Forescout OT Network Security Monitoring App for Splunk

Respond and mitigate OT threats faster and more effectively

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 for Splunk 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 months[1]

— *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 (formerly SilentDefense)
- 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 enables asset owners to act on OT threats and vulnerabilities with more accurate and contextual information. Data from Forescout eyeInspect 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.

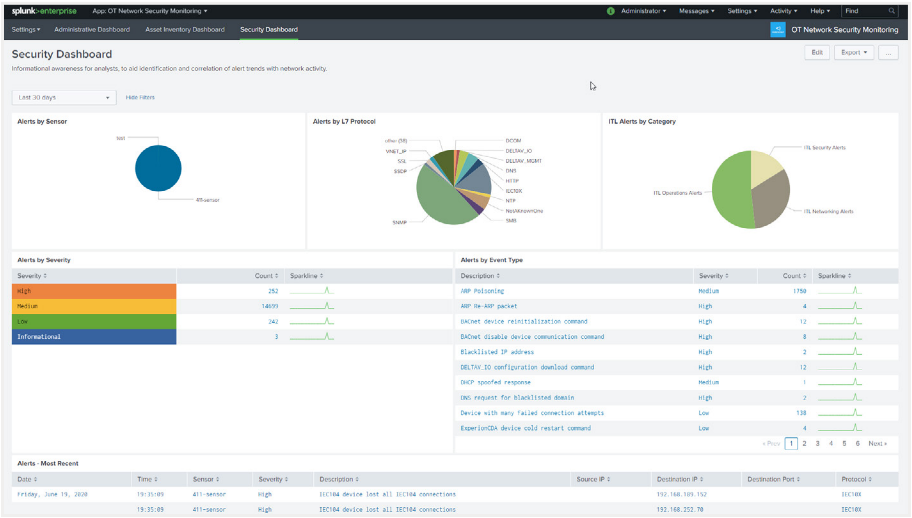
Splunk users are provided unparalleled contextual information required to secure every ICS environment by means of three dedicated dashboards. Here are summaries of the dashboards within the Splunk Enterprise Security solution.

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.



Security Dashboard

Informational awareness for analysts, to aid identification and correlation of alert trends with network activity.

Alerts by Severity

Severity	Count	Sparkline
High	252	
Medium	14699	
Low	242	
Informational	3	

Alerts by Event Type

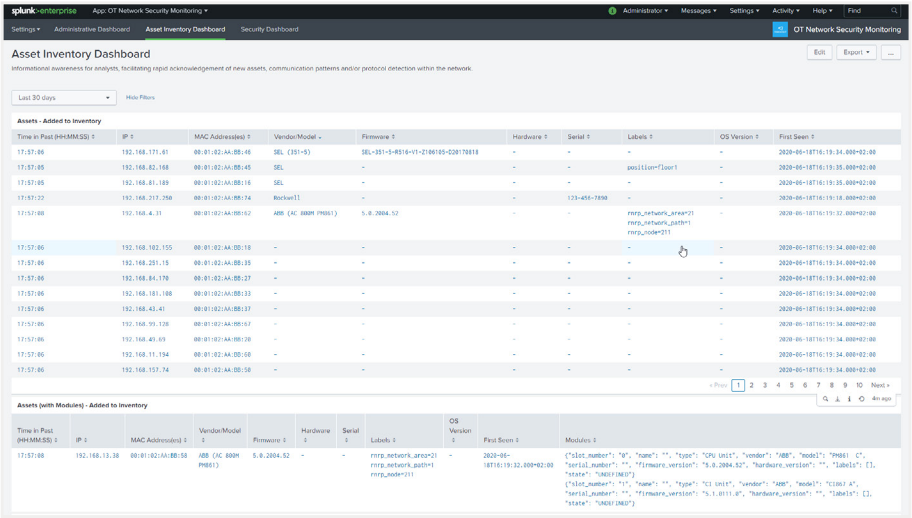
Description	Severity	Count	Sparkline
ARP Poisoning	Medium	1750	
ARP Re-ARP packet	High	4	
BACnet device reinitialization command	High	12	
BACnet disable device communication command	High	8	
Blacklisted IP address	High	2	
DELTAV_IO configuration download command	High	12	
DHCP spoofed response	Medium	1	
DNS request for blacklisted domain	High	2	
Device with many failed connection attempts	Low	138	
ExperionCDA device cold restart command	Low	4	

Alerts - Most Recent

Date	Time	Sensor	Severity	Description	Source IP	Destination IP	Destination Port	Protocol
Friday, June 19, 2020	19:35:09	411-sensor	High	IEC104 device lost all IEC104 connections		192.168.189.152		IEC10X
	19:35:09	411-sensor	High	IEC104 device lost all IEC104 connections		192.168.252.70		IEC10X

Valuable OT Asset Insight

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.



Asset Inventory Dashboard

Informational awareness for analysts, facilitating rapid acknowledgement of new assets, communication patterns and/or protocol detection within the network.

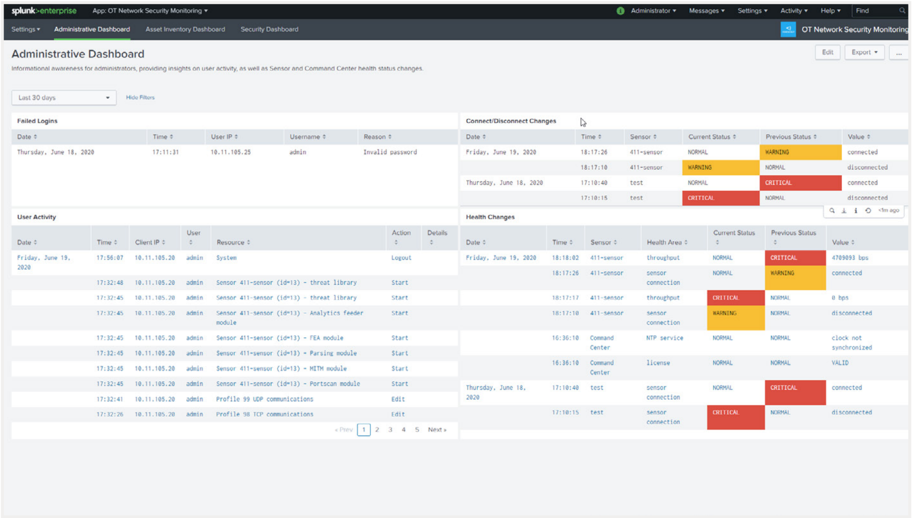
Assets - Added to Inventory

Time in Past (HH:MM:SS)	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:BB:46	SEL (351-5)	SEL-351-5-R516-V1-Z106105-D20170818	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:05	192.168.82.168	00:01:02:AA:BB:45	SEL	-	-	-	position=floor1	-	2020-06-18T16:19:35.000+02:00
17:57:05	192.168.81.189	00:01:02:AA:BB:16	SEL	-	-	-	-	-	2020-06-18T16:19:35.000+02:00
17:57:22	192.168.217.250	00:01:02:AA:BB:74	Rockwell	-	-	123-456-7890	-	-	2020-06-18T16:19:18.000+02:00
17:57:08	192.168.4.31	00:01:02:AA:BB:62	ABB (AC 800M PM861)	5.0.2004.52	-	-	rnrp_network_area=21 rnrp_network_path=1 rnrp_node=211	-	2020-06-18T16:19:32.000+02:00
17:57:06	192.168.102.155	00:01:02:AA:BB:18	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.251.15	00:01:02:AA:BB:35	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.84.170	00:01:02:AA:BB:27	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.181.108	00:01:02:AA:BB:33	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.43.41	00:01:02:AA:BB:37	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.99.128	00:01:02:AA:BB:67	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.49.69	00:01:02:AA:BB:20	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.11.194	00:01:02:AA:BB:60	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00
17:57:06	192.168.157.74	00:01:02:AA:BB:50	-	-	-	-	-	-	2020-06-18T16:19:34.000+02:00

Assets (with Modules) - Added to Inventory

Time in Past (HH:MM:SS)	IP	MAC Address(es)	Vendor/Model	Firmware	Hardware	Serial	Labels	OS Version	First Seen	Modules

17:57:08	192.168.13.38	00:01:02:AA:BB:58	ABB (AC 800M PM861)	5.0.2004.52	-	-	rnrp_network_area=21
							rnrp_network_path=1
							rnrp_node=211
								-	2020-06-18T16:19:32.000+02:00	{"slot_number": "0", "name": "", "type": "CPU Unit", "vendor": "ABB", "model": "PM861 C", "serial_number": "", "firmware_version": "5.0.2004.52", "hardware_version": "", "labels": [], "state": "UNDEFINED"}
										{"slot_number": "1", "name": "", "type": "CI Unit", "vendor": "ABB", "model": "CI867 A", "serial_number": "", "firmware_version": "5.1.0111.0", "hardware_version": "", "labels": [], "state": "UNDEFINED"}



Administrative Dashboard

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

Failed Logins

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

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

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	

Health Changes

Date ⇕	Time ⇕	Sensor ⇕	Health Area ⇕	Current Status ⇕	Previous Status ⇕	Value ⇕
Friday, June 19, 2020	18:18:02	411-sensor	throughput	NORMAL	CRITICAL	4709093 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

Manage Your OT Security Appliances at a Glance

The Administrative Dashboard provides deep, real-time insights into your OT security system health status and user activity performed on your eyeInspect appliances. This helps to prevent system failure and detect undesired user activity to maintain continuous security protection.

Why Forescout:

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

Additional Resources

Learn more about Forescout eyeInspect:
www.forescout.com/platform/eyeInspect/

Download the Forescout OT Network Security Monitoring App for Splunk:
splunkbase.splunk.com/app/5169/

Learn more about our partnership with Splunk:
www.forescout.com/splunk

[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 (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com