Projet informatique

Titre :
SIEM lab : simulation d'attaques et création des règles EDR
(Purple-team detection engineering lab)

Description du projet :
Construire un laboratoire domestique isolé de cybersécurité avec des points d'extrémité Windows et Linux, une journalisation centralisée, un système d'alerte et un rapport d'incidents à l'aide d'outils SIEM a base d'agents.

Spécification :
Le projet vise à concevoir et réaliser un environnement didactique permettant de simuler des attaques contrôlées dans un laboratoire de cybersécurité, puis de développer et valider des règles de détection EDR/SIEM associées. Le laboratoire devra inclure au minimum un poste Windows, un poste Linux et une plateforme de centralisation des journaux. L'outil devra permettre la collecte des événements de sécurité, la génération d'alertes, l'analyse des traces et la rédaction de rapports d'incidents.

Objectifs :
- Mettre en place un laboratoire isolé et reproductible.
- Centraliser les journaux issus des points d'extrémité.
- Simuler des techniques d'attaque simples et réalistes.
- Créer des règles de détection et d'alerte.
- Visualiser et analyser les événements de sécurité.
- Produire des rapports d'incidents détaillés.
- Démontrer une approche purple-team combinant attaque et défense.
- Agents a implementer:

1- Agent de triage des alertes : priorité des alertes

2- Agent d'enrichissement contextuel: transforme le log a quelque chose human readable

3- Agent de génération de résumé et de rapport: un résumé de l'incident

Fonctionnalités principales attendues :
- Déploiement d'un environnement Windows/Linux en machine virtuelle.
- Intégration d'un SIEM pour la collecte et la corrélation des logs.
- Simulation d'attaques contrôlées dans un cadre sécurisé.
- Création de règles de détection personnalisées.
- Génération d'alertes lors d'activités suspectes.
- implémentation des agents mentionnés dessus
- Export ou génération de rapports d'incidents.

Périmètre de la phase initiale :
- Mise en place du laboratoire.
- Journalisation centralisée.
- Détection de quelques scénarios d'attaque de base.
- Validation des règles de détection.
- Documentation technique du fonctionnement.

Bonus possibles :

-Agent de réponse automatique contrôlée: il pourrait lancer des actions comme mettreun serveur en quarantaine (SOAR)

- Réponse active automatisée sur certaines alertes critiques.
- Cartographie MITRE ATT&CK des techniques simulées et détectées.
- Intégration d'un enrichissement des alertes via VirusTotal.
- Surveillance de l'intégrité des fichiers (FIM).
- Analyse de fichiers suspects avec YARA.
- Génération semi-automatique de rapports d'incidents.
- Tableau de bord d'investigation avec chronologie des événements.
- Scénarios d'attaques reproductibles pour tester la couverture des détections.
- Mesure de la couverture des règles de détection.
- Réduction et suivi des faux positifs.
- assistant de notification et de synthèse d'incidents.
- Interface ou mécanisme de visualisation des traces.

Livrables :
- Code source ou configuration du laboratoire.
- Documentation d'installation et d'utilisation.
- Liste des scénarios d'attaque simulés.
- Règles de détection développées.
- Exemples d'alertes et de rapports d'incidents.
- Présentation finale du projet.