Mit SIEM in eine technologisch-innovative Zukunft

Die DTS Systeme ist ein innovativer und strategischer Partner in den Bereichen Datacenter, Technologies und Security. Mit 13 Standorten in Deutschland sowie Wien und Athen, über 300 Mitarbeitenden, zwei eigenen DTS Datacentern in Herford und Münster sowie einem Partnerrechenzentrum in Essen greift die DTS auf mehr als 35 Jahre Erfahrung als IT-Dienstleister zurück. Die DTS organisiert kritische Teilbereiche oder auch komplette IT-Infrastrukturen. Charakteristisch ist dabei das ganzheitliche Zusammenspiel aus Beratung, Installation, Betreuung und Betrieb sowie die kundenspezifische Kombination zwischen Vor-Ort-Infrastruktur, Managed Services, hybriden Szenarien, Cloud-Lösungen und IT-Sicherheit.

Das Security Operations Center (SOC) gilt als wesentliche Weiterentwicklung in der IT-Security, insbesondere in Verbindung mit einem modernen Security Information and Event Management (SIEM). Das DTS SOC ist für zahlreiche Unternehmen die zentrale Sicherheitsleitstelle zum 24/7-Schutz ihrer IT-Infrastruktur und Daten vor sämtlichen Bedrohungen.

Cyber-Angriffe werden vermehrt zielgerichteter, ausgefeilter und vielschichtiger. Sie finden sowohl am Tag als auch bei Nacht statt. Um dieser Herausforderung gerecht zu werden, überwacht das SOC vollumfänglich IT-Infrastrukturen, sammelt und verarbeitet Daten, sucht nach Anomalien und steuert mögliche Gegenmaßnahmen. Durch die permanente Datenanalyse wird durchgehend nach Angriffen gesucht, die wiederum ein sofortiges Alarmieren und Einleiten von Schutzmaßnahmen zur Folge haben. Das DTS SOC hilft somit auf zwei Ebenen gleichzeitig – proaktive und präventive Suche nach Schwachstellen sowie durchgehende Reaktionsbereitschaft bei tatsächlichen Angriffen.

Da die Angriffe rund um die Uhr erfolgen können, gestaltet sich für Unternehmen jeder Größe der Dauerbetrieb eines eigenen SOC als äußerst schwierig. Das hochqualifizierte, deutsch- und englischsprachige Expertenteam des DTS SOC ist kontinuierlich im Einsatz, 24/7 an 365 Tagen. Dabei gewährleistet DTS Systeme technisches Know-how und den sichergestellten Schutz von IT-Umgebungen mit Services rund um Managed Security, aktive Überwachung und Analyse der IT-Systeme, Erkennen und Entfernen von IT-Schwachstellen, zentrales Sicherheitsmanagement, Alarmierung und Einleiten von Abwehrmaßnahmen, Security-Assessments, Ereignis- und Protokollmanagement, Compliance-Einhaltung und Reporting.

DTS Systeme

Organisation
DTS Systeme GmbH

Industrie
IT-Dienstleistungen und Services in den Bereichen Datacenter, Technologies sowie IT-Security

Mitarbeitende
Über 300

Neue Herausforderungen

In Zeiten von Vernetzung, künstlicher Intelligenz und Big Data war DTS Systeme auf der Suche nach einem innovativen, technologisch führenden, zukunftsweisenden Anbieter, der nicht nur für die eigene Umgebung, sondern auch für das DTS SOC geeignet ist und des Weiteren in das eigene integrierte Portfolio passt sowie dieses ergänzt. In diesem Zusammenhang sind vor allem ausschlaggebend:

- Modularität: für eine verbesserte Skalierbarkeit
- Technologie: zur Korrelation von gesammelten Daten für eine Alarmierung in Echtzeit
- Granularität: der einzelnen Managementwerkzeuge für eine einfache Aufgabenzuweisung
- APIs: für die Einbindung von Infrastrukturen anderer Hersteller (z.B. im SOAR-Umfeld)
- Systemarchitektur: Berücksichtigung der Relevanz von Automation bis Reaktion ab der ersten Sekunde

Zu den besetzenden Einsatzbereichen gehören darüber hinaus die Abdeckung des Datacenters und die Bildung einer Basis für die kundenspezifischen dedizierten 24/7 SOC-Services. Unterstützt werden dabei insbesondere die Compliance-Standards ISO 27001, PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, BASEL II und SOX. Im Vordergrund standen neben dem Wunsch nach optimalem Schutz für die firmeneigene IT-Infrastruktur und kritische Informationen, die Sicherstellung eines konkreten Compliance-Managements für Kunden und deren Auditoren.

Die Lösung

Neben einer Auswahl aus fünf Top-Anbietern aus dem Gartner-Quadranten entschied sich DTS Systeme für LogRhythm aufgrund einer Menge an Out-of-the-box-Informationen: PARSER, Use Cases und Reports, fortschrittliche Technologien, auf die zurückgegriffen werden kann und woraus eine schnelle Implementierung und somit sehr schnelle Informationen für die Kunden resultieren. LogRhythm wurde in das ganzheitliche Security-Portfolio der DTS Systeme integriert. Die modular erweiterbare Plattform führt zur Investitionssicherung für DTS Systeme sowie für die unternehmenseigenen SOC-Kunden. Hierdurch ist DTS in der Lage, sowohl für sich selbst als auch für seine Kunden, ein richtlinienbasiertes Compliance-Management zu betreiben.

Erfolgreiche Einführung

Die Einführung ermöglichte, aufgrund einer vereinfachten forensischen Analyse, eine simple und effiziente Erkennung von Security-Events über die komplette Benutzeroberfläche hinweg sowie eine schnellere Reaktion auf Security-Vorfälle für DTS SOC-Kunden. Durch die Integration in das Portfolio ergab sich eine wesentlich erhöhte Qualität der Informationen, die DTS Systeme den Kunden seitdem bereitstellen konnte. Ein enorm reduzierter Administrationsaufwand bietet DTS die Möglichkeit die SOC-Plattform weiterzuentwickeln, den Service zu verbessern und somit die Kunden zufriedenzustellen.

> **“LogRhythm hat uns beim Einstieg in den SOC-Markt befähigt, uns auf die Ausbildung unserer Analysten sowie die Definition sinnhafter Prozesse für unsere Kunden zu konzentrieren, anstatt uns mit der Stabilität und Flexibilität der notwendigen Basis-Infrastruktur zu beschäftigen.”**
>
> - Axel Westerhold, Head of Datacenter & SOC Services bei DTS Systeme -