

TOC - Network Security and SOC(CBROPS)

Day 1 – Security Operations Center (SOC) Fundamentals

Topics

Course Introduction

Section 1: Defining the Security Operations Center

Section 2: Understanding SOC Metrics

Section 3: Understanding SOC Workflow and Automation

Section 4: Understanding Endpoint Security Technologies

Lab 1: Explore Endpoint Security

Day 2 – Network Security and Data Protection

Topics

Section 5: Understanding Network Infrastructure and Network Security Monitoring Tools

Section 6: Understanding Common TCP/IP Attacks

Section 7: Exploring Data Type Categories

Section 8: Understanding Basic Cryptography Concepts

Labs

Lab 2: Explore TCP/IP Attacks

Lab 3: Use NSM Tools to Analyze Data Categories

Lab 4: Explore Cryptographic Technologies

Day 3 – Cloud Security and Threat Analysis

Topics

Section 9: Cloud Security Fundamentals

Section 10: Securing Cloud Deployments

Section 11: Understanding Incident Analysis in a Threat-Centric SOC

Section 12: Identifying Common Attack Vectors

Labs

Lab 5: Investigate Hacker Methodology

Day 4 – Threat Detection and Security Monitoring

Topics

Section 12: Identifying Common Attack Vectors (Continued)

Section 13: Identifying Malicious Activity

Section 14: Identifying Patterns of Suspicious Behavior

Labs

Lab 6: Investigate Browser-Based Attacks

Lab 7: Analyze Suspicious DNS Activity

Lab 8: Explore Security Data for Analysis

Lab 9: Investigate Suspicious Activity Using Security Onion

Day 5 – Threat Hunting and Event Correlation

Topics

Section 15: Identifying Resources for Hunting Cyber Threats

Section 16: Understanding Event Correlation and Normalization

Labs

Lab 10: Hunt Malicious Traffic

Lab 11: Cisco XDR to Splunk Enterprise Integration Simulation

Lab 12: Correlate Event Logs, PCAPs, and Alerts of an Attack

Day 6 – Incident Response and SOC Operations

Topics

Section 17: Conducting Security Incident Investigations

Section 18: Using a Playbook Model to Organize Security Monitoring

Labs

Lab 13: Investigate Advanced Persistent Threats (APT)

Lab 14: Explore SOC Playbooks