HACKERS EYE ©

HACKERSRANGE ACADEMY

TIER 2 · DEFENSIVE

IR Specialist · DFIR

Course syllabus · Prerequisite HRCSA

HRCIR HackersRange Certified Incident Responder

Incident Response & Digital Forensics. Builds on the SOC Analyst track: run an incident end to end — sound evidence acquisition, host, memory, network and cloud forensics, and defensible reporting against genuinely compromised range systems.

280 h	18	12	70%
TOTAL HOURS	WEEKS	MODULES	LABORATORY

ABOUT HACKERSEYE · HackersRange Academy

We are a working offensive and incident-response firm — and we teach the way we work.

HackersEye is an elite Israeli cyber-security firm, founded by senior operators from government, military and corporate security backgrounds. The same people who built their careers attacking and defending real networks today run live offensive engagements, incident response and security operations for organisations that cannot afford to be wrong.

HackersRange Academy is the training arm of that firm, built on one principle: you learn cyber security by doing the real work — not by watching slides or answering multiple-choice questions. Every learner operates a live, fully instrumented company network, with real adversary activity, and is assessed on the evidence they produce, exactly as they would be on the job.

The range is powered by our own technology. An **AI-driven content engine** builds and refreshes scenarios drawn from live engagements, and our proprietary **HackersRange Suite** provisions each learner an isolated, browser-reachable enterprise on demand. Behind it stands a **24/7 incident-response desk** and the operators who write and teach every module.

HackersEye operates to international standards and is **certified to ISO/IEC 27001** for information security management. The credentials earned here — the HRC certifications — map to the roles employers actually hire for, because they are built by the people already doing those roles.

WHY TRAIN WITH US

- ☐ **Assessed on real work** — evidence on a live range, never multiple choice.
- ☐ **Operators, not slideware** — the team that runs real engagements writes every module.
- ☐ **An always-on range** — your own isolated enterprise, ready in the browser, day or night.
- ☐ **Credentials employers trust** — HRC certifications mapped to real job roles.

HOW THE ACADEMY WORKS

1

Learn the discipline

Concise instruction frames each topic and the tradecraft behind it.

2

Work the live range

The majority of your hours are spent operating a real, instrumented enterprise.

3

Prove it on evidence

Every module and capstone is scored on what you do, not what you memorise.

COURSE OVERVIEW · Tier 2 · Defensive

Incident Response & Digital Forensics. Builds on the SOC Analyst track: run an incident end to end — sound evidence acquisition, host, memory, network and cloud forensics, and defensible reporting against genuinely compromised range systems.

WHO THIS IS FOR

SOC analysts and defenders moving into dedicated incident response and digital forensics, and IT security staff who need to run investigations on genuinely compromised systems.

PREREQUISITES

Entry requirements

HRCSA — HRCSA (SOC Analyst) or equivalent operational experience: confident SIEM and endpoint investigation, comfort reconstructing activity from Windows and network telemetry, and a working understanding of the incident workflow.

HOW IT IS DELIVERED

Format

Instructor-led sessions establish forensic method and rigour, then the majority of your hours are spent investigating genuinely compromised hosts, memory images, captures and cloud tenants on the range — real crime scenes, not sanitised samples.

CERTIFICATION

HRCIR · practical capstone

HRCIR is awarded on a hands-on capstone: a full incident run end to end on genuinely compromised range systems, scored on forensic soundness, the accuracy of your reconstructed timeline and the defensibility of your report.

280 h	18	12	70%
TOTAL HOURS	WEEKS	MODULES	ON THE RANGE

CURRICULUM · modules 1–2 of 12

IR-01 Incident Response Lifecycle & Governance

16 HOURS

You learn the full incident lifecycle from preparation to lessons learned, and the roles and decisions at each stage. This gives you the plan you follow when a real breach lands.

LEARNING OBJECTIVES

- [ ] By the end you can walk an incident through every lifecycle stage from preparation to lessons learned.
- [ ] By the end you can assign the roles and decisions that belong to each stage.
- [ ] By the end you can build and follow an incident-response playbook.
- [ ] By the end you can identify the legal and regulatory obligations that shape a response.

TOPICS COVERED

- The PICERL and NIST IR lifecycles
- IR roles, command and escalation
- Playbook design and runbooks
- Legal, regulatory and notification duties
- Evidence-handling policy
- Preparation and readiness

RANGE LAB

You take a scoped range breach scenario and drive it through the full lifecycle on paper and console — assigning roles, invoking the right playbook, and recording the decisions each stage demands before you touch the evidence.

ASSESSMENT You produce a lifecycle-aligned response plan and playbook for a range scenario, graded on completeness, correct sequencing and sound governance decisions.

IR-02 Evidence Acquisition & Forensic Soundness

20 HOURS

You capture disks and data in a way that holds up later, with an unbroken chain of custody. You learn why how you collect evidence matters as much as what you find.

LEARNING OBJECTIVES

- [ ] By the end you can acquire a forensically sound image of a disk and of volatile data.
- [ ] By the end you can maintain and document an unbroken chain of custody.
- [ ] By the end you can verify image integrity with hashing and write-blocking.
- [ ] By the end you can order acquisition by volatility to preserve the most fragile evidence first.

TOPICS COVERED

- Order of volatility
- Disk imaging with write-blocking
- Live and triage acquisition with KAPE
- Hashing and image verification
- Chain of custody documentation
- Anti-forensics awareness

RANGE LAB

You acquire disk and volatile evidence from a compromised range host in the correct order of volatility, verify each image by hash, and maintain a chain-of-custody record that would survive scrutiny.

ASSESSMENT You submit verified evidence images with a complete chain-of-custody record, graded on forensic soundness, correct volatility ordering and integrity verification.

CURRICULUM, CONTINUED · modules 3–4 of 12

IR-03 Windows Forensics I — File System & Registry

22 HOURS

You dig into the Windows file system and registry to see what was installed, run and changed. You reconstruct attacker footprints from the traces Windows leaves behind.

LEARNING OBJECTIVES

- [ ] By the end you can parse NTFS artefacts to establish what files existed and when.
- [ ] By the end you can analyse the registry to find installed software and configuration changes.
- [ ] By the end you can recover evidence of user activity from registry hives.
- [ ] By the end you can reconstruct an attacker's footprint from file-system and registry traces.

TOPICS COVERED

- The NTFS master file table and journals
- File-system timestamps and their pitfalls
- Registry hives and structure
- RegRipper and registry parsing
- User-activity and shellbag artefacts
- Autostart and persistence keys

RANGE LAB

You examine a compromised Windows image on the range, mining the MFT and registry to establish what the attacker installed, where they persisted and which files they created or touched — rebuilding their footprint from the artefacts alone.

ASSESSMENT You document attacker file-system and registry activity from a range image, graded on artefact accuracy and correct interpretation of the evidence.

IR-04 Windows Forensics II — Logs, Execution & Timeline

24 HOURS

You pull execution evidence and event logs together into one timeline of what happened and when. You use Plaso to build a defensible sequence of the attack.

LEARNING OBJECTIVES

- [ ] By the end you can recover evidence of program execution from Windows artefacts.
- [ ] By the end you can correlate event logs to establish who did what and when.
- [ ] By the end you can build a super-timeline with Plaso.
- [ ] By the end you can produce a defensible sequence of events from mixed evidence.

TOPICS COVERED

- Execution artefacts: Prefetch, Amcache, ShimCache
- Windows event log analysis
- Logon and account-usage evidence
- Super-timeline creation with Plaso
- Timeline analysis and reduction
- Building a defensible narrative

RANGE LAB

You fuse execution artefacts and event logs from a compromised range host into a single Plaso super-timeline, then reduce it to a clear, defensible sequence of the attacker's actions from first access onward.

ASSESSMENT You deliver a reconstructed attack timeline from a range image, graded on accuracy, evidentiary support and the defensibility of the sequence.

CURRICULUM, CONTINUED · modules 5–6 of 12

IR-05 Memory Forensics

24 HOURS

You capture and analyse system memory with Volatility 3 and MemProcFS to find malware that never touched the disk. Memory often holds the clearest picture of a live intrusion.

LEARNING OBJECTIVES

- [ ] By the end you can acquire and analyse a memory image with Volatility 3.
- [ ] By the end you can find fileless and injected malware that left no disk trace.
- [ ] By the end you can recover processes, network connections and credentials from memory.
- [ ] By the end you can detect process injection and hollowing in a memory image.

TOPICS COVERED

- Memory acquisition and structure
- Volatility 3 core plugins
- MemProcFS for interactive analysis
- Process, DLL and handle enumeration
- Detecting injection and hollowing
- Recovering credentials and network state

RANGE LAB

You analyse a memory image from a range host infected with a fileless implant, using Volatility 3 and MemProcFS to expose the injected code, its network connections and the credentials it captured — evidence the disk never held.

ASSESSMENT You extract and document the in-memory footprint of an intrusion, graded on correct plugin use and on whether you identify the fileless activity.

IR-06 Linux & Cloud Forensics

24 HOURS

You investigate compromised Linux hosts and cloud accounts, including the Microsoft 365 audit log. You learn where the evidence lives when the crime scene is a server or a tenant.

LEARNING OBJECTIVES

- [ ] By the end you can investigate a compromised Linux host from its artefacts and logs.
- [ ] By the end you can analyse cloud and identity logs to reconstruct account compromise.
- [ ] By the end you can parse the Microsoft 365 Unified Audit Log for attacker activity.
- [ ] By the end you can locate evidence when the crime scene is a server or a tenant.

TOPICS COVERED

- Linux artefacts, logs and persistence
- Bash history, cron and systemd abuse
- Cloud control-plane logging
- The Microsoft 365 Unified Audit Log
- Identity and OAuth abuse evidence
- Cross-environment correlation

RANGE LAB

You investigate a compromised Linux server and a linked Microsoft 365 tenant on the range, reconstructing persistence on the host and attacker activity in the audit log — following the intrusion across the on-premises and cloud boundary.

ASSESSMENT You document a cross-environment compromise from host and cloud evidence, graded on artefact accuracy and correct reconstruction of the account abuse.

CURRICULUM, CONTINUED · modules 7–8 of 12

IR-07 Network Forensics

22 HOURS

You reconstruct an attack from captured network traffic, tracing command channels and stolen data. You learn to prove what left the network even when the host is wiped.

LEARNING OBJECTIVES

- [ ] By the end you can reconstruct an intrusion from full packet captures.
- [ ] By the end you can trace a command-and-control channel through the traffic.
- [ ] By the end you can prove what data left the network and to where.
- [ ] By the end you can recover files and artefacts carved from captured traffic.

TOPICS COVERED

- Full-packet-capture analysis
- Flow and session reconstruction
- Identifying command-and-control traffic
- Detecting and proving exfiltration
- Carving files from captures
- Encrypted-traffic analysis limits

RANGE LAB

You reconstruct an attack purely from captured range traffic — identifying the C2 channel, proving which data was exfiltrated and to where, and carving the transferred files out of the packets even though the host was wiped.

ASSESSMENT You produce a network-based reconstruction of an intrusion, graded on correct C2 identification and on proving the exfiltration from the evidence.

IR-08 Malware Triage & Behavioral Analysis

24 HOURS

You safely detonate and observe a suspicious file to learn what it does without full reverse engineering. You extract the indicators the rest of the team needs to hunt with.

LEARNING OBJECTIVES

- [ ] By the end you can safely handle and detonate a suspicious sample in isolation.
- [ ] By the end you can characterise a sample's behaviour without full reverse engineering.
- [ ] By the end you can extract host- and network-based indicators from a sample.
- [ ] By the end you can produce indicators the wider team can hunt with.

TOPICS COVERED

- Safe handling and lab isolation
- Static triage and file characterisation
- Dynamic detonation and observation
- Host and network behaviour analysis
- Extracting indicators of compromise
- Basic unpacking and obfuscation awareness

RANGE LAB

You triage a live malware sample in an isolated range sandbox, observing what it does to the host and the network, and extract the host and network indicators the SOC and hunt teams need — without a full reverse-engineering effort.

ASSESSMENT You deliver a behavioural triage report and an indicator set for an unknown sample, graded on analytical accuracy, safety and the quality of the extracted indicators.

CURRICULUM, CONTINUED · modules 9–10 of 12

IR-09 Email Compromise & BEC Investigations

22 HOURS

You investigate a hijacked mailbox and a business email fraud, following logins, rules and message paths. You learn how these common, costly attacks actually play out.

LEARNING OBJECTIVES

- [ ] By the end you can investigate a compromised mailbox from sign-in and audit evidence.
- [ ] By the end you can analyse email headers to trace a message's true origin.
- [ ] By the end you can uncover malicious inbox rules and forwarding used in fraud.
- [ ] By the end you can reconstruct how a business email compromise unfolded.

TOPICS COVERED

- Business email compromise anatomy
- Mailbox and sign-in audit analysis
- Email header and path analysis
- Malicious inbox rules and forwarding
- OAuth and token abuse in mail
- Financial-fraud reconstruction

RANGE LAB

You investigate a hijacked mailbox on the range, following the malicious sign-ins, the rules the attacker planted and the message trail — reconstructing a business email fraud from the audit evidence and headers.

ASSESSMENT You reconstruct a mailbox compromise and fraud from range evidence, graded on the accuracy of your header analysis and the completeness of the account-abuse timeline.

IR-10 Cyber Threat Intelligence & Attribution

22 HOURS

You tie the evidence to known attacker groups and techniques and judge how confident that link really is. You learn to attribute carefully without overreaching.

LEARNING OBJECTIVES

- [ ] By the end you can map observed activity to known threat-actor techniques.
- [ ] By the end you can express an attribution judgement with a defensible confidence level.
- [ ] By the end you can apply structured analytic techniques to avoid bias.
- [ ] By the end you can separate a strong evidentiary link from a weak one.

TOPICS COVERED

- TTP mapping to threat actors
- The Diamond Model of intrusion analysis
- Confidence levels and analytic rigour
- Structured analytic techniques
- Cognitive bias in attribution
- The limits of attribution

RANGE LAB

You take the evidence from a range investigation and test it against known threat-actor tradecraft, building an attribution assessment with explicit confidence levels — and stating plainly where the evidence does not support a link.

ASSESSMENT You submit an attribution assessment with calibrated confidence, graded on analytic rigour and on whether your conclusions stay inside what the evidence supports.

CURRICULUM, CONTINUED · modules 11–12 of 12

IR-11 Containment, Eradication & Recovery

24 HOURS

You cut off an active attacker, remove their access and restore the business safely without losing evidence. You practise the hard calls made under pressure during a real breach.

LEARNING OBJECTIVES

- [ ] By the end you can contain an active attacker while preserving evidence.
- [ ] By the end you can eradicate attacker access and persistence completely.
- [ ] By the end you can plan and validate a safe recovery to normal operations.
- [ ] By the end you can make and justify hard response decisions under pressure.

TOPICS COVERED

- Containment strategies and trade-offs
- Preserving evidence during containment
- Removing footholds and persistence
- Validating eradication completeness
- Recovery planning and verification
- Decision-making under pressure

RANGE LAB

You respond to a live, active intrusion on the range — cutting off the attacker, hunting down and removing every foothold, and restoring the estate to a verified clean state without destroying the evidence you still need.

ASSESSMENT You contain, eradicate and recover from an active range breach, graded on the soundness of your decisions, completeness of eradication and preservation of evidence.

IR-12 DFIR Reporting & Expert Communication

36 HOURS

You turn your investigation into a defensible report and a clear executive briefing. The graded capstone scores a full incident run end to end on genuinely compromised range systems.

LEARNING OBJECTIVES

- [ ] By the end you can write a DFIR report that withstands technical and legal scrutiny.
- [ ] By the end you can brief executives on an incident clearly and without jargon.
- [ ] By the end you can defend your reconstructed timeline against challenge.
- [ ] By the end you can run a full incident investigation end to end on compromised systems.

TOPICS COVERED

- Structuring a defensible DFIR report
- Evidence presentation and traceability
- Executive and board briefing
- Defending findings under challenge
- Lessons-learned and after-action review
- The end-to-end investigation workflow

RANGE LAB

The DFIR capstone: you run a full incident on genuinely compromised range systems — acquisition through host, memory, network and cloud forensics — and deliver both the defensible technical report and the executive briefing a real engagement demands.

ASSESSMENT Graded capstone scored on a complete incident run end to end: forensic soundness, timeline accuracy, and the defensibility of your report and briefing.

OUTCOMES & CERTIFICATION

YOU WILL GRADUATE ABLE TO

- [ ] Acquire evidence in a forensically sound manner with a defensible chain of custody.
- [ ] Perform Windows, Linux, cloud, memory and network forensics to reconstruct attacker activity.
- [ ] Reconstruct a defensible timeline and produce DFIR reporting and executive briefings.
- [ ] Aligns to GIAC GCFA, GCFE, GCIH and GREM (partial).

TOOLS YOU WILL WORK WITH

KAPE · Autopsy · Volatility 3 · MemProcFS · Plaso · RegRipper · M365 UAL

PREREQUISITE	**HRCSA** — completed before starting this track.
CERTIFICATION	**HRCIR** — HackersRange Certified Incident Responder, awarded on the practical capstone.

PLANS & ENROLMENT · individual membership

CURRENT INDIVIDUAL-PLAN PRICING

Full access to HackersRange Academy on an individual membership. Prices shown are for individual enrolment and are current at publication — they may be updated over time. Every plan includes your own always-on range and progress scored on real work.

Recruit

$29 / month

$24/mo billed yearly · $290/yr

- Guided career paths & core scenarios
- Community, leaderboard & skill map
- Your own always-on range
- Progress scored on real work

MOST POPULAR

Operator

$59 / month

$49/mo billed yearly · $590/yr

- **Everything in Recruit**
- Full scenario & machine library, all disciplines
- CISO Room executive tabletops
- Larger range, priority spin-up
- Path to an HRC certification

Elite

$99 / month

$82/mo billed yearly · $990/yr

- **Everything in Operator**
- HRC certification exams included
- Highest range capacity
- Mentor check-ins & new content first

7-day free trial · no card required · cancel anytime. Start on any plan and switch whenever you like.

Training a team? Enterprise, government, universities and partners run on dedicated ranges, priced per seat. Talk to us at **hackerseye.com**.