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. — 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 Administrative Dashboard is 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 gives 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”