CIS Controls

How to Apply Ordr to the CIS Controls

About the CIS Controls

Published by the Center for Internet Security, the CIS Controls define security best practices across 20 key functional areas focused on protecting organizations from cyberattacks. The CIS Controls are notable for being highly practical and influential across multiple industries. With contributions from the NSA, SANS Institute, and the CIS, the CIS Controls leverages the collective insights of government and industry experts including leading red team engineers, penetration testers, law enforcement, forensic analysts, and incident responder. The CIS Controls also map to other major regulatory and compliance standards such as PCI-DSS, HIPAA, and FISMA and are directly referenced in a variety of other security frameworks such as the NIST Cybersecurity Framework (CSF). The CIS Controls (alternately known as the CIS 20 and CIS CSC among others) focus on the most essential cybersecurity functions. For each function, the document prioritizes specific controls based on the maturity of the organization. For example, some specific controls are recognized as basic security hygiene that all organizations should implement, while others are more advanced and should be applied based on the size or specific risk of an organization. This allows organizations to easily focus their efforts to provide the greatest risk reduction in each category.

Key Security Challenges Facing Organizations Today

Cybersecurity is constantly evolving, and the CIS Controls are intentionally flexible so that security leaders can apply them based on the organization's unique risk profile and the changing realities of the threat landscape. There are several notable trends and challenges that organizations will want to consider in the context of the CIS Controls. These include:

The Rise of Connected Devices

Historically most organizations focused their security efforts on traditional "managed" devices such as end-user laptops and servers. However, enterprises have experienced a massive growth in unmanaged devices including IoT and OT devices such as, medical devices, HVAC systems, shadow IT, and employee BYOD devices. Just as with traditional devices, these unmanaged devices can contain vulnerabilities and increasingly play critical roles in cyberattacks. However, they can prove to be harder to secure since they can't support a security agent, and many organizations lack the tools to even see many of these devices much less actively address their risk.

BASIC CIS CONTROLS:

1. Inventory and control of Hardware Assets

2. Inventory and control of Software Assets

3. Continuous Vulnerability Assessment and Remediation

4. Controlled Use of Administrative Privileges

5. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

6. Maintenance, Monitoring, and Analysis of Audit Logs

FOUNTAIONAL CIS CONTROLS:

7. Email and Web Browser Protections

8. Malware Defenses

9. Limitation and Control of Network Ports, Protocols, and Services

10. Data Recovery Capabilities

11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

12. Boundary Defense

13. Data Protection

14. Controlled Access Based on the Need to Know

15. Wireless Access Control

16. Account Monitoring and Control

ORGANIZATIONAL CIS CONTROLS:

17. Implement a Security Awareness and Training Program

18. Application Software Security

19. Incident Response and Management

20. Penetration Tests and Red Team Exercises

The goals of frameworks such as CIS and NIST CSF apply to all devices and are not limited to traditionally managed devices. Any system that can process, store, or transmit information has the potential to carry risk, and it is up to an organization to apply appropriate controls to both managed and unmanaged devices. This does not mean, however, that organizations will necessarily need to use multiple parallel systems. Most organizations will be best served with a unified approach that can apply to all connected devices, and a platform such as Ordr can provide the consistent visibility, detection, and protection needed to meet this goal.

New and Evolving Threats

The growth of unmanaged devices directly translates to new enterprise risk in the form of vulnerabilities and threats. Large-scale threats such as the Mirai botnet have specifically evolved in order to target enterprises. For example, attackers have targeted widespread vulnerabilities in F5 Big-IP devices and SonicWall SSL-VPNs as a way to spread malware within an organization. The same vulnerabilities have been used extensively by a variety of ransomware campaigns, and several popular ransomware groups such as eCh0raix and QNAP have heavily targeted network-attached storage (NAS) devices within enterprises.

IoT and OT devices have likewise proven to be a hotbed of vulnerabilities. IoT devices will often reuse the same software libraries for key functionality such as the TCP/IP stack. This means that any vulnerabilities in these common libraries have the potential to affect an incredibly wide range of products. For example, the Ripple20 and AMNESIA:33 vulnerabilities were found to affect dozens of vendors and hundreds of IoT, industrial, and medical devices.

Additionally, the recent SUNBURST supply chain attack underscores the need for consistent visibility, analysis, and protection across all devices in an organization. Specifically, organizations need to be able to see and control how a device communicates even when the device and its code is trusted. This can not only block known malicious command-and-control (C2) channels but also identify new C2 connections such as in the case of the SolarWinds backdoor.

Limited Time and Resources for Staff

While the number of devices and threats are constantly growing, the time and resources of IT and Security teams are often relatively fixed. This has led to an industry-wide problem where teams are simply unable to keep pace with the growing demands of the job. For example, a recent study found that the volume of alerts has more than doubled in the past 5 years. Technical teams simply haven't been able to keep up. A study by Tripwire found that 83% of security staff were overworked and that 82% of security teams were understaffed.

This makes it all the more important that solutions are highly efficient and automated whenever possible. Likewise, teams will need tools that apply to all the many devices within an organization. The CIS controls are designed to be flexible, but teams will likely be overwhelmed if they need to implement multiple tools in order to address managed and unmanaged devices for each control category.

The Role of Ordr in the CIS Controls

Ordr extends visibility and security to all of an organization's connected devices including traditional servers, workstations and PCs as well as IoT, IoMT, and OT devices. Ordr covers a wide range of security functions that map directly to many of the CIS Controls. This includes device discovery and inventory, vulnerability assessment, behavioral profiling, risk and threat detection, as well as automated segmentation and isolation of hosts based on their unique needs and risk. Key capabilities include:

Real-time Asset Inventory

Ordr brings together a unique combination of traffic analysis and AI to automatically discover and classify every device on the network. This includes high-fidelity information such as make, classification, location, and application/port usage. This visibility is continuous, real-time, and provides a single source of truth for network asset inventory.

Vulnerability Management

Ordr delivers a variety of unique capabilities in the area of vulnerability management. The platform includes a built-in vulnerability scanner to identify devices affected by a variety of industry-specific security alerts or recalls. Ordr also complements traditional scanning tools with bi-directional integrations that allow staff to identify devices that may have been missed by previous scans. The solution can also be used to create customized scans that specifically include or exclude devices of a certain type - which can be critical to maintaining business operations.

Behavior and Risk Profiling

Ordr includes a built-in IDS engine to detect threats and devices that are under active attack. Ordr also automatically learns every device's unique communication patterns, known as its Ordr Flow Genome. This provides a baseline that can be used to find suspicious and anomalous behaviors that could be the sign of an unknown threat.

Automated Response

Ordr can automate controls both to proactively reduce the risks of a device as well as to isolate devices with detected risks or threats. By baselining device behavior, Ordr can dynamically create segmentation policies such as firewall rules that provide devices with necessary access while limiting unnecessary exposure. Policies can be dynamically generated and enforced on a variety of infrastructure including switches, firewalls, wireless LAN controllers, and more. Ordr also integrates with incident response and asset management workflows and can be used to quarantine compromised or high-risk devices.

Mapping Ordr to the CIS Controls

The following section lists how various Ordr Systems Control Engine (SCE) capabilities can apply to specific CIS Controls. As always, no single solution will address all CIS Controls, and organizations may need to apply a variety of technologies in a particular area.

CIS Control 1 - Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Ordr passively discovers all connected devices including traditional servers, workstations and PCs as well as traditional unmanaged devices including IoT, IoMT, and OT devices. Each device is automatically identified and classified with detailed characteristics such as make, model, serial number, software version, as well as Active Directory and VLAN information.

Ordr monitors all devices connected to the network and identifies any moves, adds, and changes, making it easy to identify the introduction of new or unauthorized devices.

The platform tracks all communications to and from every device, including ports and protocols used. Ordr can then automatically generate and optionally enforce IP and port-based controls based on the requirements of each device.

Relevant CIS Sub-Controls: 1.2, 1.4, 1.5, 1.6, 1.7

CIS Control 2 - Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Ordr's discovery and analysis includes a variety of software-specific attributes of each system including the operating system and software versions. The solution validates the current operating system and version as well as the status of software patches, hotfixes, application inventory, and other details about Windows or MAC-based systems.

The solution can additionally identify vulnerable or high-risk devices using its embedded vulnerability scanner and having bi-directional integrations with Rapid7 and Tenable.

Using Ordr's dynamically generated policies, high-risk devices can be automatically segmented and enforced on a variety of infrastructure including switches, firewalls, wireless LAN controllers, and more to reduce the organization's exposure.

Relevant CIS Sub-Controls: 2.1, 2.3, 2.4, 2.5, 2.10

CIS Control 3 - Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Ordr both provides its own vulnerability assessment capabilities and also integrates with other 3rd party scanning solutions. The solution includes the ability to specifically identify vulnerabilities and device recalls affecting devices that are often missed by traditional scanners. Devices and vulnerabilities can then be prioritized based on their overall risk determined both by the role of the device as well as threat-based risk factors.

Ordr also augments 3rd party scanners with the ability to identify devices that were missed during previous scans and create customized scans to cover any overlooked devices. It can also create customized scans to include or exclude devices based on their device type or other attributes.

Relevant CIS Sub-Controls: 3.1, 3.2, 3.6, 3.7

CIS Control 4 - Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

As part of its analysis of each device, Ordr is able to identify devices with weak or default passwords.

Relevant CIS Sub-Controls: 4.2

CIS Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Ordr monitors and logs a variety of events that can be used to detect, identify, and recover from an attack. The solution baselines the communication patterns of each device. The solution automatically correlates this data and can alert and log events based on abnormal behavior and anomalies. The built-in Ordr IDS detects and logs active threats and provides a consolidated view of incidents based on criticality and MITRE kill-chain steps. The platform also ingests STIX and TAXII threat feeds which can be used to generate threat-based alerts based on data observed by Ordr. 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. Additionally, by internally correlating event data within the Ordr SCE, the solution can provide SIEMs with pre-correlated, enriched events that reduce the need to manually correlate events within the SIEM.

Relevant CIS Sub-Controls: 6.5, 6.6, 6.7, 6.8

CIS Control 8 - Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Many unmanaged devices by definition will not be able to run traditional antivirus software as defined in Control 8. However, Ordr provides a variety of features to detect the effects of malicious code on a device without the need for an agent. The solution automatically learns the behaviors of each device and can alert on anomalous behavior that can indicate that the device is compromised. Ordr also monitors all communication for known command-and-control traffic and traffic to malicious destinations as well as internal lateral movement within a network. Devices that are observed to be compromised can be automatically quarantined by Ordr. Alternatively, the solution can integrate with other automated response tools and SIEMs.

Relevant CIS Sub-Controls: 8.1, 8.2, 8.6, 8.7

CIS Control 9 - Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Ordr analyzes and documents the traffic characteristics of all devices by VLAN, subnet, destination, port, protocol, device group, and more. The platform can further identify risky devices that have unexpected open ports.

Based on the observed needs and risks of each device, Ordr can automatically generate and enforce policies on a per device or group of devices basis. These micro-segmentation policies ensure that devices can use approved ports and protocols to communicate with approved destinations.

Relevant CIS Sub-Controls: 9.1, 9.2, 9.5

CIS Control 11 - Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Ordr analyzes and documents the traffic behavior of all devices by VLAN, subnet, destination, port, protocol, device group, and more. This provides a full overview of how traffic is actually flowing within the network, allowing teams to validate that network policies and device configurations are having the intended effect. Teams can use Ordr to identify devices that are communicating in new or unexpected ways such as connecting to unexpected VLANs or using risky protocols or communication methods. The platform can identify devices that are not properly configured by comparing devices to established baselines or by comparing observed device traits to a device's MDS2 and SBOM information.

By learning the behavior of each device, Ordr also provides a way for staff to identify the appropriate technical and business needs of each device. Ordr can automatically generate policies based on these findings and continuously enforce newly added like-devices to ensure devices always have the access they need without any unnecessary exposure.

Relevant CIS Sub-Controls: 11.1, 11.2, 11.3

CIS Control 12 - Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Ordr analyzes the network traffic and traffic flow of all connected devices. The solution identifies a baseline of appropriate traffic for each device and alerts on any anomalies. Top-down network flow characteristics can be monitored by VLAN, subnet, destination, protocol, and device group.

Ordr can then automatically create policies that limit connections to only approved devices, locations, and protocols. These policies can be manually or automatically implemented in the network via Ordr's integration with network infrastructure and network firewalls.

Ordr includes a built-in IDS and STIX/TAXII integration to identify threats that cross network boundaries including network intrusion attempts and connections to known bad URL/sites.

Relevant CIS Sub-Controls: 12.1, 12.2, 12.3, 12.4, 12.6, 12.8

CIS Control 13 - Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Ordr continuously monitors all communications in the environment and detects when devices try to connect to unauthorized networks, malicious sites, or contain anomalous types of data in the transmission. Ordr can also identify devices and communications that involve regulated data including PCI, PII, and PHI, enabling an organization to assure the systems are managed and data controls are enforced.

Relevant CIS Sub-Controls: 13.1

CIS Control 14 - Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

While many organizations want to restrict access based on the need to know, it is often difficult for teams to identify and anticipate the various needs of a device. Ordr provides an automated way to identify and review the essential services required by each device or type of device, and translate those needs into actively enforced policies.

Ordr automates the creation of network segmentation/micro-segmentation policies and enforces them across wired switches, wireless controllers and access points, firewalls, and network access control (NAC) solutions from all leading vendors. Segmentation and micro-segmentation policies can be created to ensure devices only connect to other devices, locations, VLANs, and protocols that have a valid business reason.

Relevant CIS Sub-Controls: 14.1, 14.2, 14.6, 14.7

CIS Control 15 - Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

As part of Ordr's ability to detect and classify all devices on the network, the solution can easily inventory all wireless access points connected to the network including a variety of traits including identifying open SSIDs and devices using pre-shared key encryption. The system can likewise monitor and audit that personal and untrusted devices are segmented from trusted devices and internal assets.

Relevant CIS Sub-Controls: 15.2, 15.10

CIS Control 19 - Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

By directly detecting threats and documenting the mapping the interconnectivity of all devices in the network, Ordr can provide an invaluable tool to incident responders. The solution's built IDS and threat detection capabilities can integrate with a variety of automated response and investigation tools. Additionally, when threats or incidents are detected by other systems, staff can user Ordr to look for anomalous behaviors in potentially affected devices. Staff can then use Ordr to identify all connections from affected devices to quickly establish the scope and potential spread of a threat. Likewise, Ordr can provide the location of affected devices to accelerate responses and reduce the mean time to response (MTTR).

Relevant CIS Sub-Control: 19.3

Conclusions

The CIS Controls represent one of the most widely used and influential security frameworks in use today. By leveraging a mix of government and private experience, the controls provide a highly practical approach to security based on the realities of the threat landscape.

As with any security framework, adopting the CIS Controls requires a coordinated effort that includes organizational and security leaders, managers, legal teams, IT teams, and security practitioners. Likewise, the CIS Controls will involve the use and coordination of multiple technologies, systems, and skills. And while no solution can address all the needs of a security framework, Ordr provides a strong foundation that can be applied to a wide variety of controls. With visibility into all devices, how they communicate, their vulnerabilities, and their threats, security teams will have continuous visibility into organizational risk. Ordr can then take active measures to reduce that risk by automatically creating risk-based segmentation policies and isolating risky or compromised devices.

To learn more about the CIS Controls and how Ordr can help, please contact the team at info@ordr.net.