Security Operations and Administration

Learning Objective

- What is SOCA?
- Important SOCA concepts

Topics Covered

- Understand security concepts
- Identify and implement security controls
- Document and maintain functional security controls
- Participate in asset management lifecycle (hardware, software and data)
- Participate in change management lifecycle
- Participate in implementing security awareness and training (e.g., social engineering/phishing)
- Collaborate with physical security operations (e.g., data centre assessment, badging)

Access Controls

Learning Objective

- Network Investigations
- Password Cracking and Access Attacks
- Zero Trust Principles and SIEM Best Practices

Topics Covered

- Implement and maintain authentication methods
- Support internetwork trust architectures
- Participate in the identity management lifecycle

Risk Identification, Monitoring and Analysis

Learning Objective

- ❖ Risk Concepts
- ❖ Risk Assessment and Management
- ❖ Risk Policy Planning
- ❖ Security Functions
- ❖ Network Monitoring at Scale

Topics Covered

- Understand the risk management process
- Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy)
- Participate in security assessment and vulnerability management activities
- Operate and monitor security platforms (e.g., continuous monitoring)
- Analyse monitoring results

Incident Response and Recovery

Learning Objective

- ❖ Incident Handling Lifecycle
- ❖ SOC Functional Components
- ❖ Physical Security Issues and Controls

Topics Covered

- Support incident lifecycle e. Understand and support forensic investigations g., National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO)
- Understand and support business continuity plan (BCP) and disaster recovery plan (DRP)

Cryptography

Learning Objective

- ❖ Data Protection
- ❖ Confidentiality, Integrity, Authentication, Non-Repudiation
- ❖ Encryption Algorithms and Applications

- ❖ Privacy Requirements and Regulations

Topics Covered

- Understand cryptography
- Apply cryptography concepts
- Understand and implement secure protocols
- Understand public key infrastructure (PKI)
- Understand and apply fundamental concepts of networking

Network and Communication Security

Learning Objective

- ❖ Network Architecture
- ❖ Network Protocols and Packet Analysis
- ❖ Identity and Access Management
- ❖ Web authentication mechanisms
- ❖ DNS architecture and function
- ❖ Wi-Fi Data Collection, Attacks and Analysis

Topics Covered

- Understand and Understand network attacks (e.g., distributed denial of service (DDoS), man-in-the-middle (MITM), Domain Name System (DNS) poisoning) and countermeasures (e.g., content delivery networks (CDN)) apply fundamental concepts of networking
- Manage network access controls
- Secure wireless communications
- Operate and configure network-based security devices

Systems and Application Security

Learning Objective

- ❖ Users, Permissions and Logging
- ❖ Understanding Web Applications
- ❖ Session Tracking
- ❖ Mobile Device Security
- ❖ Logging and Monitoring

Topics Covered

- Identify and analyse malicious code and activity
- Implement and operate endpoint device security
- Administer Mobile Device Management (MDM)
- Understand and configure cloud security
- Operate and maintain secure virtual environments