

Formation Analyse de vulnérabilités avec SonarQube et OWASP

Présentation

Cette formation intermédiaire sur trois jours permet aux participants d'analyser, détecter et comprendre les vulnérabilités applicatives en utilisant SonarQube et les standards OWASP. Elle offre une approche méthodique des analyses statiques et des risques de sécurité, tout en guidant les apprenants dans la mise en œuvre d'audits techniques et de bonnes pratiques de remédiation.

Durée : 21,00 heures (3 jours)

Tarif INTRA : [Nous consulter](#)

Objectifs de la formation

- Analyser les vulnérabilités identifiées par SonarQube
- Mettre en œuvre des audits de code basés sur les standards OWASP
- Configurer et exploiter un projet SonarQube pour l'analyse statique
- Évaluer les risques associés aux failles applicatives
- Mettre en œuvre des actions de remédiation adaptées

Prérequis

- Compréhension des concepts fondamentaux du développement applicatif
- Connaissance de base en gestion de versions (Git)

Public

- Développeurs souhaitant renforcer leurs compétences en sécurité applicative
- Ingénieurs qualité, DevOps ou leads techniques impliqués dans le delivery logiciel
- Professionnels IT responsables de l'analyse ou de la conformité sécurité

Programme de la formation



Jour 1 – Analyse statique avec SonarQube

Session du matin :

- Rappels sur la sécurité applicative et l'analyse statique
- Structure, modules et règles de SonarQube
- Création et configuration d'un projet SonarQube

Session de l'après-midi :

- Exécution d'analyses avec SonarScanner
- Compréhension des métriques : bugs, vulnérabilités, code smells
- Interprétation des rapports et premières remédiations

TP / Exercice :

- Configurer un projet SonarQube, exécuter une analyse complète et interpréter les résultats

Points clés & takeaways :

- Première maîtrise des analyses SonarQube
- Compréhension des principaux indicateurs
- Capacité à lire et prioriser les vulnérabilités

Jour 2 – Standards OWASP et audit de sécurité

Session du matin :

- Présentation de l'OWASP Top 10
- Risques, impacts et scénarios d'exploitation
- Cartographie des vulnérabilités entre OWASP et SonarQube

Session de l'après-midi :

- Analyse de cas réels de failles applicatives
- Priorisation des risques et construction d'un rapport d'audit
- Stratégies de remédiation sécurisées

TP / Exercice :

- Analyser des vulnérabilités OWASP sur un projet fourni : identification, classification et priorisation

Points clés & takeaways :

- Lecture experte des risques OWASP
- Méthodologie d'audit structurée
- Analyse et priorisation des failles de sécurité

Jour 3 – Intégration et remédiation**Session du matin :**

- Intégration de SonarQube dans un pipeline CI/CD
- Bonnes pratiques de remédiation des vulnérabilités
- Mise en place d'un workflow de revue de code sécurisé

Session de l'après-midi :

- Audit complet combinant SonarQube et OWASP
- Démonstration d'un pipeline automatisé
- Synthèse et validation des acquis

TP / Exercice :

- Réaliser un audit complet : analyse SonarQube, classification OWASP et plan de remédiation

Points clés & takeaways :

- Capacité à auditer un projet applicatif complet
- Mise en œuvre d'un pipeline sécurisé
- Méthodologie reproductible pour les analyses futures

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation

- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.