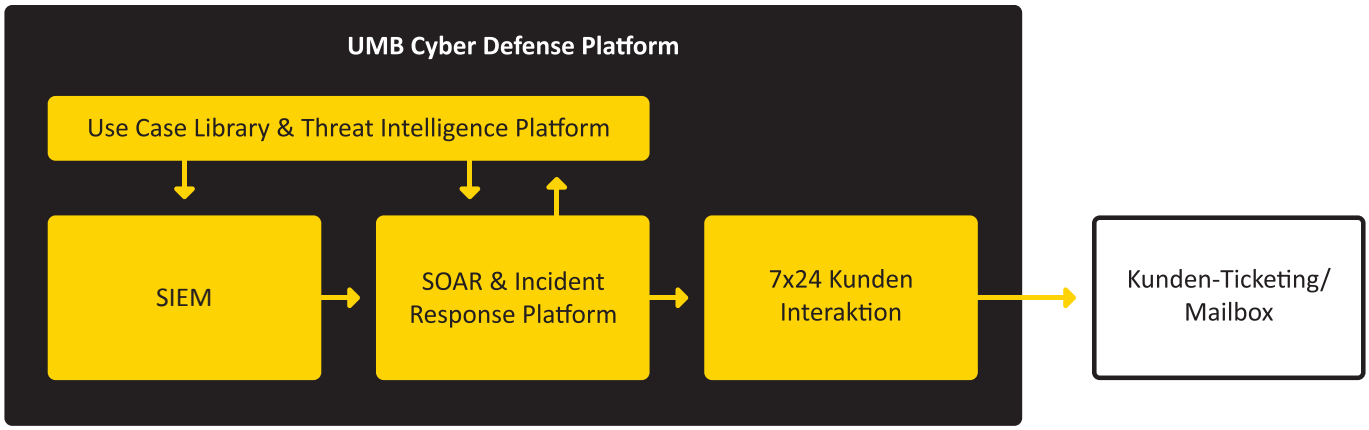
SIEM as a Service: Senken Sie jetzt Ihre Reaktionszeiten auf Cyberattacken.

Gemäss dem IBM Cost of Databreach Report 2020 dauert es im Schnitt 191 Tage, einen Datendiebstahl zu entdecken. Und es dauert nochmals 66 Tage, bis man darauf reagiert. Das ist deutlich zu langsam, denn die Kosten korrelieren gemäss den Studien stark mit der Reaktionszeit. Je länger es dauert, einen Angriff abzuwenden, desto teurer kann der Einbruch für die Firma werden. Überlassen Sie Ihre Cyberdefense den Experten von UMB und senken Sie die Reaktionszeiten dramatisch.

Das UMB Cyber Defense Center sammelt und bewertet permanent Sicherheitsvorfälle. UMB erkennt Bedrohungen aufgrund der im SIEM (Security Information and Event Management) implementierten Use Cases beinahe in Echtzeit. Im Cyber Defense Center der UMB werden diese rund um die Uhr analysiert. Bei einer typischen Infrastruktur gelangen von einer Milliarde Events rund zehn Vorfälle zwecks Analyse zu UMB. Bestätigt der Security-Analyst von UMB die Anomalie, wird dem Kunden innerhalb des vereinbarten Service-Level-Agreements (SLA) unverzüglich eine Handlungsempfehlung unterbreitet.



Unser Service aus der Cloud macht Sie rund um die Uhr sicher

Das für das Security Monitoring benötigte SIEM ist in der UMB Security Cloud platziert. Sie profitieren damit flexibel und zuverlässig von einer erstklassigen Sicherheitsanalyse, die sich rasch an sich verändernde Geschäfts-, Sicherheits- oder Datenschutzanforderungen anpassen kann. Der Zugriff auf die Daten wird mit UMB internen Programmen für die Überwachung und Überprüfung von privilegierten Benutzern streng kontrolliert und überwacht.

Das UMB Cyber Defense Center überprüft gemeldete Sicherheitsereignisse rund um die Uhr. Je nach Kritikalität des Vorfalls erhalten die Kunden einen Telefonanruf, eine Textnachricht oder eine E-Mail. Details zu Sicherheitsvorfällen und Empfehlungen zur Behebung sind über das Ticketing-System verfügbar. Alle Log-Daten werden auf dem SIEM in der sicheren UMB Security Cloud gespeichert. Zum Cyber Defense Center werden lediglich die Alarme gesendet. Für Analysen und Investigation verbinden sich unsere Analysten mit dem Hosted SIEM.

Rasche und zuverlässige Behandlung von Incidents

Die Incident Response Platform, welche integraler Bestandteil unseres Services ist, stellt eine konsistente und koordinierte Bearbeitung der Incidents sicher. Dabei sind Playbooks zentral. Playbooks müssen die Informationen aus dem SIEM und weiteren Datenquellen schnell und umfassend bearbeiten, um daraus konkrete Handlungsempfehlungen für den Kunden abzuleiten. UMB verwendet «Security Orchestration, Automation and Response»-Technologie (SOAR-Technologie), die umfangreich und kontinuierlich gepflegt und weiterentwickelt wird, damit eine zügige und fehlerfreie Verarbeitung der Incidents sichergestellt ist.

Servicebestandteile

- 7x24 Threat Monitoring & Incident Management
- 7x24 Threat Analyse & Triage
- Skalierbare Aufnahme grosser Datenmengen aus Ihren On-Premise- und Cloud-Quellen
- Handlungsempfehlung bei allen eskalierten Incidents
- 24x7-Hotline zur Kontaktaufnahme mit dem Cyber Defense Center
- Speicherung der Daten in UMB Security Cloud mit flexibler Data-Retention-Periode
- SLA gestützte Verfügbarkeit
- Monatlicher Servicebericht

Ihre Vorteile

- Sie sind jederzeit im Bild über die Bedrohungslage Ihres Unternehmens.
- Sicherheitsvorfälle (Security Incidents) werden frühzeitig erkannt: UMB analysiert Incidents rund um die Uhr, alarmiert Sie bei erhöhter Gefahrenlage unverzüglich und versorgt Sie mit Handlungsempfehlungen für Ihre Abwehrstrategie.
- Die Eintretenswahrscheinlichkeit und das Schadenspotential eines Angriffs wird deutlich gesenkt.

Klingt interessant? Kontaktieren Sie uns!

Gerne beantworten wir Ihre Fragen zum Thema SIEM as a Service.

Kontakt

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