tenable.ot
Powered by Indegy

Guidance - CISA /NSA Alert AA20-205A for OT Systems

On the heels of MITRE updating their framework for Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) to include ICS and OT Systems, yesterday the NSA and CISA issued AA20-205A recommending immediate actions to reduce exposure across operational technologies and control systems.

The agency advised that there has been an increase in activity by cyber actors targeting critical infrastructures by exploiting OT assets. OT assets play a key role in the operating of these systems, and the alert noted they also play a key role with the Department of Defense (DoD), Defense Industrial Base (DIB) and National Security Systems (NSS).

The alert goes on to recommend specific mitigation techniques. In the left column are their recommendations[1] and on the right side are details on how Tenable.ot can help you comply with these directives.

CISA Alert AA20-205A	Tenable
HAVE A RESILIENCE PLAN FOR OT	
I. Immediately disconnect systems from the Internet that do not need internet connectivity for safe and reliable operations. Ensure that compensating controls are in place where connectivity cannot be removed.	I. Tenable concurs that OT systems should not be directly accessible from the internet, and that appropriate Defense in Depth measures are in place. Tenable.ot supports a fully air gapped system and further works with unidirectional and diode based firewall vendors to ensure that where desired, air gapping is maintained. Where airgapping is not possible or desired, Tenable.ot is fully integrated within Tenable.sc for full cyber threat visibility across converged IT and OT infrastructures. Additionally there are compensating controls and integration with leading IT based security products such as NGFWs, and SIEM to ensure a complete view across IT and OT.
II. Plan for continued manual process operations should the ICS become unavailable or need to be deactivated due to hostile takeover.	II. The configuration and change control functionality within Tenable.ot can provide an "out of band" record of changes that have been made in the control logic within the OT environment, which can be extremely valuable when attempting to operate with the control system in a degraded or offline mode.
III. Remove additional functionality that could induce risk and attack surface area.	III. Tenable.ot can identify open ports that are not being used, risky protocols and functionality that is either risky or is not being used that can then be deactivated by the user.
IV. Identify system and operational dependencies.	IV. Tenable.ot creates a system wide map with all locations that shows "conversations" and the frequency between devices.
V. Restore OT devices and services in a timely manner. Assign roles and responsibilities for OT network and device restoration.	V. Snapshotting capabilities enable a full audit trail of changes as well as the ability to identify and provide the ability for an administrator to trace back to "last known good state".

1. Note: The copy provided are excerpts from the full CISA alert. You are encouraged to read the source document from which this paper was developed. It is linked above.

CISA Alert AA20-205A	Tenable
VI. Backup "gold copy" resources, such as firmware, software, ladder logic, service contracts, product licenses, product keys, and configuration information. Verify that all "gold copy" resources are stored off-network and store at least one copy in a locked tamperproof environment (e.g., locked safe).	VI. Patented active querying provides a full mapping of all OT assets and further provides deep situational analysis inclusive and not limited to firmware version, ladder logic, patch level etc. Configuration change control capabilities store a snapshot of the devices running control logic.
VII. Test and validate data backups and processes in the event of data loss due to malicious cyber activity.	VII. Although not a 'backup or firmware image' per se - the Tenable.ot product is a system of record for the details of each asset, and can be used as the authoritative source users could use to cross check that they have on hand every version of firmware that is identified and required for the restoration of their devices.

CISA Alert AA20-205A	Tenable
HARDEN YOUR NETWORK	
I. Remote connectivity to OT networks and devices provides a known path that can be exploited by cyber actors. External exposure should be reduced as much as possible.	I. Tenable.ot hardens your network by providing the following functionality a. Visibility across IT and OT b. Asset inventory with full situational awareness down to the ladder logic c. Threat detection & mitigation d. Risk based vulnerability management e. Configuration control of industrial controllers. Tenable.ot identifies all connections both locally and remotely. Powerful tools allow for white listing, black listing and grey listing to identify questionable and/or unauthorized connections.
II. Remove access from networks, such as non-U.S. IP addresses, if applicable, that do not have legitimate business reasons to communicate with the system.	II. Tenable.ot can identify specific IP addresses and address ranges for inclusion/exclusion in the OT network.
III. Use publicly available tools, such as Shodan, to discover internet-accessible OT devices. Take corrective actions to eliminate or mitigate internet-accessible connections immediately. Best practices include: - Fully patch all Internet-accessible systems. - Segment networks to protect PLCs and workstations from direct exposure to the internet. Implement secure network architectures utilizing demilitarized zones (DMZs), firewalls, jump servers, and/or one-way communication diodes. - Ensure all communications to remote devices use a virtual private network (VPN) with strong encryption further secured with multifactor authentication. - Check and validate the legitimate business need for such access.	III. Tenable agrees with and endorses the best practices summarized here. It is critical to not only check internet accessibility, but to understand what weaknesses or vulnerabilities exist in outward facing systems. Tenable.ot can make you aware of the asset, and how it may be exposed (ports, services, banners). We recommend deploying OT specific security products that provide the key functionality and features to address these recommended best practices.

CISA Alert AA20-205A	Tenable
- Connect remote PLCs and workstations to network intrusion detection systems where feasible. - Capture and review access logs from these systems. - Encrypt network traffic preferably using NIAP-validated VPN products and/or CNSSP- or NIST-approved algorithms when supported by OT system components to prevent sniffing and man-in-the-middle tactics. Available at: niap-ccevs.org	
IV. Use the validated inventory to investigate which OT devices are internet-accessible.	IV. Tenable.ot provides full asset inventory with deep situational analysis. The solution can identify open ports and protocols while also mapping conversations to identify any assets that are accessible from or communicating to external networks.
V. Use the validated inventory to identify OT devices that connect to business, telecommunications, or wireless networks.	V. As noted in the previous point, capabilities also include the ability to map conversations both internally and externally as well as identify open ports and protocols that may allow communication(s) via wireless, telecommunications, etc.
VI. Secure all required and approved remote access and user accounts. - Prohibit the use of default passwords on all devices, including controllers and OT equipment. - Remove, disable, or rename any default system accounts wherever possible, especially those with elevated privileges or remote access. - Enforce a strong password security policy (e.g., length, complexity). - Require users to change passwords periodically, when possible. - Enforce or plan to implement two-factor authentication for all remote connections.	VI. Tenable.ot enables the end user to monitor compliance with access control best practices outlined in this section.
VII. Harden or disable unnecessary features and services (e.g., discovery services, remote management services, remote desktop services, simulation, training, etc.).	VII. As noted previously, Tenable.ot offers full functionality with granular controls in this requirement.

CISA Alert AA20-205A	Tenable
CREATE AN ACCURATE "AS-OPERATED" OT NETWORK MAP IMMEDIATELY An accurate and detailed OT infrastructure map provides the foundation for sustainable cyber-risk reduction.	
• **Document and validate an accurate "as-operated" OT network map.** - Use vendor-provided tools and procedures to identify OT assets. - Use publicly available tools, such as Wireshark,[9] NetworkMiner,[10] GRASSMARLIN,[11] and/or other passive network mapping tools. - Physically walk down to check and verify the OT infrastructure map. • **Create an asset inventory.** - Include OT devices assigned an IP address. - Include software and firmware versions. - Include process logic and OT programs. - Include removable media. - Include standby and spare equipment. • **Identify all communication protocols used across the OT networks.** - Use vendor-provided tools and procedures to identify OT communications. - Use publicly available tools, such as Wireshark,[9] NetworkMiner,[10] GRASSMARLIN,[11] and/or other passive network mapping tools. • **Investigate all unauthorized OT communications.** • **Catalog all external connections to and from the OT networks.** - Include all business, vendor, and other remote access connections. - Review service contracts to identify all remote connections used for third-party services	• Tenable.ot has full functionality to map a full OT environment including multiple and distributed locations. • With "single pane of glass" functionality, it is possible to see all OT assets as well as IT assets in an OT environment. • Each asset has real time health and alarm information with the capabilities to drill down to extremely detailed information inclusive of and not limited to PCAP information at specific backplanes based on the alarm. • As noted earlier, conversations between devices are represented on the GUI to identify frequency of the conversations, dormant devices and illegal conversations. Deep tracking of network data can alarm based on policy, anomaly and crowd sourced information by leveraging the Suricata DB which is maintained by the OISF community. Additionally, Tenable operates a world renown research team of over 100 personnel dedicated to finding new threats and vulnerabilities and thus stopping them before damage is done. • At the device level, patented active querying can provide deep situational analysis including patch levels, firmware versions, users logged in, state and much more. This is performed in the native logic to the controller and does not require "scanning" as this can destabilize an OT system.

CISA Alert AA20-205A	Tenable
UNDERSTAND AND EVALUATE CYBER-RISK ON "AS-OPERATED" OT ASSETS	
I. Informed risk awareness can be developed using a variety of readily available resources, many of which include specific guidance and mitigations.	I. Tenable's research team mentioned in the previous section regularly issues alerts and advisories based on primary analysis as well as third parties such as CVSS, etc.
II. Use the validated asset inventory to investigate and determine specific risk(s) associated with existing OT devices and OT system software. a. Vendor-specific cybersecurity and technical advisories. b. CISA Advisories [12]. c. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency Cyber Security Evaluation Tool [13]. d. MITRE Common Vulnerabilities and Exposures (CVE) for both Information Technology and OT devices and system software [14]. Available at cve.mitre.org. e. National Institute of Standards and Technology – National Vulnerability Database [15]. Available at nvd.nist.gov.	II. Based on the deep asset inventory, Tenable can quickly alert you to new vulnerabilities, exploits and targeting based specifically on the devices in a network as well as the patch level, firmware, ladder logic etc. Because of this deep intelligence, the alerts are specific to the asset.
III. Implement mitigations for each relevant known vulnerability, whenever possible (e.g., apply software patches, enable recommended security controls, etc.).	III. Tenable leverages a risk-based approach to vulnerabilities and provides a score based on the asset criticality as well as the type of vulnerability. Tenable's VPR score (Vulnerability Priority Rating) triages the vulnerabilities and empowers the end-user to address high priorities that are unique to his/her situation first thus mitigating key security threats before they become an incident.
IV. Audit and identify all OT network services (e.g., system discovery, alerts, reports, timings, synchronization, command, and control) that are being used. a. Use vendor provided programming and/or diagnostic tools and procedures	IV. Full audit trail of all activity is available both for security and compliance requirements. Standard reports are included and customized reporting is available.

CISA Alert AA20-205A	Tenable
IMPLEMENT A CONTINUOUS AND VIGILANT SYSTEM MONITORING PROGRAM	
I. A vigilant monitoring program enables system anomaly detection, including many malicious cyber tactics like "living off the land" techniques within OT systems.	I. Deep tracking of network data can alarm based on policy, anomaly and crowd sourced information by leveraging the Suricata DB which is maintained by the OISF community.
II. Log and review all authorized external access connections for misuse or unusual activity.	II. Tenable.ot provides drill down information on every asset and every connection down to PCAP and backplane information. Standardized and custom reporting is also available for historical and audit purposes.
III. Monitor for unauthorized controller change attempts. a. Implement integrity checks of controller process logic against a known good baseline. b. Where possible, ensure process controllers are prevented from remaining in remote program mode while in operation. c. Lock or limit set points in control processes to reduce the consequences of unauthorized controller access.	III. Configuration control monitors and snapshots any changes made to industrial controllers. This can be set to snapshot based on a change made, time based or user invoked. Limits can be set by user, permissions and/or type of process.

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.