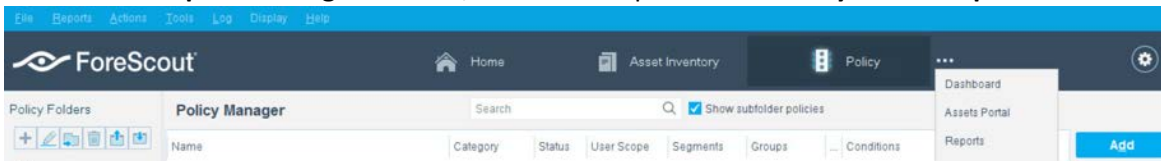
669 To complete Forescout Integration with Splunk, follow Forescout documentation found at

670 <https://www.forescout.com/platform/forescout-app-guide-splunk-2-7-0> and

671 <https://www.forescout.com/company/resources/extended-module-for-splunk-configuration-guide-2-8/>.

672 2.2.1.4.4 Schedule Reporting

673 1. From the **Enterprise Manager** Console, select the ellipsis next to **Policy**. Select **Reports**.



674  
675 2. Log in using the same credentials as the **Enterprise Manager** Console.

676 3. Select **Reports**.

677 4. Select **Add**.

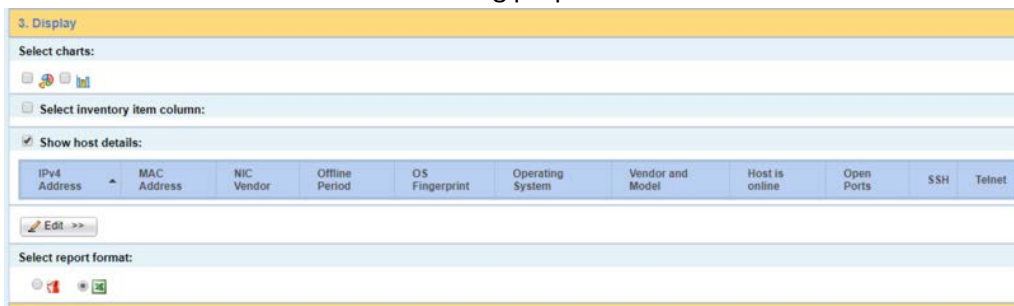


678  
679 5. Select the **Asset Inventory** template. Click **Next**.

680 6. Name the report. Select the **All IPs** toggle.

681 7. Select only the **Show host details**.

682 8. Edit the host details to show the following properties:



683  
684 9. Set a schedule. Enter an email address. Select **Save**.

685 2.2.2 CounterACT Appliance Configuration

686 2.2.2.1 Host Configuration

687 The CounterACT Appliance is delivered on a Dell PowerEdge R640 server with version 8.0.0.

### 688 *2.2.2.2 Network*

689 Network Configuration (Interface 1):

- 690     ▪ IPv4: Manual
- 691     ▪ IPv6: disabled
- 692     ▪ IPv4 address: 10.172.8.38
- 693     ▪ Netmask: 255.255.255.0
- 694     ▪ Gateway: 10.172.8.1

### 695 *2.2.2.3 Installation*

696 To install the CounterACT Appliance, follow the installation steps found at  
697 [https://www.forescout.com/wp-content/uploads/2018/10/CounterACT\\_Installation\\_Guide\\_8.0.1.pdf](https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf).

### 698 *2.2.2.4 Configuration*

699 After the CounterACT Appliance is installed, follow the steps outlined in Section 2.2.1, to connect the  
700 appliance to the enterprise manager and complete the configuration.

## 701 **2.3 Dragos Platform**

702 The Dragos Platform is an industrial control system cybersecurity-monitoring platform based around  
703 threat-behavior analytics. It is being used in this build to provide asset discovery and monitoring. A  
704 Dragos Sitestore is installed at the NCCoE enterprise site, and a midpoint sensor is installed at the Plano  
705 site. The Dragos sensor is managed by the site store.

### 706 **2.3.1 Dragos Sitestore Configuration**

707 In the example implementation, Dragos Sitestore is deployed as a pre-built appliance from the vendor.  
708 The appliance was still configured with parameters necessary for our environment. Connect to the  
709 Dragos appliance by navigating the web browser to *https://<IP address>*.

#### 710 *2.3.1.1 Host Configuration*

711 The Dragos Platform is delivered to the customer, preconfigured for the environment. The NCCoE  
712 received a Dell server utilizing iDRAC for virtualization. On the iDRAC server, VMware ESXi was installed  
713 and utilized for creating the server.

714 The VMs created to house the product have the following specifications:

- 715     ▪ Operating system (OS) Version: CentOS 7 (64-bit)
- 716     ▪ CPU: 48 cores

- 717       ▪ Memory: 192 GB
- 718       ▪ Hard disc drive (HDD) 1: 200 GB
- 719       ▪ HDD 2: 10 terabytes (TB)

### 720    2.3.1.2 Network

721    Networking for the device included a single network within ESXi to which the VM was connected. The  
722    Dell iDRAC server housing the Dragos Sitestore Puppet Server was connected to the ESAM network with  
723    the following IP addresses:

- 724       ▪ iDRAC: 10.100.200.6
- 725       ▪ ESXi: 10.100.200.7
- 726       ▪ Dragos Sitestore Puppet: 10.100.200.8

### 727    2.3.1.3 Installation

728    Installation began with setting up a VM. Utilizing the specifications in Section 2.3.1.1, Host  
729    Configuration, a VM was created for the Sitestore/Puppet server. Then the product ISO was added to  
730    the CD/DVD Drive 1 location (*DragosCustom-2019-06-18-CentOS-7-x86\_64-Everything-1810.iso*).

- 731    1. Power on the VM, and open a console. The **Dragos installation** screen will start, allowing options to  
732       be selected for installation type.
- 733    2. With the Dell R730 server used for the NCCoE, select **Install Dragos Sitestore Kickstart**. The installer  
734       automatically installs the Dragos Platform without interaction from the user.

### 735    2.3.1.4 Configuration

736    Once the installation has completed, the Sitestore will be configured with the needed files listed in Table  
737    2-1.

738    **Table 2-1 Dragos Required Files**

Dragos Files	
<i>sitestore-orchestration-1.5.1.1-1.noarch.rpm.gpg</i>	<i>midpoint-images-1.5.1.1-1.x86_64.rpm.gpg</i>
<i>midpoint-configs-1.5.1.1-1.x86_64.rpm.gpg</i>	<i>midpoint-manager-1.1.2-1.el7.x86_64.rpm.gpg</i>
<i>midpoint-1.5.1.1-1.x86_64.rpm.gpg</i>	<i>mms-cli-1.1.0-1.x86_64.rpm.gpg</i>
<i>upgrade-1.5.1-3.tar.gz.gpg</i>	<i>containerd.io-1.2.0-3.el7.x86_64.rpm</i>
<i>container-selinux-2.68-1.el7.noarch.rpm</i>	<i>docker-ce-18.09.0-3.el7.x86_64.rpm</i>
<i>docker-ce-cli-18.09.0-3.el7.x86_64.rpm</i>	

- 739    1. Upload these files to the Sitestore VM in */var/opt/releases/*.



- 740 2. Change directory to `/var/opt/releases/` and run the command `gpg --decrypt-file *.gpg`. Enter  
741 the password supplied from Dragos for the installation. This will create all the files required for the  
742 installation.
- 743 3. Change directory to `/root/` and, as root user, run `./puppet_server_setup.sh`

## 744 2.3.2 Dragos Midpoint Sensor

745 Dragos Midpoint Sensor is also deployed as a pre-built appliance from the vendor. Options for the  
746 midpoint sensor consist of configurations for small, medium, and large deployments. The appliance is  
747 configured with parameters necessary for our environment. The Dragos Midpoint Sensor can be  
748 managed from the Sitestore.

### 749 2.3.2.1 Network

750 The midpoint sensor has multiple interfaces. One interface will collect traffic via SPAN port. Another will  
751 serve as the management interface to communicate with the device.

752 Dragos Midpoint Sensor Management Interface:

- 753     ▪ DHCP: disabled
- 754     ▪ IPv6: ignore
- 755     ▪ IPv4: Manual
- 756     ▪ IPv4 address: 10.172.6.10
- 757     ▪ Netmask: 255.255.255.0

### 758 2.3.2.2 Configuration

759 After the midpoint sensor is deployed and listening on the correct interface, the midpoint sensor can  
760 connect back to the Sitestore for further configurations.

## 761 2.3.3 Dragos Splunk Integration

762 The Dragos Splunk application allows data integration from the Dragos Sitestore into the Splunk  
763 dashboard. This allows Splunk to aggregate data from Dragos and other products into a central location  
764 for analyst visualization. This process assumes the reader has downloaded the Dragos Splunk application  
765 from <https://splunkbase.splunk.com/app/4601/>.

- 766 1. To begin, log in to the Splunk instance, and select the gear icon on the top left of the screen next to  
767 **Apps**, to configure the applications.
- 768 2. On the top right of the screen, select **Install app from the file**.

- 769 3. Follow the on-screen instructions to upload the downloaded application.
- 770 4. Restart Splunk (either prompted by the installation process or self-directed).
- 771 5. From the Splunk **Settings** menu on the top right, select the **Data Inputs** option.
- 772 6. Select **Add New** under **Local Inputs** for a transmission control protocol (TCP) listener. (User  
773 datagram protocol [UDP] is not recommended, because it will cut off longer messages.)
- 774 7. Set the port to the one that you want to transfer data on. (NCCoE build used **10514**.)
- 775 8. Select **Next** to configure the Input Settings.
- 776 9. Choose **dragos\_alert** as the source type.
- 777 10. Set the **App Context** to **Dragos Splunk App**.
- 778 11. Set the **Index** to **dragos\_alerts**. (Create a new index if it does not exist.)
- 779 12. Click **Submit**.

780 Once this process is completed, Splunk is ready to receive data from Dragos. The following instructions  
781 will be for configuring the Dragos Sitestore for sending information to Splunk:

- 782 1. Navigate to the **Servers** tab at <https://<sitestore>/syslog/app/#/servers>.
- 783 2. Click **+ Add Server** to create a new server.
- 784 3. Configure the connection information to point to the Splunk server configured previously.
- 785 4. Set the following options:
  - 786 a. Protocol: TCP
  - 787 b. Message Format: RFC 5424 Modern Syslog
  - 788 c. Message Delimiter: Use newline delimiter for TCP and transport layer security (TLS) streams.
- 789 5. Click **NEXT: SET TEMPLATE**.
- 790 6. Set the following value (must be on one line for Splunk to properly process) as **Message**:

```
791 { "app": "dragos:platform", "body": "${content}", "category": "${summary}",
792 "created_at": "#{createdAt}", "dest": "${dest_asset_ip}",
793 "dest_dragos_id": "${dest_asset_id}", "dest_host":
794 "${dest_asset_hostname}", "dest_ip": "${dest_asset_ip}", "dest_mac":
795 "${dest_asset_mac}", "dest_name": "${dest_asset_domain}",
796 "dragos_detection_quad": "${detection_quad}", "dragos_detector_id":
797 "${detector_id}", "dvc": "${asset_ip}", "dvc_dragos_id":
798 "${dest_asset_id}", "dvc_host": "${dest_asset_hostname}", "dvc_ip":
799 "${asset_ip}", "dvc_mac": "${dest_asset_mac}", "dvc_name":
```

```
800   "${dest_asset_domain}", "id": "${id}", "ids_type": "network",  
801   "occurred_at": "#{occurredAt}", "severity_id": "${severity}",  
802   "signature": "${source}", "src": "${src_asset_ip}", "src_dragos_id":  
803   "${src_asset_id}", "src_host": "${src_asset_hostname}", "src_ip":  
804   "${src_asset_ip}", "src_mac": "${src_asset_mac}", "src_name":  
805   "${src_asset_domain}", "subject": "${type}", "type": "alert",  
806   "vendor_product": "Dragos Platform" }
```

807 7. Select **Save**.

## 808 2.4 FoxGuard Patch and Update Management Program

809 The solution utilizes the FoxGuard PUMP to provide patch availability and vulnerability notifications for  
810 identified assets. For this build, ConsoleWorks collects asset data from Splunk then converts that data  
811 into the JavaScript object notation (JSON) format required for PUMP. The resulting JSON file includes  
812 asset information such as vendor, product, and version, as well as serial and model information about  
813 devices from the asset inventory. Asset data often contains critical details. However, PUMP does not  
814 require sensitive data, such as asset location and IP address. The file is encrypted and provided to the  
815 PUMP team via secure delivery. FoxGuard's preferred method of file transfer is secure file transfer  
816 protocol and does not require direct access to an entities network.

817 Once the asset data is received, the FoxGuard team analyzes the file for completeness. Any missing data,  
818 such as a serial number, version, or access to private patch data, is collected during the onboarding  
819 process with the end user. The final report is provided back to ConsoleWorks in a JSON file format and  
820 includes available patches and vulnerability notifications for each device. The data is then ingested back  
821 into Splunk for viewing and reporting. Reports are also available outside of the ConsoleWorks  
822 integration in portable document format (PDF) and comma separated value (CSV) format.

823 PUMP is a service managed by the FoxGuard team. The patch availability and vulnerability notification  
824 report does not require an installation. See Section 2.1 for configuring ConsoleWorks to automatically  
825 create the required JSON input file for the integration described in this guide.

### 826 2.4.1 Patch Report

827 Below are screenshots from the final patch report for this build.

828 **Figure 2-1 Update Availability Summary**

Update Availability Summary

The following table outlines a summary of all devices, patches and updates. This list includes all devices and/or applications within the scope of this document. Where devices manufacturers have released an update in a particular month, the reader will be advised to refer to a more detailed write-up subsequently listed in the report. All entries in the summary tables will be entered in alphabetical order by vendor, then device/software application starting with available patches first.

Devices & Applications

Vendor	Device	Model No.	Patch/Update Released?	Patch Name	FoxGuard Review Date	Vendor Release Date	Update Type	Error Message
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	Private - Available Upon Request	1/14/2019	12/22/2018	Potential Security Related	N/A
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	Private - Available Upon Request	2/5/2019	01/15/2019	Non-Security	N/A
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	Private - Available Upon Request	3/26/2019	03/12/2019	Non-Security	N/A
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	Private - Available Upon Request	6/6/2019	05/18/2019	Non-Security	N/A
Schweitzer Engineering Laboratories (SEL)	SEL-451-X	R3XX	Yes	Private - Available Upon Request	1/15/2019	12/28/2018	Non-Security	N/A

829

Vendor	Device	Model No.	Patch/Update Released?	Patch Name	FoxGuard Review Date	Vendor Release Date	Update Type	Error Message
Schweitzer Engineering Laboratories (SEL)	SEL-3610XX	N/A	No	N/A	8/21/2019	N/A	N/A	N/A
Schweitzer Engineering Laboratories (SEL)	SEL-362XX	N/A	No	N/A	8/21/2019	N/A	N/A	N/A
Siemens	RSG-XXXX	4.x	No	N/A	9/6/2019	N/A	N/A	N/A
Siemens	RuggedCom RSXXX	Latest	No	N/A	9/4/2019	N/A	N/A	N/A

830

831 Figure 2-2 Device Update Availability Details-1

**Device Update Availability Details**

The entries listed on subsequent pages provide detailed information of the patches and updates released for a particular device.

Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

*Release Information*

<b>Vendor Name</b>	Schweitzer Engineering Laboratories (SEL)
<b>Vendor Product</b>	SEL-3530-X
<b>Model No/Version</b>	Latest
<b>OS/Firmware</b>	N/A
<b>Patch Name</b>	Private - Available Upon Request
<b>Release Date</b>	12/22/2018
<b>Filename</b>	Not Available - Customer Login Required
<b>SHA1</b>	5465a09b32a8f4881188beac1e1940f619a43e80
<b>SHA256</b>	5591694c3777eacfdab9949ced81b18be4c6c9e267c4fa2e2fdd7733ec1113e

*Update Classification*

<b>Severity</b>	Unknown
<b>Update Type</b>	PotentialSecurityRelated
<b>Security Summary</b>	NA

*CVE IDs*

<b>CVE ID</b>	<b>CVSS 2.0 Score</b>	<b>CVE Summary</b>

*Download Link(s)*

<b>Patch Download</b>	Private - Available Upon Request
<b>Release Notes</b>	Private - Available Upon Request

*Additional Comment(s)*

<b>Comment</b>	Instruction manual not updated to include latest firmware at the time of mining. If you would like to receive the latest Firmware for your installed product, please contact your SEL Sales Representative.
----------------	---

832

833 Figure 2-3 Device Update Availability Details-2

Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

*Release Information*

<b>Vendor Name</b>	Schweitzer Engineering Laboratories (SEL)
<b>Vendor Product</b>	SEL-3530-X
<b>Model No/Version</b>	Latest
<b>OS/Firmware</b>	N/A
<b>Patch Name</b>	Private - Available Upon Request
<b>Release Date</b>	01/15/2019
<b>Filename</b>	Not Available - Customer Login Required
<b>SHA1</b>	6a672a1eedf90dcc7fccf42a52b8bb2c798d2772
<b>SHA256</b>	a50c4b4188fef7be4d66e9041705cb25d7fca8b248360c7aca3f0e4fb069ab94

*Update Classification*

<b>Severity</b>	Unknown
<b>Update Type</b>	Non-Security
<b>Security Summary</b>	NA

*CVE IDs*

CVE ID	CVSS 2.0 Score	CVE Summary

*Download Link(s)*

<b>Patch Download</b>	Private - Available Upon Request
<b>Release Notes</b>	Private - Available Upon Request

*Additional Comment(s)*

<b>Comment</b>	NA
----------------	----

**Note:** NA

834

835 Figure 2-4 Device Update Availability Details-3

Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

*Release Information*

<b>Vendor Name</b>	Schweitzer Engineering Laboratories (SEL)
<b>Vendor Product</b>	SEL-3530-X
<b>Model No/Version</b>	Latest
<b>OS/Firmware</b>	N/A
<b>Patch Name</b>	Private - Available Upon Request
<b>Release Date</b>	03/12/2019
<b>Filename</b>	Not Available
<b>SHA1</b>	b811d84d088c13b3c54dde037fd6acab26a2a0f0
<b>SHA256</b>	6c64f292e3cd0c00f3058d4740c7f84d18d3b5afa73f2d6d6d8b1f7836cca16a

*Update Classification*

<b>Severity</b>	Unknown
<b>Update Type</b>	Non-Security
<b>Security Summary</b>	N/A

*CVE IDs*

CVE ID	CVSS 2.0 Score	CVE Summary

*Download Link(s)*

<b>Patch Download</b>	Private - Available Upon Request
<b>Release Notes</b>	Private - Available Upon Request

*Additional Comment(s)*

<b>Comment</b>	If you would like to receive the latest Firmware for your installed product, please contact your SEL Sales Representative.
----------------	--

**Note:** N/A

836

837 Figure 2-5 Device Update Availability Details-4

Schweitzer Engineering Laboratories (SEL) SEL-3530-X – Latest

*Release Information*

**Vendor Name** Schweitzer Engineering Laboratories (SEL)  
**Vendor Product** SEL-3530-X  
**Model No/Version** Latest  
**OS/Firmware** N/A  
**Patch Name** Private - Available Upon Request  
**Release Date** 05/18/2019  
**Filename** Not Available  
**SHA1** 70a1285fb6a711a29a710f0cc5f45af69694f087  
**SHA256** 409b8fa17f8989d5e75a1f4a4a8aab27e511eb2cd8b5fdc653117d9dd27064bb

*Update Classification*

**Severity** Unknown  
**Update Type** Non-Security  
**Security Summary** N/A

*CVE IDs*

CVE ID	CVSS 2.0 Score	CVE Summary

*Download Link(s)*

**Patch Download** Private - Available Upon Request  
**Release Notes** Private - Available Upon Request

*Additional Comment(s)*

**Comment** If you would like to receive the latest Firmware for your installed product, please contact your SEL Sales Representative.

**Note:** N/A

838



839 Figure 2-6 Device Update Availability Details-5

Schweitzer Engineering Laboratories (SEL) SEL-451-X – R3XX

*Release Information*

<b>Vendor Name</b>	Schweitzer Engineering Laboratories (SEL)
<b>Vendor Product</b>	SEL-451-X
<b>Model No/Version</b>	R3XX
<b>OS/Firmware</b>	N/A
<b>Patch Name</b>	Private - Available Upon Request
<b>Release Date</b>	12/28/2018
<b>Filename</b>	Not Available-Customer login required
<b>SHA1</b>	956351bd948001301a1c3726a0ece25a638aa4d0
<b>SHA256</b>	212ac18155b2b7a5d7cdabb7897c3b5cea1ebe84fb4c1bf31bd604ea5193a924

*Update Classification*

<b>Severity</b>	Unknown
<b>Update Type</b>	Non-Security
<b>Security Summary</b>	NA

*CVE IDs*

<b>CVE ID</b>	<b>CVSS 2.0 Score</b>	<b>CVE Summary</b>
---------------	-----------------------	--------------------

*Download Link(s)*

<b>Patch Download</b>	Private - Available Upon Request
<b>Release Notes</b>	Private - Available Upon Request

*Additional Comment(s)*

<b>Comment</b>	NA
----------------	----

840

841 **Figure 2-7 Patch Evidence Documentation**

**Patch Evidence Documentation**

The following table outlines a list of all devices with links to evidence of all patches released. This list includes all devices and/or applications within the scope of this document. Where devices manufacturers have released an update in a particular month, the evidence listed within the link will validate the patch information in this report. Where devices manufacturers have not released an update in a particular month, the evidence listed within the link will validate that no patches were released.

Vendor	Device	Model No.	Patch/Update Released?	FoxGuard Review Date	Patch Quantity Evidence Documentation Link
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	1/14/2019	<a href="https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX">https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX</a>
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	2/5/2019	<a href="https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX">https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX</a>
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	3/26/2019	<a href="https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX">https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX</a>
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	6/6/2019	<a href="https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX">https://portal.icsupdate.com/PatchEvidence/8267e758-edcb-a6e2-4340-525c4264cXXX</a>
Schweitzer Engineering Laboratories (SEL)	SEL-451-X	R3XX	Yes	1/15/2019	<a href="https://portal.icsupdate.com/PatchEvidence/9441285c-afc0-73cf-9acc-7084d9c45XXX">https://portal.icsupdate.com/PatchEvidence/9441285c-afc0-73cf-9acc-7084d9c45XXX</a>
Schweitzer Engineering Laboratories (SEL)	SEL-361XX	N/A	No	8/21/2019	<a href="https://portal.icsupdate.com/PatchEvidence/f263af0a-86c3-d608-464e-7b849f89cXXX">https://portal.icsupdate.com/PatchEvidence/f263af0a-86c3-d608-464e-7b849f89cXXX</a>
Schweitzer Engineering Laboratories (SEL)	SEL-362XX	N/A	No	8/21/2019	<a href="https://portal.icsupdate.com/PatchEvidence/62e1621a-5310-b484-9c6f-fcf958a5eXXX">https://portal.icsupdate.com/PatchEvidence/62e1621a-5310-b484-9c6f-fcf958a5eXXX</a>

842

Vendor	Device	Model No.	Patch/Update Released?	FoxGuard Review Date	Patch Quantity Evidence Documentation Link
Siemens	RSG-XXX	4.x	No	9/6/2019	<a href="https://portal.icsupdate.com/PatchEvidence/ca85e557-3317-2012-4b9f-c4cde2313XXX">https://portal.icsupdate.com/PatchEvidence/ca85e557-3317-2012-4b9f-c4cde2313XXX</a>
Siemens	RuggedCom RSXXX	Latest	No	9/4/2019	<a href="https://portal.icsupdate.com/PatchEvidence/81923124-e84c-9446-2fcc-83115646eXXX">https://portal.icsupdate.com/PatchEvidence/81923124-e84c-9446-2fcc-83115646eXXX</a>

843

844 **2.5 Kore Wireless**

845 This solution leverages a Kore Wireless virtual private network (VPN) to provide secure remote access to  
 846 remote assets. In this case, the remote asset is an Obvius A8812 Data Acquisition Server that provides  
 847 access to data from a Yokogawa flow meter.

848 Note: Some network information is excluded for security.

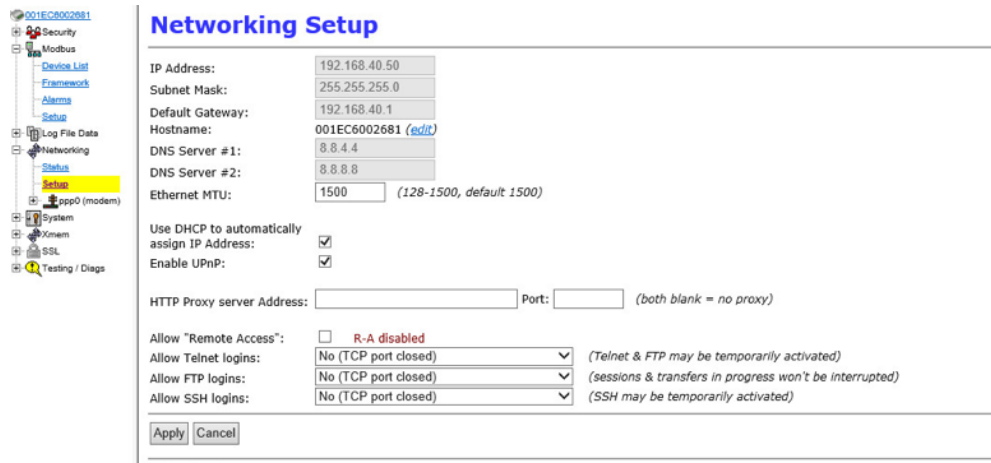
849 **2.5.1 Bridge Configuration**

850 **2.5.1.1 Installation**

- 851 1. Connect the MultiConnect eCell Ethernet port to the Ethernet port on the Obvius A8812 Data
- 852 Acquisition Server.
- 853 2. Connect the Obvius A8812 RS485 to the multidrop Modbus network with the remote steam meter
- 854 asset.

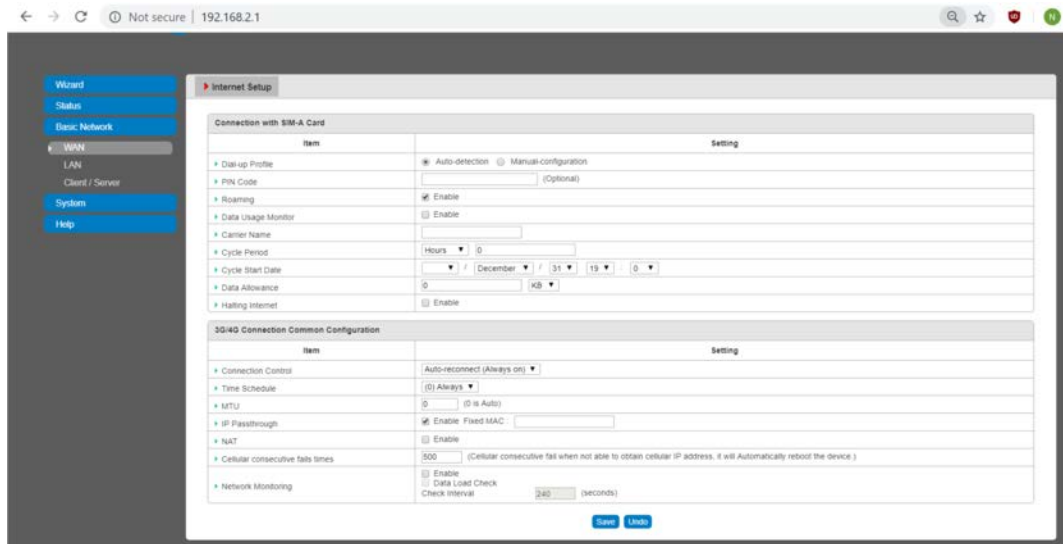
855 **2.5.1.2 Network**

- 856 1. Set Obvius A8812 to **DHCP**.
- 857 a. Navigate the IP address of the Obvius A8812. Default is *192.168.40.50*.
- 858 b. Open the **Networking** drop-down menu, and select **Setup**.
- 859 c. Check the **Use DHCP to automatically assign IP Address** checkbox.



- 860
- 861 2. Set MultiConnect eCell to Auto-detect Dialup profiles.
- 862 a. Navigate the IP address of the MultiConnect eCell. Default is *192.168.40.50*.
- 863 b. Open the **WAN** menu.

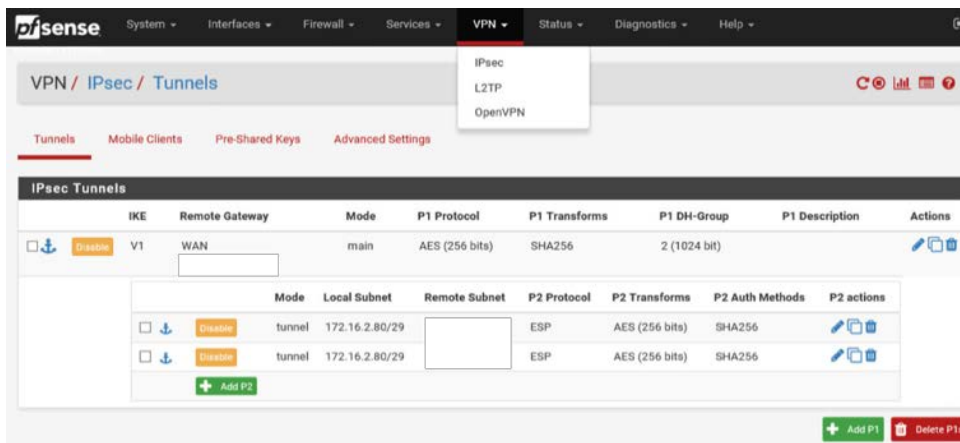
864 c. Set the Dial-up Profile to **Auto-detection**.



865

## 866 2.5.2 Virtual Private Network Configuration

867 1. Navigate to **VPN > IPsec** in pfSense.



868

869 2. Click the **Add P1** button.

870 3. Set **Remote Gateway**.

871 4. Set **Authentication Method** to Mutual PSK.

872 5. Set **Pre-Shared Key**.

873 6. Set **Encryption Algorithm** settings:

- 874 a. **Algorithm:** AES
- 875 b. **Key Length:** 256 bits
- 876 c. **Hash:** SHA256
- 877 d. **Diffie-Hellman Group:** 2 (1024 bit)

General Information	
<b>Disabled</b>	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
<b>Key Exchange version</b>	IKEv1 <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
<b>Internet Protocol</b>	IPv4 <small>Select the Internet Protocol family.</small>
<b>Interface</b>	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
<b>Remote Gateway</b>	<input type="text"/> <small>Enter the public IP address or host name of the remote gateway.</small>
<b>Description</b>	<input type="text"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Phase 1 Proposal (Authentication)	
<b>Authentication Method</b>	Mutual PSK <small>Must match the setting chosen on the remote side.</small>
<b>Negotiation mode</b>	Main <small>Aggressive is more flexible, but less secure.</small>
<b>My identifier</b>	My IP address
<b>Peer identifier</b>	Peer IP address
<b>Pre-Shared Key</b>	<input type="text"/> <small>Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.</small> <a href="#">Generate new Pre-Shared Key</a>
Phase 1 Proposal (Encryption Algorithm)	
<b>Encryption Algorithm</b>	AES 256 bits SHA256 2 (1024 bit) <a href="#">Delete</a> <small>Algorithm Key length Hash DH Group</small>

- 878
- 879 7. Return to **VPN > IPsec**.
- 880 8. Click the **Add P2** button.
- 881 9. Set **Local Network** to 172.16.2.80/29.
- 882 10. Set **Remote Network**.
- 883 11. Set **Protocol** to ESP.
- 884 12. Set **Encryption Algorithm** to AE 256 bits.

885 13. Set **Hash Algorithm** to SHA256 .

General Information	
<b>Disabled</b>	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
<b>Mode</b>	Tunnel IPv4
<b>Local Network</b>	Network: 172.16.2.80 / 29 Type: Address Local network component of this IPsec security association.
<b>NAT/BINAT translation</b>	None Type: Address If NAT/BINAT is required on this network specify the address to be translated
<b>Remote Network</b>	Address: 10.144.85.96 / 0 Type: Address Remote network component of this IPsec security association.
<b>Description</b>	A description may be entered here for administrative reference (not parsed).
Phase 2 Proposal (SA/Key Exchange)	
<b>Protocol</b>	ESP Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.
<b>Encryption Algorithms</b>	<input checked="" type="checkbox"/> AES 256 bits <input type="checkbox"/> AES128-GCM Auto <input type="checkbox"/> AES192-GCM Auto <input type="checkbox"/> AES256-GCM Auto <input type="checkbox"/> Blowfish Auto <input type="checkbox"/> 3DES <input type="checkbox"/> CAST128 Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.
<b>Hash Algorithms</b>	<input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC

886

887 **2.6 pfSense VPN**

888 pfSense is an open-source firewall/router used to create both site-to-site VPN tunnels. The following  
 889 configuration file can be used to upload all configurations to the enterprise location edge router. Both  
 890 the UMD and Plano edge routers are excluded for security purposes.

891 **2.6.1 Plano and UMD VPN Configuration**

892 To configure a site-to-site OpenVPN connection, refer to  
 893 <https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html>.

894 **2.7 Splunk**

895 Splunk is a security information and event management (SIEM) system that allows collecting and parsing  
 896 logs and data from multiple systems.

## 897 2.7.1 Splunk Enterprise Configuration

### 898 2.7.1.1 VM Configuration

899 The Splunk VM is configured as follows:

- 900     ▪ Ubuntu Mate 16.04.2
- 901     ▪ 2 CPU cores
- 902     ▪ 10 GB of RAM
- 903     ▪ 2 TB of storage
- 904     ▪ 1 NIC

### 905 2.7.1.2 Network

906 Network Configuration (Interface 1):

- 907     ▪ IPv4: Manual
- 908     ▪ IPv6: disabled
- 909     ▪ IPv4 address: *10.100.200.101*
- 910     ▪ Netmask: *255.255.255.0*
- 911     ▪ Gateway: *10.100.200.1*

### 912 2.7.1.3 Installation

913 Note: A Splunk account will be needed to download Splunk Enterprise. The account is free and can be  
914 set up at [https://www.splunk.com/page/sign\\_up](https://www.splunk.com/page/sign_up).

915 Download Splunk Enterprise from [https://www.splunk.com/en\\_us/download/splunk-enterprise.html](https://www.splunk.com/en_us/download/splunk-enterprise.html).  
916 This build uses Version 7.1.3. Splunk can be installed on Windows, Linux, Solaris, and Mac OS X. Each of  
917 these installation instructions is provided at  
918 <http://docs.splunk.com/Documentation/Splunk/7.1.3/Installation/Beforeyouinstall>.

### 919 2.7.1.4 Universal Forwarder

920 To install the universal forwarder, refer to documentation found at  
921 <https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Installtheuniversalforwardersoftware>.  
922 [ware](https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Installtheuniversalforwardersoftware).

923 Refer to each individual product to configure the universal forwarder or another means of integration  
924 with Splunk.

### 925 [2.7.1.5 Reports and Alerts](#)

926 If desired, lookup tables can be used to cross-check automated detections with human knowledge of a  
 927 device. Some properties are cross-checked with human knowledge at both the UMD and Plano sites.  
 928 Patch information from PUMP also uses a lookup table to cross-check results with devices. To upload  
 929 lookup tables:

- 930 1. Log in to Splunk.
- 931 2. Go to **Settings > Lookups**.
- 932 3. Select **+ Add New** under **Lookup table files**.  
existing lookup tables or upload a new file.

---

[.up definitions](#) + Add new  
existing lookup definitions or define a new file-based or external lookup.

- 933
- 934 4. Choose **Search** as the **Destination App**.
- 935 5. Browse for the CSV file. Name the Lookup file. Select **Save**.

936 The UMD lookup CSV file contains the following fields:

```
937 Asset Id,IP,Device,Platform
```

938 The Plano lookup CSV file contains the following fields:

```
939 Asset Id,IP,Vendor,Product Name,Serial Number,Version
```

940 Once integrations are complete, the following Splunk queries will create the desired reports:

#### 941 [2.7.1.5.1 Asset Report for Both Sites](#)

```
942 index=_* OR index=* sourcetype=CTD_csv | table asset_id site_id name_ ip_ mac_ type_  

943 vendor_ criticality_ risk_level is_ghost | sort site_id | where isnum(asset_id)
```

#### 944 [2.7.1.5.2 Asset Report for UMD](#)

```
945 index=_* OR index=* sourcetype=CTD_csv | where isnum(asset_id) | table asset_id  

946 site_id name_ ip_ mac_ type_ vendor_ criticality_ risk_level is_ghost Device Platform  

947 | sort site_id | search ip_=206.189.122* | lookup umd_lookup.csv "Asset Id" AS  

948 asset_id OUTPUT "Device" AS Device, Platform AS Platform
```

#### 949 [2.7.1.5.3 Asset Report for Plano \(Static\)](#)

```
950 index=_* OR index=* sourcetype=CTD_csv | where isnum(asset_id) | table asset_id  

951 site_id name_ ip_ mac_ type_ vendor_ criticality_ risk_level is_ghost Serial_Number  

952 Version | sort site_id | search ip_=10.172.6* | lookup plano_lookup.csv "Asset Id" AS  

953 asset_id OUTPUT "Serial Number" AS Serial_Number, Version AS Version
```



#### 954 2.7.1.5.4 Asset Report for Plano (Dynamic)

```
955 index=forescout
956 |table ip mac "host_properties.nmap_banner7{}.value" nbthost
957 "host_properties.nmap_def_fp5{}.value" "host_properties.user_def_fp{}.value"
958 "host_properties.server_session{}.value"
959 |stats
960 values(mac),values("host_properties.nmap_banner7{}.value"),values(nbthost),values("hos
961 t_properties.nmap_def_fp5{}.value"),values("host_properties.user_def_fp{}.value"),valu
962 es("host_properties.server_session{}.value") by ip
963 |rename values(mac) as mac_address, values(host_properties.nmap_banner7{}.value) as
964 ports_and_services, values(nbthost) as hostname,
965 values(host_properties.nmap_def_fp5{}.value) as device_footprints,
966 values(host_properties.user_def_fp{}.value) as device_footprints2,
967 values(host_properties.server_session{}.value) as server_session_properties
```

#### 968 2.7.1.5.5 UMD Steam Meter Data

```
969 index=modbus |rex "CWScript BCM:(?<name>.\w+)" | rex field=_raw "Flow Rate :
970 (?<flowRate>.*)" | rex field=_raw "Gal Total : (?<GalTotal>.*)" | transaction
971 maxspan=30s | table name _time flowRate GalTotal
```

#### 972 2.7.1.5.6 UMD Device Data Calls

```
973 (index=* OR index=*) (index=main host="10.100.100.111" NOT "cs2=UP") | table shost
974 src smac dhost dst dmac cs6 cs3 cs7 cs8 msg
```

#### 975 2.7.1.5.7 Patch Report for FoxGuard PUMP

```
976 index=test sourcetype="csv" | lookup plano_lookup.csv "Asset Id" AS Asset_Id OUTPUT
977 "Serial Number" AS Serial_Number, Version AS Version | table Asset_Id IP Mac Vendor
978 "Operating System" Serial_Number Version Criticality Protocols | join IP type=left
979 [search index=test sourcetype=CTD_csv_report] | fields "Asset Id" IP Mac Vendor
980 "Operating System" Serial_Number Version | where isnotnull(Serial_Number) OR
981 isnotnull(Version) | sort IP | outputcsv patchreport.csv
```

## 982 2.8 Tripwire Industrial Visibility

983 Tripwire Industrial Visibility is used to passively scan the industrial control environments at both the  
984 College Park and Plano locations in the build. Tripwire Industrial Visibility builds a baseline of assets and  
985 network traffic between those assets then alerts on anomalous activity. Logs and alerts are reported up  
986 to the SIEM.

987 Tripwire Industrial Visibility is installed at three locations: Plano, Texas (TDi); UMD; and the NCCoE. This  
988 section describes how to deploy Tripwire Industrial Visibility 3.0.0.

989 Tripwire Industrial Visibility taps into OT network communication by listening through the SPAN port of  
990 routers and switches connected to the network segment, opening data packets, and interpreting  
991 protocols without disrupting normal operations.

992 By reading network traffic, it isolates all assets on the network and maps the flow of traffic between  
993 them. This data is then used to create graphical network maps.

## 994 **2.8.1 Tripwire Industrial Visibility Configuration UMD**

995 The following subsections document the software, hardware/VM, and network configurations for the  
996 Tripwire Industrial Visibility servers.

### 997 **2.8.1.1 VM Configuration**

998 The Tripwire Industrial Visibility VM was given the following resources:

- 999       ▪ CentOS 7.5
- 1000       ▪ 4 CPU cores
- 1001       ▪ 100 GB hard disk
- 1002       ▪ 32 GB RAM
- 1003       ▪ 2 NICs

### 1004 **2.8.1.2 Network Configuration**

1005 Network Configuration:

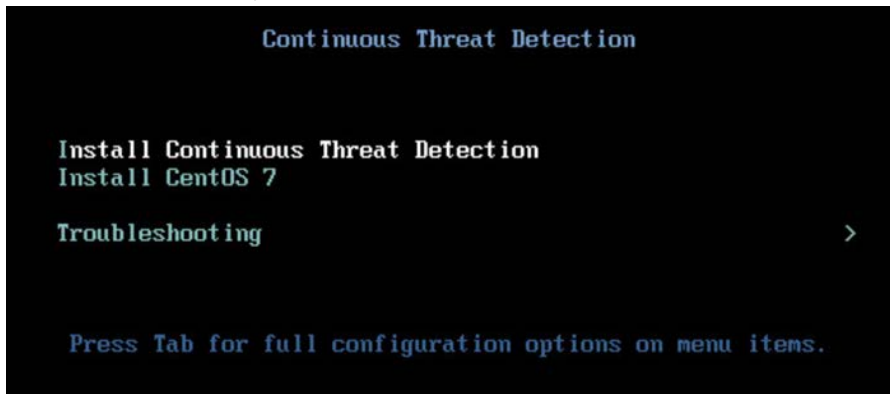
- 1006       ▪ DHCP: disabled
- 1007       ▪ IPv6: ignore
- 1008       ▪ IPv4: Manual
- 1009       ▪ IPv4 address: *10.100.100.111*
- 1010       ▪ Netmask: *255.255.255.0*
- 1011       ▪ Gateway: *10.100.100.1*

### 1012 **2.8.1.3 Installation**

1013 Tripwire supplied the Tripwire Industrial Visibility as an ISO installer. To configure TIV, use the ISO  
1014 installer for each instance at Plano, UMD, and the NCCoE. Tripwire Industrial Visibility is configured in a  
1015 sensor-server architecture. Plano and UMD instances act as sensors, and the NCCoE instance is the  
1016 central server.

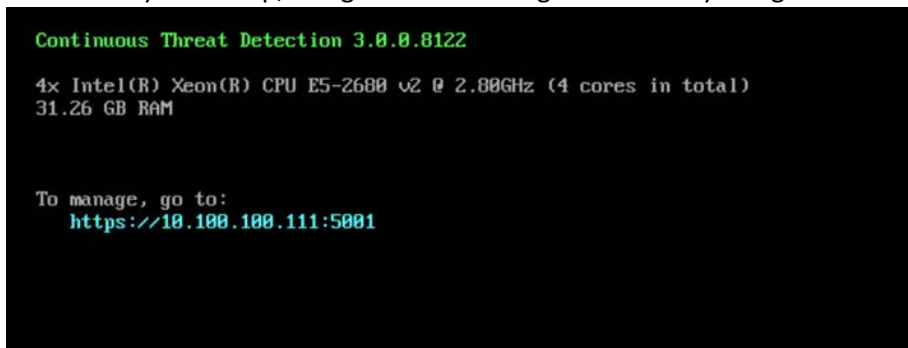
1017 To begin installation, mount the provided image to the VM, and complete the following steps:

- 1018 1. From the boot menu, select **Install Continuous Threat Detection**.



1019

- 1020 2. When the system is up, navigate to the configurator tool by using a browser.



1021

### 1022 *2.8.1.4 Configuration*

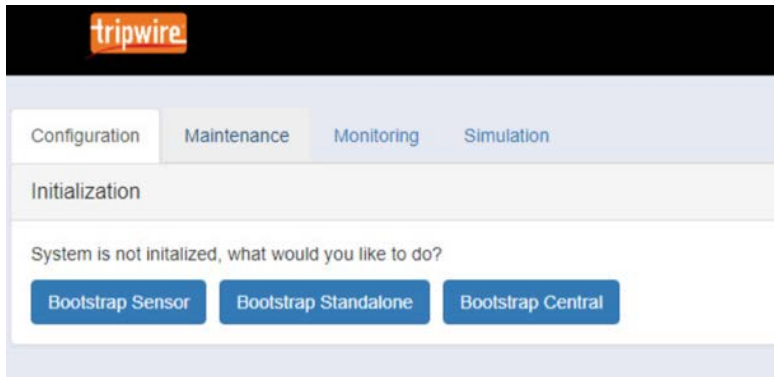
1023 Configure the Tripwire Industrial Visibility sensors.

- 1024 1. Connect to the configuration tool by entering the following URL into the browser:

1025 *https://10.100.100.11:5001.*

- 1026 2. Enter the default credentials.

- 1027 3. On the **Configuration** tab, the system will need to be initialized. Select **Bootstrap Sensor** (for Plan  
1028 and UMD sites).

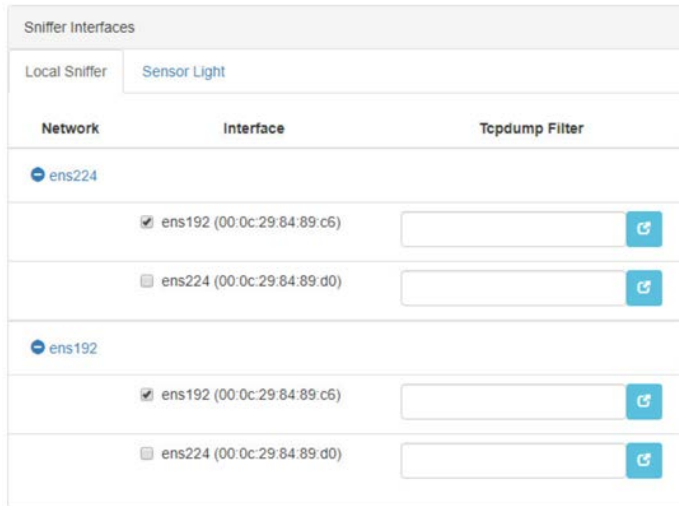


1029

1030 4. Enter the details and License Key. Select **Apply**.

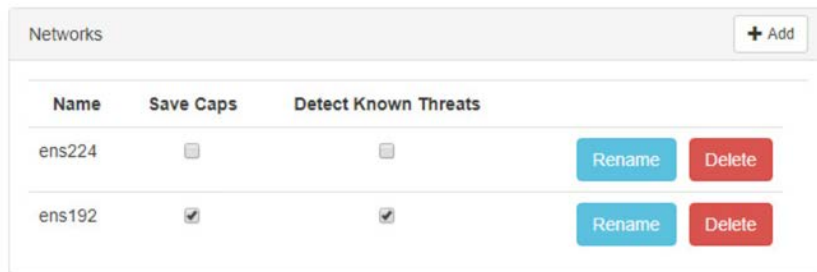
1031

1032 5. Set the Sniffer Interface on the **Configuration** tab. Select the interfacd used as the SPAN port.  
1033 Select **Apply**.



1034

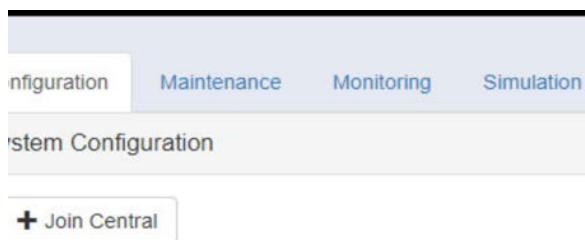
1035 6. Under **Networks**, select **Save Caps** and **Detect Known Threats** for the appropriate interface.



1036

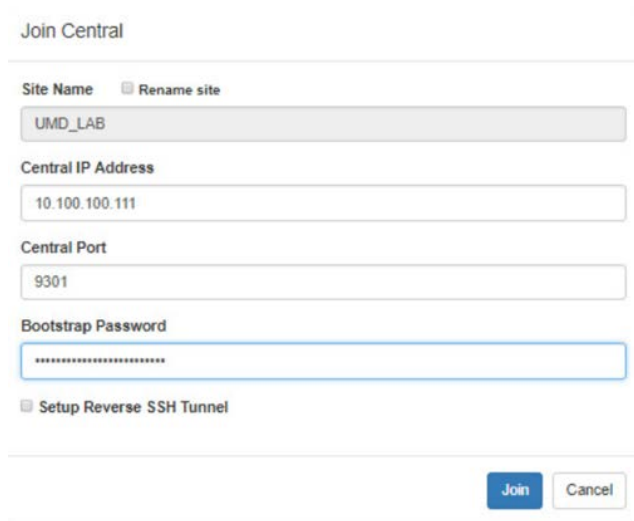
1037 7. Next, Join the Sensor to the Sensor Server. Set up the Central Server in Section 2.8.3 before  
1038 completing these steps.

1039 8. Select **Join Central**, from the **Configuration** tab.



1040

1041 9. Name the Sensor, and enter the IP address of the Central Server. Enter the Bootstrap password  
1042 found on the Central Server. Select **Join**.



Join Central

Site Name  Rename site

UMD\_LAB

Central IP Address

10.100.100.111

Central Port

9301

Bootstrap Password

\*\*\*\*\*

Setup Reverse SSH Tunnel

Join Cancel

1043

1044 10. Connect to the continuous threat detection (CTD) Dashboard: <https://10.100.1.17:5000>.

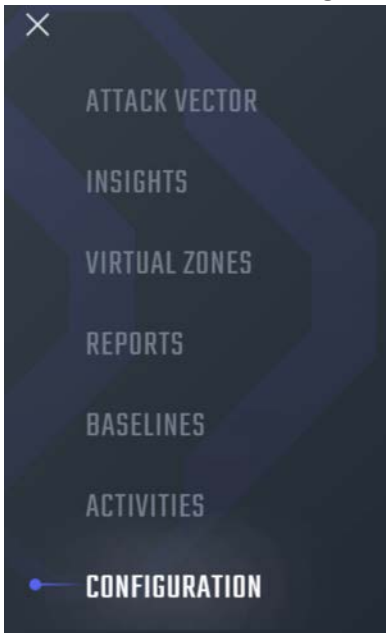
1045 The system is started in Training Mode. After an acceptable amount of time passes, place the system in  
1046 Operational Mode. This build used one month as the training period.

1047 1. Select the hamburger icon in the top left corner.



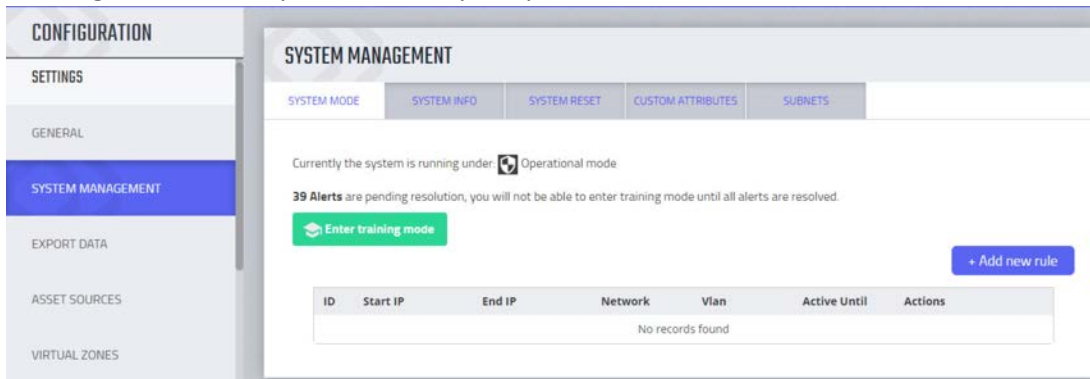
1048

1049 2. Scroll down to select **Configuration**.

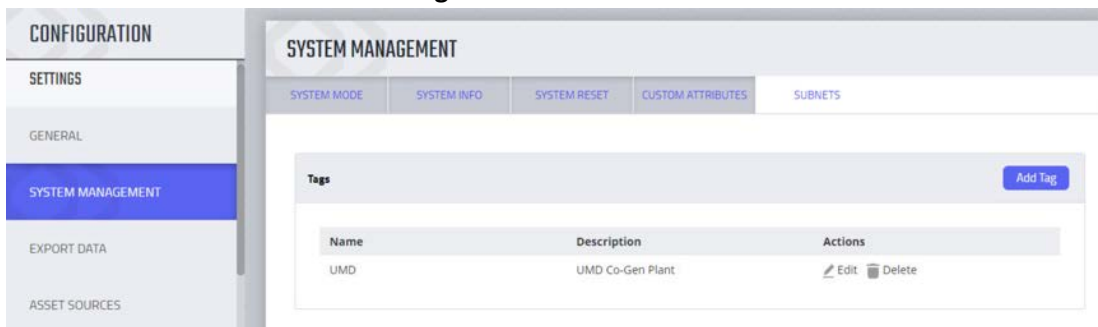


1050

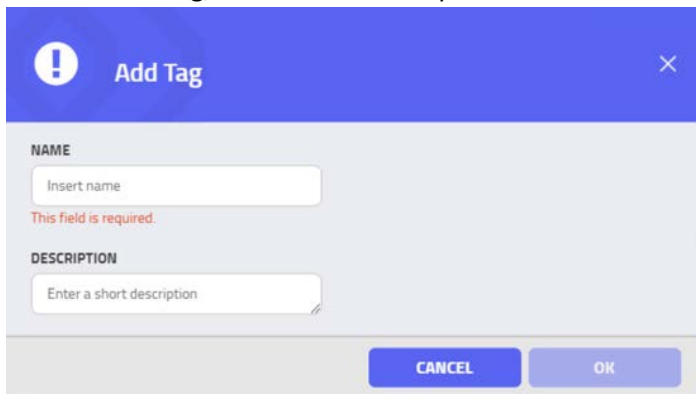
- 1051 3. Select **System Management**.
- 1052 4. Select the **System Mode** tab. Click **Enter Operational Mode**. Note: The screen will show **Enter**
- 1053 **Training Mode**, if the system is already in Operational Mode.



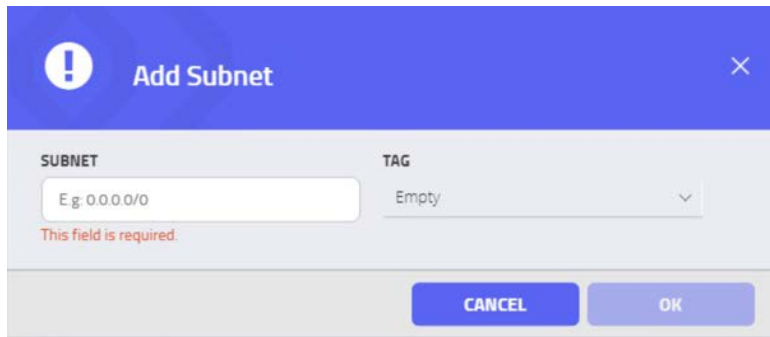
- 1054
- 1055 5. Select the **Subnets** tab. Click **Add Tag**.



- 1056
- 1057 6. Name a new Tag, and add the description. Select **OK**.



- 1058
- 1059 7. Click **Add Subnet**. Enter the Subnet that the assets are on and the previously created TAG. Select
- 1060 **OK**.



1061

1062 8. Repeat Steps 16 and 17 for multiple subnets.

## 1063 2.8.2 Tripwire Industrial Visibility Configuration Plano

1064 The following subsections document the software, hardware/VM, and network configurations for the  
1065 Tripwire Industrial Visibility servers.

### 1066 2.8.2.1 VM Configuration

1067 The Tripwire Industrial Visibility VM was given the following resources:

- 1068     ▪ CentOS 7.5
- 1069     ▪ 1 CPU Core
- 1070     ▪ 8 GB RAM
- 1071     ▪ 200 GB hard disk
- 1072     ▪ 3 NICs

### 1073 2.8.2.2 Network Configuration

1074 Network Configuration:

- 1075     ▪ DHCP: disabled
- 1076     ▪ IPv6: ignore
- 1077     ▪ IPv4: Manual
- 1078     ▪ IPv4 address: *10.100.100.111*
- 1079     ▪ Netmask: *255.255.255.0*
- 1080     ▪ Gateway: *10.100.100.1*

### 1081 2.8.2.3 Installation

1082 Repeat steps in Section 2.8.1.3.



1083 *2.8.2.4 Configurations*

1084 Repeat steps in Section 2.8.1.4.

1085 *2.8.3 Tripwire Industrial Visibility Configuration National Cybersecurity Center of*  
1086 *Excellence*

1087 Tripwire Industrial Visibility at the NCCoE serves as the central server.

1088 *2.8.3.1 VM Configuration*

1089 The Tripwire Industrial Visibility VM was given the following resources:

- 1090     ▪ CentOS 7.5
- 1091     ▪ 4 CPU cores
- 1092     ▪ 80 GB hard disk
- 1093     ▪ 32 GB RAM
- 1094     ▪ 1 NIC

1095 *2.8.3.2 Network Configuration*

1096 Network Configuration:

- 1097     ▪ DHCP: disabled
- 1098     ▪ IPv6: ignore
- 1099     ▪ IPv4: Manual
- 1100     ▪ IPv4 address: *10.100.100.111*
- 1101     ▪ Netmask: *255.255.255.0*
- 1102     ▪ Gateway: *10.100.100.1*

1103 *2.8.3.3 Installation*

1104 Repeat steps in Section 2.8.1.3.

1105 *2.8.3.4 Configurations*

1106 Repeat Steps 1–4 in Section 2.8.1.4.

1107 In Step 3, select **Bootstrap Central**.

1108 To complete the configuration: set up syslog, schedule a report, and install the Claroty application on  
1109 Splunk.

DRAFT

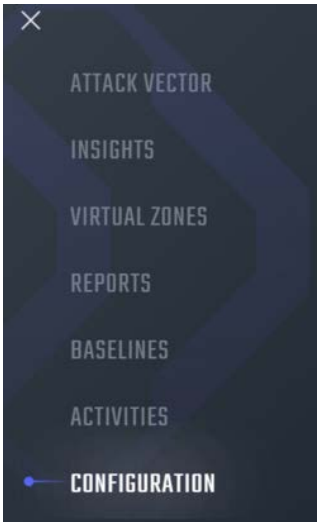
1110 1. Connect to the CTD Dashboard: *https://10.100.100.1111:5000*.

1111 2. Select the hamburger menu in the top left corner.



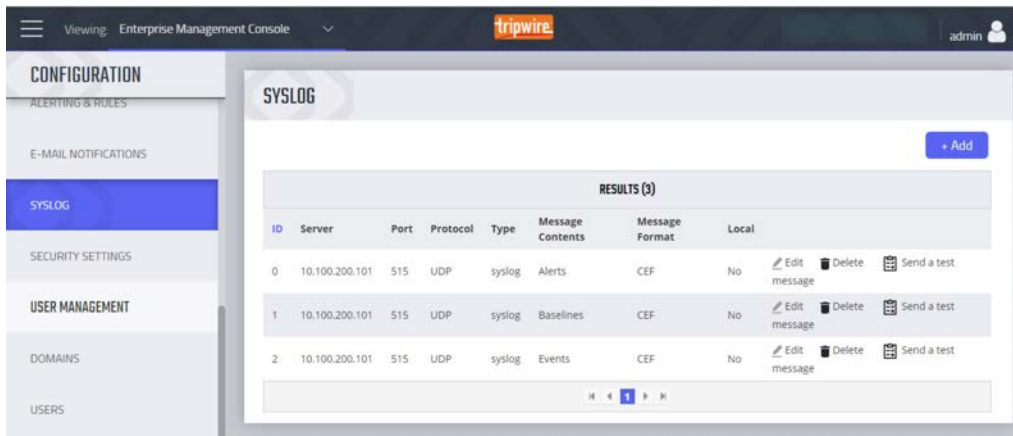
1112

1113 3. Scroll down to select **Configuration**.



1114

1115 4. Select **Syslog**. Select **Add**.



1116

1117 5. Uncheck **Local**. Do not Select a Site.

1118

1118

1119

1120

1121

6. Select Alerts for the **Log Level**. Enter the IP address for the Splunk server under **Server**. Enter **Port** 515 and **Protocol** UDP. Select all boxes under **Category** and all boxes under **Type**. Leave the **System URL** and the **Message Format** as the default.

1122

1122

1123

1124

1125

7. Select **Save**.
8. Select **Add** to add another.
9. Select **Baselines** under **Message Contents**.

The screenshot shows a configuration interface with two main sections: 'MESSAGE CONTENTS:' and 'MESSAGE FORMAT:'. Under 'MESSAGE CONTENTS:', there is a dropdown menu currently set to 'BASELINES'. Under 'MESSAGE FORMAT:', there is a dropdown menu currently set to 'CEF'. Below these sections, there are several input fields: 'Name' (text input), 'Transmission' (text input), 'Source port' (text input), 'Destination port' (text input), 'Protocol' (dropdown menu with 'Select Protocol...' selected), 'Communication Type' (dropdown menu with 'Select Communication Type...' selected), and 'Access Type' (dropdown menu with 'Select Access Type...' selected).

1126

1127

1128

10. Enter the Splunk IP for **Server**, **Port** 515, and **Protocol** UDP. Leave **System URL** as the default. Click **Save**.

The screenshot shows a configuration form with four sections: 'SERVER:' with a text input containing '10.100.200.101'; 'PORT:' with a text input containing '515'; 'PROTOCOL:' with a dropdown menu set to 'UDP'; and 'SYSTEM URL:' with a text input containing 'https://10.100.100.111:5000'.

1129

1130

1131

1132

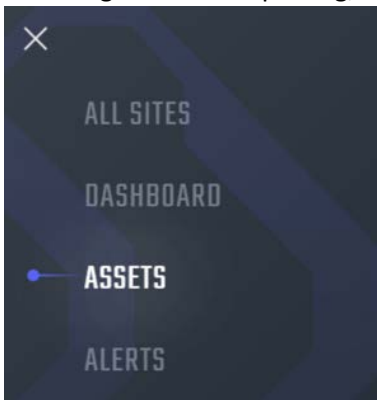
11. Select **Add** to add another.
12. Select **EVENTS** for **Message Contents**. Enter the Splunk IP for **Server**, **Port** 515, and **Protocol** UDP. Leave the **System URL** as default.

The screenshot shows a configuration interface with two main sections: 'MESSAGE CONTENTS:' and 'MESSAGE FORMAT:'. Under 'MESSAGE CONTENTS:', there is a dropdown menu currently set to 'EVENTS'. Under 'MESSAGE FORMAT:', there is a dropdown menu currently set to 'CEF'. Below these sections, there is a heading 'Select filters for the corresponding alerts' followed by two dropdown menus: 'Category' (set to 'Select Category...') and 'Type' (set to 'Select Type...'). Further down, there are input fields for 'SERVER:' (containing '10.100.200.101'), 'PORT:' (containing '515'), and 'PROTOCOL:' (a dropdown menu set to 'UDP'). At the bottom, there is a 'SYSTEM URL:' section with an input field containing 'https://10.100.100.111:5000'.

1133

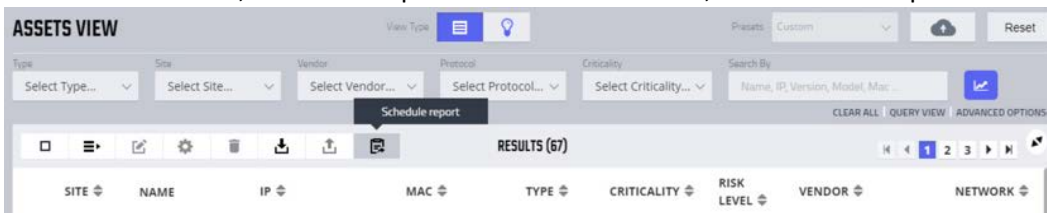
1134 13. Click **Save**.

1135 14. To configure Asset Reporting, select **Assets** from the hamburger menu.



1136

1137 15. From the **Assets** list, select the report icon in the menu bar, to schedule a report.



1138

- 1139 16. Name the report, and select **CSV** as the **Format**. Enter a recipient to receive and download the  
 1140 report. Schedule the report to run at an acceptable interval. This build scheduled the report to run  
 1141 daily. Click **Create**.

1142

### 1143 *2.8.3.5 Tripwire Splunk Integration*

1144 To integrate Tripwire with Splunk, install the Claroty Continuous Detection Application for Splunk.  
 1145 Additionally, install the Splunk Universal Forwarder to forward the CSV report.

- 1146 1. Download the Claroty Continuous Detection Application for Splunk from  
 1147 <https://splunkbase.splunk.com/app/4529/>.
- 1148 2. Log in to Splunk.
- 1149 3. On the **Apps** menu, click **Manage Apps**.
- 1150 4. Click **Install app** from file.
- 1151 5. In the **Upload app** window, click **Choose File**.
- 1152 6. Locate the downloaded `.tar.gz` file, and then click **Open** or **Choose**.
- 1153 7. Click **Upload**.
- 1154 8. Click **Restart Splunk**, and then confirm the restart.
- 1155 9. To install Splunk Universal Forwarder, follow the steps in Section 2.7.1.4.
- 1156 10. Place the following text in the `/opt/splunkforwarder/etc/system/local/outputs.conf` file:

```
1157     [tcpout]
1158     defaultGroup = default-autolb-group
1159     [tcpout:default-autolb-group]
1160     Server = 10.100.200.101:9997
1161     [tcpout-server://10.100.200.101:9997]
```

- 1162 11. Place the following text in the */opt/splunkforwarder/etc/system/local/deploymentclient.conf* file:
- 1163 12. [target-broker:deploymentserver]
- 1164 13. targetURI = 10.100.200.101:8089
- 1165 14. Log in to Splunk. Go to **Settings > Data Inputs > Files & Directories**.
- 1166 15. Select **New Remote File & Directory**.
- 1167 16. Select the host on which the forwarder is installed. Name the Server Class. Click **Next**.
- 1168 17. Input the CSV file to monitor, i.e., */home/esam/attachments/report.csv*.
- 1169 18. Select **Next**.
- 1170 19. Select **Review**.
- 1171 20. Select **Submit**.

## Appendix A List of Acronyms

<b>CSV</b>	Comma Separated Value
<b>CPU</b>	Central Processing Unit
<b>CTD</b>	Continuous Threat Detection
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DVD</b>	Digital Versatile Disc
<b>ESAM</b>	Energy Sector Asset Management
<b>ESP</b>	Encapsulating Security Payload
<b>GB</b>	Gigabyte
<b>HDD</b>	Hard Disk Drive
<b>IP</b>	Internet Protocol
<b>IPv</b>	Internet Protocol version
<b>ISO</b>	Optical Disc Image
<b>IT</b>	Information Technology
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIC</b>	Network Interface Controller/Card
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>OT</b>	Operational Technology
<b>PUMP</b>	Patch and Update Management Program
<b>RAM</b>	Random Access Memory
<b>SIEM</b>	Security Information and Event Management
<b>SPAN</b>	Switched Port Analyzer
<b>TB</b>	Terabyte
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>UDP</b>	User Datagram Protocol
<b>UMD</b>	University of Maryland
<b>VM</b>	Virtual Machine
<b>VPN</b>	Virtual Private Network
<b>XML</b>	Extensible Markup Language