August 30,2023 Task- CIS Top 20 Critical Security Controls

Basic:

1. Inventory and Control of Hardware Assets: This control involves creating and maintaining an up-to-date inventory of all hardware assets, including servers, computers, and network devices. It ensures that unauthorized or rogue devices do not compromise the network.

2. Inventory and Control of Software Assets: This control focuses on keeping track of software licenses, versions, and usage. It helps organizations manage software assets efficiently and avoid compliance issues.

3. Continuous Vulnerability Management: Regular vulnerability assessments and scanning are essential for identifying and addressing security weaknesses promptly, reducing the risk of exploitation.

4. Controlled Use of Administrative Privileges: Limiting administrative privileges ensures that only authorized personnel can make critical system changes, reducing the risk of insider threats or unauthorized access.

5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Configuring devices and software securely involves applying recommended security settings, reducing potential vulnerabilities that can be exploited.

6. Maintenance, Monitoring, and Analysis of Audit Logs: This control includes maintaining logs of system and network activities, monitoring them in real-time, and analyzing them for signs of security incidents or policy violations.

Foundational:

7. Email and Web Browser Protections: Implementing email filtering and web content filtering to block malicious attachments, links, and websites, reducing the risk of phishing attacks and malware infections.

8. Malware Defenses: Utilizing antivirus software, anti-malware tools, and intrusion detection systems to detect and prevent malware infections.

9. Limitation and Control of Network Ports, Protocols, and Services: Disabling unnecessary network ports, protocols, and services reduces the attack surface and limits the avenues attackers can exploit.

10. Data Recovery Capabilities: This control involves implementing data backup and recovery solutions to ensure data availability in the event of data loss or cyberattacks.

11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches: Configuring network devices securely involves setting up firewalls and routers to control traffic, filter content, and protect the network.

12. Boundary Defense: Implementing firewalls and intrusion prevention systems at network perimeters to monitor and block potentially malicious traffic from entering the network.

13. Data Protection: Safeguarding sensitive data with encryption, access controls, and data loss prevention measures to prevent unauthorized access or data breaches.

14. Controlled Access Based on the Need to Know: Ensuring that employees only have access to the data and systems required for their job roles, minimizing the risk of unauthorized access.

15. Wireless Access Control: Implementing strong authentication and encryption protocols for wireless networks and managing access to wireless devices.

16. Account Monitoring and Control: Continuously monitoring user account activities, login attempts, and privilege levels to detect and respond to suspicious behavior and potential insider threats.

Organizational:

17. Implement a Security Awareness and Training Program: Regularly educating employees about cybersecurity threats and best practices to create a security-conscious culture within the organization.

18. Application Software Security: Incorporating security measures throughout the software development lifecycle to identify and mitigate vulnerabilities in applications.

19. Incident Response and Management: Developing a structured incident response plan, which outlines procedures for detecting, responding to, and recovering from security incidents.

20. Penetration Tests and Red Team Exercises: Conducting simulated attacks (penetration tests) and engaging red teams to mimic real-world adversaries, evaluating the effectiveness of security controls and response procedures. This helps organizations proactively identify and address vulnerabilities and weaknesses.