HOW ORDR MAPS TO THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) CONTROLS

ordr

The Cybersecurity Maturity Model Certification (CMMC) defines a particularly broad set of security requirements that apply to virtually any organization that does business with the U.S. Department of Defense (DoD). CMMC aims to bolster the security of the extended DoD supply chain, which has increasingly come under attack from a wide range of malicious actors. CMMC is expected to be implemented by more than 300,000 companies that make up the Defense Industrial Base (DIB) that provide support for the DoD. The new CMMC mandate will also include university-based research labs and facilities—as well as Federally Funded Research and Development Centers (FFDRCs) and University Affiliated Research Centers (UARCs).

The CMMC framework's overarching goal is to protect federal information that resides in an organization's environment, including Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Any computer or electronic device that processes federal data considered sensitive will need to be protected from the associated range of many threats. Organizations will need to consider a wide range of security best practices when developing their compliance strategies, including all connected devices -- from traditional servers, workstations and PCs to IoT, IoMT and OT devices.

Many organizations today lack visibility and security their devices and what sensitive data or information is flowing in and out of their organization. Below is how Ordr System Controls Engine (SCE) maps to CMMC controls:

CMMC CONTROLS THAT ARE ADDRESSED BY ORDR

Control ID	Maturity Description Level	How Ordr Maps
AC.1.003	Verify and control/limit connections to and use of external information systems.	Ordr enables 1.003 on a per-device (or per-device type) basis.
AC.2.013	Monitor and control remote access sessions.	Ordr can correlate protocol inspection results with data from MS Active Directory, LDAP, and WinRM/WMI to understand who was logged in while remote access protocols are in use.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	Ordr enables automated network policy generation and enforcement on existing infrastructure to restrict the flow of information at the Firewall, NAC, or Switch.

Control ID	Maturity Description Level	How Ordr Maps
AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Ordr is applicable when used to segment business groups or functional areas (e.g., segmenting manufacturing devices from the IT network).
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Ordr is applicable when "privileged functions" involve use of specific network ports/protocols (e.g., RDP, Telnet, FTP, SSH, etc.)
AC.3.020	Control connection of mobile devices.	Ordr can identify mobile devices, including those without MDM installed; limit mobile device connections to certain networks, segments, or protocols (when connected via Wi-Fi); and ensure mobile PC anti-virus software is properly connecting to an update server.
AC.4.023	Control information flows between security domains on connected systems.	Ordr policy profiles can group devices into security domain groups and create policies to limit communications between CUI authorized and CUI not-authorized components or systems.
AC.5.024	Identify and mitigate risk associated with unidentified wireless access points connected to the network.	Ordr provides clear visibility into all network connected devices, including wireless access points, with rich device context and associated risk.
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to	Ordr can understand who accesses each device and when using

Control ID	Maturity Description Level	How Ordr Maps
	those users so they can be held accountable for their actions.	integrations with Microsoft Active Directory/LDAP, WinRM/WMI. This can be correlated with device behavior to identify anomalous activity.
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.	Ordr maintains a record of network transmissions for every device to every internal and external destination, on every port, on every protocol. This record can be critical to investigations of unlawful or unauthorized system activity.
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	Ordr has integrations with all major SIEMs.
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	Ordr's queryable data lake aggregates information about devices, threats, and network behaviors from multiple sources, including external intel feeds, allowing analysis and reporting on suspicious or unusual activity. Information can also be exported to SIEMs or other reporting tools.
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	All information can be exported via Ordr to spreadsheets or databases for summarization, and predefined automated reports can be generated for on-demand access.
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators	Ordr automatically analyzes device, network, and security information and

Control ID	Maturity Description Level	How Ordr Maps
	(TTPs) and/or organizationally defined suspicious activity.	alerts when it detects critical indicators of compromise. Information can also be sent to a SIEM for external analysis and alerting.
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Ordr delivers passive and continuous monitoring of your network assets, which can provide a clear picture of the effectiveness of controls (e.g., speed of patching systems, connections to malicious URLs, accuracy of VLAN assignments, etc.), across the organization.
CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Ordr integrates with IT workflow automation systems to trigger the appropriate workflow for a given deficiency or vulnerability. This ensures written plans are implemented and executed properly when vulnerabilities or malicious behaviors are found.
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Ordr delivers passive and continuous monitoring of your network assets, which will provide a clear picture of the controls needed and effectiveness of implementation. For example, Ordr identifies devices first seen in the last 24 hours, allowing the organization to confirm that every device has followed the documented onboarding process.

Control ID	Maturity Description Level	How Ordr Maps
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system.	Ordr discovers every connected device, identifies devices with vulnerabilities, outdated operating systems, weak ciphers, weak certificates, active threats, and those that exhibit malicious or suspicious behaviors.
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Ordr dynamically generates network segmentation policies so that you can isolate mission-critical devices, those that share protected data, or run vulnerable operating systems.
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Ordr's network segmentation policies automatically update when new devices get added to the network, or when IP addresses change. This automatic enforcement of network security configurations reduces the burden on network administrators to implement network-centric policies to augment device-based configuration settings.
CM.3.068	Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.	Ordr dynamically generates network segmentation policies so that you can restrict, disable, or prevent the communication of devices with nonessential functions, ports, protocols and services.
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	Ordr can look for weak or default passwords on network-connected devices.

Control ID	Maturity Description Level	How Ordr Maps
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.	Ordr discovers every connected device, identifies devices with vulnerabilities, outdated operating systems, weak ciphers, weak certificates, active threats, and those that exhibit malicious or suspicious behaviors. Then, with this rich device context, Ordr dynamically generates network segmentation policies so that you can isolate mission-critical devices, those that share protected data, or run vulnerable operating systems. In addition, we have integrations with all major ITSM/CMDB/SIEM vendors.
IR.3.098	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Ordr in conjuntion with SIEM or workflow tools (e.g., ServiceNow or Nuvolo).
MP.2.119	Protect (ie., physically control and securely store) system media containing CUI, both paper and digital.	Ordr can assist with implementation as part of a complete system.
MP.2.120	Limit access to CUI on system media to authorized users.	Ordr can assist with implementation as part of a complete system.
PE.1.134	Control and manage physical access devices.	Ordr can assist with implementation as part of a complete system.
PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.	Ordr can assist with implementation as part of a complete system.

Control ID	Maturity Description Level	How Ordr Maps
PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Ordr can assist with implementation as part of a complete system. For example, Ordr can quickly create and implement segmentation policies that block access between systems containing CUI and external sites until terminations and transfers are complete.
RM.2.141	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	Ordr plays an integral role in any risk or vulnerability assessment by continuously monitoring (and reporting on) every action taken by organizational assets and systems.
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Ordr is passive and continuously discovers all network-connected devices. It identifies devices with vulnerabilities, outdated operating systems, weak ciphers, weak certificates, active threats, and those that exhibit malicious or suspicious behaviors.
RM.2.143	Remediate vulnerabilities in accordance with risk assessments.	Ordr risk rates vulnerabilities identified by inspecting network traffic, creating a prioritized list of vulnerabilities for remediation. It also dynamically generates network segmentation policies to continuously isolate mission-critical devices, those that

Control ID	Maturity Description Level	How Ordr Maps
		share protected data, or run vulnerable operating systems. This can help develop a prioritized remediation list which incorporates compensating controls for systems that cannot be patched or updated.
RM.3.147	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	Ordr discovers every connected device, identifies devices with vulnerabilities, outdated operating systems, weak ciphers, weak certificates, active threats, and those that exhibit malicious or suspicious behaviors. Then, with this rich device context, Ordr dynamically generates network segmentation policies so that you can isolate non-vendor supported products, mission-critical devices, those that share protected data, or run vulnerable operating systems.
RM.4.149	Catalog and periodically update threat profiles and adversary TTPs.	Ordr is continuously updating our 3rd party threat intelligence to enrich device context. In addition, we look at device behavior and are able to alert based on any deviation from the normal attributes.
RM.4.150	Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting and response and recovery activities.	Ordr ingests multiple sources of threat intelligence; FDA recalls, CareCERT, banned devices, validated blacklists, known signatures, etc. for our data lake that is used to inform device attributes.

Control ID	Maturity Description Level	How Ordr Maps
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's internet network boundaries and other organizationally defined boundaries.	Ordr is able to pull port data as well.
SC.1.175	Monitor, control and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Ordr can identify devices that transmit PCI, PHI, and PII data and those devices can be properly segmented.
SC.1.176	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	With Ordr's clear visibility of all your network-connected devices, you can set up VLANs or subnets to make sure that your network is properly segmented.
SC.2.178	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Ordr can prohibit remote activation of collaborative devices.
SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Ordr is FIPS 140-2 certified.
SC.3.180	Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.	Ordr ensures passive and continuous monitoring of all network-connected devices to provide clear information security.

Control ID	Maturity Description Level	How Ordr Maps
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.	Ordr dynamically generates network segmentation policies so that you can continuously isolate mission-critical devices, those that share protected data, or run vulnerable operating systems.
SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (ie., deny all, permit by exception).	Ordr dynamically generates network segmentation policies so that you can continuously isolate mission-critical devices, those that share protected data, or run vulnerable operating systems.
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Ordr dynamically generates network segmentation policies so that you can continuously isolate mission-critical devices, those that share protected data, or run vulnerable operating systems.
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Ordr can identify expiring certificates, but cannot perform end-to-end key management.
SC.4.228	Isolate administration of organizationally defined high-value critical network infrastructure components and servers.	Ordr dynamically generates network segmentation policies so that you can continuously isolate mission-critical devices, those that share protected data, or run vulnerable operating systems.
SC.5.198	Configure monitoring systems to record	Ordr discovers every connected

Control ID	Maturity Description Level	How Ordr Maps
	packets passing through the organization's internet network boundaries and other organizationally defined boundaries.	device, identifies devices with vulnerabilities, outdated operating systems, weak ciphers, weak certificates, active threats, and those that exhibit malicious or suspicious behaviors. Then, with this rich device context, Ordr dynamically generates network segmentation policies so that you can isolate mission-critical devices, those that share protected data, or run vulnerable operating systems.
SC.5.230	Enforce port and protocol compliance.	Using the Ordr Flow Genome, users can identify ports and protocols used by every device and dynamically generate network segmentation policies to continuously isolate mission-critical devices, those that share protected data, or devices that run vulnerable operating systems.
SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	Ordr ensures passive and continuous monitoring of all network-connected devices for timely reporting and remediation.
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	Ordr identifies malware moving laterally through the network using IDS signatures.
SI.2.214	Monitor system security alerts and advisories and take action in response.	Ordr ingests multiple sources of threat intelligence, advisories, and

Control ID	Maturity Description Level	How Ordr Maps
		vulnerability data bases; FDA recalls, CareCERT, banned devices, validated blacklists, known signatures, etc. for our data lake that is used to inform device attributes and alert users.
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Not only does Ordr monitor north-south traffic, we also monitor east-west traffic and alert users based on a myriad of IOCs.
SI.2.217	Identify unauthorized use of organizational systems.	Through integrations with Microsoft Active Directory/LDAP, WinRM/WMI, organizations can use Ordr to establish approved behavior/access and alert/segment based on abnormal behavior.
SI.4.221	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	Ordr delivers the network and device context enriched with threat intelligence information that is relevant to mitigating risk.
SI.5.223	Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.	Ordr can identify the result of malicious scripts via network traffic analysis (e.g., unauthorized FTP, RDP, or SMB traffic), but not the activity on a device itself.
SI.5.223	Monitor individuals and system	Ordr is passive and continuously

Control ID	Maturity Description Level	How Ordr Maps
	components on an ongoing basis for anomalous or suspicious behavior.	monitors network assets, alerts on anomalous or suspicious behavior, and automates network segmentation on existing infrastructure (firewalls, NAC, switch).

CMMC compliance will force many organizations to take a fresh look at their cybersecurity program and make changes to align with DoD requirements. Core security functions such as inventory, risk management, and threat detection will be essential to maintaining compliance, and organizations should look for efficient, automated systems that can help provide coverage for all connected devices including all connected devices — from traditional servers, workstations and PCs to IoT, IoMT and OT devices. Ordr SCE can arm organizations with a powerful tool to gain visibility into their network-connected devices, automatically expose potential risk, and enforce policies to either isolate high-risk devices, or to segment systems based on their unique needs. To learn more about Ordr and how the solution can help meet your CMMC goals, contact the Ordr team at info@ordr.net.