SOLUTION BRIEF

tenable.ot™
Powered by Indegy

Industrial Cybersecurity Solution Brief

The OT Security Challenge

Modern-day industrial and critical infrastructure organizations rely heavily on operational technology (OT) environments to produce goods and services. Beyond traditional IT operations that utilize servers, routers, PCs and switches, these organizations also rely on OT, such as programmable logic controllers (PLCs), distributed control systems (DCSs) and human machine interfaces (HMIs) to run physical plants and factories. While OT devices have been in commercial use since the late 1960s, major changes are underway to modernize OT operations.

The Convergence Initiative

Today, an increasing number of organizations are considering—and adopting—convergence in their IT and OT environments. Others have no intention to converge IT and OT, however, even under the most favorable circumstances, this isolation is nearly impossible to maintain. The introduction of one seemingly harmless variable into a sterile environment can permanently destroy the most stringently enforced air-gap. This is known as “accidental convergence”.

Industry 4.0

Many organizations are rapidly adopting Industry 4.0 technology. In industrial and critical infrastructure environments, this can translate into thousands of devices connected via the Industrial Internet of Things (IIoT).

Both of these initiatives can result in substantial efficiencies and cost savings, but they are not without risk. Without proper OT security, you can introduce new attack surfaces and vectors and can put your OT infrastructure and operations at risk.

Comprehensive OT Cybersecurity

Tenable.ot protects industrial and critical infrastructure from cyber threats, malicious insiders and human error. From threat detection and mitigation to asset tracking, vulnerability management, configuration control and adaptive assessment checks, Tenable’s industrial control systems (ICS) security capabilities maximize your operational environnments visibility, security, and control.

Visibility

Gain full visibility and deep situational awareness across your converged IT/OT environment.

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.

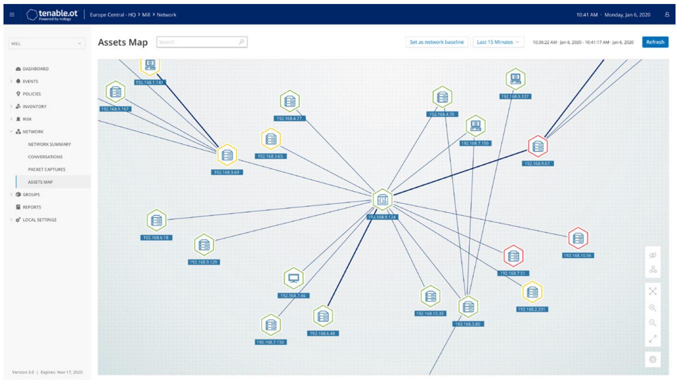
Tenable.ot offers comprehensive security tools and reports for IT security personnel and OT engineers. It provides unmatched visibility into converged IT/OT operations, and delivers deep situational awareness across all sites and their respective OT assets—from Windows servers to PLC backplanes—in a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

Solution Components

- **Complete Visibility**
  Up to 50% of your OT infrastructure contains IT assets. Attacks can easily propagate across IT/OT infrastructure. Why fly blind by only having visibility into OT assets and traffic?

  Tenable.ot, now with built-in Nessus, provides complete visibility into your converged attack surface while measuring and controlling cyber risk across your OT and IT systems.

  Tenable.ot also integrates with the Tenable product portfolio and leading IT security and operational tools for a best-in-class "ecosystem of trust" that leverages your entire security infrastructure.



- **Threat Detection and Mitigation**
  Tenable.ot leverages a multi-detection engine you can fine-tune as each unique environment dictates. It also finds high-risk events and behaviors that can impact OT operations.

  These engines include:

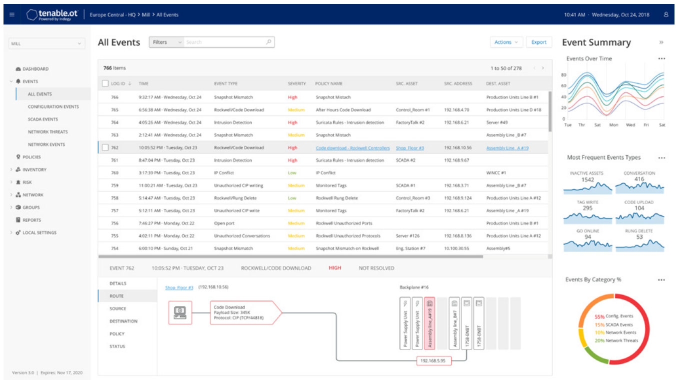
  Policy-Based: With this unique capability, you can activate predefined policies or create custom policies that whitelist and/or blacklist specific granular activities that may indicate cyber threats or operational mistakes that trigger alerts. Policies can also trigger active checks for predefined situations. 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 and you can select and customize them to address new threats as they evolve.

  Adaptive Assessment: Tenable.ot actively queries assets on your network. Active querying gives you deep insights and unparalleled situational awareness into your infrastructure without impacting operations. This patented approach gathers far more information than passive monitoring alone, including identification of devices that do not communicate on your network.

- **Risk-Based Vulnerability Management**
  Tenable.ot leverages domain expertise in industrial security for OT assets, and Nessus for IT assets. Tenable's Vulnerability Priority Rating (VPR) scoring generates vulnerability and risk levels using intelligence gained for each asset in your OT network. Reports include detailed insights, along with mitigation suggestions. This enables authorized personnel to quickly identify the highest risk for priority remediation before attackers can exploit vulnerabilities.



766 Items — 1 to 50 of 278

LOG ID	TIME	EVENT TYPE	SEVERITY	POLICY NAME	SRC. ASSET	SRC. ADDRESS	DEST. ASSET
766	9:32:17 AM · Wednesday, Oct 24	Snapshot Mismatch	High	Snapshot Mistach			Production Units Line B #1
765	6:56:38 AM · Wednesday, Oct 24	Rockwell/Code Download	Medium	After Hours Code Download	Control_Room #1	192.168.4.70	Production Units Line D #18
764	4:05:26 AM · Wednesday, Oct 24	Intrusion Detection	High	Suricata Rules - Intrusion detection	FactoryTalk #2	192.168.6.21	Server #49
763	2:12:41 AM · Wednesday, Oct 24	Snapshot Mismatch	Medium	Snapshot Mistach			Assembly Line _B #7
762	10:05:52 PM · Tuesday, Oct 23	Rockwell/Code Download	High	Code download - Rockwell Controllers	Shop_Floor #3	192.168.10.56	Assembly Line _A #19
761	8:47:04 PM · Tuesday, Oct 23	Intrusion Detection	High	Suricata Rules - Intrusion detection	SCADA #2	192.168.9.67	
760	3:17:39 PM · Tuesday, Oct 23	IP Conflict	Low	IP Conflict			WINCC #1
759	11:00:21 AM · Tuesday, Oct 23	Unauthorized CIP writing	Medium	Monitored Tags	SCADA #1	192.168.3.71	Assembly Line _B #7
758	5:14:47 AM · Tuesday, Oct 23	Rockwell/Rung Delete	Low	Rockwell Rung Delete	Control_Room #3	192.168.9.124	Production Units Line A #12
757	5:12:11 AM · Tuesday, Oct 23	Unauthorized CIP write	Medium	Monitored Tags	FactoryTalk #2	192.168.6.21	Assembly Line _A #19
756	7:46:27 PM · Monday, Oct 22	Open port	Medium	Rockwell Unauthorized Ports			Production Units Line B #1
755	4:02:11 PM · Monday, Oct 22	Unauthorized Conversations	Medium	Rockwell Unauthorized Protocols	Server #126	192.168.8.136	Production Units Line A #12
754	6:00:10 PM · Sunday, Oct 21	Snapshot Mismatch	Medium	Snapshot Mismatch on Rockwell	Eng. Station #7	10.100.30.55	Assembly#5

EVENT 762 10:05:52 PM · TUESDAY, OCT 23 ROCKWELL/CODE DOWNLOAD HIGH NOT RESOLVED

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 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 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

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

- **Sensors**
  You can deploy small optional rack mount or DIN rail, sensors on layered or complex network segments that need monitoring. They are typically connected to one sensor per managed switch.

Integrations

Tenable.ot integrates with the larger Tenable product portfolio including:

tenable.sc

Gain full visibility of all vulnerabilities that include both your IT and OT assets. You'll know which vulnerabilities take priority with a Vulnerability Priority Rating (VPR) score with each and every alert.

tenable.io

For distributed environments or locations that cannot accommodate additional physical gear, leverage to power of the cloud with all of the intelligence gained from Tenable.ot being send to Tenable.io for a "zero footprint" OT security solution.

For More Information:
Contact Us: Please email us at sales@complytec.com