CyberLifeCycle

PRÉSENTATION COMMERCIALE / 2026

GESTION DES VULNÉRABILITÉS & OBSOLESCENCES

Le suivi de vos vulnérabilités, clé en main.

Vous nous confiez vos inventaires. CyberLifeCycle prend en charge la veille, la qualification des vulnérabilités et la gestion des faux positifs. Vous recevez des alertes ciblées, des priorités, des indicateurs et des rapports pour organiser les corrections et anticiper les fins de support.

01	02	03
SURVEILLER	**QUALIFIER**	**PILOTER**
Veille sur vos inventaires	Applicabilité et priorités	Alertes, rapports et actions

DE VOS INVENTAIRES À UN SUIVI OPÉRATIONNEL

Une solution de gestion des vulnérabilités clé en main à partir de vos produits et versions : mise en place de la veille, suivi des vulnérabilités et des obsolescences, alertes et reporting dans la durée.

POUR QUI ?

Directions générales • DSI et RSSI • ESN, éditeurs et industriels

01 / ENJEU POUR VOTRE ORGANISATION

Une gestion des vulnérabilités maîtrisée.

Identifier ce qui concerne votre parc et organiser les traitements prioritaires.

01 Surveiller votre parc

À partir des inventaires, suivre les avis de sécurité et les informations éditeurs pour identifier les vulnérabilités qui vous concernent.

VEILLE CIBLÉE

02 Qualifier l'applicabilité

Vérifier les produits, versions, configurations et avis éditeurs. Documenter les alertes non applicables ou encore incertaines.

BRUIT RÉDUIT

03 Hiérarchiser le risque

Confronter la gravité CVSS aux signaux d'exploitation, à l'exposition et à l'importance métier des actifs concernés.

ARBITRAGES JUSTIFIÉS

04 Piloter la remédiation

Associer des responsables et échéances aux actions ; suivre les arbitrages, les corrections et les preuves disponibles.

ACTIONS TRAÇABLES

DES QUALIFICATIONS JUSTIFIÉES ET RÉVISABLES

Une alerte applicable s'appuie sur des éléments vérifiables. Une alerte écartée conserve sa justification. Un dossier incomplet reste à confirmer et précise les informations à obtenir.

UN SUIVI À PARTIR DE VOS INVENTAIRES

Un inventaire ou un SBOM permet de démarrer. Nous organisons les échanges et leur actualisation : CSV, Excel, JSON ou API selon les données disponibles. Les outils déjà en place peuvent compléter le suivi.

02 / MÉTHODE & INTEROPÉRABILITÉ

Des priorités expliquées pour décider.

Une lecture consolidée, justifiée et intégrable à vos processus existants.

EXEMPLE : DES DOSSIERS AUX ACTIONS À MENER — CHIFFRES FICTIFS

4	6	2	3
DOSSIERS SUIVIS	**OCCURRENCES**	**OCCURRENCES CONFIRMÉES**	**ACTIONS OUVERTES**
3 vulnérabilités et 1 support	4 liées aux vulnérabilités, 2 au support	1 dossier, 2 systèmes	Correction, investigation, migration

DES CRITÈRES EXPLICITES POUR ARBITRER LES PRIORITÉS

CVSS	Mesure la gravité technique, pas la probabilité d'attaque.
EPSS	Estime la probabilité d'exploitation dans les 30 prochains jours.
CISA KEV	Signale des vulnérabilités exploitées dans la nature.
CONTEXTE	Exposition, version, configuration, criticité et compensations.

DE VOS DONNÉES AUX LIVRABLES

Vos inventaires → Veille et qualification CyberLifeCycle → Alertes, priorités, indicateurs et rapports

- Échanges via API, CSV, Excel, JSON ou SBOM, en fonction des formats et accès disponibles.
- Interopérabilité et règles d'échange validées au cadrage, outil par outil.
- États justifiés : applicable / non applicable / à confirmer, avec traçabilité des sources.

VEILLE & ADAPTATION CONTINUE

Une méthode qui évolue avec la cybersécurité

Nous examinons les nouvelles sources, les évolutions CVSS et les formats comme OSV pour améliorer la veille et la qualification sur votre périmètre.

Votre suivi évolue sans reconstruire systématiquement les dossiers et les échanges existants.

Les adaptations sont choisies selon vos besoins et les données disponibles.

Pour votre organisation : les équipes techniques concentrent leur effort sur les corrections ; les décideurs disposent d'une vue actualisée des risques, des responsabilités et de l'avancement.

03 / VEILLE & CYCLE DE VIE LOGICIEL

Une veille qui suit vos versions.

Les logiciels restent surveillés tant qu'ils font partie du périmètre convenu.

UN DISPOSITIF PRIS EN CHARGE PAR CYBERLIFECYCLE

INVENTAIRES
Produits / versions

→

VEILLE
Avis / qualification

→

LIVRABLES
Alertes / rapports

Nouveaux avis, informations éditeurs et évolutions du parc alimentent le suivi.

VULNÉRABILITÉS

Qualifier et alerter

- Suivre les avis de sécurité liés aux logiciels et versions inventoriés.
- Vérifier l'applicabilité, les configurations et les correctifs éditeurs.
- Justifier les faux positifs et identifier les cas encore à confirmer.
- Proposer les priorités et transmettre les alertes utiles à vos équipes.

OBSOLESCENCES

Anticiper les fins de support

- Vérifier les dates et les conditions de support auprès des éditeurs.
- Relier chaque échéance aux versions et aux systèmes concernés.
- Préparer les options de migration ou de prolongation du support.
- Suivre les arbitrages et les actions avant les échéances de maintenance.

MAINTENIR LE SUIVI DANS LA DURÉE

La veille suit les produits et versions du périmètre convenu. Vos équipes nous transmettent les évolutions du parc ; nous actualisons les dossiers, les alertes, les indicateurs et les rapports.

04 / PILOTAGE & TRAÇABILITÉ

Une vision consolidée pour décider.

Un état des risques accessible à la direction et exploitable lors des audits.

Retrouvez les vulnérabilités applicables, les échéances de support, les actions ouvertes et les décisions en attente dans une même synthèse.

EXEMPLE DE RAPPORT DE SUIVI

DONNÉES FICTIVES

4	6	1	1
dossiers suivis	occurrences	cas à investiguer	échéance de support

SUIVI DES TRAITEMENTS ET ARBITRAGES

- 1 correction en cours
- 1 investigation
- 1 migration à arbitrer

Chaque action est associée à un risque, un responsable, une échéance et un statut documenté.

UN HISTORIQUE EXPLOITABLE POUR LES AUDITS ET LA CONFORMITÉ

Sources, qualifications, arbitrages et preuves de traitement sont conservés avec les dossiers concernés. Vous pouvez retrouver le raisonnement et l'état des actions lors d'une revue, d'un questionnaire de sécurité ou d'un audit.

ALERTE / ACTIF	ANALYSE	ACTION	PREUVE
Référence + version	Applicabilité + priorité	Pilote + échéance	Statut + historique

Pour la direction : visibilité et arbitrages. Pour les équipes : actions ciblées. Pour les audits : un suivi des risques et des décisions documenté.

05 / EXPERTISE & COLLABORATION

Un interlocuteur pour votre suivi des vulnérabilités.

De la mise en place de la veille aux rapports et au suivi des actions.

UNE EXPERTISE AU SERVICE DE VOTRE PARC LOGICIEL

CyberLifeCycle

Veille, qualification et suivi des vulnérabilités

CyberLifeCycle est issu d'un parcours de près de dix ans en cybersécurité. La méthode relie les avis éditeurs aux versions déployées pour transformer les cas complexes en priorités claires et en actions suivies.

Volumes CVE · CVSS / EPSS / KEV · Interopérabilité · Remédiations

CONFIDENTIALITÉ & PROTECTION DES INFORMATIONS ÉCHANGÉES

Avant toute transmission sensible, les canaux, accès, responsabilités et règles de conservation sont convenus avec le client.

01 **Minimiser**
Métadonnées utiles et données strictement nécessaires.

02 **Protéger les transferts**
Canaux convenus, chiffrement adapté, secrets séparés.

03 **Limiter les accès**
Personnes habilitées, accès restreints, purge définie.

04 **Formaliser**
Confidentialité et rôles RGPD, selon le contexte.

NOTRE DÉMARCHE — CADRER → SURVEILLER → QUALIFIER → PILOTER

CyberLifeCycle assure la veille, la qualification et le suivi. Vos équipes ou votre prestataire technique appliquent les corrections. La proposition précise le périmètre, les livrables et la fréquence des alertes et des rapports.

Échangeons sur vos enjeux de sécurité.

Présentez votre suivi actuel, vos difficultés et les résultats attendus.

Échanger sur votre besoin →

CyberLifeCycle
Votre suivi des vulnérabilités