DTS
Security Operations Center (SOC)

Security Operations Center

Cyberangriffe werden vermehrt ausgefeilter, vielschichtiger und finden zu jeder denkbaren Zeit statt. Zu den hochentwickelten Bedrohungen kommen zudem fehlende Visibilität, Alarmmüdigkeit und nicht zuletzt unzureichendes Know-how. Die wichtigste Weiterentwicklung im Bereich der Cyber Security, um den gestiegenen Anforderungen an eine professionelle Cybersicherheit gerecht zu werden, ist das Security Operations Center (SOC).

Ein SOC, bestehend aus hochqualifizierten IT-Security-Experten, überwacht durchgehend IT-Infrastrukturen und Daten. Jedoch kann nicht jedes Unternehmen ein solches Team aufbauen und rund um die Uhr betreiben, da dies teuer und zeitaufwendig ist. Das Stichwort lautet: „SOC Services".

Unser DTS SOC bzw. unsere DTS SOC Services sind die ideale Lösung. Wir ermöglichen Ihnen eine zentrale IT-Sicherheitsleitstelle zum 24/7/365 Schutz Ihrer IT-Umgebung. Das DTS SOC überwacht vollumfänglich Ihre IT-Infrastruktur, sammelt, verarbeitet und analysiert Daten, sucht nach Anomalien bzw. Attacken und steuert mögliche Gegenmaßnahmen. Wir helfen Ihnen auf gleich zwei Ebenen: proaktive sowie präventive Erkennung und Reaktion!

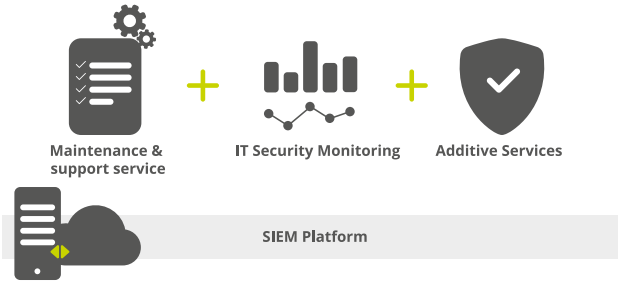
- Hochqualifizierte SOC-Spezialisten, 24/7/365 kontinuierlich im Einsatz
- Zertifizierter Betrieb in Europa
- Fusion aus Technologie & Manpower
- Anomalien schnell erkennen, analysieren & Abwehrempfehlungen erteilen
- Nutzung zentraler DTS SOC Threat Intelligence
- Sichtbarkeit in Ihrer IT-Infrastruktur Compliance-Einhaltung durch Dokumentation von Ereignissen & Maßnahmen
- Schwachstellenanalyse & fortlaufende Optimierung
- Regelmäßiges Reporting – als Grundlage für weiterführende Sicherheitsentscheidungen
- Deutsch- & englischsprachiges Projekt-Team, englischsprachiges Analysten-Team

Jedes Unternehmen und jede IT-Landschaft profitiert von einem SOC. Egal welche Form und welches Ausmaß eine Cyber-Attacke aufweist, wird sie zu spät erkannt, können massive Schäden die Folge sein. Außerdem haben Angreifer stets die Möglichkeit, Zugänge und Daten später erneut zu nutzen, zu beschädigen oder Folgeangriffe zu starten. Umso wichtiger ist eine Kombination aus Cyber Security Know-how, Sichtbarkeit, Diagnose, Analyse und Verteidigung. Außerdem sollten alle Gegebenheiten der individuellen IT-Infrastruktur berücksichtigt werden. Somit spielt auch die technische Kompetenz eine wesentliche Rolle. Die Angriffe können zudem rund um die Uhr erfolgen. Für Unternehmen jeder Größe ist es eine schwierige Herausforderung, den Dauerbetrieb eines SOC zu gewährleisten, um dagegen gewappnet zu sein.

Das hochqualifizierte Team des DTS SOC ist jederzeit im Einsatz. Es verbindet die automatische Erkennung von Angriffen, aktives Monitoring durch Cyber Security Experten, schnelle Detektion möglicher Cyberattacken und die rechtzeitige Einleitung adäquater Maßnahmen. Dabei bietet DTS alle Vorteile eines erstklassigen 24/7/365 SOC, ohne die hohen Kosten, die Komplexität und die Herausforderungen, welche mit dem Aufbau, dem richtigen Personal und dem Betrieb eines eigenen SOC verbunden sind. Wir entlasten Sie maßgeblich, damit Sie sich auf Ihr Kerngeschäft konzentrieren können. Dazu bieten wir Ihnen diese SOC Services: Managed Security Services, aktive Überwachung & Analyse Ihrer IT-Systeme, Erkennen und Entfernen von IT-Schwachstellen, zentrales Sicherheitsmanagement, Alarmierung & Einleiten von Abwehrmaßnahmen, Security-Assessments, Ereignis- und Protokollmanagement, Compliance-Einhaltung, Reporting u.v.m.

Die DTS SOC Services bestehen aus einer Vielzahl von Leistungen sowie Modulen und sind weit mehr als die Summe ihrer Teile. Alle Module werden nach einer ersten Planungs- und Implementierungsphase als monatlicher Service zur Verfügung gestellt. Abhängig von Ihren Anforderungen, bieten wir dabei mehrere Wege der Bereitstellung: zum einen das IT-Security Monitoring (SIEM-basiert), zum anderen über MDR Services (Cortex XDR-basiert).

SOC Services basierend auf LogRhythm SIEM
Die Grundlage der SIEM-basierten SOC Services ist der XDR-Stack von LogRhythm. Potenziell gefährliche Auffälligkeiten werden über diese Technologie zentral identifiziert, dokumentiert und gemeldet. Auf diese Weise erhalten Unternehmen eine ganzheitliche Sicht auf Ihre Sicherheitslage. Zudem tragen SIEM-Lösungen dazu bei, die Einhaltung von gesetzlichen Vorgaben und Compliance-Anforderungen nachzuweisen sowie operative Ereignisse zu überwachen. Aufbauend auf diesem System bieten wir verschiedene Service-Bausteine an, um Ihre Anforderungen bestmöglich abzubilden. Von der Implementierung, der Bereitstellung als Managed SIEM, dem vollwertigen SOC Service bis hin zu additiven Services wie Vulnerability Management bietet DTS den passenden Service, um für Ihr optimale Unterstützung.



Vorteile:

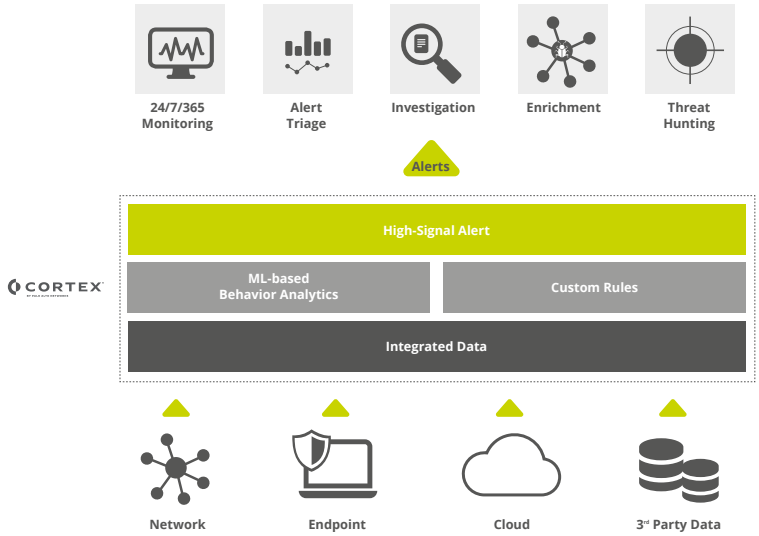
- 24/7/365 Service
- Platform Management On-Premises oder in der Cloud
- Threat & Risk Korrelation & Auswertung Ihrer Logfiles
- Nutzen von DTS Best Practices & kundenspezifischen Use Cases
- Erkennung von Sicherheitsvorfällen durch die zertifizierten DTS SOC Analysten
- Umgehende Informationen zu Incidents über definierte Meldewege, inkl. Berichten & relevanten Informationen, wie Ereignisinformationen, Empfehlungen zur Beseitigung & Eindämmung
- Monatliche Jour Fixes zur Besprechung & Überprüfung des Service
- Repoting, u. a. über Bedrohungen, koordinierten Aktivitäten, IT-Sicherheitsereignissen & Empfehlungen
- Spezifische Reports zu regulatorischen Vorgaben oder Audits
- Quartalsweise Reports zu Analyse der Gesamt-bedrohungslage & Darstellung, inkl. Empfehlung von Gegenmaßnahmen

Use Cases von SOC Services basierend auf LogRhythm SIEM:

- SIEM Platform Management
- IT-Security Monitoring
- Compliance Managment
- Operation Information

MDR Service basierend auf Cortex XDR

Der DTS Managed Detection and Response (MDR) Service erhöht den Reifegrad Ihrer IT-Sicherheit in Bezug auf die Erkennung und Reaktion auf Bedrohungen erheblich. Das Geheimnis ist eine Kombination aus hochqualifiziertem Fachwissen und erstklassiger Technologie zur schnellen Erkennung dynamischer Bedrohungen in Ihrem gesamten IT-Ökosystem. Unser Service bietet eine aktive 24/7/365 Bedrohungsüberwachung und -abwehr durch ausgebildete SOC-Experten, basierend auf der Cortex XDR Plattform von Palo Alto Networks. Wir koppeln automatisierte, auf modernsten Technologien gestützte Erkennung, Analyse und Reaktion mit proaktivem und kontinuierlichem Threat Hunting, Datenforensik sowie Mitigation von Incidents in einem Service.



Vorteile:

- 24/7/365 Managed Detection, Überwachung der Ereignisse & Aktionen der Cortex XDR Plattform
- Proaktive & kontinuierliche Bedrohungssuche
- Automatisierte, auf Technologie basierende Analyse & Reaktion
- Ursachenanalyse, Prozesseingrenzung & -behebung
- Bedrohungserkennung auf Basis der Informationen führender Threat Intelligence Plattformenn
- Digitale, forensische Untersuchungen
- Health-, Status- & Verfügbarkeitssystemmanagement

Use Cases von MDR Service basierend auf Cortex XDR

- Detection & Analyse auf Basis von Endpoint Informationen
- Response auf Incidents über die Cortex XDR Plattform
- Detection & Analyse auf Basis von Endpoint, Netzwerk, Cloud & 3rd Party Informationen mit IT-Security-Fokus

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de

DTS SOC 28032022