SOLUTION OVERVIEW

Tenable.ot for RSA

Business Challenge

Industrial control systems (ICS) quite literally control our lives. While ICS was once isolated from other parts of your organization or network and considered static systems, this is no longer the case.

ICS devices, which are on your OT network, are now connected to enterprise and IT systems that are vulnerable to malware, cyber-attacks, insider threats, misconfigurations and even failed maintenance.

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 to keep nefarious activity undetected for as long as possible.

Unlike IT networks, industrial control systems lack a proper foundation for visibility and security controls. Most devices don't require authentication, making it difficult to prevent unauthorized access or changes to critical devices. There are also no event logs or historical data to help with event detection and response. Without this proper foundation of visibility and control, added challenges emerge in managing assets, detecting threats and managing systems configurations in OT environments.

Solution

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

The interoperability between Tenable.ot and RSA NetWitness provides customers with a seamless solution to collect, analyze and report on all activity helping to reduce the time it takes to identify security related issues within your IT and OT network infrastructure including industrial controller and device activity, who accesses files, what privileged user activity takes place, and which potential threats exist on your devices and in your network.

Technology Components

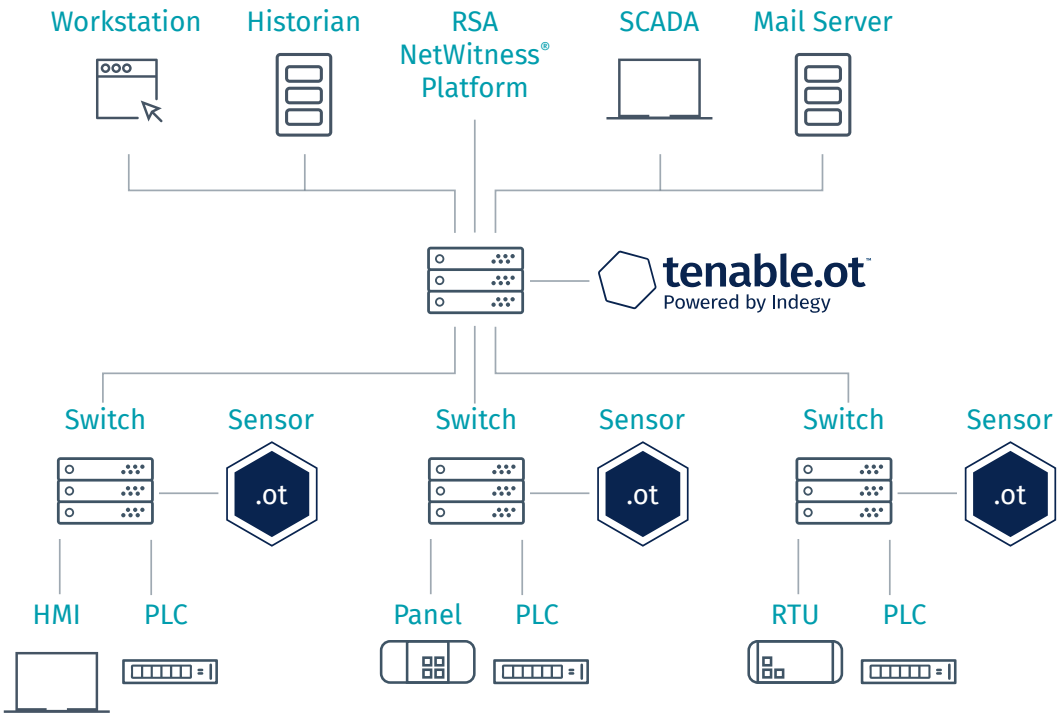
- Tenable.ot
- RSA Netwitness

The Challenge

- Single "pane of glass" visibility of potential threats in and across your IT and OT environments
- Detection and mitigation of threats to the safety, reliability and continuity of industrial processes
- Ability to snapshot changes made to PLCs
- Full and instant inventory of assets on your OT network
- Full forensic capabilities that provide context when an incident occurs

Key Benefits

- Improved security automation, sensing and visibility
- Increased control over distributed operations
- Better compliance with regulatory requirements and tracking
- Higher responsiveness when incidents occur and improved organizational performance
- Better decision-making based on more detailed information
- Proactive maintenance and reduced response times to unforeseen disruptions
- Improved flow of information to stakeholders



Key Components

The RSA NetWitness Platform provides pervasive visibility across a modern IT infrastructure, enabling better and faster detection of security incidents, with full automation and orchestration capabilities to investigate and respond efficiently. RSA NetWitness Platform takes security "beyond SIEM," extending the traditional log-centric, compliance-focused approach to security to include state-of-the-art threat analytics, including user and entity behavior analytics (UEBA), and visibility into cloud, network and endpoints.

Organizations are experiencing a rapidly changing threat environment so you need tools and services that can keep up with the changes. RSA NetWitness Platform offers the maximum amount of visibility, with automated analysis and prioritization, and in context of real business risk of a threat.

Tenable.ot provides situational awareness and real-time security for industrial control systems to ensure operational continuity and reliability. It delivers comprehensive visibility and oversight into all OT activities, whether they are network-based or device-based. These include changes to controller logic, configuration and state across all vendor devices, network communication patterns, rouge devices, malware propagation and more. This is done by utilizing both the deep packet inspection engine of proprietary control communications, and patented active querying technology that can query devices safely in their native communication protocols without ever affecting them. This enables validation of PLC and PCs firmware/OS code/software and configuration.

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 RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Learn more at **www.rsa.com**

Tenable.ot provides a critical feed into RSA's NetWitness Platform and delivers visibility, security and control for your operational environment. This, combined with the native capabilities of the NetWitness Platform, delivers the intelligence required across both your OT and IT environments.

The interoperability between Tenable.ot and RSA NetWitness offers visibility, security and control for industrial networks, enabling security professionals to effectively detect and mitigate threats to the safety, reliability and continuity of industrial processes. As part of the joint solution, monitoring occurs across your IT and OT environments to ensure early and comprehensive threat detection and mitigation that other point products can easily miss.

More Information

For support please contact: **support@tenable.com**