

Your vulnerability management, taken care of.

You provide your inventories. CyberLifeCycle handles vulnerability monitoring, assessment and false positives. Receive targeted alerts, priorities, metrics and reports to organise fixes and plan for end of support.

01

MONITOR

Inventory-based monitoring

02

ASSESS

Applicability and priorities

03

MANAGE

Alerts, reports and actions

FROM YOUR INVENTORIES TO A WORKING PROCESS

A turnkey service based on your products and versions: monitoring setup, vulnerability and support tracking, alerts and ongoing reporting.

WHO IS IT FOR?

Business leaders • CIOs and CISOs • IT providers, software vendors and industry

01 / YOUR ORGANISATION'S CHALLENGE

Vulnerability management under control.

Identify what affects your estate and organise priority treatments.

01 Monitor your software estate

Use inventories to monitor security advisories and vendor information and identify vulnerabilities that affect you.

TARGETED
MONITORING

02 Assess applicability

Check products, versions, configurations and vendor advisories. Document non-applicable alerts and uncertain cases.

LESS NOISE

03 Prioritise risk

Combine CVSS severity with exploitation signals, exposure and asset business importance.

EVIDENCE-BASED
DECISIONS

04 Manage remediation

Assign owners and deadlines; track decisions, fixes and available evidence.

TRACEABLE ACTIONS

EVIDENCE-BASED, REVIEWABLE ASSESSMENTS

An applicable alert is supported by verifiable evidence. An excluded alert retains its rationale. An incomplete case remains unconfirmed and identifies the information required.

MANAGEMENT BASED ON YOUR INVENTORIES

An inventory or SBOM is enough to start. We organise exchanges and updates through CSV, Excel, JSON or APIs according to available data. Existing tools can supplement the service.

02 / METHOD & INTEROPERABILITY

Explained priorities for informed decisions.

A consolidated, evidenced view that fits your existing processes.

EXAMPLE: FROM CASE FILES TO ACTIONS

ILLUSTRATIVE
FIGURES

4

TRACKED CASES

3 vulnerabilities and 1 support case

6

INSTANCES

4 vulnerability-related, 2 support-related

2

CONFIRMED INSTANCES

1 case, 2 systems

3

OPEN ACTIONS

Correction, investigation, migration

CLEAR CRITERIA FOR PRIORITY DECISIONS

CVSS	Measures technical severity, not attack probability.
EPSS	Estimates exploitation probability in the next 30 days.
CISA KEY	Identifies vulnerabilities exploited in the wild.
CONTEXT	Exposure, version, configuration, criticality and compensating controls.

FROM YOUR DATA TO DELIVERABLES

Your inventories → CyberLifeCycle monitoring and assessment → Alerts, priorities, metrics and reports

- Exchanges through APIs, CSV, Excel, JSON or SBOMs, subject to available formats and access.
- Interoperability and exchange rules verified during scoping, tool by tool.
- Documented states: applicable / not applicable / to confirm, with traceable sources.

MONITORING & CONTINUOUS IMPROVEMENT

A method that evolves with cybersecurity

We review new sources, CVSS changes and formats such as OSV to improve monitoring and assessment within your scope.

Your process evolves without routinely rebuilding existing case files and exchanges.

Adaptations are selected according to your needs and available data.

For your organisation: technical teams focus on fixes while decision-makers have an updated view of risks, responsibilities and progress.

03 / MONITORING & SOFTWARE LIFECYCLE

Monitoring that follows your versions.

Software remains monitored while it is within the agreed scope.

A SERVICE RUN BY CYBERLIFECYCLE

INVENTORIES

Products / versions



MONITORING

Advisories / assessment



DELIVERABLES

Alerts / reports

New advisories, vendor information and estate changes feed ongoing tracking.

VULNERABILITIES

Assess and alert

- Monitor security advisories for inventoried software and versions.
- Check applicability, configurations and vendor fixes.
- Document false positives and identify cases still awaiting confirmation.
- Recommend priorities and send relevant alerts to your teams.

END OF SUPPORT

Plan for end of support

- Verify support dates and conditions with vendors.
- Link every deadline to affected versions and systems.
- Prepare migration or extended-support options.
- Track decisions and actions before maintenance deadlines.

KEEP TRACKING OVER TIME

Monitoring covers the products and versions in the agreed scope. Your teams communicate estate changes; we update case files, alerts, metrics and reports.

04 / MANAGEMENT & TRACEABILITY

A consolidated view for decisions.

A risk overview accessible to management and usable during audits.

Find applicable vulnerabilities, support deadlines, open actions and pending decisions in one overview.

SAMPLE VULNERABILITY MANAGEMENT REPORT

FICTIONAL DATA

4

Tracked cases

6

Instances

1

case under investigation

1

support deadline

TREATMENT AND DECISION TRACKING



● 1 fix in progress

● 1 investigation

● 1 migration awaiting a decision

Every action is linked to a risk, owner, deadline and documented status.

USABLE HISTORY FOR AUDITS AND COMPLIANCE

Sources, assessments, decisions and treatment evidence stay with the relevant cases. Retrieve the reasoning and action status for a review, security questionnaire or audit.

ALERT / ASSET

Reference + version

ANALYSIS

Applicability + priority

ACTION

Owner + deadline

EVIDENCE

Status + history

For management: visibility and decisions. For teams: targeted actions. For audits: documented risks and decisions.

05 / EXPERTISE & COLLABORATION

One contact for your vulnerability management.

From monitoring setup to reporting and action tracking.

EXPERTISE FOR YOUR SOFTWARE ESTATE

CyberLifeCycle

Monitoring, assessment and vulnerability tracking

CyberLifeCycle grew out of nearly ten years of cybersecurity experience. The method connects vendor advisories to deployed versions, turning complex cases into clear priorities and tracked actions.

CVE volumes

CVSS / EPSS / KEV

Interoperability

Remediation

CONFIDENTIALITY & INFORMATION PROTECTION

Before sensitive information is shared, transfer channels, access, responsibilities and retention rules are agreed with the client.

01 Minimise

Useful metadata and strictly necessary information.

03 Restrict access

Authorised people, restricted access, defined deletion.

02 Protect transfers

Agreed channels, suitable encryption, separate secrets.

04 Formalise

Confidentiality and GDPR roles, according to context.

OUR APPROACH

SCOPE → MONITOR → ASSESS → MANAGE

CyberLifeCycle handles monitoring, assessment and tracking. Your teams or technical provider implement fixes. The proposal defines scope, deliverables and alert and reporting frequency.

Let's discuss your security priorities.

Tell us about your current process, challenges and expected outcomes.

[Discuss your requirements →](#)

CyberLifeCycle

Your vulnerability management