Offre de service

Cloud Infrastructure

Technologies concernées :
- Saporo

Charge estimée : 1-3 Jours

Budget estimé : 2-5 KCHF

Projet pilote ASM Saporo

Introduction

Les identités numériques représentent aujourd'hui l'un des principaux vecteurs d'attaque pour les cybercriminels. Comptes administrateurs, identités hybrides, infrastructures d'authentification et services de certificats sont autant de points d'entrée critiques qui peuvent être exploités en cas de mauvaise configuration ou de privilèges excessifs.

Les environnements modernes reposent souvent sur une combinaison d'Active Directory, Microsoft Entra ID (anciennement Azure AD) et d'infrastructures PKI telles que Microsoft ADCS. Cette complexité multiplie les dépendances et les risques, notamment lorsque les relations de confiance, les privilèges et les chemins d'attaque ne sont pas clairement identifiés.

La solution Saporo permet d'analyser et de visualiser la surface d'attaque liée aux identités, afin d'identifier les chemins d'attaque potentiels, les privilèges excessifs et les vulnérabilités de configuration.

Notre offre de projet pilote Saporo permet d'évaluer ces risques dans votre environnement réel et de démontrer concrètement comment renforcer la sécurité de votre infrastructure d'identité.

Périmètre de la prestation

Les infrastructures d'identités modernes sont interconnectées et complexes à protéger.

L'hybridation généralisée des environnements Active Directory et EntraID engendre une croissance massive des volumes d'identités, une multiplication des comptes à privilèges et des chemins d'attaque.

Dans ce contexte, il devient quasiment impossible pour les équipes IT d'assurer une gestion efficiente et sécurisée de ces identités.

Le projet pilote Saporo permet d'analyser la surface d'attaque liée aux identités, d'identifier les chemins d'escalation de privilèges, de détecter les mauvaises configurations, de mettre en évidence les risques critiques, et de prioriser les actions de remédiation.

Cette approche offre une visibilité stratégique sur la sécurité des identités et des privilèges.

Attention, cette prestation est un projet pilote et non un audit à proprement parler, ce qui signifie que vous aurez de la visibilité sur votre niveau de sécurité global post-audit, mais que la solution ne vous permettra pas d'exporter l'intégralité des résultats. En effet, selon notre conception, la gestion de la surface d'attaque a pour objectif d'améliorer durablement votre sécurité, et ne peut être traitée uniquement de manière ponctuelle.

SAPORO
ORDER IN CHAOS

CloudEdge
Make IT more Human

Offre de service

Cloud Infrastructure

Prérequis du mandat

Ce mandat nécessite la pleine collaboration des équipes du client durant tout le déroulement de la prestation, et leur disponibilité pour les phases de transfert de compétences. Il implique également l'autorisation par le client d'héberger le collecteur au sein de l'infrastructure virtuelle du client.

Après le setup initial, les équipes de CloudEdge doivent pouvoir disposer d'un accès à distance pour la finalisation des phases de test, et de droits suffisants pour les différentes analyses (compte utilisateur (Read Only), Enterprise App pour le tenant M365 du client).

Déroulement de la prestation

Le projet pilote Saporo est conçu pour fournir rapidement une vision claire des risques liés à votre gestion des identités. La première étape du mandat consiste à identifier les gestionnaires d'identité qui seront intégrés au périmètre du pilote, qu'il s'agisse des environnements Active Directory ADDS, EntraID et PKI ADCS.

La seconde phase du pilote consiste à déployer Saporo sous forme de machine virtuelle au sein de l'infrastructure du client, à configurer les premières sources de données qui permettront de collecter toutes les informations liées aux identités et privilèges, d'analyser les configurations de sécurité et enfin de cartographier les relations et dépendances entre les identités et les systèmes. Après quelques minutes ou heures d'attente, vous disposerez d'une une vision détaillée et automatisée de votre surface d'attaque.

L'étape suivant consiste à analyser conjointement avec le client les données préalablement collectées pour identifier les privilèges excessifs, détecter les configurations vulnérables et visualiser les potentiels chemins d'attaque. Les résultats permettent de d'évaluer votre niveau de maturité global prioriser les actions de remédiation.

À l'issue du projet pilote, vous disposerez d'une expérience concrète sur la plateforme Saporo, de recommandations pour renforcer la sécurité de vos identités, de bonnes pratiques pour la gestion des privilèges et d'un plan de déploiement complet de la solution Saporo. Vous disposerez ainsi d'une feuille de route claire pour sécuriser votre infrastructure d'identité.

Bénéfices attendus par le client

Le projet pilote Saporo permet à votre organisation de comprendre et maîtriser la surface d'attaque liée aux identités, un élément critique de la cybersécurité moderne.

Grâce à cette démarche, vous bénéficiez d'une visibilité complète sur les privilèges, les dépendances et les risques potentiels, vous permettant de sécuriser efficacement vos environnements Active Directory, EntraID et PKI.

Votre infrastructure d'identité devient ainsi plus résiliente, mieux gouvernée et prête à faire face aux menaces actuelles et futures.

SAPORO
ORDER IN CHAOS

CloudEdge
Make IT more Human