

ADVANCED CYBERSECURITY ENGINEERING

Autonomous AI-Driven Cyberattack & Cyber Defense Training

RCCE Level 3 Certification

Five days. One connected enterprise environment.
The complete Zelfire learning experience.

5

intensive days

40

scheduled hours

20

core platforms

16

labs + final mission



Cloud-based. Browser-accessible.

Hundreds of preconfigured virtual machines across enterprise scenarios. AINA-powered automated attacks against assigned training targets.

01

**Attack**

02

**Defend**

03

**Investigate**

04

**Code**

05

**Operate**

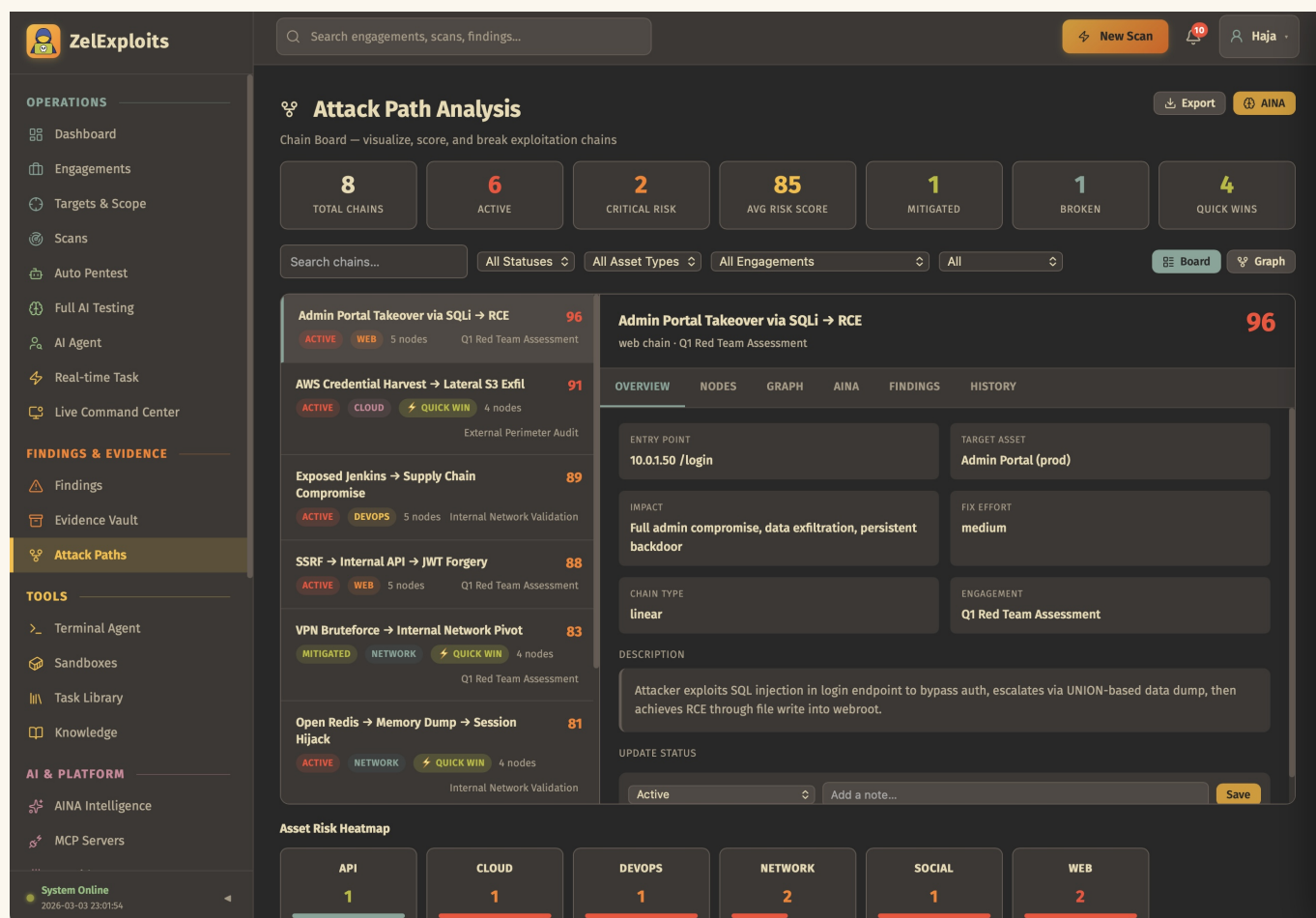
Advanced, hands-on cybersecurity training with Zelfire and AINA.

01 / THE EXPERIENCE

Your Browser. Hundreds of Virtual Machines.

Access Rocheston's Zelfire cloud training platform through your web browser. Work across interconnected applications, APIs, endpoints, identities, cloud workloads, networks, development pipelines, and AI-enabled workflows.

The platform library spans multiple enterprise scenarios. Students operate the targets assigned to their course environment.



ZelExploits: attack-path analysis. Inspect the proposed path, review the supporting evidence, and verify what actually happened on the target. Product screenshot; figures shown are product data.

AINA automates execution

Coordinates discovery, planning, testing, evidence collection, and adaptive follow-up.

You own the decisions

Configure scope, supervise operations, investigate evidence, and prove defensive improvement.

02 / LEARNING & PREPARATION

Build the skills. Bring the foundation.

COURSE OBJECTIVES

01 Own the attack surface

Discover assets, establish ownership, prioritize exposure, and preserve the baseline.

03 Engineer effective defenses

Test application, network, identity, zero-trust, and cloud controls without losing business function.

05 Build security automation

Write scoped ZelC and response workflows with approvals, failure handling, and verification.

07 Repair and secure releases

Review code, secrets, dependencies, SBOM changes, regression tests, and CI/CD gates.

02 Validate automated attacks

Scope an AI-assisted campaign and separate reported findings from verified target activity.

04 Hunt and reconstruct incidents

Calibrate detections and connect enterprise events, retrieval records, and AI-agent activity.

06 Evaluate AI-agent security

Test prompt injection, poisoned context, excessive permissions, and unsafe tool use.

08 Protect and assess evidence

Verify evidence integrity and map supported findings to selected RCF controls in Noodles.

Who should attend

- Penetration testers and red teams
- SOC analysts, threat hunters, and responders
- Security engineers and architects
- Application security and DevSecOps teams
- Cloud and identity specialists
- Experienced RCCE graduates
- Technical security leaders

Prerequisites

RCCE Level 2 or equivalent practical experience is recommended.

- TCP/IP, DNS, HTTP and networking
- Linux and Windows administration
- Web applications, APIs and authentication
- Cloud and identity fundamentals
- Log analysis and security investigation
- Basic scripting

Prior Zelfire or ZelC experience is not required.

03 / THE FIVE-DAY OUTLINE

From exposure to defense.

01 ATTACK

8 HOURS / 4 LABS

Attack surface management and autonomous penetration testing

LAB 01

Map the attack surface

Access the cloud range, review permissions, preserve Epoch Zero, and build an owned asset inventory.

LAB 02

Discover and prioritize vulnerabilities

Operate Vines AI, investigate false positives, enrich findings, and model selected paths in ZelBreach.

LAB 03

Run automated penetration testing

Configure ZelExploits and Zombiecop runners, practice pause/stop, and validate execution evidence.

LAB 04

Attack the AI-enabled enterprise

Test prompt injection, retrieval manipulation, context poisoning, and excessive tool permissions.

What you produce: Owned asset register, preserved baseline, prioritized test plan, validated findings, and an AI attack record.

02 DEFEND

8 HOURS / 4 LABS

Exposure reduction, continuous zero trust, and cloud defense

LAB 05

Protect services and measure exposure

Apply ZelWall policies, compare exposure, rescan, and repeat attack and business-transaction tests.

LAB 06

Engineer continuous verification

Simulate access policies, restrict agent capabilities, and rehearse emergency access and rollback.

LAB 07

Investigate cloud risk and drift

Trace multi-cloud risk, prioritize fixes, detect a configuration change, and verify remediation.

LAB 08

Secure tunnels and private services

Configure ZelTunnel, Zelton, and Vega; test permitted destinations, authentication, and revocation.

What you produce: Tested controls, exposure scorecard, agent capability worksheet, and emergency-recovery records.

Each lab: 105 minutes of practical work + 15 minutes of operational briefing or review. Breaks are additional.

03 / THE FIVE-DAY OUTLINE

From investigation to engineering.

03 INVESTIGATE

8 HOURS / 4 LABS

Enterprise threat hunting, agent forensics, and incident response

LAB 09

Hunt across enterprise sources

Search heterogeneous logs with ZelKill; test detections against malicious and benign activity.

LAB 10

Reconstruct the intrusion

Correlate events, source documents, retrieval records, agent memory, and actual tool actions.

LAB 11

Preserve onion-service evidence

Investigate a synthetic leak claim and record sources, UTC times, hashes, and custody history.

LAB 12

Coordinate and verify response

Build ZelSOAR workflows, reconcile partial actions, use supported communications, and record gaps.

What you produce: Tested detection, incident timeline, retrieval audit, custody records, and a response playbook.

04 CODE

8 HOURS / 4 LABS

Agentic AI Programming Language ZelC, DevSecOps, and protected evidence

LAB 13

Program scoped ZelC operations

Declare targets and permitted impact; compare rejected and allowed cases and verify runtime results.

LAB 14

Automate exposure comparison

Compare inventories and permissions, request or perform permitted remediation, and verify outcomes.

LAB 15

Secure software and the release

Repair code, compare SBOMs, test a failing CI/CD gate, and re-test the running application.

LAB 16

Protect evidence and assess controls

Test Zelen recovery and tamper rejection; review integrity, control mappings, and missing proof.

What you produce: ZelC automation, verified repair, differential SBOM, cryptographic tests, and reviewed control evidence.

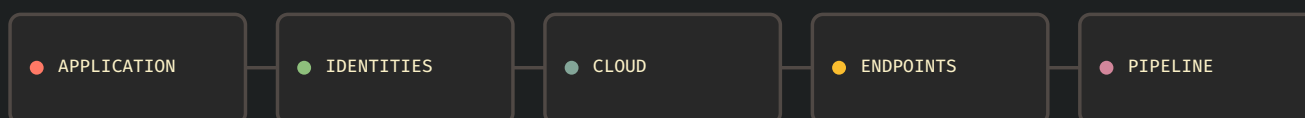
Each lab: 105 minutes of practical work + 15 minutes of operational briefing or review. Breaks are additional.

DAY 05 / OPERATE / 8 HOURS

One enterprise. One evolving incident.

Northstar Supply is a fictional enterprise with a customer application, identities, cloud workloads, endpoints, a source repository, a delivery pipeline, synthetic business data, and connected security telemetry.

Teams rotate through attack validation, defense, investigation, automation, and incident coordination.



The situation changes. A new exposure or privileged identity appears. AINA offers an unsupported conclusion. A response connector fails. A containment choice threatens a business service.

01

120 MIN

Discover, prioritize, validate

Rediscover with ZelMap, scan with Vines AI, model a scenario, and validate the selected campaign with ZelExploits.

02

120 MIN

Detect, hunt, reconstruct

Trace the incident and AI-agent activity. Investigate the surprise change and synthetic leak claim using evidence.

03

120 MIN

Contain, repair, recover

Reconcile partial actions, apply controls, repair weaknesses, rescan, repeat tests, and verify business transactions.

04

120 MIN

Demonstrate the result

Present a five-minute executive briefing and ten-minute technical review. Deliver the signed portfolio and Noodles remediation plan.

Four two-hour mission blocks include briefing, instructor review, and individual learning feedback.

04 / WHAT YOU TAKE AWAY

Leave with evidence. And work you can explain.

For students: a connected portfolio of practical work. For companies and HR teams: clear learning objectives, daily work products, and evidence of applied skills.

Testing and exposure

Owned assets, baseline, test engagement, validated findings, and an exposure-reduction scorecard.

Automation and access

Response playbook, ZelC source, failure tests, and an AI-agent capability boundary worksheet.

Protected evidence

Encrypted evidence package, tamper tests, recovery checks, fingerprints, and verification records.

Investigation and detection

Hunt logic, calibrated detection, incident timeline, agent-context audit, and custody records.

Software and release

Verified repair, regression checks, differential SBOM, and failing and passing CI/CD gate results.

Assessment and reporting

Selected RCF control assessment in Noodles, owners and target dates, briefings, and a signed manifest.

20 CORE ZELFIRE PLATFORMS

ZelMap

Assets and exposure

ZelTester

Testing engagements

ZelExploits

Automated penetration tests

ZelBreach

Scenario simulation

ZelWall

Network protection

ZelAccess

Identity and access

ZelZero-Trust

Contextual verification

ZelCloud

Multi-cloud risk

ZelDrift

Configuration changes

ZelXDR

Connected detection

ZelKill

Enterprise threat hunting

ZelScan

Artifact analysis

ZelRank

Threat intelligence

ZelSOAR

Response orchestration

ZelPosture

Operational posture

ZelCode

Software security

ZelC

Agentic AI programming

ZelDB

Evidence relationships

ZelFone

Mobile operations

ZelTunnel

Secure service access

Course-wide AI: AINA. **Supporting technologies:** Vulnerability Vines AI, Zombiecop Docker runners, Vega, Zelton, Wasabi, Zelen, Rosecoin, Noodles, and RCF.

RCF defines selected controls. Noodles organizes and analyzes the evidence used to assess them.

05 / COURSE COMPLETION

RCCE Level 3 Certification

Participants are awarded the RCCE Level 3 Certification upon completing the five-day Autonomous AI-Driven Cyberattack & Cyber Defense course.

The final exercise is a practical capstone and technical review. Teams demonstrate their work, explain their decisions, and review the evidence accumulated throughout the course.

Plan your training.

Students, teams, and HR enquiries

info@rocheston.com

rocheston.com

Enquire About RCCE Level 3



Scan or click
to enquire

Ask Rocheston about upcoming dates, delivery options, location, fees, included access, and team participation.

Five days. One connected learning experience.