Hackstrix Certified Incident Responder

Complete training program to lead end-to-end incident response operations, handle ransomware and breach incidents, and operate in SOC/IR environments.

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

Module 1: Cybersecurity & Modern Threat Landscape

Build a solid foundation in cybersecurity principles and understand the attacker mindset, threat actors, and the full lifecycle of modern cyberattacks.

Core Concepts

- Cybersecurity fundamentals for incident responders
- What is a cyber incident?
- Types of security incidents: malware, ransomware, breach, insider threats

Threat Actors & Behavior

Threat actors and motivations, APT vs opportunistic attackers, attack lifecycle overview, and real-world attack examples.

12+

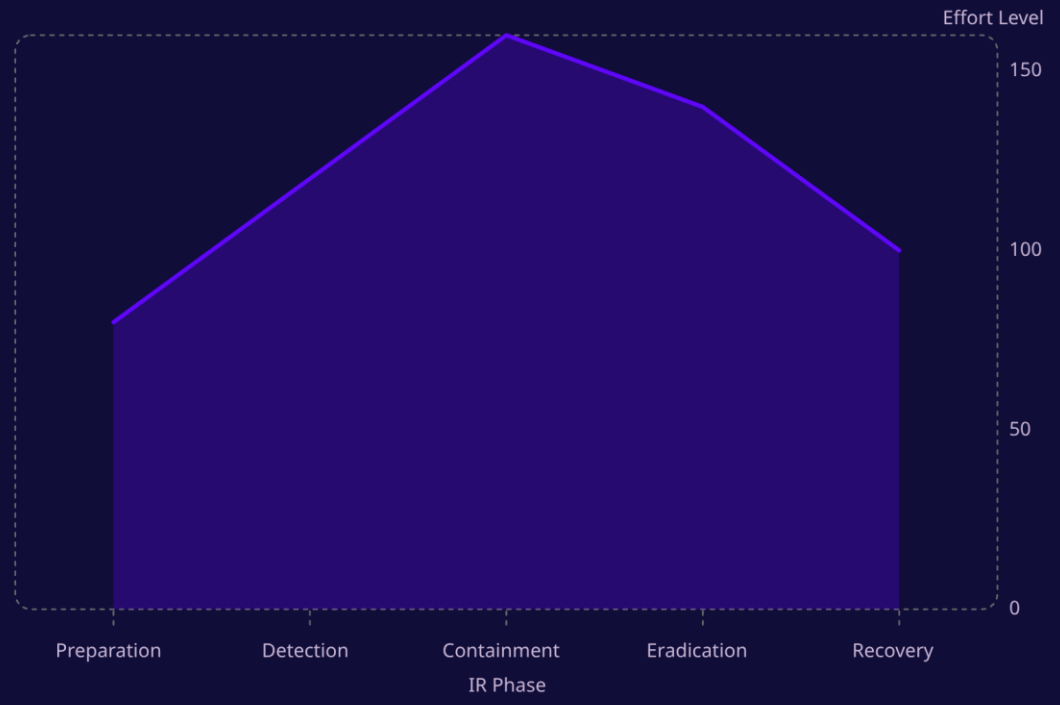
Modules in Full Program

Covering the entire incident response lifecycle from detection to capstone simulation.

Module 2: Incident Response Fundamentals

IR Lifecycle & Frameworks

Understand how IR functions in an enterprise structure — from preparation through recovery — using industry-standard frameworks like NIST and SANS.



IR Frameworks

NIST and SANS IR frameworks provide the structural backbone for all incident response activities, ensuring consistent and repeatable processes.

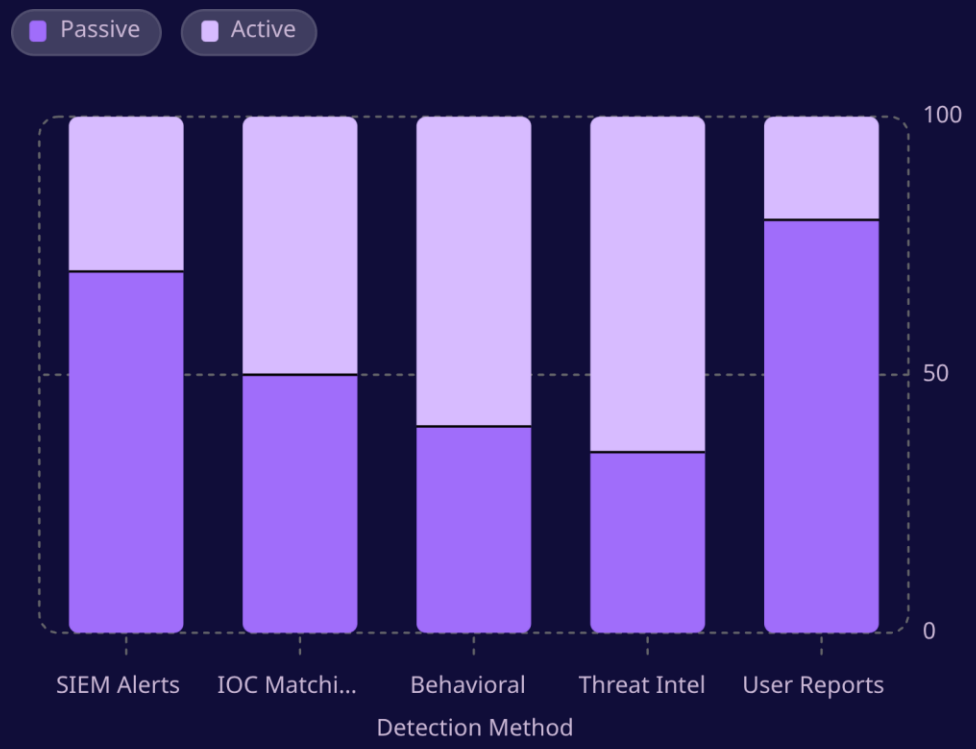
Roles & Responsibilities

Define IR team structure, roles and responsibilities, incident severity classification, and SOP development for enterprise readiness.

IR Policy Development

Build IR policies and standard operating procedures that align with organizational risk tolerance and regulatory requirements.

Modules 3 & 4: Detection, Monitoring & Triage



Detection & Triage Topics

01

Detect

IOCs, behavioral anomalies, SIEM, security baselining, threat intelligence basics, and passive vs active monitoring.

02

Validate

Incident triage workflow, alert validation, false positive identification and filtering for accurate threat assessment.

03

Prioritize

Severity scoring, initial impact assessment, and scope identification to focus response efforts effectively.

04

Escalate

Escalation procedures to ensure the right stakeholders are engaged at the right time during an active incident.

Modules 5 & 6: Containment, Eradication & Remediation

Learn how to stop active attacks from spreading and then completely eliminate attacker presence — covering endpoint isolation, network containment, system cleanup, and credential recovery.

M5

Containment Strategies

Short-term vs long-term containment planning, endpoint isolation, network containment techniques, account disablement, blocking malicious IPs/domains, and preventing lateral movement.

M6

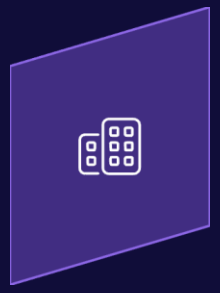
Eradication & Remediation

Removing malicious artifacts from systems, system cleanup coordination, credential resets, patch management, vulnerability remediation, and validation of remediation success.

Modules 7 & 8: Recovery, Communication & Reporting

Restore Operations & Communicate Effectively

Safely restore normal business operations after an incident while ensuring clear, structured communication to all stakeholders — from technical teams to executives and external parties.



Module 7 — Incident Recovery & Restoration

System and service restoration, return-to-production planning, post-recovery monitoring, ensuring system integrity, business continuity coordination, and gradual system reintroduction. *(Outcome: Safely restore normal business operations.)*

Module 8 — Incident Communication & Reporting

Internal communication structure, crisis communication management, executive reporting formats, external communication, breach notification principles, and incident report writing. *(Outcome: Communicate incidents effectively across all stakeholders.)*

Modules 9 & 10: Case Management & Threat Intelligence

Master the operational and intelligence-driven sides of incident response — from structured case tracking to leveraging threat intelligence for faster, smarter decisions during active incidents.

1

Document & Track

Incident lifecycle tracking and documentation standards

2

Manage & Collaborate

Ticketing workflows, SLA management, escalation matrix handling

3

Intelligence-Driven Response

MITRE ATT&CK mapping, IOC usage, threat actor profiling

Module 9 — Incident Case Management

Incident lifecycle tracking, ticketing systems and workflows, documentation standards, team collaboration during incidents, SLA and response time management, and escalation matrix handling.

Module 10 — Threat Intelligence in IR

Role of threat intelligence in IR, IOC usage in investigations, threat actor profiling, MITRE ATT&CK mapping, context enrichment during incidents, and intelligence-driven decision making.

Module 11: IR Simulation Lab

Apply all incident response skills in realistic, hands-on scenarios designed to simulate the pressure and complexity of real-world SOC and IR environments.

Simulation Scenarios

Ransomware incident handling, website defacement response, data breach incident simulation, and SOC alert investigation exercises.

Practical Drills

Triage Drills: Incident triage and containment exercises
Decision Making: Handling pressure and ambiguity under real IR conditions
Outcome: Apply IR skills in authentic real-world scenarios

Module 12: Continuous Improvement & Capstone

Build Enterprise-Level IR Leadership

Close the loop on every incident with structured reviews, root cause analysis, and playbook improvements — then prove your readiness in a final end-to-end simulation.

Post-Incident Review

Post-incident review (PIR), root cause analysis, and lessons learned processes to continuously strengthen your IR capability.

Playbook & Tabletop

IR playbook improvements and tabletop exercises that validate team readiness and expose gaps before a real incident occurs.

Final Capstone

End-to-end incident response simulation covering the full IR lifecycle from detection through recovery and reporting.

Final Program Outcomes

Upon completing all 12 modules of the Hackstrix Certified Incident Responder program, learners will be equipped to operate confidently in professional SOC and IR environments.

Lead IR Operations

Lead end-to-end incident response operations across the full lifecycle from detection and triage through containment, eradication, and recovery.

Handle Critical Incidents

Manage ransomware attacks, data breach incidents, and insider threat scenarios with structured, professional-grade response procedures.

Operate in SOC/IR Teams

Function effectively within enterprise SOC and IR team structures, using industry frameworks, case management tools, and threat intelligence platforms.

🎓 **Certification Outcome:** Graduates will be ready to lead enterprise-level incident response, drive continuous IR improvement, and serve as a trusted resource during active security incidents.