Course Content

- Describing the Security Operations Center
- Understanding Network Security Monitoring Tools and Data
- Understanding Incident Analysis in a Threat-Centric SOC
- Identifying Resources for Hunting Cyber Threats
- Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior
- Conducting Security Incident Investigations
- Describing the SOC Playbook and Metrics
- Understanding the SOC Workflow Management System (WMS) and Automation
- Describing the Incident Response Plan
- Describing the Computer Security Incident Response Team