# HACKSTRIX

OFFENSIVE & DEFENSIVE CYBER SOLUTIONS

# Hackstrix Certified SOC Analyst

HSOC Syllabus — Detect, Defend, and Dominate Cyber Threats

## Detect

Monitor signals, identify anomalies, and surface threats before they escalate.

## Defend

Contain attacks, protect critical systems, and respond with precision under pressure.

## Dominate

Hunt proactively, sharpen mastery, and stay ahead of evolving adversaries.

# About the HSOC Certification

The Hackstrix Certified Security Operations Center (HSOC) program is a comprehensive, hands-on training path designed to build world-class SOC analysts capable of detecting, investigating, and responding to real-world cyber threats.

## Who Is This For?

Security analysts, blue team professionals, and aspiring SOC engineers seeking structured, practical training across monitoring, threat hunting, digital forensics, and incident response.

## What You Will Master

From SOC fundamentals and SIEM operations to advanced malware analysis, memory forensics, and threat hunting — this program covers the full SOC analyst skill stack across 20 structured modules.

20

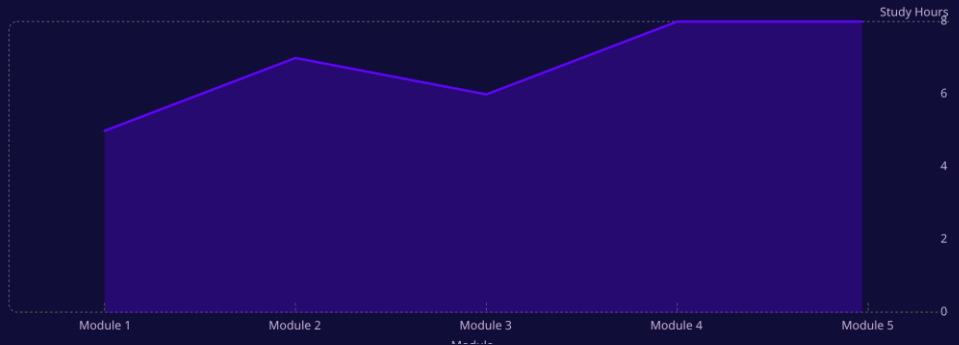
Modules Across 4 Phases

40+ hours of study covering SOC operations, threat intelligence, DFIR, and advanced lab scenarios.

# Phase 1 — SOC Foundations & Core Security Concepts

## Modules 1–5: Building Your SOC Foundation

This phase introduces the security operations ecosystem, network infrastructure, log analysis, and the threat landscape. Students develop core analyst skills including event prioritization, alert management, and MITRE ATT&CK framework mapping.




### Module 1–2: SOC & Infrastructure Basics

SOC overview, roles, tiers (L1/L2/L3), Blue Team fundamentals, network security, firewalls, IDS/IPS architecture, and logging workflows. **5–7 hrs | Easy–Medium**

### Module 3–4: Monitoring & Log Analysis

Security event lifecycle, alert management, SOC workflows, Windows/Linux log analysis, web server logs, and authentication log monitoring. **6–8 hrs | Medium**

### Module 5: Threat Landscape & ATT&CK

Threat actor profiles, cyber attack lifecycle, MITRE ATT&CK framework, Indicators of Compromise (IoCs), and Indicators of Attack (IoA). **8 hrs | Medium**

# Phase 2 — Threat Hunting & Analysis (Modules 6–10)


## Key Topics by Module

01

### Threat Intelligence

Strategic, operational and tactical intelligence, threat feeds, intelligence lifecycle. **6 hrs | Medium**

02

### Threat Hunting

Hypothesis-driven hunting, behavioral analytics, IOC-based hunting, adversary tracking. **9 hrs | Hard**

03

### Malware Detection & Analysis

Malware categories, static/dynamic analysis concepts, malware indicators and artifacts. **8 hrs | Medium**

04

### SIEM Fundamentals

SIEM architecture, log correlation, event analysis, dashboard creation, and security investigations. **10 hrs | Hard**

# Phase 3 — SOC Operations & Incident Response

Modules 11–15 bring together SIEM operations, incident handling, digital forensics, endpoint detection & response, and advanced memory and disk forensics to equip analysts for real incident investigations.

10 hrs

## Module 11 — Splunk Security Operations

Data ingestion, Search Processing Language (SPL), dashboards and alerts, correlation searches, and end-to-end investigation workflows. **Difficulty: Hard**

8 hrs

## Module 12 & 13 — Incident Handling + Digital Forensics

Security incident lifecycle, classification, escalation procedures, evidence acquisition, chain of custody, disk imaging, and forensic investigation process. **Difficulty: Medium**

10 hrs

## Module 14 — Incident Response & EDR

Preparation, detection, containment, and recovery. Endpoint Detection & Response concepts and practical containment procedures for active incidents. **Difficulty: Hard**

9 hrs

## Module 15 — Memory & Disk Forensics

Memory acquisition, process investigation, disk artifact analysis, forensic timeline creation, and investigation reporting. **Difficulty: Hard**

# Phase 4 — Advanced SOC Operations

## Modules 16–20: Real-World Labs & Mastery

The final phase elevates analysts into advanced network security monitoring, IDS/IPS operations, professional reporting, and hands-on threat investigation labs culminating in a full SOC assessment.

### Modules 16–18 — Network Monitoring, IDS/IPS & Reporting

Packet analysis, network visibility, Snort and Suricata architecture, signature understanding, alert investigation, incident reporting, executive summaries, and case documentation. *(Study time: 7–8 hrs each | Medium difficulty)*

### Modules 19–20 — Threat Investigation Lab & SOC Capstone

IOC investigation exercises, malware investigation scenarios, log correlation labs, threat hunting challenges, full SOC analyst simulations, and end-to-end final practical assessment. *(Study time: 9–12 hrs | Hard difficulty)*

# Your Learning Path

The HSOC program is structured as four progressive phases, each building upon the last — from foundational SOC concepts to advanced threat hunting, incident response, and real-world lab simulations.

1

## Phase 1 — SOC Foundations

Modules 1–5 · 34 hrs

2

## Phase 2 — Threat Hunting & Analysis

Modules 6–10 · 41 hrs

3

## Phase 3 — Incident Response + Digital Forensics

Modules 11–15 · 45 hrs

## Phase 4 — Advanced Labs + SOC Operations

Modules 16–20 · 41 hrs. Network security monitoring, IDS/IPS operations with Snort and Suricata, SOC reporting and documentation, threat investigation labs, and a final capstone practical assessment.

## Hackstrix Motto

Detect • Defend • Dominate Cyber Threats. The HSOC certification is designed for analysts who are committed to mastering the complete SOC analyst skill set across monitoring, hunting, forensics, and response.

# Tools Covered in HSOC

The HSOC program provides hands-on experience with the most widely used SOC, DFIR, and threat-hunting tools in the industry — ensuring graduates are ready to operate in real security operations environments from day one.

## SOC, SIEM & Threat Hunting Tools

Splunk, MISP, MITRE ATT&CK, VirusTotal, YARA, CyberChef, Any.Run, Sysmon, Procmon, Process Explorer, etc.

## DFIR & Network Analysis Tools

Wireshark, Tcpdump, Network Miner, Snort, Suricata, Volatility, FTK Imager, Autopsy, Strings, etc.