SIEM und SOC as a Service für den Mittelstand

Die doppelte Verteidigungslinie für effektiven Schutz vor Cyberbedrohungen

T Systems

Let's power higher performance

Bodyguards für Homeoffice und IoT

Laptops, Smartphones, vernetzte Maschinen: Das Zeitalter des Homeoffice und die rasante Verbreitung von IoT-Geräten haben die Art und Weise, wie Unternehmen arbeiten, revolutioniert. Diese Entwicklungen bieten viele Vorteile, doch bringen sie vor allem für den Mittelstand auch neue Herausforderungen in Bezug auf die Cybersicherheit mit sich. Die zunehmende Anzahl dezentraler Arbeitsumgebungen vergrößert die Angriffsfläche für potenzielle Cyberkriminelle, um Schwachstellen in IT-Systemen und ungeschützten Netzwerken ausnutzen zu können. Gleichzeitig werden immer mehr IoT-Geräte in Geschäftsumgebungen integriert, die zum Einfallstor für Angriffe werden können. Und all das vor dem Hintergrund des anhaltenden IT-Fachkräftemangels, der es Unternehmen erschwert, versierte Security-Experten zu finden.

Unsichtbare Schutzschilde: Wie SIEM und SOC Unternehmen sichern

- Früherkennung von Bedrohungen und schnellere Reaktionszeiten
- Schutz sensibler Daten und verbesserte Compliance
- Identifizierung von Sicherheitslücken
- Effektive Ressourcennutzung
- Verbessertes Sicherheitsbewusstsein im Unternehmen
- Bessere Incident-Response-Fähigkeiten

Von Lockvögeln und schädlichen Attachments

Social Engineering, Ransomware-Attacken oder Spyware-Angriffe – es gibt kaum ein mittelständisches Unternehmen, das nicht schon mit einer dieser Varianten Bekanntschaft gemacht hat. Besonders beliebt ist dabei Phishing: Stellen Sie sich vor, ein Mitarbeiter erhält eine E-Mail, die scheinbar von einem vertrauenswürdigen Lieferanten stammt. Die Mail enthält einen Anhang, der angeblich eine wichtige Rechnung enthält. Klickt der Mitarbeiter darauf, wird ein Skript ausgeführt, das eine Verbindung zu Servern krimineller Gruppen aufbaut und beispielsweise Ransomware einschleust. Die Schäden sind kaum abzusehen. Mithilfe von SIEM und SOC können solche potenziell gefährlichen Angriffe frühzeitig erkannt, analysiert und effektiv abgewehrt werden. Das SIEM erkennt verdächtige Aktivitäten und ermöglicht eine Echtzeitüberwachung von Datenverkehr und Ereignissen. SOC-Analysten untersuchen die Bedrohungen, ergreifen sofortige Abwehrmaßnahmen und aktualisieren die Sicherheitsrichtlinien, um das Unternehmen besser zu schützen.

SIEM & SOC in Kürze

So funktioniert's

Das SIEM erfasst und analysiert Daten aus verschiedenen Quellen, um Anomalien und verdächtige Aktivitäten zu erkennen.

Die SOC-Analysten nutzen SIEM-Daten, um Bedrohungen zu identifizieren, zu untersuchen und entsprechende Maßnahmen zur Abwehr zu ergreifen.

Das bringt's

Das SIEM ermöglicht eine zentrale Überwachung von Sicherheitsereignissen, eine schnellere Erkennung von Bedrohungen und eine verbesserte Reaktionszeit.

Das SOC bietet spezialisierte Sicherheitsexperten, die proaktiv Bedrohungen identifizieren, Schadsoftware genau untersuchen und Abwehrmaßnahmen ergreifen können.

Sicherheit im Team: SOC und SIEM

Ein SIEM (Security Information and Event Management) ist eine hochmoderne Technologieplattform, die Ereignis- und Protokolldaten aus verschiedenen Quellen sammelt, analysiert und miteinander in Beziehung setzt. Diese intelligente Korrelation ermöglicht die Erkennung von verdächtigen Aktivitäten und potenziellen Sicherheitsbedrohungen in Echtzeit. Mit umfassenden Funktionen wie dem Einsatz von Machine Learning zur Generierung von Warnmeldungen sowie der Unterstützung bei der Analyse und Priorisierung von Sicherheitsvorfällen ist das SIEM eine effektive Lösung zur frühzeitigen Erkennung und schnellen Reaktion auf Bedrohungen.

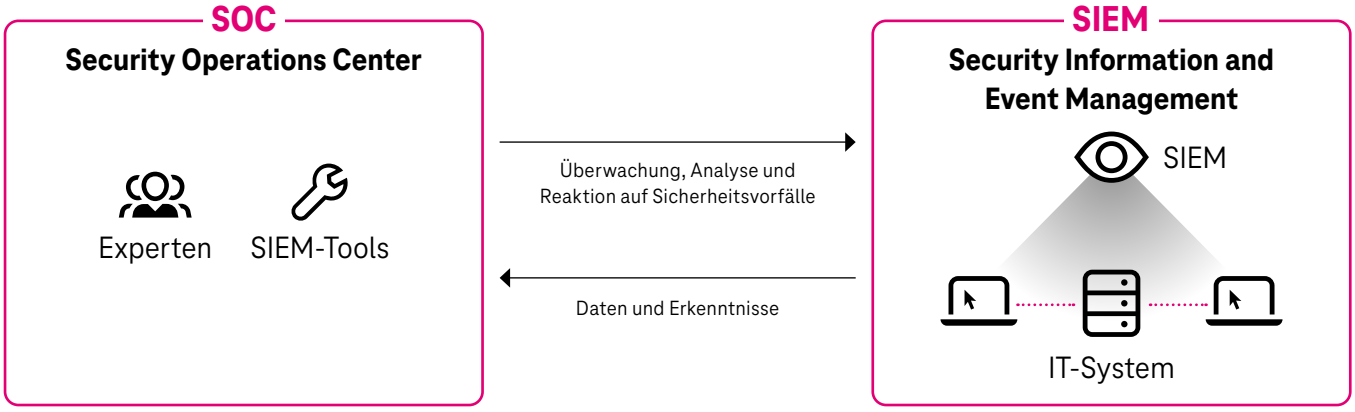
Ein SOC (Security Operations Center) ist eine organisatorische Einheit, die mit SIEM-Tools und erfahrenen Experten arbeitet, um eine kontinuierliche Überwachung, Analyse und Reaktion auf Sicherheitsvorfälle zu gewährleisten. Das SOC nutzt dabei die Daten und Erkenntnisse aus dem SIEM.

Dazu überwachen etwa im SOC der Telekom mehr als 200 Cyberexperten die Systeme der Kunden rund um die Uhr.

Gemeinsam bilden SIEM und SOC ein unschlagbares Duo, das kostengünstig mit abgestimmten Aktionen eine effektive und umfassende Sicherheitsstrategie ermöglicht – für einen starken Schutz vor Cyberbedrohungen.

Sie möchten wissen, ...

- was in Ihrer IT-Landschaft passiert?
- ob es verdächtige Aktivitäten oder Angriffe gibt?
- ob ein Datendiebstahl oder eine illegale Verschlüsselung Ihrer Daten stattfinden?
- wie Sie Ihre Compliance-Anforderungen erfüllen können?
- wie Sie schneller auf Sicherheitsvorfälle reagieren?
- wie Sie effektiv Ihre Sicherheitsstrategie verbessern?



Setzen Sie auf SIEM und SOC für Cybersicherheit ohne Kompromisse

Vertrauen Sie auf unseren modernen SIEM & SOC Service und das Fachwissen unserer Cyber-Security-Experten, die Ihnen jederzeit zur Seite stehen und Sie bei der Abwehr und Bewältigung von Sicherheitsvorfällen unterstützen.

T Systems Let's power higher performance

T-Systems International GmbH
Channel & Midmarket Sales
Hahnstraße 43d
60528 Frankfurt am Main
E-Mail: Midmarket-Sales@t-systems.com
Internet: www.t-systems.com