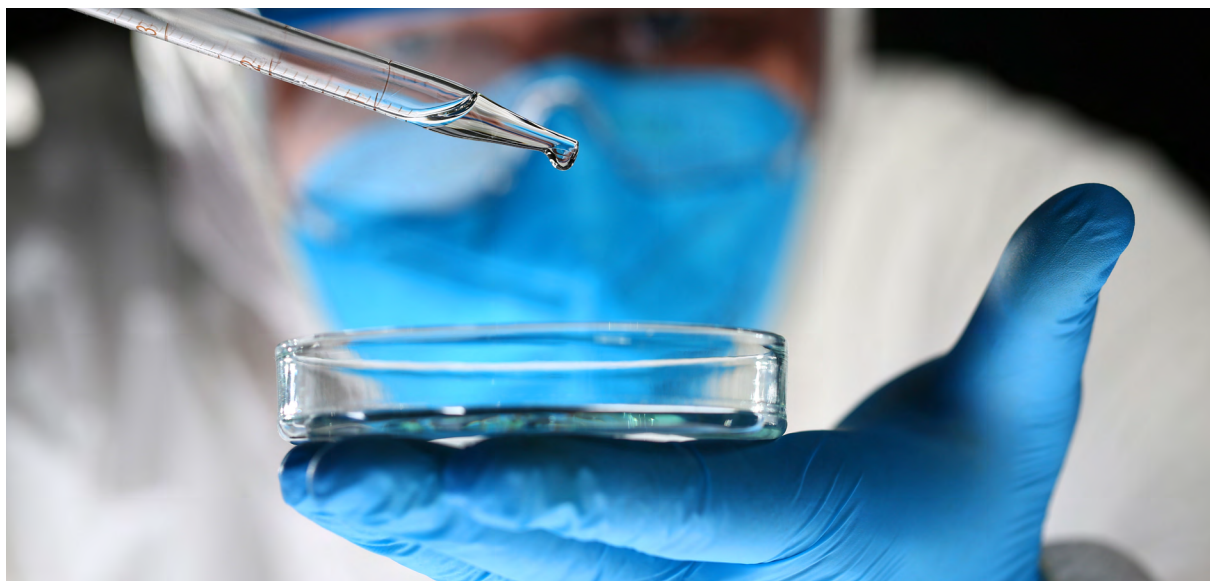


Konvergenz für IT-/OT-Sicherheit mit Lösungen von Trellix

Hersteller von Spezialchemikalien
verleiht Personal, Prozessen und
Technologie neuen Schwung



Hersteller schützt seine IT-Umgebung mit einem einzigen Anbieter

/// Kundenprofil

Fertigungsindustrie

Dieses weltweit tätige Fortune-500-Unternehmen stellt Materialien her, welche die Grundlage für eine Vielzahl von Produkten bilden, die in den meisten wichtigen Industriezweigen und Verbraucheranwendungen eingesetzt werden.

In einer vertikalen Produktionskette, in der Fehler katastrophale Schäden verursachen können, ist es für den Hersteller von großer Bedeutung und eine Verpflichtung, die Sicherheit der Mitarbeiter, der lokalen Gemeinden und der Umwelt zu gewährleisten. Einen sicheren Betrieb bei einer Massenproduktion von Spezialchemikalien aufrechtzuerhalten erfordert eine außerordentlich heterogene globale Infrastruktur, die sich sowohl aus der traditionellen Back-Office-Informationstechnologie (IT) als auch aus der Betriebstechnologie (OT) zusammensetzt.

/// Lösungen und Dienste

Trellix Network Security

Trellix Endpoint Security

Trellix Helix Security
Operations Platform

Trellix Threat Intelligence

Trellix Malware Analysis

Trellix Security Orchestrator

/// Trellix überzeugte von Anfang an durch das großartige Team, das für uns zuständig ist. Ich beschäftige mich seit 25 Jahren mit Cyber-Sicherheit, und die Kundenbetreuer von Trellix sind wohl die besten, mit denen ich je zu tun hatte.

— Chief Information Security Officer, Hersteller von Spezialchemikalien

/// Vorteile

- Die Einführung von Sicherheitslösungen eines einzigen Anbieters sorgt für reibungslosen Schutz in einem hybriden Umfeld
- Einheitliches Monitoring von konsolidiertem IT-/OT-Verkehr mit einem zentralem Dashboard
- Von Trellix erstellte Umgebungsdaten ermöglichen Risikobewertung und Kostenanalyse von Sicherheitsinvestitionen
- Intuitive Lösung beschleunigt die Lernkurve für neue Mitarbeiter und optimiert Ressourcenzuweisungen

Der Hersteller ist nicht nur wegen seiner IT-Bereiche ein attraktives Ziel für Cyber-Angriffe, sondern auch aufgrund dessen, was jenseits der Infrastruktur seiner OT-Umgebung liegt.

Der CISO betont, wie wichtig es ist, Schwachstellen zu beseitigen, die sich aus dem gemeinsamen Weg von IT- und OT-Bereichen ergeben: „Eines unserer größten Probleme im OT-Bereich war der Zugriff durch Dritte.

Wir haben ca. 15 bis 20 Anbieter, die zu einem bestimmten Zeitpunkt an einer Anlage arbeiten, und ihr physischer Zugang zu unserer Infrastruktur, ihre Fähigkeit, Hardware in unsere Systeme einzubinden, und die Möglichkeiten der Verbindung zu unserem Netzwerk, die sie hatten, stellten eine Reihe von Herausforderungen dar, denen eine herkömmliche Sicherheitsstrategie nicht gerecht wurde.“

Ein erstklassiges Paket

Jeder Sicherheitsbeauftragte muss sich entscheiden, ob einzelne Produkte von verschiedenen Anbietern in die Sicherheitslösung aufgenommen werden sollen, oder ob ein integrierter Ansatz verfolgt wird, in dem ein primärer Anbieter von Sicherheitslösungen ausgewählt wird, der Schutz über mehrere Bedrohungsvektoren hinweg bietet. Der CISO entschied sich für Letzteres und bat sein Team, den optimalen Anbieter zu finden.

„Unsere Recherchen führten uns schnell zum Trellix-Portfolio“, erinnert sich der CISO. „Trellix bot nicht nur besonders hochwertige Lösungen, sondern überzeugte von Anfang an durch das großartige Team, das für uns zuständig war. Ich beschäftige mich seit 25 Jahren mit Cyber-Sicherheit, und die Kundenbetreuer von Trellix sind wohl die besten, mit denen ich je zu tun hatte.“



Der Hersteller verwendete eine Kombination aus dem NIST-Rahmenwerk für Cyber-Sicherheit und dem NICE-Rahmenwerk für Cyber-Sicherheitspersonal von NIST, um zu ermitteln, wie die Referenzarchitektur am besten optimiert werden kann. Der CISO erkannte, dass die Weiterentwicklung seines Security Operations Center (SOC) und seiner drei Hauptsäulen – Menschen, Prozesse und Technologie – entscheidende Möglichkeiten zur Verbesserung der Sicherheit des Unternehmens bot. Zudem wurden Trellix Malware Analysis und Trellix Security Orchestrator eingeführt, um die Sicherheitsprozesse noch robuster zu gestalten.

Die Lösungen von Trellix sind in einer nahtlos integrierten Schnittstelle in Trellix Helix aufeinander abgestimmt. Der CISO bemerkt hierzu, „dass die Lösungen von Trellix besonders benutzerfreundlich sind. Wir haben alles von einer zentralen Stelle aus im Blick. Im Übrigen können neue Mitarbeiter sehr schnell eingearbeitet werden, was für unsere jüngeren und erfahreneren Leute von großem Vorteil ist.“

Alles, was gemessen wird, wird verbessert

Die Analyse der Daten, die aus der vereinheitlichten IT-/OT-Umgebung abgerufen werden, hat eine wesentliche Rolle dabei gespielt, dass der Hersteller in der Lage ist, Kennzahlen zu erfassen, die die Effektivität seiner Cyber-Sicherheitsmaßnahmen belegen. „Wir haben speziell für unseren OT-Bereich einen Mechanismus zur Risikobewertung entwickelt, der die jährlichen Einnahmen mit einer Anlage anhand von SOC-Daten bewertet, die von Trellix-Lösungen stammen und die Gefährdung und Anfälligkeit für Bedrohungen detailliert aufzeigen. Die sich daraus ergebende Risikobewertung hilft unserer Geschäftsleitung, die Rendite einzuschätzen, die wir mit den Investitionen in unsere Sicherheitsinfrastruktur erzielen.“

// Wenn ich in Gesprächen mit dem Vorstand über unsere Abwehrstrategie den Namen „Trellix“ erwähne, löst sich die Anspannung im Raum merklich.

– Chief Information Security Officer, Hersteller von Spezialchemikalien

„Wir haben auch Mitarbeiter von Trellix bei uns vor Ort, die in-house beim Aufbau eines Programms zur Kontrolle von Schwachstellen unterstützen. Hierzu fließen die Erkenntnisse aus Threat Intelligence und Schwachstellendaten in die Risikogesamtbewertung mit ein – zusammen mit ausgewählten Kennzahlen wie durchschnittliche Dauer zur Wiederherstellung und Triage“, so der CISO. „Trellix-Daten sind für uns besonders wichtig. Wir folgen der Devise, dass alles, was gemessen wird, verbessert wird, und 95% der von uns verwendeten Daten stammen aus unseren Lösungen von Trellix.“

Trotz der dynamischen IT-/OT-Infrastruktur des Unternehmens trägt Trellix dazu bei, im gesamten Unternehmen zu vermitteln, dass der Hersteller gut aufgestellt ist, um Cyber-Kriminellen immer einen Schritt voraus zu sein. „Wenn ich in Gesprächen mit dem Vorstand über unsere Abwehrstrategie den Namen „Trellix“ erwähne, löst sich die Anspannung im Raum merklich. Das bedeutet für mich alles“, so der CISO.



Cyber-Sicherheit gehört zur DNA des Unternehmens

Das übergreifende Ziel des Unternehmens liegt letztendlich darin, seine Mitarbeiter, seine Auftragnehmer, die Umwelt und die Gemeinden, in denen es tätig ist, vor Schäden zu bewahren und gleichzeitig 100% Qualität und Zuverlässigkeit zu erreichen.

Im Rahmen dessen hat der Hersteller eine Initiative ins Leben gerufen, die den Zusammenhang zwischen geschäftlichem Erfolg und Verantwortung unterstreicht. „Wir integrieren Cyber-Sicherheit in die DNA unserer Organisation und richten uns nach den geschäftlichen Prioritäten, indem wir Schulungen, Kennzahlen und Zuständigkeiten für unseren Cyber-Sicherheitsansatz im gesamten Unternehmen einführen“, so der CISO.



Er fasst zusammen: „Trellix ist ein Partner von unschätzbarem Wert, der uns bei der Verbesserung unserer Sicherheitslage, der Absicherung unserer IT-Bereiche und der Zusammenarbeit bei der Ausweitung des Schutzes auf den OT-Bereich geholfen hat.“

Erfahren Sie mehr über Trellix auf trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com



Über Trellix

Trellix ist ein globales Unternehmen, das die Zukunft der Cybersicherheit neu definiert. Mit der offenen und nativen Plattform Extended Detection and Response (XDR, erweiterte Erkennung und Reaktion) gewinnen Organisationen, die mit den größten Bedrohungen von heute konfrontiert sind, Vertrauen in den Schutz und die Widerstandsfähigkeit ihrer Abläufe. Die Sicherheitsexperten von Trellix beschleunigen zusammen mit einem umfangreichen Netz an Partnern technologische Neuheiten durch maschinelles Lernen und Automatisierung, um über 40.000 Kunden aus Wirtschaft und Behörden zu unterstützen.