SOLUTION BRIEF

tenable.ot™
Powered by Indegy

Industrial Cybersecurity Solution Brief

The Impending Security Cyberstorm

Modern day industrial operations often span complex IT (information technology) and OT (operational technology) infrastructures. In standard industrial and critical infrastructure environments, thousands of devices exist and are increasingly accessed via the Industrial Internet of Things (IIoT). This creates new challenges in securing industrial environments specifically because cybersecurity threats are becoming more difficult to detect, investigate and remediate.

The Industry Cybersecurity Challenge

Today's sophisticated operational technology (OT) environment is a target for new attacks. The convergence of IT and OT, and rapid adoption of IoT across both, increases the overall attack surface, as well as attack vectors.

Without complete coverage, the likelihood of an attack is not a matter of "if," but "when."

Industrial controllers are a focal point for attacks on industrial operations and critical infrastructure. Depending on the industry type, this may be referred to as programmable logic controllers (PLCs), remote terminal units (RTUs) or distributed control systems (DCSs).

These controllers are extremely reliable and control everything from cooling stations to turbines, electrical grids, oil and gas and much more.

Industrial Control Systems (ICS) literally keep the lights on. Because of their reliability, many of these devices have been in place for years. They are the workhorses of today's modern society, which is why they are ground zero for attacks.

Comprehensive ICS Cybersecurity

Tenable.ot protects industrial networks from cyber threats, malicious insiders and human error. From threat detection and mitigation to asset tracking, vulnerability management, configuration control and device integrity checks, Tenable's ICS security capabilities maximize your operational environments visibility, security and control.

Visibility

Gain crystal-clear situational awareness across your converged IT/OT environment in a single pane of glass.

Security

Protect your industrial network from advanced cyber threats and risks posed by hackers and malicious insiders.

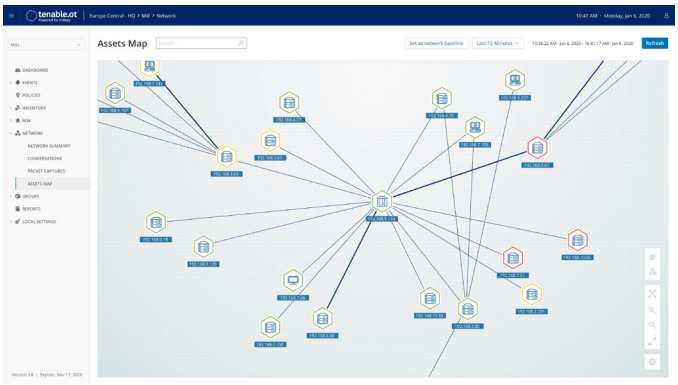
Control

Take full control of your operations network by tracking ALL changes to any ICS device.

Tenable.ot offers comprehensive security tools and reports for IT security personnel and OT engineers. It provides unmatched visibility into converged IT/OT segments and ICS activity, and delivers crystal-clear situational awareness across all sites and their respective OT assets—from Windows Servers to PLC backplanes—in a single pane of glass.

Solution Components

- **360-Degree Visibility**
  Attacks can easily propagate in an IT/OT infrastructure. With a single platform to manage and measure cyber risk across your OT and IT systems, you have complete visibility into your converged attack surface. Tenable.ot also natively integrates with leading IT security and operational tools, such as your Security Information and Event Management (SIEM) solution, log management tools, next-generation firewalls, and ticketing systems. Together, this builds an ecosystem of trust where all of your security products can work together as one to keep your environment secure.



- **Threat Detection and Mitigation**
  Tenable.ot leverages a multi-detection engine to find high-risk events and behaviors that can impact OT operations. These engines include:

  Policy-Based: With this unique capability, you can activate predefined policies or create custom policies that whitelist and/or blacklist specific granular activities that may indicate cyber threats or operational mistakes that trigger alerts. Policies can also trigger active checks for predefined situations. This is crucial to discover risky events that don't rise above the statistical noise (e.g. malware, reconnaissance activity, querying device firmware versions from a human machine interface (HMI).

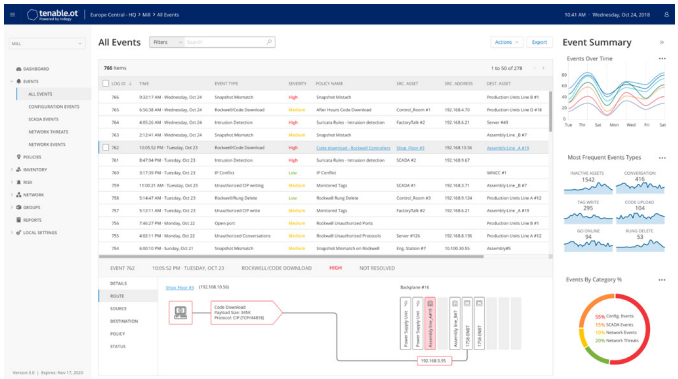
  Behavioral Anomalies: The system detects deviations from a network traffic baseline based on traffic patterns. Pattern baselines include a mixture of time ranges, protocols, devices, etc. Among other things, it allows detection of suspicious scans indicative of malware or rogue devices in your network. It then sends context-aware alerts with detailed information to your team so you can quickly respond and launch forensic investigations into what happened.

  Signature Updates: In a partnership with the Open Information Security Foundation (OISF), Tenable.ot leverages the Suricata set of signatures along with Tenable's proprietary signature rules. By leveraging crowdsourced data, you can detect attacks throughout all stages and get alerts with context about suspicious traffic that can indicate reconnaissance, exploits, installed malware, lateral propagation and more. The threat detection engine ingests new signature updates to address new threats as they evolve.

- **Asset Inventory and Active Detection**
  Leveraging groundbreaking and patented technology, Tenable.ot provides unparalleled visibility into your infrastructure—not only at the network level, but down to the device level. It combines native communication protocols to actively query IT, as well as OT devices in your ICS environment, to identify all of the activities and actions across your network.

- **Risk-Based Vulnerability Management**
  Drawing on comprehensive and detailed IT and OT asset tracking capabilities, Tenable.ot generates vulnerability and risk levels using **Predictive Prioritization** for each asset in your ICS network. These reports include risk-scoring and detailed insights, along with mitigation suggestions.

  Tenable's vulnerability assessment includes parameters such as firmware versions, relevant CVEs, proprietary research, default passwords, open ports, installed hotfixes and more. This enables authorized personnel to quickly identify the highest risk for priority remediation before attackers exploit vulnerabilities.



- **Configuration Control**
  With Tenable.ot, you can track malware and user-executed changes made over your network or directly on a device.

  Configuration control provides a full history of device configuration changes over time, including granularity of specific ladder logic segments, diagnostic buffers, tag tables and more. This enables administrators to establish a backup snapshot with the "last known good state" for faster recovery and compliance with industry regulations

Tenable.ot Components

Tenable.ot's solution is comprised of several components:

- **Core Platform**
  Collects and analyzes network traffic either directly from the network (via a span port on the switch to which it is connected or through a network tap) and/or using the data feed (of captured network traffic) from the sensors.

- **Active Detection**
  Includes a device-querying capability for enhanced device-based security and visibility.

- **Sensors**
  You can deploy optional, small, and lightweight sensors on network segments with devices that need monitoring and are connected to one sensor per managed switch.

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**.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**