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 Kuruvilla 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





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: <u>energy_nccoe@nist.gov</u>.

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: <u>nccoe@nist.gov</u>

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
- established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
- 14 Maryland.

To learn more about the NCCoE, visit <u>https://www.nccoe.nist.gov/</u>. To learn more about NIST, visit
 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
- 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
- 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**

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.

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

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
Dragos, Inc.	Dragos Platform v1.5
Forescout Technologies, Inc.	ForeScout CounterACT v8.0.1
FoxGuard Solutions, Inc.	FoxGuard Solutions Patch and Update Management Program v1
KORE Wireless Group, Inc.	KORE Wireless Cellular Connectivity with Cellular Gateway v2.0
<u>Splunk, Inc.</u>	Splunk Enterprise v7.1.3
TDi Technologies, Inc.	TDi Technologies ConsoleWorks v5.2-0u1
Tripwire, Inc.	Tripwire Industrial Visibility v3.2.1

50 **Contents**

51	1	Intr	oduct	ion	1
52		1.1	Practic	e Guide Structure	1
53		1.2	Build C	Overview	2
54		1.3	Typogr	raphic Conventions	4
55		1.4	Logical	Architecture Summary	4
56	2	Pro	duct Ir	nstallation Guides	4
57		2.1	Consol	eWorks	4
58			2.1.1	ConsoleWorks Configurations at the NCCoE	5
59		2.2	Foresc	out 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	FoxGu	ard Patch and Update Management Program	47
67			2.4.1	Patch Report	47
68		2.5	Kore V	Vireless	54
69			2.5.1	Bridge Configuration	55
70			2.5.2	Virtual Private Network Configuration	56
71		2.6	pfSens	e 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	Tripwi	re 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	Appendix A	List of Acronyms	.76

81 List of Figures

82	Figure 1-1 High-Level Topology	3
83	Figure 2-1 Update Availability Summary	.48
84	Figure 2-2 Device Update Availability Details-1	.49
85	Figure 2-3 Device Update Availability Details-2	.50
86	Figure 2-4 Device Update Availability Details-3	.51
87	Figure 2-5 Device Update Availability Details-4	.52
88	Figure 2-6 Device Update Availability Details-5	.53
89	Figure 2-7 Patch Evidence Documentation	.54

90 List of Tables

91 Table 2-1 Dragos Required Files	44
------------------------------------	----

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
- to be widely available. Rather, these volumes show how we incorporated the products together in our
- 97 environment.
- Note: These are not comprehensive tutorials. There are many possible service and security configurations
 for these products that are out of scope for this reference design.

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
- asset management solution in the energy sector. This reference design is modular and can be deployed
- 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 here)
- 110 Depending on your role in your organization, you might use this guide in different ways:
- Senior IT executives, including chief information security and technology officers, will be interested in 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
- Technology or security program managers who are concerned with how to identify, understand, assess,
 and mitigate risk will be interested in NIST SP 1800-23B, which describes what we did and why. The
 following sections will be of particular interest:
- 119 Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- Section 3.4.4, Security Control Map, maps the security characteristics of this example solution to 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,
- 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
- 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
- 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
- these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- 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
- success stories will improve subsequent versions of this guide. Please contribute your thoughts to
- 144 <u>energy_nccoe@nist.gov</u>.
- 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.





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

163 1.4 Logical Architecture Summary

A logical architecture summary can be found in Volume B of this practice guide, Section 4.1, ArchitectureDescription.

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
- 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 I 100 gigabyte (GB) hard disk
- 183 IO 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 (IPv)6: ignore
- 188 IPv4: Manual
- 189 IPv4 address: 10.100.100.6
- 190 Netmask: 255.255.255.0
- 191 *2.1.1.3 Installation*
- Download the installation kit from the <u>http://support.tditechnologies.com</u> website. A username and
 password are required, so contact TDi Support at <u>support@tditechnologies.com</u> 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 consoleworkssssl-<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

		* ADMIN: Server Man	agement: Registration	+_□×
		Registration X		
		ConsoleWorks Re	gistration	Complete My Offline Registration
		Contact Name:		► PROXY DETAILS
		Contact Email:		► ADVANCED OPTIONS
		Telephone:		
		Facility (Site) Name:	NCCoE]
		Address Line 1:	9700 Great Seneca Highway]
		Address Line 2:]
		City:	Rockville]
		State/Province:	MD	1
		Zip/Postal Code:	20850	Ĩ
		Country:	US	ī — — — — — — — — — — — — — — — — — — —
		View ourrent registration	etatue of all licaneae	~
200		Register Online Regis	ter Offline	Cancel Save
201	8.	Fill in the details	for Registration. Click R	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration	for Registration. Click R agement: Registration	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re	for Registration. Click R agement: Registration gistration	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name:	for Registration. Click R agement: Registration gistration	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email:	for Registration. Click R agement: Registration gistration	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: 	for Registration. Click R agement: Registration gistration	Register Online. Click Save. (+) [] X Complete My Offline Registration > PROXY DETAILS > ADVANCED OPTIONS
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name:	for Registration. Click R agement: Registration gistration	Register Online. Click Save. Complete My Offline Registration PROXY DETAILS ADVANCED OPTIONS
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1:	for Registration. Click R agement: Registration gistration NCCoE 9700 Great Seneca Highway	Register Online. Click Save. Complete My Offline Registration PROXY DETAILS ADVANCED OPTIONS
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 2: 	for Registration. Click R agement: Registration gistration	Register Online. Click Save. (*)X Complete My Offline Registration > PROXY DETAILS > ADVANCED OPTIONS
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 2: City: 	for Registration. Click R agement: Registration gistration 	Register Online. Click Save. Complete My Offline Registration PROXY DETAILS ADVANCED OPTIONS
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 2: City: State/Province: 	for Registration. Click R agement: Registration gistration NCCoE 9700 Great Seneca Highway Rockville	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 2: City: State/Province: Zin/Postal Code:	for Registration. Click R agement: Registration gistration I NCCoE 9700 Great Seneca Highway Rockville MD	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 1: Address Line 2: City: State/Province: Zip/Postal Code: 	for Registration. Click R agement: Registration gistration NCCoE 9700 Great Seneca Highway Rockville MD 20850	Register Online. Click Save.
201	8.	Fill in the details ADMIN: Server Man Registration X ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 1: Address Line 2: City: State/Province: Zip/Postal Code: Country:	for Registration. Click R agement: Registration gistration NCCoE 9700 Great Seneca Highway Rockville MD 20850 US	Register Online. Click Save. Complete My Offline Registration PROXY DETAILS ADVANCED OPTIONS
201	8.	Fill in the details ADMIN: Server Man Registration ConsoleWorks Re Contact Name: Contact Email: Telephone: Facility (Site) Name: Address Line 1: Address Line 1: City: State/Province: Zip/Postal Code: Country:	for Registration. Click R agement: Registration gistration i Signature Signa	Register Online. Click Save.

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

View
Add
Edit
Profiles
Change My Profile
Reset Passwords
Change Passwords
Change My Password
Preferences
Sessions
Send Message

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

204

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

USERS: Add		♥_□
dd User 🔀	Find an Example	
Name:	··· PROFILES	(0)
Description: Login Expiration: User Created: Last Login: Use External Authentication	None	Add Remove
Disable Session Timeout Password	► REMEDIATION HISTORY	(0)
Password:	► TAGS	(0)
Retype Password:		
Password Rules		
et As Default Save As	Change Password	Delete Cancel Sa

		8	Selected Profiles
ONSOLE_MANAGER	ConsoleWorks Administrator		CONSOLE_MANA
JEFAULT	Default Profile	> > *	

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.



Import XML			
XML File: Choose	Files FORESCOUT5228.xml		
Change case	Invalid character	Change length	
Change value	Reset Log directory		
Resource Name Confli	cts		
Auto Exclude			
P Auto-Exclude			

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



	urations X FORESCOUT-NETWORK	SCAN-INFO X	
Baseline Configur	ation A Description		
FORESCOUT-NE	TWORK Collect the Forescout Netwo	rk scan data	

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

220

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

iew Baseline Configuratio	INS IN FORESCOUT-NETWOR	RK_SCAN-INFO						
Reference Manual Refre	sh History	Vi	iew Active R	un Reduction	Run Repair	Run	Collectio	
Name:	FORESCOUT-NETWORK_S		► CONS	OLES + SC	HEDULES		(0)	
Description:	Collect the Forescout Network	scan da	> TAGS				(0)	
Profile:	CONSOLE_MANAGER	-					(4)	
Timeout:	30 \$ (0-604800 s	seconds)	Console	Co	llection Time			
Runs to keep:	10 20-1000 Run	is (0=unlimited)	SPLUNKCO	NSOLE 201	9/08/14 08:19	N	N	
Auto-Purge Runs:	\$ 0-9999 Day	s Old (0=disabled)	SPLUNKCO	NSOLE 201	9/08/14 12:31	N	N	
	Run on Non-Connected Con	nsoles	SPLUNKCO	NSOLE 201	9/08/14 12:34	N	N	
Compare to:	Single Master	Ŧ	SPLUNKCO	NSOLE 201	9/08/14 17:54	N	N	
			Delete				View	
Name	Description							
FORESCOUT-SCAN	Collection Forescout Scan	i						
Add Bamaun	Edit	Deuro						
Add Remove	Edit	Down						

- 6. Under **Collection**, update the path to match where Splunk saves the inventory, as shown in thescreenshot.
- 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);

TOOLS: Baseline Cor	figurat	ions: Processor	rs: Edit *				201	+_	
View Baseline Configuratio	ns 🗙	FORESCOUT-NET	WORK_SCAN	INFO >	FORESCO	DUT-SCAN *	×		
Refresh History									
Name:	FORES	COUT-SCAN		► B	ASELINES				(2)
Description:	Collecti	on Forescout Scar	information	► T/	AGS			8	(0)
← Collection									
// TODO: Change path to p	parent di	rectory of CSV dat	ta file						
// Read the newest file in t runCommand("cat \'is -t f	he direct	lory ", "Forescout_Info	rmation"						
4									
▶ Reduction	_								
Repair									
Normalize									
Custom Fields									
Set As Default Save As							Delete	Cancel	Save

229

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

TOOLS: Baseline Con	nfigurations:	Edit *					
View Baseline Configuration	ons 🗙 FORE	SCOUT-NETWORK	SCAN-INFO X	FORESO	OUT-NETWORK	SCAN-INFO *	×
Reference Manual Refre	sh History		Vie	ew Active	Run Reduction	Run Repair	Run Collection
Name:	FORESCOUT	NETWORK_S		▶ CO	NSOLES + SCH	EDULES	(1)
Description:	Collect the For	escout Network sca	an da	► TA	GS		(0)
Profile:	CONSOLE_M	ANAGER	Ŧ	► BA	SELINE RUNS		(8)
Timeout:	30	\$ (0-604800 sec	conds)				
Runs to keep:	10	2 0-1000 Runs (0=unlimited)				
Auto-Purge Runs:		C-9999 Days (Old (0≈disabled)				
	Run on No	n-Connected Conso	bles				
Compare to:	Single Master		-				
Collection							
 Reduction 							
function correctHeader(st return(//[w/-\]*type\b/i.te : (/\bip\w/-\]*fi.test(st	r) { est(str)) ?"Appi lr)) ?"IPAddre	icationType" ss"					
▶ Repair							
Custom Fields							
Set As Default Save As.						Delete	Cancel Save

232	<pre>include("UTIL");</pre>
233	include("UTIL_CUSTOM_FILE");
234	include("UTIL_JSON");
235 236	//////////////////////////////////////
237	// Massage the header
238	<pre>function correctHeader(str) {</pre>
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"
249 250	: String(str).replace(/[\W_]+/g, " ").camelSpaced().toCapCase().replace(/\ +/g, ""));
251	}
252 253	·/////////////////////////////////////
254	<pre>// ref: http://stackoverflow.com/a/1293163/2343</pre>
255	<pre>function CSVToArray(strData, strDelimiter) {</pre>
256	// Check to see if the delimiter is defined. If not, then default to comma.
257	<pre>strDelimiter=(typeof strDelimiter!='undefined')?strDelimiter:",";</pre>
258	// Create a regular expression to parse the CSV values.
259 260	// Delimiters Quoted fields Standard fields.
261 262 263	<pre>var objPattern=new RegExp(("(\\"+strDelimiter+" \\r?\\n \\r ^)(?:\"([^\"]*(?:\"\"[^\"]*)*)\" ([^\" \\"+strDelimiter+"\\r\\n]*))"), "gi");</pre>
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;
268 269	// Keep looping over the regular expression matches until we can no longer find a match.
270	<pre>while(arrMatches=objPattern.exec(strData)) {</pre>
271	// Get the delimiter that was found.
272	<pre>var strMatchedDelimiter=arrMatches[1];</pre>
273 274	// Check to see if the given delimiter has a length (is not the start of 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) {
277 278	<pre>// Since we have reached a new row of data, add an empty row to our data array.</pre>
279	arrData.push([]);
280	}
281	var strMatchedValue;
282 283	<pre>// Now that we have our delimiter out of the way, let's check to see which kind of value we captured (quoted or unquoted).</pre>
284	if(arrMatches[2]) {
285 286	<pre>// We found a quoted value. When we capture this value, unescape any double quotes.</pre>
287	<pre>//strMatchedValue=arrMatches[2].replace(new RegExp("\"\"", "g"), "\"");</pre>
288	<pre>strMatchedValue=arrMatches[2].replace(/\"{2}/g, '"');</pre>
289	} else {
290	// We found a non-quoted value.
291	<pre>strMatchedValue=arrMatches[3];</pre>
292	}
293	// Now that we have our value string, let's add it to the data array.
294	<pre>arrData[arrData.length-1].push(strMatchedValue);</pre>
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	<pre>var outputDir="/FOXGUARD/"+(now.slice(0,8));</pre>
304	<pre>var outputFile=""+outputDir+"/"+(now.slice(8,14));</pre>
305	<pre>var result=[];</pre>
306	// Default of negative feedback
307	<pre>var tracker=false;</pre>
308	if(typeof csv!='undefined' && csv.length>0) {
309	try {
310	<pre>var lines=CSVToArray(csv);</pre>
311	<pre>lines.shift();</pre>
312	if(lines.length>1) {
313	try {
314	// Header names
315	<pre>var props=lines[0];</pre>
316	if(props.length>0) {
317	// Massage header names
318	<pre>for(var k=0;k<props.length;k++) pre="" {<=""></props.length;k++)></pre>
319	<pre>if(props[k].length>0) {</pre>
320	<pre>props[k]=correctHeader(props[k]);</pre>
321	}
322	}
323	<pre>for(i=1;i<lines.length;i++) pre="" {<=""></lines.length;i++)></pre>
324	<pre>var j=lines[i];</pre>
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++) {</pre>
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
                              break;
349
                             case "MACAddress":
350
351
          //obj.MACAddress=(rEMAC.test(j[k]))?j[k].match(rEMAC)[1]:"unspecified";
352
                              break;
353
                             case "OperatingSystem":
354
                              obj.ApplicationType="Operating System";
355
                              obj.OperatingSystem=j[k];
356
                              obj.ProductName=j[k];
357
                              break;
358
                             case "VendorName":
359
                              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) {</pre>
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.**

^	▼ CONSOLES: Add *		+_0
No Favorites saved	Add Console * 🗶 Browse Example Consoles 🔀		
CONSOLES	Refresh Find an Example Lo	gs Events	Monitored Eve
View	Name: Splunk Console III GROUPS		(0)
Edit	Nickname: > SCANS		(0)
Change State	Description:		(0)
VIRTUALfx	Status: - Enable ACKNOWLEDGE ACTIONS	ŝ	(0)
View Hypervisors Virtual Machines	Device: PURGE ACTIONS		(0)
Groups	Connector: SSH with Password EXPECT-LITE SCRIPTS Connector: SSH with Password		(0)
View	Connection betalls MULTI-CONNECT Enable Failover: Unavailable		(0)
Edit	Exclusive Connect REMEDIATION HISTORY		(0)
Send Command	Host IP: 10.100.200.101 SCHEDULES + EVENTS		(0)
Multi-Connect	Port: 22 C TAGS		(0)
Add	Username: administrator BASELINES + SCHEDULE:	s	(0)
Edit	Password: BASELINE RUNS		(0)
Expect-Lite Scripts	Retype Password: GRAPHICAL CONNECTION	NS	(0)
Add	Command:		
Edit	Set As Default Save As	Delete	Cancel
Usage			

454

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

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

ten esti			Find an Example	
Name:		1	CONSOLES + BASELINES	
Description:	-		CONSOLES + EVENTS	
✓ Repeat			GROUPS + EVENTS	1
Starting date/time:			CWSCRIPT	
Repeat Every:	1 Days	-	REPORTS	9
Custom Fields			▶ ВАСКИР	

460	arrow. Click OK.	
	Add Association	
	Console Baseline Configuration FORESCOUT-NETWORK_S CONVIRKS CONVIRKS_OUT SPLUNKCONSOLE	Baseline Configuration FORESCOUT-NETWORK_SCA
461 462 2	14. Click Save.	
	Add Schedule * 🗙	
	Refresh Control Es - Diset un	r
	Name: Daily	· (1)
	Description: Console Baseline C	UT-NET
	Kepeat	Remove
	Peneat Event 1 Dave	View Console
	Custom Fielde	View Baselin
	CONSOLES + EVENTS	(0)
	GROUPS+EVENIS CWSCOUPT	(0)
		(0)
	> BACKID	(0)
	► TAGS	(0)
463	Set As Default Save As	Delete Cancel Save
403		

459 13. Select the previously created Splunk console and the imported baseline configuration. Click the

464 2.1.1.5 ConsoleWorks Configurations UMD

The following subsections document the software, hardware/VM, and network configurations for theConsoleWorks 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	1.1	100 GB hard Disks
472	1.1	12 GB RAM
473	1.1	2 NIC
474	2.1.1.	7 Network Configuration
475	Netwo	rk Configuration (Interface 1):
476	1.1	DHCP: disabled
477	1.1	IPv6: ignore
478	1.1	IPv4: Manual
479	1.1	IPv4 address: 10.100.1.6
480	1.1	Netmask: 255.255.255.0
481	Netwo	rk Configuration (Interface 2):
482	1.1	DHCP: disabled
483	1.1	IPv6: ignore
484	1.1	IPv4: Manual
485	1.1	IPv4 address: 172.16.2.82
486		Netmask: 255.255.255.248
487	2.1.1.	8 Installation
488 489	1. Do pa	wnload the installation kit from the http://support.tditechnologies.com website. A username and ssword are required, so contact TDi Support at support@tditechnologies.com to request them.
490	2. Ru	n the installer cw_server_ <version>.exe.</version>

- 491 3. Download the Splunk universal forwarder installer from the
 492 <u>https://www.splunk.com/en_us/download/universal-forwarder.html</u> 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 <i>https://10.</i>	100.1.6:5176. Log in us	ing the default creden
		ADMIN: Server Man	agement: Registration		+_
		Registration X			
		ConsoleWorks Re	gistration		Complete My Offline Registration
		Contact Name:		PROXY DETAILS	<u>^</u>
		Contact Email:		► ADVANCED OPTIONS	
		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 Register Online Regist	etatue of all licenses		Cancel Save
497	6	Fill in the detail	for Pogistration Clic	k Pagistar Online Click	Sava
490	0.		anoment: Projectation	k Register Omme. Chek	
		Registration X	agement. Registion		
		ConsoleWorks Re	gistration		Complete My Offline Registration
		Contact Name:		▶ PROXY DETAILS	^
		Contact Email:		ADVANCED OPTIONS	
		Telephone:			
		Facility (Site) Name:	NCCoE	Ξ.	
		Address Line 1:	9700 Great Seneca Highway	Ξ́	
		Address Line 2:		Ξ.	
		City:	Rockville	Ξ.	
		State/Province:	MD	Ξ.	
		Zip/Postal Code:	20850	=	
		Country	US	=	
		country.	1-5 1-		
		View ourrent renistration	etatue of all licenses		~

using the default credentials. c.//10 100 1 6.5176 Log in ما خ at httr \sim 00 . .

V	USERS	
	View	
	Add	
	Edit	
Þ	Profiles	
	Change My Profile	
	Reset Passwords	
	Change Passwords	
	Change My Password	
	Preferences	
	Sessions	
	Send Message	

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

501 502

8. Enter the name and password. Select Add.

USERS: Add			+_0
Idd User 🔀	Find an	Example	
Name:	PROFI	LES	(0)
Description:		None	Add
Last Login:	ation		View
Password		DIATION HISTORY	(0)
Password:	► TAGS		(0)
Retype Password:			
Require Password Change On Next Login			
Password Rules			
iet As Default Save As	Change Password		Delete Cancel S

Profile	Description	8	Selected Profiles
CONSOLE_MANAGER	ConsoleWorks Administrator		CONSOLE_MANA
DEFAULT	Default Profile	× × ×	

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.**

Refresh History	tus 🗙		
Name:	ÞBVIUS	×	1
Nickname:	Obvius		
Description:			
Status:	NORMAL Disable		
Device:			-
Connector:	Port Forward Fr	ontend	=
- Connection Detail	s		
	Priority Start	tup	
Remote Host:	10.144.85.96		
Demote Dort	502		-

		⇒ ADMIN
		Server Management
		Backups
		Restore
		> XML Exports
		View
		Import
		Orphan Files
514		Template Management
515	4.	Select Upload a file, then click Next.
		How would you like to provide the XML to Import?
516		Upload a file
517	5	Click Browse then find the XML file
517	5.	
		College Administrator (i Diowse
		Corrections Corrections
		Resource Name Conflicts
518		Auto-Exclude
519	6.	Click Next. ConsoleWorks will import the two CWScripts: UTIL_MODBUS and UTIL_MODBUS_GE. ADMIN: Catabase Management: XML Imports: Import Prover STR
		Yew Log
		Valdation regested and sinsby Complete Starling Commit & delabase modifications Complete Commit, Status: Success
520		Reat

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

520

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

V	TOOLS
	CWCLIent
	Windows Event Forwarder
	Graphical Gateway
Þ	Network Manager
₽	CWScripts
Þ	Baseline Configurations
\forall	Schedules
	View
	Add
	Edit
₽	External Tools
Þ	Mass Change
₽	Custom Files

522

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

Name:	MODBUS		
Description:			
 Repeat Starting date/time: 		2019/08/13	13:36
Starting autoranto.			

	▼ TOOLS	
	CWCLIent	
	Windows Event Forwarder	
	Graphical Gateway	
	Network Manager	
	CWScripts	
	View	
	Add	
	Edit	
	Runs	
	Active	
	Differences	
	Processors	
	Schedules	
	External Tools	
	Mass Change	
526	Custom Files	
520		
527	10. Name the baseline, and set th	e Profile to CONSOLE MANAGER.
	* TOOLS: Baseline Configurations: Edit *	+_D
	View Baseline Configurations 🔀 STEAM_METER * 🔀	
	Reference Manual Refresh History	View Active Run Reduction Run Repair Run Collection
	Name: STEAM_METER	- CONSOLES + SCHEDULES *(1)
	Description:	Console Schedule Add

OBVIUS

> TAGS

► BASELINE RUNS

Ŧ

Ψ

Up Down

(0-604800 seconds)

Run on Non-Connected Consoles

Description

Edit

C-1000 Runs (0=unlimited)

C-9999 Days Old (0=disabled)

MODBUS

Profile: CONSOLE_MANAGER

Compare to: Master per Console

Timeout 30 Runs to keep: 10

Auto-Purge Runs:

- Processors Name

MODBUS_REG

Add Remove

+_ **X**

Rem

View Console

View Schedule

(0)

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

530

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

Reference Man	ual Refresh	History		View Act	tive Run Reduction F	tun Repair Run Colle		
Name:	STEAM_MET	TER	100	- CONSOLI	ES + SCHEDULES	* (1)		
Description:				Console	Schedule	Add		
Profile:	CONSOLE_M	MANAGER	-	OBVIUS	MODBUS	Remove		
Timeout: 30 \$ (0-6048		0 seconds)	seconds)					
Runs to keep:	10	C-1000 R	uns (0=unlimited)			View Console		
Auto-Purge	0-9999 Days Old (0=disabled)					View Schedule		
Runs.	Runs:		Consoles	► TAGS (0)				
Compare to:	Master per C	onsole	Ŧ	► BASELIN	E RUNS	(10)		
- Process	iors							
Name		Description						
MODBUS_RE	G							

12. Name the Processor, then click the highlighted button. Enter the text that follows, then click Save.
 TOOLS: Baseline Configurations: Processors: Edit

	View Baseline Configurations 🔀 STEAM_METER 🔀 MODBUS_REG 🗙
	Refresh History
	Name: MODBUS_REG)
	Description: TAGS
	← Collection
532	include("UTIL_MODBUS"); include("UTIL_MODBUS_GE"); // Config sections=[{name:"Product Information", fields:[{addr:288, num:1, format:"F001", name:"Gal Total", fun {addr:289, num:1, format:"F001", name:"Flow Rate", fun]}]; var port=502; var unit=95;
533 534	<pre>include("UTIL_MODBUS"); include("UTIL_MODBUS_GE");</pre>
535 536 537 538 539 540 541 542 543	<pre>// Config sections=[{name:"Product Information", fields:[{addr:288, num:1, format:"F001", name:"Gal Total", functionName: readHoldingRegisters}, {addr:289, num:1, format:"F001", name:"Flow Rate", functionName: readHoldingRegisters},]}];</pre>

```
544
      var port=502;
545
      var unit=95;
546
       // Execute
547
      var server=console.port;
548
       for(var s=0;s<sections.length;s++) {</pre>
549
        setOutput(sections[s].name, formatGEOutput(modbusConnection(server, port, unit,
550
      sections[s].fields)));
551
552
553
        log("SPLUNK",formatGEOutput(modbusConnection(server, port, unit,
       sections[s].fields)));
       }
```

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

Reference Man	al Refresh	History		View Active	Run Reduction	Run Repair	Run Collectio
Name:	STEAM_MET	ER	- F		SCHEDULES		* (1)
Description:				Console	Schedule		Add
Profile:	CONSOLE_M	ANAGER	-	OBVIUS	MODBUS		Remove
Timeout.	30	\$ (0-604800 s	econds)				ramore
Runs to keep: 10 0-1000 Runs		s (0=unlimited)		v v		rw Console	
Auto-Purge	0-9999 Davs Old (Dedisabled)						w Schedule
Runs:	Dun on No	Connected Con		▶ TAGS			(0)
Compare to:	Master per Co	nsole	•	BASELINE R	UNS		(10)
+ Process	ors						
Name		Description					
MODBUS_RE	G		-				

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



557
Refresh History			Logs Eve	nts Monitore
Name:	SPLUNK	10 D	GROUPS	(
Nickname:		•	SCANS	(
Description:			AUTOMATIC ACTIONS	(
Status:	NORMAL Disable		ACKNOWLEDGE ACTIONS	
Device:		-	PURGE ACTIONS	
Connector:	Chained Session	-	EXPECT-LITE SCRIPTS	
 Connection Detail 	s		MULTI-CONNECT	
Connect			REMEDIATION HISTORY	
			SCHEDULES + EVENTS	
Logging Type:	Go ▼ Secure		TAGS	
Log Directory:	Files\SplunkUniversalForwarder\ var\log\splunk		BASELINES + SCHEDULES	
Auto-Purge Logs:	Days Old (0=disabled)		BASELINE RUNS	
▶ Events			GRAPHICAL CONNECTIONS	
Links				

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

559

- 16. Name the Console, and set the connector to Chain Session, the log type to Governed, and the Log
 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
- 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 <u>https://www.forescout.com/platform/specifications/#virtual-appliance</u>
- 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 <u>https://www.forescout.com/company/resources/forescout-installation-guide-8-1/.</u>
- 599 2.2.1.4 Configuration
- The following steps contain configuration instructions for scanning devices at the Plano location. For
- additional CounterACT configuration details, refer to the administration guide at
- 602 <u>https://www.forescout.com/wp-content/uploads/2018/11/counteract-administration-guide-8.0.1.pdf.</u>

- 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 screen607 opens.



- 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**.



Setup ForeScout Co	unterACT 8.0.0	
Installation Directory	,	ForeScou
Please specify the dire	ctory where ForeScout CounterACT will be installed	
Installation Directory	C:\Users\test\ForeScout CounterACT 8.0.0	1 2
InstallBuilder		
nstanounaci	< Back Next >	Cancel

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

613

614 6. Click Next.

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

Setup ForeScout Co	unterACT 8.0.0	- • ×
	Completing the ForeScout CounterACT 8 Wizard	0.0_TEST Setup
ForeScout	Setup has finished installing ForeScout Cou your computer. Create Desktop shortcut	nterACT 8.0.0_TEST on
	< Back	nish Cancel

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

	-	
ForeSco	out	
CounterACT [®] Ve	ersion 8.0	
IP/Name:		
10.100.100.33		
Login Method:		
Password	~	
User Name:		
admin		
Password:		
🗹 Save address and user na	me	
A CONTRACTOR OF		

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

		📩 Home	Asset Inventory	B Policy	۲
Views	ď				
Search	Q				
All Hosts (23) ① Policies ⑦ Compliance ⑦ Compliance ⑦ Compliance ⑦ Compliance ⑦ NAC Policy ▲ NAC Policy					

•		CounterACT Options 10.100.100.33	- 0				
Options							
Search Q	CounterACT Devices						
> 😫 CounterACT Devices	Perform CounterACT device management tasks, including adding and removing CounterACT Appliances and Recovery En						
> R Modules	When upgrading the entire syst	em, first select the Enterprise Manager and click Upgrade, then select all other devices and	click Upgrad				
E Channels	~ Devices	Caserb O Z Charge righ folders					
Microsoft SMS/SCCM	Enterprise Manager						
Advanced Tools Plugin	MI Appliances	Status Type D., A IP/., IP., Assigned, #, Us, Devic, Description	Add				
📴 IoT Posture Assessment Enj			Edit				
IOC Scanner		No items to display	Remov				
AWS			IP/Por				
S Wireless			Start				
😵 NetFlow			Stop				
C RADIUS			Upgrad				
MAC Address Repository			Licens				
CEF			Dashu				
C HPS Inspection Engine			Backup				
VMware NSX			Recove				
VMware vSphere							

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

IP/Name	1
Port	13000 0
User <u>N</u> ame	admin
Password	
/Appliances	Folder

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



628

629 14. Enter the required information. Select Submit.

Appliance to be lice	nsed:
10.172.8.38	
Company Name	NIST-NCCOE
Contact Person	
Phone Number	
Freed & dates	
Email Address	
Comment	for NCCoF ESAM project Appliance in Plano. Tx
License Type	
O Permanent	
Demo For:	120 🗘 Days
Request Submissi	onmethod
(Cuburtus	
Submit reques	t via <u>w</u> eb
 Submit reques Submit reques 	it via <u>w</u> eb t by email
Submit reques Submit reques Submit reques Save request t	rt via <u>web</u> 1 by email 0 file
Submit reques Submit reques Submit reques Save request t	rt via <u>w</u> eb it by email o file

631 15. Select OK.



632

633 2.2.1.4.1 Appliance Interfaces Configurations

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

	CounterACT Options 10.100.100.33											
Options												
Search Q	CounterACT Devices											
CounterACT Devices	Perform CounterACT device m	anagemer	nt tasks,	including adding	and rer	novin	Cou	interA	CT Appliance	is and	Recovery E	interprise
R Modules	Managers, starting and stoppin When upgrading the entire syst	g Appliand em, first si	es, as v elect the	vell as handling i Enterprise Man	apgrade ager and	click	licens Upgra	es for ade, th	all devices. Ien select all	other d	levices and	click Upgrade.
Microsoft SMS/SCCM Advanced Tools Plugin	Novices	Search			Q		Show	r sub-f	olders			
DIOT Posture Assessment En(Appliances	Status	Type	Device Na	A11	IP/		#H	Device	Use	Des	Add
AWS		4	100	10.100.1.33		10.1	1	0	License, N	Com.	umd	Edit
S Wireless		0		10.172.8.38	tdi	10.1_	1	0	Disconnect	Com.	NCC	
@ NetFlow		4	62	Enterprise Ma		10.1	1)	4	License	Com.	ESA	Remove
C RADIUS												IP/Port
MAC Address Repository		2 Barris / Augustad								Others		
CEF										guart		
HPS Inspection Engine		Licenze		Demo	- 01 da	n latt						Stop
VMware NSX		License	Reque	st Licen	e Read	to In:	stall (submit	tted: Feb 21,	2019)	install Car	Upgrade
> Splunk		Bandwidth: Current 0.0Mbps, Average 0.0Mbps, Max 0.01Mbps High Availability: HA is not enabled							opgrade			
VMware vSphere								und .				License
∆ Linux		Lost Pa	ckets:	0.00%	alies he		114					Backup
d Mac OS X		CPU UI	ilization	c 1.80%								
Guest Registration		Time G	ap from	EM: 31.33	4 second	is earl	iër					Recovery
User Directory		Uptime	CIT EN	78 da	/s and 1	hour						
Switch												-
A Centralized Network Control												Help

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

	Details of 10.100.1.33
	Status Channels Fingerprint
	Channels
	A channel is a pair of monitor and response interfaces used by the CounterACT Appliance to interact with the network. A monitor interface examines traffic going through the network and a response interface generate it raffic back to the network. Make sure the physical connections made at the Data Center match the logical channel setting below and that your network traffic is earn physical connections made at the Data Center match the logical channel setting below and that your network
	VLAN discovery after channel configuration might take a few moments.
	Channel VLAN V Traffic Vise DHCP by Default
	Channel Alert
	Help Apply Ur
	Heip Apply Un Ci
3.	Heip Apply Un Gi Under Channel, select Add.
3.	Help Apply Un CR Under Channel, select Add. Channel V VLAN V Traffic V Use DHCP by Default
3.	Help Apply Un Cte Under Channel, select Add. Channel V VLAN V IFattic V Use DHCP by Detault + Add
3.	Help Apply Un CH Under Channel, select Add. Channel V VLAN V Trattic V Use DHCP by Detault + Add C was detected on the following VLANs: [eth0.Untagged] Details
3.	Help Apply Ora GI Under Channel, select Add. Channel V VLAN V Trattic V Use DHCP by Default + Add Channel V VLAN V Trattic Use DHCP by Default + Add C C Was detected on the following VLANs: [eth0.Untagged] Details © Remove Remove C

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



643 5. Under Tools, select Segment Manager.



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

	Name:						
	Select where to place the folder:						
	🗸 🛥 Segments						
	✓ ♂ In_Scope	_					
	Tor tor						
	a plano out						
8	ок Can Highlight the <i>tdi</i> seg Filter detections at the Informa Use segments when working	gment ation Pane	. Click Ac	id to add the	e range of IF	P addresses to sca	nn. Click OK.
8	OK Can Highlight the <i>tdi</i> seg Filter detections at the Informa Use segments when working Generate reports organized p	gment ation Pane at the Cor er segme	. Click Ac el per segment nsole, e.g. crea nt.	id to add the	e range of IF	P addresses to sca	nn. Click OK.
8	OK Can Highlight the tdi seg Filter detections at the Informa Use segments when working Generate reports organized p Assign segments to a specific	gment ation Pane at the Cor ber segme c geograph	C. Click Ac el per segment. nsole, e.g. crea nt. hic location. Us	dd to add the te a policy that blocks e this option when w	e range of IF s Internet access to o orking with the site r	P addresses to sca endpoints in the finance depar nap.	nn. Click OK. tment
8	OK Can Highlight the tdi seg • Filter detections at the informa • Use segments when working • Generate reports organized p • Assign segments to a specific • I I I I I I I I I I I I I I I I I I I	gment ation Pane at the Cor eer segmen ; geograph	Click Ac el per segment. nsole, e.g. creai nt. hic location. Us <u>N</u> ame	dd to add the te a policy that block e this option when w tdi	e range of I Internet access to o orking with the site r	P addresses to sca endpoints in the finance depar map.	nn. Click OK. tment.
8	OK Can Highlight the tdi seg Filter detections at the Informa Use segments when working Generate reports organized p Assign segments to a specific Filter detection of the Information Use segments to a specific Search	gment ation Pane at the Cor ber segment c geograph	Click Ac el per segment, nsole, e.g. creai nt, hic location. Us Name Description	dd to add the te a policy that block e this option when w tdi	e range of If s Internet access to (orking with the site r	P addresses to sca endpoints in the finance depar map.	nn. Click OK. tment.
8	OK Can Highlight the tdi seg • Filter detections at the Informa • Use segments when working • Generate reports organized p • Assign segments to a specific • • • • • • • • • • • • • • • • • • •	gment ation Pane at the Cor er segme ; geograph Q	C. Click Ac el per segment nsole, e.g. crea nt hic location. Us <u>N</u> ame <u>D</u> escription Location	dd to add the te a policy that blocks e this option when w tdi	e range of IF s internet access to o orking with the site r	P addresses to sca	nn. Click OK. tment
8	OK Can Highlight the tdi seg • Filter detections at the Informa • Use segments when working • Generate reports organized p • Assign segments to a specific • Image of the Image of th	gment ation Pane at the Cor er segme c geograph	C. Click Ac el per segment nsole, e.g. creai nt hic location. Us <u>Name</u> <u>D</u> escription Location No locati	dd to add the te a policy that block e this option when w tdi	e range of IF s Internet access to o orking with the site r	P addresses to sca	nn. Click OK. tment
8	OK Can Highlight the tdi seg • Filter detections at the Informa • Use segments when working • Generate reports organized p • Assign segments to a specific • Search • Segments ~ & In_Scope • tdi	cel gment ation Pane at the Cor er segme c geograph Q	Click Ac el per segment nsole, e.g. creai nt hic location. Us Name Description Location	dd to add the te a policy that block e this option when w tdi	e range of IF s Internet access to o orking with the site r	P addresses to sca endpoints in the finance depar map.	nn. Click OK. tment
8	OK Can Highlight the tdi seg Filter detections at the informa Generate reports organized p Assign segments to a specific Search Segments Search Construction Segments	cel gment ation Pane at the Cor ber segmen ; geograph	Click Ac el per segment. nsole, e.g. creai nt. hic location. Us Name Description Location No locati Location	dd to add the te a policy that block e this option when w tdi ton Plano, Tx	e range of I Internet access to o orking with the site r	P addresses to sca endpoints in the finance depar map.	tment.
8	OK Can Highlight the tdi seg Filter detections at the Informa Use segments when working Generate reports organized p Assign segments to a specific Search Search Segments Search Contemport Search Contemport Search Contemport Segments Segments Contemport Segments Segments Contemport Segments S	cel gment ation Pane at the Cor ber segment : geograph	Click Ac el per segment. Insole, e.g. creat nt. hic location. Us Name Description Location No locati e Location Range	dd to add the te a policy that blocks e this option when w tdi ton Plano, Tx	e range of If s Internet access to e orking with the site r	P addresses to sca endpoints in the finance depar map.	tment.
8	OK Can Highlight the tdi seg • Filter detections at the informa • Use segments when working • Generate reports organized p • Assign segments to a specific • In Scope • In Scope • Idi • Out_Scope • plano_out	cel gment ation Pane at the Con- ber segment : geograph	Click Ac el per segment. nsole, e.g. creai nt. hic location. Us Name Description Location O No location Range Search	dd to add the te a policy that block e this option when w tdi ton Plano, Tx	e range of I s Internet access to o orking with the site r	Add Show sub-segm	nn. Click OK. tment.
8	OK Can Highlight the tdi seg • Filter detections at the Informa • Use segments when working • Generate reports organized p • Assign segments to a specific • Implements • Search • Segments • Segments • Sei In_Scope • toi • Sout_Scope • plano_out	cel gment ation Pane at the Con er segme : geograph	Click Ac el per segment. nsole, e.g. creat nt. hic location. Us Name Description Location O No location Range Search Path	dd to add the te a policy that block e this option when w tdi Plano, Tx Segment *	e range of If s Internet access to o orking with the site r	Add Add Show sub-segm Range	nn. Click OK. tment.
8	OK Can Highlight the tdi seg • Filter detections at the informat • Use segments when working • Generate reports organized p • Assign segments to a specific • Image of the segments • Image o	cel gment ation Pane at the Cor her segment : geograph	Click Ac el per segment. nsole, e.g. creai nt. hic location. Us Name Description Location No location Range Search Path In_Scope/tdl	dd to add the te a policy that block e this option when w tdi ion Plano, Tx Segment •	e range of IR s Internet access to o orking with the site r	Add Show sub-segm 10.172.6.2-10.172.6.50	n. Click OK. tment.
8	OK Can Highlight the tdi seg • Filter detections at the informa • Use segments when working • Generate reports organized p • Assign segments to a specific • Image the segments • Search • Segments • Segments	cel gment ation Pane at the Cor her segment : geograph	Click Ac el per segment. nsole, e.g. creai nt. hic location. Us <u>Name</u> <u>Description</u> Location <u>Cocation</u> Range <u>Search</u> Path In_Scope/Idi In_Scope/Idi	dd to add the te a policy that block e this option when w tdi Plano, Tx Segment •	e range of II s Internet access to o orking with the site r	Addresses to sca endpoints in the finance departmap.	nn. Click OK. tment.

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

- 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.



661

- 659 3. Name the folder. Click **OK.**
- 660 4. Select the **import policy** icon.



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

0	Import Policy Folder -
Target Node:	Policy
Import Mode:	Add folder to the target
	O Add folder content to the target
File Name:	
	OK Cancel

- 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 <u>https://www.forescout.com/platform/forescout-app-guide-splunk-2-7-0</u> and
- 671 <u>https://www.forescout.com/company/resources/extended-module-for-splunk-configuration-guide-2-8/.</u>

672 2.2.1.4.4 Schedule Reporting

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



- 675 2. Log in using the same credentials as the **Enterprise Manager** Console.
- 676 3. Select Reports.
- 677 4. Select **Add.**

674

678

Deshow	a 🔍 Assets (P Reports				ForeScr
◆ AddEd	it 🐁 Duplicate 📋 Ro	move 🔄 Scope 🛅 Schedule	🖸 Email 🕕 🛈 Run		a	tmin I 🐨 🎃 🕞
000	Name -	Description	o Scope	0 Format 0 Email	o Schedule	0 1 0
	SSH Report	Show detailed results for a selected policy.	All IPs	CI.	None	

- 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:

elect charts:											
0 🔊 🛈 🖬											
Select inv	entory	item column:									
Show hos	t deta	ils:									
IPv4	13	MAC	NIC	Offline	OS Eingerprint	Operating	Vendor and Model	Host is	Open	SSH	Telnet

- 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 <u>https://www.forescout.com/wp-content/uploads/2018/10/CounterACT_Installation_Guide_8.0.1.pdf.</u>
- 698 2.2.2.4 Configuration
- After the CounterACT Appliance is installed, follow the steps outlined in Section 2.2.1, to connect theappliance 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
- 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
- site. The Dragos sensor is managed by the site store.

706 2.3.1 Dragos Sitestore Configuration

- In the example implementation, Dragos Sitestore is deployed as a pre-built appliance from the vendor.
 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
- received a Dell server utilizing iDRAC for virtualization. On the iDRAC server, VMware ESXi was installed
- 713 and utilized for creating the server.
- 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

- Dell iDRAC server housing the Dragos Sitestore Puppet Server was connected to the ESAM network withthe 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
- the CD/DVD Drive 1 location (*DragosCustom-2019-06-18-CentOS-7-x86_64-Everything-1810.iso*).
- Power on the VM, and open a console. The **Dragos installation** screen will start, allowing options to
 be selected for installation type.
- With the Dell R730 server used for the NCCoE, select Install Dragos Sitestore Kickstart. The installer
 automatically installs the Dragos Platform without interaction from the user.
- 735 *2.3.1.4 Configuration*
- Once the installation has completed, the Sitestore will be configured with the needed files listed in Table2-1.
- 738 Table 2-1 Dragos Required Files

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

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

Change directory to /var/opt/releases/ and run the command gpg --decrypt-file *.gpg. Enter
 the password supplied from Dragos for the installation. This will create all the files required for the installation.

743 3. Change directory to /root/ and, as root user, run ./puppet_server_setup.sh

744 2.3.2 Dragos Midpoint Sensor

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

749 2.3.2.1 Network

- The midpoint sensor has multiple interfaces. One interface will collect traffic via SPAN port. Another will
 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
- After the midpoint sensor is deployed and listening on the correct interface, the midpoint sensor canconnect back to the Sitestore for further configurations.

761 2.3.3 Dragos Splunk Integration

The Dragos Splunk application allows data integration from the Dragos Sitestore into the Splunk
 dashboard. This allows Splunk to aggregate data from Dragos and other products into a central location
 for analyst visualization. This process assumes the reader has downloaded the Dragos Splunk application

- 765 from https://splunkbase.splunk.com/app/4601/.
- To begin, log in to the Splunk instance, and select the gear icon on the top left of the screen next to
 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.
- 4. Restart Splunk (either prompted by the installation process or self-directed).
- 5. From the Splunk **Settings** menu on the top right, select the **Data Inputs** option.
- Select Add New under Local Inputs for a transmission control protocol (TCP) listener. (User
 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.
- 10. Set the App Context to Dragos Splunk App.
- 11. Set the Index to dragos_alerts. (Create a new index if it does not exist.)
- 779 12. Click Submit.
- Once this process is completed, Splunk is ready to receive data from Dragos. The following instructions
 will be for configuring the Dragos Sitestore for sending information to Splunk:
- 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.**
- 6. Set the following value (must be on one line for Splunk to properly process) as **Message**:

```
{ "app": "dragos:platform", "body": "${content}", "category": "${summary}",
"created_at": "#{createdAt}", "dest": "${dest_asset_ip}",
791
792
793
       "dest_dragos_id": "${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": "${asset_ip}", "dvc_dragos_id":
       "${dest_asset_id}", "dvc_host": "${dest_asset_hostname}", "dvc_ip":
798
799
       "${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": "${src_asset_hostname}", "src_ip":
805 "${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 require sensitive data, such as asset location and IP address. The file is encrypted and provided to the 814 815 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,
- 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
- 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

831 Figure 2-2 Device Update Availability Details-1

Device Update Availa The entries listed on sub- released for a particular	bility Details sequent pages provide detailed information of the patches and updates device.					
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 Palazza Data	Private - Available Upon Request					
Filename	12/22/2010 Not Available - Customer Login Required					
SHA1	5465a09b32a8f4881188beac1e1940f619a43e80					
SHA256	5591694c3777eaccfdab9949ced81b18be4c6c9e267c4fa2e2fdd7733ec1113e					
Update Classification						
Severity	Unknown					
Update Type	PotentialSecurityRelated					
Security Summary	NA					
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	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.					

Schweitzer Engineering	g 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	01/15/2019
Filename	Not Available - Customer Login Required
SHA1	6a672a1eedf90dcc7fccf42a52b8bb2c798d2772
SHA256	a50c4b4188fef7be4d66e9041705cb25d7fca8b248360c7aca3f0e4fb069ab94
Update Classification	
Severity	Unknown
Update Type	Non-Security
Security Summary	NA
CVE IDs	
CVE ID CVSS	S 2.0 Score CVE Summary
Download Link(s)	
Patch Download	Private - Available Upon Request
Release Notes	Private - Available Upon Request
Additional Comment(s)	
Comment	NA
Note: NA	

835 Figure 2-4 Device Update Availability Details-3

Release Informat	tion								
Vendor Na	ne	Schweitzer E	Engineering Laboratories (SEL)						
Vendor Product		SEL-3530-X	SEL-3530-X						
Model No/	Version	Latest	Latest						
OS/Firmwa	re	N/A	N/A						
Patch Name	2	Private - Ava	allable Upon Request						
Kelease Da	te	03/12/2019							
Filename			e						
SHADES		D811084008	38C13D3C3400e0371008C8D20828010 cd0c00f2058d4740c7f84d18d2b5cfc72f3d6d6d8b1f7826ccc164						
JIA230		00041292850	cu0c001505604740c716401605D5d1d7512000006D117650ccd106						
Update Classifica	ition								
Severity	_	Unknown							
Opdate Typ	e	Non-Security							
Security Su	i i i i i ai y	N/A							
CVE IDs									
CVE ID	CVSS	2.0 Score	CVE Summary						
Download Linkle	1								
Patch Down	beak	Private - A	vailable Unon Request						
Release No	tes	Private - A	vallable Upon Request						
nereuse no									
Additional Comn	nent(s)								
Comment		If you woul please con	ld like to receive the latest Firmware for your installed product, tact your SEL Sales Representative.						

837 Figure 2-5 Device Update Availability Details-4

Schweitzer Engineering	g 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	
CVEID CVS	S 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	
NOLE: N/A	

839 Figure 2-6 Device Update Availability Details-5

Schweitzer Engineering	Laboratories (SEL) SEL-451-X – R3XX						
Release Information							
Vendor Name	Schweitzer Engineering Laboratories (SEL)						
Vendor Product	SEL-451-X						
Model No/Version	R3XX						
OS/Firmware	N/A						
Patch Name Private - Available Upon Request							
Release Date 12/28/2018							
Filename	Not Available-Customer login required						
SHA1	956351bd948001301a1c3726a0ece25a638aa4d0						
SHA256	212ac18155b2b/a5d7cdabb7897c3b5cea1ebe84tb4c1bt31bd604ea5193a924						
Update Classification							
Severity	Unknown						
Update Type	Non-Security						
Security Summary	NA						
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	NA						

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	https://portal.icsupdate.com/PatchEvidence/8267e758- edcb-a6e2-4340-525c4264XXX
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	2/5/2019	https://portal.icsupdate.com/PatchEvidence/8267e758- edcb-a6e2-4340-525c4264cXXX
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	3/26/2019	https://portal.icsupdate.com/PatchEvidence/8267e758- edcb-a6e2-4340-525c4264cXXX
Schweitzer Engineering Laboratories (SEL)	SEL-3530-X	Latest	Yes	6/6/2019	https://portal.icsupdate.com/PatchEvidence/8267e758- edcb-a6e2-4340-525c4264cXXX
Schweitzer Engineering Laboratories (SEL)	SEL-451-X	R3XX	Yes	1/15/2019	https://portal.icsupdate.com/PatchEvidence/9441285c- afc0-73cf-9acc-7084d9c45XXX
Schweitzer Engineering Laboratories (SEL)	SEL-361XX	N/A	No	8/21/2019	https://portal.icsupdate.com/PatchEvidence/f263af0a- 86c3-d608-464e-7b849f89cXXX
Schweitzer Engineering Laboratories (SEL)	SEL-362XX	N/A	No	8/21/2019	https://portal.icsupdate.com/PatchEvidence/62e1621a- 5310-b484-9c6f-fcf958a5eXXX

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	https://portal.icsupdate.com/PatchEvidence/ca85e557- 3317-2012-4b9f-c4cde2313XXX
Siemens	RuggedCom RSXXX	Latest	No	9/4/2019	https://portal.icsupdate.com/PatchEvidence/81923124- e84c-9446-2fcc-83115646eXXX

843

844 **2.5 Kore Wireless**

845 This solution leverages a Kore Wireless virtual private network (VPN) to provide secure remote access to

remote assets. In this case, the remote asset is an Obvius A8812 Data Acquisition Server that providesaccess 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*
- Connect the MultiConnect eCell Ethernet port to the Ethernet port on the Obvius A8812 Data
 Acquisition Server.
- 853 2. Connect the Obvius A8812 RS485 to the multidrop Modbus network with the remote steam meter854 asset.
- 855 *2.5.1.2 Network*
- 856 1. Set Obvius A8812 to **DHCP.**
- a. Navigate the IP address of the Obvius A8812. Default is *192.168.40.50*.
- b. Open the **Networking** drop-down menu, and select **Setup**.
- c. Check the Use DHCP to automatically assign IP Address checkbox.

ion List	TO Address of	192 168 40 50
nework	IP Address:	055.055.055.0
ms	Subnet Mask:	255.255.255.0
D.	Default Gateway:	192.168.40.1
File Data	Hostname:	001EC6002681 (edit)
vorking	DNS Server #1:	8.8.4.4
us	DNS Server #2:	8.8.8
ap ppp0 (modem)	Ethernet MTU:	1500 (128-1500, default 1500)
em em	Use DHCP to automatically assign IP Address:	×
ing / Diegs	Enable UPnP:	V
	HTTP Proxy server Address:	Port: (both blank = no proxy)
	Allow "Remote Access":	R-A disabled
	Allow Telnet logins:	No (TCP port closed) V (Telnet & FTP may be temporarily activated)
	Allow FTP logins:	No (TCP port closed)
	Allow SSH logins:	No (TCP port closed) V (SSH may be temporarily activated)

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

← → C ① Not secure | 192.168.2.1 Q 🖈 🤨 🔞 Internet Setup Connection with SIM-A Card item Setting · Auto Dial-up PIN Code 🗑 Enab Roaming Data Usage E Enable Carrier Name Cycle Period Hours er * / 31 * 19 * 0 * • / De Cycle Start Date Data Allowance Enance Halting Internet 30/40 Connection Co Setting

> Auto-reco (0) Atways 🔻

Enable Fix

Save Unx

Enable

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

Time Sch MTO:

D Pas NAT

Cel

865

864

2.5.2 Virtual Private Network Configuration 866

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

Tunnels Mobile Clie	nts Pre-Share			Openvi	N				
IPsec Tunnels	Remote Gateway	d Keys	Advanced Setti	ngs P1 Protocol	P1 Transforms	P1 DH-G	roup P1	Description	Actions
	WAN		main	AES (256 bits)	SHA256	2 (1024	bit)	e e e c i p d o i i	101
		Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Method	ls P2 actions	
	Disable	tunnel	172.16.2.80/29		ESP	AES (256 bits)	SHA256	100	
	Disable	tunnel	172.16.2.80/29		ESP	AES (256 bits)	SHA256	100	

- 869 2. Click the Add P1 button.
- 870 3. Set Remote Gateway.
- 4. Set Authentication Method to Mutual PSK. 871
- 872 5. Set Pre-Shared Key.
- 873 6. Set Encryption Algorithm settings:

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

General Information									
Disabled	Set this opti	ion to disable	this phase1 witho	ut removing i	t from the list.				
Key Exchange version	IKEv1				~				
	Select the Inter	net Key Exch	ange protocol vers	ion to be use	d. Auto uses IKEv2	when initiat	or, and accepts eithe	er IKEv1 or I	KEv2 as responder.
Internet Protocol	IPv4				~				
	Select the inter	net Protocol	family.		654				
Interface	WAN								
And a second sec	Select the inter	face for the lo	ocal endpoint of th	is phase1 ent	iry.				
Remote Gateway	<u> </u>	1							
Nemote Catenay	Enter the public	IP address o	or host name of the	e remote gate	way.				
	2								
Description	A description m	any ha antara	d hara far administ	trativo roforo	use (pot parend)				
	Aussaption	iay de amere	a here for earthing	ourrererer	ice (not pareed).				
Phase 1 Proposal (A	uthentication)								
Authentication Method	Mutual PSK				~				
	Must match the	e setting chos	sen on the remote :	side.					
Negotiation mode	Main				~				
	Aggressive is n	nore flexible,	but less secure.						
My identifier	My IP address	1			~				
Poor identifier	Peer IP addre	55			~				
reenaenanen			2						
Pre-Shared Key									
	Enter the Pre-S This key should	hared Key str I be long and	ing. This key must random to protect	match on bo the tunnel ar	th peers. nd its contents. A v	veak Pre-Sha	red Key can lead to	a tunnel cor	mpromise.
	2 Generate new	w Pre-Shared Ki	2						
Phase 1 Proposal (Er	ncryption Algo	orithm)							
Encryption Algorithm	AES	~	256 bits	~	SHA256	~	2 (1024 bit)	~	Deloto
	Algorithm		Key length		Hash		DH Group		

- 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.



General Information					
Disabled	Disable this phase 2 entry without removing it from th	e list.			
Mode	Tunnel IPv4	~			
Local Network	Network Type	~	172.16.2.80 Address	/ 29	~
NAT/BINAT translation	Local network component of this IPsec security association in the IPsec se	ress to be translate	Address	/ 0	~
Remote Network	Address Type Remote network component of this IPsec security associ	ation.	10.144.85.96 Address	/ 0	~
Description	A description may be entered here for administrative refe	rence (not parsed).			
Phase 2 Proposal (S	A/Key Exchange)				
Protocol	ESP Encapsulating Security Payload (ESP) is encryption, Auth	entication Header (AH) is authentication only.		
Encryption Algorithms	✓ AES		256 bits		~
	AES128-GCM		Auto		~
	AES192-GCM		Auto		~
	AES256-GCM		Auto		~
	Blowfish		Auto		~
	□ 3DES				
	CAST128 Note: Blowfish, 3DES, and CAST128 provide weak securit	y and should be av	oided.		
Hash Algorithms	□ MD5 □ SHA1 ☑ SHA256 □ SHA38	4 🗌 SHA512	AES-		

887 2.6 pfSense VPN

- 888 pfSense is an open-source firewall/router used to create both site-to-site VPN tunnels. The following
- configuration file can be used to upload all configurations to the enterprise location edge router. Boththe 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 <u>https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html.</u>

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 <u>https://www.splunk.com/page/sign_up.</u>
- 915 Download Splunk Enterprise from <u>https://www.splunk.com/en_us/download/splunk-enterprise.html</u>.
- 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 <u>https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/Installtheuniversalforwardersoft</u>
- 922 <u>ware.</u>
- 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. xisting lookup tables or upload a new file.

up definitions + Add new Existing lookup definitions or define a new file-based or external lookup.

- 933 xisting automatic lookups or configure a new lookup to run automatically.
- 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.
- Tripwire Industrial Visibility is installed at three locations: Plano, Texas (TDi); UMD; and the NCCoE. This
 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.

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
- The following subsections document the software, hardware/VM, and network configurations for theTripwire 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.**



1021

- 1022 2.8.1.4 Configuration
- 1023 Configure the Tripwire Industrial Visibility sensors.
- Connect to the configuration tool by entering the following URL into the browser:
 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).

tripwi	re		
Configuration	Maintenance	Monitoring	Simulation
Initialization			
System is not in	italized, what woul	d you like to do?	
Bootstrap Ser	isor Bootstrap	p Standalone	Bootstrap Central

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

Site Name	
Site	
DB Name	
dibi	
DB Server	
localhost	
DB User	
lkpo_backend	
DB Password	
License key	
970b1cb06026fc0bbd5a9624de466c ef55af1e039cb92c4834498a1a2f98b	bdd2344dbaab7a6acd9c2807055114383fce4e9 de0a89f480a5452711024

1031

Set the Sniffer Interface on the Configuration tab. Select the interfaced used as the SPAN port.
 Select Apply.

Local Sniffer	Sensor Light	
Network	Interface	Tcpdump Filter
ens224		
	ens192 (00:0c:29:84:89:c6)	c
	ens224 (00:0c:29:84:89:d0)	c
🗢 ens192		
	✓ ens192 (00:0c:29:84:89:c6)	C
	ens224 (00:0c:29:84:89:d0)	e

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

letworks				+ A0
Name	Save Caps	Detect Known Threats		
ens224			Rename	Delete
ens192			Rename	Delete

1036

- 1037 7. Next, Join the Sensor to the Sensor Server. Set up the Central Server in Section 2.8.3 before1038 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 password1042 found on the Central Server. Select Join.
Site Name 🔲 Rename site	
UMD_LAB	
Central IP Address	
10.100.100.111	
Central Port	
9301	
Bootstrap Password	
Setup Reverse SSH Tunnel	

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 in1046 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**.



- 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.

CONFIGURATION	CVCTEM MAN	ACEMENT	_				
SETTINGS	JTJTEM MAN	AULMENT					
GENERAL	SYSTEM MODE	SYSTEM INFO	SYSTEM RESET	CUSTOM ATTRIBUTES	SUBNETS		
SYSTEM MANAGEMENT	Currently the sys	tem is running under: nding resolution, you w	Operational mode	training mode until all a	lerts are resolved.		
EXPORT DATA	🤝 Enter train	ing mode				+ Ad	d new r
ASSET SOURCES	ID Sta	rt IP End	JIP Ne	twork Vlan	Active Until	Actions	
				No records found			
VIRTUAL ZONES							

1054

1055 5. Select the Subnets tab. Click Add Tag.

CONFIGURATION	SYSTEM MAN	AGEMENT				
SETTINGS	SYSTEM MODE	SYSTEM INFO	SYSTEM RESET	CUSTOM ATTRIBUTES	SUBNETS	
GENERAL						
SYSTEM MANAGEMENT	Tags					Add Tag
EXPORT DATA	Name		Descript	ion	Actions	
	UMD		UMD Co-	Gen Plant	🗾 Edit 🗑 Delete	
ASSET SOURCES						

1056

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

NAME		
Insert name		
This field is required.		
DESCRIPTION		
Enter a short description		

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



- 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.

- 1110 1. Connect to the CTD Dashboard: *https://10.100.100.1111:5000*.
- 1111 2. Select the hamburger menu in the top left corner.



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

 \equiv



1114

1115 4. Select Syslog. Select Add.

CONFIGURATION	- SYS	LOG									
-MAIL NOTIFICATIONS											+ Ad
VSLOG						RE	SULTS (3)				
	10	Server	Port	Protocol	Туре	Message Contents	Message Format	Local			
ECURITY SETTINGS	0	10.100.200.101	515	UDP	syslog	Alerts	CEF	No	<u>∦</u> Edit message	👕 Delete	🛱 Send a test
SER MANAGEMENT	1	10.100.200.101	515	UDP	syslog	Baselines	CEF	No	∉ Edit message	Delete	Send a test
IOMAIN5	2	10.100.200.101	515	UDP	syslog	Events	CEF	No	▲ Edit message	Delete	😫 Send a test

1116

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

+ Add new syslog		
То		
Fram		
Select Site V		
Note that the syslog message is always sent from the EMC	2	
MESSAGE CONTENTS:	MESSAGE FORMAT:	
SELECT LOG LEVEL	CEF	~
THIS FIELD IS REQUIRED.		
SERVER:		
Choose server		
THIS FIELD IS REQUIRED. PORT:		

1118

- Select Alerts for the Log Level. Enter the IP address for the Splunk server under Server. Enter Port
 and Protocol UDP. Select all boxes under Category and all boxes under Type. Leave the System
- 1120 515 and Protocol UDP. Select all boxes under Category at
 1121 URL and the Message Format as the default.

MESSAGE CONTENTS:		MESSAGE FORMAT:	
ALERTS	~	CEF	~
Category			
All			
Туре			
All	\sim		
SERVER:			
PORT:			
515			
PROTOCOL:			
UDP	~		
SYSTEM URL:			

1123 7. Select **Save**.

- 1124 8. Select **Add** to add another.
- 1125 9. Select **Baselines** under **Message Contents.**

IESSAGE CONTENTS:		MESSAGE FORMAT:	
BASELINES	~	CEF	
Name			
Name			
Transmission			
Transmission			
Source port			
Source port			
Destination port			
Destination port			
Protocol			
Select Protocol	\sim		
Communication Type			
Select Communication Type	~		
Access Type			
Select Access Type	~		

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

10 100 200 101	
PORT:	
515	
PROTOCOL:	
UDP	~
SYSTEM URL:	

1129

- 1130 11. Select **Add** to add another.
- 1131 12. Select EVENTS for Message Contents. Enter the Splunk IP for Server, Port 515, and Protocol UDP.
- 1132 Leave the **System URL** as default.

MESSAGE CONTENTS:		MESSAGE FORMAT:	
EVENTS	~	CEF	~
Select filters for the correspondin	g alerts		
Category			
Select Category	~		
Туре			
Select Type	~		
SERVER:			
10 100 200 101			
PORT:			
515			
PROTOCOL:			
UDP	~		
SYSTEM LIDI .			
STSTEM ORE.			
https://10.100.100.111.5000			

1134 13. Click **Save.**

1133

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.

ASSETS	VIEW	1						en Type			Presets		0	Reset
Type			Sita			Venidor			Printocol	Criticality	Search By			
Select Ty	ype	~	Select S	ite	~	Select V	endor	¥ .	Select Protocol \lor	Select Criticality 🗸	Name, I	P. Version, Model, Mac	Le le	
							Sc	hedule rej	port			CLEAR ALL QU	ERY VIEW ADVA	VCED OPTIONS-
	≣•	Ľ	¢	Û	Ŧ	Ť.	R	1	RESULTS (67)			н	4 1 2 3	н н и
5	SITE \$	N	AME		IP ‡			MAC \$	¢ type ¢	CRITICALITY 🗢	RISK LEVEL ≑	VENDOR \$	NETV	VORK \$

- 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
- daily. Click **Create.**

Report Detai	13
Report name:	CTD Assets Report
Description:	Explain what this report is about, what's its goals, main filters, etc. (Optional)
Display and I	Data Scope
Filters:	Chost Assats Don't show phost assats Address Tune Unicast
Include:	Rack Slots Nested Devices

- 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.
- 11461.Download the Claroty Continuous Detection Application for Splunk from1147https://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.

1172 Appendix A List of Acronyms

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