Details Course Outlines

Module-01

Cisco Cyber Ops Introduction

- ☑ Introduction
- ☑ Kali Linux

Module-02

Network Concepts

- ☑ Network Fundamentals
- ☑ Network Protocols - ICMP
- ☑ Network Protocols - ARP
- ☑ Network Protocols - DHCP
- ☑ Network Protocols - DNS
- ☑ Network Devices
- ☑ Firewalls
- ☑ IPS & AMP
- ☑ Email & Web Security
- ☑ Inline Traffic Interrogation, Taps & NetFlow
- ☑ Network Concepts

Module-03

Security Concepts

- ☑ CIA Triad
- ☑ Defense in Depth Strategy
- ☑ Vulnerabilities
- ☑ Exploits & Risks
- ☑ Security Terms & Access Control Models
- ☑ Threat Hunting
- ☑ Zero Trust
- ☑ Threat intelligence platform (TIP)
- ☑ Authentication, Authorization, Accounting
- ☑ Rule-based, Time-based & Role-based Access Control
- ☑ CVSS 3.0 & 5-tuple
- ☑ Rule-based detection vs. Behavioral and Statistical detection
- ☑ Rule-based, Time-based & Role-based Access Control

Module-04

Security Monitoring

- ☑ Attack Surface Analysis
- ☑ Network Attacks
- ☑ Web Application Attacks
- ☑ Endpoint-Based Attacks
- ☑ Social Engineering and Phishing Attacks
- ☑ Evasion Methods
- ☑ Network Logging & Packet Captures
- ☑ NetFlow & Application Visibility and Control (AVC)
- ☑ Monitoring Challenges
- ☑ NextGen IPS Event Types
- ☑ Encryption and Hashing
- ☑ PKI

Module -05

Host-Based Analysis

- ☑ Microsoft Windows - Introduction
- ☑ Microsoft Windows - Terms
- ☑ Microsoft Windows File System
- ☑ Linux - Introduction
- ☑ Linux - Terms
- ☑ Linux File System
- ☑ Endpoint Protection
- ☑ Whitelisting and Blacklisting
- ☑ Systems-Based Sandboxing
- ☑ System Logs
- ☑ Indicators of Compromise and Attack
- ☑ Evidence and Attribution

Module -06

Network Intrusion Analysis

- ☑ Common Artifact Elements and Protocol Headers
- ☑ Security Analysis with Wireshark
- ☑ NetFlow v5 and Security Events
- ☑ Map Events to Source Technologies
- ☑ Impact Flags with the Firepower Management Center (FMC)
- ☑ Interpret Basic Regular Expressions
- ☑ Application Layer Protocols (SMTP/POP3/IMAP/HTTP/HTTPS/HTTP2)

Module -07

Security Policies and Procedures

- ☑ Security Management
- ☑ NIST.SP800-61 r2
- ☑ Apply the incident handling process (such as NIST.SP800-61) to an event
- ☑ CSIRT & Network Profiling
- ☑ PCI & Server Profiling
- ☑ HIPAA & SOX
- ☑ PSI & Intellectual Property
- ☑ SOC Metrics
- ☑ Cyber Kill Chain Model