



TERAS

CYBER FROM THE CENTRE

SAMPLE SYLLABUS · FIRST SEMESTER

What a Teras-powered *first semester* looks like.

A worked example of a 12-week Foundation semester: the modules, the weekly hours, the on-platform labs and missions, and how learners are assessed. A starting point to take to your committee, shaped with your faculty before it runs.

PROGRAMME

Foundation

MODULES

CYB101 + CYB102

STRUCTURED HOURS

60 over 12 weeks

DELIVERY

Faculty-led

Two foundation modules. *One semester.*

A Teras first semester delivers the Foundation pathway, CYB101 and CYB102, as one faculty-led course. Learners spend roughly five hours a week in structured work: short sessions led by your faculty, then hands-on labs and missions on the Teras platform between classes. Across 12 weeks that is 60 hours of structured time, and the practical baseline every later module builds on. The sample below uses Foundation because it is where most institutions start. Your faculty can re-sequence it, or swap in a different pair of modules, during scoping.

CYB101 Cyber Fundamentals

30 HOURS · NO PRE-REQS

Establishes the conceptual and practical baseline for every later module. Learners develop the analyst's habits of mind: they read a security alert and articulate its impact in terms of confidentiality, integrity and availability, use the Windows command line and PowerShell to triage a host, and place attacker techniques within the MITRE ATT&CK matrix.

TOPICS COVERED

- CIA triad & security principles
- MITRE ATT&CK framework
- Identity, access & MFA
- Network & process triage
- Threat actors & motivation
- Cryptography & TLS
- Windows CLI & PowerShell
- Encoding & threat modeling

LEARNERS WALK AWAY ABLE TO

- Triage a Windows host from the command line
- Place an attack within the MITRE ATT&CK matrix
- Reason about authentication, hashing and TLS without relying on jargon

CYB102 Linux for Security Practitioners

30 HOURS · NO PRE-REQS

Builds the operational fluency every defensive analyst needs on Linux endpoints, servers and cloud instances. Learners operate confidently from the shell to investigate active processes, network connections, scheduled tasks and authentication events, configure SSH securely, and read Linux audit logs to reconstruct system activity.

TOPICS COVERED

- Filesystem & navigation
- Text-processing pipelines
- User & group administration
- SSH config & key management
- Permissions & ownership
- Process & service management
- Linux networking from CLI
- Logs: auth, syslog, journald, auditd

LEARNERS WALK AWAY ABLE TO

- Investigate a compromised Linux host from the shell
- Configure SSH and key management to baseline
- Read auth.log, syslog, journald and auditd to reconstruct activity

The 12-week plan.

CYB101 runs first to set the baseline, then CYB102 builds Linux fluency on top of it. Each week pairs a faculty-led session with on-platform labs and missions, and most weeks carry an assessment touchpoint so progress is visible to faculty in real time. Hours shown are structured time per week.

WEEK	FOCUS	ON-PLATFORM WORK	HRS	ASSESSMENT
CYB101 • CYBER FUNDAMENTALS				
Week 1	Security principles & the CIA triad	Orientation lab; first guided lab on triage concepts	5	Diagnostic quiz
Week 2	Threat actors & the ATT&CK matrix	ATT&CK mapping lab; technique-spotting exercise	5	Knowledge check
Week 3	Cryptography, identity & access	Hashing & TLS lab; MFA configuration lab	5	Graded lab
Week 4	Windows CLI & host triage	PowerShell triage lab; process enumeration mission	5	Mission rubric
Week 5	Network state & encoding	Network-state lab; encode/decode challenge	5	Knowledge check
Week 6	Threat modeling & consolidation	Capstone triage mission on the live cyber range	5	CYB101 module assessment
CYB102 • LINUX FOR SECURITY PRACTITIONERS				
Week 7	Filesystem, permissions & ownership	Guided shell labs; permissions investigation	5	Graded lab
Week 8	Processes, services & users	Service-management lab; account-audit exercise	5	Knowledge check
Week 9	Text-processing & scripting	Pipeline lab; shell-scripting fundamentals lab	5	Graded lab
Week 10	Linux networking & SSH	CLI networking lab; SSH & key-management lab	5	Mission rubric
Week 11	Logging & activity reconstruction	auth.log / journald / auditd investigation mission	5	Graded mission
Week 12	Compromised-host capstone	End-to-end Linux investigation on the live range	5	CYB102 module assessment
Total structured time • 2 Foundation modules			60	2 module assessments

HOW TO READ THIS

This is an illustrative cadence, not a fixed timetable. Faculty set session times and pacing; the platform work, labs, missions and assessments are ready out of the box. Institutions running on a longer calendar often spread the same 60 hours across a 14 or 15-week term, or run CYB101 and CYB102 in parallel threads.

How learners are *assessed*.

Assessment on Teras is continuous and evidence-based. Learners are scored on what they can do on a live system, not only on what they can recall, and faculty see progress as it happens rather than at the end of term.

RUBRIC-GRADED LABS

Hands-on, scored work

Guided labs and split-pane exercises are graded against the same rubrics security operations centres use to evaluate hires, so a grade maps to a real-world competency.

MISSION SIMULATIONS

The live cyber range

Mission-based incident scenarios run on real cloud-hosted virtual machines. Learners work an incident end to end and are assessed on the decisions and actions they take.

ASSESSMENT BANK

Anti-cheating by design

A large assessment bank with anti-cheating variants maps to the underlying skill taxonomy, so each cohort sees a different set and results stay comparable and credible.

VERIFIABLE PORTFOLIO

Evidence that travels

Every learner finishes with a portfolio of completed labs and missions, scored to a recognised framework, that they can show employers. A record of capability, not just a certificate.

— HOW IT IS DELIVERED

Faculty-led, *platform-supported*.

Your faculty teach the course. CFCI certifies and refreshes them through Train-the-Trainer, and they inherit a curriculum that is already current and stays that way. Between sessions, learners work on the platform with support built in:

SOCRATIC AI TUTOR

Support without shortcuts

A peripheral hint assistant that points learners toward the next step and never hands them the answer. It keeps learners moving between classes and directly addresses the AI-cheating concern.

CYBER ENGLISH LAB

Technical language, built in

An embedded CEFR-aligned English module with a cyber glossary, available alongside the course in six languages, so a mixed-proficiency cohort can keep pace.

See the *real* thing, with your modules.

Book a 30-minute platform demonstration and we will shape a syllabus around your programme, standards and faculty.

earnest@cfcsea.com