OT CSA

OT
Cyber Security
Alliance

OTCSA White Paper
October 2019

Vulnerability Management for Operational Technology

Table of content

Introduction

This white paper demonstrates how the Operational Technology Cyber Security Alliance (OTCSA) intends to deliver on its mission in the focus area "Visibility, Intelligence, and Response" as described in the OTCSA's *Introducing the Operational Technology Cyber Security Alliance* white paper (OTCSA, October 2019). It is a first version, and we welcome feedback from the community to improve its usability in future iterations.

With guidance from OTCSA asset owners and operators, we selected technical vulnerability management (VM) as defined in international standards and guideline documents as the topic for the first white paper in the OTCSA focus area "Visibility, Intelligence, and Response". Vulnerability management is the practice of monitoring the public domain and other accessible information sources for vulnerabilities and then evaluating exposure to identified vulnerabilities and taking appropriate mitigating measures to address any risks.

The objective of this document is two-fold:

1. To provide actionable guidance for performing technical VM in an OT environment. This can be achieved by providing workflow descriptions and technologies that can be used to support and automate the workflows to the greatest extent possible.
2. To serve as an example of an OTCSA Work Product (see the OTCSA's *Introducing the Operational Technology Cyber Security Alliance* white paper, OTCSA, October 2019) and provide the community with a better understanding of our mission and strategy for OT security.

SCOPE AND OBJECTIVE

Various international standards for security management systems mandate or recommend vulnerability management or assessment. The scope here is to map publicly known vulnerabilities to assets in an OT system (or a fleet of systems) and, based on risk assessment, identify and execute an appropriate response.

VM depends on creating an inventory of OT assets and gathering the sources of vulnerability information and remediation plans that can be instantiated to address identified vulnerabilities. VM activities include:

- Creating and maintaining an inventory of relevant OT assets.
- Identifying sources for vulnerability information and regularly obtaining updated disclosures.
- Mapping known vulnerabilities to assets—identifying which vulnerabilities affect products in an OT asset inventory.
- Analyzing the risk associated with vulnerabilities and identifying and executing mitigations to address them.

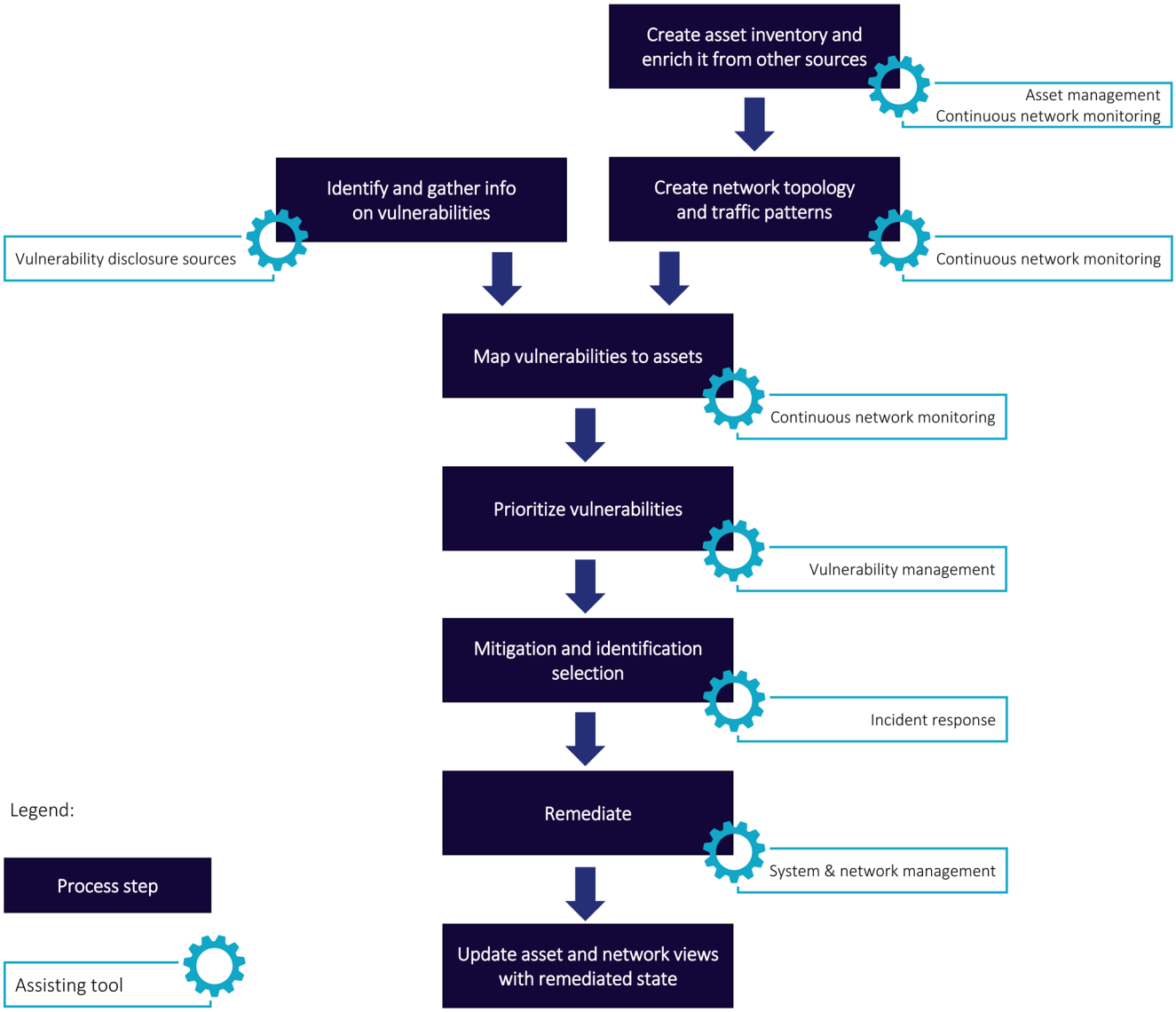

Figure 1: Technical vulnerability management activities

Asset inventories

You can't protect what you can't see. Keeping an accurate and up-to-date asset inventory is a vital first step in any comprehensive cyber security program. Unfortunately, a lack of visibility into Industrial Control System (ICS) assets is common across industries worldwide. A 2017 survey by the SANS Institute[1] found that 40 percent of ICS security practitioners "lack visibility or sufficient supporting intelligence into their ICS network." To make informed decisions on prioritizing spending and creating security plans to safeguard employees, business reputation, and the bottom line, an organization needs complete knowledge of its assets and vulnerabilities.

Asset inventory is defined as resources (hardware, software, documents, services, people, facilities, etc.) that are of value to an organization and need to be protected from potential risks. Organizations cannot rely on traditional IT systems or physical security to protect OT assets. As threats evolve, attacks on critical infrastructure and ICS have become increasingly sophisticated and occur more frequently.

[1] *Securing Industrial Control Systems—2017*, SANS Institute, July 2017

Performing manual inventories is costly and is constrained by various limitations:

- Time invested can be costly.
- Ignorance of components or facilities.
- Lack of permissions to access assets.
- Human error and incomplete data.

Also, teams may discover that, while various devices are connected to the network, the connections were never approved or documented in the first place.

There is a plethora of IT inventory tools, however, use of such tools in OT environments requires a clear understanding of their impact on control equipment. Such impacts are often due to the nature of the information or network traffic volumes. In other words, tools that are acceptable in IT systems may not be suitable for OT.

Several OT technology suppliers offer vendor-specific tools that are precise, but work only in limited sectors of an asset owner's network. Fortunately, a new generation of OT asset inventory tools that combine broad vendor compatibility, automation, and carefully designed OT-specific characteristics is now on the market. A solution that seamlessly manages an organization's IT *and* OT assets is optimal.

The following table lists the pros and cons of different inventory mechanisms currently available.

	Manual inventory	**IT asset management tools**	**OT vendor-specific tools**	**OT asset inventory tools**
Pros	• Flexible	• Reactive • Centralized • Quick detection of changes	• Purpose built • Very detailed • Quick detection of changes	• Purpose built • Detailed • Quick detection of changes • Extensive applicability
Cons	• Training time • Error prone • Labor cost • Slow updating	• Unspecific • Less information extracted • Can severely impact OT networks	• Limited applicability • Isolated data • Multiple formats • Terminology	• Integration into business processes

ASSET INVENTORY COMPOSITION

An OT asset inventory is comprised of:

Asset information

- Hardware components
  CPU, communication modules, I/O modules, etc.
- Software components
  Firmware, OS, SCADA or DCS software components.

Information should include detailed aspects of each asset

- System information
  Asset name, vendor, type (PLC, RTU, HMI, SCADA server, remote I/O), model, serial number, OS or firmware, domain or workgroup.
- Network information
  IP addresses, Mac address, domain, protocols used, open ports, gateway.

- Asset state information
  Running, stop, program, test, decommissioned.
- Contextual information
  Geographic, plant, and process location, CPE (Common Platform Enumeration), and other contextual aspects relevant for mapping vulnerabilities.

Network Topology

The asset inventory should also display the network topology to provide complete visibility of the OT environment, including:

- Communication relationships
  Industrial and/or IT protocols used, peer connections, role in the communication (client/server, master/slave).

Network topology for OT can be depicted based on the Purdue Model showcasing assets and their communications between Purdue Levels 0 and 3 (see the OTCSA's *Introducing the Operational Technology Cyber Security Alliance* white paper, OTCSA, October 2019, for information about the Purdue Model). To simplify exploration, the information should be made available as an intuitive, interactive network architecture map organized in Purdue Levels and network segments. In addition, it should be easy to manipulate the information in tabular or graphical formats through configurable dashboards and be exportable in office formats for simplified reporting and analysis.

CREATING AN ASSET INVENTORY

The process of creating an asset inventory can be largely automated. Precise, efficient, and secure, automation can substantially reduce incident management costs.

Asset information can be gathered using multiple technologies, including:

Passive sensors	• Sniffs OT network traffic via mirror ports or network taps. • Field-proven and 100 percent safe for OT networks.
Active probing	• Actively queries OT devices for asset information in the native industrial protocol language. • Rapidly discovers network communications and asset details down to the I/O level.
Configuration files	• Ingests and parses inventory files or OT equipment project or configuration files. • Requires access to well-maintained and up-to-date project files.
Hybrid approach	• Passive, active, and configuration file parsing for inventory creation.

Network Topology creation can be automated using the following technologies:

Passive traffic flow analysis	Analysis of traffic flows sniffed via passive sensors to map network topology.
NetFlow collector	Configuration of NetFlow/SFlow protocols to capture network traffic relayed by OT equipment and network devices.
Configuration files of network devices	Accessing industrial switch/router network configuration files and data tables to map network topology.

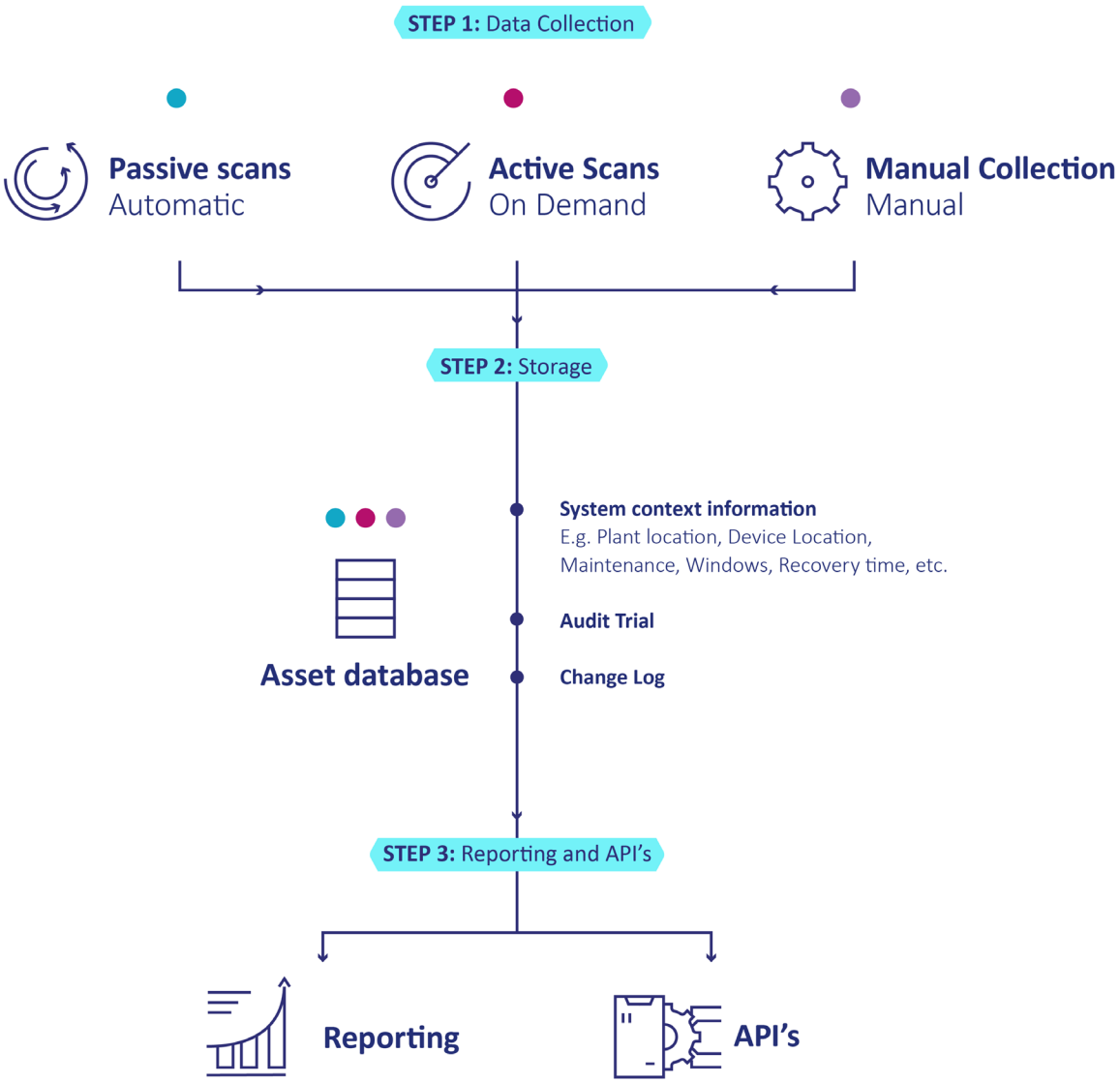

Figure 2: Asset inventory creation and maintenance

ENHANCING AN ASSET INVENTORY

Once an asset inventory is created, the following steps should be taken to enhance inventory data and give contextual information to each asset:

Bootstrap or add system details
In the event that certain configuration details cannot be automatically discovered, the system can be fed manually. For example, system details and configurations can be added through import files for devices connected via a serial point-to-point connection or fieldbus.

Collect and enter system context information
Provide a granular context framework to enable easy navigation through the asset inventory. Context helps users quickly find information and dependencies that may not be obvious. Such contextual information can include: plant and device location, maintenance windows, recovery time in case of device failure, asset owner details, redundancy systems associated with the asset, etc.

Create change and audit trails
All configuration changes should be logged automatically and made available for review in a timeline recorded for each OT device.

REPORTS AND DASHBOARDS

The inventory system should provide dashboards, analytics, and reporting tools that simplify compliance across key standards, including NERC-CIP, NIST, ISA99/IEC 62443, and FDA. The analytics should be configurable and provide access to the inventory in:

- Graphical form with point and click interface.
- Tabular form.
- Dashboards with configurable widgets.

Report data should be exportable in Microsoft Word and Excel formats with the self-generation of documents. The system needs to integrate with corporate authentication servers (e.g., federation services or corporate user directories) and allow for the mapping of user groups to roles and their related privileges in order to provide appropriate access levels to users (e.g., administrative vs. non-privileged users). For high-privileged access, multifactor authentication should be supported.

INTEGRATION WITH ENTERPRISE ECOSYSTEMS

Asset inventory information should be made available throughout the organizational ecosystem. By combining sensor-derived information from across the network with other data sources such as controls configuration and asset management, a comprehensive, visual, and interactive model can be constructed.

The information should be available through different channels and be easily integrated with common enterprise systems, such as SIEM solutions (including CEF, LEEF, and Splunk-specific formatting and apps). To allow programmatic access for system integration, a comprehensive API should be developed to enable established IT and OT vendors to use the information within their products. Access control mechanisms (e.g., API keys, tokens) and appropriate permissions must be enforced to control access to data accessed via APIs.

Gathering vulnerability information

As defined in ISO 27002, vulnerabilities are characterized as “a weakness of an asset or group of assets that can be exploited by one or more threats.” VM is the process of identifying, classifying, prioritizing, remediating, and mitigating such vulnerabilities. All International standards for security management systems (e.g., ISO 27001/2, IEC 62443) mandate or recommend vulnerability management or assessment.

The Security Content Automation Protocol (SCAP) was created for automating VM processes. SCAP identifies Common Vulnerabilities and Exposures (CVE) for publicly known cyber security vulnerabilities. Sourcing and mapping CVEs to asset inventory data is critical step in VM.

SOURCING VULNERABILITIES

Vulnerability information can be downloaded from various government and publicly available sources:

NIST CVE database	A US government repository of standards-based VM data
ICS-CERT (Cyber Emergency Readiness Team)	A database maintained by the US government's National Cybersecurity and Communications Integration Center
MITRE	A US non-profit that supports government agencies and hosts CVE, an international cyber security collaboration
Microsoft security bulletins	A library of security documents released by the Microsoft Security Response Center
SecurityFocus	Hosts BugTraq, full-disclosure mailing list of security vulnerabilities
Vendor-disclosed vulnerabilities	Data provided by OT vendors concerning disclosed vulnerabilities in their products

Additionally, there are multiple sources such as zerodayinitiative.com, vulners.com, securiteam.com, cxsecurity.com, and exploit-db.com that maintain updated databases of OT-related vulnerabilities.

Mapping vulnerabilities to assets

The generic publishers in the table above (NIST, ICS-CERT, and MITRE) make multiple formats available for downloading CVE information, including CSV, XML, JSON, text, and HTML. Data is updated frequently, often on an hourly basis, and should be synced regularly to an asset inventory.

Downloaded CVEs can be matched with inventoried assets using Common Platform Enumeration (CPE) product identifiers to check for vulnerabilities. CPE includes vendor names, versions, and other details to identify products. When creating an asset inventory, it's important to ensure that all CPEs are properly set.

It is the responsibility of VM process owners to update asset inventories with vulnerability disclosure information per OT device. Notification to process owners should be issued according to asset inventory creation and maintenance procedures.

Remediation and mitigation

PRIORITIZE VULNERABILITIES

The Common Vulnerability Scoring System (CVSS) produces a numerical score reflecting the severity of a vulnerability, which helps organizations assess and prioritize VM activities. An initial risk score can be associated with each asset based on a vulnerability's severity and the criticality of the asset (Critical, High, Medium or Low). This risk score and number of assets impacted should be considered when prioritizing mitigation.

ASSESS RISKS AND THEIR POTENTIAL IMPACTS

An asset inventory review should be performed to determine the severity and impact of any vulnerability. The CVSS score does not include asset-specific contextualization. However, CVSS provides an environmental score that allows the process owner to adjust the CVSS score based on context-specific requirements. The asset record should be updated as needed with contextualized vulnerability severity rankings.

PRIORITIZE ASSET REMEDIATION

Vulnerability management process owners should prioritize OT device remediation activities per the severity of impacts. Remediation plans should provide a clear timeline for each activity, and asset inventories need to be updated noting the specific risks to which an asset is exposed.

IDENTIFY MITIGATION STRATEGY

OT teams need to identify mitigation options for affected devices and evaluate each option for its potential impact on asset operations. Some mitigations impact asset availability. For example, updating firmware or software often requires restarting the asset. Most vulnerabilities require more than one security patch to mitigate. If a patch is available, it may not be vendor approved or it may be incompatible with other software.

Sometimes an obvious root-cause fix cannot be made due to the absence of a patch or lack of a suitable maintenance window. In such cases, alternative or temporary mitigating actions should be evaluated. A firewall should always be used as a segmentation layer between the IT and OT networks. Firewalls running IDS/IPS can detect and prevent exploits of known vulnerabilities and provide virtual patching when actual patching isn't possible.

IMPLEMENT MITIGATION

The VM process owner should implement mitigation according to service priority and share the mitigation status with the OT operation owner. Once mitigation is implemented, the asset inventory must reflect any changes made (e.g., if software was updated, the new version needs to be included in the inventory). If a vulnerability is fixed or mitigated (temporarily or permanently), the information must be updated, and if only partial mitigations are possible, as opposed to root cause fixes, that, too, should be documented.

Solutions

Products from several vendors are available to support the various VM processes as outlined in this white paper. Solutions from OTCSA members include: SCADAfence, Forescout SilentDefense, Qualys VM, and Microsoft Defender ATP.

Each security product has its own forte and capabilities for solving some pieces of the puzzle. However, as a whole, a single-product solution may not be suited to address all that's needed to create and maintain asset inventories, perform VM, and implement mitigation and remediation. An optimal solution may require a compilation of select point-products.

Challenges

Interoperability between various vendor products and the lack of common data models and interfaces can make the integration of a complete VM solution difficult. Most products adhere to the CVE format for reporting vulnerabilities. However, the mapping of vulnerabilities to inventories is largely driven by the internal workings of a product rather than by standard formats like Common Platform Enumeration (CPE). A large part of the mapping challenge is due to the lack of support and/or missing CPEs for software, OS, hardware, and applications.

Such gaps lead to limitations whereby additional vertical- and environment-specific sources of OT vulnerabilities cannot be easily integrated. A standardized information model enabling seamless data flows across different vendor products is desired. In addition, to seamlessly pass data across the entire vulnerability management process, and even across vendors, a standard set of interfaces needs to be defined for each stage: inventory, vulnerability mapping, and mitigation and remediation.

The OTCSA is committed to defining specifications for a common information model and standardized interfaces that OT security product vendors can adopt. Such flexibility will allow OT operators to choose the solutions most suitable to their needs and seamlessly integrate them with ease.

Conclusions and outlook

In this whitepaper, we have outlined an end-to-end workflow for technical VM for OT systems. The workflow spans from asset inventory creation and maintenance and continuous vulnerability tracking, to mitigation and implementation of a fix. As envisioned, the workflow is designed to be automated, but we acknowledge that some steps may require human interaction.

The OTCSA created the workflow to help organizations get started along the path of OT cyber security management and is intended to serve as a blueprint that can be adopted to an organization's specific context. Furthermore, organizations that already have a technical VM solution in place can compare their approach to what we have described here. This may generate improvement suggestions for their approach, and, of course, it may also generate feedback for improvement of ours. In the latter case, we encourage the submission of such feedback to the OTCSA.

LOOKING FORWARD

Full and consistent automation is not yet possible with tools available on the market today. While discrete stages can be automated, we are not aware of a single tool or tool chain that supports or automates the entire VM workflow. The main challenges are the lack of a consistent information model and the lack of a unified interface to bridge the gap between various tools. Accordingly, the OTCSA has prioritized for its future work the establishment of information models and APIs or interfaces that will enable seamless automation across the entire workflow.

Besides addressing VM, we have identified other relevant areas for further investigation, which fall broadly under the theme of "Visibility, Intelligence, and Response." Included here are threat management workflows that will, through integration of threat intelligence within asset inventories, be able to identify when an OT system is exposed to specific threats. Appropriate countermeasures and follow-up on implementation will also be covered. The integration of threat intelligence and improved real-time monitoring should enable threat hunting—that is, proactively analyzing OT systems for indicators of potential compromise. Further work on improving visibility into OT systems will have to address the changes we currently see gaining traction—specifically the adoption of encrypted

protocols for which passive network analysis will require redesign. Finally, we also see a greater need for research on threats to OT systems and for more consistent and responsible disclosure of vulnerabilities that threaten them.

About the Operational Technology Cyber Security Alliance (OTCSA)

The Operational Technology Cyber Security Alliance (OTCSA) is a group of global industry-leading organizations focused on providing operational technology (OT) operators with resources and guidance to mitigate their cyber risk in an evolving world. Founded in 2019, OTCSA is the first group of its kind to architect a technical and organizational framework–the who, what, and how–for safe and secure OT. Membership is open to all OT operators and IT/OT solution providers. Current members include ABB, BlackBerry Cylance, Check Point Software Technologies, Forescout Technologies, Fortinet, Microsoft, Mocana, NCC Group, Qualys, SCADAfence, Splunk Technology, and Wärtsilä.

To learn more about the OTCSA or becoming a member, visit https://otcsalliance.org.

Acknowledgements

The following people served as active members of the OTCSA Working Group 2 in the preparation of this document:

Name	Affiliation
Michelle Balderson	Fortinet
Luca Barba	Forescout Technologies
Mati Epstein	Check Point Software Technologies
Dharmesh Ghelani	Qualys
Daniel Krieger	Microsoft
Jim McKinney	NCC Group
Ragnar Schierholz	ABB
Ofer Shaked	SCADAfence
Damon Small	NCC Group
Tom Thirer	SCADAfence
Davide Zanetti	ABB

Use of information