Edversity.

## CYBERSECURITY ANALYST PROGRAM

# PROGRAM SYLLABUS

A 12-week, cohort-based program that produces a job-ready entry-level SOC analyst: weekly graded labs, a public portfolio, and a capstone.

Blue-Team First · SOC · Cloud · Web · AI Security

| DURATION | LIVE HOURS | SCHEDULE | SELF-STUDY |
|---|---|---|---|
| **12 WEEKS** | **72 HOURS** | **3 DAYS / WEEK** | **3–5 HRS / WEEK** |
| live cohort | instructor-led | 2 hours per day | labs & portfolio |

# PROGRAM POSITIONING

This program produces a job-ready entry-level Cybersecurity (SOC) Analyst, not a generalist who has merely touched many tools. It is built **blue-team-first** because defensive/SOC roles are the highest-volume, most remote-friendly, and most AI-resistant entry point into the field, today and in the future. Web application security is included as the realistic freelance and bug-bounty on-ramp; cloud and AI security are included as future-proofing.

**TARGET FIRST ROLES**

SOC Analyst (Tier 1), Security Analyst, Junior Security Engineer, IT Security Support.

**SECONDARY PATH**

Freelance web-app security and bug bounty.

**Honest expectation set with students up front:** the first job is almost always an analyst/defensive role, not “ethical hacker” on day one. Students who skip the weekly labs will not be job-ready; the portfolio, not attendance, is what gets them hired.

# LEARNING OUTCOMES

By completion, students will be able to:

01 Read network traffic and logs, and operate confidently across Linux and Windows

02 Understand the full attack lifecycle (MITRE ATT&CK) well enough to detect and respond to it

03 Find, exploit, and professionally report common web vulnerabilities (OWASP Top 10)

04 Run SIEM queries, write detections, and triage alerts like a Tier-1 SOC analyst

05 Execute an incident-response workflow and perform basic forensics and malware triage

06 Secure cloud (AWS/IAM) environments and detect suspicious cloud activity

07 Understand AI-driven threats, secure AI systems, and automate SOC work with Python

08 Apply GRC frameworks (NIST, ISO 27001, SOC 2) and build a remote/freelance career

09 Graduate with a public portfolio, ranked lab profiles, a security resume, and a cert roadmap

# 12-WEEK CURRICULUM

Three live sessions per week, each pairing theory with a graded hands-on lab.

## WEEK 01 SECURITY FOUNDATIONS & NETWORKING

**Goal:** Build the shared language and understand how networks work. You can't defend what you don't understand.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Intro to Cybersecurity & Career Map** | CIA triad, threat actors, attack surface, security roles (SOC/AppSec/Cloud/GRC), how hiring actually works | Set up home lab (VirtualBox + Kali + victim VM); create TryHackMe account |
| 2 | **Networking Essentials** | TCP/IP, OSI, ports, DNS, HTTP/S, common protocols | Wireshark: capture and read live traffic |
| 3 | **Network Security Concepts** | Firewalls, NAT, VPNs, segmentation, defense-in-depth | Analyze a pcap; flag suspicious traffic |

**SELF-STUDY 3–5 HRS** · TryHackMe “Pre-Security” path (free).

## WEEK 02 OPERATING SYSTEMS & SCRIPTING FOR SECURITY

**Goal:** OS fluency across Linux and Windows. Analysts live in terminals and logs.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Linux Essentials** | Filesystem, permissions, users, processes, services | Kali CLI drills: chmod/chown/sudo, process & service inspection |
| 2 | **Windows for Security** | Accounts, registry, processes, Event Viewer, key Event IDs, PowerShell basics | Explore Windows security logs; identify key Event IDs |
| 3 | **Scripting for Automation** | Bash + intro to Python for security tasks | Write a log-parsing script (Bash and/or Python) |

**SELF-STUDY 3–5 HRS** · TryHackMe Linux & Windows fundamentals rooms.

## WEEK 03 THE ATTACKER'S MINDSET

**Goal:** Understand how attacks work so you can detect and stop them. Offense is condensed into one focused week.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Attack Lifecycle & Frameworks** | Cyber Kill Chain, MITRE ATT&CK, recon & scanning concepts | Nmap: map and scan a target; navigate MITRE ATT&CK |
| 2 | **Common Attack Techniques** | Phishing, malware, credential attacks, lateral movement | Guided Metasploit demo: observe an exploit end to end |
| 3 | **Attacks as Seen by Defenders** | How each technique shows up in logs and telemetry | Run an attack in the lab and watch the artifacts it generates |

**SELF-STUDY 3–5 HRS** · MITRE ATT&CK Navigator exploration; TryHackMe “Cyber Kill Chain” room.

## WEEK 04 WEB APPLICATION SECURITY

**Goal:** Hands-on OWASP Top 10, the most freelance-viable skill in the program. Doubles as the freelance and bug-bounty bridge.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Web Architecture & Interception** | HTTP/S, cookies, sessions, authentication | Burp Suite: intercept and modify requests |
| 2 | **OWASP Top 10 in Practice** | SQLi, XSS, CSRF, IDOR, broken authentication | Exploit OWASP Juice Shop / DVWA |
| 3 | **Finding & Reporting Vulnerabilities** | Writing a professional vulnerability / bug-bounty report | Full write-up of a discovered vulnerability: the actual paid skill |

**SELF-STUDY 3–5 HRS** · TryHackMe web rooms; create a HackerOne / Bugcrowd account.

## WEEK 05 SOC FUNDAMENTALS & LOG ANALYSIS

**Goal:** Enter the blue team. This is the core employable skill of the program.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Inside a SOC** | SOC tiers, alert triage, workflow, log sources that matter | Analyze authentication logs; detect a brute-force attempt |
| 2 | **SIEM Hands-On** | SIEM concepts; searching and correlating events | Splunk (free) / Elastic: ingest logs and run queries |
| 3 | **Writing Detections** | Turning attacker behavior into alerts and use-cases | Build detection rules for the Week 3 attacks |

**SELF-STUDY 3–5 HRS ·** TryHackMe “SOC Level 1” path (begin).

## WEEK 06 THREAT DETECTION & MONITORING

**Goal:** Deepen detection: the day-to-day meat of SOC work. Mid-program assessment week.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Network Detection** | IDS/IPS with Snort/Suricata; signatures vs anomalies | Write and trigger Snort/Suricata rules |
| 2 | **Endpoint Detection** | EDR concepts, Windows event & Sysmon analysis | Hunt malicious activity in Windows/Sysmon logs |
| 3 | **Threat Intelligence** | IOCs, feeds, enrichment, reputation | Enrich an alert using VirusTotal & AbuseIPDB |

**SELF-STUDY 3–5 HRS ·** Continue SOC Level 1 path. Mid-program practical assessment due.

## WEEK 07 INCIDENT RESPONSE & FORENSICS BASICS

**Goal:** Know exactly what to do when something goes wrong.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Incident Response Lifecycle** | PICERL, playbooks, triage, containment | Run a tabletop IR scenario |
| 2 | **Investigation & Forensics** | Timelines, host/network artifacts, evidence handling | Investigate a compromised host end to end |
| 3 | **Malware Analysis Basics** | Safe static & dynamic analysis fundamentals | Analyze a sample in a sandbox (Any.Run / REMnux) |

**SELF-STUDY 3–5 HRS ·** TryHackMe DFIR / incident-response rooms.

## WEEK 08 CLOUD SECURITY

**Goal:** Cloud is where the jobs, the money, and the future are, and it's remote-heavy.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Cloud & IAM Fundamentals** | Shared responsibility model, identity, least privilege (AWS focus) | Build and test least-privilege IAM policies |
| 2 | **Cloud Misconfigurations & Attacks** | Public storage, exposed keys, over-privileged roles | Find and fix common misconfigurations |
| 3 | **Cloud Logging & Monitoring** | CloudTrail, GuardDuty concepts, cloud detections | Detect suspicious activity in cloud logs |

**SELF-STUDY 3–5 HRS ·** Microsoft SC-900 learning path (free) / AWS free-tier labs.

## WEEK 09 AI SECURITY & MODERN THREATS

**Goal:** The future of the field, and Edversity's natural edge over every local competitor.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **AI in Attack & Defense** | AI-driven phishing, deepfakes, automation; using AI in a SOC | Use an LLM to accelerate log triage and analysis |
| 2 | **Securing AI Systems** | LLM/prompt-injection attacks, OWASP Top 10 for LLMs, data poisoning | Prompt-injection exercise against a test app |
| 3 | **Automation & SOAR Basics** | Scripting repetitive work; playbook automation | Automate an alert-enrichment workflow in Python |

**SELF-STUDY 3–5 HRS** · Read OWASP Top 10 for LLMs; extend the automation script.

## WEEK 10 GRC & THE REMOTE CAREER PLAYBOOK

**Goal:** The most AI-resistant niche, plus how graduates actually earn remotely.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Governance, Risk & Compliance** | Risk, NIST CSF, ISO 27001, SOC 2: why compliance means jobs | Conduct a mini risk assessment |
| 2 | **Policies, Audits & Vendor Risk** | Security policies, audit readiness, third-party risk | Draft a security policy / gap assessment |
| 3 | **The Remote & Freelance Playbook** | Upwork/Fiverr security gigs, bug-bounty income reality, personal brand | Build LinkedIn + security resume; pick a freelance niche |

**SELF-STUDY 3–5 HRS** · Polish portfolio and public profiles.

## WEEK 11 CAPSTONE PROJECT

**Goal:** Prove it. The portfolio centerpiece that replaces a meaningless certificate.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Capstone Kickoff** | Choose a track: SOC investigation / web pentest report / cloud audit | Scope and begin the capstone |
| 2 | **Build & Mentorship** | Guided build with instructor feedback | Continue project; incorporate feedback |
| 3 | **Full-Scenario Challenge** | End-to-end attack/defense or investigation scenario | Complete the capstone deliverable |

**SELF-STUDY 3–5 HRS ·** Finalize GitHub portfolio and write-ups.

## WEEK 12 FINAL ASSESSMENT & JOB LAUNCH

**Goal:** Convert skills into interviews and offers.

| DAY | TOPIC | THEORY | PRACTICAL / LAB |
|---|---|---|---|
| 1 | **Final Practical Exam** | Scenario-based, CTF-style blue-team challenge | Timed hands-on exam |
| 2 | **Portfolio Review & Mock Interviews** | Capstone presentations; technical + behavioral prep | Peer mock interviews with feedback |
| 3 | **Career Launch** | Job-search strategy, cert roadmap, application sprint | Apply to 5 real roles / set up bug-bounty profile. Graduation |

**SELF-STUDY 3–5 HRS ·** Ongoing cert prep and job applications.

# ASSESSMENT & GRADING

Grades are practical and continuous. Attendance alone earns nothing. The portfolio and hands-on labs are the core of the assessment.

| COMPONENT | WEIGHT |
|---|---|
| Weekly lab submissions (graded pass / redo with feedback) | 30% |
| Weekly quizzes | 10% |
| Mid-program practical assessment (Week 6, SOC investigation) | 15% |
| Capstone project (Week 11) | 25% |
| Final practical exam + presentation (Week 12) | 20% |

**GRADUATION GATES: MANDATORY, PASS / FAIL**

Minimum 80% attendance; a complete public portfolio (GitHub write-ups + capstone); an active TryHackMe / HackTheBox profile; and a finished security resume + LinkedIn. The Edversity certificate is issued only when these are met, so it means something to an employer.

# CERTIFICATION & PROOF STRATEGY

Edversity does not pay for student certifications. Instead, the program is designed so graduates leave with free, verifiable proof of skill and are fully prepared to sit paid exams later at their own choice.

## FREE / NO-COST PROOF: BUILT INTO THE PROGRAM

- **Public GitHub portfolio** of lab write-ups and the capstone: Edversity's core proof artifact
- **Ranked TryHackMe "SOC Level 1"** completion and HackTheBox profile: third-party-verifiable hands-on skill
- **Fortinet NSE 1–3**: free, employer-recognized network security fundamentals
- **Google Cybersecurity Certificate**: free foundational blue-team training (Coursera, audit)

## PAID CERTS STUDENTS CAN PURSUE LATER: WE PREPARE THEM, THEY BUY THE EXAM

**ISC2 Certified in Cybersecurity (CC)** ~$199

The free-voucher program closed to new sign-ups on 20 May 2026, so this is now a paid exam.

**Microsoft SC-900** ~$99

The study path is free, and occasional free vouchers appear via Microsoft events.

**CompTIA Security+** ~$404

The aspirational gold-standard entry cert. Our curriculum is mapped to its domains, so a graduate can study toward it directly.

# TOOLS COVERED

All tools are free or free-tier, with no license cost to students.

| DOMAIN | TOOLS |
|---|---|
| **Traffic & Networking** | Wireshark, tcpdump, Nmap |
| **Web Security** | Burp Suite (Community), OWASP Juice Shop, DVWA |
| **Offense (awareness)** | Metasploit, theHarvester |
| **SIEM & Detection** | Splunk Free, Elastic/ELK, Snort/Suricata, Sysmon |
| **Incident Response & Malware** | Security Onion, Any.Run, REMnux |
| **Threat Intelligence** | MITRE ATT&CK, VirusTotal, AbuseIPDB |
| **Cloud** | AWS (free tier), IAM, CloudTrail |
| **Automation & AI** | Python, Git/GitHub, LLM assistant |
| **Practice Platforms** | TryHackMe, HackTheBox |

# CAREER & JOB-READINESS OUTCOMES

Every graduate leaves with a complete, employer-facing package, not just knowledge:

- A working home lab they can keep building on
- A public GitHub portfolio of write-ups and a capstone project
- A ranked TryHackMe / HackTheBox profile
- A security-specific resume and optimized LinkedIn profile
- Mock-interview reps, technical and behavioral
- A personalized certification roadmap (Fortinet/Google → CC/SC-900 → Security+)
- At least 5 live job or freelance applications submitted before graduation

# DESIGN RATIONALE

Internal note for the Edversity team.

> **Blue-team-first:** SOC/defense is the highest-volume, most remote-friendly, and most AI-resistant entry path. It is the honest answer to what the world needs now and in future.

> **Offense condensed to one week:** students learn to detect attacks without turning the course into a pentest program that can't be finished, or placed, in 12 weeks.

> **Web security retained:** it is the realistic freelance / bug-bounty income path for a global-remote audience.

> **Cloud + AI security added:** future-proofing and Edversity's clearest differentiator over local competitors.

> **Windows, Python and GRC added:** all job-critical and all missing from the previous curriculum.

> **Certificate tied to portfolio, not attendance:** fixes the “meaningless certificate” problem and reduces the drop-out-and-blame dynamic by setting honest expectations.

> **Assumes ~3–5 hrs/week self-study** on top of live hours. This is stated to students at enrollment; without it, no 12-week program produces a hire.