ISAUnited CYBER ACADEMY

CYBER ACADEMY | PROFESSIONAL COURSE & CREDENTIAL PATHWAY

CYBERSECURITY AUTOMATION ENGINEER

Specialized Engineering Course + Certified Professional License Pathway

Build a disciplined automation engineering practice for cybersecurity operations and technology environments. Learn to define automation missions, analyze process and trust boundaries, engineer secure workflow logic across APIs, identities, and events, validate safety and rollback, and prove your work through an evidence-based cyber capstone.

COURSE IN ONE VIEW

Field: Automation Engineering
Level: Certified Professional
Delivery: 100% online, self-paced + instructor support
Pace: 5 days / 1 week
CPEs: 10
Assessment: Cyber Capstone Portfolio
Pathway: Cybersecurity Automation Engineer CPL
Tuition: $2,495 Pro Bundle=Course + CPL included. Payment options available

WHY THIS COURSE

- Move beyond isolated scripting and learn cybersecurity automation as a repeatable engineering discipline.
- Engineer secure workflows across APIs, events, identities, secrets, and security tooling with clear authority boundaries.
- Practice testing, rollback, telemetry, and evidence so automated actions can withstand operational and audit scrutiny.
- Finish with a real-world capstone portfolio rather than a multiple-choice exam.

WHAT YOU WILL LEARN

- Define automation missions, scope, workflows, human approvals, and authority constraints.
- Map control-plane components, APIs, events, identities, secrets, data flows, and trust boundaries.
- Engineer secure workflow logic with branching, retries, timeouts, idempotency, and safe failure behavior.
- Implement safeguards for authentication, authorization, schema validation, approval gates, and least privilege.
- Validate automations through simulation, release control, rollback, and telemetry analysis under normal and adverse conditions.
- Document evidence, operational metrics, residual risk, and improvement actions to defend automation decisions.

WHO THIS COURSE IS FOR

- Security engineers and architects building or improving automations.
- Practitioners supporting SOAR, DevSecOps, cloud, or security-tool integrations.
- Experienced cybersecurity professionals moving into automation engineering responsibilities.
- Professionals preparing for the Cybersecurity Automation Engineer CPL and public credential verification.

FIVE-MODULE LEARNING PATH

The course combines a common engineering foundation with a dedicated cybersecurity automation track. The sequence advances from mission and boundary analysis into structural design, secure workflow implementation, simulation-based validation, and operational reliability.

01	**Scope, System Dissection & TADA Threat Surface** **Define the mission and map the automation environment.** Clarify mission scope, workflows, owners, authority limits, and required human approvals. Map the automation control plane, target systems, APIs, events, identities, data flows, trust boundaries, and credible threat paths.
02	**Defensible 10 Architecture (D10A) & Structural Controls** **Design defensible automation architecture and control intent.** Use D10A and D10S to define micro-perimeters, identity and secrets boundaries, event paths, failure-domain isolation, least privilege, human approval gates, rollback expectations, and observability requirements.
03	**Advanced TADA Defensive Engineering & Protocol Security** **Engineer secure workflows and controlled action.** Implement secure workflow logic, API and webhook protections, schema validation, service identities, secrets discipline, retries, timeouts, idempotency, error handling, and release-ready safeguards.
04	**Applied Simulation & Telemetry Verification** **Validate behavior, safety, and operational evidence.** Run Cyber Simulations to test normal and adverse conditions. Capture execution, API, identity, queue, target-state, and telemetry evidence to prove correctness, safety boundaries, rollback readiness, and corrective actions.
05	**Operational Resilience & System Defense Synthesis** **Turn automation evidence into resilient operations.** Establish degraded and manual fallback modes, recovery baselines, lifecycle controls, value metrics, and the final Domain Defense Specification that explains ownership, evidence, and prioritized improvement.

APPLIED ENGINEERING PRACTICE ACROSS THE COURSE

01 DEFINE	Clarify mission, workflows, system boundaries, owners, authority limits, and conditions that must be protected.
02 MAP	Map the control plane, APIs, events, identities, secrets, data flows, trust boundaries, and critical dependencies.
03 ENGINEER	Build secure workflow logic, integration safeguards, release controls, and bounded automated actions.
04 VALIDATE	Test normal and adverse conditions, confirm telemetry, prove rollback behavior, and record corrective findings.
05 OPERATE	Measure health, reliability, coverage, and residual risk so you can maintain and improve automation.

OFFICIAL COURSE MATERIAL

- Digital Book
- Videos
- Templates
- Lab files and more

LEARNING EXPERIENCE

- 100% online and self-paced
- Technical instructor support
- Hands-on automation engineering labs
- Evidence-driven preparation for the Cyber Capstone portfolio

COMPLETE THE COURSE. PROVE THE CAPABILITY.

The professional path concludes with a solo, written Cyber Capstone Portfolio. You receive a real-world cybersecurity automation scenario and submit a concise set of defensible artifacts for evaluation - no multiple-choice test and no interview.

CYBER CAPSTONE PORTFOLIO - FIVE REQUIRED ARTIFACTS

1 Automation Mission & Workflow Coverage Plan	Define mission and system context, candidate workflows, automation-suitability decisions, owners, authority, constraints, and expected value.
2 Threat & Attack Path Analysis	Show process and data flows, APIs and events, schemas, trust boundaries, identities, permissions, secrets, and health dependencies.
3 Defensive Architecture	Present workflow logic, code or configuration, branching, safeguards, state handling, retries, timeouts, idempotency, and operating guidance.
4 Verification & Telemetry	Document test plans, expected and actual results, failure testing, approvals, release controls, rollback, and post-release validation.
5 Recovery & Engineering Evidence	Summarize execution health, coverage, reliability, outcome quality, residual manual paths, incidents, rollbacks, and prioritized improvements.

HOW YOU ARE EVALUATED

Part 1 - Technical Artifact Evaluation checks completeness, correctness, traceability, safety, and defensibility across the submitted work.

Part 2 - SKA Capability Profile evaluates disciplined engineering practice, reasoning, judgment, and professional communication using evidence from the portfolio.

COURSE & CPL OUTCOMES

- Certified Professional License (CPL) and Number
- Digital certification + verifiable License ID and issue date
- Public registry entry after successful evaluation
- License term: 3 years
- Renewal requirement: 40 CPE credits

READY TO REGISTER?

1 CHECK FIT

Cybersecurity Essentials is required. Review the program, schedule, tuition, and certification pathway before registering.

2 PREP YOUR INFO

Have your contact details, LinkedIn profile, and resume/CV ready for the Cyber Academy registration form.

3 REGISTER

Select the course program, identify your enrollment goal, submit the form, and follow the Academy onboarding instructions.

TAKE THE NEXT STEP

Register: isaunited.org/isaunited-school-of-engineering-cyber-defense-form
Tuition & Plans: isaunited.org/isaunited-membership-pricing-and-plans
Questions: info@isaunited.org

Workforce-Informed | Evidence-Governed | Publicly Verifiable

Tuition, course sequence, eligibility, and program details may change. Confirm current information on ISAUnited.org before enrollment.