Blue AcademIA
Blue AcademIA est une marque de BlueMarketing
contact@blueacademia.fr
www.blueacademia.fr

Programme de formation : Gestion des vulnérabilités à l'ère du code généré par IA

Vos développeurs produisent désormais du code plus vite qu'ils ne peuvent le relire. Le rôle du développeur évolue : il doit évaluer, sécuriser et corriger du code qu'il n'a pas toujours écrit. Face à ce changement d'échelle, les processus classiques de gestion des vulnérabilités atteignent leurs limites.

Cette formation apporte une réponse sur deux volets complémentaires :
- structurer un processus complet de gestion des vulnérabilités (inventaire, détection, priorisation, remédiation et vérification des correctifs)
- traiter les risques propres au code généré par l'IA, notamment les dépendances fictives.
Une étude publiée à l'USENIX Security en 2025, portant sur 576 000 échantillons de code, révèle qu'au moins 5,2 % des paquets recommandés par les modèles commerciaux et 21,7 % de ceux proposés par les modèles ouverts n'existent pas. Parmi eux, 43 % réapparaissent lorsque la même requête est soumise à nouveau, créant une faille exploitable par des attaquants.

Les participants s'exercent sur une application volontairement vulnérable, générée par un assistant de code et fournie avec son environnement d'exécution. Ils apprennent ainsi à identifier et corriger des failles dans un cadre maîtrisé, puis repartent avec l'environnement complet pour reproduire l'exercice auprès de leurs équipes.

Durée : 14.00 heures ou 2.00 jour(s) si formation en présentiel.

Lieu : À distance ou en présentiel

Profils des stagiaires

- Développeurs et responsables applicatifs utilisant un assistant de génération de code.
- Ingénieurs DevOps et DevSecOps en charge des chaînes de construction et de déploiement.
- Responsables sécurité des systèmes d'information et directeurs des systèmes d'information de PME et d'ETI.
- Responsables techniques chargés de la qualité et de la sécurité du code livré.
- Prestataires et éditeurs devant justifier de la sécurité de leur chaîne logicielle auprès de leurs clients.

Prérequis

- Pratique courante d'au moins un langage de programmation, Python ou JavaScript de préférence.
- Connaissance du fonctionnement d'un gestionnaire de dépendances (pip, npm ou équivalent) et usage courant d'un dépôt de code versionné.
- Utiliser, ou envisager d'utiliser, un assistant de génération de code dans l'activité de l'équipe.
- Un poste disposant d'un accès internet, d'un éditeur de code et des droits nécessaires pour installer un environnement de travail local.
- Aucune connaissance préalable en sécurité applicative n'est exigée : la partie 1 pose le socle.
- Aucun code de l'entreprise n'est requis ni demandé : l'application support est fournie par le formateur.

- Les pré-requis sont validés lors d'un échange avec le commanditaire du projet de formation et retranscrits dans le document de recueil des besoins. Il s'agit d'un document collaboratif partagé systématiquement avec le commanditaire à l'issue du premier entretien pour co-construire l'action de formation. Par ailleurs, nous adressons à chaque apprenant, 2 semaines avant le début de la formation, un questionnaire de préparation de la formation pour adapter au mieux la formation à ses besoins.

Objectifs pédagogiques

- Construire l'inventaire des composants logiciels de son périmètre et en définir le périmètre de surveillance.
- Prioriser les vulnérabilités détectées selon la criticité, l'exposition et l'exploitabilité réelle.
- Vérifier l'existence et la légitimité des dépendances proposées par un assistant de code avant leur installation.
- Reconnaître les attaques par confusion de paquets, y compris leur variante induite par les modèles de langage.
- Produire un inventaire des composants logiciels (SBOM) et verrouiller les versions d'un projet.
- Repérer les défauts de sécurité récurrents du code généré : secrets en dur, validation d'entrée absente, contrôle d'accès insuffisant.
- Élaborer un plan de remédiation priorisé et en mesurer l'efficacité.
- Définir les indicateurs de pilotage du processus et le rythme de revue.

Contenu de la formation

- Le socle : un processus de gestion des vulnérabilités qui tient
  - Inventaire des actifs et définition du périmètre de surveillance
  - Sources de détection : scan, avis de sécurité, référentiels de vulnérabilités publiques
  - Priorisation : criticité, exposition, exploitabilité réelle
  - Plan de remédiation et vérification de l'efficacité des correctifs
  - Cas pratique appliqué : construction de la matrice de priorisation appliquée au périmètre de l'apprenant, à partir d'un inventaire type.
- Ce que le code généré par IA change
  - Volume, vitesse, déplacement du rôle du développeur vers la relecture
  - L'hallucination de paquets : nature du phénomène et mesure (étude USENIX Security 2025)
  - Confusion de paquets : typosquatting, dependency confusion, et leur variante induite par les modèles
  - Cas pratique appliqué : identifier les dépendances inexistantes ou douteuses dans un ensemble d'extraits de code générés.
- Contrôler ce que l'assistant produit
  - Vérification systématique des dépendances avant installation
  - Verrouillage des versions et reproductibilité des constructions
  - Inventaire des composants logiciels (SBOM) : production et exploitation
  - Revue de code assistée : ce qui peut être délégué, ce qui ne doit pas l'être
  - Cas pratique appliqué : mise en place d'un contrôle de dépendances sur l'application fournie, et repérage des paquets inexistants qu'elle contient.
- Les défauts applicatifs récurrents du code généré
  - Rappels des catégories de risques applicatifs de référence (OWASP)
  - Motifs récurrents observés dans le code produit par assistant
  - Secrets en dur, jeux de données de test, configurations laissées en clair
  - Cas pratique appliqué : audit complet de l'application fournie et relevé des défauts, comparé ensuite à la liste des vulnérabilités réellement présentes.

- Remédier et vérifier
  - Construction du plan de remédiation priorisé
  - Correction assistée : bénéfices et pièges de la remédiation générée par IA
  - Vérification que le correctif corrige effectivement
  - Cas pratique appliqué : production du plan de remédiation de l'application auditée en partie 4, puis vérification que les correctifs referment bien les failles.
- Industrialiser et piloter
  - Intégration des contrôles dans la chaîne de construction
  - Indicateurs et tableau de bord de suivi
  - Gouvernance : qui décide, qui corrige, qui vérifie, à quel rythme
  - Cas pratique appliqué : définition de cinq indicateurs et du rythme de revue de l'équipe.

Organisation de la formation

Equipe pédagogique
Sébastien Wald possède 20 ans d'expérience en cybersécurité opérationnelle. Diplômé d'un Master 2 en sécurité informatique (OPSIE, Université Lyon 2) et d'une licence en sciences de l'éducation, il associe expertise technique et maîtrise pédagogique.

À la RATP, il a conçu et déployé un processus complet de gestion des vulnérabilités : inventaire des actifs exposés, définition des politiques, campagnes de scan, plans de remédiation, tableaux de bord et contrôle de l'efficacité des correctifs avec les équipes applicatives. Il a également formé les intervenants aux bonnes pratiques de développement sécurisé.

Son parcours l'a conduit à exercer comme adjoint au responsable de la sécurité chez Sogetrel, consultant SIEM chez Orange et ingénieur produit pour un éditeur de solutions de corrélation d'événements de sécurité. Il y développait notamment des scénarios d'attaque et des règles de détection.

Aujourd'hui, il se consacre à la sécurité des systèmes d'intelligence artificielle et à l'audit du code généré par les assistants de développement. Sa veille continue sur les nouvelles techniques d'attaque et l'évolution du cadre réglementaire européen nourrit des contenus de formation actualisés au moins une fois par an.

Moyens pédagogiques et techniques
- Supports pédagogiques commentés et partagés
- Apports méthodologiques structurés
- Templates prêts à l'emploi
- Cas pratiques appliqués à l'entreprise
- Etudes de cas concrets
- Quiz
- Mise à disposition en ligne de documents supports à la suite de la formation
- Outils d'analyse de composition logicielle et de génération d'inventaire des composants (SBOM), en version libre.
- Fonctions d'audit intégrées aux gestionnaires de dépendances (npm, pip).
- Scanners de vulnérabilités, présentés en démonstration : principes communs et critères de choix.
- Une application volontairement vulnérable, produite par un assistant de code et fournie par le formateur avec son environnement d'exécution.
- Un assistant de génération de code, utilisé en démonstration pour observer en direct la production de dépendances inexistantes.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation
- Feuilles de présence

- Questions orales ou écrites (QCM)
- Mises en situation
- Formulaires d'évaluation de la formation
- Certificat de réalisation de l'action de formation
- 10 jours avant l'entrée en formation : nous transmettons à chaque apprenant un questionnaire de préparation de la formation permettant d'adapter au mieux la formation à ses besoins.
- Pendant la formation : le contrôle de connaissances et des acquis se font de façon continue via des cas pratiques à réaliser et des quiz en ligne avec notation instantanée. En fin de formation, les apprenants restituent leurs travaux avec feedback du formateur.
- A l'issue de la formation : nous adressons aux apprenants un questionnaire de satisfaction à chaud et d'auto-diagnostic. Nous mesurons ainsi leur satisfaction et constatons directement l'évolution des compétences en comparaison avec les données recueillies avant la formation. Nous adressons un questionnaire d'évaluation au formateur.
- 15 jours après la fin de la formation : Nous adressons un questionnaire d'évaluation au financeur (OPCO).
- Un mois après la formation : Nous adressons un questionnaire d'évaluation aux différentes parties prenantes : commanditaire /manager.
- 3 mois après la formation : Nous transmettons aux apprenants un questionnaire d'évaluation à froid pour évaluer l'impact de la formation dans son activité professionnelle.

Tarif de la formation

À partir de 3080.00 €HT
TVA non applicable, art. 261-4-4 du CGI