

Mis à jour le 26/10/2026

S'inscrire

Formation Trivy

2 jours (14 heures)

Présentation

Trivy est un outil de sécurité applicative permettant de détecter les vulnérabilités, les secrets exposés et les mauvaises configurations. Avec ses scanners, son mode client-serveur et son intégration à GitHub Actions, il accompagne les équipes dans la sécurisation des images et des dépendances applicatives.

Notre formation Trivy vous permettra de maîtriser la terminologie de la sécurité applicative et de déployer des contrôles adaptés à vos pratiques DevSecOps au quotidien.

Vous apprendrez à interpréter les CVE et les niveaux de sévérité, à configurer les scanners et à analyser des images de Docker Hub avec un serveur Trivy hébergé sur AWS dans un environnement sécurisé.

À l'issue de la formation, vous serez en mesure de construire des workflows GitHub Actions pour scanner des applications dans des dépôts publics et privés, gérer les permissions et appliquer des seuils de blocage cohérents avec vos exigences de sécurité.

Cette formation aborde également les rapports de scan, la priorisation des corrections, les exceptions documentées et la validation des remédiations. Les ateliers vous permettront de relier détection, automatisation et réduction des risques dans une chaîne de livraison applicative.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Maîtriser la terminologie de la sécurité applicative et les principaux scanners de Trivy

- Configurer les analyses de vulnérabilités, de secrets et de mauvaises configurations avec Trivy dans un projet applicatif
- Déployer un serveur Trivy sur AWS et analyser des images issues de Docker Hub
- Automatiser les scans des applications de dépôts publics et privés avec GitHub Actions dans les workflows
- Exploiter les rapports pour prioriser les corrections et vérifier les remédiations

Public visé

- Ingénieur DevSecOps
- Ingénieur DevOps
- Développeur applicatif
- Ingénieur sécurité applicative
- Administrateur cloud

Pré-requis

- Pratique de la ligne de commande sous Linux pour les opérations courantes
- Connaissance de Docker et des principes de construction des images
- Utilisation de Git et de GitHub pour gérer un dépôt
- Compréhension des pipelines CI/CD et lecture de fichiers YAML de configuration
- Notions de AWS et des règles réseau associées aux machines virtuelles

Pré-requis techniques

- Poste avec 8 Go de RAM minimum, 20 Go libres et environnement Ubuntu 24.04 LTS natif ou en machine virtuelle
- Installation de Docker Engine, de Git et de Trivy dans les versions validées avant la session, avec droits d'installation
- Compte GitHub autorisant la création de dépôts publics et privés et l'exécution de GitHub Actions pour les ateliers
- Accès à un environnement AWS de laboratoire avec droits encadrés sur Amazon EC2 et les groupes de sécurité, ainsi qu'un compte Docker Hub pour les analyses authentifiées
- Connexion Internet stable autorisant les accès à GitHub, Docker Hub, aux bases de vulnérabilités de Trivy et à l'environnement AWS de formation

Programme de notre formation Trivy

[Jour 1 - Matin]

Comprendre la sécurité applicative et prendre en main Trivy

- Terminologie de la sécurité applicative : vulnérabilité, menace, risque, dépendance et chaîne d'approvisionnement logicielle

- Lecture des CVE, du score CVSS et des niveaux de sévérité, distinction entre gravité et risque contextualisé
- Périmètre de Trivy : analyse des dépendances, détection de secrets et contrôle des configurations, distinction avec les tests dynamiques et l'analyse du code source
- Installation et vérification de Trivy, bases de vulnérabilités, cache et sélection explicite des scanners
- Premières commandes image, fs et config, lecture des paquets détectés et des versions corrigées
- Atelier pratique : Scanner une image et un projet de démonstration, repérer une vulnérabilité, un secret factice et une mauvaise configuration, puis expliquer les résultats.

[Jour 1 - Après-midi]

Scanner Docker Hub avec un serveur Trivy sur AWS

- Architecture client-serveur : analyse de l'image côté client, recherche des vulnérabilités côté serveur et maintien des contrôles de secrets et de configurations côté client
- Déploiement du serveur Trivy sur une instance Amazon EC2 de laboratoire, stockage du cache et actualisation des bases
- Protection des communications par tunnel SSH, authentification par jeton et restriction des accès avec les groupes de sécurité AWS
- Accès aux images de Docker Hub depuis le client installé sur EC2, authentification au registre, tags, digests et limites de téléchargement
- Exécution des scans avec --server, filtrage par sévérité et export des résultats au format JSON
- Atelier pratique : Déployer un serveur Trivy sur AWS, connecter un client sur la même instance et analyser deux images de Docker Hub pour comparer leurs vulnérabilités.

[Jour 2 - Matin]

Automatiser les analyses avec GitHub Actions

- Structure d'un workflow GitHub Actions : événements push et pull_request, jobs, runners et étapes de scan
- Récupération du dépôt avec actions/checkout et configuration de trivy-action pour analyser les dépendances, secrets et configurations du projet
- Analyse des dépôts publics et privés, permissions minimales du GITHUB_TOKEN et authentification dédiée pour les accès à un autre dépôt privé
- Sécurisation des workflows : secrets GitHub, restrictions des contributions externes et actions épinglées sur des SHA vérifiés
- Construction puis scan d'une image applicative, gestion du cache et configuration partagée dans trivy.yaml
- Atelier pratique : Créer et exécuter un workflow de scan sur un dépôt public puis sur un dépôt privé, analyser le projet et son image, puis vérifier les permissions et les rapports produits.

[Jour 2 - Après-midi]

Exploiter les résultats et fiabiliser les contrôles

- Définition des seuils de blocage avec severity et exit-code, distinction entre vulnérabilités détectées et erreurs d'exécution
- Publication des rapports JSON en artefacts et des résultats SARIF dans GitHub Code Scanning lorsque les droits et l'offre du dépôt le permettent
- Qualification des alertes : contexte d'exposition, disponibilité d'un correctif, faux positifs et limites de la détection
- Gestion des exceptions documentées, exclusions ciblées, responsables de validation et échéances de réexamen
- Remédiation par mise à jour des dépendances et des images de base, retrait des secrets, correction des configurations et nouveau scan
- Atelier pratique : Faire échouer un workflow sur une vulnérabilité prioritaire, conserver le rapport malgré l'échec, appliquer une correction et valider le nouveau scan avant de nettoyer les ressources AWS.

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.