Hackstrix HCACD

Hackstrix Certified Advanced Cyber Defender — an industry-ready cybersecurity program covering Security Operations, Threat Hunting, Incident Response, Digital Forensics, SIEM, Malware Analysis, and Threat Intelligence.

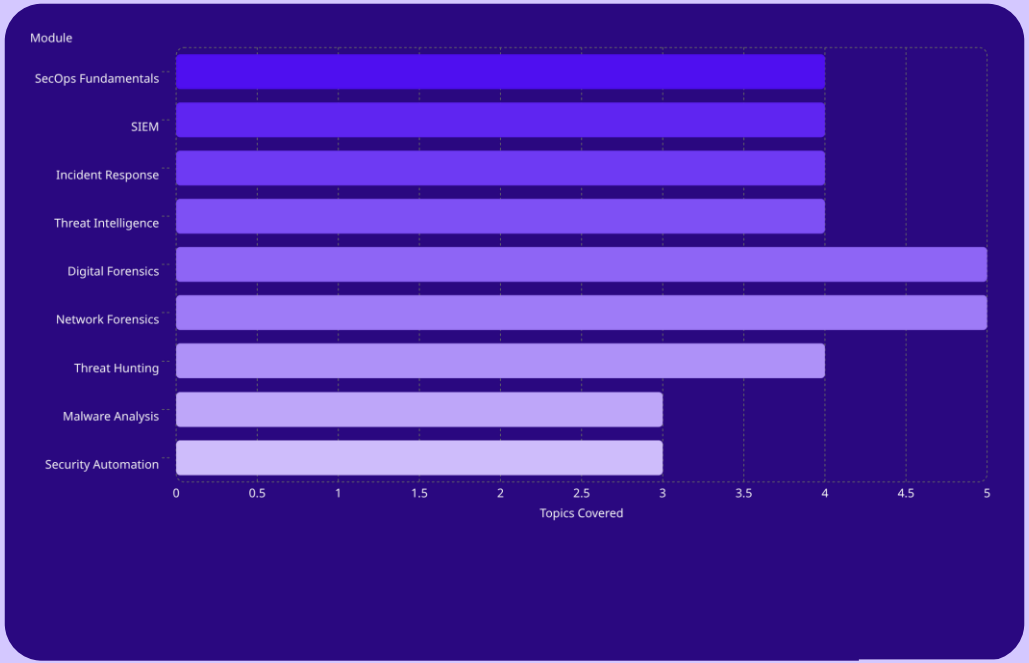
Contact-Us: 8796381043
info@hackstrix.com

COURSE OVERVIEW

Detect, Defend, and Dominate Cyber Threats

The HCACD program is designed to build industry-ready cybersecurity defenders with practical, hands-on skills. Covering 10 comprehensive modules, students will progress from SOC fundamentals through advanced digital forensics, malware analysis, and security automation.

Program Pillars



Built on four core pillars — a complete defensive cybersecurity skill set for modern enterprise environments.

MODULES 1–2

Security Operations & SIEM

Module 1: Security Operations (SecOps) Fundamentals

1

SOC Fundamentals

Core concepts of Security Operations Center structure and functions.

2

SOC Architecture & Organization

Roles, tiers, tools, and workflows within an enterprise SOC.

3

Zero Trust Concepts

Principles of never-trust, always-verify security architecture.

4

SOC Metrics & Operations

KPIs, SLAs, and operational effectiveness in security operations.

Module 2: Security Information & Event Management (SIEM)

1

SIEM Fundamentals

Architecture, log ingestion, correlation rules, and alerting.

2

Query Languages

Writing effective queries for log analysis and threat detection.

3

Detection Engineering

Building and tuning detection logic to reduce false positives.

4

Visualization & Reporting

Dashboards, reports, and communicating security posture.

MODULES 3–4

Perimeter Defense & Network Forensics

Defend the organization's perimeter from email-based attacks and develop deep visibility into network traffic — analyzing packets, protocols, and advanced threat patterns across the wire.

Email Security Fundamentals

Understanding email protocols, authentication mechanisms (SPF, DKIM, DMARC), and common attack vectors targeting enterprise inboxes.

Email & Phishing Security + Analysis

Identifying phishing campaigns, analyzing suspicious email headers, URLs, and attachments. Recognizing spear phishing and BEC techniques.

Email Threat Response

Containment and remediation workflows for email-borne threats — isolation, user notification, and incident documentation.

Module 4: Network Forensics — Key Topics

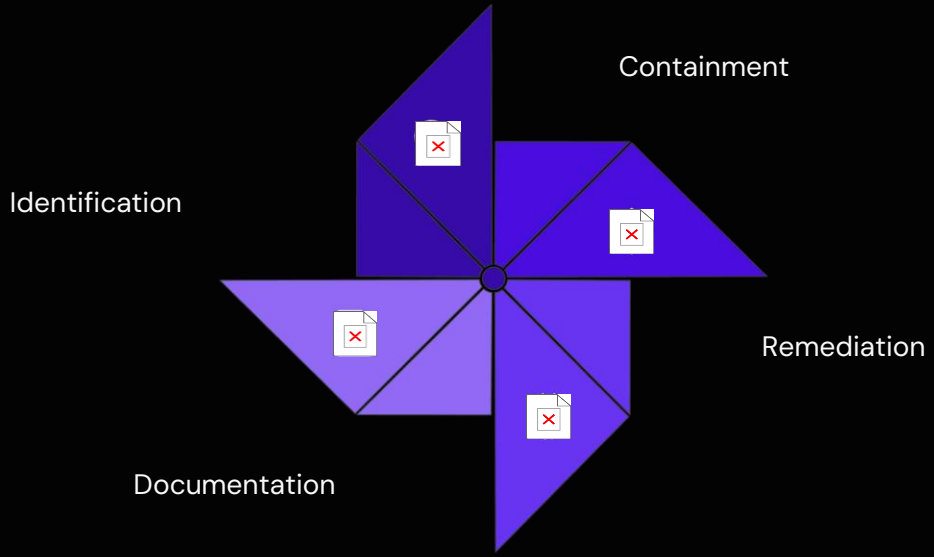
```
Topics Covered:
- Network Security Monitoring
- Packet & Protocol Analysis
- Network Threat Detection
- Advanced Traffic Analysis
- Network Security Tools

Tools & Skills:
  Wireshark, TCPDump, Network Minner
  PCAP analysis workflows
  Protocol dissection (DNS, HTTP, TLS)
  Anomaly detection in traffic
```

Students perform hands-on packet captures and analyze real-world attack traffic patterns including C2 beaconing, lateral movement, and data exfiltration.

MODULES 5–6

Incident Response & Threat Intelligence

Master the full incident response lifecycle from initial detection through containment, remediation, and post-incident review — while leveraging structured threat intelligence to anticipate adversary behavior and prioritize defensive actions.



IR Fundamentals

Incident classification, escalation procedures, and response team coordination across enterprise environments.

Threat Intel Operations

Intelligence lifecycle, MITRE ATT&CK, Diamond Model, and applying CTI feeds to active investigations.

Frameworks & Models

Cyber Kill Chain, MITRE ATT&CK, and STIX/TAXII for structured intelligence sharing and threat modeling.

Key Outcome: Students will be able to **lead a full incident response engagement** — from initial alert triage through root cause analysis — and produce actionable threat intelligence reports aligned to industry frameworks.

MODULES 7–8

Advanced Threat Hunting & Malware Analysis

Module 7: Advanced Threat Hunting & Emulation

Threat Hunting Fundamentals

Hypothesis-driven hunting, data sources, and establishing a baseline of normal behavior across endpoints and networks.

Hunt Methodologies & Techniques

TTP-based hunting using MITRE ATT&CK, behavioral analytics, and advanced pattern recognition across log sources.

Hunt Across Environments

Extending hunts into cloud, hybrid, and on-premise environments using SIEM, EDR, and threat emulation tools.

Module 8: Memory Forensics & Malware Analysis

Malware Classification

Trojans, ransomware, rootkits, RATs — categorizing malware families and their behavioral signatures.

Static Analysis

Examining malware without execution — PE headers, strings, imports, and YARA rule creation.

Dynamic Analysis

Sandboxing, behavioral monitoring, network traffic capture, and memory dumping during live execution.

Security Automation & Digital Forensics

The final two modules equip students with cutting-edge automation capabilities and deep forensic investigation skills — enabling faster response times and thorough evidence collection across Windows, Linux, macOS, and memory artifacts.

Module 9: Security Automation & Orchestration

01

SOAR Fundamentals

Security Orchestration, Automation, and Response platforms — architecture, use cases.

02

Automation Workflows

Designing automated triage, enrichment, and response workflows to reduce analyst workload and mean time to respond (MTTR).

03

Playbook Development

Building, incident response playbooks for common attack scenarios including phishing and ransomware.

Module 10: Digital Forensics & Evidence Collection

Advanced Windows Forensics

Registry analysis, event logs, prefetch, LNK files, and artifact correlation on Windows systems.

Advanced Network & Linux/macOS Forensics

PCAP reconstruction, Linux syslog analysis, macOS unified logs, and filesystem artifact collection.

Advanced Memory & Timeline Forensics

Volatility-based memory analysis and super-timeline construction for full attack chain reconstruction.

Learning Outcomes, Methodology & Who Should Enroll

The HCACD program delivers job-ready defenders through a rigorous blend of theory and practical, hands-on training — preparing students to operate effectively in enterprise SOC environments from day one.

Learning Outcomes

Monitor and defend enterprise environments. Investigate cyber incidents. Perform advanced threat hunting. Analyze malware and memory artifacts. Conduct digital forensic investigations. Build SIEM detections. Apply threat intelligence.

Recommended For

SOC Analysts, Blue Team Professionals, Incident Responders, Threat Hunters, Digital Forensics Investigators, Security Analysts, and Cybersecurity Enthusiasts looking to advance their defensive security skills.

Training Methodology

Instructor-Led Training · Practical Labs · Real-World Attack Simulations · Hands-On Investigations · Threat Hunting Exercises · Malware Analysis Labs — every concept reinforced through direct practice.

Hackstrix Goal: Graduates of the HCACD program will be equipped to **Detect, Defend, and Dominate** cyber threats — ready to take on SOC, IR, and threat hunting roles in enterprise environments immediately upon certification.

Contact-Us: 8796381043

info@hackstrix.com