SOCWISE

POWERED BY EURO ONE

SOCWISE

IHRE HERAUSFORDERUNG IST UNSERE MISSION

socwise.eu

EINE MDR-STORY MIT "HAPPY END"

SOCWISE Managed Detect and Response Fallstudie bei einem Pharmaunternehmen

DER KUNDE: MULTINATIONALES UNTERNEHMEN, DAS ARZNEIMITTEL HERSTELLT UND VERTREIBT

IM JAHR 2019 kam es zu einer großen Datenpanne, die Produktionsausfälle, Datenverluste und Hunderte von zusätzlichen Arbeitstagen außerhalb der Geschäftszeiten für die IT-Abteilung zur Folge hatte. In Anbetracht der Verluste und des Markenschadens forderte die Geschäftsleitung entsprechende Gegenmaßnahmen. Sie war zutiefst besorgt, dass ein zweiter Angriff erfolgen würde, während man immer noch nicht in der Lage ist zu reagieren. Während des Angriffs machte man die Erfahrung, dass nicht genügend Daten zur Verfügung standen, um die Angriffskette zu untersuchen. Ja, es waren sogar zu wenige Daten vorhanden, um festzustellen, ob die Angreifer weitergemacht hatten. So war es unmöglich, angemessen zu reagieren. Außerdem waren die Sicherheitsspezialisten in ihrem IT-Einsatzteam nicht für Maßnahmen in einem solchen Fall gerüstet. Die internen Prozesse waren darüber hinaus nicht ausreichend, um Abwehrmaßnahmen des Teams zu unterstützen. Nach den mühsamen Neuinstallationen, Wiederherstellungen und Zurücksetzungen behielten sie daher die Kontrolle und werteten die gewonnenen Erkenntnisse aus.

Sich der Herausforderung stellen

Das Unternehmen beschloss, seinen Schutz im Bereich Mitarbeiter, Technologien und Prozesse völlig neu zu gestalten. Auf technischer Seite strebte das Unternehmen eine vollständige Transparenz seiner IT und OT, seines Vor-Ort- und seines Cloud-Netzwerks an. Man wollte die Erkennungs- und Reaktionsfähigkeit ausbauen und beschloss daher, ein weiterentwickeltes SIEM-System zu implementieren und ein eigenes SOC-Team aufzubauen. Das SOCWISE Team erhielt den Zuschlag für die SIEM-Ausschreibung, weil RSA NetWitness® nachweislich die beste Transparenz des Netzwerks bot, perfekt skalierbar war und sich flexibel integrieren ließ. Andere Tools boten zwar eine gute KI, aber es fehlte ihnen an maßgeschneiderten Inhalten und Fallmanagement.

Kombination von Lösungen mehrerer Anbieter wäre teurer gewesen und hätte mehr Ressourcen verbraucht. Das SOCWISE Team implementierte eine verwaltete SIEM-Lösung auf Basis der RSA NetWitness®Suite, entwickelte auch die Erkennungsinhalte und führte die erste Betriebsphase durch. Die nächste Herausforderung bestand darin, dass das Unternehmen trotz seiner kontinuierlichen aggressiven Personalrekrutierung nicht in der Lage war, die gewünschten Rollen zu besetzen, sodass kein SOC-Team gegründet werden konnte. Deshalb wurde eine Ausschreibung für die Bereitstellung von MDR-Diensten veröffentlicht, mit der SOCWISE beauftragt wurde.

SOCWISE

POWERED BY EURO ONE

SOCWISE

IHRE HERAUSFORDERUNG IST UNSERE MISSION

socwise.eu

Ergebnisse

Das SOCWISE Team entwarf zunächst ein detailliertes Servicemodell und erstellte die entsprechenden strategischen Pläne, wie bei Vorfällen reagiert werden sollte. Nach der anfänglichen Feinabstimmung war das Security Operations Center des Kunden schließlich einsatzbereit, wobei die SOCWISE Experten dem Kunden weiterhin bei der Implementierung der ausgefeilten Verfahren zur Seite standen.

Das SOCWISE Team und das IT-Betriebsteam des Kunden arbeiten tagtäglich als ein Team zusammen, sei es bei der Feinabstimmung von Inhalten, der Abwehr eines Phishing-Angriffs oder dem Auffinden von Risikonutzern auf Grundlage ihres Identitätsverhaltens und deren Beratung für eine bessere Sicherheit. Der Service wird auf der Grundlage eines betrieblichen Handbuchs erbracht und anhand vereinbarter Prozesskennzahlen gemessen. Der Kunde ist nun überzeugt, dass er einen vollständigen Überblick über die internen Netzwerkereignisse und den ausgehenden Datenverkehr hat.

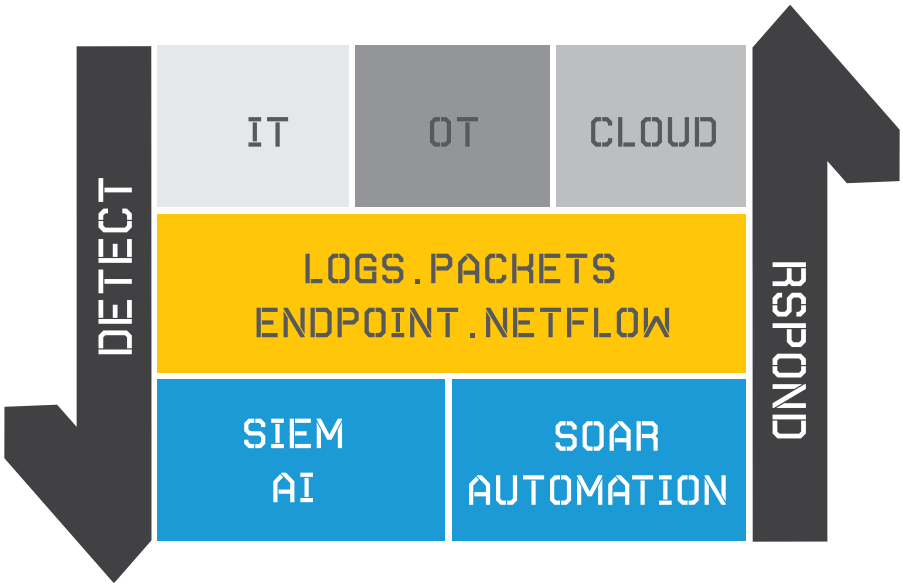
Anhand verschiedener Beispiele haben das SOC-Team und die Plattform gezeigt, dass ein gut vorbereitetes, zu 100 % engagiertes und geschultes Team unerlässlich ist, um auf riskante Veränderungen und unerwünschte Aktivitäten aufmerksam zu werden und gleichzeitig den IT-Betrieb zu unterstützen.

Diese Zusammenarbeit ermöglichte es dem CISO, die Fähigkeiten seiner Abteilung unter Beweis zu stellen, den Stress für sein Team zu reduzieren und eine Arbeitsumgebung zu schaffen, in der alle Beteiligten viel angenehmer arbeiten können.

Überblick über die Lösung

SOCWISE verwaltete den Detektions- und Reaktionsdienst, der Remote-Personalressourcen, das Know-how erfahrener Berater und die Technologieplattform umfasst.

Die Entwicklung der SIEM- oder SOAR-Inhalte ist auf die genauen Geschäftsrisiken zugeschnitten und der Service basiert immer auf den exakten Bedürfnissen des Kunden. Die NetWitness® Plattform ist die weltweit führende SOC-Technologie und immer noch die einzige Plattform, die alle Logs, Netzwerk- und Endpunktdaten als Grundeinstellung verarbeitet. Sie führt eine mehrstufige KI-Analyse durch und umfasst auch eine führende SOAR- und eine Bedrohungsanalyse-Plattform.



PAGE TWO