ORDR EXTENDS NIST CYBERSECURITY FRAMEWORK TO ALL CONNECTED ASSETS

ördr

ORDR EXTENDS NIST CYBERSECURITY FRAMEWORK TO ALL CONNECTED ASSETS

The National Institute of Technology (NIST) Cybersecurity Framework (CSF) provides security guidelines designed to secure critical infrastructure from cyber threats and improve cybersecurity risk management. The Framework Core provides the foundation for modern cybersecurity programs and controls, based upon five functions: Identify, Protect, Detect, Response, and Recover.

The rapid rise in the use of IOT and OT devices by the hyper-connected enterprise demands extending the use of CSF to cover all connected assets, not just traditional IT-managed systems. Healthcare, industrial, building automation, transportation, supply chain, physical security, and enterprise workgroup devices are increasingly network-enabled and exposed to cyberattack. These devices are appliances and cannot be inventoried, managed, or secured with classic tools as the enterprise does not have direct access or control of the software on them and cannot install agents to bring them into governance.

Ordr Systems Control Engine (SCE) enables organizations to extend the NIST CSF to cover all assets, inclusive of IOT/OT devices. SCE allows organizations to rapidly inventory everything in the domain, classify it based on type and business function, and assess it for risk. It learns behaviors and creates device flow genomes, to determine what each device should be talking to. It protects using microsegmentation to logically segregate groups of devices from anything that's non-essential and can rapidly stop active threats and isolate compromised devices. Plus, it is non-disruptive to the device, the network, and the enterprise operations.

The tables that follow enumerate how Ordr SCE help extend NIST CSF to cover all devices in the environment by mapping capabilities to the functions, categories, and subcategories defined by the specifications.

IDENTIFY (ID)

CATEGORY	SUBCATEGORY	ORDR SCE
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Ordr SCE passively discovers existing and new devices quickly, accurately and completely; identifying, classifying and profiling all devices and their detailed characteristics such as make, model, serial number, and software version using advanced machine learning and protocol decoding.
	ID.AM-2: Software platforms and applications within the organization are inventoried	Ordr SCE obtains and tracks the following software information about all assets including IOT devices, without requiring agents: • Device details such as manufacturer, make, model, operating system, software version, serial number • Validation of the current operating system and versions, including status of the software patches, hotfixes, application inventory and other details about Windows-based systems • Exposure to known vulnerabilities using its embedded (or via 3rd-party-integrated) vulnerability assessment scanner; includes validation of networked devices listening on unauthorized ports
	ID.AM-3: Organizational communication and data flows are mapped	Ordr SCE monitors and presents all flows for each device using the raw packet or NetFlow summarization. For IOT devices, this information is normalized to determine "baseline," or expected/appropriate, and "anomalous. Top down network flow characteristics can be monitored by VLAN, subnet, destination, protocol, and device group.

IDENTIFY (ID)

CATEGORY	SUBCATEGORY	ORDR SCE
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **ID.GV-4:** Governance and risk management processes address cybersecurity risks	Ordr SCE risk scores every device, and device type, to inform risk management process. The score is continuously updated as new vulnerability and threat intelligence information is obtained. Ordr SCE can identify devices and communications that involved regulated data including PCI and ePHI, enabling an organization to assure the systems are managed and data controls are enforced.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources **ID.RA-3:** Threats, both internal and external, are identified and documented **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk **ID.RA-6:** Risk responses are identified and prioritized	Ordr SCE monitors incidents and risk for IOT and other devices. Incident information is comprised of vulnerability from device manufacturer and ICS-CERT databases, combined with observed network-based vulnerabilities and threats within an organizations environment. This includes performing anomaly detection, network intrusion detection, bad URL/site connections, and other malicious activity. Each incident is mapped to the devices affected, and this information is maintained over a time window with reports and time-based views for trend analysis. The security dashboard provides a consolidated view of incidents based on criticality and MITRE kill-chain steps. All devices are assigned a risk score to ensure response efforts are prioritized. Scheduled and ad-hoc reports may be generated, and the incident information can be sent to a SIEM or IT workflow tool for further consolidation.

PROTECT (PR)

CATEGORY	SUBCATEGORY	ORDR SCE
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	Ordr SCE automates device identification, uses artificial intelligence to baseline normal communication behavior and then translates these behaviors into a device-specific security policy. The policy can be passed via API integration to NAC tools, zone-based firewalls, or pushed to switches and wireless controllers directly. Enabling this capability limits network communications to approved systems only, resulting in a reduced IOT/OT fleet attack surface. Ordr SCE can control access to the network based on a device's MAC address, or, for Windows systems, an agentless software compliance check.
	PR.AC-3: Remote access is managed	Ordr SCE can restrict remote access to internal OT/IOT devices by implementing microsegmentation policies that are enforced in the network infrastructure or zone-based firewalls.
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Ordr SCE can restrict access to OT/IOT devices over the network to only an approved set of devices/locations/protocols using micro-segmentation policies that are enforced in the network infrastructure or zoneo-based firewalls.
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	Ordr SCE automates the provisioning of network segmentation / microsegmentation policy across wired switches, wireless controllers and access points, firewalls, and network access control (NAC) solutions from all leading vendors.

PROTECT (PR)

CATEGORY	SUBCATEGORY	ORDR SCE
		SCE is highly network-aware, so not only does it understand which policies to apply, but where and how to apply them. In summary, the Ordr SCE quickly determines which devices are on the network and what they should be allowed to do, and then automatically translates this knowledge to a language your network understands to provide effective microsegmentation.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	Ordr SCE can identify devices and communications that involve regulated data including PCI and ePHI, enabling an organization to assure the systems are managed and data controls are enforced. SCE can implement whitelist controls to limit where those devices can communicate to prevent data-at-rest departing the device over the network.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Ordr SCE constantly monitors an environment and automatically identifies and classifies all devices on the network and gains rich information about each including make, model, and software version. This aids in maintaining accurate inventory of the systems while simplifying the auditing process. SCE can identify the geographic location devices are deployed based on the network they use to gain access to the environment. All moves, adds, and changes are detected and initiate a change management process.
	PR.DS-5: Protections against data leaks are implemented	Ordr SCE continuously monitors all communications in the environment and detects when devices try to connect to unauthorized

PROTECT (PR)

CATEGORY	SUBCATEGORY	ORDR SCE
		networks, malicious sites, or contain anomalous types of data in the transmission. SCE can be used to implement white-list micro-segmentation policies for IOT/OT devices that restricts their communications to only approved systems.
	PR.DS-7: The development and testing environment(s) are separate from the production environment	Ordr SCE tracks all the devices in the testing and production environment and monitors the communication patterns of each system. It can implement controls in firewalls and network infrastructure to limit communications, keeping the domains separate.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	Ordr SCE tracks what devices are connected to the network, details about each device inclusive of manufacturer/type/software version, learns the network topology along with the associated placement of devices within the network. SCE tracks all communications to and from every device, establishing baselines for OT/IOT devices automatically. This provides a baseline of systems and communication.
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	Ordr SCE tracks lifecycle events for connected assets related to cybersecurity: onboarding/ connection to the network, communication activity, exposed vulnerabilities, risk scores, indications of compromise, active threats, and decommissioning/disconnecting from the environment. This information fuels the system management lifecycle.

PROTECT (PR)

CATEGORY	SUBCATEGORY	ORDR SCE
	PR.IP-12: A vulnerability management plan is developed and implemented	Ordr SCE embeds numerous security intelligence feeds and integrations with vulnerability management platforms to extend the scope of the effort by covering OT/IOT assets and other neglected areas of the environment (facilities, physical security, medical, and industrial networks).
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality	Ordr SCE can restrict access to OT/IOT devices over the network to only an approved set of devices/locations/protocols using micro-segmentation policies that are enforced in the network infrastructure or zoneo-based firewalls.
	PR.PT-4: Communications and control networks are protected	Ordr SCE tracks all the devices in the C&C networks and monitors the communication patterns of each system. It can implement controls in firewalls and network infrastructure to restrict traffic flow, thus segregating the domain.

DETECT (DE)

CATEGORY	SUBCATEGORY	ORDR SCE
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	Ordr SCE tracks what devices are connected to the network, details about each device inclusive of manufacturer/type/software/users, learns the network topology along with the associated placement of devices within the network. It tracks all communications to and from every device, establishing baselines for OT/IOT devices automatically. This provides a baseline of systems and communication.
	DE.AE-2: Detected events are analyzed to understand attack targets and methods **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors **DE.AE-4:** Impact of events is determined **DE.AE-5:** Incident alert thresholds are established	Ordr SCE monitors incidents and risk for IoT device, mapping that information to each affected IoT device. Incident information is comprised of vulnerability from device manufacturer and ICS-CERT databases, combined with observed network-based vulnerabilities and threats within an organizations environment. Remediation recommendations are provided. Each incident is mapped to the devices affected, and this information is maintained over a time window with reports and time-based views to aid trending analysis. The security dashboard provides a consolidated view of incidents based on criticality and MITRE kill-chain steps. Scheduled and ad-hoc reports may be generated, and the incident information can be sent to a SIEM or IT workflow tool for further consolidation. Real-time alerts can be issued based on the security event type to specific staff responsible for the cybersecurity of the effected asset.

DETECT (DE)

CATEGORY	SUBCATEGORY	ORDR SCE
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	Ordr SCE passively monitors the network to identify cybersecurity issues including behavioral anomalies, network intrusion detection attempts, connections to known bad URL/sites, unexpected open ports, and observed vulnerabilities.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Ordr SCE passively tracks physical connectivity details for each device in the network, including the switch/port and wireless AP/SSID a device is using. All moves, adds, and changes are noticed and an audit log is maintained over time.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Ordr SCE monitors what devices are connected to the network and spots moves, adds, and changes. Detailed information about each device is tracked including the manufacturer, type, OS & patch, Windows software installed, and Active Director user access. It tracks all communications to and from every device, establishing baselines for OT/IOT devices automatically.
	DE.CM-8: Vulnerability scans are performed	Ordr SCE continuously monitors the network to identify vulnerabilities, active threats, and indications of compromise. This passive monitoring is non-disruptive to the environment and devices on the network. Ordr SCE has an embedded active vulnerability scanner optimized for OT/IOT that can be scheduled to run on regular intervals. SCE integrates with leading vulnerability management tools and can orchestrate scheduled scans that may be customized to be non-disruptive to OT/IOT devices.

DETECT (DE)

CATEGORY	SUBCATEGORY	ORDR SCE
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-4:** Event detection information is communicated to appropriate parties	Ordr SCE alerts security operations when cybersecurity events occur. SCE integrates with leading SIEM and ITAM products to tie into existing procedures and workflows.

RESPOND (RS)

CATEGORY	SUBCATEGORY	ORDR SCE
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained **RS.MI-2:** Incidents are mitigated **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	Ordr SCE can reactively block device communications or blacklist systems to contain compromised or unauthorized assets. The enforcement can be done directly in the network (on switches and wireless controllers), orchestrated by a NAC tool, or performed on a firewall for perimeter protection. SCE can implement whitelist microsegmentation policies to mitigate the effects of an incident and ensure it cannot reach critical or vulnerable devices. This can be enforced in the network infrastructure or firewalls.

INFO@ORDR.NET WWW.ORDR.NET 2445 AUGUSTINE DRIVE SUITE 601, SANTA CLARA, CA 95054