CyberLifeCycle

FORMATION POUR VOS ÉQUIPES

Piloter les vulnérabilités et le cycle de vie logiciel

Apprenez à décider quelles alertes traiter, à organiser les corrections et à anticiper les fins de support. Sur un cas pratique, vous construisez le suivi que vous pourrez adapter à votre organisation.

Ouverture prochaine · Date d'ouverture confirmée avant inscription

14 h de parcours, en deux unités de 7 h	À distance, à votre rythme, avec accompagnement écrit
32 vidéos, des travaux pratiques et un dossier final	990 € HT par participant

Ce document présente les onze modules, les activités, les livrables, les prérequis, les modalités d'accompagnement et les tarifs. Il ne constitue ni une inscription ni une offre contractuelle.

OBJECTIFS ET PUBLIC

Ce que vous saurez faire

- Construire un inventaire qui sert vraiment à qualifier, et faire apparaître ce qui manque.
- Mettre en place une veille CERT-FR fiable et suivre les mises à jour des avis.
- Analyser vos artefacts avec Trivy et Syft, et savoir trancher quand deux outils ne disent pas la même chose.
- Lire un score CVSS avec recul et justifier une priorité selon l'usage et l'exposition réels du système.
- Alimenter Dependency-Track, avec ou sans pipeline, et garder sous surveillance les anciennes versions encore en service.
- Organiser le suivi : qui qualifie, qui décide, qui corrige et qui vérifie.
- Situer DefectDojo dans la chaîne de suivi et repérer une clôture qui n'est pas prouvée.
- Suivre les corrections, les exceptions et les fins de support, puis préparer les arbitrages.

À qui s'adresse la formation

Public	Utilisation du parcours
RSSI et adjoints	Superviser le dispositif, préparer les arbitrages et suivre les risques résiduels.
Administrateurs sécurité ou systèmes et réseaux	Qualifier sur leur périmètre, organiser les actions et apporter les preuves techniques.
Ingénieurs sécurité et analystes vulnérabilités	Analyser rapports et SBOM, prioriser et suivre les constats.
Équipes IT et DevSecOps	Relier dépendances, services, changements et contrôle de correction.
Coordinateurs MCS et consultants ESN	Attribuer les actions et restituer au responsable du SI, en interne ou en prestation.

Prérequis

Bases systèmes et réseaux, utilisation d'un tableur, lecture d'un JSON simple et exécution des commandes fournies. Tous les participants réalisent les manipulations.

FORMAT ET MODALITÉS

14 heures, deux unités de 7 heures

Le parcours répartit 14 heures de travail entre vidéos, exercices et évaluations, à votre rythme avec un accompagnement écrit.

Unité	Vidéos	Pratique guidée	Évaluations	Total
Unité 1 · Observer et qualifier	150 min	210 min	60 min	7 h
Unité 2 · Prioriser et piloter	140 min	250 min	30 min	7 h
Total	4 h 50 de vidéos	7 h 40 de pratique guidée	1 h 30 d'évaluations	14 h

Accompagnement

Vous disposez de 30 jours pour suivre le parcours, recommandé sur deux semaines. Les démonstrations, exercices à déposer et corrigés vous guident à chaque étape.
L'accompagnement est écrit : réponse sous sept jours calendaires au maximum et retour individuel sur le dossier final sous sept jours après dépôt. Une reprise ciblée peut être proposée. Un blocage technique est pris en compte dans la fixation des échéances de dépôt.
Il vous faut un ordinateur, une connexion internet, un tableur, un terminal et l'accès au laboratoire pédagogique. Une vérification technique précède l'ouverture des accès. Le temps d'installation et de téléchargement s'ajoute aux 14 h du parcours.

Le problème traité

Un rapport de scan ou un avis de sécurité ne suffit pas à décider d'une correction. Il faut retrouver le composant, confirmer son applicabilité, comprendre l'exposition, attribuer l'action et vérifier le résultat. La formation fait construire cette chaîne de travail sur un même cas pratique.

- Une version ou une configuration manque : quelle investigation lancer ?
- Plusieurs sources donnent des scores différents : que conserver et comment décider ?
- Un constat disparaît après un réimport : la correction est-elle démontrée ?
- Un logiciel approche de sa fin de support : qui arbitre la trajectoire et à quelle date ?

PROGRAMME DÉTAILLÉ

Les onze modules

Unité 1 · Observer et qualifier · 7 h

M01 Organiser le suivi des vulnérabilités — 1 h

vidéos 30 min · pratique 15 min · évaluation 15 min

Objectif. Répartir les responsabilités et définir les vérifications attendues à chaque étape.

- Faire le point sur votre organisation actuelle, en interne ou en prestation.
- Répartir les rôles : collecte, qualification, correction, vérification et acceptation du risque.
- Définir les étapes, les preuves attendues, le traitement des urgences et les suppléances.

Résultat à remettre. Une fiche de processus, un périmètre de travail et un rythme de revue.

M02 Relier inventaire, projets, versions et déploiements — 45 min

vidéos 15 min · pratique 30 min · évaluation 0 min

Objectif. Créer un inventaire qui permet de vérifier l'applicabilité et d'attribuer les actions.

- Identifier les actifs, leurs propriétaires et ce qu'ils représentent pour le métier.
- Relier chaque projet à ses versions et à leurs lieux de déploiement, anciennes versions comprises.
- Garder trace des informations manquantes et désigner qui doit les compléter.

Résultat à remettre. Un inventaire exploitable et un registre des versions déployées.

M03 Collecter et traiter les avis CERT-FR — 1 h

vidéos 20 min · pratique 40 min · évaluation 0 min

Objectif. Recevoir les publications pertinentes et tracer leurs révisions jusqu'à la décision locale.

- Choisir les bonnes sources officielles et paramétrer la collecte.
- Automatiser la récupération des avis et contrôler qu'elle fonctionne dans la durée.
- Repérer ce qui change d'une révision à l'autre et en tirer les actions.

Résultat à remettre. Une veille CERT-FR opérationnelle et une file de revue attribuée.

M04 Scanner et analyser avec Trivy — 1 h 45

vidéos 40 min · pratique 65 min · évaluation 0 min

Objectif. Produire des rapports fiables et faire la différence entre une détection, une preuve et une conclusion.

- Cadrer l'analyse : périmètre autorisé, versions analysées et fraîcheur de la base de vulnérabilités.
- Comparer un scan avant et après correction dans des conditions identiques.
- Expliquer pourquoi un résultat disparaît, ou pourquoi il persiste.

Résultat à remettre. Des rapports Trivy comparables et une lecture argumentée des écarts.

M05 Produire et importer des SBOM avec et sans pipeline — 1 h 30

vidéos 30 min · pratique 60 min · évaluation 0 min

Objectif. Produire des SBOM fiables et les faire arriver au bon endroit, avec ou sans pipeline.

- Générer des SBOM avec Syft et Trivy, puis comprendre leurs différences.
- Publier depuis un pipeline et vérifier que l'import a bien abouti sur la bonne version.
- Organiser la collecte sans CI : SBOM fournisseurs, provenance et renouvellement.

Résultat à remettre. Une chaîne d'alimentation vérifiée, avec et sans pipeline.

M06 Qualifier et valider la première unité — 1 h

vidéos 15 min · pratique 0 min · évaluation 45 min

Objectif. Qualifier seul le cas pratique et argumenter ses choix.

- Qualifier en autonomie les signalements du cas pratique.
- Argumenter les cas difficiles et vérifier la cohérence de l'ensemble.
- Comparer avec le corrigé et ajuster son analyse.

Résultat à remettre. Une qualification complète, notée et commentée.

Unité 2 · Prioriser et piloter · 7 h

M07 Prioriser et exploiter les scores — 1 h 15

vidéos 25 min · pratique 50 min · évaluation 0 min

Objectif. Justifier une priorité au-delà du score brut.

- Rassembler les scores CVSS disponibles et traiter les cas où il en manque.
- Adapter un score à votre environnement et justifier l'ajustement.
- Prioriser le backlog et lancer les investigations nécessaires.

Résultat à remettre. Un backlog priorisé et des choix de priorité traçables.

M08 Surveiller le portefeuille dans Dependency-Track — 2 h

vidéos 35 min · pratique 85 min · évaluation 0 min

Objectif. Suivre un portefeuille de versions dans Dependency-Track et situer DefectDojo dans le dispositif.

- Vérifier l'état des sources et importer les SBOM.
- Rattacher les versions à leurs déploiements, anciennes versions comprises.
- Traiter un signalement sur une ancienne version et repérer une clôture non prouvée dans DefectDojo.

Résultat à remettre. Un portefeuille suivi, des imports contrôlés et des décisions documentées.

M09 Piloter les corrections et les exceptions — 1 h 15

vidéos 25 min · pratique 50 min · évaluation 0 min

Objectif. Rédiger des actions vérifiables et traiter un report sans masquer le risque.

- Rédiger des tickets de correction avec des critères de clôture clairs.
- Encadrer une exception temporaire : qui la demande, qui la valide et jusqu'à quand.
- Vérifier les preuves après correction avant de clore.

Résultat à remettre. Des tickets exploitables, une exception encadrée et des clôtures prouvées.

M10 Anticiper les obsolescences logicielles — 1 h

vidéos 20 min · pratique 40 min · évaluation 0 min

Objectif. Vérifier la couverture et déclencher une trajectoire de migration avant la fin de support.

- Lire une fiche de support éditeur et identifier la bonne édition et la bonne branche.
- Documenter l'échéance, sa source, son propriétaire et ce qui reste à confirmer.
- Préparer l'arbitrage et les jalons de la migration.

Résultat à remettre. Une trajectoire de migration documentée avant l'échéance.

M11 Restituer et évaluer le dossier complet — 1 h 30

vidéos 35 min · pratique 25 min · évaluation 30 min

Objectif. Présenter des décisions claires aux responsables du SI et démontrer la maîtrise du parcours.

- Vérifier la cohérence des chiffres et construire une synthèse.
- Présenter les constats et les décisions attendues aux responsables, sans masquer les limites.
- Évaluation finale sur des situations nouvelles.

Résultat à remettre. Un dossier final et une restitution prête à présenter.

TRAVAUX ET LABORATOIRE

Un dossier adaptable à votre périmètre

- Inventaire et registre des sources
- Fiche de processus : rôles, preuves, suivi régulier, remplacements et escalades
- Registres projets, versions, déploiements et imports de SBOM
- Dossiers d'applicabilité avec preuves et inconnues
- Lecture comparée de rapports Trivy et de SBOM
- Priorités argumentées, bilan du portefeuille Dependency-Track et analyse du cas DefectDojo
- Exemple de pipeline et procédure d'alimentation sans CI/CD
- Tickets de correction et exception temporaire
- Suivi des fins de support avec propriétaires et jalons
- Synthèse de décision et plan de mise en pratique

Deux modes d'alimentation du portefeuille

Avec pipeline CI/CD

Générez une SBOM depuis l'artefact livré, conservez sa provenance et publiez-la sur le bon projet et la bonne version. Vérifiez la fin du traitement et reliez les résultats au suivi des actions.

Sans liaison aux pipelines

Centralisez les SBOM reçues des équipes et fournisseurs, rattachez-les aux versions réellement déployées et organisez leur réanalyse et leur renouvellement. Une ancienne version encore utilisée reste suivie.

Sans pipeline, le serveur continue d'actualiser ses sources de vulnérabilités pendant que les SBOM arrivent manuellement. Un environnement totalement isolé demande un circuit de transfert spécifique.

Cas et laboratoire

Le cas pratique Atelier Nova est fictif : vous n'avez aucune donnée de votre employeur ou de vos clients à fournir. Les exercices se font dans un laboratoire dédié, vérifié avant l'ouverture des accès.

TARIFS ET INSCRIPTION

Deux formules, le même parcours

Individuel

990 € HT

par participant

14 h de parcours, accès 30 jours, vidéos, exercices et modèles du parcours, laboratoire pédagogique dédié, évaluations, accompagnement écrit et retour sur le dossier final.

Équipe de cinq participants

3 990 € HT

pour 5 accès nominatifs, soit 798 € HT par participant

Même parcours asynchrone, même durée d'accès et mêmes modalités individuelles. Les accès d'équipe sont activés selon la période convenue au devis.

TVA selon régime applicable, précisée au devis. Date d'ouverture et conditions d'inscription confirmées par écrit. Les prestations propres à votre SI et les sessions privées font l'objet d'un devis distinct. Pour un autre effectif, contactez-nous.

Questions fréquentes

Est-ce adapté à une équipe interne ?
Oui. Les méthodes s'appliquent aux équipes internes comme aux prestataires qui assurent le suivi d'un client.

Faut-il être développeur ?
Non. Il faut toutefois lire un JSON simple et exécuter les commandes fournies. Les prérequis systèmes et réseaux restent nécessaires.

S'agit-il de deux journées en direct ?
Non. Le parcours est asynchrone et accompagné, organisé en deux unités de sept heures à répartir pendant les trente jours d'accès.

Les outils sont-ils utilisés en pratique ?
Oui. Vous travaillez avec Trivy, Syft et Dependency-Track dans un laboratoire dédié, avec et sans pipeline. DefectDojo est présenté en démonstration commentée. Les accès sont vérifiés avant l'ouverture.

La formation délivre-t-elle une certification ?
Une attestation de réalisation peut être remise avec les résultats des évaluations. Le parcours n'est pas certifiant.

Peut-on s'inscrire immédiatement ?
Les inscriptions ne sont pas encore ouvertes. Vous pouvez consulter le programme, demander un devis ou être informé de l'ouverture.

Puis-je partager un accès avec mon équipe ?
Les accès sont individuels. L'offre équipe prévoit cinq accès nominatifs.

Contact et devis

Pour un devis ou une information sur l'ouverture, utilisez le formulaire de cyberlifecycle.fr/formation ou écrivez au contact ci-dessous. Précisez le nombre de participants et votre besoin.

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

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