REFERENZ LTS LOHMANN THERAPIE-SYSTEME AG

24x7 Cyber Security für die Pharma-Produktion

↳ SOC as a Service von SVA schützt geistiges Eigentum und sichert Compliance bei der LTS Lohmann Therapie-Systeme AG

AUF EINEN BLICK

Aufgabe
24x7-Überwachung der IT-Infrastruktur zur frühzeitigen Erkennung von Cyberangriffen und zur Erfüllung regulatorischer und versicherungstechnischer Anforderungen

Systeme und Software
– SOC by SVA Security Intelligence Platform, Modul mit Splunk Enterprise Security
– SOC by SVA Monitoring
– SUSE Linux Betriebssystem
...

LTS LOHMANN THERAPIE-SYSTEME AG

Die LTS AG mit Hauptsitz in Andernach ist ein international führender Spezialist für die Entwicklung und Produktion von alternativen Darreichungsformen für Arzneimittel. Als Lohnfertiger im Bereich Pharma und Biotechnologie arbeitet das Unternehmen mit globalen Firmen zusammen. Höchste Anforderungen an Qualität, Regulierung und den Schutz von geistigem Eigentum prägen daher die IT- und Sicherheitsstrategie des Unternehmens.

HERAUSFORDERUNG

In der stark regulierten Pharma- und Biotechnologiebranche sind IT-Sicherheit und Compliance zentrale Voraussetzungen für den Geschäftsbetrieb. Bei LTS bestand bereits ein hoher Reifegrad in der Cyber-Sicherheit, dennoch sollte das bestehende Sicherheitsniveau weiter ausgebaut werden. Insbesondere der Schutz von geistigem Eigentum sowie die Anforderungen aus Kunden- und Lieferanten-Audits – teilweise orientiert an regulatorischen Rahmenwerken wie KRITIS oder NIS2 – machten eine weitergehende Überwachung der IT-Infrastruktur notwendig.

Zusätzlich stellte auch die Cyber-Risk-Versicherung konkrete Anforderungen an ein Security Operations Center (SOC), um den Versicherungsschutz langfristig aufrechtzuerhalten. Zwar existierten bereits verschiedene Sicherheitsmaßnahmen wie

...

Vorteile
– kontinuierliche 24x7-Überwachung und schnelle Reaktion auf Sicherheitsvorfälle
– höherer Cyber-Security-Reifegrad und Erfüllung regulatorischer Anforderungen
– Schutz von geistigem Eigentum und sensiblen Produktionsdaten
– Entlastung der internen IT durch Managed SOC-Service
– Log-Daten verbleiben vollständig im Kundennetzwerk
– direkte Kommunikation mit Security-Experten aus Deutschland

Perimeter-Schutz und Netzwerksicherheitslösungen, jedoch fehlte eine zentrale Plattform, die sicherheitsrelevante Ereignisse korrelieren und im Zusammenhang auswerten konnte. Auch eine durchgängige 24x7-Überwachung war intern nicht realisierbar, da ein eigener Drei-Schicht-Betrieb wirtschaftlich unverhältnismäßig gewesen wäre.

Gleichzeitig existierte bislang kein SIEM-System, sodass sicherheitsrelevante Log-Daten nicht zentral analysiert werden konnten. Ziel war es daher, verdächtige Aktivitäten und potenzielle Angriffe frühzeitig zu erkennen, automatisiert zu bewerten und im Ernstfall schnell reagieren zu können – ohne die bestehende IT-Organisation personell weiter zu belasten.

LÖSUNG

Gemeinsam mit den Experten von SVA entschied sich LTS für **SOC as a Service** – ein vollständig gemanagter Security Operations Service mit durchgängiger Überwachung der IT-Infrastruktur. Nach einem initialen SOC-Readiness-Workshop wurden die bestehende IT-Landschaft, Sicherheitsmaßnahmen und Anforderungen analysiert und in ein maßgeschneidertes Servicekonzept überführt.

Im Rahmen der Implementierung wurde eine **SOC by SVA Security Intelligence Platform** als dedizierte Appliance im Netzwerk von LTS installiert. Diese Plattform basiert auf **Splunk Enterprise Security (ES)**, eine der führenden SIEM- und Security-Analytics-Lösungen. Sie sammelt und korreliert sicherheitsrelevante Ereignisse aus unterschiedlichen Quellen, erkennt bekannte Angriffsmuster und identifiziert auch bislang unbekannte Anomalien.

Ergänzt wird die Plattform durch das Modul **SOC by SVA Monitoring**, bei dem ein erfahrenes Team von Security-Spezialisten im SVA Security Operations Center die Ereignisse rund um die Uhr analysiert. Die automatisierte Anreicherung mit Threat-Intelligence-Daten sowie die manuelle Bewertung durch Experten ermöglichen eine präzise Einschätzung potenzieller Sicherheitsvorfälle. Bei kritischen Ereignissen erfolgt eine sofortige Alarmierung des Kunden, inklusive Handlungsempfehlungen oder der Einleitung vordefinierter Reaktionsmaßnahmen.

Ein besonderer Vorteil der Lösung liegt darin, dass die Log-Daten vollständig im Netzwerk des Kunden verbleiben und die SOC-Leistungen ausschließlich aus Deutschland erbracht werden – ein wichtiger Aspekt im Hinblick auf Datenschutz und regulatorischen Anforderungen. Gleichzeitig profitieren die Verantwortlichen bei LTS von festen Ansprechpartnern und dem Zugriff auf die umfangreiche Technologie- und Security-Expertise von SVA.

Die neue Lösung ermöglicht eine kontinuierliche Weiterentwicklung der Sicherheitsarchitektur. Gleichzeitig wurde mit dem SIEM-System eine Plattform geschaffen, die künftig auch für weitere Analysezwecke – etwa im Bereich IT-Performance oder OT-Analyse – genutzt werden kann.

FAZIT

Mit der Einführung des **SOC as a Service** konnte LTS den Reifegrad seiner Cyber Security signifikant steigern und gleichzeitig regulatorische Anforderungen erfüllen. Die kontinuierliche 24x7-Überwachung sorgt für dafür, dass sicherheitsrelevante

> Das SOC by SVA liefert genau die richtigen Informationen zur richtigen Zeit. Wir erhalten relevante Sicherheitsmeldungen, können Vorfälle schnell bewerten und stehen im engen Austausch mit den Experten von SVA.

Johann Haag,
Head of IT Security, LTS Lohmann Therapie-Systeme AG

Ereignisse frühzeitig erkannt und bewertet werden können – ein entscheidender Faktor, wenn potenzielle Ausfälle in der Produktion schnell Schäden in Millionenhöhe verursachen könnten.

Auch organisatorisch bringt die Lösung klare Vorteile: Das interne IT-Team wird entlastet, während gleichzeitig ein professionelles Security Incident Management aufgebaut wurde. Durch die enge Zusammenarbeit mit den Experten von SVA entstehen zudem kontinuierlich neue Ideen für weiterführende Auswertungen und Anwendungsfälle innerhalb der Sicherheitsplattform.

Besonders geschätzt werden von LTS die direkte Kommunikation mit festen Ansprechpartnern sowie die hohe Qualität der Analysen. Sicherheitsmeldungen sind präzise und relevant – ein entscheidender Faktor, um Fehlalarme zu vermeiden und gleichzeitig schnell auf echte Bedrohungen reagieren zu können.

Auch in kritischen Situationen zeigt sich der Mehrwert des SOC: So wurde beispielsweise ein technischer Vorfall im Rechenzentrum frühzeitig erkannt und gemeldet, noch bevor andere Systeme Alarm schlugen.

Mit Blick auf die Zukunft plant LTS bereits den weiteren Ausbau der Plattform, unter anderem durch zusätzliche SAP- und SOC-Module.

KONTAKT

SVA System Vertrieb
Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel. +49 6122 536-0
mail@sva.de