Mis à jour le 10/10/2024

S'inscrire

Formation Checkmarx : Assurer la sécurité des applications

1.5 jour (10h30)

PRÉSENTATION

Notre formation Checkmarx vous permettra de connaître les étapes à suivre pour sécuriser vos applications en effectuant différents types de tests. Vous pourrez suivre en temps réel les vulnérabilités qui menacent vos logiciels.

Grâce à notre cours, votre équipe sera capable de protéger chaque phase de développement pour chacune des applications en équilibrant les besoins dynamiques des [RSSI](#) et de développement.

Découvrez tous les outils de scan automatisés de sécurité des applications tels que SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing) ou SCA (Software Composition Analysis).

Cette formation va permettre à votre organisation d'apporter un niveau de sécurité performant pour les applications qui seront déployées à l'avenir.

Comme dans toutes nos formations, celle-ci vous présentera la dernière version stable de Checkmarx (à la date de rédaction de l'article [Checkmarx 1.1](#)).

OBJECTIFS

- Personnaliser et optimiser efficacement les outils de la plateforme
- Automatiser et intégrer dans une usine de développement sans ralentissement
- Savoir affiner les politiques de scan pour réduire le nombre des résultats
- Connaître les modèles de gouvernance autour des outils de la plateforme Checkmarx One

PUBLIC VISÉ

- Développeurs
- Hackers éthiques
- DevOps
- Administrateurs système
- Chefs de projets

Pré-requis

Connaissance de base en sécurité des applications.

PROGRAMME DE NOTRE FORMATION CHECKMARX

Introduction générale

- Partage des objectifs de formation et présentation générale de la plateforme Checkmarx One
- Introduction générale sur les vulnérabilités et les risques applicatifs
- Comprendre la méthode de scoring et d'évaluation de la criticité/impact d'une vulnérabilité de manière générale et dans la plateforme Checkmarx One

Exploration des différents modules de la plateforme Checkmarx One

- Analyse SCA (Software Composition Analysis)
 - Mode de fonctionnement
 - L'intérêt de la génération/utilisation SBOM
 - Modèle d'intégration possible
 - L'importance de la définition d'une politique de sécurité pour la gestion des bibliothèques open source
 - Exercice/TP : analyse et interprétation d'un rapport Checkmarx One de type SCA, et établissement d'un plan d'action
- Analyse SAST (Static Application Security Testing)
 - Mode de fonctionnement
 - Les modes d'intégration
 - Les limites
 - Astuces pour la qualification rapide des résultats de scan et optimisation des faux positifs
 - Exercice/TP : analyse et interprétation d'un rapport Checkmarx One de type SAST, et établissement d'un plan d'action
- Test DAST (Dynamic Application Security Testing)
 - Mode de fonctionnement des outils DAST
 - Les différences entre les outils DAST et les tests d'intrusion manuels
 - Modes d'intégration possibles
 - Limites et mesures à prévoir pour une intégration à grande échelle
 - Exercice/TP : analyse et interprétation d'un rapport Checkmarx One de type DAST, et établissement d'un plan d'action

- Sécurité des APIs
 - Mode de fonctionnement et comment compléter les résultats de l'analyse SAST
 - Les limites, et les bonnes pratiques de mise en œuvre à grande échelle
 - Exercice/TP : analyse et interprétation d'un rapport Checkmarx One d'analyse d'une API, et établissement d'un plan d'action
-

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.