K7 ACADEMY

SOC Foundation Programme

Overview

The SOC Foundation Programme is designed for beginners and early-career professionals who wish to build a solid foundation in Security Operations. This hands-on programme covers cybersecurity fundamentals, networking, OS internals, threat detection, SIEM concepts, and incident response basics – preparing you for a Tier 1 SOC Analyst role.

Mode	Duration	Level
Online/Offline Classes	24 Hours	Beginner to Intermediate

Who Should Enrol?

- Freshers & Cybersecurity Students seeking a structured entry point
- IT Professionals transitioning into cybersecurity
- Network/System Administrators wanting security skills
- Help Desk/Support Engineers aiming for SOC roles

Learning Outcomes

- Explain core cybersecurity concepts: CIA Triad, threat types, and attack vectors
- Navigate and analyse Windows & Linux OS environments from a security perspective
- Understand networking fundamentals and read packet captures using Wireshark
- Map attacker behaviour to the MITRE ATT&CK Framework and Cyber Kill Chain
- Perform basic malware identification using sandboxes (ANY.RUN) and VirusTotal
- Understand SIEM concepts, log sources, and alert triage methodology
- Conduct phishing email header analysis
- Complete a full attack mapping exercise and write a basic incident report

Modules

Module 1 – Cybersecurity & IT Fundamentals

- Understanding Cybersecurity
- CIA Triad (Confidentiality, Integrity, Availability)
- Types of Threats & Attackers
- How the Internet Works
- Common Attack Terminology
- Cybersecurity Career Paths
- Lab Environment Setup (VirtualBox + Kali Linux)
- SOC Roles & Responsibilities – L1/L2/L3 Analyst structure
- Blue Team vs Red Team vs Purple Team – overview for beginners
- Cybersecurity domains overview (Network, Cloud, App, Endpoint, IR)

Module 2 – Operating System Basics

- Understanding Windows OS
- Process, Thread & DLL
- Essential Tools & PowerShell
- Event Viewer
- Identity & Access Management: AD, MFA, Zero Trust
- Securing access with permissions
- Audit Policies & Network Auditing
- Linux Distributions & Connecting
- Using essential Linux tools
- Files, directories, and text files
- Bash Shell basics
- Managing Users & Permissions
- Managing Processes & syslogs
- Windows Critical Event IDs for SOC (4624, 4625, 4688, 4698, 4732...)
- Linux /var/log analysis: auth.log, syslog, secure – SOC triage focus

Module 3 – Networking Fundamentals

- MAC Addresses & IPv4/IPv6
- Hubs, Switches & Routers
- Ethernet 101
- HTTP, HTTPS, SSL & TLS
- TCP/IP Suite
- Ports & Protocols
- DNS System
- Network Tools (ping, traceroute, nmap, etc.)
- Network Security & Logs
- Firewall & VPN
- Cloud Networking Basics
- Wireshark Basics — reading PCAP, filtering, identifying anomalies
- Common Attack Protocols: DNS Tunnelling, C2 over HTTP/HTTPS

Module 4 – Core Cybersecurity Concepts

- Control Objective & Security Controls
- Fundamental Security Concepts & CIA Triad
- Change Management & Security Impact
- Cryptographic Solutions
- Threats, Vulnerabilities & Mitigations
- Common Threat Vectors & Attack Surfaces
- Types of Vulnerabilities & Management
- Mitigation Techniques & Secure Design
- MITRE ATT&CK Framework Basics – Tactics, Techniques, Sub-techniques
- Cyber Kill Chain – mapping attacker stages to SOC defender actions

Module 5 – Security Tools, Malware & Incident Response Basics

- Malware Types, Kill Chain & IOC Concepts
- Static vs Dynamic Analysis – Introduction
- ANY.RUN Sandbox Analysis Lab
- VirusTotal & MalwareBazaar – quick hash/file reputation lookup
- NIST IR Lifecycle: Prepare, Detect, Contain, Recover
- SIEM Concepts: Log Sources, Correlation, Alert Triage
- Alert Triage Methodology – False Positive vs True Positive decision workflow
- Phishing Email Analysis Basics – Headers, URL analysis, Attachment Indicators

Module 6 – Capstone & Track Selection

- OS + Network Rapid Skill Check
- Full Attack Mapping Exercise (Kill Chain + ATT&CK)
- Compromise Detection: Find It, Trace It, Report It

Tools & Technologies Covered

VirtualBox
Lab environment setup

Kali Linux
Security-focused OS

Wireshark
Packet capture & analysis

nmap
Network scanning

ANY.RUN
Interactive malware sandbox

VirusTotal
File/hash reputation

MalwareBazaar
Malware sample repository

Event Viewer
Windows log analysis

PowerShell
Windows scripting & triage

Wazuh
SIEM concepts demonstration

MITRE ATT&CK
Threat mapping framework

MxToolbox
Email header analysis

Career Opportunities

Role

- SOC Analyst – Tier 1
- Cybersecurity Analyst (Entry)
- IT Security Support Engineer
- Network Security Analyst
- Incident Response Associate

Certification & Assessment

- Module-wise Quizzes
- Lab Submission Reports – graded hands-on exercises
- Final Certification Exam – Passing Score: 70%

K7 ACADEMY

www.k7academy.com

202607172