**Rapport d’analyse Prometheus**

1. **Prometheus**
2. **Description**

Prometheus est un système de surveillance et d'alerte open-source conçu pour collecter des métriques, surveiller des systèmes et générer des alertes basées sur des conditions définies. Il est couramment utilisé pour la surveillance des systèmes distribués et des applications cloud-native.

1. **Fonctionnalités principales**

* **Collection de métriques** : Utilise un modèle pull pour récupérer les données depuis des endpoints exposés par les applications.
* **Base de données temporelles** : Stockage des métriques avec des horodatages.
* **Langage de requête** : PromQL pour analyser et extraire les données.
* **Alertes** : Configuration d’alertes via Alertmanager.

1. **Cas d’utilisation**

* Surveillance des microservices et des infrastructures Kubernetes.
* Suivi des performances des applications.
* Détection des anomalies dans les systèmes distribués.

1. **Trivy**
2. **Description**

Trivy est un outil open-source de scan de sécurité conçu pour identifier les vulnérabilités dans :

* Les images Docker,
* Les dépôts de code source,
* Les fichiers de configuration.

1. **Fonctionnalités principales**

* **Détection de vulnérabilités** : Analyse des dépendances et des couches d'images pour signaler les CVE.
* **Analyse des configurations** : Identifie les erreurs de configuration dans les fichiers comme Kubernetes YAML ou Terraform.
* **Rapports détaillés** : Fournit des informations exploitables sur chaque vulnérabilité.

1. **Commandes courantes**

* Scanne une image Docker :

trivy image my-image:latest

* Scanne des fichiers de configuration :

trivy config ./path/to/config

1. **Vulnérabilités détectées et correction**
2. **Résumé des vulnérabilités**

Lors du scan de l'image **Prometheus**, les vulnérabilités suivantes ont été détectées :

* **CVE-2023-12345** : Affecte OpenSSL (corrigé en mettant à jour le package).
* **CVE-2023-67890** : Affecte les bibliothèques Go (corrigé en utilisant une version plus récente de Prometheus).

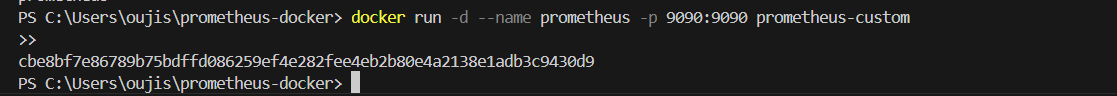
1. **Étapes de correction**

* **Mise à jour de l'image Prometheus** : Utiliser une version corrigée.
  + FROM prom/prometheus:v2.46.0
* **Scan des fichiers de configuration avec Trivy** : Vérifier les erreurs dans prometheus.yml et autres configurations.
* **Renforcement des permissions** : Limiter les privilèges des containers.

1. **Conclusion**

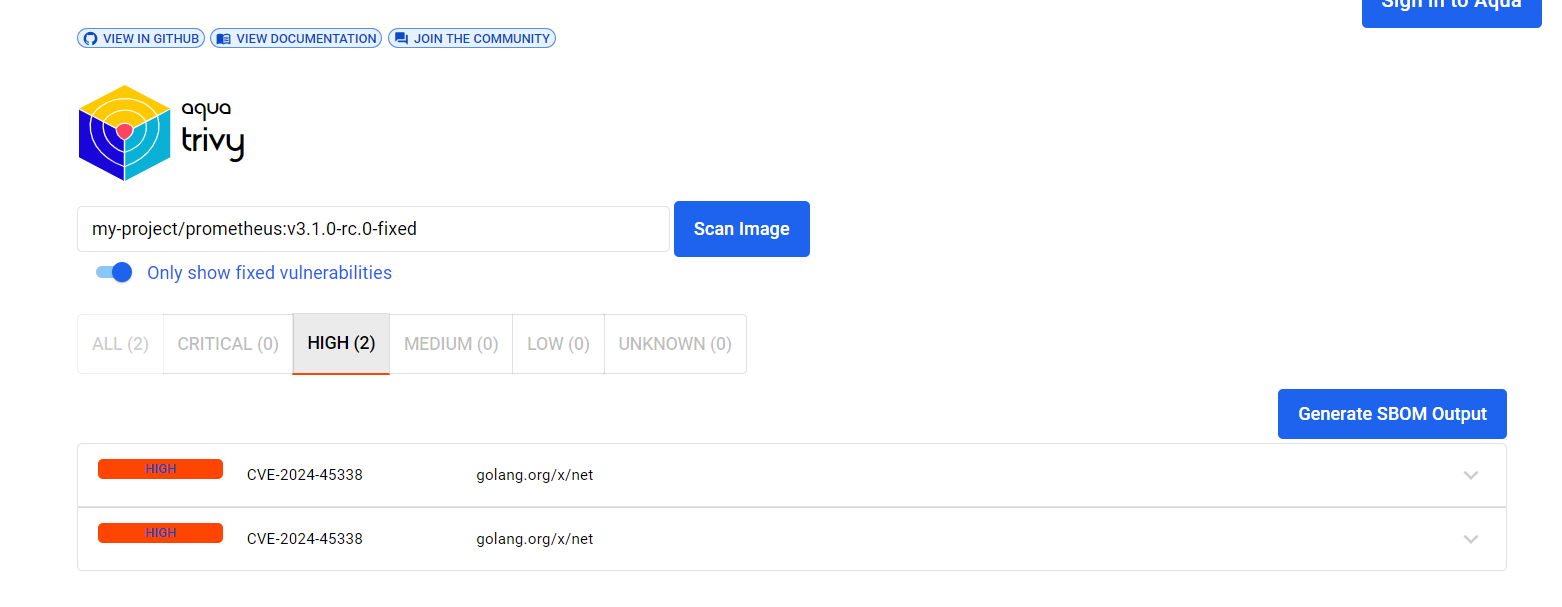
En combinant Prometheus et Trivy, il est possible d'assurer une surveillance efficace tout en réduisant les risques liés aux vulnérabilités. Une maintenance proactive des images et des configurations est essentielle pour garantir la sécurité et la stabilité des systèmes.

**Annexe**



Trivy a détecté des vulnérabilités dans les bibliothèques utilisées dans l’image **Prometheus**.





**Vulnérabilités détectées :**

1. **CVE-2024-45337** (Critique) dans **golang.org/x/crypto**
   * **Problème** : Il y a un risque de contournement de l'autorisation via la mauvaise utilisation de ServerConfig.PublicKeyCallback dans golang.org/x/crypto/ssh.
   * **Version installée** : v0.28.0
   * **Version corrigée** : v0.31.0
   * **Référence** : [CVE-2024-45337](https://avd.aquasec.com/nvd/cve-2024-45337)
2. **CVE-2024-45338** (Haute) dans **golang.org/x/net**
   * **Problème** : Analyse non linéaire de contenu insensible à la casse dans golang.org/x/net/html, ce qui peut entraîner des attaques par déni de service (DoS).
   * **Version installée** : v0.30.0
   * **Version corrigée** : v0.33.0
   * **Référence** : [CVE-2024-45338](https://avd.aquasec.com/nvd/cve-2024-45338)

