

Forescout OT Network Security Monitoring App for Splunk

Rapidly Detect and Mitigate Threats without Disrupting Operations

To prevent operational disruptions, operational technology (OT) asset owners need to know what devices are on their networks and monitor them to detect threats in real time. The Forescout OT Network Security Monitoring App streamlines threat detection and response workflows for faster and more effective risk mitigation.

Challenges

Industrial organizations are under pressure to secure and monitor their growing OT and industrial control system (ICS) networks with fewer resources. To accomplish this, asset owners require cohesive visibility into devices and network operations in a manageable, digestible way. Currently, attaining this type of information requires multiple tools and resources. Common challenges include:

- Slow and incomplete threat/incident response times
- Inefficient implementation and enforcement of compliance tasks
- Complex integrations with SIEMs and other enterprise tools
- Limited budget and staff to implement required IT-OT security strategies
- Elevated risk of downtime of critical business operations

79%

of organizations with a SCADA/ICS network have suffered a breach in the past 24 months¹

— Forrester

Customer Benefits

- Enable accurate detection and prioritization of OT threats for remediation with Splunk
- Gain real-time, intelligent alerting with highly configurable Splunk messages leveraging information gathered from eyeInspect
- Reduce MTTR to cyber and operational threats by providing device-specific, contextual asset information
- Identify recent changes in the network and asset configuration

The Forescout Solution

The Forescout OT Network Security Monitoring App for Splunk Enterprise Security enables asset owners to act on OT threats and vulnerabilities with more accurate and contextual information. Data from Forescout eyeInspect (formerly SilentDefense™) is directly available in pre-built dashboards for Splunk Enterprise Security allowing asset owners to address OT threats in timely, flexible ways. Powerful and configurable widgets included in the App streamline threat detection, simplify threat analysis and reduce mean time to response (MTTR) to threats across the OT network.

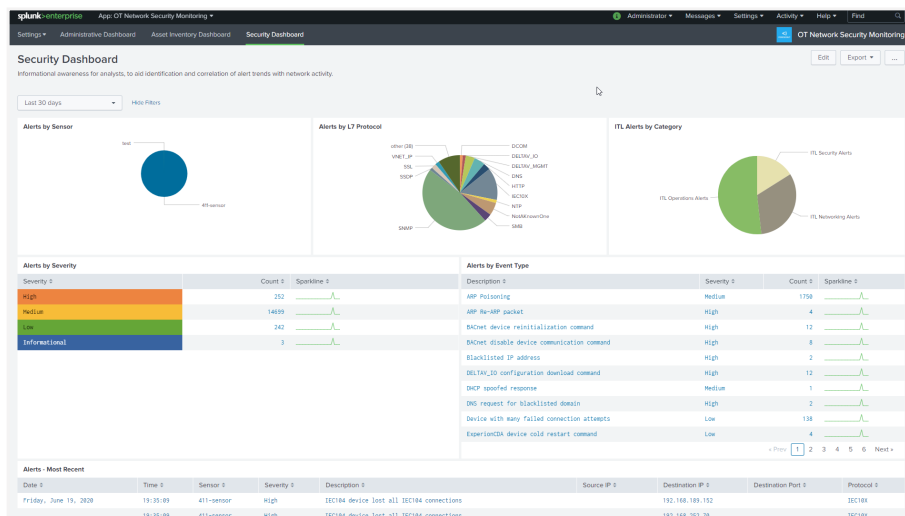
Splunk users are provided unparalleled contextual information required to secure every ICS environment by means of three dedicated dashboards. Here are summaries of within the Splunk Enterprise Security solution.

Integrating OT-specific threat indicators into Splunk

The Security Dashboard helps users identify alert trends and correlate them with other network activities to enable device compliance enforcement as well as anomaly and threat detection. This valuable context helps reduce threat and incident response times.

Alert prioritization according to business impact

Through the combination of detailed OT asset inventory information and critical operational and security alert data, the solution facilitates the prioritization of risks and vulnerabilities according to urgency and risk level. Analysts and asset owners now have granular threat intelligence behind each alert on a single dashboard, driving faster and more informed remediation action.



Asset management from Splunk

The Asset Inventory Dashboard lets asset owners and analysts access high-value device information to enhance detection of unexpected changes in the network. With this feature, you can rapidly prioritize investigations and acknowledge new assets, communication patterns and protocols within the network.

The screenshot shows the 'Asset Inventory Dashboard' in Splunk Enterprise Security. It displays a table of assets with the following columns:

Time in Past (hours:minutes:seconds)	IP	MAC Address(es)	Vendor/Model	Firmware	Hardware	Serial	Labels	OS Version	First Seen
17:57:06	192.168.171.61	00-01-02-AA-08-46	SEL (301-5)	SEL-301-5-0510-01-2180185-020178018	-	-	-	-	2020-06-18T10:19:32.000+02:00
17:57:05	192.168.82.168	00-01-02-AA-08-45	SEL	-	-	-	positionFloor1	-	2020-06-18T10:19:35.000+02:00
17:57:05	192.168.81.189	00-01-02-AA-08-16	SEL	-	-	-	-	-	2020-06-18T10:19:35.000+02:00
17:57:22	192.168.217.258	00-01-02-AA-08-74	Rockwell	-	-	123-456-7890	-	-	2020-06-18T10:19:18.000+02:00
17:57:08	192.168.4.31	00-01-02-AA-08-62	ABB (AC 800H PM801)	5.8.2084.52	-	-	rrsp_network_area01 rrsp_network_gate01 rrsp_node011	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.182.155	00-01-02-AA-08-18	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.201.15	00-01-02-AA-08-35	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.84.178	00-01-02-AA-08-27	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.181.188	00-01-02-AA-08-33	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.43.41	00-01-02-AA-08-37	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.39.128	00-01-02-AA-08-67	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.49.69	00-01-02-AA-08-28	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.11.194	00-01-02-AA-08-68	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00
17:57:06	192.168.157.74	00-01-02-AA-08-58	-	-	-	-	-	-	2020-06-18T10:19:34.000+02:00

Below the table, there is a section for 'Assets (with Modules) - Added to Inventory' with columns for Time in Past, IP, MAC Address(es), Vendor/Model, Firmware, Hardware, Serial, Labels, OS Version, First Seen, and Modules.

splunk

enterprise

App: OT Network Security Monitoring

Settings

Administrative Dashboard

Asset Inventory Dashboard

Security Dashboard

Administrator

Messages

Settings

Activity

Help

Find

OT Network Security Monitoring

Administrative Dashboard

Informational awareness for administrators, providing insights on user activity, as well as Sensor and Command Center health status changes.

Last 30 days

Hide Filters

Failed Logins

Date	Time	User IP	Username	Reason
Thursday, June 18, 2020	17:11:31	10.11.105.25	admin	Invalid password

User Activity

Date	Time	Client IP	User	Resource	Action	Details
Friday, June 19, 2020	17:56:07	10.11.105.20	admin	System	Logout	
	17:32:48	10.11.105.20	admin	Sensor 411-sensor (id=13) - threat library	Start	
	17:32:45	10.11.105.20	admin	Sensor 411-sensor (id=13) - threat library	Start	
	17:32:45	10.11.105.20	admin	Sensor 411-sensor (id=13) - Analytics feeder module	Start	
	17:32:45	10.11.105.20	admin	Sensor 411-sensor (id=13) - FEA module	Start	
	17:32:45	10.11.105.20	admin	Sensor 411-sensor (id=13) - Parsing module	Start	
	17:32:45	10.11.105.20	admin	Sensor 411-sensor (id=13) - MITM module	Start	
	17:32:45	10.11.105.20	admin	Sensor 411-sensor (id=13) - Portscan module	Start	
	17:32:41	10.11.105.20	admin	Profile 99 UDP communications	Edit	
	17:32:26	10.11.105.20	admin	Profile 98 TCP communications	Edit	

« Prev

1

2

3

4

5

Next »

Connect/Disconnect Changes

Date	Time	Sensor	Current Status	Previous Status	Value
Friday, June 19, 2020	18:17:26	411-sensor	NORMAL	WARNING	connected
	18:17:10	411-sensor	WARNING	NORMAL	disconnected
Thursday, June 18, 2020	17:10:40	test	NORMAL	CRITICAL	connected
	17:10:15	test	CRITICAL	NORMAL	disconnected

Health Changes

Date	Time	Sensor	Health Area	Current Status	Previous Status	Value
Friday, June 19, 2020	18:18:02	411-sensor	throughput	NORMAL	CRITICAL	4789893 bps
	18:17:26	411-sensor	sensor connection	NORMAL	WARNING	connected
	18:17:17	411-sensor	throughput	CRITICAL	NORMAL	0 bps
	18:17:10	411-sensor	sensor connection	WARNING	NORMAL	disconnected
	16:36:10	Command Center	NTP service	NORMAL	NORMAL	clock not synchronized
	16:36:10	Command Center	license	NORMAL	NORMAL	VALID
Thursday, June 18, 2020	17:10:40	test	sensor connection	NORMAL	CRITICAL	connected
	17:10:15	test	sensor connection	CRITICAL	NORMAL	disconnected

The Administrative Dashboard in one of three unique dashboards available in the Splunk Enterprise Security solution. By integrating OT-specific threat indicators and enriching alerts with detailed context, the Administrative Dashboard give users a central look into their OT operation in real-time.

Why Forescout:

The Forescout OT Network Security Monitoring App is the only App to consider for Industrial users of Splunk who require richer OT asset intelligence and threat detection capabilities.

Learn more about our partnership with Splunk:

<https://www.forescout.com/splunk>

Download the app:

<https://splunkbase.splunk.com/app/5169/>

1 Forrester Research 2018 – "Protecting Industrial Control Systems And Critical Infrastructure From Attack"



Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Int'l) +1-408-213-3191
Support +1-708-237-6591

Learn more at [Forescout.com](https://forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 08_20