Forebrain — SOC Analyst & Incident Response (3 Months / 12 Weeks)

Duration: 3 Months (12 Weeks / 60 instructional days)

Format: 1 hour class + 1 hour lab practice (Monday–Friday)

Focus: Building practical SOC analysts capable of detection, investigation, and incident response.

Outcome: Job-ready skills in SIEM operations, detection engineering, threat hunting, and IR playbooks.

Phase 1 — Foundations & Log Collection (Weeks 1–3)

- Introduction to SOC, roles, tiers (L1–L3) and workflows

- Log sources: Windows Event Logs, Sysmon, Linux logs, network PCAPs, cloud telemetry

- Log forwarding: Syslog, Filebeat, Winlogbeat, and Windows Event Forwarding

- ELK Stack and Splunk basics — log ingestion, field extraction, indexing

- Log normalization and parsing using KQL, SPL, and Lucene syntax

- Practical lab: Collect host logs and build basic Splunk/Kibana dashboards

Deliverable: Working log ingestion setup + dashboard visualization

Phase 2 — Detection Engineering & Threat Signatures (Weeks 4–6)

- Threat modeling for detection using MITRE ATT&CK mapping

- Creating Sigma rules and converting to SIEM queries (SPL/KQL)

- YARA rules for malware detection and tuning

- Configuring alert thresholds and false positive reduction techniques

- Intrusion Detection Systems: Zeek and Suricata overview and rule creation

- Lab: Implement custom Sigma rule and verify alert triggers in ELK/Splunk

Deliverable: Detection rule pack + alert configuration report

Phase 3 — Threat Hunting & Endpoint Forensics (Weeks 7–9)

- Threat hunting methodologies: hypothesis generation and investigation
- Host forensics using Sysinternals Suite, Volatility, and FTK Imager
- Disk and memory forensics using Autopsy and Volatility framework
- IOC enrichment: VirusTotal, MISP, and open-source threat intel feeds
- Endpoint telemetry using Sysmon and event ID mapping for attacks
- Lab: Conduct a threat hunt for credential dumping and correlate artifacts

Deliverable: Threat hunting report + IOC summary with screenshots

Phase 4 — Incident Response Operations & SOC Maturity (Weeks 10–12)

- Incident Response lifecycle: preparation, detection, analysis, containment, recovery
- Developing playbooks for ransomware, data breaches, and insider threats
- Artifact collection and maintaining chain-of-custody for investigations
- SOAR (Security Orchestration, Automation, and Response) fundamentals
- SOC reporting metrics: MTTD, MTTR, and incident KPIs for SOC maturity
- Capstone: End-to-end incident simulation (red/blue team IR drill)

Deliverable: Final IR Playbook + SOC metrics dashboard + Incident Report

Tools & Technologies Covered

SIEM / Log Management:

- ELK Stack (Elasticsearch, Logstash, Kibana)
- Splunk Enterprise / Free

Log Collection:

- Filebeat
- Winlogbeat
- Syslog

- Windows Event Forwarding

Network & IDS:

- Zeek (Bro)
- Suricata
- Wireshark
- tcpdump

Forensics:

- Volatility
- Autopsy
- FTK Imager

Detection & Hunting:

- Sigma
- YARA
- Sysmon
- Sigma2Splunk/KQL tools

Threat Intel & Automation:

- MISP
- VirusTotal
- OpenCTI
- Python scripts for enrichment

SOC Operations:

- SOAR concept tools
- Git
- Markdown
- Jupyter Notebooks

Forebrain — SOC Analyst & Incident Response (3-Month Syllabus)

Deliverables & Assessments

- Weekly lab exercises and dashboards

- Detection engineering rule pack (Sigma/YARA)

- Threat hunting investigation report

- Incident Response playbook and final IR report

- Capstone simulation report with SOC metrics