Datenblatt

SOC-as-a-Service

24/7 Sicherheitsüberwachung und Gefahrenabwehr als Managed Service

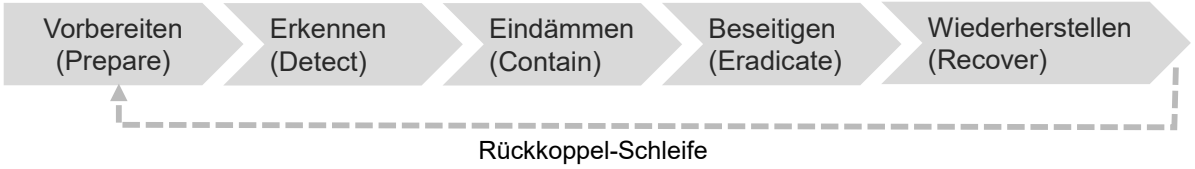
Ihre Vorteile

- **Minimale Angriffsfläche**
  Analyse von Schwachstellen und Beseitigung von Sicherheitslücken
- **Schnelle Reaktion**
  Umfassende Angriffserkennung zum Einleiten von Gegenmaßnahmen
- **Flexibilität und Effizienz**
  Externe Ressourcen anstelle von eigener Sicherheitstechnik und eigenem Personal
- **Schutz rund um die Uhr**
  24/7-Betrieb des SOC an deutschem Standort
- **Umfassende Kompetenz**
  Erfahrene Sicherheitsexperten und bewährte, KI-unterstützte Prozesse
- **Regulatorische Compliance**
  Rechtssichere Einhaltung bestehender und neuer gesetzlicher Anforderungen

Überblick

Die zunehmende Bedrohung durch Cyberangriffe erfordert effiziente Maßnahmen zur frühen Erkennung von Sicherheitsvorfällen und sofortige Gegenmaßnahmen. Diese Aufgaben überfordern oft die Sicherheitsexperten vieler IT-Teams. Ein Security Operations Center (SOC) als Managed Security Service bietet eine kostengünstige Möglichkeit, Unternehmen mit hohem Sicherheitsbedarf vor den negativen Folgen von Cyberangriffen zu schützen.

Wir bieten unseren Kunden eine optimale, auf ihre spezifischen Anforderungen abgestimmte Kombination von SOC-Komponenten. Dabei umfassen unsere Schutzlösungen die Schwachstellen- und Angriffserkennung sowie die Bedrohungsanalyse. Alle Informationen laufen in der zentralen Leitstelle zusammen und werden dort von unseren SOC-Experten ausgewertet. Sie entwickeln Strategien zur wirksamen Gefahrenabwehr und stimmen diese mit den Kunden ab.
Der gemanagte SOC-as-a-Service schützt Unternehmen zuverlässig vor Datenverlusten und Netzwerkstörungen. Schwerwiegende Betriebsstörungen und Imageschäden können abgewendet werden. Zusätzlich werden die regulatorischen Anforderungen von NIS-2 und anderen regulatorischen Vorgaben erfüllt.



SOC-AS-A-SERVICE

Technische Komponenten

Netzwerküberwachung (NDR, Network Detection and Response)

24/7-Netzwerküberwachung: Durch die Auswertung der Meldungen von Netzelementen sowie deren Login-Daten werden Angriffe zuverlässig erkannt. So kann unerwünschter Datenverkehr identifiziert und isoliert werden. Das Einschleusen von Schadsoftware wird sofort unterbunden. NDR erkennt nicht nur veröffentlichte Angriffsvektoren, sondern auch Zero-Day-Angriffe anhand atypischer Verkehrsmuster.

Überwachung der Endpunkte (EDR, Endpoint Detection and Response)

Gefahrenabwehr im Endgerät: Kompromittierte Endgeräte sind oft der Ausgangspunkt für schwerwiegende Angriffe. EDR verhindert das Einschleusen von Schadsoftware und den unerlaubten Datenabfluss. Es überwacht kontinuierlich alle Prozesse und Vorgänge und ermöglicht so eine schnelle Reaktion auf Sicherheitsvorfälle. EDR blockiert auch Verbindungen zu kompromittierten Netzknoten und verhindert die Teilnahme an Botnetzen.

Security Information and Event Management (SIEM)

Sammlung von Sicherheitsinformationen und Abwehrkoordination: SIEM sammelt und korreliert Logdaten und Meldungen von IT-Infrastrukturkomponenten wie Firewalls und Intrusion Detection-/Prevention-Systemen. Anhand dieser Informationen können Anomalien und Sicherheitsvorfälle erkannt werden. Unsere Sicherheitsexperten im SOC empfehlen und veranlassen effektive Abwehrmaßnahmen und erarbeiten Empfehlungen zur Stärkung der IT-Infrastruktur.

Schwachstellen-Management (Vulnerability Assessment System, VAS)

Identifizierung und Behebung von Schwachstellen: Unser Vulnerability Assessment System erfasst Hard- und Software und vergleicht diese mit bekannten Schwachstellen, um die richtigen Maßnahmen zu identifizieren und zu priorisieren. Auch Fehlkonfigurationen und unzureichend geschützte Schnittstellen werden identifiziert. Penetrationstests sichern die Ergebnisse ab. Zusätzlich erhalten unsere Kunden Empfehlungen zur Härtung ihres IT-Systems.

Threat Intelligence Service (TIS)

Reaktion auf die Bedrohungslage: Schutzmaßnahmen müssen kontinuierlich mit aktuellen Bedrohungsinformationen abgeglichen werden. Unser Wissen über Angriffswerkzeuge und aktuelle Angriffsschwerpunkte ermöglicht zielgerichtetes Handeln. Die Analyse basiert auf Informationen von staatlichen Sicherheitsbehörden, IT-Sicherheitsberatungsunternehmen, Sicherheitsforen und öffentlichen Quellen (Open Source Intelligence, OSINT). Konkrete Maßnahmen umfassen Awareness-Schulungen, Passworterneuerungen, Backup-Überprüfungen und Anpassungen von Notfallplänen.