

Certified SOC Analyst

Course Outline

(Version 1)

Module 00: SOC Essential Concepts

- Computer Network Fundamentals
 - Computer Network
 - TCP/IP Model
 - Comparing OSI and TCP/IP
 - Types of Networks
 - Local Area Network (LAN)
 - Wide Area Network (WAN)
 - Metropolitan Area Network (MAN)
 - Personal Area Network (PAN)
 - Campus Area Network (CAN)
 - Global Area Network (GAN)
 - Wireless Networks (WLAN)
 - Network Topologies
 - Bus Topology
 - Star Topology
 - Ring Topology
 - Mesh Topology
 - Tree Topology
 - Hybrid Topology
 - Network Hardware Components
 - Types of LAN Technology
 - Ethernet
 - Fast Ethernet
 - Gigabit Ethernet
 - 10 Gigabit Ethernet
 - Asynchronous Transfer Mode (ATM)

- Power over Ethernet (PoE)
- Types of Cables: Fiber Optic Cable
- Types of Cables: Coaxial Cable
- Types of Cables: CAT 3 and CAT 4
- Types of Cables: CAT 5
- Types of Cables: CAT 5e and CAT 6
- Types of Cables: 10/100/1000BaseT (UTP Ethernet)
- TCP/IP Protocol Suite
- Application Layer Protocols
 - Dynamic Host Configuration Protocol (DHCP)
 - DHCP Packet Format
 - DHCP Packet Analysis
 - Domain Name System (DNS)
 - DNS Packet Format
 - DNS Packet Analysis
 - DNSSEC
 - How DNSSEC Works?
 - Managing DNSSEC for your Domain Name
 - What is a DS Record?
 - How does DNSSEC Protect Internet Users?
 - Operation of DNSSEC
 - Hypertext Transfer Protocol (HTTP)
 - Secure HTTP
 - Hyper Text Transfer Protocol Secure (HTTPS)
 - File Transfer Protocol (FTP)
 - How FTP Works?
 - FTP Anonymous Access and its Risk
 - Hardening FTP Servers
 - Secure File Transfer Protocol (SFTP)
 - Trivial File Transfer Protocol (TFTP)
 - Simple Mail Transfer Protocol (SMTP)
 - Sendmail
 - Mail Relaying

- S/MIME
- How it Works?
- Pretty Good Privacy (PGP)
- Difference between PGP and S/MIME
- Telnet
- SSH
- SOAP (Simple Object Access Protocol)
- Simple Network Management Protocol (SNMP)
- NTP (Network Time Protocol)
- RPC (Remote Procedure Call)
- Server Message Block (SMB) Protocol
- Session Initiation Protocol (SIP)
- RADIUS
- TACACS+
- Routing Information Protocol (RIP)
- OSPF (Open Shortest Path First)
- Transport Layer Protocols
 - Transmission Control Protocol (TCP)
 - TCP Header Format
 - TCP Services
 - User Datagram Protocol (UDP)
 - UDP Operation
 - Secure Sockets Layer (SSL)
 - Transport Layer Security (TLS)
- Internet Layer Protocols
 - Internet Protocol (IP)
 - IP Header: Protocol Field
 - What is Internet Protocol v6 (IPv6)?
 - IPv6 Header
 - IPv4/IPv6 Transition Mechanisms
 - IPv6 Security Issues
 - IPv6 Infrastructure Security Issues
 - IPv4 vs. IPv6

- Internet Protocol Security (IPsec)
- IPsec Authentication and Confidentiality
- Internet Control Message Protocol (ICMP)
- Error Reporting and Correction
- ICMP Message Delivery
- Format of an ICMP Message
- Unreachable Networks
- Destination Unreachable Message
- ICMP Echo (Request) and Echo Reply
- Time Exceeded Message
- IP Parameter Problem
- ICMP Control Messages
- ICMP Redirects
- Address Resolution Protocol (ARP)
- ARP Packet Format
- ARP Packet Encapsulation
- ARP Packet Analysis
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- Link Layer Protocols
 - Fiber Distributed Data Interface (FDDI)
 - Token Ring
 - WEP (Wired Equivalent Privacy) Encryption
 - WPA (Wi-Fi Protected Access) Encryption
 - WPA2 Encryption
 - WEP vs. WPA vs. WPA2
 - TKIP
 - EAP (Extensible Authentication Protocol)
 - How EAP Works?
 - Understanding LEAP / PEAP
 - CDP (Cisco Discovery Protocol)
 - HSRP (Hot Standby Router Protocol)
 - Virtual Router Redundancy Protocol (VRRP)

- VLAN Trunking Protocol (VTP)
- STP (Spanning Tree Protocol)
- IP Addressing and Port Numbers
 - Internet Assigned Numbers Authority (IANA)
 - IP Addressing
 - Classful IP Addressing
 - Address Classes
 - Subnet Masking
 - Subnetting
 - Supernetting
 - IPv6 Addressing
 - Difference between IPv4 and IPv6
 - Port Numbers
- Network Security Controls
 - Network Security Controls
 - Access Control
 - Access Control Terminology
 - Access Control Principles
 - Access Control System: Administrative Access Control
 - Access Control System: Physical Access Controls
 - Access Control System: Technical Access Controls
 - Types of Access Control
 - Discretionary Access Control (DAC)
 - Mandatory Access Control (MAC)
 - Role-based Access
 - Network Access Control List
 - User Identification, Authentication, Authorization and Accounting
 - Types of Authentication: Password Authentication
 - Types of Authentication: Two-factor Authentication
 - Types of Authentication: Biometrics
 - Types of Authentication: Smart Card Authentication
 - Types of Authentication: Single Sign-on (SSO)
 - Types of Authorization Systems

- Authorization Principles
- Encryption
- Symmetric Encryption
- Asymmetric Encryption
- Encryption Algorithms: Data Encryption Standard (DES)
- Encryption Algorithms: Advanced Encryption Standard (AES)
- Encryption Algorithms: RC4, RC5, RC6 Algorithms
- Hashing: Data Integrity
- Message Digest Function: MD5
- Message Digest Function: Secure Hashing Algorithm (SHA)
- Hash-based Message Authentication Code (HMAC)
- Digital Signatures
- Digital Certificates
- Public Key Infrastructure (PKI)
- Network Security Devices
 - What is a Firewall?
 - Hardware Firewall
 - Software Firewall
 - What Does a Firewall Do?
 - What Can't a Firewall Do?
 - Types of Firewalls
 - Packet Filtering
 - Address Filtering
 - Network Filtering
 - Firewall Policy
 - Periodic Review of Information Security Policies
 - Firewall Implementation
 - Build a Firewall Ruleset
 - Egress Filtering and its Importance
 - Ingress Filtering and its Importance
 - Firewall Rulebase Review
 - Maintenance and Management of Firewall
 - Introduction to Intrusion Detection System (IDS)

- Types of Intrusion Detection Systems
 - Network-Based Intrusion Detection Systems (NIDS)
 - Host-Based Intrusion Detection Systems (HIDS)
- Application-based IDS
- Multi-Layer Intrusion Detection Systems (mIDS)
- Multi-Layer Intrusion Detection System Benefits
- Wireless Intrusion Detection Systems (WIDSs)
- Common Techniques Used to Evade IDS Systems
- Proxy Server
- Virtual Private Network (VPN)
- VPN Security
- Windows Security
 - Patch Management
 - Configuring an Update Method for Installing Patches
 - System Management Server: SMS
 - Microsoft Software Update Services: SUS
 - Windows Software Update Services: WSUS
 - Microsoft Baseline Security Analyzer (MBSA)
 - Windows Registry
 - Identifying Running Process and its Associated Sockets
 - Analyzing Registry ACLs
 - Disabling Unused System Services
 - Finding Suspicious/Hidden/Interesting Files
 - File System Security: Setting Access Controls and Permission
 - File System Security: Setting Access Controls and Permission to Files and Folders
 - Creating and Securing a Windows File Share
 - Desktop Locked Down
 - Active Directory(AD)
 - Active Directory Roles: Global Catalog (GC)
 - Active Directory Roles: Master Browser
 - Active Directory Roles: FSMO
 - How AD Relies on DNS
 - How AD Relies on LDAP Group Policy

- Windows Passwords: Password Policy
- Account Lockout Policy
- Microsoft Authentication
- Security Accounts Manager (SAM) Database
- Microsoft Exchange Server and its Concerns
- Unix/Linux Security
 - Linux Baseline Security Checker: buck-security
 - Password Management
 - Disabling Unnecessary Services
 - Killing Unnecessary Processes
 - Linux Patch Management
 - File System Security: Unix/Linux
 - Understanding and Checking Linux File Permissions
 - Changing File Permissions
 - Check and Verify Permissions for Sensitive Files and Directories
- Web Application Fundamentals
 - Overview of Web Application Architecture
 - Web Application Architecture
 - HTTP Communication
 - Exchange of HTTP Request and Response Messages
 - HTTP Request Message Format
 - HTTP Response Message Format
 - HTTP Message Parameters
 - HTTP Request Methods
 - HTTP GET and POST Request Method
 - HTTP Response Status Codes and Phrases
 - HTTP Header Fields: General Header
 - HTTP Header Fields: Request Header
 - HTTP Header Fields: Response Header
 - HTTP Header Fields: Entity Header
 - An Overview to HTTPS Protocol
 - Encoding and Decoding
 - Encoding Techniques

- ASCII
- Unicode
- HTML Encoding
- Hex/ Base 16 Encoding
- URL Encoding
- Base64
- Differences between Encryption and Encoding
- ASCII Control Characters Encoding
- Non-ASCII Control Characters Encoding
- Reserved Characters Encoding
- Unsafe Characters Encoding
- Information Security Standards, Laws and Acts
 - Payment Card Industry Data Security Standard (PCI-DSS)
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Information Security Acts: Sarbanes Oxley Act (SOX)
 - Information Security Acts: General Data Protection Regulation (GDPR)
 - Information Security Acts: Gramm-Leach-Bliley Act (GLBA)
 - Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)

Module 01: Security Operations and Management

- Security Management
- Security Operations
- Security Operations Center (SOC)
- Need of SOC
- SOC Capabilities
 - Situational awareness deliverance
 - Threat Control and prevention
 - Forensics
 - Audit and compliance support
- SOC Operations
 - Log Collection
 - Log Retention and Archival

- Log Analysis
- Monitoring of Security Environments for Security Events
- Event Correlation
- Incident Management
- Threat Identification
- Threat Reaction
- Reporting
- SOC Workflow
 - Collect
 - Ingest
 - Validate
 - Report
 - Respond
 - Document
- Components of SOC: People, Process and Technology
- People
 - L1: SOC Analyst
 - L2: SOC Analyst
 - Incident Responder
 - Subject Matter Expert/Hunter
 - SOC Manager
 - Chief Information Security Officer (CISO)
- Technology
 - SIEM Solutions
 - Security Monitoring Tools
 - Dashboard
 - Ticketing System
 - Automated Assessment Tool
- Processes
 - Business Processes
 - Technology Processes
 - Operational Processes

- Analytical Processes
- Types of SOC Models
 - In-House/Internal SOC Model
 - Outsourced SOC Model
 - Hybrid SOC Model
- SOC Maturity Models
 - SOC-Capability Maturity Model
 - Control Objectives for Information Technology (CoBIT)
 - National Institute of Standards and Technology (NIST) Cybersecurity Framework
 - Systems Security Engineering Capability Maturity Model (SSE-CMM)
- SOC Generations
 - 1st Generations
 - 2nd Generations
 - 3rd Generations
 - 4th Generations
 - 5th Generations
- SOC Implementation
 - Planning
 - Designing and Building the SOC
 - Operating the SOC
 - Reviewing and Reporting the SOC
- SOC Key Performance Indicators (KPI) and Metrics
- Challenges in Implementation of SOC
- Best Practices for Running SOC
- SOC vs NOC

Module 02: Understanding Cyber Threats, IoCs, and Attack Methodology

- Cyber Threats
- Intent-Motive-Goal
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness

- Network Level Attacks
 - Reconnaissance Attacks
 - Network Scanning
 - Port Scanning
 - DNS Footprinting
 - Network Sniffing
 - Man-in-the-Middle Attack
 - Password Attacks
 - Password Attack Techniques
 - Dictionary Attack
 - Brute Forcing Attack
 - Hybrid Attack
 - Birthday Attack
 - Rainbow Table Attack
 - Privilege Escalation
 - DNS Poisoning
 - DNS Cache Poisoning
 - ARP Poisoning
 - DHCP Starvation Attacks
 - DHCP Spoofing Attack
 - Switch Port Stealing
 - MAC Spoofing/Duplicating
 - Network-based Denial-of-Service Attack (DoS)
 - Distributed Denial-of-Service Attack (DDoS)
 - Malware Attacks
 - Advanced Persistent Threats (APTs)
 - Characteristics of Advanced Persistent Threats (APTs)
 - Advanced Persistent Threat Lifecycle
- Host Level Attacks
 - Common Threats Specific to Host Security
 - Host based DoS attacks
 - Where do they Come from?
- Application Level Attacks

- SQL Injection Attacks
- Cross-site Scripting (XSS) Attacks
- Parameter Tampering
- Directory Traversal
- Cross-site Request Forgery (CSRF) Attack
- Application-level DoS Attack
- Session Attacks: Cookie Poisoning Attacks
- Session Attacks: Session Fixation
- Email Security Threats
 - Malicious Email Attachments
 - Malicious User Redirection
 - Phishing
 - Email Security Threats: Hoax Mail
 - Email Security Threats: Spamming
- Understanding Indicators of Compromise (IoCs)
 - Indicators of Compromise (IoCs)
 - Why Indicators of Compromise Important?
 - Categories of IoCs
 - Key Indicators of Compromise
- Understanding Attacker's Hacking Methodology
 - EC-Council's- Hacking Methodology
 - Lockheed Martin's - Cyber Kill Chain Methodology
 - Kill Chain Deep Dive Scenario - Spear Phishing
 - Gaining Knowledge of Attacker's TTPs Through Hacking Forums

Module 03: Incidents, Events, and Logging

- Incident
- Event
- Log
- Typical Log Sources
- Need of Log
- Logging Requirements
- Typical Log Format

- Logging Approaches
 - Local Logging
 - Centralized Logging
- Local Logging
 - Windows Logs
 - Windows Log
 - Windows Event Log Types and Entries
 - Event Types
 - Monitoring and Analysis of Windows Logs
 - Linux Logs
 - Linux Log
 - Different Linux Log Files
 - Linux Log Format
 - Severity Level and Value of Linux Logs
 - Monitoring and Analysis of Linux Logs
 - Mac Logs
 - Mac Logs
 - Types of Logs in Mac
 - Mac Log Files
 - Log Format in Mac System
 - Monitoring and Analysis of Mac Logs
 - Firewall Logs
 - Firewall Logging
 - Monitoring and Analysis of Firewall Logs
 - Windows Firewall Logs
 - Monitoring and Analysis of Windows Firewall Log
 - Mac OS X Firewall Logs
 - Monitoring and Analysis of Firewall Log in Mac
 - Linux Firewall Logs
 - Linux Firewall: Iptables
 - Monitoring and Analysis of IP Tables logs
 - Cisco ASA Firewall
 - Monitoring and Analyzing Cisco ASA Firewall Logs

- Check Point Firewall
 - Monitoring and Analyzing Check Point Firewall Logs
- Router Logs
 - Cisco Router Log
 - Monitoring and Analysis of Router Logs
- Web Servers Logs
 - Internet Information Services (IIS) Logs
 - Monitoring and Analyzing Log Files in IIS
 - Apache Logs
 - Monitoring and Analysis of Apache Log
- Centralized Logging
 - Why Centralized Logging?
 - Centralized Logging
 - Centralized Logging Infrastructure
 - Centralized Logging, Monitoring, and Analysis Process
 - Log Collection
 - Log Transmission
 - Example: Syslog Log Transport Mechanism
 - Log Storage
 - Log Normalization
 - Log Correlation
 - Micro-level Correlation
 - Macro-level Correlation
 - Log Analysis
 - Log Analysis Approaches
 - Manual Log Analysis
 - Automated Log Analysis
 - Log Analysis Best Practices
 - Alerting and Reporting
 - What is an Alert?
 - Centralized Logging Best Practices
 - Centralized Logging/Log Management Tools
 - Centralized Logging Challenges

Module 04: Incident Detection with Security Information and Event Management (SIEM)

- Security Information and Event Management(SIEM)
- Security Analytics
- Need of SIEM
- Typical SIEM Capabilities
 - Log Collection
 - Log Analysis
 - Event Correlation
 - Log Forensics
 - IT Compliance
 - Application Log Monitoring
 - Object Access Auditing
 - Real-time Alerting
 - User Activity Monitoring
 - Dashboards
 - Reporting
 - File Integrity Monitoring
 - System and Device Log Monitoring
 - Log Retention
- SIEM Architecture and Its Components
- SIEM Solutions
 - Types of SIEM Solutions
 - In-House SIEM
 - Cloud-based SIEM
 - Managed SIEM
 - SIEM Solutions
 - Micro Focus ArcSight Enterprise Security Manager (ESM)
 - Splunk Enterprise Security (ES)
 - IBM Security QRadar
 - AlienVault Unified Security Management (USM)
 - Additional SIEM Solutions
 - Elastic Stack
 - LogRhythm SIEM

- McAfee Enterprise Security Manager (ESM)
- Micro Focus Sentinel Enterprise
- SolarWinds Log & Event Manager
- Trustwave SIEM Enterprise and Log Management Enterprise
- RSA NetWitness Suite
- SIEM Deployment
 - Challenges in SIEM Deployment
 - Recommendations for Successful SIEM Deployment
 - Implementing Phased SIEM Deployment
 - Use Phased approach for SIEM deployment
 - Deploying Log Management Component First and then SIEM Component
 - Use-Case-by-Use-Case (Output-Driven) Approach
 - Determining the Scope, Use Cases, and its Associated Requirements
 - SIEM Scope
 - Audit and compliance
 - Security
 - Operations
 - SIEM Use Cases
 - Stages in Use Case Development and Implementation
 - Requirements
 - Log Data
 - Contextual Data
 - Traffic Flow Data
 - EPS, Volume, and Hardware Requirements
 - Implementing a Suitable Deployment Architecture
 - SIEM Deployment Architecture
 - Self hosted, Self Managed
 - Self hosted, MSSP Managed
 - Self-hosted-Jointly Managed
 - Cloud, MSSP Managed
 - Cloud, Jointly Managed
 - Cloud, Self-Managed
 - Hybrid Model, Jointly Managed

- Additional Recommendations for Successful SIEM Deployment
- Incident Detection with SIEM
 - SIEM Incident Detection: Signature-based vs Anomaly-based Detection
- Examples of commonly Used Use Cases Across all SIEM deployments
 - Use Case Examples for Application Level Incident Detection
 - Detect an Attempt of SQL Injection
 - Detect an Attempt of XSS
 - Detect an Attempt of Directory Traversal
 - Detect an Attempt of Parameter Tampering
 - Detect an Attempt of Brute Force
 - Monitor Web Requests for High Number of Return Codes
 - Monitor for Use of Bad Bot User-Agents
 - Monitor Use of TRACE or OPTIONS Request Methods
 - Monitor Traffic from Known Bad IP reputation
 - Use Case Examples for Insider Incident Detection
 - Monitor Abnormal Authentication Attempts
 - Detect Data Exfiltration Attempts Made through USB or CD Drives
 - Detect Data Exfiltration Attempts Made Through FTP
 - Detect Data Exfiltration Attempts using Personal Web Mail Accounts
 - Detect Data Deletion Attempt
 - Detect an Attempt of Account Compromise
 - Detect Attempt of Accessing or Modifying Unusual Data
 - Detect Attempt of Communicating over Private Network (TOR Network)
 - Detect Which IP's are Connecting to Specific Port
 - Detect Data Exfiltration Attempts Through Cloud Storage
 - Use Case Examples for Network Level Incident Detection
 - Monitor Network for Use of Insecure Protocols and Services
 - Detect Services Running on Non Standard Ports
 - Detect Non-Standard Use of Standards Ports
 - Detect Network Scanning Attempts
 - Detect Port Scan Attempts
 - Detect Excessive Firewall Denies Attempts
 - Detect Attempt of Accessing Disabled Account

- Detect Attempt of Account Creation, Usage, and Deletion
- Perform Registry Monitoring
- Monitor Attempts of Ransomware Attack
- Detect Rogue DNS Servers (DNS Hijacking/ DNS Spoofing)
- Detect DNS Tunneling Attempts
- Detect DNS Exfiltration Attempts
- Detect Other DNS Related Anomalous Behavior
- Detect Rogue DHCP Servers
- Detect Slow DoS Attack
- Detect Zero-Day Attack
- Detect Attempt of Covering Tracks
- Detect VPN Connections from Countries that Don't Have an Organizational Presence
- Detect Attempt of Concurrent Establishment of VPN Connections
- Additional Useful SIEM Use Cases
 - Router and Switches Use Cases
 - ASA and Checkpoint Firewall Use Cases
 - Web Proxy Use Cases
 - Wireless/VPN Use Cases
 - Database Use Cases
 - Antivirus Use Cases
- Use Case Examples for Host Level Incident Detection
 - Windows
 - Typical Events to Look for in Windows
 - Monitor on Creation of Suspicious/Administrative Processes
 - Monitor for Logon Success and Failure Events
 - Monitor for File Shares
 - Monitor for Service Changes
 - Additional Useful SIEM Use Cases
 - List of Windows Security Audit Events
 - Linux
 - Monitor for Logon Success and Failures Events
 - Additional Useful SIEM Use Cases
- Use Case Examples for Compliance

- Compliance Relevant Use Cases
 - PCI-DSS
 - GDPR, HIPPA and SOX
- Handling Alert Triaging and Analysis
 - Alert Triage
 - Challenges in Handling Alert Triage
 - Effective Alert Triage
 - Triaging Alerts: Was this an actual attack?
 - Eliminating False Positives
 - Triaging Alerts: Has the Attack Been Successful?
 - Alert Classification and Prioritization
 - Escalation to IRT

Module 05: Enhanced Incident Detection with Threat Intelligence

- Understanding Cyber Threat Intelligence
 - Cyber Threat Intelligence (CTI)
 - Objectives of Threat Intelligence
 - Enhanced and automated incident prevention
 - Automation of security operations and remediation activities
 - Guidance to cyber security activities
 - Improved risk management
 - Improved incident detection
 - How can Threat Intelligence Help Organizations?
 - Types of Threat Intelligence
 - Strategic Threat Intelligence
 - Tactical Threat Intelligence
 - Operational Threat Intelligence
 - Threat Intelligence Strategy
 - Threat Intelligence Requirements Analysis
 - Intelligence and Collection Planning
 - Asset Identification
 - Threat Reports
 - Threat Trending
 - Intelligence Buy-In

- Threat Intelligence Sources
 - Open Source Intelligence (OSINT)
 - Human Intelligence
 - Counter Intelligence
 - Internal Intelligence
- Threat Intelligence Lifecycle
 - Planning and Direction
 - Collection
 - Processing and Exploitation
 - Analysis and Production
 - Dissemination and Integration
- Threat Analyst Roles in Threat Intelligence Lifecycle
- Cyber Threat Analyst Responsibilities
- Threat Intelligence Platform (TIP)
 - TC Complete™
- Additional Threat Intelligence Platforms
 - IBM X-Force Exchange
 - Pulsedive
 - FireEye iSIGHT Threat Intelligence
 - IntelMQ
 - RSA NetWitness Platform
 - DeepSight™ Intelligence
 - AlienVault® USM® Anywhere
 - LogRhythm TLM Platform
 - Splunk® Enterprise Security
 - Argos Threat Intelligence Platform
 - Malstrom
 - threat_note
 - RiskIQ
 - AutoFocus™
 - AbuseHelper
- Why Threat Intelligence-driven SOC?
 - Key Challenges in Traditional (Non Intelligence-driven) SOC

- Threat Intelligence-driven SOC
- How Threat Intelligence Helps SOC
- Benefits of CTI to SOC Team
- Benefit of Threat Intelligence to SOC Analyst
 - Tactical Threat Intelligence
 - Strategic Threat Intelligence
 - Operational Threat Intelligence
- Threat Intelligence Use Cases for SOC Analyst
 - Machine based prioritization
 - Incident alert and event triage
 - Analysis and validation
- How Threat Intelligence can help SOC Analyst
- Threat Intelligence Use Cases in SOC
 - Alarms, Events and Alerts Prioritization
 - Incident Response
 - Assists in Investigation and Mitigation
 - Fusion Analysis
- Integration of Threat Intelligence into SIEM
- Threat Intelligence Use Cases for Enhanced Incident Response
 - Phases of escalation involved in the incident response management
 - Phase 1: Pre-Planning
 - Phase 2: Event
 - Phase 3: Incident
 - Phase 4: Breach
- Enhancing Incident Response by Establishing SOPs for Threat Intelligence

Module 06: Incident Response

- Incident Response
- Incident Response Team (IRT)
- Where Does IRT Fits in the Organization?
- SOC and IRT Collaboration
- Incident Response (IR) Process Overview
- Step 1: Preparation for Incident Response
 - Process Flow of Preparation for Incident Response

- Determine the Need for IR Processes
- Define IR Vision and Mission
- Management Approvals and Funding
- Develop IR Plan
- Develop IR Policy
- Develop IR Procedures
- Define Incident Response Criteria
- Build IR Team
- Develop Incident Readiness Procedures
- Build Incident Response Toolkit
- Setting Up a Computer Forensics Lab
- Establish Reporting Facilities
- Establish Structured Record Keeping Facilities
- Evaluate the Current Security Posture
- Implement Security Policy, Procedures, and Awareness
- Implement Security Controls
- Implement Successful Backup Strategy
- Have a Cyber Insurance
- **Step 2: Incident Recording and Assignment**
 - Process Flow of Incident Recording and Assignment
 - Ticketing System
- **Step 3: Incident Triage**
 - Process Flow of Incident Triage
 - Incident Analysis and Validation
 - Incident Classification
 - Severity Assessment
 - Risk/Impact Assessment
 - Risk Matrix
 - Incident Prioritization
 - Incident Prioritization Approaches
 - Incident Prioritization Categories
 - Best Practices for Incident Classification and Prioritization
- **Step 4: Notification**

- Communicating Incident
- Point of Contact
- Details to Notify
- Incident Notification Form
- **Step 5: Containment**
 - Containment
 - Guidelines for Incident Containment
- **Step 6: Evidence Gathering and Forensic Analysis**
 - Evidence Gathering and Forensics Analysis
 - Evidence Handling
- **Step 7: Eradication**
 - Process Flow of Eradication
- **Step 8: Recovery**
 - Process Flow of Recovery
 - Systems Recovery
- **Step 9: Post-Incident Activities**
 - Process Flow of Post-Incident Activities
 - Incident Documentation
 - Report Writing Tools
 - Magic Tree
 - KeepNote
 - Incident Impact Assessment
 - Review and Revise Policies
 - Training and Awareness
 - Close the Investigation
 - Incident Disclosure
 - Incident Disclosure Procedure
- **Responding to Network Security Incidents**
 - Containment of Unauthorized Access Incidents
 - Eradication of Unauthorized Access Incidents
 - Physical Security Measures
 - Authentication and Authorization Measures
 - Host Security Measures

- Network Security Measures
- Recovery after Unauthorized Access Incidents
- Containment of Inappropriate Usage Incidents
- Eradication of Inappropriate Usage Incidents
- Recovery after Inappropriate Usage Incidents
- Containment of DoS/DDoS Incidents
- Eradicating DoS/DDoS Incidents
 - Blocking Potential Attacks
 - Disabling Botnets
 - Neutralizing Handlers
- Recovery after DoS/DDoS Incidents
- Responding to Application Security Incidents
 - Containment of Application Security Incidents
 - Containment Methods
 - Whitelisting/Blacklisting
 - Web Content Filtering
 - Proxy Servers
 - Containment Tools
 - Whitelisting/Blacklisting Tools
 - Web Content Filtering Tools
 - Web Proxy Tools
 - How to Eradicate Web Application Security Incidents?
 - Eradicating Injection Attacks
 - SQL Injection Attacks
 - Command Injection Attacks
 - File Injection Attacks
 - LDAP Injection Attacks
 - Eradicating Broken Authentication and Session Management Attacks
 - Eradicating Sensitive Data Exposure Attacks
 - Eradicating Broken Access Control Attacks
 - Eradicating Security Misconfiguration Attacks
 - Eradicating XSS Attacks
 - Eradicating Insecure Deserialization Attacks

- Eradicating Attacks due to Known Vulnerabilities in Components
- Eradicating Insufficient Logging and Monitoring Attacks
- Eradicating Web Services Attacks
- Eradicating CAPTCHA Attacks
- Eradicating other Web Application Attacks
 - Directory Traversal Attacks
 - Unvalidated Redirect and Forward Attacks
 - Watering Hole Attacks
 - Cross-Site Request Forgery Attacks
 - Cookie/Session Poisoning Attacks
- Implement Encoding Schemes
 - URL Encoding
 - HTML Encoding
 - Unicode Encoding
 - Base64 Encoding
 - Hex Encoding
- Eradicate XSS Attacks using HTML Encoding
- Eradicate SQL Injection Attacks using Hex Encoding
- Recovery from Web Application Incidents
- Tools to Recover from Web Application Incidents
 - ApexSQL Log
 - CrowdStrike Falcon™ Orchestrator
- Responding to Email Security Incidents
 - Containing Emails Incidents
 - Eradicating Email Attacks
 - Recovery Steps to Follow after Email Incidents
 - Recovery of Deleted Emails
 - Gmail
 - Outlook PST
- Responding to an Insider Incidents
 - Containment of Insider Threats
 - Eradicating Insider Threats
 - Human Resources

- Network Security
- Access Controls
- Privileged Users
- Audit Trails and Log Monitoring
- Physical Security
- Recovering from Insider Attacks
- Responding to Malware incidents
 - Containment of Malware Incidents
 - Eradication of Malware Incidents
 - Recovery after Malware Incidents