SkillCred

Cybersecurity Program

Master Offensive & Defensive Security. Build Security Tools. Protect Systems.

8	96	4	6
Weeks	Hours	Projects	Days/Week

HYBRID MODEL 2 Solo + 1 Pair + 1 Group Capstone

Dual Track
8W Standard + 4W Fast Track

Mentor Verified
Every project reviewed

PAT Certified
Score visible to all HRs

8-Week Syllabus

Mon–Sat | 2 Hrs/Day | 48 Sessions | 96 Contact Hours

01 Security Foundations & Networking

SOLO 1 START

CIA triad, TCP/IP, Wireshark, DNS/ARP, iptables, Nmap, OSI security

02 Linux Security & Scripting

SOLO 1 DELIVERY

Linux CLI, permissions, hardening (CIS), bash scripting, Python/Scapy

03 Web Application Security

SOLO 2 START

OWASP Top 10, SQLi, XSS, CSRF, SSRF, Burp Suite, secure coding, WAF

04 Penetration Testing

SOLO 2 DELIVERY

PTES methodology, OSINT, Nessus/OpenVAS, Metasploit, priv escalation

05 Crypto & Defensive Security

PAIR START

Encryption, PKI, TLS/SSL, SIEM (ELK), IDS (Snort/Suricata), threat hunting

06 Incident Response & Forensics

PAIR DELIVERY

IR lifecycle, forensics (Autopsy, Volatility), malware analysis, playbooks

07 Cloud Security & Architecture

CAPSTONE START

AWS/Azure IAM, CloudTrail, container security, compliance (ISO/NIST)

08 Capstone CTF & Demo Day

CAPSTONE DELIVERY

Red/blue team exercises, attack simulation, defense, CTF competition, demo

DAILY 2-HOUR SESSION

0:00–0:10	0:10–0:40	0:40–1:30	1:30–1:50	1:50–2:00
Recap	Concept	Build Sprint	Standup	Wrap

Your 4 Portfolio Projects

2 Solo (individual) + 1 Pair (collaborative) + 1 Group Capstone (team)

SOLO 1 | INDIVIDUAL | Weeks 1–2 Difficulty:

Automated Network Security Auditor

Multi-threaded port scanner with service version detection, OS fingerprinting, vulnerability mapping against CVE database, SSL/TLS audit, DNS enumeration, structured HTML/PDF reports with severity ratings. Scans /24 subnet in <60s, 90% port detection accuracy.

Tech: Python 3.10+, Scapy, Socket, python-nmap, Jinja2, asyncio HR Signal: Junior Security Engineer / SOC Analyst hire bar

SOLO 2 | INDIVIDUAL | Weeks 3–4 Difficulty:

Web Application Penetration Testing Toolkit

SQL injection scanner (union, blind, time-based), XSS scanner (reflected, stored, DOM), directory bruteforcer, auth tester (brute force, default creds), HTTP header analyzer, session tester. OWASP-aligned PDF reports with PoC payloads. 80%+ detection on Juice Shop.

Tech: Python, Requests, BeautifulSoup, Selenium, concurrent.futures, ReportLab HR Signal: Junior Penetration Tester hire bar

PAIR PROJECT | 2–3 STUDENTS | Weeks 5–6 Difficulty:

SIEM & Incident Response Command Center

Multi-source log ingestion, real-time parsing and normalization, correlation rules (brute force, port scan, priv escalation, lateral movement), alert generation with severity scores, investigation dashboard, IR playbook templates, forensic evidence collection. 5+ attack patterns, <30s alert latency, 1000+ events/sec.

Tech: ELK Stack (Elasticsearch, Logstash, Kibana) or Wazuh, Python, Flask/FastAPI, Docker

Student A: Log collection, parsing, Elasticsearch indexing, correlation rule engine | Student B: Kibana dashboards, alert management, IR playbook system, forensics integration

GROUP CAPSTONE | 5 STUDENTS | Weeks 7–8 | Pick 1 of 3 Difficulty:

Option 1: Enterprise Security Operations Platform

Asset discovery, continuous vulnerability scanning, compliance checker (CIS/NIST), SIEM with custom correlation, automated IR playbooks, executive security dashboard, API for Slack/Jira, role-based views (CISO/Analyst/Admin). Tech: Python, ELK, React, PostgreSQL, Docker, Nmap, OpenVAS

Option 2: AI-Enhanced Threat Intelligence Platform

Threat feed aggregation from OSINT, ML-based threat classification, IOC management and search, threat actor profiling, automated briefing generation, SIEM/SOAR integration API. Tech: Python, HuggingFace NLP, Elasticsearch, React, FastAPI, Docker

Option 3: Zero-Trust Network Access Controller

Device posture assessment, identity verification with MFA, micro-segmentation policy engine, continuous auth, risk-based access, session monitoring, admin console, audit logging. Tech: Python, React, PostgreSQL, Redis, Docker, OAuth/OIDC

Module Ownership (all capstones): A: Device/identity assessment | B: Policy engine, access rules | C: Monitoring, anomaly detection | D: Dashboard, audit logs | E: API, deployment, hardening

Two Career Pathways

Both available simultaneously — not mutually exclusive

Employment Track

1. Complete 4 verified projects
2. Take PAT certification exam
3. Portfolio published to HR Portal
4. HRs discover and shortlist you
5. Interview scheduled via platform
6. Offer extended — placement tracked

Startup Track

1. Build investor-grade capstone
2. Mentor verifies for Investor Portal
3. List project with pitch deck & demo
4. Investors discover your project
5. Pitch invitation and presentation
6. Startup mentorship and funding

Project Assessment Test (PAT)

Your certification score — visible to every HR on the platform

MCQs 20% | Coding 25% | Architecture 20% | Viva Defense 25% | Peer Review 10%

90–100 Elite
Top 5% — senior roles, startup founding

75–89 Pro
Job-ready with solid fundamentals

60–74 Certified
Entry-level — core concepts proven

Mentor Verification — The Trust Engine

No project reaches HR or Investor portal without rigorous mentor review.

Code Quality 25% | Functionality 25% | Architecture 20% | Docs 15% | Deployment 15%

Ready to Build Your Future?

4 verified projects | PAT certification | Two career pathways

ENROLL NOW

DOWNLOAD SYLLABUS