Cisco Certified CyberOps Associate

Course Outline

- SOC Overview
- Defining the Security Operations Center
- Understanding NSM Tools and Data
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Security Incident Investigations
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations
- SOC Operations
- Describing the SOC Playbook
- Understanding the SOC Metrics
- Understanding the SOC WMS and Automation
- Describing the Incident Response Plan

Lab outline

- Explore Network Security Monitoring Tools
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious DNS Activity
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks