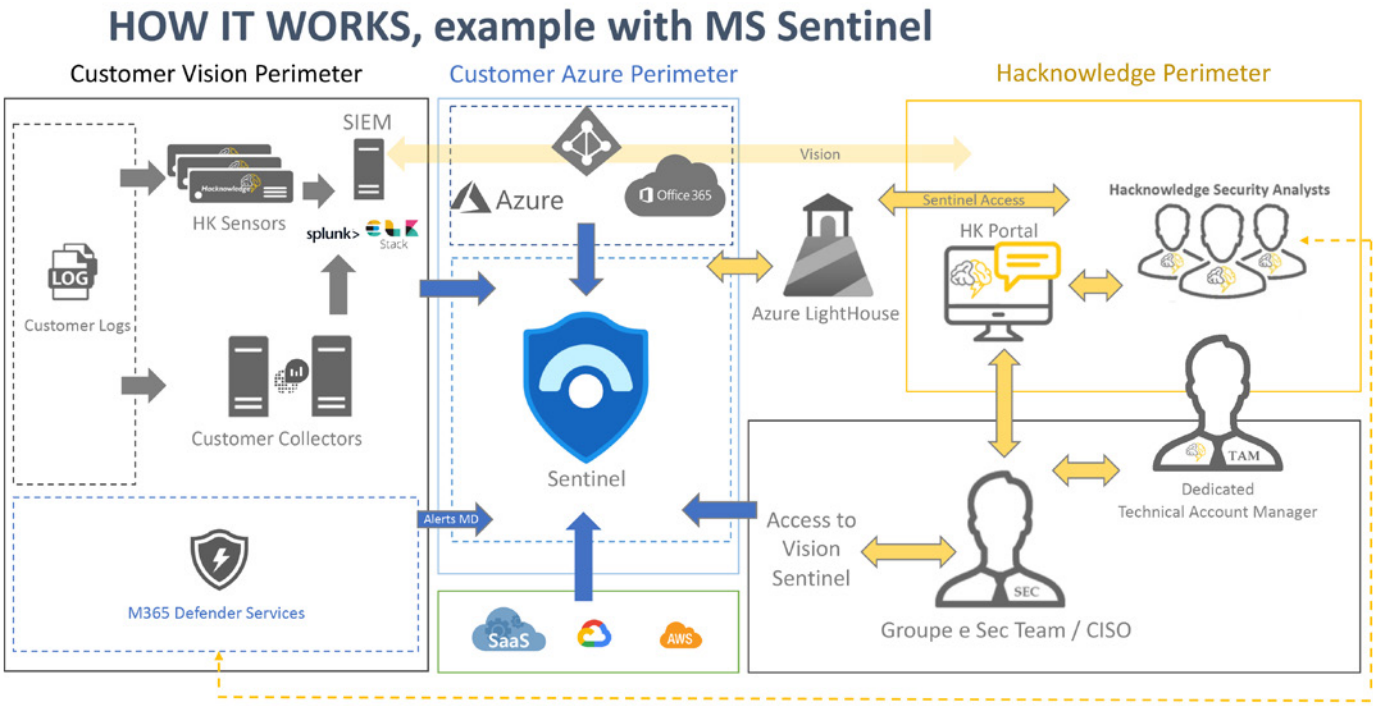
Cybersurveillance
Réduire le délai de détection de violations de la sécurité

La cybercriminalité ne relève pas de la science-fiction, c'est une menace réelle pour les entreprises. Les organisations touchées peuvent très vite être confrontées à des demandes de rançon, à des arrêts de production et à des opérations de remise en état coûteuses. Il faut en moyenne 100 jours à une entreprise pour découvrir ou être informée d'une violation. Il est donc d'autant plus important de mettre en place une surveillance permanente des systèmes. Le service géré par le spécialiste de la cybersécurité Hacknowledge vise à réduire ce délai au minimum ainsi qu'à aider les clients à prendre des mesures et à prévenir toute activité de piratage sur leur réseau.

Security Operations Center (SOC)

Hacknowledge fournit un SOC et un SIEM (Security Incident and Event Management) gérés pour collecter les journaux si ceux-ci ne sont pas disponibles. Il s'agit d'un produit tout-en-un qui s'adapte parfaitement à l'environnement des clients. Le service est suisse, simple et efficace. En effet, les données restent en Suisse à tout moment, Hacknowledge construit sur l'environnement de sécurité informatique existant et le service est capable de s'adapter au contexte des clients.



Vos avantages

– Surveillance 24 heures sur 24 et 7 jours sur 7: les ingénieurs experts en sécurité détectent les menaces et réagissent avec les solutions de pointe VISION Cyber Management™.

– Signalement des incidents de sécurité qualifiés et libération de votre équipe de sécurité pour qu'elle puisse se concentrer sur les événements importants: nous prenons en charge le traitement des journaux pour vous, ce qui vous laisse plus de temps pour travailler sur les incidents qualifiés.

– Solution suisse: toutes les données sont stockées en Suisse, les ingénieurs travaillent de la Suisse, il n'y a pas de problèmes de données confidentielles ou personnelles à l'étranger.

– Hacknowledge est certifiée ISO 27001 (sans exceptions) et se conforme au RGPD.

– Entreprise neutre: vous avez la garantie de bénéficier de l'assistance d'un prestataire de services indépendant.

– La solution est transparente et vous avez un accès complet à vos données (p. ex., les journaux et les événements de sécurité) à tout moment.

– Les services annexes couvrent toute la cybersécurité: tests d'intrusion, criminalistique, sensibilisation du personnel.

Surveille. Détecte. Réagit.

1) La première étape consiste à définir le périmètre à couvrir, tant en termes d'environnement informatique que de cas d'utilisation. Il vaut mieux commencer petit et étendre le concept par la suite.

2) Hacknowledge peut déployer un SIEM pour consolider et corréler les journaux de sécurité; si un SIEM est déjà en place, Hacknowledge est en mesure de s'y connecter pour fournir le service SOC.

3) Hacknowledge aide les clients à collecter les journaux et à les transmettre au SIEM. Des capteurs peuvent être utiles pour enrichir et analyser les journaux plus près de la source, ce qui évite de surcharger le réseau et optimise la quantité de données envoyées au SIEM.

4) Hacknowledge déploie les cas d'utilisation un par un pour garantir un suivi fonctionnel et efficace. Nous testerons les scénarios ensemble et nous filtrerons les faux positifs.

5) En plus de signaler les incidents de sécurité dès que nécessaire, Hacknowledge fournit des rapports de sécurité réguliers afin d'améliorer la collaboration en continu.

Solution adaptative et flexible

Trois SIEM sont pris en charge nativement par le SOC: SPLUNK, Microsoft Sentinel et Vision (Kibana et ELK stack). La solution Hacknowledge est très adaptable et flexible, ce qui permet de déployer le contrôle de la sécurité dans votre environnement informatique et technologique en douceur et de manière efficace.

Poste CH Communication SA
Digital Business
Wankdorfallee 4
3030 Berne
Suisse

E-mail digital-business@poste.ch
poste.ch/hacknowledge-business