AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

Task-6: Information about CIS (Centre for Internet Security) Controls

- **BASIC CONTROLS**

1. Inventory and Control of Hardware Assets: Maintaining an up-to-date inventory of all hardware devices within the organization's network to manage and secure them effectively. All the hardware devices should be updated time to time.

2. Inventory and Control of Software Assets: Keeping track of all software applications running on the network, ensuring only authorized and updated software is used. All the software applications should be updated for the smooth running.

3. Continuous Vulnerability Management: Regular scanning for vulnerabilities in the organization's systems and applications, and promptly apply patches and fixes. Vulnerability check should be done periodically in order to reduce the attacks on systems.

4. Controlled Use of Administrative Privileges: Limiting the access to administrative privileges, which is, only to authorized people and reducing the potential for unauthorized system changes.

5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Apply secure configuration settings to hardware and software to prevent vulnerabilities and attacks.

6. Maintenance, Monitoring, and Analysis of Audit Logs: Maintain logs of system activities, regularly monitor them for suspicious activities, and analyze them to identify potential security incidents.

- **FOUNDATIONAL CONTROLS**

7. Email and Web Browser Protections: Implement security measures to protect against email and web-based threats, including phishing, malware, and malicious links.

8. Malware Defenses: Deploy and maintain effective antivirus and anti-malware solutions to detect and block malicious software.

9. Limitation and Control of Network Ports, Protocols, and Services: Minimize potential attack surfaces by disabling or controlling unnecessary network ports, protocols, and services.

10. Data Recovery Capabilities: Establish reliable and tested data backup and recovery processes to ensure data can be restored in the event of data loss or a cyberattack.

11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches: Configure network devices with secure settings to prevent unauthorized access and attacks.

12. Boundary Defense: Implementing security measures at network boundaries to monitor and control incoming and outgoing traffic.

13. Data Protection: Implementing encryption and data protection mechanisms to safeguard sensitive data from unauthorized access.

14. Controlled Access Based on the Need to Know: Grant access to data and systems based on user roles and responsibilities, ensuring least privilege and reducing the risk of data exposure.

15. Wireless Access Control: Secure wireless networks with strong authentication and encryption mechanisms to prevent unauthorized access.

16. Account Monitoring and Control: Monitor user accounts for suspicious activities and implement controls to manage and secure user access.

- **ORGANIZATIONAL CONTROLS**

17. Implement a Security Awareness and Training Program: Educate employees about cybersecurity risks and best practices to help them recognize and respond to potential threats.

18. Application Software Security: Develop and maintain secure software applications, including regular testing and patching to prevent vulnerabilities.

19. Incident Response and Management: Establish a clear plan to detect, respond to, and recover from security incidents effectively.

20. Penetration Tests and Red Team Exercises: Conduct controlled simulations of cyberattacks to identify vulnerabilities and weaknesses in the organization's defenses.