// CADRE 1

BLUEGUARDIA

SOC Analyst Training Syllabus

14-Week Practitioner Program · Theory + Hands-On Labs · Job-Ready Outcomes

SECTION 1 — FOUNDATION & THEORY | WEEKS 1 – 4

Week 1 · Basic Knowledge & Organizational Context

- Infrastructure of an organization and roles of different departments
- Role of cybersecurity in an organization
- Information security vs cybersecurity
- Market job trends for cybersecurity
- Security awareness for employees
- Basics of computer hardware & software
- Basics of the Internet (WWW, DNS, HTTP/HTTPS, client-server model)

Week 2 · Cybersecurity Fundamentals

- Different domains of cybersecurity
  - SOC (Security Operations Center)
  - DFIR (Digital Forensics & Incident Response)
  - Penetration Testing
  - GRC (Governance, Risk & Compliance)
- CIA Triad (Confidentiality, Integrity, Availability)
- AAA (Authentication, Authorization, Accounting)
- Types of attackers (insiders, outsiders, hacktivists, etc.)
- Common attacks (brute force, DoS/DDoS, MITM, ransomware, etc.)
- Malware types (virus, worm, trojan, spyware, ransomware)
- Phishing & spear phishing
- Social engineering
- Encryption fundamentals
- Hashing & integrity checks

Week 3 · Operating Systems Fundamentals

- Windows & Linux basics
- User accounts, permissions, authentication mechanisms
- Domains vs Workgroups
- File system basics
- Command-line basics (Windows CMD, Linux Shell)

Week 4 · Networking Fundamentals

- IP Addressing (IPv4 & IPv6 basics)
- MAC Address
- Routers & Switches
- VLANs
- Subnets & subnetting
- LAN vs WAN
- TCP/IP model
- OSI model
- Common ports & services
- Protocols (HTTP/S, FTP, DNS, SMTP, SSH, etc.)
- Firewalls
- Proxies
- IDS/IPS basics
- VPNs (concepts & usage)

SECTION 2 — All About SOC | WEEKS 5 – 12

Different Job Roles in SOC

- Analyst Role — L1, L2, L3
- SOC Manager
- SOC / SIEM Engineer
- Incident Responders
- Threat Hunter

Responsibilities of Different Job Roles

- Threat Intelligence (Overview)
- L1 Analyst Role
- L2 Analyst Role
- L3 Analyst Role
- SOC Manager
- SOC SIEM Engineer
- Threat Hunter (Overview)

Types of SOC Environments

- In-house SOC
- Outsourced SOC
- Hybrid SOC

Day-to-Day Terminologies Used in SOC

- Logs · Incident · Events · Log Source
- APT · Advisories
- Exploit Chain / Kill Chain
- False Positive / False Negative

- Proof of Concept (PoC) · Zero-Day
- Privilege Escalation · Lateral Movement

MITRE ATT&CK Framework (Overview)

- What is MITRE ATT&CK and why it matters in SOC
- Tactics, Techniques & Procedures (TTPs) — high-level understanding
- Mapping alerts and incidents to ATT&CK techniques

Technologies You Should Be Aware Of

- Active Directory
- Proxies
- Email Gateways
- Web Gateways
- Exchange Servers

Tools Used in SOC

- SIEM · EDR · SOAR
- TI Platforms · WAF
- Firewalls · IPS/IDS · NDR
- EPP / Antivirus · FIM
- IAM · PAM

Environment Setup

- Creating VMs for Linux and Windows

SIEM — Wazuh Environment

- Setting up Wazuh (SIEM)
  - Log collection
  - Creating detection rules
  - Creating use-cases
  - Understanding detection rules
  - Investigate security alerts
  - 5 Ws (What, When, Why, Who, Where)
  - Incident Response Lifecycle

SIEM — Elastic (Alternative to Wazuh)

- Setting up Elastic SIEM
  - Log ingestion & index management
  - Kibana dashboards & alert investigation

Phishing Analysis Lab

- Analyzing phishing email headers
- Identifying malicious URLs & attachments
- Spear phishing vs generic phishing — case studies
- Triaging & escalating phishing alerts in the SIEM

Threat Hunting & Threat Intelligence (Overview)

- What is threat hunting and how it differs from alert monitoring
- Using threat intelligence feeds to enrich investigations (OSINT, IOCs)

Incident Reporting

- Structure of a SOC incident report
- Writing clear, concise incident summaries
- Escalation communication — what to include when handing off to L2/L3
- Hands-on: Writing a mock incident report from a lab scenario

EDR — OpenEDR

- Setting up OpenEDR
  - Looking into how EDR works
  - Purpose of using EDR
  - EDR vs XDR

SECTION 3 — JOB-READY PROFILE | WEEKS 13 – 14

Building Your Professional Presence

- Setting up LinkedIn Profile

- Dos and Don'ts
- Preparing a job-ready resume
- Preparation for interviews

BONUS ITEMS

★ Collection of questions asked during interviews

★ Meet with industry experts with extensive real-world experience

★ Live Q&A session with industry experts

TRAIN THE TALENT · BUILD THE FIRM · DEFEND THE INDUSTRY