Case Study

Cyber Security

CIMO

Quelques chiffres :

- 80 Bâtiments
- Site de 120ha
- 450 Employés
- 200 Serveurs

Technologies :

- Saporo
- Microsoft AD Tiering
- SentinelOne
- Microsoft Intune
- Environnements ADDS, EntraID, ADCS

Sécurisation des identités & gestion de la surface d'attaque

Depuis deux ans, CIMO a engagé plusieurs initiatives sécurité complémentaires afin de sécuriser durablement son SI, notamment par l'adoption d'outils dédiés à la gestion de sa surface d'attaque et à la sécurisation de ses identités numériques.

Introduction

Forte d'une histoire de plus de 125 ans, la Compagnie industrielle de Monthey SA, ci-après CIMO, est une entreprise qui fournit des prestations en production et distribution d'énergie, traitement des résidus, analyses environnementales, gestion des infrastructures, et maintenance technique pour le site de Monthey, soit un campus industriel de 120 hectares historiquement dédié à l'industrie chimique.

CIMO fournit ses services d'infrastructure à un certain nombre de fleurons de l'industrie chimique parmi lesquels Syngenta ou BASF. Dans ce contexte, la sécurité de l'infrastructure du site de Monthey est une priorité absolue pour les équipes IT de CIMO.

Depuis la fin 2023, CIMO a recruté Didier Martenet pour reprendre progressivement la direction de son département informatique. Après une phase d'analyse, il a décidé d'engager les premiers chantiers en lien avec la sécurisation des identités et des accès.

Sécurisation des identités

Quelque soit l'origine d'une attaque ou d'une infection, 90% des incidents liés à la cybersécurité exploitent les faiblesses des systèmes de gestion d'identités pour pouvoir effectuer des mouvement latéraux au sein d'un environnement IT après une première compromission (humaine ou technique).

L'avènement du Cloud amplifie ce phénomène en raison de l'explosion des volumes d'identités, ce qui complexifie la mise en œuvre d'une segmentation efficace des accès et expose toujours plus les assets critiques d'une organisation.

L'adoption combinée des différents «frameworks» de sécurité, qu'il s'agisse par exemple du MITRE ATT&CK, du CIS (Center for Internet Security) ou encore de l'ANSSI en France, nécessite un outillage adapté pour permettre aux équipes opérationnelles d'améliorer progressivement la qualité de leurs pratiques.

Une démarche structurée

Avec le conseil de CloudEdge, CIMO a ainsi engagé plusieurs chantiers afin d'adresser les différentes thématiques liées à la sécurisation de ses identités.

CloudEdge

Make IT more Human

Case Study

Cyber Security

Didier MARTENET
Responsable IT

« CloudEdge nous a permis de mettre en œuvre une approche structurée de la sécurisation des identités et de renforcer durablement notre posture »

Avant de s'intéresser aux identités « utilisateurs », l'équipe IT de CIMO s'est d'abord concentrée sur les comptes privilégiés, c'est-à-dire à toutes les identités numériques liées à l'administration des systèmes (Ex : comptes de service, comptes administrateurs, gestion des mots de passe).

Un modèle de tiering Active Directory a été mis en œuvre pour segmenter les identités suivant la criticité des assets auxquels ils avaient accès. A cet effet, Microsoft décrit de manière théorique le modèle de tiering en question mais fournit peu d'informations sur sa mise en œuvre pratique.

La seconde étape de ce projet a consisté à déployer une solution de gestion des accès privilégiés (PAM) pour canaliser et sécuriser les interventions à distante des différents prestataires externes impliqués dans la gestion de certains systèmes au sein du SI de CIMO.

En s'appuyant sur le travail préalable d'une société spécialisée, CloudEdge a pu accompagner CIMO sur la remédiation d'un certain nombre de faiblesses liées à l'environnement Microsoft 365, qu'il s'agisse du tenant Microsoft du client, ou de configurations de sécurité déployées au travers d'Intune.

Gestion de surface d'attaque centrée sur les identités

L'aboutissement de cette démarche de sécurisation des identités repose sur le déploiement d'une solution avancée de gestion de la posture sécurité spécialisée sur les identités, soit l'éditeur suisse Saporo.

Cette plateforme n'a pas été déployée pour un audit ponctuel, mais dans une logique d'amélioration continue afin de permettre à CIMO d'augmenter drastiquement sa résistance en cas d'attaque, et aux équipes IT d'adapter durablement leurs pratiques.

CIMO a pu prioriser ses tâches de remédiation, qu'il s'agisse de couper les chemins d'attaque représentant le risque ou la probabilité les plus élevés, ou corriger les défauts de configuration de ses système de gestion des identités pour respecter les bonnes pratiques.

En complément de sa gestion de l'Active Directory, CIMO a également pu étendre le périmètre de son analyse aux services de fichiers.

Les deux prochaines extensions de l'analyse Saporo concernent son ouverture au périmètre Cloud et à l'analyse de son environnement de gestion de certificats (PKI).

En effet, la couverture croisée de l'Active Directory (ADDS) pour les identités on-premise et d'EntraID pour les identités Cloud permettra de couper les derniers héritages de droits inhérents aux environnement hybrides.

La combinaison de ces différentes initiatives a ainsi permis à l'équipe IT de CIMO d'augmenter sa maturité en matière de cybersécurité, offrant au métier des garanties crédibles et pérennes quant à la sécurité et à la résilience de son système d'information.

CloudEdge
Make IT more Human