Forebrain — Blue Team Operations & Threat Hunting (3 Months / 12 Weeks)

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

Format: 1 hour class + 1 hour lab practice (Monday–Friday). Saturday = Activity Day (practical session based on weekly topics).

Focus: Building SOC and Threat Hunting expertise, mastering SIEM tools, incident response workflows, and real-time detection engineering.

Outcome: Students will perform full SOC operations, create custom detections, conduct threat hunts, and complete an enterprise-grade capstone investigation.

Phase 1 — SOC Foundations & Log Analysis (Weeks 1–3)

- Introduction to Blue Teaming, SOC structure, and defensive security mindset

- Understanding SOC tiers, analyst responsibilities, and alert lifecycles

- Windows and Linux log sources — Sysmon, Event Viewer, journalctl

- Parsing and analyzing logs using ELK Stack and Wazuh

- SIEM basics: log ingestion, normalization, correlation, and alerting

- Hands-on setup of Wazuh and Elastic for monitoring

- Log source integration: Sysmon, Zeek, and Suricata

- MITRE ATT&CK Framework introduction and mapping detection rules

Deliverable: Configured SIEM environment with live data sources and mapped ATT&CK detections

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

- Threat hunting fundamentals and hypothesis creation

- Data enrichment and correlation with KQL and Sigma rules

- Custom rule creation in Wazuh and Splunk (Use Case Development)

- Identifying attacker techniques: process injection, credential dumping, lateral movement

- Automated alert generation using MITRE mapping and correlation rules

- Threat hunting using Sysmon logs, Zeek traffic, and event correlation

- Hunting adversary behavior using Atomic Red Team and Caldera simulations

Deliverable: Custom detection rules and hunt reports mapped to MITRE ATT&CK techniques

Phase 3 — Incident Response & Threat Intelligence (Weeks 7–9)

- Incident response lifecycle: identification, containment, eradication, recovery

- Forensic triage using Velociraptor, OSQuery, and Volatility

- Threat intelligence sources: MISP, OpenCTI, VirusTotal, and Intel sharing

- Automated enrichment using Cortex analyzers and TheHive integration

- Use case: correlating phishing attack or malware infection in SIEM

- Building IR playbooks and runbooks for SOC automation

- Reporting and escalation workflows for SOC incidents

Deliverable: End-to-end incident report and IOC enrichment workflow using MISP and Cortex

Phase 4 — Advanced Threat Hunting & Capstone (Weeks 10–12)

- Advanced hunting using ELK queries, Sigma conversions, and visualization

- Behavioral detection engineering and false positive tuning

- Threat actor profiling and tracking TTPs across data sources

- Correlation of endpoint and network telemetry for detection chaining

- Automation with Python scripts for log parsing and IOC correlation

- Capstone project: Enterprise Threat Hunting Simulation & Investigation

- Final presentation, peer review, and blue team readiness assessment

Deliverable: Full SOC investigation with report, IOC mapping, and incident timeline reconstruction

Tools & Technologies Covered

SIEM & Log Management:

- Splunk
- Wazuh
- ELK Stack (Elasticsearch, Logstash, Kibana)
- IBM QRadar (overview)

Threat Hunting & Detection:

- Sysmon
- Velociraptor
- Zeek
- Suricata
- Sigma
- KQL

Incident Response & Forensics:

- TheHive
- Cortex
- OSQuery
- GRR
- Volatility

Threat Intelligence:

- MISP
- OpenCTI
- MITRE ATT&CK Navigator
- VirusTotal

Automation & Scripting:

- Python

- Sigma2ELK
- PowerShell scripts
- Log ingestion parsers

Lab Setup Requirements

- Virtualized SOC lab environment (VMware/VirtualBox)
- Windows 10 + Sysmon logging machine
- Ubuntu Server with Wazuh/ELK installation
- Zeek and Suricata network traffic monitoring nodes
- TheHive + Cortex stack for case management and enrichment
- Simulated attack datasets (Atomic Red Team, Caldera, and Red Canary telemetry)
- Sample malware and phishing logs for incident simulation

Deliverables & Assessment

- Phase-wise SOC lab exercises and hunt reports
- Custom detection rules and correlation dashboards
- Incident Response reports and IOC analysis
- Final Capstone: Enterprise Threat Hunting Simulation
- Professional SOC report presentation and assessment