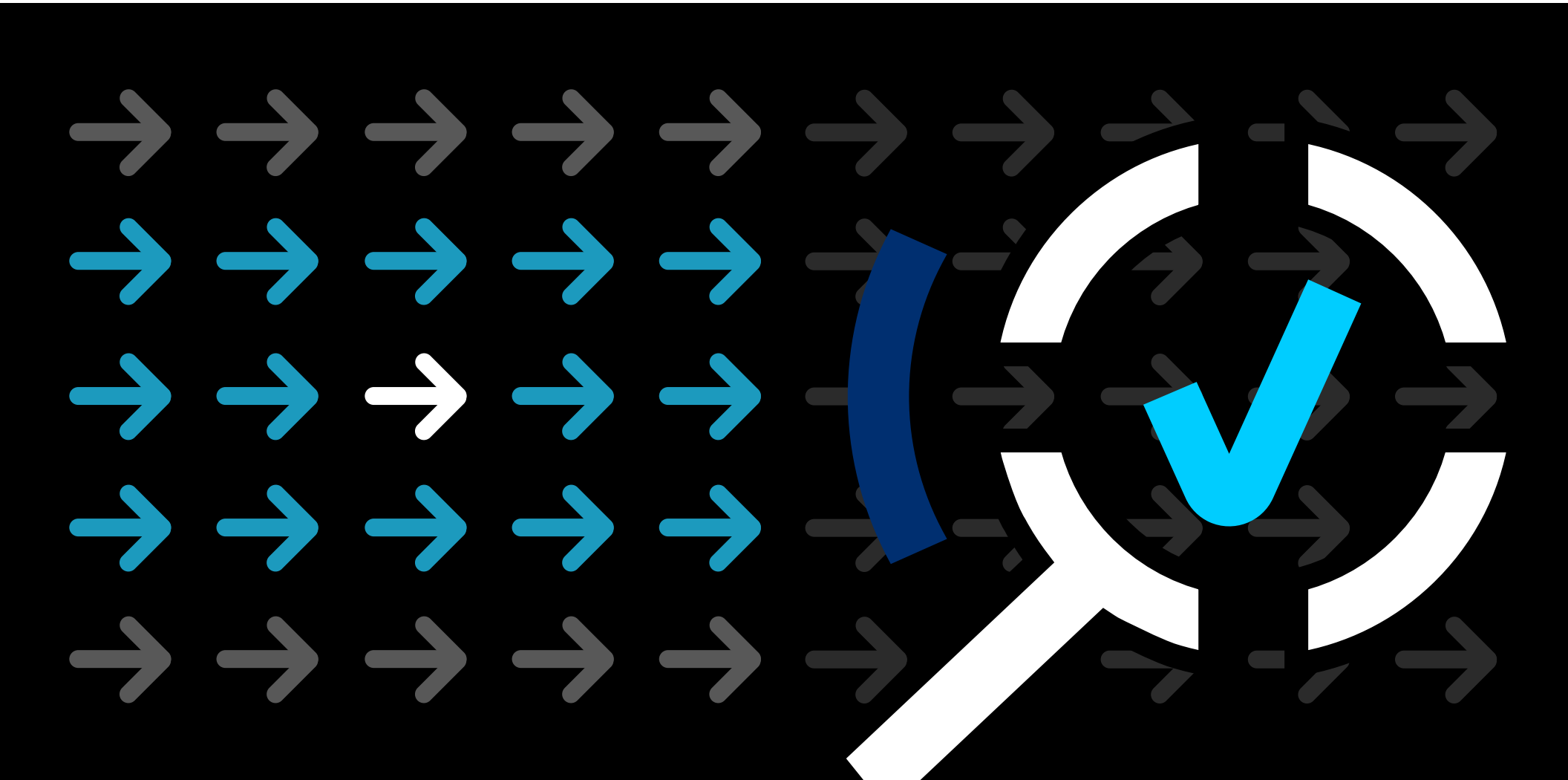
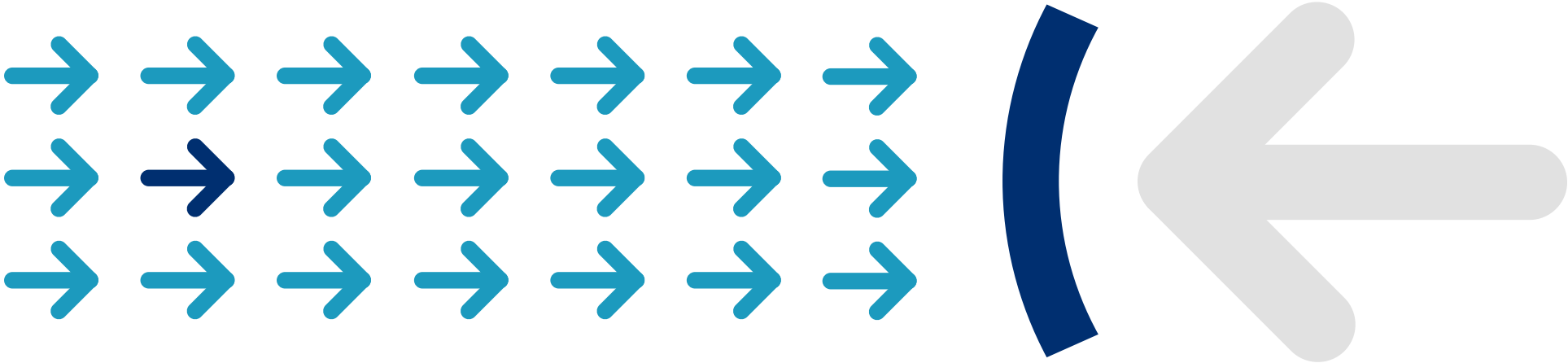
FORESCOUT
Active Defense for the Enterprise of Things.

Reduce Exposure Across Operational Technologies and Control Systems and comply with **CISA Alert (AA20-205A)**



As attacks on civilian infrastructure continue to make news headlines[1] the NSA and CISA recently issued AA20-205A[2], which recommends immediate actions to reduce exposure across operational technologies and control systems. This alert is based on the MITRE framework for Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)[3].

The Forescout platform's latest innovations enable IT-OT convergence and deliver non-disruptive segmentation for sensitive OT environments. Forescout eyeInspect (formerly SilentDefense™) protects OT and ICS networks from a wide range of threats, provides both passive and active discovery capabilities that create an automatic, real-time asset inventory and enables targeted remediation actions based on potential business impact. Read below for details on how we protect systems and apply the guidelines from Alert AA20-205A.



CISA Alert AA20-205A	Forescout
HAVE A RESILIENCE PLAN FOR OT	
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.	Forescout has a number of capabilities that identify devices communicating internally as well as externally to the internet. These capabilities include communications mapping, deep packet inspection, baselining and threat analytics. Forescout can identify known good communications while also identifying malicious or unusual behavior. Forescout's rich control and orchestration offerings provide the ability to automatically respond to any red flags raised by the capabilities above. This includes integrations with switches, NGFWs, SIEMs, ITSM, endpoints, etc.
Plan for continued manual process operations should the ICS become unavailable or need to be deactivated due to hostile takeover.	Forescout's OT offering is designed to run in an air-gapped environment. Updates, patching, licensing, etc., can all be done out of band. Forescout will continue to monitor all operations on the air-gapped network and keeps PCAP copies of all security and operational events that occur on the network for forensic investigations. The product will also keep a running log of all changes made to hosts on the network.
Remove additional functionality that could induce risk and attack surface area.	Forescout starts by inventorying the network for all connected devices. Devices that don't belong are quickly identified and classified, and network context as to where they are physically located can be provided. There is a wide variety of use cases that can be achieved to identify non-essential devices, communications, processes, etc.

CISA Alert AA20-205A	Forescout
Identify system and operational dependencies.	Forescout's mapping and baselining capabilities create a communication profile of what "known good" looks like on the network. Operational dependencies can be identified and deviations from the baseline can create actionable outcomes. In addition, Forescout has an extensive OT Industrial Threat Library that is capable of identifying abnormalities in OT communications right out of the box. This can be done on day one with zero baselining or knowledge of the network.
Restore OT devices and services in a timely manner. Assign roles and responsibilities for the OT network and device restoration.	N/A
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, tamper-proof environment (e.g., locked safe).	N/A
Test and validate data backups and processes in the event of data loss due to malicious cyber activity.	N/A

CISA Alert AA20-205A	Forescout
HARDEN YOUR NETWORK	
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.	As mentioned above, Forescout can identify and remediate internet communications. In addition, Forescout's offering is well-suited for identifying remote communications through communication mapping, deep packet inspection, baselining and threat analytics. Forescout can identify "known good" communications while also identifying malicious or unusual behavior. Forescout's rich control and orchestration offerings provide the ability to automatically respond to any red flags raised by the capabilities above. This includes integrations with switches, NGFWs, SIEMs, ITSM, endpoints, etc.
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.	Forescout can identify communications with risky or non-legitimate networks and automatically block those communications. The most common approach would be to whitelist legitimate networks.
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.	Forescout agrees with these best practices. While publicly available tools can be used to identify internet-facing devices or potentially vulnerable assets, Forescout's communication baselining and deep packet inspection provides a much clearer picture of devices that are exposed to the internet or communicating with the internet. Forescout is able to use its knowledge of device communications to simulate network segmentation. These simulations can identify potential challenges prior to actually segmenting devices. Once the simulated segmentation outcomes are deemed acceptable, Forescout has automated integrations with the network that can instantiate segmentation through VLANs, ACLs, NGFW rules, etc.

CISA Alert AA20-205A	Forescout
• 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. • 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	As mentioned previously, Forescout offers a wide variety of capabilities in its arsenal. The data collected helps support business operations mentioned in these best practices.
Use the validated inventory to investigate which OT devices are internet-accessible.	Forescout employs many techniques to identify devices at the time they connect. The platform integrates with the network via SNMP, CLI and a mirror or tap. This offers the ability to actively query for connected devices, receive traps when devices connect or see communications of devices on the network. This allows Forescout to passively identify devices on the network without directly querying them. This approach also allows Forescout to actively identify devices without relying on a scanning interval. The combination of integrations allows Forescout to provide a full inventory of connected assets. This information can also be shared automatically with third-party asset inventory products.

CISA Alert AA20-205A	Forescout
Use the validated inventory to identify OT devices that connect to business, telecommunications, or wireless networks.	As noted previously, Forescout employs many techniques for identiying devices and all device communications. This includes viewing device communications by OT roles. This allows an operator to clearly see which devices should or shouldn't be communicating across network boundaries.
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.	The Forescout platform has the ability to identify cleartext passwords being used over insecure protocols across the wire. Forescout has a database of known default passwords used by IT and OT vendors that can be flagged if they are seen on the wire. This could indicate a scenario where a device wasn't properly configured, or it could indicate an attacker trying to access a device with default credentials. Customers can also update a database of outdated credentials that shouldn't be used on devices. If those credentials are identified on the wire, an alert can be triggered. Forescout also has the ability to inspect Windows, Mac, and Linux operating systems to check for all sorts of compliance attributes. This can include system user accounts.
Harden or disable unnecessary features and services (e.g., discovery services, remote management services, remote desktop services, simulation, training, etc.).	Forescout is able to check for all sorts of compliance requirements on Windows-, Mac-, and Linux-based systems. This includes inventorying services, processes, agents, applications, users, etc. Proactive compliance policies can be created to identify devices the moment they deviate from an acceptable state.

CISA Alert AA20-205A

Forescout

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, NetworkMiner, GRASSMARLIN, 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.

- The Forescout solution is capable of creating a network map of all devices and their respective communications. Furthermore, Forescout removes the challenge of physically verifying devices and their locations. Forescout's integrations with network infrastructure provide physical device locations.
- Forescout provides one of the most robust asset inventories available. This can include information such as MAC address, IP address, device classification, OS, OT role, CVEs, ports/protocols in use, modules, firmware, software, processes, applications, removable media, registry values, files, switch IP, switch port, switch VLAN, switch port configuration, logged-in user, etc.
- Forescout can identify all communications in use while providing detailed attributes about said communications.
- Forescout eyeInspect comes with one of the industry's most robust Industrial Threat Libraries for identifying OT-related incidents. Threat Library entries include both malicious events and misconfigured or malfunctioning device events. Further investigation is simple with the trimmed PCAPs offered by the product for each incident.
- External communications can easily be viewed and alerted on for further validation by the business.

CISA Alert AA20-205A

- **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, NetworkMiner, GRASSMARLIN, 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

Forescout

UNDERSTAND AND EVALUATE CYBER-RISK ON "AS- OPERATED" OT ASSETS

Informed risk awareness can be developed using a variety of readily available resources, many of which include specific guidance and mitigations.

Forescout has internal teams that comb many third-party risk repositories to create risk profiles for all OT assets on the network in a single view. These profiles include links to all third-party information used as well as recommended risk mitigation techniques.

CISA Alert AA20-205A	Forescout
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. c. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency Cyber Security Evaluation Tool. d. MITRE Common Vulnerabilities and Exposures (CVE) for both Information Technology and OT devices and system software. Available at cve.mitre.org. e. National Institute of Standards and Technology– National Vulnerability Database. Available at nvd.nist.gov.	As mentioned above, Forescout has internal teams that comb many third-party risk repositories, including those mentioned in this section. These repositories are used to create concatenated risk profiles for all OT assets in a single view. These profiles include links to all third-party information used as well as recommended risk mitigation techniques.
Implement mitigations for each relevant known vulnerability, whenever possible (e.g., apply software patches, enable recommended security controls, etc.).	Forescout's integrations with devices and networks allow organizations to implement all sorts of mitigating controls. For anything that can't be done on the device or the network, Forescout can share information through integrations with third-party systems to trigger mitigations from other vendors.

CISA Alert AA20-205A	Forescout
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.	Forescout keeps a full audit trail of all activities both on the network and in the product.
IMPLEMENT A CONTINUOUS AND VIGILANT SYSTEM MONITORING PROGRAM	
A vigilant monitoring program enables system anomaly detection, including many malicious cyber tactics like "living off the land" techniques within OT systems.	Forescout's Industrial Threat Library, LAN Communication Profiler and security modules allow eyeInspect to detect all sorts of malicious events, security anomalies and operational anomalies. These can range from network reconnaissance, to malware propagation, to command and control traffic, or simply misconfigured OT assets.
Log and review all authorized external access connections for misuse or unusual activity.	Forescout has the ability to monitor all communications, keep a network and host change log, monitor for any anomalies, and keep trimmed alert PCAPs or full PCAPs of the events.
Monitor for unauthorized controller change attempts. a. Implement integrity checks of controller process logic against a known good baseline.	Forescout is capable of identifying all sorts of host changes. This includes patches, software/firmware changes, added/removed modules, new ports being used, etc. The product can also monitor the state or mode of PLCs and PLC modules.

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.

*Footnotes:

1. Israeli attempted cyberattack on water systems: https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/
2. NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems. https://us-cert.cisa.gov/ncas/alerts/aa20-205a
3. MITRE Attack Framework: https://attack.mitre.org/matrices/enterprise/

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

www.forescout.com/solutions/compliance/ salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com