DTS

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

SECURITY INFORMATION & EVENT MANAGEMENT

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 folgenschwere Bedrohungen abzuwenden. Als LogRhythm Services Authorized Partner ermöglichen wir Ihnen diese Lösung und damit einen proaktiven Cyberschutz, vor allem in Verbindung mit unserem DTS Security Operations Center (SOC) als ganzheitliche, zentrale 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 Korrelations- & Mustererkennung
- Minimale Erkennungs- & Reaktionszeit
- Skalierbarer Ansatz & Workflow-fähige Automatisierung
- DTS Managed Services
- DTS SOC Services

Herkömmliche SIEM-Lösungen beinhalten den richtigen, präventiven Ansatz. Allerdings sind sie nicht in der Lage mit den Anforderungen einer modernen Cyber Security mitzuhalten. Sie sammeln und analysieren lediglich Daten von Sicherheitsereignissen, erfordern viel Administration durch fehlende Automatisierung und erschweren die Erweiterung für zusätzliche Anwendungsfälle. Zudem tragen sie wenig zur Selektierung von Warnungen und zur Orchestrierung bei, was Alarmmüdigkeit sowie -unsicherheit fördert.

Der Schutz vor modernen Bedrohungsszenarien erfordert eine durchgehende Transparenz der gesamten IT-Umgebung. Außerdem sind im Ernstfall Schnelligkeit und Präzision gefragt. In einer vollständig integrierten Plattform kombiniert LogRhythms SIEM das Logmanagement, Überwachung der Dateiintegrität 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. Die stark reduzierte Erkennungs- und Reaktionszeit bei Anomalien sowie Bedrohungen unterscheidet sich wesentlich zu gewöhnlichen Lösungen.

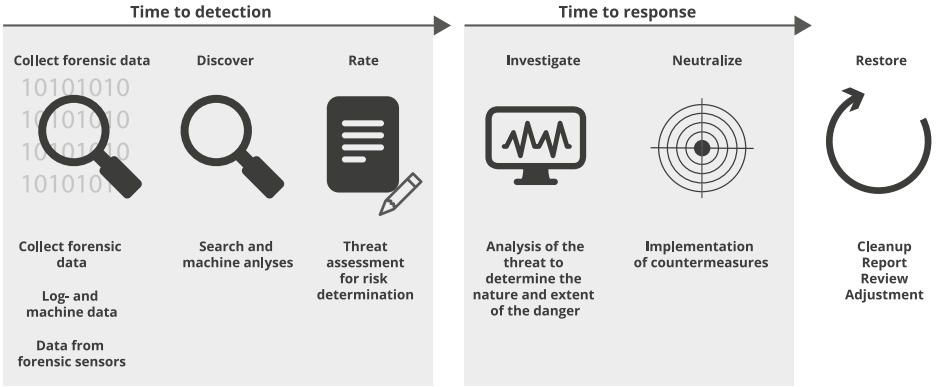
Die Architektur des LogRhythm XDR Stacks bietet eine einheitliche Lösung, die sich flexibel und skalierbar an die individuellen Bedürfnisse der Unternehmensumgebung anpasst. Mit Hilfe der Module Log Management & Analytics, Security Analytics & Security Orchestration, Automation & Response (SOAR), werden Bedrohungen vollständig erkannt bzw. es wird adäquat auf sie reagiert.

LOGRHYTHM ANALYTIX hilft Ihnen bei der Diagnose von Sicherheits- und Betriebsproblemen, indem es eine zentralisierte und umfassende Transparenz Ihres gesamten Datenbestands schafft. AnalytiX optimiert die Erfassung und den Zugriff auf kritische Protokoll- und andere Maschinendaten. Es normalisiert und bereichert Ihre Daten, sodass Suche und Auswertung schnell durchgeführt werden können, unabhängig davon, wie und wo die Daten generiert wurden.

LOGRHYTHM DETECTX liefert anpassbare Sicherheitsanalysen, die bösartige Aktivitäten genau erkennen können und die Bedrohungssuche aktiv unterstützen. Durch Korrelation der Daten erkennt die Sicherheitsanalyse solche Aktionen, um priorisierte, risikobasierte Alarme zu generieren.

LOGRHYTHM RESPONDX vereinfacht die Untersuchung und Abwehr von Bedrohungen, indem so viele Schritte wie möglich im Reaktionsablauf koordiniert und automatisiert werden. Es etabliert einheitliche Prozesse, die unserem DTS Security Operations Center (SOC) Team bei der Organisation, Priorisierung und Zusammenarbeit helfen, um maximale Effizienz und Geschwindigkeit zu erreichen.

Das LogRhythm SIEM bietet einen einzigartigen Threat Lifecylce Management Ansatz. Durch die Integration wesentlicher Funktionen in einer Plattform ermöglicht Ihnen der XDR-Stack nicht nur ein kosteneffizientes SIEM, sondern auch eine umgehende Erkennung von Bedrohungen.



DTS MANAGED SERVICES & SOC SERVICES

DTS ist auf die Konzeptionierung, Implementierung und den Betrieb des LogRhythm SIEM spezialisiert. Wir bündeln diese Technologie für unsere Kunden mit unserem Know-how und unseren Prozessen, um dedizierte SIEMaaS- und SOCaaS-Modelle zu ermöglichen. Auf dieser Grundlage bieten wir Ihnen nicht nur ein erhöhtes Niveau der Cybersicherheit, sondern auch das Sparen von Kosten, Zeit und Personalressourcen.

Unser DTS SOC ist eine wesentliche Weiterentwicklung im Bereich Cyber Security, insbesondere in Verbindung mit dem hochmodernen SIEM von LogRhythm. Es ist eine 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 Abwehrempfehlungen und leiten permanent neue Regeln für eine effektive Abwehr ab. Unsere hoch qualifizierten, erfahrenen, eingespielten, 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.

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de