Contexte Installation Agent XDR

Le but est de sécuriser le parc informatique et d'avoir un visuel sur le traffic, que ce soit au niveau des postes utilisateurs tout autant que sur les serveurs applicatif pour réduire le risque d'attaque qui peuvent notamment conduire à une indisponibilité des services ou une fuite de données, pour ce faire le GSIC (groupement des systèmes d'informations et de communications) a décidé de mettre en place la solution Cortex XDR de l'entreprise Palo Alto.

Livrable Associé :

- Doc Installation XDR.pdf

Présentation de la Solution Cortex XDR

Cortex XDR représente une évolution majeure dans la protection des infrastructures IT modernes.

Cortex XDR (Extended Detection and Response) est une plateforme de sécurité native dans le cloud développée par Palo Alto Networks.

Contrairement aux solutions antivirus traditionnelles EDR fonctionnant en silo, l'XDR analyse tout l'ecosysteme numerique de l'entreprise, comprenant les données des machines ainsi que ce qui ce passe dans le réseau et dans le cloud.

On dit qu'il casse ces silo et corrèle toute les données en eux sur une platforme hebergé chez Palo Alto

Architecture XDR

Le XDR unifie :

- Les terminaux (postes et serveurs)
- Le réseau
- Le cloud

Cette approche permet une corrélation complète des événements de sécurité.

Fonctionnalités Clés de Cortex XDR

Cortex XDR se distingue par quatre piliers fondamentaux qui en font une solution de sécurité de nouvelle génération :

Visibilité étendue

Il collecte et corrèle les données provenant non seulement des terminaux (serveurs/poste), mais aussi du réseau et du cloud.

Détection par l'IA

Il utilise l'apprentissage automatique (Machine Learning) pour identifier des comportements anormaux qui pourraient indiquer une cyberattaque furtive.

Réponse aux incidents

Il permet de stopper instantanément une menace (isolement d'un serveur du réseau, arrêt d'un processus malveillant) depuis une console centralisée.

Investigation

Il offre une chronologie complète des événements pour comprendre comment une menace a pénétré dans l'infrastructure.

À ce jour, à la décision du RSSI, la solution est uniquement mise en place pour surveiller, elle ne bloque aucune donnée mais à l'avenir une fois qu'on se sera assuré que le service ne pose pas de problème de fonctionnement sur nos serveurs, il sera mis en mode blocage

Implantation des Agents Clients

Pour ce projet, j'ai donc été assigné à un ticket et chargé d'implanter les agents clients dans certains de nos serveurs.

Critères de Sélection des Serveurs

une extraction du parc informatique à été effectué avec un outil de VMware et nous avons établi un tableur comme celui ci pour avoir un visuel de toute les machines à traiter

Nom de VM	OS d'après VMware	Etats installation XDR	Version de Cortex

Système d'exploitation et Distribution

En fonction de leur OS et distribution (Windows, Linux Debian, Ubuntu, CentOS, etc.). Car certaines vieille distribution ne sont pas compatible, par exemple Debian 8

Machines de prod

au vu du coup conséquent des licences pour ce produit, les Agents vont être déployé uniquement sur les machines de prod ainsi que les recettes qui sont "sensibles"