Centre d'Opérations des Vulnérabilités

EyeSec est une plateforme intégrée pour la détection et la gestion des vulnérabilités open source.

– Cahier de charges –

Plan

Introduction:..... 3
Objectifs:..... 3
Fonctionnalités:..... 3
Scénario d'utilisation:..... 3
Périmètre du projet.....4
Critères d’acceptabilité:.....4
Délais et Budget:..... 4

Introduction:

EyeSec est une plateforme open source conçue pour détecter, analyser et gérer les vulnérabilités dans les systèmes informatiques. Elle est essentielle pour les organisations qui cherchent à protéger leurs infrastructures contre les menaces de sécurité tout en utilisant des outils accessibles et modulables.

Il offre des fonctionnalités avancées telles que l'enrichissement des vulnérabilités, la gestion automatisée des tickets, et la visualisation des données via des tableaux de bord interactifs. Elle permet également de programmer des scans automatiques hebdomadaires, assurant une surveillance continue et une détection précoce des failles de sécurité. Cette approche centralisée et automatisée permet aux organisations de réduire les risques et d'améliorer leur posture de sécurité de manière significative.

Objectifs:

- **Détection proactive** : Identifier les vulnérabilités avant qu'elles ne soient exploitées.
- **Gestion centralisée** : Offrir une vue unifiée des menaces et des actions correctives.
- **Automatisation** : Réduire le temps de réponse grâce à des scans et analyses automatisés.

Fonctionnalités:

- **Enrichissement des vulnérabilités** : Utilisation de Shodan et VirusTotal pour des données détaillées.
- **Gestion des tickets** : Intégration avec TheHive pour le suivi des incidents.
- **Tableaux de bord** : Visualisation des données via Grafana et Kibana.
- **Scans hebdomadaires** : Opérés par Wazuh pour une surveillance continue.

Scénario d'utilisation:

Une entreprise découvre une vulnérabilité critique dans son système. SecEye permet de :

1. Détecter la vulnérabilité via des scans automatisés.
2. Enrichir les informations avec Cortex et Shodan.

3. Créer un ticket dans TheHive pour suivi.
4. Visualiser l'impact via les tableaux de bord.

Périmètre du projet

- **Éléments clés** : Shodan, VirusTotal, Wazuh, TheHive, Cortex.
- **Acteurs** :
    - **Analystes de sécurité** : Utilisent la plateforme pour détecter et gérer les vulnérabilités.
    - **Administrateurs système** : Configurent et maintiennent les outils.
    - **Responsables de la sécurité** : Supervisent les rapports et prennent des décisions stratégiques.

Critères d’acceptabilité:

- **Fiabilité** : Les outils open source utilisés sont largement reconnus et maintenus par des communautés actives.
- **Robustesse** : La plateforme est conçue pour gérer de grandes quantités de données et fonctionner en temps réel.
- **Sécurité** : Tous les composants respectent les meilleures pratiques de sécurité, avec des mises à jour régulières et des audits de code.

Délais et Budget:

- **Phase de conception :** 2 semaines.
- **Configuration initial :** 4 à 6 semaines.
- **Tests et mise en ligne :** 2 semaines.