

Cybersecurity

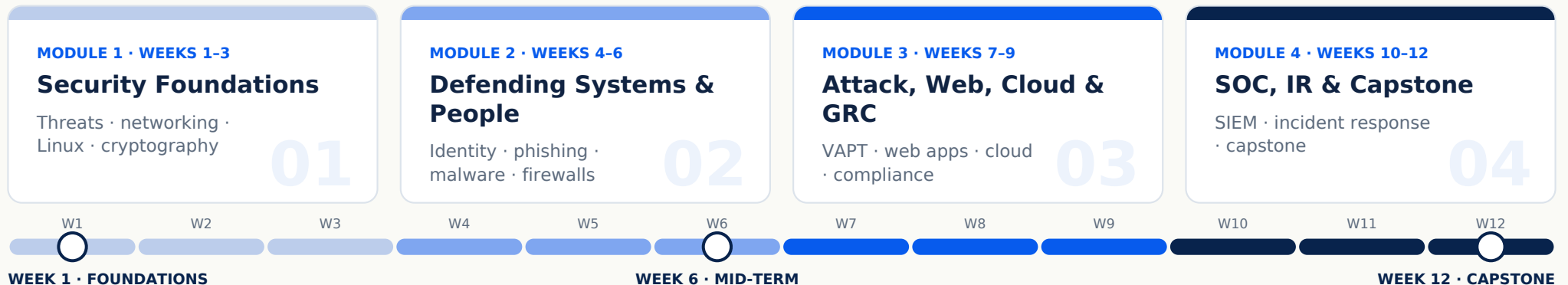
Investigate and protect. Takes final-year CS/IT students from foundations to SOC-ready, aligned to CompTIA Security+.

Target roles: SOC Analyst (L1) · Junior Security Analyst · GRC / ISMS Associate

12 WEEKS	4 MODULES	72 CONTACT HOURS	70% PRACTICAL GRADING	3 / 5 DIFFICULTY
--------------------	---------------------	----------------------------	---------------------------------	----------------------------

AT A GLANCE

Your 12-week journey



Capstone = the final team project in Week 12: students apply the whole course to one real-world problem, then present it and write it up.

YOU LEAVE WITH

✓ Capstone and a lab portfolio

✓ Ready for ISC2 CC, then Security+

✓ SOC Analyst (L1) · GRC Associate

Course outline is subject to change to reflect industry trends and vendor updates. See Important notes on the last page.

BEFORE YOU START

Difficulty and prerequisites

WHY IT'S INTERMEDIATE

Breadth: defense, offense, cloud and GRC in 12 weeks; many tools; Security+ level content.

PREREQUISITES · EDUCATION - Final-year bachelor's student or recent graduate - CS, IT, ECE or a related field - Comfortable reading technical English	PREREQUISITES · SKILLS - Networking basics: OSI, TCP/IP, IP addressing - Operating system basics - Any programming language helps (optional)	LAPTOP AND SETUP 64-bit laptop, virtualization enabled 16 GB RAM recommended (Kali + target VM) 50 GB free disk - Stable internet connection
--	---	--

PROGRAM FORMAT

How every week runs

Session	Format	What happens
Learn class	Instructor-led · 2 hrs	Concepts, terminology and a live instructor demo
Practice class	Instructor-led · 2 hrs	Instructor-led hands-on practice, then a case study discussion
Lab	2 hrs · instructor available	Guided ticket-style task done by the student, with the instructor on hand for questions; submitted with a short written report

Week 1: Foundations Every track opens the same way: a baseline skills quiz, lab and tool setup, how IT systems fit together, Linux and Windows command-line basics, and workplace habits (tickets, documentation, professional email). It levels the batch before track content starts.

Instructor access Students can email the instructor anytime for clarifications, outside class and lab hours.

Assessment 70% of the grade is practical: weekly lab reports, the mid-term practical in Week 6 and the capstone in Week 12. Every module has a required core lab (entry level) and an optional stretch lab (mid-level). The capstone is graded Core or Advanced; Advanced requires the stretch labs.

CAREER LADDER

Entry roles, and where they lead

ENTRY · 0-2 YEARS SOC Analyst (L1) / Associate Analyst, Cyber Defence Center · Junior Security Analyst (vulnerability and patch management) · GRC / ISMS Associate Core labs in Modules 2-4 · ISC2 CC, then Security+	→	NEXT STEP · 2-5 YEARS SOC Analyst (L2) / Incident Responder · VAPT / Application Security Engineer · GRC / ISO 27001 Analyst · Cloud Security Engineer Stretch labs: detection tuning, client-ready VAPT report, MFA rollout · CySA+, eJPT or CEH, ISO 27001 LA
---	---	---

Next-step roles need on-the-job experience. Stretch labs and the next certifications give graduates a head start toward them.

CURRICULUM

Four modules, twelve weeks

Module 1 · Security Foundations

Weeks 1-3

Outcome: Explains how attacks happen, reads network traffic, works on Linux and Windows command lines.

Week	Learn class	Practice class	Lab (instructor available)	Case study
1. Foundations	Baseline quiz; how IT systems fit together; CIA triad, threats, vulnerabilities, risk; career map	Linux and Windows command-line basics; the kill chain and MITRE ATT&CK; at a glance	Set up VirtualBox with Kali and a target VM; TryHackMe account; first CLI tasks	WannaCry 2017
2. Networking for security	TCP/IP, ports, DNS, HTTP/S, DHCP, ARP through an attacker's eyes	Wireshark: cleartext credentials, ARP spoofing, DNS abuse	Answer 10 questions from a packet capture	Dyn DNS / Mirai 2016
3. Operating systems and cryptography	Linux and Windows security: users, permissions, processes, logs	Hashing, encryption, TLS, certificates, password storage	Crack weak hashes with John or Hashcat, then fix the storage	LinkedIn 2012 hash leak

STRETCH LAB · MID-LEVEL Script a log parser in Python or Bash that flags brute-force attempts; harden a Linux server against a CIS benchmark checklist.

Module 2 · Defending Systems and People

Weeks 4-6

Outcome: Hardens identity, email, endpoints and networks. Ends with the mid-term.

Week	Learn class	Practice class	Lab (instructor available)	Case study
4. Identity and access	Authentication, MFA, password attacks, least privilege, Active Directory basics	Session and token attacks, SSO, OTP and SIM-swap fraud	Brute-force a test login with Hydra, then harden it	Twitter 2020 admin tool compromise
5. Social engineering and malware	Phishing, vishing, UPI and "digital arrest" scams; analyzing a suspicious email	Malware families, ransomware lifecycle, basic static analysis, EDR	Dissect a phishing email and write a user advisory	AIIMS Delhi 2022; Kudankulam 2019
6. Network and endpoint defense	Firewalls, IDS/IPS, VPN, segmentation, zero trust, hardening	Mid-term assessment (quiz + practical)	Write firewall rules and Suricata signatures	Cosmos Bank 2018

STRETCH LAB · MID-LEVEL Roll out MFA and conditional access in a lab Active Directory or Entra ID tenant; write a phishing response playbook.

Module 3 · Attacker's View, Web, Cloud and GRC

Weeks 7-9

Outcome: Runs a scoped vulnerability assessment, tests a web app, audits a cloud account against regulation.

Week	Learn class	Practice class	Lab (instructor available)	Case study
7. Ethical hacking and VAPT	Scope and rules of engagement; recon, OSINT, Nmap	Vulnerability scanning, CVE/CVSS, Metasploit demo, writing a finding	Scan and exploit a vulnerable VM; one-page VAPT finding	Equifax 2017
8. Web application security	OWASP Top 10: SQL injection, XSS, broken access control	Burp Suite, API security, secure coding habits	Attack then fix DVWA or OWASP Juice Shop	BigBasket 2020; Domino's India 2021
9. Cloud security and GRC	Shared responsibility, IAM misconfiguration, exposed storage	ISO 27001, NIST CSF, IT Act, DPDP Act 2023, CERT-In reporting	Audit a misconfigured cloud account; write a risk register	Capital One 2019; Star Health 2024

STRETCH LAB · MID-LEVEL Run a full scoped VAPT on a multi-host lab; deliver a client-ready report with risk ratings and a remediation plan.

Module 4 · SOC, Incident Response and Capstone

Weeks 10-12

Outcome: Triage alerts in a SIEM, works an incident end to end, presents a capstone.

Week	Learn class	Practice class	Lab (instructor available)	Case study
10. SOC and monitoring	SOC tiers, SIEM, log sources, alert triage, SLAs, escalation	Hands-on Wazuh SIEM: searching logs, building a detection; Microsoft Sentinel and KQL basics	Triage 8 simulated alerts as tickets	SolarWinds 2020
11. Incident response and forensics	NIST IR lifecycle, containment, evidence, basic forensics	Ransomware tabletop exercise with changing injects	Investigate a compromised host; write the incident report	Colonial Pipeline 2021; WazirX 2024
12. Capstone and career launch	Capstone presentations: one real breach analyzed end to end	Final practical; certification and career planning	Capstone report; mock technical interview	Student-chosen

STRETCH LAB · MID-LEVEL Tune Wazuh rules to cut false positives and write custom detections mapped to MITRE ATT&CK; act as incident commander in the tabletop.

TOOLS AND CERTIFICATIONS

What students use and where they go next

Tools: Kali Linux, Wireshark, Nmap, Metasploit, Burp Suite, Wazuh SIEM, Microsoft Sentinel (KQL), Suricata, TryHackMe.



Third-party certification exam fees are not included in the program. See Important notes.

CAREER SERVICES

Support through all 12 weeks

Service	What the student gets	When
Instructor access by email	Questions answered anytime by email, beyond class and lab hours	Weeks 1-12
Resume builder assistance	A track-specific resume built from lab reports and the capstone; one-to-one review and LinkedIn profile check	Draft by Week 6, final in Week 12
Certification path	Personal plan naming the first exam, the anchor exam and the next step; exam-style practice questions	Plan in Week 1, review in Week 12
Career build assistance	Role map for the track, portfolio of lab work on GitHub, interview prep and a mock technical interview	Weeks 1, 6 and 12
Talent Pool	Top performers, especially those with an Advanced capstone, are considered for Ampleopp Solutions and client opportunities	After Week 12

IMPORTANT NOTES

Curriculum updates	This outline reflects current industry practice. Topics, tools, labs, case studies, sequence and schedule may be updated to keep pace with industry trends, vendor and exam changes, and the needs of each batch. Core learning outcomes are maintained.
Certifications	Certification names, exam codes, content and fees are set by third-party vendors and may change. Exam fees are not included in the program.
Career outcomes	Career opportunities are not guaranteed and are subject to candidate performance, skill suitability, actual client requirements and the respective organization's selection process.
Trademarks	Product and certification names mentioned are trademarks of their respective owners. Ampleopp TechBuild is not affiliated with or endorsed by these vendors unless stated.