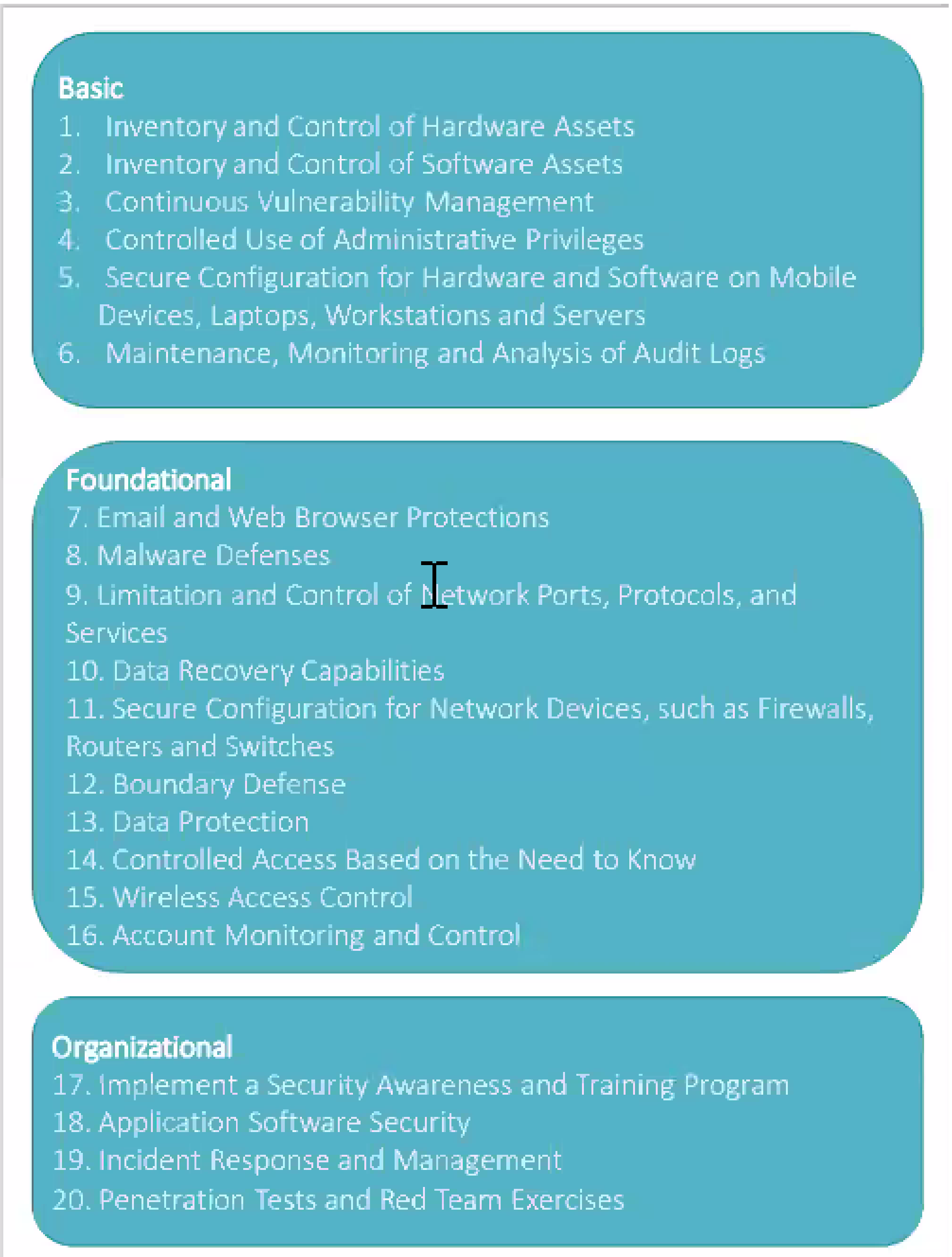
task 5 (30-08-2023)

collect small information regarding these topics



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

1. **Inventory and Control of Hardware Assets**:
   Maintain an up-to-date inventory of all hardware devices in your network. This helps in monitoring and managing devices to ensure they are secure and up-to-date.
2. **Inventory and Control of Software Assets**:
   Keep track of all software installed on network devices and systems. This control helps manage software vulnerabilities and ensure authorized software usage.
3. **Continuous Vulnerability Management**:
   Regularly scan systems for vulnerabilities and apply patches and updates to address them. This control aims to reduce the window of opportunity for attackers to exploit known vulnerabilities.
4. **Controlled Use of Administrative Privileges**:
   Limit administrative privileges to authorized personnel. This minimizes the risk of unauthorized access and reduces the potential impact of insider threats.
5. **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**:
   Configure systems securely to reduce the attack surface and enforce security settings on devices used within the organization.
6. **Maintenance, Monitoring, and Analysis of Audit Logs**:
   Monitor and review audit logs to detect and respond to suspicious activities. This helps in identifying potential security incidents and breaches.
7. **Email and Web Browser Protections**:
   Implement security measures to protect against phishing attacks, malicious attachments, and malicious websites in email and web browsers.
8. **Malware Defenses**:
   Deploy and maintain defenses against malware, including antivirus and anti-malware solutions, to prevent and mitigate malware infections.
9. **Limitation and Control of Network Ports, Protocols, and Services**:
   Restrict unnecessary network ports, protocols, and services to minimize potential attack vectors and reduce exposure to threats.
10. **Data Recovery Capabilities**:
    Implement data backup and recovery processes to ensure critical data can be restored in the event of data loss or a cyber incident.

11. **Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches**:
    Configure network devices securely to prevent unauthorized access and ensure that they are properly maintained and updated.
12. **Boundary Defense**:
    Implement security measures to protect the network perimeter, including firewalls and intrusion detection/prevention systems.
13. **Data Protection**:
    Implement encryption and other protective measures to safeguard sensitive data, both in transit and at rest.
14. **Controlled Access Based on the Need to Know**:
    Grant access to systems and data on a need-to-know basis to limit the potential impact of unauthorized access.
15. **Wireless Access Control**:
    Secure wireless networks to prevent unauthorized access and implement proper encryption for wireless communication.
16. **Account Monitoring and Control**:
    Monitor user accounts for suspicious activities and ensure proper account management practices are in place.
17. **Implement a Security Awareness and Training Program**:
    Provide security training and education to employees to promote cybersecurity awareness and safe practices.
18. **Application Software Security**:
    Implement security measures in the development, deployment, and maintenance of application software to prevent vulnerabilities.
19. **Incident Response and Management**:
    Develop and implement an incident response plan to effectively manage and respond to security incidents and breaches.
20. **Penetration Tests and Red Team Exercises**:
    Conduct penetration tests and simulated attacks to identify vulnerabilities and weaknesses in the organization's security defenses.