tenable

SOLUTION BRIEF

UNIFIED IT/OT RISK MANAGEMENT

Market opportunities and competitive pressures are driving organizations to increase operations reliability, optimize asset utilization and improve productivity. These trends blur the traditional line separating IT from operational technology (OT). IT-based assets are increasingly deployed in OT environments, and IT and OT networks are increasingly interconnected. The result: an expanded, converged attack surface that security leaders must measure and manage.

Cyber security responsibility without adequate visibility imposes unacceptable uncertainty. However, many security leaders have an incomplete cyber risk view of the end-to-end operational processes that drive their organizations' value chain. They struggle to answer these risk management questions:

- Where are we exposed?
- Where should we prioritize, based on risk?
- How are we reducing exposure over time?

KEY CHALLENGES

OT environments are a blind spot for many security leaders. Therefore, the first steps are to identify assets in the OT environment, assess and prioritize weaknesses and then remediate weaknesses based on risk.

Identifying the Attack Surface

Knowing what you must protect is foundational to any security program, and the simpler days of air-gapped OT environments are gone. How, adversaries can pivot from OT systems to IT, and vice versa. A joint Technical Alert issued by the DHS and FBI warns organizations that adversaries can compromise business networks and then move laterally into Industrial Control Systems (ICS).

This expanded the attack surface and requires security leaders to consider not only OT assets, but IT assets in the OT environment, and connected business systems, such as ERP systems, building automation and control systems and connected lab environments. Connections to remote employees, contractors and business partners must also be catalogued. A comprehensive asset inventory is likely to include PLC's. RTUs, HMIs, IIoT devices, network devices, desktops, servers, web apps, and possibly virtual machines, containers, mobile and the cloud.

Identifying and Prioritizing Vulnerabilities

Nearly 19,000 new vulnerabilities were discovered in 2018, and more than 100 per day on average of them were rated critical. A converged IT/OT environment could easily contain tens of thousands of vulnerabilities. Therefore, vulnerabilities should be regularly identified and prioritized to identify those that are so serious they must be immediately addressed, those that can wait until the next maintenance shutdown or patching cycle, and those that can be accepted.

Managing Remediation

IT/OT convergence complicates remediation processes because vulnerabilities in the diverse asset types are typically managed by different asset owners. Questions such as, "Who is responsible to remediate vulnerabilities on this application?" and "Was the remediation that was scheduled for last month's maintenance shutdown completed as planned?" must be answered with facts, not informed guesses.

SOLUTION REQUIREMENTS

Inventory Assets

Manual inventories are expensive, often incomplete, and quickly out-of-date. Automated approaches are required, and different technologies are needed for different asset types. For example, passive monitoring is needed to avoid disrupting PLCs, RTUs, and other potentially sensitive devices. Agents may be required for laptops used by remote staff, and active scanners may be appropriate for IT devices and networks.

Additionally, the system should send an alert to a SIEM when it discovers new assets so staff can confirm that additions were authorized.

Map Asset Connections

Asset-to-asset communications must be cataloged so you can identify and investigate unexpected and/or unauthorized connections that an adversary could be exploit.

Continuously Manage Vulnerabilities

A vulnerability management solution must perform two functions well. First, it must continuously detect vulnerabilities in both OT and IT assets. It is very likely that the solution will discover many more vulnerabilities than you have resources to remediate. This leads to the second function.

The solution must also provide a mechanism to identify the most critical vulnerabilities. Effective prioritization requires insight about the vulnerability, including knowledge of its impact on availability, accessibility by attackers, and exploitability. This detailed vulnerability information helps plan remediation to be implemented during the next maintenance shutdown, if not before.

Automate the Remediation Workflow

An automated closed-loop process is required to effectively remediate vulnerabilities. The workflow must describe the vulnerability, document the steps needed to remediate it, assign remediation to the correct asset owner, and then confirm that remediation occurred as planned.

COPYRIGHT 2019 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.

SOLUTION OVERVIEW

Tenable OT and IT security solutions, in conjunction with technology alliance partners, enable safe discovery, thorough assessment, and efficient remediation of converged IT/OT systems, enabling customers to understand and reduce risk.

Industrial Security

Industrial Security™ provides an up-to-date inventory of systems and applications and their vulnerabilities to help organizations understand their OT cyber exposure and protect operational performance. Purpose-built for operational technology (OT) systems, the solution uses passive monitoring to provide safe and reliable insight – so you know what you have and what is vulnerable. Covering a wide range of ICS, SCADA and traditional IT systems, Industrial Security helps IT and OT security, plant operations, and compliance teams enhance security, improve asset protection and strengthen regulatory compliance.

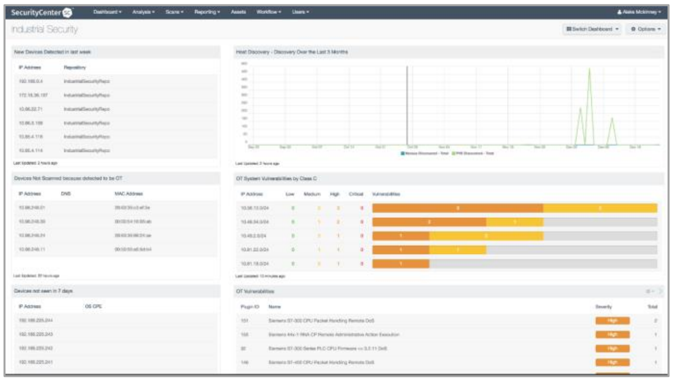
Features and Capabilities for Converged IT/OT Systems

- Support for thousands of OT systems from dozens of manufacturers, including Siemens, ABB, Emerson, GE, Honeywell, Rockwell/Allen-Bradley, and Schneider Electric
- Supported OT protocols include BACnet, CIP, DNP3/TCP, Ethernet/IP, ICCP, IEC 60870-5-104, IEEE C37.118, Modbus/TCP, OPC DA/SE/US, OpenSCADA, Profinet-DCP, Siemens S7/S7-plus and more
- Support for a wide range of IT assets, including servers, desktops, laptops, network devices, web apps, virtual machines, mobile, cloud, and containers

Tenable.sc Cyber Exposure Platform

Tenable.sc helps organizations manage risk in IT assets connected to OT networks in converged IT/OT systems. Tenable.sc includes active and agent-based sensors to discover and gather a wealth of security-related information about installed software, security configuration settings and known malware for full range of on-premises systems.

Tenable.sc can automatically import selected asset and vulnerability data from Industrial Security to help security leaders understand and defend the entire attack surface. Tenable.sc reports and interactive dashboards can easily be tailored to present near real-time status of both IT and OT assets supporting critical operational processes.


SecurityCenter
Dashboard
Analysis
Scans
Reporting
Assets
Workflow
Users
Industrial Security
Switch Dashboard
Options
New Devices Detected in last week
Host Discovery - Discovery Over the Last 3 Months
Devices Not Scanned because detected to be OT
OT System Vulnerabilities by Class C
Devices not seen in 7 days
OT Vulnerabilities

Tenable.sc dashboards deliver insight into the security of converged IT/OT environments

Technology Alliance Partners

Tenable.sc integrates with many partners in the Tenable Cyber Exposure Technology Ecosystem to enhance existing processes and investments. Examples include:

- Siemens professionals are available to deliver and deploy Industrial Security and to provide a range of industrial control systems design and vulnerability management services.
- ITSM solutions, such as ServiceNow Security Operations Vulnerability Response, to synchronize assets, incorporate asset criticality to enhance risk scoring, manage the remediation workflow and report status.
- SIEM solutions, such as Splunk Enterprise to enrich events with vulnerability information and centralize alerting and reporting.
- Privileged Access Management systems, such as CyberArk Application Identity Manager to provide deep vulnerability insight while protecting privileged accounts.

KEY BENEFITS

- ***Manage Converged Risk***
  Visibility of IT and OT assets, connections and vulnerabilities informs risk assessment
- ***Identify Weaknesses***
  Identify suspicious connections and vulnerabilities that require investigation
- ***Prioritize Remediation***
  Vulnerability prioritization based on factors such as asset accessibility, availability impact and exploitability efficiently focuses remediation on what matters most
- ***Measure Exposure over Time***
  Interactive dashboards chart progress over time and highlight possible trouble spots
- ***Leverage Existing IT and Security Technology***
  Integrations with installed enterprise IT and security solutions enhance existing processes and procedures

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 Tenable.io®, 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

COPYRIGHT 2019 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, LUMIN, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.