Lycée Elie Vinet
16300 BARBEZIEUX ST HILAIRE
BTS SIO

Atelier de Professionnalisation 4

Société DMH

Projet Phase 2

Sommaire

CONTEXTE ET ORGANISATION

Contexte et objectifs

Avec l'augmentation des cyberattaques et des menaces de sécurité, DMH a pris conscience de la nécessité de renforcer la sécurité de son infrastructure informatique. Actuellement, la société utilise des solutions de sécurité basiques qui ne sont plus suffisantes pour protéger efficacement ses données sensibles et ses systèmes critiques. Plusieurs incidents récents ont mis en lumière des failles de sécurité qui pourraient avoir des conséquences désastreuses si elles étaient exploitées par des attaquants.

Objectifs du Projet

L'objectif principal de ce projet est de sécuriser l'infrastructure de la société DMH en mettant en place un SIEM (Security Information and Event Management), un IPS (Intrusion Prevention System) et un centre de supervision. Ces solutions permettront de :

1. Détecter et Répondre aux Menaces en Temps Réel : Le SIEM centralisera les logs et les événements de sécurité provenant de différentes sources, permettant une analyse en temps réel et une réponse rapide aux incidents.
2. Prévenir les Intrusions : L'IPS surveillera le trafic réseau et bloquera les activités malveillantes avant qu'elles ne puissent causer des dommages.
3. Superviser et Gérer la Sécurité : Le centre de supervision offrira une vue d'ensemble de l'état de sécurité de l'infrastructure, permettant aux équipes de sécurité de DMH de surveiller et de gérer efficacement les incidents.

Organisation

- Chaque membre de l’équipe aura en charge un des sous-projets
- Chaque semaine, un étudiant jouera le rôle de chef de projet. Un compte rendu sera systématiquement rédigé pour chaque séance suivante. Il s’appuiera sur les états d’avancement tenus par tous les membres de son équipe sur leur travail respectif. Un outil de travail collaboratif et / ou de gestion de projet de votre choix (*par exemple Trello*) pourra être utilisé.
- Il s’agit aussi d’un travail d’équipe, l’étudiant en difficulté bénéficiera de l’aide de ses partenaires.

SOUS-PROJETS ATELIER DE PROFESSIONNALISATION 4

Sous-projet D – SIEM (splunk ou graylog)

Objectifs

- Identifier les différentes sources de log
- Installation de l'outil
- Paramétrage de la centralisation des logs sur l'outil
- Configuration des forwarders de log sur les sources pour définir les alertes à remonter
- Définir les règles de détection d'anomalies
- Configurer les alertes pour prévenir l'équipe de supervision (email, sms …)

Attendus

- Une documentation sur l'outil et la mise en œuvre de l'outil choisi
- Un document décrivant les procédures de surveillance continue pour détecter et répondre aux incidents de sécurité.
- Un document précisant comment mettre à jour régulièrement les règles et les configurations pour maintenir la sécurité de l'infrastructure
- Une fiche de procédure des tests réalisés.

Sous-projet E – Mise en place d'une solution de supervision

Objectifs

- Installer et configurer PRTG sur une machine Windows dédiée à cette fonction
- Établir un cahier des charges permettant de définir ce qui doit être supervisé, quels sont les éléments et informations à remonter, quels sont les éléments critiques donnant lieu à une alerte et quels sont les rapports à produire .
- Mettre en œuvre la supervision suivant ce cahier des charges.

Attendus

- Un document décrivant la configuration du superviseur mis en place.
- Le cahier des charges
- Des services de supervision opérationnels
- Une fiche de procédure des tests réalisés.

Sous-projet F – IPS (snort ou suricata)

Objectifs

- Choix justifié de l'outil
- Installation et configuration de l'outil
- Définition et configuration des règles
- Intégration avec l'outil SIEM

Attendus

- Une documentation sur l'outil et la mise en œuvre de l'outil choisi
- Un document décrivant les procédures de surveillance continue pour détecter et répondre aux incidents de sécurité.
- Un document précisant comment mettre à jour régulièrement les règles et les configurations pour maintenir la sécurité de l'infrastructure
- Une fiche de procédure des tests réalisés.