Security Analytics as a Service

Steigern Sie Ihre Cybersicherheit mit einer Security-Analytics-Plattform, die Bedrohungen Ihrer Systemlandschaft in Echtzeit erkennt.

Mit Security Analytics as a Service (SAaaS) bietet Swisscom eine Plattform, um Sicherheitsvorfälle proaktiv über die ganze Systemlandschaft zu erkennen.
In der heutigen hochgradig vernetzten und digitalisierten Welt ist es von entscheidender Bedeutung, Ihre Unternehmensressourcen effektiv vor Cyberbedrohungen zu schützen. Genau hier kommen Security Information and Event Management (SIEM) ins Spiel – ein unverzichtbares Instrument, um Ihr Unternehmen umfassend zu schützen und potenzielle Sicherheitsvorfälle proaktiv zu erkennen und zu bekämpfen.

Ihre Nutzen mit SAaaS

SIEM-Plattform als Service

Sie profitieren von einer SIEM-Plattform zur Sammlung, Aggregierung und Korrelierung von Logdaten aus verschiedenen Datenquellen. ✓

Threat Detection Use Cases

Schnelle Reaktion auf potenzielle Sicherheitsvorfälle (Security Incidents) möglich – durch Threat Detection Use Cases. ✓

Compliance und Reporting

Compliance und Security Reporting für regulatorische Anforderungen. ✓

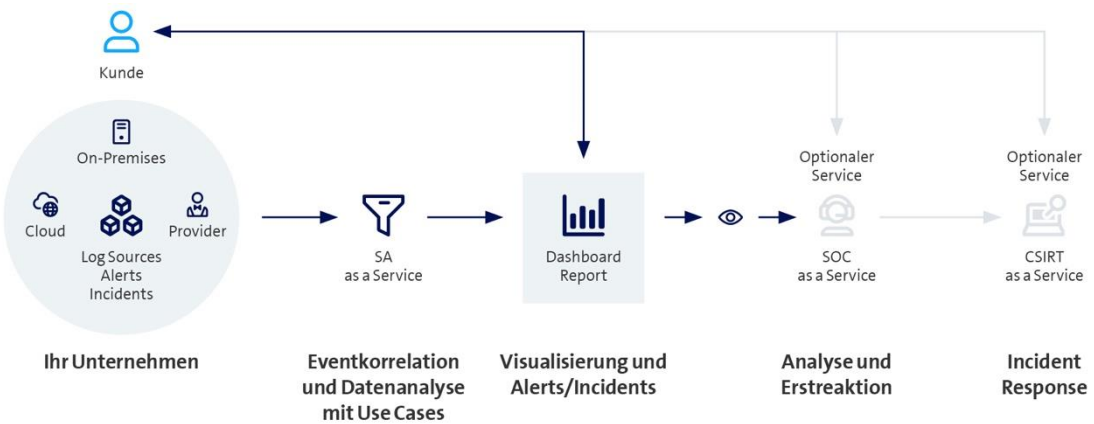
Skalierbarkeit und Flexibilität

Skalierbarkeit und Anpassungsfähigkeit für die wachsende Systemlandschaft. ✓

Basis-Servicefunktionen

Basis-Servicefunktionen der SOC-Plattform: Incident Management, Change Management, Service Request Management, SLA Reporting. ✓

So funktioniert SAaaS



swisscom

Facts & Figures

Basisleistungen

Security Analytics as a Service wird für die Sammlung, Aggregierung und Korrelation von Logdaten aus verschiedenen Datenquellen eingesetzt, um potenzielle Security Incidents schnell zu erkennen und darauf zu reagieren. Regulatorische Anforderungen werden über Compliance und Security Reporting adressiert.
Die flexible Security-Analytics-Plattform skaliert problemlos mit Ihrer wachsenden Systemlandschaft, um sich an Ihre sich ändernden Bedürfnisse anzupassen.

Optionale Leistungen

- Wir entwickeln Ihre individuellen Use Cases.
- Sie definieren selbst die Data Retention Time.
- Sie wählen die Threat Detection Technologie.

Zusatzservices

- **Security Operation Center as a Service (SOCaaS):**
  Unsere professionellen Security-Spezialist*innen analysieren Sicherheitswarnungen (Security Alerts) und identifizieren und bewerten daraus resultierende Sicherheitsvorfälle (Security Incidents) auf deren Kritikalität und Auswirkungen von möglichen Risiken auf Ihre Organisation. Erstreaktionen im Rahmen von Pre-approved Actions sowie Handlungsempfehlungen erlauben Ihnen eine schnelle Reaktion auf Cyberangriffe. Auf kritische Security Incidents reagieren Sie selbstständig.
- **CSIRT as a Service (CSIRTaaS):**
  Zur Analyse und Bewältigung von Sicherheitsvorfällen ziehen Sie Fachleute von Swisscom bei. Wir leiten den Security-Incident-Management-Prozess remote oder bei Ihnen vor Ort und unterstützen Sie bei der Beweissicherung sowie der Kommunikation mit Kunden und Partnern.
- **Network Detection and Response as a Service (NDRaaS):**
  Wird als Erweiterung zu den statischen Erkennungsmöglichkeiten von SAaaS durch eine dynamische Threat Detection basierend auf Machine-Learning-Modellen unterstützt. Der Mehrwert ergibt sich in den Bereichen Web (Proxy) und Netzwerk (DNS, Netflow und Firewall-Traffic-Daten), was maximale Visibilität erlaubt.
- **Digital Risk Protection as a Service (DRPaaS):**
  Sie werden proaktiv informiert über das Vorkommen von sensiblen Geschäfts- und persönlichen Informationen Ihres Unternehmens in öffentlichen und geschlossenen Netzen (z.B. Darknet). Unsere Handlungsempfehlungen für potenzielle Sicherheitsvorfälle setzen Sie selbstständig um.
- **XDR as a Service (by Palo Alto Networks):**
  Lizenz-Management, Lifecycle und Health Management der XDR-Agenten, Konfiguration der Security Policies, Kommunikation von neuen Funktionen und Änderungen und ein jährliches Security Policy Assessment sind in der Verantwortung von Swisscom.
- **Microsoft XDR as a Service:**
  Lifecycle Management der XDR-Agenten, Health Management der Service-Komponenten, Konfiguration der Security Policies, Kommunikation von neuen Funktionen und Änderungen und ein jährliches Security Policy Assessment sind in der Verantwortung von Swisscom.

Mehr Informationen und den Kontakt zu unseren Experten finden Sie auf swisscom.ch/soc

Swisscom (Schweiz) AG Enterprise Customers, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise