SUCCESS STORY

VON DER ZUSAMMENARBEIT

sure[secure]
your security operations center

OQEMA

Kurzvorstellung des Partners

Die OQEMA Deutschland, bis 2017 Overlack, ist einer der führenden Chemiedistributoren in Deutschland. Knapp über 1.600 Mitarbeiter sind derzeit an 50 Standorten in 25 Ländern für die OQEMA Gruppe tätig. An der Schnittstelle zwischen Chemikalienherstellern und der chemieverarbeitenden Industrie erbringt OQEMA Dienstleistungen entlang der Lieferketten. Von der Beschaffung über die Produktentwicklung und individuelle Abmischung bis hin zu Logistik und Recycling.

OQEMA

OQEMA AG

Branche:	Chemiedistribution
Mitarbeitende:	1.600
Gründung:	1922
Umsatz:	1,7 Mrd. EUR

Diese Themen sind Bestandteil der Success Story

- IT-Sicherheit im Zusammenhang mit Mergers & Acquisition
- Security Operations Center as a Service

Welche Herausforderungen hatte der Partner?

Die Unternehmensgruppe wächst kontinuierlich. Dieses Wachstum erfolgt organisch als auch durch Mergers & Acquisition Aktivitäten. Deshalb müssen parallel zum organischen Wachstum neue IT-Infrastrukturen an den Kern der OQEMA IT angebunden werden. Diese Integration fremder Infrastrukturen birgt das Risiko einer möglichen Infektion für das gesamte IT-Netzwerk der Unternehmensgruppe. Es muss also sichergestellt werden, dass die essenziellen Geschäftsprozesse bestmöglich geschützt werden.

Darüber hinaus ist OQEMA von der NIS2-Richtlinie betroffen und muss daher nachweisen Cyberangriffe 24x7 zu detektieren und angemessen darauf zu reagieren. Deshalb hat das Unternehmen Lösungen evaluiert, die diese Herausforderungen deckeln können.

In dieser Gemengelage gilt es zu Beginn zu evaluieren, ob eine Umsetzung mit internen Kräften realistisch scheint. Dabei gilt es auch zu berücksichtigen, dass bei der Wahl der Technologie, bedingt durch das schnelle und internationale Wachstum, auch die Skalierbarkeit eine große Rolle spielt. Dies gilt für die identifizierten Haupttechnologien SIEM und SOAR. Diese Umsetzung sollte möglichst mit einer planbaren Kostenstruktur einhergehen.

> Für uns im Cyber Defense Center sind diese komplexen und dynamischen Strukturen sehr anspruchsvoll, aber auch total spannend.
>
> Durch die starke Dynamik entwickeln wir gemeinsam mit dem Partner kontinuierlich neue Playbooks und Detection Rules.

Philip Schildein
Head of Cyber Defense Center
suresecure GmbH

Wie haben wir die Herausforderung gelöst?

Unser SOC-Service konnte sich am Ende durchsetzen, weil er alle Herausforderungen abdeckt. Unser SOC basiert auf der Google SecOps Plattform, welche als SaaS aus der Cloud zur Verfügung gestellt wird.

Dementsprechend sind neue Infrastrukturen jederzeit binnen kürzester Zeit anbindbar. Auch wenn die neu anzubindenden Systeme noch keine Tiefenüberprüfung erfahren haben, ist es OQEMA dadurch möglich, eventuell kompromittierte Systeme frühzeitig zu erkennen und weitere Infektionen vorzeitig zu unterbinden.

Die Kalkulation wird auf Basis der zu schützenden Mitarbeitenden ausgerichtet. Das Log-Volumen und die Anzahl der IT-Assets spielen dabei keine Rolle und bieten den perfekten Rahmen für kostenneutrale Skalierung. Es sind eben genau diese zwei Punkte, die zu Beginn eines SOC-Projektes in der Regel nur schwer zu definieren sind. Mehr Systeme und Log-Volumen führen dann schnell zu einem völlig neuen Preisgefüge, welches dann schon außerhalb des abgestellten Budgets liegen kann.

In der Vergangenheit wurden bei der OQEMA Group bereits diverse Cyberangriffe erkannt und dokumentiert.

Gerade aufgrund der internationalen Bekanntheit, der Branchenzugehörigkeit und des starken Wachstums ist das Unternehmen ein attraktives Target.

Deshalb war ein Schlüsselelement bei der Evaluierung möglicher Dienstleister auch die Kompetenzen im Bereich Incident Response. Im Falle eines Angriffs sollte schnell und richtig reagiert werden, um einen möglichen Schaden abzuwenden. An dieser Stelle konnten wir mit unserem umfassenden Incident Management Framework punkten, welches eben auch Segmente wie Behörden-Management und Krisenkommunikation umfasst.

Die OQEMA Group ist damit gut gerüstet für zukünftige Aktivitäten und kann den Wachstumsbestrebungen weiterhin uneingeschränkt nachgehen.

Thomas Janssen, Group Director IT Operations

Wir sind froh, einen Partner gefunden zu haben, der unsere Herausforderungen kennt, unser Business versteht und von dem wir sowohl SOC-Services als auch umfangreiche Incident Response Dienstleistungen beziehen können. Dadurch erfüllen wir alle Pflichten in Bezug auf Erkennung und Reaktion.

Key Take-Aways:

- Die Absicherung der wichtigen Business-Prozesse sollte Priorität haben. D.h. diese sollten genau identifiziert, beschrieben und abgesichert werden
- Visibilität und Transparenz sind Schlüsselelemente in der Abwehr von Cyberangriffen
- Sicheres Management eines wachsenden IT-Netzwerks durch organische Expansion und Übernahmen sowie die Einhaltung der NIS2-Richtlinie, die eine 24/7-Überwachung von Cyberbedrohungen erfordert, ist komplex
- Implementierung eines skalierbaren, cloudbasierten SOC-Services auf Basis der Google SecOps Plattform sorgt für verbesserte Sicherheit, Einhaltung regulatorischer Vorgaben, flexible Skalierbarkeit und Planungssicherheit bei den Kosten

suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de