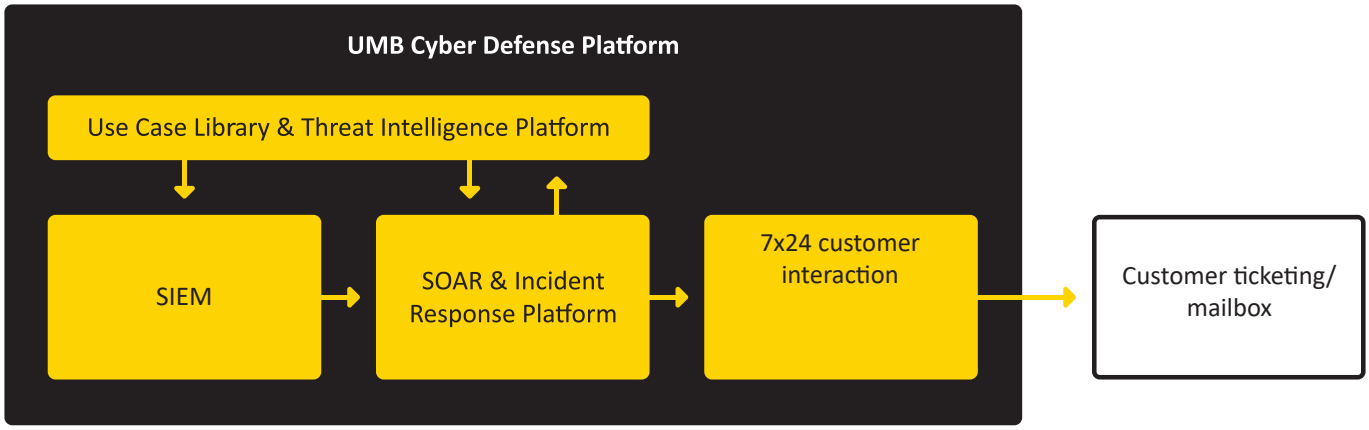
SIEM as a Service : réduisez dès maintenant votre temps de réaction face aux cyberattaques.

Selon le rapport 2020 d'IBM sur le coût d'une violation de données, il faut en moyenne 191 jours pour découvrir un vol de données et il faut encore 66 jours pour réagir. C'est nettement trop lent, car selon les études, les coûts sont fortement corrélés au temps de réaction. Plus il faut de temps pour contrer une attaque, plus l'intrusion peut coûter cher à l'entreprise. Confiez votre cyberdéfense aux experts d'UMB et réduisez considérablement vos temps de réaction.

L'UMB Cyber Defense Center collecte et évalue en permanence les incidents de sécurité. UMB détecte les menaces quasiment en temps réel grâce aux cas d'utilisation mis en œuvre dans le SIEM (Security Information and Event Management), qui sont analysées 24 heures sur 24 dans le Cyber Defense Center d'UMB. Avec une infrastructure classique, environ dix incidents sur un milliard d'événements parviennent à UMB pour analyse. Si l'analyste de sécurité d'UMB confirme l'anomalie, une recommandation d'action est immédiatement soumise au client dans le cadre du service level agreement (SLA) convenu.



Notre service cloud vous sécurise 24h/24 et 7j/7

Le SIEM nécessaire à la surveillance de la sécurité est placé dans l'UMB Security Cloud. Vous profitez ainsi de manière fiable et flexible d'une analyse de sécurité de premier ordre qui peut s'adapter rapidement à l'évolution des exigences de l'entreprise, de la sécurité ou de la protection des données. L'accès aux données est strictement contrôlé et surveillé par des programmes internes d'UMB dédiés à la surveillance et à la vérification des utilisateurs privilégiés.

L'UMB Cyber Defense Center examine 24 heures sur 24 les événements de sécurité signalés. Selon la criticité de l'incident, les clients reçoivent un appel téléphonique, un message texte ou un e-mail. Les détails des incidents de sécurité et les recommandations pour y remédier sont disponibles via le système de ticketing. Toutes les données du journal sont stockées sur le SIEM dans le Security Cloud sécurisé d'UMB. Seules les alarmes sont envoyées au Cyber Defense Center. Pour les analyses et les investigations, nos analystes se connectent au SIEM hébergé.

Traitement rapide et fiable des incidents

La plateforme de réponse aux incidents, qui fait partie intégrante de notre service, garantit un traitement cohérent et coordonné des incidents. Pour ce faire, les playbooks jouent un rôle central en traitant de manière rapide et globale les informations provenant du SIEM et d'autres sources de données afin d'en déduire des recommandations d'action concrètes pour le client. UMB utilise la technologie « Security Orchestration, Automation and Response » (technologie SOAR), qui est continuellement actualisée et développée afin de garantir un traitement rapide et sans erreur des incidents.

Éléments du service

- Surveillance des menaces et gestion des incidents 7x24
- Analyse et tri des menaces 7x24
- Capture évolutive de grands volumes de données à partir de vos sources sur site et dans le cloud
- Recommandation d'action pour tous les incidents transférés en escalade
- Hotline 24h/24 et 7j/7 permettant de contacter le Cyber Defense Center
- Stockage des données dans l'UMB Security Cloud avec une période de rétention flexible des données
- Disponibilité basée sur les SLA
- Rapport de service mensuel

Vos avantages

- Vous êtes à tout moment au courant de l'état des menaces qui pèsent sur votre entreprise.
- Les incidents de sécurité (Security Incidents) sont détectés à temps : UMB analyse les incidents 24 heures sur 24, vous alerte immédiatement en cas de danger accru et fournit des recommandations d'action pour votre stratégie de défense.
- La probabilité d'occurrence et le potentiel de dommages d'une attaque sont considérablement réduits.

Cela vous intéresse ? Contactez-nous !

Nous répondrons volontiers à vos questions sur le thème du SIEM as a service.

Contact

Markus Kaegi
Business Lead Security
markus.kaegi@umb.ch
+41 44 805 14 47
www.umb.ch