

**DTS**  
Managed SIEM

# Managed SIEM

*Noch immer nutzen viele Unternehmen ausschließlich reaktive Mechanismen, um sich vor Cyberangriffen zu schützen. Jedoch können diese konventionellen Maßnahmen den Schaden meistens nur eingrenzen. Die besten Abwehrchancen bestehen im Bereich der Cyber Security bei der frühzeitigen Entdeckung von möglichen Gefahren. Security Information and Event Management (SIEM) ist dabei ein großartiger Präventionsansatz. Die beeindruckende Security Intelligence Plattform von LogRhythm, Leader im Gartner SIEM Magic Quadrant, erkennt Anomalien in Echtzeit, mit der Möglichkeit umgehend Gegenmaßnahmen durchzuführen und folgen-schwere Bedrohungen abzuwenden. Als LogRhythm Services Authorized Partner ermöglichen wir Ihnen diese Lösung in Verbindung mit unserem DTS Security Operations Center (SOC) als ganzheitlichen, proaktiven Cyberschutz in Form einer zentralen Sicherheitsleitstelle*

- Durchgehende Transparenz der IT-Umgebung in Echtzeit
- Mehrdimensionale Identifizierung von Anomalien im Benutzer-, Host- & Netzwerkverhalten
- Unabhängige Überwachung von forensischen Daten & Dateiintegrität
- Hochmoderne Hardwareanalyse & Analyse großer Datasets
- Intelligente Korrelation- & Mustererkennung
- Minimale Erkennungs- & Reaktionszeit
- Skalierbarer Ansatz & Workflow-fähige Automatisierung
- DTS Managed Services

Unser DTS SOC ist eine wesentliche Weiterentwicklung im Bereich Cyber Security, insbesondere in Verbindung mit dem hochmodernen SIEM von LogRhythm. Der Schutz vor modernen Bedrohungsszenarien erfordert eine durchgehende Transparenz der gesamten IT-Umgebung. Im Ernstfall sind Schnelligkeit und Präzision gefragt. In einer vollständig integrierten Plattform kombiniert LogRhythms SIEM das Logmanagement, Überwachung der Dateintegrität und Hardwareanalysen, Monitoring sowie künstliche Intelligenz mit forensischen Host- und Netzwerkdaten. Der globale Überblick über sämtliche Aktivitäten ermöglicht die Erkennung von Anomalien, welche andernfalls unbemerkt bleiben würden, inkl. stark reduzierter Erkennungs- und Reaktionszeit.

Das DTS SOC ist unsere zentrale Sicherheitsleitstelle zur 24/7 Überwachung bzw. Betreuung Ihrer IT-Infrastruktur und Daten. Wir sorgen u. a. mit Hilfe des LogRhythm SIEM durchgängig für Sichtbarkeit, analysieren spezielle IT-Ressourcen sowie Daten nahezu in Echtzeit, erkennen die genannten Anomalien, alarmieren bzw. erteilen Abwehempfehlungen und leiten permanent neue Regeln für eine effektive Abwehr ab. Unsere hochqualifizierten, deutsch- und englischsprachigen Sicherheitsexperten gewährleisten rund um die Uhr: Managed Security Services, aktive Überwachung & Analyse Ihrer IT-Systeme, Erkennen und Entfernen von IT-Schwachstellen, zentrales Sicherheitsmanagement, Alarmierung & Abwehrmaßnahmen, Security-Assessments, Ereignis- und Protokollmanagement, Compliance-Einhaltung und Reporting.