CIS Controls®

CIS Top - 20 Critical Security Controls (V 7.0)

Introduction

The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

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 Configuration 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

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Basic

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.

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.

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.

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.

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

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

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.

7. Email and Web Browser Protections

- Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

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.

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.

10. Data Recovery Capabilities

- The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

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.

12. Boundary Defense

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

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.

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.

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.

16. Account Monitoring and Control

- Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Organizational

17. Implement a Security Awareness and Training Program

- For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

18. Application Software Security

- Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

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.

20. Penetration Tests and Red Team Exercises

- Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.