2-Month SOC Analyst Training

Week 1: SOC Fundamentals & Environment Setup

- **SOC Architecture & Analyst Roles**

Lab: Set up virtual lab (VirtualBox, Ubuntu, Windows 10 VMs)

- **Cyber Kill Chain & Attack Lifecycle**

Lab: Map 5 real-world attack scenarios to Kill Chain phases

- **MITRE ATT&CK Framework**

Lab: Navigate ATT&CK Matrix, identify 10 techniques, map to APT groups

- **Log Fundamentals**

Lab: Analyze Windows Event Logs, identify logon events (4624, 4625)

- **Linux Log Analysis**

Lab: Analyze /var/log/auth.log, identify failed SSH attempts

Week 2: SIEM Foundations & Log Ingestion

- **SIEM Concepts**

Lab: Install Elastic Stack (Elasticsearch, Kibana, Beats)

- **Log Ingestion - Windows**

Lab: Configure Winlogbeat, ingest Security logs to Elastic

- **Log Ingestion - Linux**

Lab: Configure Filebeat, ingest auth.log and syslog

- **Sysmon Deployment**

Lab: Install Sysmon with SwiftOnSecurity config, ingest to Elastic

- **Basic Kibana Dashboards**

Lab: Create 3 dashboards (Logon Activity, Failed Auth, Process Creation)

Week 3: Alert Triage & Investigation Workflow

- **Alert Triage Methodology**

Lab: Create detection rule for multiple failed logon attempts

- **Investigating Failed Logons**

Lab: Simulate brute force attack, investigate in SIEM

- **Process Creation Analysis**

Lab: Analyze Sysmon Event ID 1, identify malicious PowerShell

- **False Positive Handling**

Lab: Review 10 alerts, classify as TP/FP/Benign, tune rules

- **Incident Documentation**

Lab: Write formal incident report for brute force investigation

---

Week 4: Network Traffic Analysis & Threat Intelligence

- **Network Fundamentals for SOC**

Lab: Capture traffic with Wireshark, filter HTTP/DNS/SMB

- **Malicious Traffic Detection**

Lab: Analyze PCAP with malware traffic, identify C2

- **Threat Intelligence Basics**

Lab: Investigate 5 suspicious IPs with VirusTotal, AbuseIPDB, OTX

- **Firewall Log Analysis**

Lab: Analyze firewall logs, identify port scanning and anomalies

- **DNS Analysis**

Lab: Analyze DNS logs, detect high-entropy domains, DGA detection

Week 5: Email Security & Phishing Analysis

- **Email Security Fundamentals**

Lab: Analyze 5 email headers, identify sender spoofing

- **Phishing Detection**

Lab: Investigate 3 phishing emails, extract IOCs

- **SPF, DKIM, DMARC**

Lab: Check DMARC/SPF/DKIM records for 10 domains

- **Malicious Attachments**

Lab: Analyze malicious Office document, identify macros

- **Email Alert Triage**

Lab: Simulate email security alert, investigate mailbox logs

Week 6: Endpoint Detection & Response + Malware Basics

- **EDR Fundamentals**

Lab: Configure Wazuh agent on endpoints, ingest EDR telemetry

- **Suspicious Process Investigation**

Lab: Investigate PowerShell/WMI/PsExec in Sysmon logs

- **File Reputation Analysis**

Lab: Extract file hashes, check reputation in VirusTotal

- **Malware Behavior Analysis**

Lab: Analyze 2 sandbox reports, extract TTPs and IOCs

- **Persistence Mechanisms**

Lab: Hunt for persistence in Windows registry using Sysmon

Week 7: Web Attacks, Insider Threats & Advanced Detection

- **Web Attack Detection**

Lab: Analyze web server logs, detect SQL injection and scanning

- **Insider Threat Indicators**

Lab: Create detection rules for data exfiltration, off-hours access

- **Cloud Log Analysis (Intro)**

Lab: Analyze sample cloud logs, identify unauthorized access

- **SOAR & Case Management**

Lab: Install TheHive, create cases for previous investigations

- **Advanced Correlation Rules**

Lab: Create detection rule for credential dumping + lateral movement

---

Week 8: Capstone Project & Interview Preparation

- **Capstone: Environment Setup**

Lab: Deploy target VMs, configure logging, ingest to SIEM

- **Capstone: Attack Execution**

Lab: Execute simulated attack chain (Phishing → Exfiltration)

- **Capstone: Detection & Investigation**

Lab: Monitor SIEM, triage alerts, investigate each stage

- **Capstone: Incident Response**

Lab: Create timeline, map to ATT&CK, write incident report

- **Mock Interviews & Presentation**

Lab: Present capstone findings, conduct 2 mock interviews