Cahier des charges

Projet M2 Mastère Cybersécurité

Création d'une solution automatisée de déploiement d'une plateforme de sécurité

DIGISEC

Table des matières

I. Contexte 3
II. Objectifs.....4
III. Livrables attendus 4

I. Contexte

Le client est une filiale industrielle dans le domaine des produits chimiques.

Elle rachète des sites de productions et des usines partout dans le monde afin d'accroitre sa position dominante sur le marché.

Le secteur du client est soumis à un grand nombre de réglementations et de normes, en plus de celles imposées par la direction pour rassurer ses clients.

Les systèmes d'information des services supports (RH, finances, ...) sont raccordés au reste du groupe. Néanmoins, les systèmes d'informations industriels restent isolés, mais à sécuriser.

Dans ce cadre, le client est à la recherche d'une solution leur permettant de déployer un socle de sécurité minimum dans les SI Industriels des usines nouvellement acquises.

Ces systèmes d'information ne sont pas homogènes d'une usine à l'autre, le client souhaite donc une solution couvrant les besoins primaires :

- Sécurisation de l'environnement Active Directory (Priorité sur la mise en place de *Tiering*)
- Mise en place d'un bastion, avec intégration de l'architecture mise en place avec le *Tiering* pour assurer le cloisonnement des connexions au SI
- Mise en place d'une plateforme SIEM, intégration des logs (Active Directory, Bastion) et mise en place d'alertes.
- Automatisation du déploiement uniquement en PowerShell et Python pour l'intégrabilité aux nouveaux SI.

L'ensemble des plateformes déployées doivent répondre aux impératifs de base en matière de sécurité (Chiffrement, authentification, ...)
L'ensemble de la solution doit être documenté afin de permettre aux équipes sur site d'intégrer de nouvelles sources dans le bastion et/ou le SIEM.

II. Objectifs

Ce projet vise à concevoir une plateforme de démonstration fonctionnelle, sécurisée, documentée et industrialisable.

Objectifs généraux :
- Déployer un socle de sécurité dans un SI répondant aux nouvelles attentes normatives et réglementaires ;
- Créer un environnement de démonstration opérationnel ;
- Fournir un système industrialisable, intégrable dans un modèle d'infogérance.

Objectifs pédagogiques :
- Concevoir une solution d'intégration automatisée du *Tiering* en environnement *Active Directory*.
- Déployer et configurer une solution de bastion ;
- Déployer et configurer un SIEM open-source ;
- Intégrer des sources de logs variées ;
- Créer des dashboards et règles de détection ;
- Concevoir une architecture sécurisée, scalable, interopérable.

III. Livrables attendus

- Analyse initiale ;
- Architecture technique (DAT) ;
- Démonstrateur opérationnel ;
- scripts de déploiement focntionnels
- Dashboards & alertes configurés ;
- Playbooks / procédures ;
- Rapport technique complet ;
- Guide de déploiement & d'utilisation ;
- Vidéo de démonstration.