Course Title: SOC Analyst 101

Duration: 46 hours, 23 lessons

Cybersecurity SOC101.1: Overview of SOC and Tools

- Blue Team Mission
- SOC Overview
- Network Defense Concepts
- Events and Alerts
- Anomalies and Incidents
- Incident Management
- Threat Intelligence
- SIEM: Building them and Using Them
- Automation and Orchestration
- Identifying Threats

Cybersecurity SOC101.2: The Network

- Corporate Network Architecture
- Traffic Capture and Analysis
- Understanding DNS
- DNS attacks and analysis
- Understanding modern HTTP(S)
- Analyzing HTTP(S)
- SMTP and Email
- Daily Protocols

Cybersecurity SOC101.3: Logging, Endpoints and Filesystems

- Endpoint Attacks
- Defending an Endpoint
- Windows Logging
- Linux/Unix Logging
- Understanding Events
- Collection, Parsing and Normalization
- Files and File Systems

Cybersecurity SOC101.4: Analysis

- Understanding Alerts
- Mental Models for InfoSec
- Analysis Techniques
- Analysis Questions and Tactics
- OPSEC!
- Intrusion Discovery
- Incident Closing and Review

Cybersecurity SOC101.5: Analytics and Automation

- SOC++
- Applying Analytics on Logs
- Analytics Design, Testing and Sharing
- Tuning
- Automation and Orchestration
- Operational Automation, Workflow and Playbooks