SOC Analyst 10 hours of content | 100 hours of practice | Exam

1. Introduction to Windows Environments

- Inroduction to virtualization
- VirtualBox Installation
- Virtualization Networking
- Deploy a virtual machine
- Windows Server2016 installation
- Domain Controller
- DC Pre configurations
- AD DS installation on DC
- Windows 10 Client installation
- Virtualization and Windows10 client
- Client domain join
- DHCP Service
- DHCP deployment
- IP ranges
- IP Reservations
- DNS record types
- DNS Zones
- Creating and managing domain users
- Creatubg and managing domain groups
- Creating and managing GPO's

2. Fundamentals of Defense

- CIA Triad
- Risk Consideration
- Identity Threats
- Risk Assessment
- Risk Control
- AAA Security
- Hashing
- Cryptography And Encryption
- Web Security
- Malwares

3. Introduction to the Attacker's Perspective

- Layer ll cyber attacks
- Layer lll cyber attacks
- Various cyber attacks types
- Cyber Kill Chain
- IOC's

4. SIEM/SOC Fundamentals

- Organization Monitoring
- SOC Fundamentals
- The Adaptive Security Architectures
- Cyber Security Components And Vendors
- SIEM Introduction
- Qradar SIEM Introdoction
- WinCollect Installtion
- Windows Audit

5. Qradar SIEM Hands-on

- Qradar Log Activity
- Qradar Log Source
- Qradar Console
- Qradar DSM&Parsing
- Qradar Building Block
- Qradar Rules
- Qradar Reference Lists

6. Forensics, Threat intelligence & SOAR

- Qradar Log Activity
- Windows sysinternals
- Windows Sysmon
- Cyber Attack Summary
- Log Analysis
- Threat Intelligence
- SOAR Concept

7. SOC Analyst - Labs

- Lab 1:
  - IBM Wincollect Installation On Dedicated Server
- Lab 2:
  - Qradar - Custom Log Activity
- Lab 3:
  - Qradar - Parsing Fields From Payload
- Lab 4:
  - Qradar - Custom Building Block
- Lab 5:
  - Qradar - Custom Rules
- Lab 6:
  - Qradar - Reference Lists
- Lab 7:
  - Sysmon
- Lab 8:
  - Find The Suspicious Log
- Lab 9:
  - Threat intelligence With Qradar