HACKERS EYE ©

HACKERSRANGE ACADEMY

TIER 1 · DEFENSIVE

SOC Analyst

Course syllabus · Prerequisite HRCF

HRCSA HackersRange Certified SOC Analyst

Security Operations & Defensive Analysis. Monitor an enterprise, triage and investigate alerts, engineer detections and hunt — on Splunk and the Elastic Stack against live attacks.

200 h	14	12	70%
TOTAL HOURS	WEEKS	MODULES	LABORATORY

+972 52-425-7718 · Emergency@hackerseye.com

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 1 · Defensive

Security Operations & Defensive Analysis. Monitor an enterprise, triage and investigate alerts, engineer detections and hunt — on Splunk and the Elastic Stack against live attacks.

WHO THIS IS FOR

Aspiring and junior SOC analysts, blue-team defenders and IT professionals moving into a monitoring, detection or threat-hunting role in a security operations centre.

PREREQUISITES
Entry requirements

HRCF — HRCF (Intro to Cyber) or equivalent proven ability: comfort on the Linux and Windows command lines, a working grasp of TCP/IP and packet analysis, and the security fundamentals covered in the foundation track.

HOW IT IS DELIVERED
Format

Instructor-led sessions establish each defensive discipline, then roughly seventy percent of your hours are spent operating a live, instrumented enterprise on the range — a real SIEM, EDR and network sensors with genuine adversary activity replayed in.

CERTIFICATION
HRCSA · practical capstone

HRCSA is awarded on a hands-on capstone: a full monitor-triage-hunt run against a live attack on the range, scored on your investigation quality, the detections you write and the evidence you produce — never multiple choice.

PROGRESSION
Next tracks

IR Specialist · DFIR

200 h	14	12	70%
TOTAL HOURS	WEEKS	MODULES	ON THE RANGE

CURRICULUM · modules 1–2 of 12

SOC-01 SOC Operations & Frameworks

12 HOURS

You learn how a security operations centre is run day to day and how work flows from alert to action. You map that work to the frameworks a real team uses so you fit in from day one.

LEARNING OBJECTIVES

- [ ] By the end you can describe how work flows through a SOC from detection to closure.
- [ ] By the end you can map an observed technique to the relevant MITRE ATT&CK tactic and technique.
- [ ] By the end you can locate a case at the correct analyst tier and know when to escalate.
- [ ] By the end you can explain the shared metrics that measure a SOC's performance.

TOPICS COVERED

- SOC roles, tiers and shift structure
- The alert-to-action workflow
- MITRE ATT&CK as a common language
- The NIST and SANS incident frameworks
- Case management and ticketing
- Core SOC metrics: MTTD and MTTR

RANGE LAB

You work a mock alert queue through a case-management workflow on the range, classifying each item, mapping it to ATT&CK, and deciding what stays at tier one and what escalates — learning the rhythm of a real shift.

ASSESSMENT You triage and route a set of live cases with correct ATT&CK mapping and escalation decisions, graded on classification accuracy and workflow discipline.

SOC-02 Log Sources & Telemetry

14 HOURS

You collect logs from Windows, Linux, network and cloud systems and learn what each one can and cannot tell you. This teaches you where to look before an alert ever fires.

LEARNING OBJECTIVES

- [ ] By the end you can enumerate the primary log sources across an enterprise estate.
- [ ] By the end you can state what question each telemetry source can and cannot answer.
- [ ] By the end you can identify visibility gaps in a given environment.
- [ ] By the end you can normalise and map fields across disparate log formats.

TOPICS COVERED

- Windows event and Sysmon telemetry
- Linux auditd and syslog
- Network flow and firewall logs
- Cloud and identity provider logs
- Log normalisation and common schemas
- Coverage mapping and visibility gaps

RANGE LAB

You onboard several log sources from a range estate into the SIEM, then chart the visibility they give you against the kill chain — proving where you can see an attacker and, more importantly, where you cannot.

ASSESSMENT You deliver a telemetry coverage map for a range environment, graded on correct source identification and on how well you expose the blind spots.

CURRICULUM, CONTINUED · modules 3–4 of 12

SOC-03 SIEM Fundamentals — Splunk & Elastic Security

18 HOURS

You load real data into Splunk and the Elastic Stack and write your own searches to find suspicious activity. This is the core console you will live in as an analyst.

LEARNING OBJECTIVES

- [ ] By the end you can write SPL and Elastic queries to surface suspicious activity in a dataset.
- [ ] By the end you can build a dashboard that answers a defensive question at a glance.
- [ ] By the end you can correlate events across multiple sources within the SIEM.
- [ ] By the end you can tune a search to balance signal against noise.

TOPICS COVERED

- SIEM architecture and data ingestion
- Splunk Search Processing Language
- Elastic KQL and EQL queries
- Filtering, aggregation and statistics
- Correlation across sources
- Building dashboards and saved searches

RANGE LAB

You load live attack data into both Splunk and the Elastic Stack and write queries that pull the malicious activity out of the noise, then assemble your searches into a working analyst dashboard on the range.

ASSESSMENT You answer a set of investigative questions against a live dataset in both SIEMs, graded on query correctness and on whether your searches actually isolate the malicious activity.

SOC-04 Network Security Monitoring

16 HOURS

You inspect live network traffic with Zeek and Suricata to spot scanning, beacons and data leaving the estate. You learn to separate normal chatter from a real intrusion.

LEARNING OBJECTIVES

- [ ] By the end you can analyse Zeek logs to reconstruct network activity.
- [ ] By the end you can read and write Suricata signatures to detect known threats.
- [ ] By the end you can identify scanning, beaconing and exfiltration patterns in traffic.
- [ ] By the end you can baseline normal traffic to expose the abnormal.

TOPICS COVERED

- Network security monitoring concepts
- Zeek connection and protocol logs
- Suricata rules and signatures
- Detecting port scans and enumeration
- Spotting command-and-control beaconing
- Recognising data exfiltration

RANGE LAB

You monitor a range network under active attack with Zeek and Suricata, pinpointing a scan, a beaconing implant and an exfiltration channel in the traffic — and writing a signature that would catch the beacon next time.

ASSESSMENT You detect and document the network stages of a live intrusion from sensor data, graded on detection accuracy and on the quality of a signature you author.

CURRICULUM, CONTINUED · modules 5–6 of 12

SOC-05 Endpoint Detection & Response

17 HOURS

You use an EDR and Sysmon data to watch what programs actually do on a machine and catch malicious behaviour. You investigate a compromised host from the endpoint outward.

LEARNING OBJECTIVES

- [ ] By the end you can interpret Sysmon and EDR telemetry to reconstruct process activity on a host.
- [ ] By the end you can detect malicious behaviour such as process injection and credential access.
- [ ] By the end you can triage a compromised endpoint and scope the damage.
- [ ] By the end you can distinguish benign administrative activity from an attack.

TOPICS COVERED

- Endpoint telemetry and Sysmon configuration
- Process trees and command-line auditing
- EDR detections and behavioural analytics
- Living-off-the-land binary abuse
- Credential access and process injection
- Host triage and scoping

RANGE LAB

You investigate a compromised Windows host on the range from the endpoint outward, using Sysmon and the EDR to rebuild the attacker's process tree and determine exactly what ran, what was touched and how far it spread.

ASSESSMENT You scope a compromised endpoint and produce a process-level narrative of the intrusion, graded on completeness and on correctly separating attacker activity from normal noise.

SOC-06 Detection Engineering

18 HOURS

You write detections as code — Sigma and Elastic rules — then test and tune them against real attacks on the range. You learn to cut false alarms without missing the real thing.

LEARNING OBJECTIVES

- [ ] By the end you can author a Sigma rule and convert it to a target SIEM.
- [ ] By the end you can test a detection against real attack telemetry to confirm it fires.
- [ ] By the end you can tune a rule to reduce false positives without creating false negatives.
- [ ] By the end you can express a detection's coverage in terms of MITRE ATT&CK.

TOPICS COVERED

- Detection-as-code principles
- Writing Sigma rules
- Converting Sigma to Splunk and Elastic
- Testing detections against real telemetry
- False-positive and false-negative tuning
- Mapping coverage to ATT&CK

RANGE LAB

You write a set of Sigma detections for techniques used in a live range attack, convert them into the SIEM, then run the attack again to confirm they fire — and tune out the false alarms they raise against normal activity.

ASSESSMENT You submit tested, tuned detection rules with evidence they catch the real attack and stay quiet on benign traffic, graded on efficacy and false-positive rate.

CURRICULUM, CONTINUED · modules 7–8 of 12

SOC-07 Alert Triage & Investigation

18 HOURS

You take a queue of live alerts and decide quickly which are real, which are noise and which need to escalate. You build the evidence trail that supports each decision.

LEARNING OBJECTIVES

- [ ] By the end you can triage an alert queue and prioritise by risk under time pressure.
- [ ] By the end you can investigate an alert to a confident true- or false-positive verdict.
- [ ] By the end you can build an evidence trail that justifies each disposition.
- [ ] By the end you can decide when and how to escalate to incident response.

TOPICS COVERED

- Alert prioritisation and risk scoring
- Investigation methodology
- Pivoting across data sources
- True positive versus false positive
- Evidence collection and case notes
- Escalation criteria and handoff

RANGE LAB

You work a realistic, mixed alert queue on the range — some real, most noise — investigating each to a verdict, recording the evidence behind it, and escalating the genuine intrusion with a clean handoff package.

ASSESSMENT You clear a live alert queue with correct verdicts and a documented evidence trail for each, graded on accuracy, speed and the defensibility of your escalation.

SOC-08 Cyber Threat Intelligence for the SOC

15 HOURS

You enrich alerts with threat intelligence in MISP and learn which indicators are worth acting on. This turns a raw alert into a picture of who might be attacking and why.

LEARNING OBJECTIVES

- [ ] By the end you can enrich an alert with threat intelligence to add context.
- [ ] By the end you can assess the reliability and relevance of an indicator.
- [ ] By the end you can operate MISP to store, share and correlate intelligence.
- [ ] By the end you can turn a raw indicator into an actionable detection.

TOPICS COVERED

- The threat-intelligence lifecycle
- Strategic, operational and tactical intelligence
- Indicators of compromise and their limits
- MISP for storage and sharing
- Enriching alerts with context
- Operationalising intelligence into detections

RANGE LAB

You take indicators from a live range intrusion into MISP, correlate them against known activity, judge which are worth acting on, and turn the reliable ones into detections that feed back into the SOC.

ASSESSMENT You produce an enriched intelligence picture for a range incident and a detection derived from it, graded on the soundness of your indicator assessment and its operational value.

CURRICULUM, CONTINUED · modules 9–10 of 12

SOC-09 Threat Hunting Fundamentals

17 HOURS

You form a hypothesis about how an attacker might be hiding and go looking for them before any alert fires. Your hunts are mapped to MITRE ATT&CK so the results are repeatable.

LEARNING OBJECTIVES

- [ ] By the end you can form a testable threat-hunting hypothesis grounded in ATT&CK.
- [ ] By the end you can hunt across SIEM and endpoint data to prove or disprove it.
- [ ] By the end you can find attacker activity that raised no alert.
- [ ] By the end you can turn a successful hunt into a lasting detection.

TOPICS COVERED

- Hypothesis-driven hunting
- The hunting loop and maturity models
- Hunting for persistence and lateral movement
- Baselining to surface anomalies
- Mapping hunts to MITRE ATT&CK
- From hunt finding to detection rule

RANGE LAB

You hunt a defended range estate for an intruder who triggered no alerts — forming a hypothesis, testing it against the telemetry, and running the attacker down before feeding your findings back as a new detection.

ASSESSMENT You execute a documented, hypothesis-driven hunt on the range and evidence what you found, graded on rigour, repeatability and whether you surfaced the hidden activity.

SOC-10 Incident Handling for Analysts

16 HOURS

You run a live incident through its early stages and learn a clean handoff to the incident response team. You practise keeping calm records while an attack is still unfolding.

LEARNING OBJECTIVES

- [ ] By the end you can drive an incident through its early lifecycle stages.
- [ ] By the end you can take initial containment actions without destroying evidence.
- [ ] By the end you can keep an accurate incident record under live pressure.
- [ ] By the end you can hand off cleanly to a dedicated IR team.

TOPICS COVERED

- The incident-handling lifecycle for analysts
- Declaring and classifying an incident
- Initial containment options and trade-offs
- Preserving evidence during response
- Incident logging and communication
- The handoff to incident response

RANGE LAB

You take a live, unfolding intrusion on the range through detection, classification and initial containment while keeping a running incident log — then package a clean handoff for the IR team without losing evidence.

ASSESSMENT You handle an unfolding range incident to a clean IR handoff, graded on the soundness of your containment choices and the quality of your contemporaneous record.

CURRICULUM, CONTINUED · modules 11–12 of 12

SOC-11 SOAR & Automation

15 HOURS

You build simple automated playbooks so repetitive tasks handle themselves and analysts focus on real judgement. You see how automation speeds response without removing the human decision.

LEARNING OBJECTIVES

- [ ] By the end you can design an automated playbook for a repetitive SOC task.
- [ ] By the end you can integrate tools through a SOAR platform.
- [ ] By the end you can decide which steps to automate and which need a human.
- [ ] By the end you can measure the time a playbook saves.

TOPICS COVERED

- SOAR concepts and architecture
- Playbook design and logic
- Automating enrichment and triage
- Tool integration and APIs
- Human-in-the-loop decision points
- Measuring automation impact

RANGE LAB

You build a SOAR playbook that automatically enriches and triages a common alert type on the range, leaving a clear decision point for the analyst — then measure how much handling time it removes from the queue.

ASSESSMENT You deliver a working, tested playbook with a justified human-decision point, graded on correctness, safety and the measurable time it saves.

SOC-12 Reporting, Metrics & Communication

24 HOURS

You write clear incident write-ups and track the metrics that show whether the SOC is working. The graded capstone scores a full monitor-triage-hunt run on the live range.

LEARNING OBJECTIVES

- [ ] By the end you can write an incident report a technical and a non-technical reader can both use.
- [ ] By the end you can select and present the metrics that show SOC effectiveness.
- [ ] By the end you can communicate findings clearly under operational pressure.
- [ ] By the end you can run a full monitor-triage-hunt cycle end to end on a live estate.

TOPICS COVERED

- Structured incident reporting
- Writing for technical and executive readers
- SOC metrics and KPIs
- Presenting findings and evidence
- Communication during an incident
- The end-to-end analyst workflow

RANGE LAB

The SOC capstone: you monitor a live enterprise on the range, triage the alerts a real attack generates, hunt for what slipped past, and produce the incident report and metrics a genuine SOC would deliver.

ASSESSMENT Graded capstone scored on a complete monitor-triage-hunt run against a live attack — your investigation, the detections you wrote, and the clarity and accuracy of your reporting.

OUTCOMES & CERTIFICATION

YOU WILL GRADUATE ABLE TO

- [ ] Operate a SIEM and an EDR to monitor and investigate an enterprise estate.
- [ ] Write, test and tune detections as code, including Sigma and Elastic rules.
- [ ] Run hypothesis-driven threat hunts mapped to MITRE ATT&CK and hand off to IR.
- [ ] Aligns to BTL1, CompTIA CySA+ and Microsoft SC-200.

TOOLS YOU WILL WORK WITH

Splunk · Elasticsearch · Kibana · Sysmon · Zeek · Suricata · MISP

PREREQUISITE	**HRCF** — completed before starting this track.
CERTIFICATION	**HRCSA** — HackersRange Certified SOC Analyst, awarded on the practical capstone.
NEXT TRACKS	IR Specialist · DFIR

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**.