

CYBERSÉCURITÉ

OPEN SOURCE

# Trivy : Le Scanner de Sécurité Tout-en-Un pour la Cybersécurité

Découvrez l'outil qui révolutionne l'analyse de vulnérabilités dans les environnements cloud natifs, adopté par des milliers d'organisations à travers le monde.

**Cours de David DONISA , Enseignant en BTS SIO**



# Qu'est-ce que Trivy ?

Trivy est un outil **open-source** développé par **Aqua Security**, conçu pour détecter les vulnérabilités (CVE (Common Vulnerabilities and Exposures : base de données publique des failles de sécurité connues)), les erreurs de configuration IaC (Infrastructure as Code : gestion de l'infrastructure via du code), les secrets exposés et les problèmes de licences dans vos environnements.



## Multi-cibles

Images conteneurs, systèmes de fichiers, dépôts Git, clusters Kubernetes et clouds



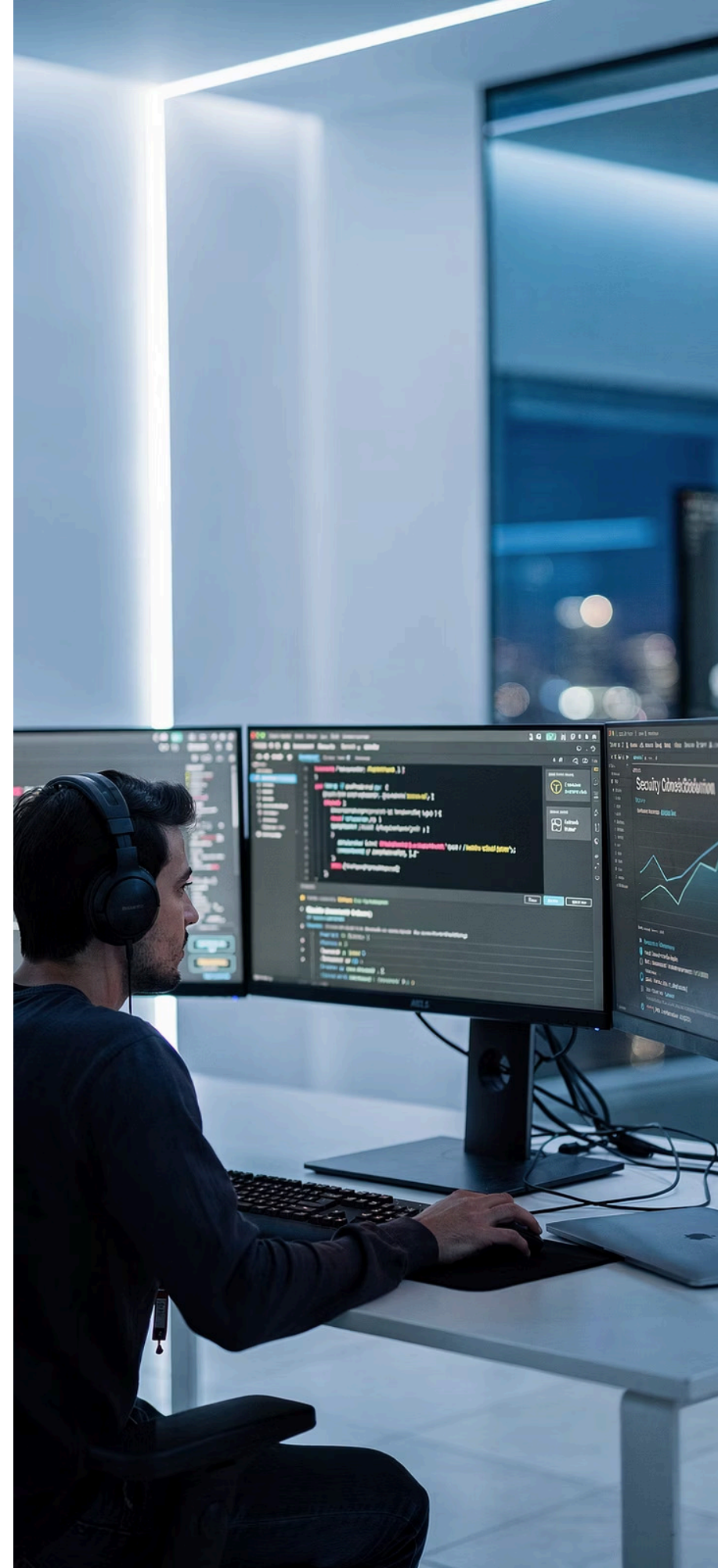
## CI/CD (Continuous Integration/Continuous Deployment : automatisation des tests et déploiements) natif

Fonctionne localement, en pipeline DevOps (Development and Operations : collaboration entre développement et opérations) et comme opérateur Kubernetes



## Installation simple

Un seul binaire statique, prêt à l'emploi en quelques secondes



# Fonctionnalités Clés de Trivy

## Analyse multi-cibles

Conteneurs, IaC (Infrastructure as Code : gestion de l'infrastructure via du code) (Terraform, Dockerfiles), VM (Virtual Machine : machine virtuelle) et clusters Kubernetes

## Base de données enrichie

Mise à jour continue — 31 000+ ★  
GitHub et 500+ contributeurs

## SBOM (Software Bill of Materials : inventaire détaillé des composants logiciels) & Conformité

Inventaire logiciel, rapports NSA (National Security Agency : agence de sécurité nationale américaine) et CIS (Center for Internet Security : référentiel de bonnes pratiques de sécurité) benchmarks

## Intégration DevSecOps (Development, Security, and Operations : intégration de la sécurité dans le cycle de développement)

Support natif VS Code, JetBrains et pipelines CI/CD (Continuous Integration/Continuous Deployment : automatisation des tests et déploiements) pour un shift-left efficace



# Popularité et Retours d'Utilisateurs

31K+

Étoiles GitHub

Scanner open-source le plus populaire  
(fév. 2026)

500+

Contributeurs

Communauté active et en croissance  
constante

100+

Intégrations

Dont Azure Container Registry et  
pipelines CI/CD (Continuous  
Integration/Continuous Deployment :  
automatisation des tests et  
déplloiements) majeurs

“

**GitLab** — « Leader du marché en  
fonctionnalités »

“

**Mirantis** — « Se démarque  
nettement de la concurrence »

“

**MasterCard** — « Un outil qui ne  
cesse de s'améliorer »

“

”

Adoption massive par les géants du cloud — innovation et fiabilité garanties par une communauté mondiale.

# Conclusion : Trivy, un Pilier de la Sécurité Cloud Native

## 1 Démocratise la sécurité

Scan complet des vulnérabilités et configurations, accessible à toutes les équipes.

## 2 Outil clé DevSecOps

Garantit des déploiements plus sûrs et conformes pour DevSecOps (Development, Security, and Operations : intégration de la sécurité dans le cycle de développement) et DevOps (Development and Operations : collaboration entre développement et opérations) et équipes sécurité.

## 3 Standard incontournable

En constante évolution, Trivy s'impose pour sécuriser les environnements cloud natifs.

## 4 Adoptez-le aujourd'hui

Renforcez votre posture de sécurité dès maintenant avec un outil éprouvé et gratuit.