SOLUTION OVERVIEW

tenable

Tenable.ot for McAfee

Business Challenge

Industrial control systems (ICS) can have major impacts on society, organizations and individuals' lives. While 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 enterprise and IT systems. That also means they are vulnerable to malware, cyber-attacks, insider threats, misconfigurations and even failed maintenance.

Your modern attack surface now encompasses both IT and OT. Because these two different worlds are 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.

The Joint 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 to keep the 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 patterns of usage, qualify possible security and compliance threats to reduce false positives, and alert organizations when needed.

How It Works

McAfee Enterprise Security Manager (ESM), the foundational SIEM solution, delivers the performance, actionable intelligence, and real-time situational

McAfee

Technology Components

- Tenable.ot
- McAfee ESM

The Challenge

- Inability to see both IT and OT in a single "pane of glass"
- How to effectively detect and mitigate threats to the safety, reliability and continuity of industrial processes
- Lack of access to the last known "good state" in an OT environment
- Full and instant inventory management on each device
- Absent or deficient audit and paper trail
- 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

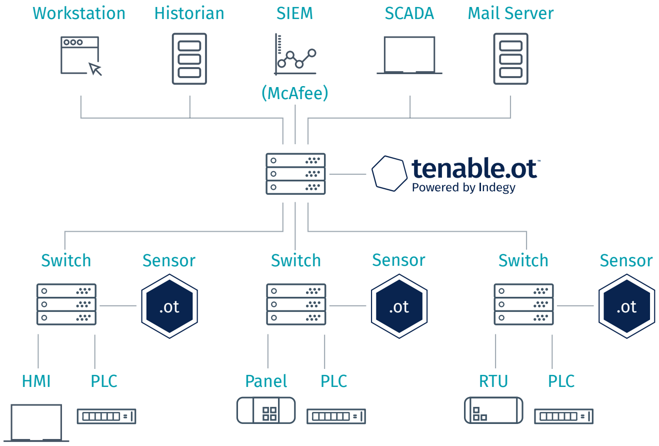
ABOUT TENABLE

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 MCAFEE

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

Learn more at **mcafee.com**.



awareness at the speed and scale you need to identify, understand, and respond to stealthy threats, while the embedded framework simplifies your ability to audit and proactively report on compliance.

Tenable.ot provides situational awareness and real-time security for industrial control networks to ensure operational continuity and reliability. It delivers comprehensive visibility and oversight into all of your OT activities, whether on network 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.

Monitoring and detection utilize both a hybrid detection engine and patented active-querying technology that can query devices safely in their native communication protocols without ever affecting them. This allows for validation of PLC and PCs firmware/OS code/software and configuration.

Tenable.ot provides a critical feed into McAfee's ESM and delivers visibility, security and control for your operational environment. Advanced OT security, combined with the native capabilities of the ESM, delivers the intelligence you need across your OT and IT environments.

The joint solution 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**