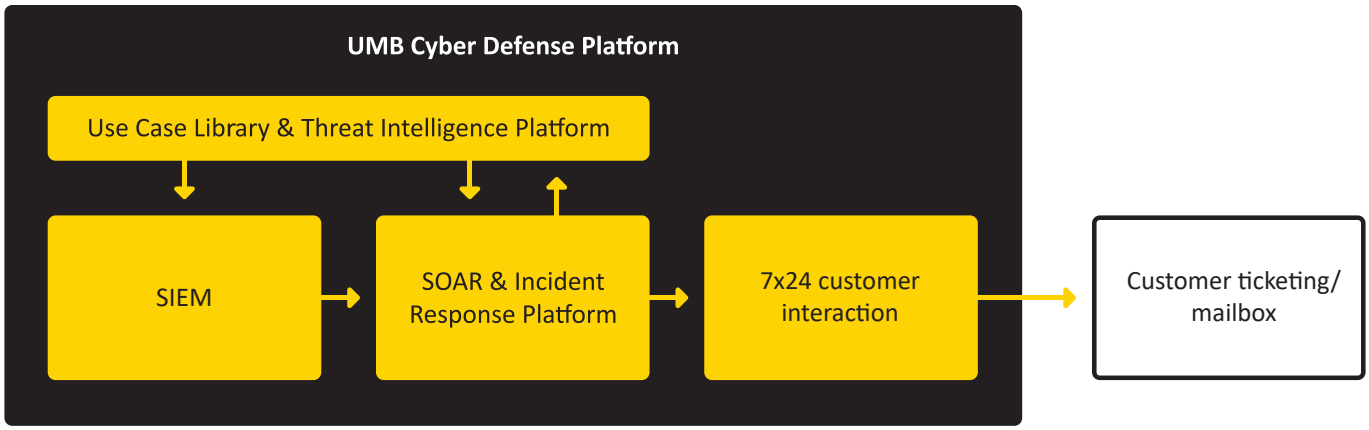
SIEM as a Service: Reduce Your Response Times to Cyberattacks Now.

According to IBM's Cost of a Data Breach Report 2020, it takes an average of 191 days to discover a data theft. Then it takes another 66 days to respond to it. This is clearly too slow, because, as studies show, costs correlate strongly with response time. The longer it takes to fend off an attack, the more expensive the intrusion will be for the company. Leave your cyber defense to the experts at UMB and reduce response times dramatically.

The UMB Cyber Defense Center continuously collects and evaluates security incidents. UMB detects threats almost in real time due to the use cases implemented in our security information and event management (SIEM). Incidents are being analyzed around the clock in UMB's Cyber Defense Center. In a typical infrastructure, around ten incidents out of a billion events reach UMB for analysis. If the UMB security analyst confirms the anomaly, a recommendation for action will immediately be submitted to the customer in accordance with the agreed service level agreement (SLA).



Our service delivered from the cloud keeps you safe around the clock

The SIEM required for security monitoring is operating from the UMB security cloud. This provides you with flexible and reliable first-class security analysis that adapts quickly to changing business, security or data protection requirements. Access to data is tightly controlled and monitored with UMB internal privileged user monitoring and auditing programs.

The UMB Cyber Defense Center reviews any reported security events around the clock. Depending on the criticality of the incident, customers receive a phone call, text message, or email. Details of security incidents and recommendations for remediation are available through the ticketing system. All log data is stored on the SIEM in the secure UMB security cloud. Only alerts are sent to the Cyber Defense Center. Our analysts connect to the hosted SIEM for analytics and investigative purposes.

Rapid and reliable handling of incidents

Our Incident Response Platform, an integral part of our service, ensures consistent and coordinated incident handling. Playbooks are central to this. Playbooks must process the information from the SIEM and other data sources quickly and comprehensively in order to derive concrete recommendations for action for the customer. UMB uses security orchestration, automation and response technology (SOAR technology), which is extensively and continuously maintained and enhanced to ensure rapid and error-free processing of incidents.

Service components

- 7x24 threat monitoring & incident management
- 7x24 threat analysis & triage
- Scalable intake of large amounts of data from your on-premises and cloud sources
- Recommendation for action on all escalated incidents
- 24x7 hotline for contacting the Cyber Defense Center
- Storage of data in the UMB security cloud with flexible data retention period
- SLA supported availability
- Monthly service report

Your benefits

- You will always have an accurate picture of the threat situation in your company.
- Security incidents will be detected at an early stage: UMB analyzes incidents around the clock, alerts you immediately in case of an increased threat situation and provides you with recommendations for your defense strategy.
- The probability of an attack occurring and the potential for damage is significantly reduced.

Sounds interesting? Contact us!

We are happy to answer your questions about

SIEM as a service.

Contact

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