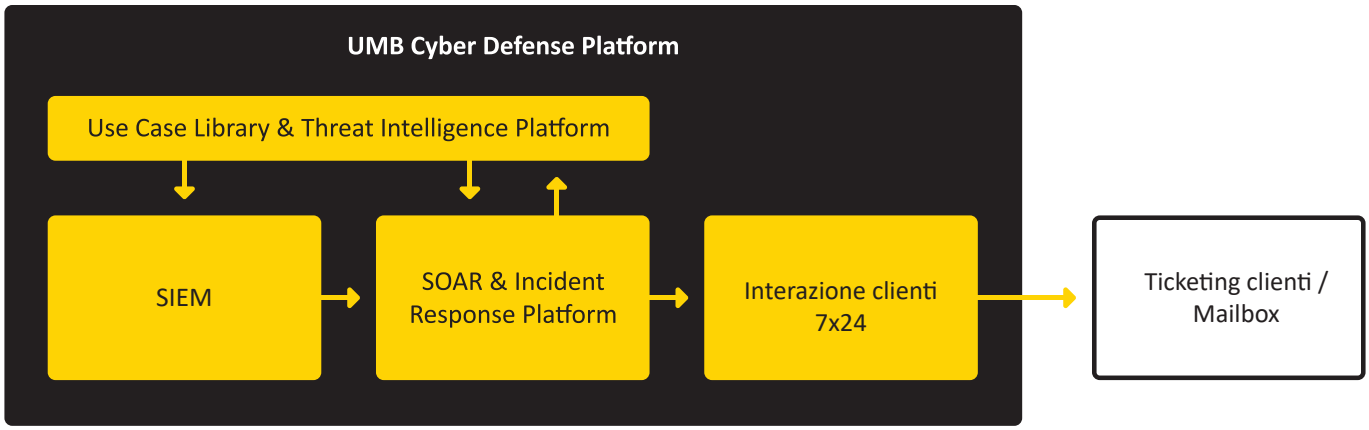
SIEM as a Service: riducete subito i tempi di risposta alle minacce informatiche.

Secondo l'IBM Cost of Databreach Report 2020, ci vogliono in media 191 giorni per scoprire un furto di dati. E ci vogliono altri 66 giorni per reagire. Si tratta chiaramente di una lentezza eccessiva, perché secondo gli studi i costi sono fortemente correlati ai tempi di risposta. Più tempo ci vuole per evitare un attacco, più costosa può essere l'intrusione per l'azienda. Lasciate che la vostra difesa informatica sia affidata agli esperti di UMB e ridurrete significativamente i tempi di risposta.

L'UMB Cyber Defense Center raccoglie e valuta costantemente gli incidenti di sicurezza. UMB rileva le minacce quasi in tempo reale grazie ai casi d'uso implementati nel SIEM (Security Information and Event Management). Questi vengono analizzati 24 ore su 24 nel Cyber Defense Center di UMB. In un'infrastruttura tradizionale, circa dieci incidenti su un miliardo di eventi raggiungono UMB per essere analizzati. Se l'analista di sicurezza di UMB conferma l'anomalia, viene immediatamente presentata al cliente una raccomandazione di intervento nell'ambito del service level agreement (SLA) concordato.



Il nostro servizio cloud vi garantisce una sicurezza 24h su 24

Il SIEM necessario per il monitoraggio della sicurezza è collocato nell'UMB Security Cloud. In questo modo potete beneficiare in modo flessibile e affidabile di un'analisi di sicurezza di prima categoria, in grado di adattarsi rapidamente alle mutevoli esigenze aziendali, di sicurezza o di protezione dei dati. L'accesso ai dati è seriamente controllato e monitorato con i programmi interni di monitoraggio e verifica degli utenti privilegiati di UMB.

L'UMB Cyber Defense Centre esamina gli eventi di sicurezza segnalati 24 ore al giorno. A seconda della criticità dell'incidente, i clienti ricevono una telefonata, un SMS o una e-mail. I dettagli degli incidenti di sicurezza e le raccomandazioni per la loro risoluzione sono disponibili tramite il sistema di ticketing. Tutti i dati di log vengono archiviati sul SIEM nel cloud sicuro di UMB Security. Solo gli avvisi vengono inviati al Centro di Difesa Informatica. Per le analisi e le indagini, i nostri analisti si collegano al SIEM in hosting.

Gestione rapida ed affidabile degli incidenti

La piattaforma di risposta agli incidenti, che è parte integrante del nostro servizio, garantisce una gestione coerente e coordinata degli incidenti. I libri di gioco sono fondamentali per raggiungere questo scopo. I playbook devono elaborare le informazioni provenienti dal SIEM e da altre fonti di dati in modo rapido e completo, al fine di ricavare raccomandazioni concrete per l'azione del cliente. UMB utilizza la tecnologia „Security Orchestration, Automation and Response" (tecnologia SOAR), che viene ampiamente e continuamente mantenuta e ulteriormente sviluppata per garantire un'elaborazione rapida e impeccabile degli incidenti.

Componenti del servizio

- Monitoraggio delle minacce e gestione degli incidenti 24h su 24
- Analisi e triage delle minacce 24h su 24
- Assorbimento scalabile di grandi quantità di dati da fonti on-premise e sul cloud
- Raccomandazione di azione per tutti gli incidenti segnalati
- Linea diretta 24h su 24, 7 giorni su 7, per contattare il centro di difesa cibernetica
- Archiviazione dei dati in UMB Security Cloud con un periodo di conservazione dei dati flessibile
- Disponibilità supportata da SLA
- Rapporto di servizio mensile

I vostri vantaggi

- Siete sempre informati sulle situazioni potenzialmente minacciose per la vostra azienda.
- Gli incidenti di sicurezza vengono rilevati nella loro fase iniziale: UMB analizza gli incidenti 24h su 24, vi avvisa immediatamente in caso di aumento del rischio e vi fornisce raccomandazioni per la vostra strategia di difesa.
- La probabilità di accadimento e il potenziale danno di un attacco sono notevolmente ridotti.

Suona interessante? Contattateci!

Saremo lieti di rispondere ad ogni vostra domanda sul SIEM as a Service.

Contatti

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