**Business Challenge**

Industrial control systems (ICS) can have major impacts on society, organizations and individuals’ lives. While ICS were once isolated from other parts of your organization or network—and considered static systems—this is no longer the case.

Today, ICS devices are on your OT network and connected to your enterprise and IT systems. That means they are vulnerable to malware, cyberattacks, insider threats, misconfigurations and even failed maintenance.

Because these two different worlds are now connected, an attack that starts in your IT environment can quickly move to your OT environment and vice versa. Lateral movement is a standard attack vector for hackers because it’s relatively easy to find a weak link in your system, leverage it as a point of entry, and then quickly own your entire network.

Today’s IT and OT security personnel, risk departments and even your C-suite face challenges of being able to gain insight in a single “pane of glass” to ensure complete visibility, security and control of potential attacks in both your IT and OT environments.

**Solution**

Today’s attacks are significantly more sophisticated and include Zero-day and targeted attacks, social engineering, and spear phishing—all designed to establish a beachhead and modify or destroy critical industrial operations.

The key to a successful breach is keeping nefarious activity undetected for as long as possible. Some of the most effective tools for fighting these attacks involve security intelligence and event management (SIEM) solutions. SIEM solutions monitor both real-time events and a mountain of long-term data to find anomalous usage patterns, qualify possible security and compliance threats to reduce false positives, and alert organizations when needed.

**Technology Components**

- Tenable.ot
- Splunk Enterprise

**The Challenge**

- Blind spots to security incidents that may traverse IT/OT operations
- Inability to get real-time incident information to mitigate threats before they propagate across your environment
- Full audit and drill-down options to pinpoint trouble spots and vulnerabilities
- Maintain a current inventory of assets to perform proper maintenance, including patch management and capacity planning

**Key Benefits**

- Single pane of glass view
- Get an in-depth view of external and internal threats targeting OT environments that can be addressed via firewall rules
- Address security and regulatory compliance and change management requirements
- Take advantage of automated asset discovery, classification and tracking to facilitate better firewall management
- Full inventory of all deployed industrial assets including state and configuration that enables change control tracking within your IT framework
The partnership between Tenable.ot and Splunk Enterprise provides you with visibility, security and control across your IT and OT operations. By downloading the Tenable.ot app from Splunkbase, the joint solution will monitor activity across your IT and OT environments to ensure early and comprehensive threat detection and mitigation often missed by other point products.

Key Components

Tenable.ot is purpose-built to provide real-time situational visibility, security and control into your ICS networks. It combines behavioral anomaly detection with policy-based rules and active querying to deliver comprehensive threat detection and mitigation and unique visibility into your asset inventory. Industrial facilities, including critical infrastructures, utilities, water, energy, pharmaceutical and manufacturing organizations, use Tenable.ot to automate operational oversight processes, identify human errors such as misconfigurations and failed maintenance, and protect against malware, cyber attacks and insider threats.
ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world’s first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

ABOUT SPLUNK

Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data.

Learn more at splunk.com.

More Information

For support please contact: support@tenable.com