CyberDefense Pro (V2)

Competency Assessment Objectives

Monitoring and Log Analysis

Monitor networks

- Monitor network traffic
- Monitor network ports and sockets

Monitor software and systems

- Configure execution control and verify digital signatures
- Analyze executable processes
- Review web application security
- Monitor email for malware
- Analyze email headers and impersonation attempts

Implement logging

- Manage and perform analysis using Security Information and Event Management (SIEM) tools
- Review event logs
- Send log events to a remote syslog server
- Review firewall logs

Threat Analysis and Detection

Perform threat analysis

- Review firewall configuration
- Conduct a trend analysis

- Determine the types of vulnerabilities associated with different attacks

Detect threats using analytics and intelligence

- Use an Intrusion Detection System (IDS)
- Use a protocol analyzer and packet analysis to determine threats
- Use endpoint protection tools
- Check for privilege escalation
- Perform digital forensics investigations

Risk Analysis and Mitigation

Implement security controls to mitigate risk

- Detect unpatched systems
- Configure host firewall policies
- Implement anti-virus and endpoint security
- Implement Intrusion Prevention System (IPS)
- Implement cloud security
- Perform application and data protection tasks
- Implement and configure a security appliance

Implement system hardening

- Disable unnecessary services
- Check service configuration
- Disable unnecessary ports

Perform penetration tests

- Perform internal penetration testing
- Perform external penetration testing

Implement defensive deception methods

- Deploy a honeypot
- Implement a black hole or sinkhole
- Configure a captive portal

Incident Response

Manage security incidents

- Resolve malware, ransomware, and phishing attacks
- Eradicate Advanced Persistent Threats (APT)
- Respond to Distributed Denial of Service (DDoS) attacks

Manage devices

- Secure smartphones, tablets, and laptops
- Implement data loss prevention
- Secure embedded devices
- Secure IOT devices
- Implement network access control (NAC)

Analyze indicators of compromise

- Examine applications for any signs of compromise
- Inspect systems for any signs of compromise
- Investigate networks for any signs of compromise
- Analyze indicators for false positives and false negatives

Audit and Compliance

Implement Identity and Access Management (IAM)

- Administer user accounts
- Manage user-based and role-based access
- Manage certificates
- Configure account policies and account control

Implement physical security controls

- Analyze physical security design to protect systems.
- Analyze system security design to protect systems.
- Implement drive encryption
- Implement physical access controls