



RDX ACADEMY

A DIVISION OF RDX ENTERPRISE, LLC

SOC ANALYST → SOAR ENGINEER · COURSE SYLLABUS

RDX SOAR Engineer Program

Build the governed automation that works your alert queue for you — Python, REST APIs, SOAR playbooks, AI-assisted operations, and governance.

★ Earn the **RDX Certified SOAR Engineer (RCSE)** credential

Human-led. Agent-assisted. Evidence-proven.

10 modules · 30+ hours · 3 core labs + capstone

Control the action. Prove the outcome.

Program overview — why this program exists

The RDX SOAR Engineer Program was created to address a growing gap in modern security operations: organizations need faster incident response, but speed without governance can create risk. Security Operations Centers face increasing alert volume, analyst fatigue, false positives, tool sprawl, and a shortage of professionals who can build reliable automation. Traditional SOC roles often focus on triage and escalation, while the next generation of security operations requires engineers who can design, test, govern, and prove automated response workflows.

Security Orchestration, Automation, and Response (SOAR) is not simply a technology category — it is a discipline that connects detection, enrichment, decision-making, response, documentation, and governance into a repeatable operational process. A strong SOAR engineer understands the SOC lifecycle, writes automation logic, integrates tools through APIs, designs playbooks, applies MITRE ATT&CK context, builds approval gates, and maintains an evidence trail that shows what happened and why.

Human-led. Agent-assisted. Evidence-proven.

Automation should not remove human judgment from consequential security decisions. Instead, it should remove repetitive toil, enrich alerts faster, recommend actions, and support analysts while keeping humans in command of high-impact response. Actions such as disabling accounts, isolating hosts, blocking infrastructure, or quarantining mailboxes are governed through approval workflows, role-based access control, and auditable evidence.

The program prepares learners to move beyond basic alert monitoring and into security automation engineering — spanning SOC foundations, Python automation, threat-intelligence enrichment, REST API integration, SOAR playbook design, SIEM and SOAR integration, incident-response automation, AI-assisted operations, governance workflows, and career development. The goal is not only to teach tools, but to develop the **judgment** required to build automation that is safe, explainable, and operationally useful.

A central theme is that **proof matters**. Certifications can open doors, but working projects demonstrate capability. The program is designed to help learners create portfolio-ready automation work that shows they can build real playbooks, integrate real security concepts, apply approval gates, document decisions, and produce an evidence-backed outcome.

The program also reflects where the field is heading. As AI agents become more common in security operations, the role of the SOAR engineer is moving upward. The future is not simply writing scripts or clicking through alerts — it is governing automation, validating agent recommendations, defining safe response boundaries, and proving that automated actions were authorized, appropriate, and effective. RDX Academy built this program to help students, SOC analysts, IT professionals, career changers, veterans, and security teams build practical SOAR skills in a structured way — to create engineers who can control the action and prove the outcome.

The mission

Build something real. Keep a human in command. Prove the outcome.

Course description

RDX SOAR Engineer Program is a hands-on, self-paced certification course that takes security practitioners from *working alerts by hand* to *building the governed automation that works the alert queue for them*. Across ten modules, students learn modern SOC operations, Python for security automation, REST API integration, threat-intelligence enrichment, SOAR playbook development, SIEM/SOAR integration, incident-response automation, AI-assisted operations, and the governance that makes automation production-ready. Students build three working automation tools and an end-to-end capstone, then earn the **RDX Certified SOAR Engineer (RCSE)** credential.

The course reflects how RDX builds in the real world: automation and AI **assist**, a human stays in **command** of consequential decisions, and every action leaves **evidence**.

FORMAT

Online · Self-paced

CONTENT

10 modules · 30+ hrs

TYPICAL PACE

6–10 weeks

HANDS-ON

3 core labs + capstone

ACCESS

Lifetime + updates

CREDENTIAL

RCSE digital badge

Who should take this course

- SOC Analysts (Tier 1 / Tier 2)
- Junior Security Engineers and Incident Responders
- Cybersecurity students and IT professionals transitioning into security
- Anyone targeting a **SOAR Engineer / Security Automation Engineer** role

Prerequisites

- Basic familiarity with security concepts (alerts, indicators, the incident lifecycle)
- Willingness to write a little code — **no prior Python required** (Module 2 starts from zero)
- A computer (Windows/macOS/Linux) and an internet connection
- **No paid SOAR platform or API keys required** — labs run with provided code and an offline mock mode

Learning outcomes

On completion, students will be able to:

1. Run modern SOC operations and reason about the alert-to-resolution lifecycle
2. Write Python confidently for security automation tasks
3. Call and integrate REST APIs across the security stack
4. Automate threat-intelligence enrichment of indicators
5. Build SOAR playbooks that codify response logic
6. Integrate SIEM and SOAR into a working detection-and-response loop
7. Automate incident-response actions safely

8. Apply AI assistants to security operations responsibly
9. Design governance and human-in-the-loop approval workflows
0. Position and advance a SOAR engineering career

Course outline — 10 modules

Core labs (★) ship as working Python the student keeps for their portfolio.

Module 1 — Modern SOC Operations

~2.5 hrs

The alert lifecycle (detect → triage → enrich → respond → close), SOC roles and tiers, why manual triage doesn't scale, and where SOAR adds leverage.

Lab: triage a 10-alert queue by hand and capture a baseline.

Module 2 — Python for Security Automation

~4.0 hrs

Python from zero for security work: data structures, files/JSON/CSV, functions, and the standard library a security engineer actually uses.

Lab: build a reusable IOC parser + log-line extractor.

Module 3 — Threat Intelligence Enrichment ★

~3.5 hrs

Indicator types and intel sources, your first REST API call, normalizing messy responses, scoring/confidence, caching and rate limits.

Lab: `module3_enrichment.py` — enrich a batch of indicators and emit verdicts.

Module 4 — REST APIs for Security Tooling

~3.0 hrs

HTTP/REST, authentication, pagination, rate limits, and robust error handling so you can integrate any tool in the stack.

Lab: authenticate to a security API; query it; handle paging and failures.

Module 5 — SOAR Playbook Development ★

~4.0 hrs

Playbook anatomy, triggers/tasks/branching, idempotency, context passing, testing, and human-in-the-loop approval gates.

Lab: `module5_playbook.py` — a phishing-triage playbook with an approval gate.

Module 6 — SIEM & SOAR Integration

~3.0 hrs

SIEM vs SOAR vs XDR, alert schemas and normalization, triggering SOAR from a SIEM, and closing the loop.

Lab: wire a SIEM alert into a SOAR trigger end-to-end and write back the verdict.

Module 7 — Incident Response Automation

~3.5 hrs

The automated IR lifecycle, what's safe to automate vs gate, containment actions, rollbacks, and measuring time-to-respond.

Lab: automate containment with safe rollbacks; re-run Module 1's queue and compare.

Module 8 — AI-Assisted Security Operations ★

~3.0 hrs

Where AI helps (and where it must not act alone), prompting for security tasks, grounding AI in evidence, the risks (hallucination, data leakage, prompt injection), and governance.

Lab: `module8_ai_assistant.py` — AI summary + recommendations behind a human-review gate.

Module 9 — Governance & Approval Workflows

~3.0 hrs

Approval gates, segregation of duties, audit logging and evidence, least privilege, change control, and mapping to compliance (SOC 2 / NIST concepts).

Lab: add an approval gate + immutable audit trail to your Module 5 playbook.

Module 10 — Career Development & RCSE Certification

~2.0 hrs

The SOAR engineer market, building a portfolio from your labs, résumé/LinkedIn, interview prep, capstone walkthrough, and the RCSE exam.

Deliverable: capstone kickoff + portfolio assembly.

Capstone project

Students design and build an end-to-end, governed automation: ingest an alert → enrich indicators → run a branching playbook → take a **gated** response action → produce an audit trail and an AI-written incident summary. Submitted as a code repo plus a short recorded walkthrough and scored against the certification rubric. The capstone gates the RCSE credential and is the student's primary portfolio piece.

Certification — RDX Certified SOAR Engineer (RCSE)

To earn the RCSE credential, students must:

1. Complete all 10 modules and their knowledge checks
2. Pass each module quiz (**75%**) and the final exam (**80%**)
3. Submit and pass the capstone against the rubric

Graduates receive a **verifiable digital badge** for LinkedIn and résumés, signaling demonstrated, hands-on ability to build **governed** security automation.

Assessment & support

COMPONENT	DETAIL
Knowledge checks	Ungraded, inline — instant feedback while you learn
Module quizzes	Graded, 75% to pass; contribute to completion
Final exam	Graded, 80% to pass; randomized question bank
Capstone	Scored against the certification rubric; gates RCSE
Support	Course Q&A / community; mentoring + capstone review on Professional
Guarantee	14-day satisfaction guarantee

Pricing & enrollment

PLAN	PRICE	INCLUDES
Basic	\$499	Full course, all labs, RCSE exam & credential, self-paced lifetime access + updates
Professional	\$999	Everything in Basic + capstone review, 1:1 mentoring, priority support, résumé/portfolio review
Elite	\$1,999	Everything in Professional + extended 1:1 coaching, portfolio & interview support

Founding Launch — 30% off through July 11: Basic \$349 · Professional \$699 · Elite \$1,399. Pre-order now to lock founding pricing; course access opens July 4, 2026.

Ready to enroll or learn more?

Enroll / request info: academy.rdxenterprise.com/soar-engineer · RDXenterprise@rdxenterprise.com

RDX Enterprise, LLC · RDX Academy · *Control the action. Prove the outcome.*
Syllabus subject to refinement as modules are updated; enrolled students receive all updates at no additional cost. Last updated: June 13, 2026.