



Mapping Ordr Capabilities To CISA Mitigation Guide: Healthcare and Public Health (HPH) Sector

On November 20, 2023, the Cybersecurity Infrastructure and Security Agency (CISA) issued guidance for healthcare delivery organizations (HDOs) struggling to secure their data and systems against a growing and pernicious onslaught of attacks from threat actors across the globe. The purpose of CISA’s Mitigation Guide: Healthcare and Public Health (HPH) Sector is to articulate “best practices to combat pervasive cyber threats affecting the Healthcare and Public Health (HPH) Sector.”

The Mitigation Guide follows CISA’s Cyber Risk Summary: Healthcare and Public Health (HPH) Sector Calendar Year 2022 in which the agency identified six common weaknesses in healthcare cybersecurity, including:



Web application vulnerabilities



Encryption weaknesses



Unsupported software



Unsupported Windows operating systems (OS)



Known exploited vulnerabilities (KEVs)



Vulnerable services

To help HDOs and other enterprises in the healthcare sector address these weaknesses, and create and execute more effective cybersecurity strategies, CISA identifies three key mitigation areas for improving security, with several focus areas.

Ordr's whitepaper recommends requirements for organizations to consider as they evaluate each of these focus areas, and also shares Ordr capabilities and benefits.

Mitigation Strategy #1: Asset Inventory and Security



CISA Recommendations

Focus area 1: Asset inventory

CISA emphasizes the importance of knowing your assets and discusses discovery approaches using active scans, passive processes, or both.



Ordr Capabilities

While CISA recommends utilizing active scans, passive processes, or both to discover assets, Ordr recommends organizations start with a passive approach in order to not impact operations of sensitive medical devices, IoT and OT.

Ordr provides a “whole hospital” view of all connected assets – from traditional devices such as servers, workstations, and PCs as well as unmanaged assets such as IoT, IoMT, and OT devices.

Each asset is automatically identified and accurately classified with detailed information such as make, model, serial number, operating system, installed software, network details, and business/IT owners. This data can be viewed within the Ordr dashboard, exported as a report, or sent via API to an inventory tool such as a CMMS or CMDB as well as other IT tools.



Ordr Benefits

- Automate inventory on all assets in the network including IT, IoMT and OT for a single source of truth
- Repurpose resources working on manual inventory task to higher value responsibilities.
- Improve efficiencies by continuously update CMDBB in real-time for improved efficiencies
- Enhance security by triggering workflows when new devices are discovered on the network or missing from the network

Mitigation Strategy #1: Asset Inventory and Security



CISA Recommendations

Focus area 2: Securing Your Assets

CISA recommends that healthcare organizations segment their networks, separating IT from OT in different segments. CISA recommends limiting which assets can access the internet from an internal network, and which assets should be siloed into their own compartment

Recommended mitigations in this category include:

- Port and service exposure | Observe the Principle of Least Privilege when it comes to network access.
- Network and Security Monitoring | Update IDS signature sets regularly.
- Database Security | Sanitize your database inputs and revoke the “execute” function on generous SQL server functions.



Ordr Capabilities

Segmentation:

- Ordr simplifies segmentation by dynamically generating policies based on asset attributes – for example, “segment infusion pumps running Windows 7”, or based on governance such as “segment medical devices from any communications to the Internet”
- Ordr simplifies Zero Trust or micro segmentation by dynamically generating policies to only allow “baseline communications” for least privilege access
- Ordr-created policies are enforced through integrations with security and/or networking products such as firewalls, switches and NAC that exist in the environment.
- Ordr can share asset context, and automate the creation of policies to accelerate network access control (NAC) segmentation initiatives
- Ordr segmentation policies can be optimized based on enforcement points



Ordr Benefits

- Reduce errors when dynamically generating segmentation policies
- Enhance security by delivering least-privilege access via Zero Trust segmentation
- Optimize performance by customizing segmentation policies based on the type of enforcement point and asset profile
- Accelerate identification of issues via visualization of traffic analysis – between VLANs/subnets and to the Internet

Mitigation Strategy #1: Asset Inventory and Security



CISA Recommendations



Ordr Capabilities



Ordr Benefits

Port and Service Exposure:

The Ordr dashboard delivers immediate context about assets that use vulnerable and exploitable protocols and ports.

Once identified, security teams can mitigate risks by monitoring and segmenting these assets.

- Understand and mitigate risks from potentially vulnerable and exploitable assets
- Enhance security by monitoring assets and users using high privilege protocols

Network and Security Monitoring:

Ordr provides multiple capabilities to help teams detect, manage, and report potential security incidents. The solution utilizes an integrated intrusion detection system (IDS) to identify known attack traffic. Signature updates are automated, and can be configured based on security team preference.

The solution also creates a baseline of normal behavior for each device and uses machine learning (ML) to detect potentially malicious deviations that may indicate compromise or an attack, including zero-day activity. This is real-time and requires no updates.

- Identify and prioritize issues from assets with exploits, active threats and anomalies, via customizable risk scores and threat intelligence
- Accelerate risk mitigation efforts for compromised assets via automated security policies

Mitigation Strategy #2: Identity Management and Device Security



CISA Recommendations



Ordr Capabilities



Ordr Benefits

Focus Area 1: Email security and phishing

Ordr is not an email security/anti-phishing tool, however, the solution does detect malware activity by identifying communications with known C2 servers or other malicious destinations. Ordr also creates a baseline of normal activity for each device and detects deviations from that baseline to identify malicious activity for zero-day threats that do not have a defined indicator of compromise (IoC).

Ordr enables teams to block malicious communications and/or isolate impacted devices to stop the spread of threats. This is done with automated actions and dynamically created policy enforced with existing security and network products.

Enhance security by blocking asset communications to known malware and phishing sites.

Focus Area 2: Access Management

CISA recommends that healthcare organizations segment their networks, separating IT from OT in different segments. CISA recommends limiting which assets can access the internet from an internal network, and which assets should be siloed into their own compartment

Ordr provides very robust tracking of users using AD/RADIUS and wireless integration, enabling security teams to monitor which user is accessing what assets at what time.

Ordr provides two key perspective:

Enhance security by tracking and monitoring details about assets and users, such as which assets each user has access to, and which user was logged into an asset, the duration and timeframe.

Mitigation Strategy #2: Identity Management and Device Security



CISA Recommendations



Ordr Capabilities



Ordr Benefits

- User tracking – analysis of all connected assets accessed by a user.
- Asset tracking – analysis of which users were logged into a specific assets, at what time, duration and more

Ordr also monitors all assets that use supervisory protocols like SSH, telnet, ftp, etc., associates them with user names, correlates them with the network they logged in from (corporate or guest), and maintains an accurate access record for each and every device as well as each and every user.

We also track and monitor corporate and guest network users. Corporate resources need to be accessed by corporate users with the right credentials from the corporate network. Ordr can alert or trigger the appropriate incident response workflow when a guest network user crosses over to the corporate network.

Finally, organizations can take advantage of all this rich user authentication during a security incident to provide qualifying details such as which network was the entry point, which device the “user” used to get into the network and what authentication methods they used, in addition to detailed Ordr Flow Genome flows.

Mitigation Strategy #2: Identity Management and Device Security



CISA Recommendations



Ordr Capabilities



Ordr Benefits

Focus area 3: Password Policies

CISA pushes the Healthcare sector to observe a minimum 15-character length and switch out default passwords.

Ordr can identify assets with default or weak passwords. Assets with default or weak passwords are highlighted in the Ordr dashboard as well as reports that can be viewed or exported

Improve security by identifying assets with default and weak passwords.

Focus Area 4: Data Protection and Loss Prevention

CISA recommends:

- Sensitive data be secured in safe places, and accessed only by authenticated and authorized users
- Maintain strong encryption protocols and algorithms such as transport layer security (TLS)

Ordr provides granular details such as make, model, serial number, operating system, and software version for every asset. The solution also identifies if devices transmit and/or hold encrypted or unencrypted PHI or other sensitive data.

Ordr can also identify via Ordr Software Inventory Collector granular details about every asset, including applications deployed, patching levels, and whether disk encryption is enabled.

Enhance security by tracking and monitoring assets that have PHI, PII and disk encryption.

Focus area 5: Device Logs and Monitoring Solutions

CISA recommends implementing an endpoint detection and response (EDR) solution that incorporates user and entity behavior analytics (UEBA) and "closely monitor access logs to detect deviations outside of normal behavior." A SIEM is also suggested as a way to store logs securely for the time required by compliance guidelines.

Ordr Software Inventory Collector provides details of granular details on assets including EDR installation status, version number, and active/inactive state.

With these insights, Ordr helps teams identify assets with out of date, disabled or missing EDR software. Ordr can also confirm devices are communicating with update servers, to ensure devices are in compliance and have the latest software patches. These details can be viewed in the Ordr dashboard, integrated with ITSM tools, or exported in reports.

Ordr logs can be shared with SIEM to provide security teams with a single, source of truth about assets.

- Identify security coverage gaps such as assets that should have EDR agents.
- Accelerate threat detection by identifying abnormal behavior that may be indicative of the early stages of a cyberattack
- Accelerate incident response and analysis by sharing granular details about assets with SIEM.

Mitigation Strategy #3: Vulnerability, Patch and Configuration Management



CISA Recommendations

Focus area 1: Vulnerability and Patch Management



Ordr Capabilities

Ordr identifies devices with vulnerabilities and risk such as outdated operating systems, unpatched or unauthorized software, PHI, recalls, risky communications, and anomalous behavior.

The solution combines these factors with customizable parameters and calculates a real-time risk rating per device to help organizations prioritize remediation and mitigation efforts.

Ordr also provides robust vulnerability management and mitigation capabilities and integrates with existing IT tools and workflows in addition to network and security infrastructure to help teams efficiently manage risk for all connected devices.



Ordr Benefits

- Improve security and efficiencies by using risks scores to prioritize for vulnerability management efforts
- Optimize ROI with a complete lifecycle vulnerability management capabilities that integrates with existing tools
- Accelerate risk mitigation efforts for assets where patches do not exist by automating network segmentation policies as compensating control

Focus area 2: Configuration and Change Management

Ordr Software Inventory Collector is a lightweight endpoint device query that automatically gathers software inventory details directly from devices and returns these details to a customer's Ordr instance, similar to a real-time "SBOM" (Software Bill of Materials).

This approach simplifies how software stack, patch data, and other device details are gathered for all managed and unmanaged devices. While not a true configuration and change management solution, Ordr can identify if elements like EDR, MDM, or disk encryption on assets meet an organization's security standards before being allowed onto the network by network access management solutions

- Improve security by identifying whether assets comply to organizational security standards

For organizations looking to improve their cybersecurity posture, CISA provides a simple and easy-to-understand cybersecurity guidelines. Ordr has partnered with many healthcare organizations to address their cybersecurity challenges. **Reach out to us at www.ordr.net to learn more about how we can help secure your connected assets, and align to these CISA guidelines.**

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, Northgate Capital, Kaiser Permanente Ventures, and Unusual Ventures.

To learn more, please reach out to us at www.ordr.net, or info@ordr.net