# Hackstrix Certified Cyber Threat Hunter

An advanced, industry-oriented cybersecurity training program in proactive threat detection, adversary hunting, behavioral analysis, and cyber threat intelligence operations.


Contact-Us: +91 8796381043
info@hackstrix.com

Hackstrix.com

# Program Overview

The **Hackstrix Certified Cyber Threat Hunter Program** focuses on real-world attack simulations, enterprise threat hunting methodologies, MITRE ATT&CK mapping, incident investigation, and advanced detection techniques used by modern Blue Teams, SOC Analysts, and Threat Hunters.

## Offensive & Defensive Focus

Equips learners with practical skills in proactive threat detection, adversary hunting, behavioral analysis, malware investigation, network forensics, and cyber threat intelligence operations.

## Industry-Oriented Training

Designed for Blue Team professionals, SOC Analysts, and Threat Hunters seeking real-world, hands-on experience with enterprise-grade detection techniques and MITRE ATT&CK based learning.

★★★★★ 7

## Core Training Modules

Covering threat hunting, CTI, network forensics, malware analysis, endpoint detection, and adversary simulation.

# Core Modules

## Module 1: Introduction to Cyber Threat Hunting

Covers the Cyber Threat Hunting Lifecycle, Threat Intelligence Fundamentals, Indicators of Compromise (IoCs), MITRE ATT&CK Framework, and key hunting methodologies including Attack-Based, Data-Based, Intelligence-Driven, and Hypothesis-Based Hunting.

## Module 2: Cyber Threat Intelligence & Threat Actor Analysis

Covers Cyber Threat Intelligence (CTI), Open-Source Intelligence (OSINT), Threat Intelligence Platforms, Advanced Persistent Threats (APTs), Threat Reporting & Documentation, and Threat Actor Profiling Techniques.

### MITRE ATT&CK Framework

Foundational framework for mapping adversary tactics, techniques, and procedures (TTPs) to real-world attack scenarios, enabling structured and intelligence-driven threat hunting operations.

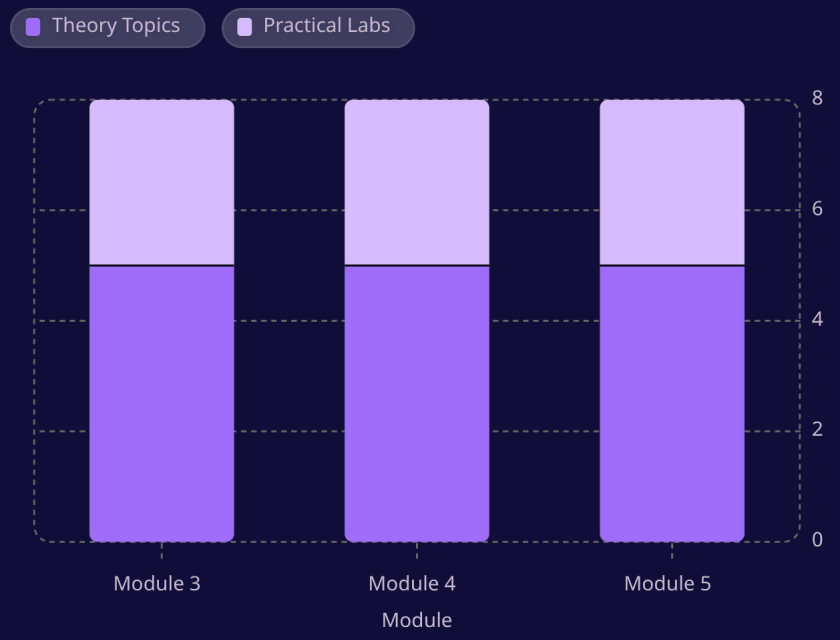
### Threat Actor Profiling

Learn to identify, track, and document Advanced Persistent Threats (APTs) and threat actor groups using OSINT and structured intelligence platforms for proactive defense.

### Hunting Methodologies

Master all four hunting approaches — Attack-Based, Data-Based, Intelligence-Driven, and Hypothesis-Based — to systematically uncover hidden threats in enterprise environments.

# Network, Malware & Endpoint Threat Hunting




## Module Highlights

01

### Module 3: Network Threat Hunting & PCAP Analysis

Packet Capture (PCAP) analysis, Protocol Anomaly Detection, DNS & SSH Tunnel Detection, Ransomware Traffic Analysis, SQL Injection Detection, and Web Shell Detection.

02

### Module 4: Malware Hunting & Memory Forensics

DLL Injection, Process Hollowing, Memory Dump Analysis, Malware Persistence Mechanisms, ZEUS Botnet Analysis, Stuxnet Memory Analysis, and Malware Behavior Investigation.

03

### Module 5: Endpoint Threat Hunting & Log Analysis

Event ID Hunting, Windows Security Logs Analysis, Threat Hunting with Osquery, VirusTotal Intelligence, LOLBAS Detection Techniques, Persistence Hunting, and Endpoint Threat Correlation.

04

### Key Outcome

Gain hands-on proficiency across network, host, and memory layers — forming a comprehensive defensive posture against modern adversaries.

# Advanced Detection & Adversary Simulation

Modules 6 and 7 elevate your threat hunting capabilities beyond known indicators — enabling detection of unknown threats through behavioral analysis, anomaly detection, and hands-on adversary simulation exercises mapped to the Cyber Kill Chain.

M6

## Advanced Threat Hunting Without IoCs

Master Behavioral Threat Hunting, Anomaly-Based Hunting, hunting unknown threats, Advanced Detection Techniques, and Detection Engineering Basics — the pinnacle of proactive cyber defense.

M7

## Adversary Simulation & Threat Detection

Real-World Attack Scenarios, Cyber Kill Chain Mapping, TTP-Based Detection, Persistence & Evasion Techniques, and comprehensive Adversary Simulation Exercises to stress-test your detection skills.

TTPs

## TTP-Based Detection Engineering

Go beyond IoC-based detection by learning to engineer detections around adversary Tactics, Techniques, and Procedures — ensuring resilience even against previously unseen attack patterns.

KCC

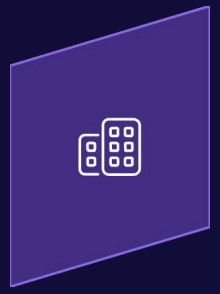
## Cyber Kill Chain Mapping

Understand and apply Cyber Kill Chain Cycle methodology to systematically detect, interrupt, and neutralize adversary operations at every stage of the attack lifecycle.

# Career Opportunities

## Where This Certification Takes You

Graduates of the Hackstrix Certified Cyber Threat Hunter program are prepared for high-demand roles across enterprise security operations, government agencies, MSSPs, and incident response teams worldwide.



### Blue Team & SOC Roles — Threat Hunter · SOC Analyst · Blue Team Professional

Leverage your expertise in endpoint detection, log analysis, and behavioral hunting to protect enterprise environments as a frontline defender. These roles sit at the core of modern Security Operations Centers. *(High demand across financial, healthcare, and government sectors.)*

### Intelligence & Analysis Roles — Security Analyst · Malware Analyst · Threat Intelligence Analyst · Incident Response Analyst

Apply your skills in malware forensics, memory analysis, CTI, and adversary profiling to investigate breaches, analyze threats, and deliver actionable intelligence to executive and technical stakeholders. *(Critical roles in MSSPs, CERTs, and enterprise IR teams.)*

# Why Learn with Hackstrix?

Hackstrix delivers a uniquely practical, career-focused cybersecurity education built around the real tools, frameworks, and methodologies used by professional threat hunters and blue team practitioners in the field today.

1

## Job-Oriented Training

Career guidance & mentorship

2

## MITRE ATT&CK Based Learning

Industry-standard framework integration

3

## Real-World Attack Simulations

Practical hands-on lab experience

### Industry-Relevant Blue Team Skills

Every module is designed around the tools, techniques, and workflows used by practicing blue team professionals — ensuring graduates are immediately productive in real SOC and threat hunting environments.

### Practical Hands-On Labs & Mentorship

Learn by doing with guided lab exercises, real malware samples, live PCAP analysis, and adversary simulations — backed by expert mentors with deep industry experience to guide your career journey.

# Detect, Defend, and Dominate Cyber Threats

Join the Hackstrix Certified Cyber Threat Hunter program and gain the advanced skills needed to protect enterprises, neutralize adversaries, and build a high-impact career in cybersecurity. Real-world simulations. MITRE ATT&CK aligned. Career-ready outcomes.

## Enroll in the Hackstrix Certified Cyber Threat Hunter Program

Begin your journey into professional threat hunting with structured modules, expert mentorship, and hands-on labs designed for real-world impact.

**Program:** Hackstrix Certified Cyber Threat Hunter

**Focus:** Offensive & Defensive Cyber Solutions

**Website:** www.hackstrix.com

**Tagline:** Detect, Defend, and Dominate Cyber Threats