tenable

SOLUTION BRIEF

INDUSTRIAL CYBER SECURITY 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 for more than 50 years, there have been major upgrades to OT infrastructure. The face of OT infrastructure is rapidly evolving.

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 CYBER SECURITY

Tenable.ot disrupts attack paths and protects industrial and critical infrastructure from cyber threats. From inventory management and asset tracking to threat detection at the device and network level, vulnerability management and configuration control, Tenable's OT security capabilities maximize your visibility, security, and control across your entire operations.

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.

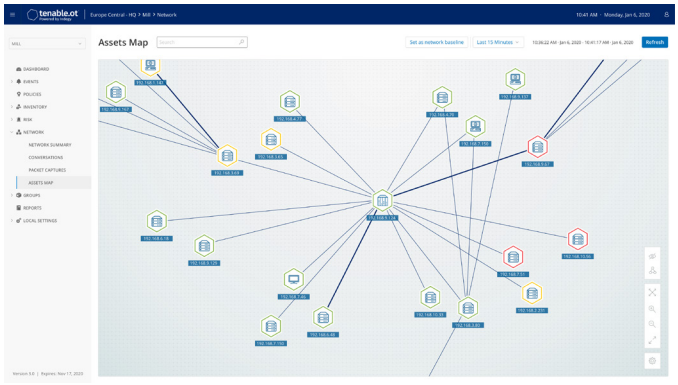
Tenable.ot offers comprehensive security tools and reports for IT and OT security personnel and engineers. It provides unmatched visibility into converged IT/OT operations, and delivers deep situational awareness across all sites, large and small and their respective OT assets—from Windows servers to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

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.



- **Detect Threats Faster**
  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.

  Advanced network detection that can find more in converged environments. This includes OT specific checks as well as IT checks that leverage Nessus Network Monitor (NNM).

  Policy Enforcement: With this unique capability, you can activate predefined policies or create custom policies that allowlist and/or blocklist specific activities that may indicate cyber threats or operational mistakes. 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).

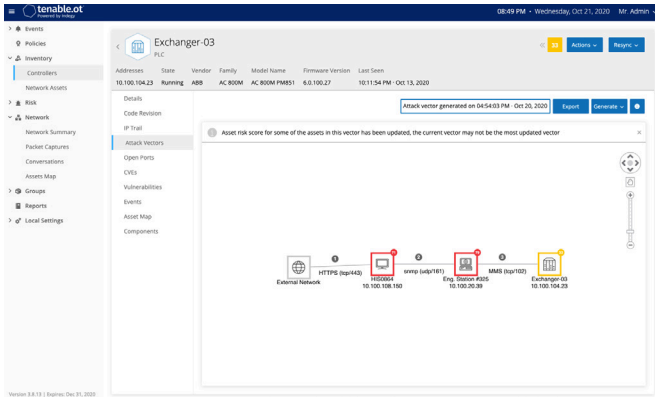
  Behavioral Anomalies: The system detects deviations from a network traffic baseline based on traffic patterns. Pattern baselines include a mixture of time ranges, protocols, devices, etc. Among other things, it allows detection of suspicious activity indicative of malware or rogue devices in your network.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

  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.

  Patented and fully configurable device based checks that can find risk before propagation occurs.

  Adaptive Assessment: Up to 30% of the devices in an OT environment do not communicate over the network.Tenable.ot goes beyond network detection by performing device checks in the device's native language. Fully configurable and customizable to each unique environment's requirements, active querying gives you deep insights and unparalleled situational awareness into your infrastructure without impacting operations. This patented approach gathers far more information than network monitoring alone.

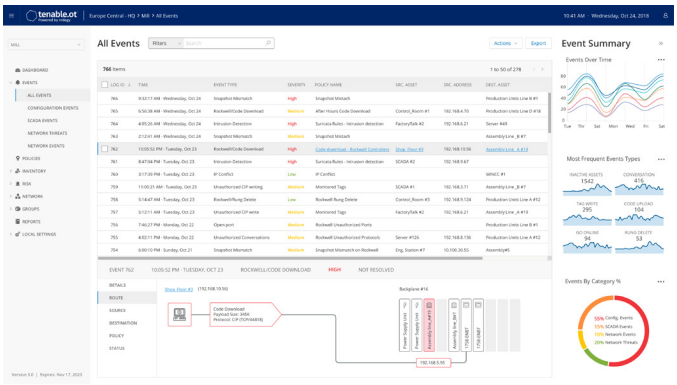
- **Attack Vectors**
  Increased security incidents in OT environments in addition to the lateral creep of attacks between IT and OT require advanced proactive threat detection methods by predicting likely pathways of an attack. Tenable.ot can map attack vectors, provide risk guidance as well as mitigation techniques to harden the attack pathways.



- **Tenable.ot Attack Vector functionality:**
  - Identifies the communication paths along the chain and validates their relevance (or lack thereof) to the process.
  - Reduces the associated and individual risk scores of the assets which participate in the attack vector.
  - Identifies which surrounding systems to patch when a patch to the controller may not yet be available.

- **Role Based Access Control**
  Different roles within the organization should have difference access to resources. Tenable.ot helps ensure that the right access levels are maintained for each role in the organization so that authorized personnel have the access they require and do not have extended privileges to sensitive areas that their job does not require.

- **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.



- **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.

ECOSYSTEM OF TRUST

Tenable.ot integrates with leading SIEM, SOAR, next generation firewalls and diode based firewalls in order to provide insights to the rest of the organization outside of OT specific titles. Tenable.ot also works in cooperation with the the larger Tenable product portfolio including:

tenable.ad

To eliminate ransomware attacks that take advantage of Active Directory misconfigurations and privilege escalation to gain access to OT environment.

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 leverage the 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: Please visit tenable.com

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

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.