# Managed Cyber Defense

Firmennetzwerke umfassend absichern

## Klassische IT Security reicht nicht mehr aus

Das Vorgehen von Hackern wird immer raffinierter. Gezielte, individuell auf das Opfer zugeschnittene Cyber-Attacken („Advanced Persistent Threats“)sind für traditionelle IT-Sicherheit kaum erkennbar. Die Schäden sind immens: Eine Studie von Ponemon und IBM zeigt für 2018, dass eine gestohlene bzw. kopierte Datei die Geschädigten im Durchschnitt 130 € gekostet hat. Ein einziger Sicherheitsvorfall hat den betroffenen Unternehmen durchschnittlich 3,4 Mio. € an Schäden verursacht! Unternehmen brauchen daher dringend neue Sicherheitslösungen, die gezielte Attacken frühzeitig registrieren und abblocken können. Das ist jedoch nicht immer möglich. Hat ein Angriff Erfolg, müssen Unternehmen auch in der Lage sein, die Vorgehensweise der Hacker aufzudecken und möglichst schnell gezielte Gegenmaßnahmen einzuleiten.

## Doch Unternehmen können sich schützen

Präventive Maßnahmen allein bieten keinen ausreichenden Schutz mehr: Sicherheitsbedrohungen ändern sich heute permanent und wirken über multiple Angriffsvektoren. Davon ausgehend, dass Cyber Angriffe nicht vollständig verhindert werden können, rückt die Erkennung von Bedrohungen und Sicherheitsvorfällen in den Fokus. Entsprechende Erkenntnisse müssen in einer zentralen Instanz, dem Security Operation Center (SOC) zusammengeführt werden. Dort werden Zusammenhänge erkannt und von Sicherheitsexperten Empfehlungen zu geeigneten Gegenmaßnahmen erstellt und dem Kunden übermittelt.

Moderne Abwehrmethoden wie Managed Cyber Defense von T-Systems schützen Unternehmen auf aktuellstem Wissenstand: Das Verhalten von Netzwerk und IT-Systemen wird kontextbezogen und in Echtzeit überwacht. So können Angriffe sehr schnell erkannt und Gegenmaßnahmen ergriffen werden, bevor Schaden entsteht: Zum Beispiel durch die Sammlung und Analyse von Log- und Netzwerk daten durch ein„SecurityIncident and Event Management“-System (SIEM). Hier werden Informationen aus einer Vielzahl von Security-, Netzwerk-und IT-Systemen zusammengetragen und automatisiert in Echtzeit analysiert. Festgelegte Regeln, die genau auf die Situation und den Schutzbedarf des jeweiligen Unternehmens zugeschnitten sind, lösen Alarme aus, sobald etwas nicht stimmt. Ein vordefinierter Prozess leitet den Alarm an Experten, um die Situation zu beurteilen und, wenn nötig, Gegenmaßnahmen einzuleiten.

## Unser Angebot

Wir bieten: von der Beratung über die Integration bis hin zu Betriebsleistungen alles aus einer Hand! Die Beratungsleistungen konzentrieren sich auf die individuelle Bedrohungsanalyse beim Kunden und die Ausarbeitung einer Cyber-Sicherheitsstrategie, um eine Referenzarchitektur für Cybersicherheit zu entwickeln.

T-Systems Sicherheitsdienste und -lösungen werden global angeboten – entlang der Verbünde aus weltweiten Rechen- und Sicherheitszentren. Im Fokus steht dabei die Implementierung von Sicherheitsabläufen übergreifend über alle Security Bereiche che und Funktionen hinweg. Die Dienstleistungen werden in einem SOC der nächsten Generation erbracht: Kernstück ist das 2017 eröffnete integrierte Cyber Defense & Security Operation Center in Bonn, das mit mehr als 240 Mitarbeitern weltweit und 24/7 Verfügbarkeit aktuell das größte seiner Art in Europa ist. Es ist integriert in einem SOC-Verbund aus mehreren angeschlossenen SOCs in Deutschland sowie SOCs in Ungarn, Österreich, Tschechien, der Slowakei, Polen, Spanien, Griechenland, Südafrika, USA, Mexiko, Brasilien und demnächst auch in Singapur.

Diese Leistungen bietet T-Systems externen Organisationen und Kunden als Managed Cyber Defense Service zum Schutz ihrer eigenen Infrastrukturen an.

T · · Systems ·

Let’s power
higher performance

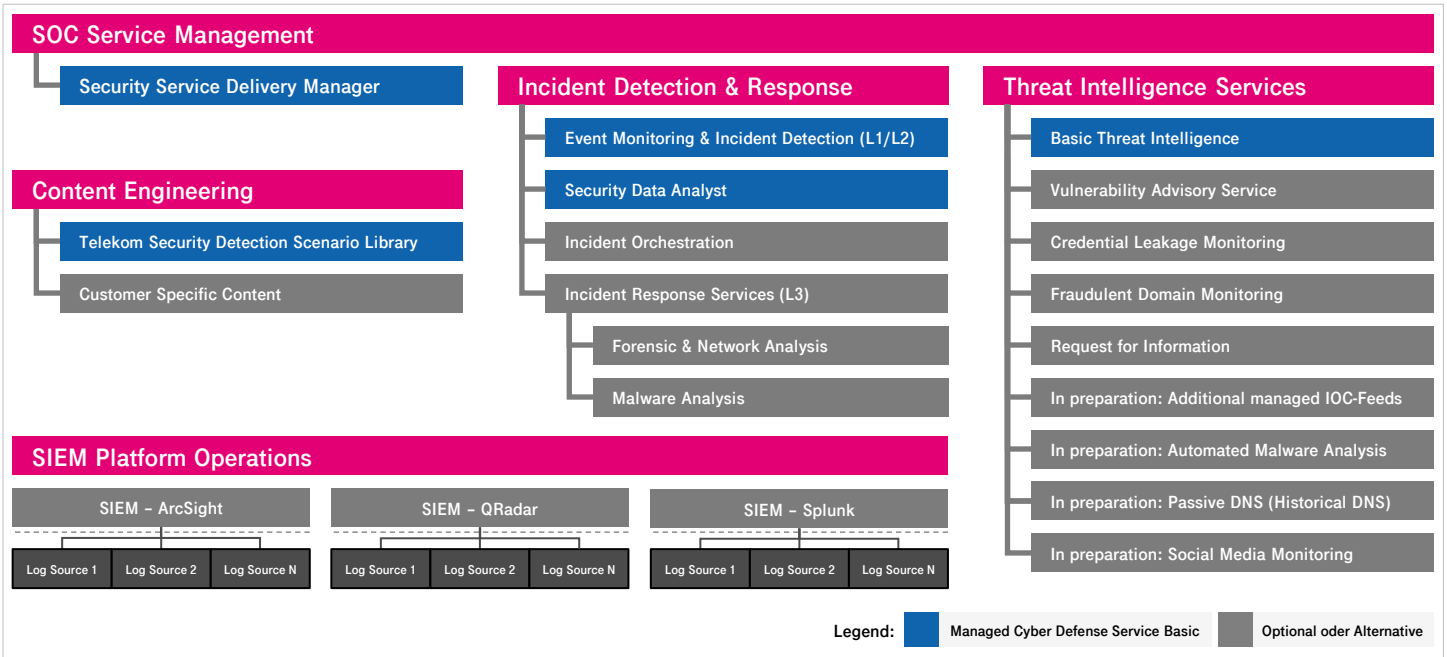
## Flexible Service Module

Um die Kundenanforderungen wirksam und auf hohem Niveau nach aktuellem Stand der Technik umzusetzen, bietet T-Systems einen Managed Cyber Defense Service auf Basis standardisierter Leistungsmodule an. Diese werden individuell gemäß den spezifischen Anforderungen der Kunden zusammengestellt und angepasst.

- Der Service kombiniert automatisierte und manuelle Analysen von sicherheitsrelevanten Logs aus den IT-Netzwerken und Systemen der Kunden.
- Zusätzlich werden tagesaktuelle Threat Intelligence Informationen der T-Systems genutzt, um die Qualität der Analysen zu steigern.
- Der Aufbau des zentralen SIEM-Systems erfolgt an den Standorten der Kunden, alle Log-Daten werden ausschließlich dort gespeichert und verarbeitet.

Die Administration des SIEM-Systems sowie die Analyse von Event-Daten oder Alarmen durch T-Systems erfolgt remote. Die Gesamtlösung ist in hohem Maße jederzeit skalierbar. Auch im Regelbetrieb können bedarfsbezogen

- die SIEM-Lösung z.B. bei steigenden Leistungsanforderungen erweitert,
- Log-Quellsysteme hinzu- oder herausgenommen,
- sowie Services angepasst oder ausgetauscht werden,
- ohne den Betrieb der Lösung zu beeinträchtigen.




**Managed Cyber Defense Flexible Service Module**

## Unsere Mehrwerte (Value Proposition)

T-Systems Managed Cyber Defense Services ermöglichen es,

- Kompromittierungen von Systemen, Diensten, Anwendungen oder Identitäten unmittelbar bzw. zeitnah erkennen und Gegenmaßnahmen einleiten zu können;
- Angriffsversuche sowie ggf. erfolgreiche potenziellen wirtschaftlichen Schaden durch beispielsweise Datenverlust, Beeinträchtigung der Produktivität oder Reputationsbeschädigung abwenden oder minimieren zu können;
- durch qualifizierte Threat Intelligence Informationen (TI Feeds) eine erhebliche Verringerung von False Positive Ereignissen zu erzielen, wodurch der Incident Response Aufwand in der Kundenorganisation deutlich reduziert wird.

**Sinem Sahin**
Phone +49 228 181744498
Sinem-Gueher.Sahin@t-systems.com
www.t-systems.com/security

T · · Systems ·

Let's power higher performance