Système de Détection d'Activités Suspectes

Table des matières

Chapitre 1 : Introduction

1. Contexte

Détection et surveillance des comportements suspects et des activités non autorisées au sein d'un réseau d'entreprise à l'aide d'une analyse avancée du trafic et de l'apprentissage automatique.

2. Objectif

Développer un Système de Détection d'Activités Suspecte pour la direction, offrant :

- Concevoir un système de détection des anomalies en temps réel dans le trafic réseau
- Identifier les activités utilisateur suspectes et les comportements non autorisés
- S'appuyer sur une infrastructure robuste pour surveiller efficacement le réseau
- Intégrer des algorithmes avancés pour détecter les menaces
- Utiliser des outils de reporting pour améliorer la sécurité du réseau
- Garantir la conformité aux normes de sécurité

Chapitre 2 : Fonctionnalités Principales

1. Planification et Analyse des Besoins

Tâches :

- Définir le périmètre du réseau et les exigences en matière de sécurité.
- Identifier les fonctionnalités clés (ex. : surveillance du trafic en temps réel, détection d'anomalies, conformité à la norme **ISO 27001**).
- Analyser l'infrastructure réseau existante et planifier l'intégration.

Livrables :

- Document détaillé des exigences.
- Plan d'architecture réseau.

2. Mise en Place de l'Infrastructure

Tâches :

- Configurer le réseau pour une mise en place d'un proxy transparent avec **Squid**.
- Installer **Elasticsearch** pour le stockage et l'analyse des journaux.
- Assurer une segmentation réseau adéquate et des politiques de sécurité efficaces.

Livrables :

- Proxy entièrement fonctionnel.
- Cluster **Elasticsearch** prêt pour l'ingestion des journaux.

3. Surveillance du Réseau et Journalisation

Tâches :

- Mettre en œuvre des outils de surveillance du trafic en temps réel.
- Configurer la journalisation pour toutes les activités réseau (ex. : accès des utilisateurs, transferts de fichiers, volume de données).
- Mettre en place des alertes pour détecter les anomalies de base (ex. : accès non autorisé, transferts de fichiers inhabituels).

Livrables :

- Système de surveillance du trafic en temps réel.
- Mécanisme de journalisation intégré avec **Elasticsearch**.

4. Tableau de Bord et Système de Reporting

Tâches :

- Développer un tableau de bord interactif avec **Kibana** pour la surveillance en temps réel.
- Implémenter des fonctionnalités de reporting pour une analyse détaillée des activités réseau.
- Mettre en place des systèmes de notifications (e-mail) pour les alertes critiques.

Livrables :

- Tableau de bord **Kibana** fonctionnel.
- Système automatisé de reporting et d'alertes.

5. Intégration et Tests

Tâches :

- Intégrer le système de surveillance réseau avec l'infrastructure existante.
- Effectuer des tests de charge pour garantir la scalabilité et la gestion de volumes élevés de trafic.
- Vérifier la conformité avec les normes **ISO 27001**.

Livrables :

- Système de surveillance réseau entièrement intégré et testé.
- Rapport de conformité.

6. Optimisation et Documentation

Tâches :

- Optimiser les performances du système pour minimiser la latence et l'impact sur le réseau.
- Documenter l'installation, la configuration et l'utilisation du système.
- Rédiger un manuel utilisateur pour le tableau de bord et les outils de reporting.

Livrables :

- Système optimisé avec une latence minimale.
- Documentation complète.