CyberLifeCycle

TRAINING FOR YOUR TEAMS

Managing vulnerabilities and the software lifecycle

Learn to decide which alerts to address, organise fixes and plan for end of support. Through a practical case, build a process you can adapt to your organisation.

Opening soon · Opening date confirmed before enrolment

14 hours, in two 7-hour units	Remote, self-paced, with written support
32 videos, practical exercises and a final case file	€990 excluding VAT per participant

This document sets out the eleven modules, activities, deliverables, prerequisites, support arrangements and pricing. It is neither enrolment nor a contractual offer.

OBJECTIVES AND AUDIENCE

What you will be able to do

- Build an inventory that genuinely supports assessment and shows what is missing.
- Set up reliable CERT-FR monitoring and keep track of advisory updates.
- Analyse your artefacts with Trivy and Syft, and know how to decide when two tools disagree.
- Read CVSS scores critically and justify priorities based on how a system is actually used and exposed.
- Feed Dependency-Track, with or without a pipeline, and keep older versions still in service under watch.
- Organise responsibilities: who assesses, decides, fixes and verifies.
- Understand where DefectDojo fits in the process and spot a closure that lacks evidence.
- Track fixes, exceptions and support deadlines, then prepare decisions.

Who should take this course?

Who it is for	Using the course
CISOs and deputies	Oversee the process, prepare decisions and track residual risks.
Security, systems and network administrators	Assess their scope, organise actions and supply technical evidence.
Security engineers and vulnerability analysts	Analyse reports and SBOMs, prioritise and track findings.
IT and DevSecOps teams	Connect dependencies, services, changes and fix verification.
Vulnerability coordinators and IT consultants	Assign actions and report to the system owner, in-house or as a service.

Prerequisites

Basic systems and networking knowledge, spreadsheet skills, reading simple JSON and running the supplied commands. All participants complete the practical exercises.

FORMAT AND ARRANGEMENTS

14 hours, two 7-hour units

The course divides 14 hours between videos, exercises and assessments, at your own pace with written support.

Unit	Videos	Guided practice	Assessments	Total
Unit 1 · Identify and assess	150 min	210 min	60 min	7 hours
Unit 2 · Prioritise and manage	140 min	250 min	30 min	7 hours
Total	4 h 50 min of video	7 h 40 min of guided practice	1 h 30 min of assessment	14 h

Support

You have 30 days to complete the course, with a recommended two-week schedule. Demonstrations, submitted exercises and answer keys guide you at each stage.
Support is provided in writing: replies within seven calendar days and individual feedback on the final case file within seven days of submission. Targeted resubmission may be offered. Technical blockers are taken into account when setting submission deadlines.
You need a computer, internet connection, spreadsheet software, a terminal and access to the training lab. A technical check precedes access activation. Installation and download time is additional to the 14-hour course.

The problem addressed

A scan report or security advisory is not enough to decide a fix. Identify the component, confirm applicability, understand exposure, assign the action and verify the result. The course builds this workflow through one practical case.

- A version or configuration is missing: what should you investigate?
- Sources report different scores: what should you retain and how do you decide?
- A finding disappears after reimport: has remediation actually been proved?
- Software is approaching end of support: who decides the next steps, and when?

DETAILED SYLLABUS

The eleven modules

Unit 1 · Identify and assess · 7 hours

M01 Organise vulnerability management — 1 hour

video 30 min · practice 15 min · assessment 15 min

Objective. Allocate responsibilities and define the checks required at each stage.

- Review how vulnerability tracking is organised today, in-house or through a provider.
- Assign roles: collection, assessment, remediation, verification and risk acceptance.
- Define the steps, expected evidence, emergency handling and cover during absences.

Required output. A process sheet, a working scope and a review schedule.

M02 Connect inventories, projects, versions and deployments — 45 min

video 15 min · practice 30 min · assessment 0 min

Objective. Build an inventory that supports applicability checks and action assignment.

- Identify assets, their owners and what they mean for the business.
- Link each project to its versions and where they are deployed, older versions included.
- Record missing information and assign who should provide it.

Required output. A usable inventory and a register of deployed versions.

M03 Collect and process CERT-FR advisories — 1 hour

video 20 min · practice 40 min · assessment 0 min

Objective. Receive relevant publications and trace revisions through to the local decision.

- Choose the right official sources and configure collection.
- Automate advisory retrieval and check that it keeps working over time.
- Spot what changes between revisions and turn it into actions.

Required output. Working CERT-FR monitoring and an assigned review queue.

M04 Scan and analyse with Trivy — 1 h 45 min

video 40 min · practice 65 min · assessment 0 min

Objective. Produce reliable reports and tell the difference between a detection, evidence and a conclusion.

- Frame the scan: authorised scope, versions analysed and freshness of the vulnerability database.
- Compare scans before and after a fix under identical conditions.
- Explain why a finding disappears, or why it persists.

Required output. Comparable Trivy reports and a reasoned reading of the differences.

M05 Produce and import SBOMs with and without a pipeline — 1 h 30 min

video 30 min · practice 60 min · assessment 0 min

Objective. Produce reliable SBOMs and get them to the right place, with or without a pipeline.

- Generate SBOMs with Syft and Trivy, then understand how they differ.
- Publish from a pipeline and check that the import reached the right version.
- Organise collection without CI: supplier SBOMs, provenance and renewal.

Required output. A verified SBOM supply chain, with and without a pipeline.

M06 Assess and validate the first unit — 1 hour

video 15 min · practice 0 min · assessment 45 min

Objective. Assess the case study on your own and justify your choices.

- Assess the case-study alerts independently.
- Justify the difficult cases and check overall consistency.
- Compare with the model answer and refine your analysis.

Required output. A complete assessment, graded with feedback.

Unit 2 · Prioritise and manage · 7 hours

M07 Prioritise and interpret scores — 1 h 15 min

video 25 min · practice 50 min · assessment 0 min

Objective. Justify priorities beyond the raw score.

- Gather available CVSS scores and handle cases where none exists.
- Adjust a score to your environment and justify the change.
- Prioritise the backlog and launch the necessary investigations.

Required output. A prioritised backlog with traceable priority decisions.

M08 Monitor a portfolio in Dependency-Track — 2 hours

video 35 min · practice 85 min · assessment 0 min

Objective. Track a portfolio of versions in Dependency-Track and see where DefectDojo fits.

- Check source status and import SBOMs.
- Link versions to their deployments, older versions included.
- Handle an alert on an older version and spot an unproven closure in DefectDojo.

Required output. A tracked portfolio, verified imports and documented decisions.

M09 Manage fixes and exceptions — 1 h 15 min

video 25 min · practice 50 min · assessment 0 min

Objective. Write verifiable actions and manage deferral without hiding risk.

- Write remediation tickets with clear closure criteria.
- Frame a temporary exception: who requests it, who approves it and until when.
- Check the evidence after a fix before closing.

Required output. Actionable tickets, a well-framed exception and evidence-based closures.

M10 Plan for software end of support — 1 hour

video 20 min · practice 40 min · assessment 0 min

Objective. Verify coverage and trigger a migration plan before support ends.

- Read a vendor support page and identify the right edition and branch.
- Record the deadline, its source, its owner and what still needs confirming.
- Prepare the decision and the migration milestones.

Required output. A documented migration path before the deadline.

M11 Present and assess the complete case file — 1 h 30 min

video 35 min · practice 25 min · assessment 30 min

Objective. Present clear decisions to system owners and demonstrate the course skills.

- Check that the figures add up and build a summary.
- Present findings and the decisions required to leadership, without hiding limitations.
- Final assessment on new situations.

Required output. A final case file and a presentation ready to deliver.

PRACTICAL WORK AND LAB

A case file adaptable to your scope

- Inventory and source register
- Process sheet: roles, evidence, regular tracking, cover and escalation
- Project, version, deployment and SBOM import registers
- Applicability case files with evidence and unknowns
- Side-by-side review of Trivy reports and SBOMs
- Justified priorities, Dependency-Track portfolio review and DefectDojo case analysis
- Sample pipeline and a non-CI/CD data-input procedure
- Remediation tickets and a temporary exception
- Support deadline tracking with owners and milestones
- Decision summary and implementation plan

Two portfolio data-input workflows

With a CI/CD pipeline

Generate an SBOM from the delivered artefact, retain its provenance and publish it to the correct project and version. Verify that processing has completed and connect results to action tracking.

Without a pipeline connection

Centralise SBOMs from teams and suppliers, link them to deployed versions and organise reassessment and updates. Older versions still in use remain monitored.

Without a pipeline, the server still refreshes its vulnerability sources while SBOMs arrive manually. A fully isolated environment needs a dedicated transfer process.

Case study and lab

The Atelier Nova case study is fictional, so you never need to share data from your employer or clients. Exercises take place in a dedicated lab, checked before access opens.

PRICING AND ENROLMENT

Two options, the same course

Individual

€990 excluding VAT

per participant

14-hour course, 30-day access, videos, exercises and templates, dedicated training lab, assessments, written support and feedback on the final case file.

Team of five participants

€3,990 excluding VAT

for 5 named accounts, equivalent to €798 excluding VAT per participant

The same self-paced course, access period and individual support arrangements. Team access is activated for the period agreed in the quote.

VAT treatment is specified in the quote. Opening date and enrolment terms are confirmed in writing. Work specific to your systems and private sessions require a separate quote. Contact us for other team sizes.

Frequently asked questions

Is this suitable for an in-house team?
Yes. The methods apply to in-house teams and to providers managing a client's software.

Do I need to be a developer?
No. You do need to read simple JSON and run the supplied commands. Basic systems and networking knowledge remains necessary.

Does this mean two live training days?
No. This is a supported, self-paced course in two seven-hour units, completed during the thirty-day access period.

Will I use the tools in practice?
Yes. You work with Trivy, Syft and Dependency-Track in a dedicated lab, with and without a pipeline. DefectDojo is covered in a guided demonstration. Access is checked before the course opens.

Does the course lead to certification?
A completion statement may be issued with assessment results. The course does not award a professional certification.

Can I enrol immediately?
Enrolment is not yet open. You can view the syllabus, request a quote or ask for an opening notification.

Can I share an account with my team?
Access is individual. The team offer includes five named accounts.

Contact and quotes

For a quote or opening information, use cyberlifecycle.fr/en/training. Please indicate participant count and your requirements.

CyberLifeCycle · cyberlifecycle.fr/en/contact · +33 6 03 85 17 57
cyberlifecycle.fr/en/training

CyberLifeCycle · SIREN 941 082 026 · 27 impasse des Réfractaires et Maquisards, 31100 Toulouse