

Threat Detection & Response

Umfassender Unternehmensschutz dank Früherkennung und professionellem Agieren bei Cyber Security Attacks

Heute sind gigantische Mengen an Unternehmens- und Personeninformationen auf unterschiedlichen Datenquellen (Netzwerke, Applikationen, Endgeräte, Social Media, Cloud, Darknet uvm.) verfügbar. Mit der stetig wachsenden Vernetzung und Digitalisierung wächst die Vielschichtigkeit der Bedrohungen. Eine frühzeitige Erkennung von sicherheitsrelevanten Vorfällen ist deshalb essentiell.

Professionelles Threat Detection & Response erfordert spezifische Prozesse, Tools, langjährige Erfahrung sowie hochspezialisierte Mitarbeitende. Als einzelnes Unternehmen ist es kaum mehr möglich, die sich ständig ändernden Cyber Security Attacks zu verstehen und entsprechend zu reagieren. Ein erfahrener Partner bietet Unterstützung.

Swisscom schützt die Netzinfrastruktur, Kunden- und Produktdaten sowie sich selbst seit Jahren erfolgreich gegen Cyber Bedrohungen. Diese Erfahrungen nutzt sie, um gemeinsam mit Kunden Cyber-Risiken zu minimieren. Eine gute Visualisierung der Daten unterstützt die frühzeitige Erkennung von potentiellen

Sicherheitsvorfällen. Die zeitnahe Analyse und die richtige Reaktion bei einem Security Incident verbessert das Sicherheitsniveau und die Ressourcenaufwendungen im Unternehmen.

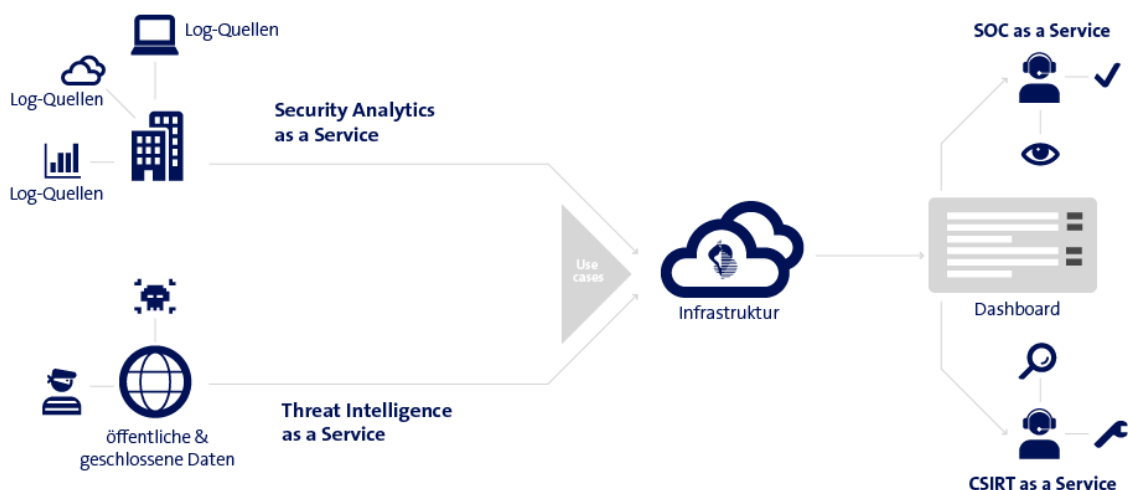
Mit Threat Detection & Response können Sie zwischen vier Service-Ausprägungen wählen, je nachdem wie weit Swisscom Sie bezüglich Cyber Security unterstützen soll.

Ihre Nutzen

Mit Threat Detection & Response

- > sind Sie in Echtzeit über die Bedrohungslage und potentielle Sicherheitsvorfälle informiert (bezogen auf Ihr Unternehmen)
- > werden potentiellen Gefährdungen rund um die Uhr analysiert
- > nutzen Sie etablierte Tools und Prozesse
- > müssen Sie sich weder um Entwicklung noch Betrieb einer Security Analytics Infrastruktur kümmern
- > profitieren Sie vom Swisscom CSIRT und unserem Security Partner Öko-System

Die Lösung auf einen Blick



Facts & Figures

Threat Detection & Response – Service-Ausprägungen

Security Analytics as a Service

Sie erhalten einen Überblick via Dashboard über potentielle Sicherheitsvorfälle aus definierten Log-Daten Ihrer Unternehmung. Analyse und Reaktion auf Sicherheitsvorfälle übernehmen Sie selber.

Warum Security Analytics as a Service von Swisscom:

Wir sind Spezialisten auf dem Thema Security und Big Data und stellen unsere bewährte Security Analytics Infrastruktur zur Verfügung. Zusätzlich profitieren Sie von einem auf die Schweiz optimierten Threat Intelligence Feeds, welcher in dieser Form nirgendwo sonst bezogen werden kann.

SOC as a Service

Sie erhalten via Dashboard einen Überblick über potentielle und bestätigte Sicherheitsvorfälle aus definierten Log-Daten Ihrer Unternehmung sowie Analysen mit konkreten Handlungsempfehlungen. Auf kritische Security Incidents reagieren Sie selbständig.

Warum SOC as a Service von Swisscom:

Seit mehr als 10 Jahren erbringen wir SOC Dienstleistungen für Schweizer Unternehmen im In- und Ausland. Unsere SOC Analysten wissen worauf es ankommt und können Security Events & Incidents kompetent interpretieren.

CSIRT as a Service

Sie definieren kritische Sicherheitsvorfälle eigenständig oder beziehen SOC as a Service. Zur Analyse und Bewältigung ziehen Sie Experten von Swisscom bei. Wir leiten den Security Incident Management Prozess Remote oder bei Ihnen vor Ort, unterstützen Sie bei der Beweissicherung sowie der Kommunikation zu Kunden und Partnern.

Warum CSIRT as a Service von Swisscom:

Das Swisscom CSIRT (Computer Security Incident Response Team) mit etablierten Tools, Prozessen und erfahrenen Incident Response Experten nimmt seit Jahren eine führende Rolle im Bereich CSIRT ein und Sie als Kunde können von dieser Expertise profitieren.

Threat Intelligence as a Service

Sie werden proaktiv informiert über das Vorkommen von sensitiven Business- und Personeninformationen Ihrer Unternehmung in öffentlichen und geschlossenen Netzen (z.B. Darknet). Unsere Handlungsempfehlungen für bestätigte Sicherheitsvorfälle setzen Sie selbständig um.

Warum Threat Intelligence as a Service:

Als Swisscom und Betreiberin von relevanten ICT-Infrastrukturen haben wir eine umfassende und einzigartige Sicht auf reelle Cyber Gefahren in der Schweiz und wissen wie auf diese zu reagieren ist.

Facts & Figures

Leistungsumfang

	SA as a Service	SOC as a Service	CSIRT as a Service	TI as a Service
Support Zeiten				
5 x 8	●			●
7 x 24		●	●	
Infrastruktur SLA				
99,9 %	●	●		●
Leistungen				
Release Management	●	●		●
Detection	●	●		●
Response			●	
Big Data Infrastruktur	●	●		●
Log- und Data-Collection	●	●		●
Vordefinierte Use Cases	●	●		●
Log- und Data-Analytics	●	●		●
Threat Intelligence Feeds	●	●		●
Security Event Notification	●			
Security Event Management		●		●
Security Incident Notification		●		●
Security Incident Management			●	
Swisscom CSIRT			●	
Incident Response Forensic			●	
Dashboard	●	●		●
Echtzeit-Reporting	●	●		●

● im Preis inbegriffen

Mit Swisscom in die digitale Zukunft

Visionäre Unternehmen nutzen die Möglichkeiten der Digitalisierung, um die Zukunft neu zu erfinden. Auch Swisscom erschliesst mit zahlreichen Innovationen neue Geschäftsfelder.

Deshalb sehen wir es als unsere Aufgabe, Sie zu unterstützen, die Chancen der Digitalisierung zu nutzen. Für Sie vernetzen wir die beste Netzinfrastruktur mit sicherer Datenhaltung, zuverlässiger Projektleitung, erfolgreicher Implementierung und zahlreichen innovativen Lösungen.

Willkommen im Land der Möglichkeiten.

Mehr Informationen und den Kontakt zu unseren Experten finden Sie auf [swisscom.ch/detection](https://www.swisscom.ch/detection)