Security Operations Center (SOC) Analyst Syllabus

Introduction to Security Operations Center (SOC)	2 Hours

- Overview of SOC functions and responsibilities (Day 1)
- Understanding the SOC analyst role (Day 1)
- Introduction to the incident response lifecycle (Day 1)

Cyber Threat Landscape	2 Hours

- Overview of common cyber threats and attack vectors (Day 2)
- Understanding threat actors and their motivations (Day 2)
- Current trends in cyber attacks (Day 2)

Security Event Monitoring and Analysis	4 Hours

- Introduction to security event monitoring and log analysis (Day 3 & 4)
- Common security event sources (logs, network traffic, system alerts) (Day 3 & 4)
- Log analysis techniques and tools (Day 3 & 4)

Security Incident Detection and Classification	2 Hours

- Techniques for detecting security incidents (Day 5)
- Incident classification and severity levels (Day 5)
- Establishing incident response priorities (Day 5)

Security Incident Response Procedures	2 Hours

- Incident response planning and frameworks (e.g., NIST, ISO 27035) (Day 6)
- Incident response roles and responsibilities (Day 6)
- Incident containment and eradication strategies (Day 6)

Threat Intelligence and Threat Hunting	2 Hours

- Introduction to threat intelligence (Day 7)
- Threat hunting methodologies and tools (Day 7)
- Leveraging threat intelligence in SOC operations (Day 7)

Vulnerability Management and Patching	2 Hours

- Overview of vulnerability management processes (Day 8)
- Prioritizing and remediating vulnerabilities (Day 8)
- Patch management best practices (Day 8)

Security Incident Investigation	2 Hours

- Techniques for investigating security incidents (Day 9)
- Digital forensics fundamentals (Day 9)
- Preserving and analyzing digital evidence (Day 9)

Security Incident Reporting and Communication	2 Hours

- **Creating incident reports and documenting findings (Day 10)**
- **Communication strategies for different stakeholders (Day 10)**
- **Presenting incident analysis and recommendations (Day 10)**