splunk> turn data into doing™

CASE STUDY

Cybersicherheitssoftware-Anbieter Check Point gewinnt mit Splunk tiefgreifende Erkenntnisse

Zentrale Herausforderungen

Check Point wollte aus verschiedenen Datensätzen aussagekräftigere Erkenntnisse gewinnen, um den Betrieb und die Effektivität zu verbessern und gleichzeitig Bedrohungen abzuschwächen.

Wichtige Ergebnisse

Splunk bietet Echtzeiterkenntnisse über Geschäftsabläufe, sodass die Mitarbeiter und Systeme von Check Point auch bei unvorhergesehenen Ereignissen, wie z. B. bei Remote-Arbeit während der Pandemie, immer einen Schritt voraus sind.

Check Point SOFTWARE TECHNOLOGIES LTD.

Branche: Technologie

Lösungen: Security

Wie sichert ein Anbieter von Security-Software seine eigenen Systeme?

Check Point entwickelt Lösungen für Cybersicherheit, die mehr als 100.000 Unternehmen aller Größenordnungen zugutekommen. Beim Schutz der eigenen Systeme und seiner 5.400 Mitarbeiter legt Check Point die Messlatte denkbar hoch. Das Unternehmen wollte aussagekräftigere Erkenntnisse aus den vielen Terabyte an Daten gewinnen, die seine Systeme täglich erfassen, um sich ein besseres Bild von Geschäftsabläufen machen und die Sicherheit aller Prozesse optimieren zu können.

Schnelle, intelligente Untersuchungen und wirksame Bedrohungsprävention

Als Check Point ein Security Operations Center (SOC) einrichtete, um die Rechenschaftsmechanismen zum Schutz des Unternehmens zu verbessern, entschied man sich für Splunk Enterprise Security. Der Grund ist einfach: Splunk kann all die vielen Datenformate aufnehmen, die im Unternehmen genutzt werden, und funktioniert mit allen Technologien, auf die das Unternehmen angewiesen ist.

„Wir sind ein datengestütztes Unternehmen“, erklärt Jony Fischbein, Global Chief Information Security Officer bei Check Point. „Die größte Herausforderung besteht im Aggregieren der enormen Datenmengen, die wir erfassen, und die Umwandlung dieser Daten in nützliche Informationen.“

Datengestützte Ergebnisse

5x
schnellere Sicherheits-untersuchungen

17
Tage für die Migration zu Splunk

100%
der Remote-Mitarbeiter erfüllen die neuen Covid-19-Sicherheitsrichtlinien

17 Tage nach dem Umstieg auf Splunk konnte Check Point bereits erste Vorteile erkennen, beispielsweise ein geschärftes Bedrohungsbewusstsein und schnellere Sicherheitsuntersuchungen im Vergleich zum früheren SIEM-Tool.

Mithilfe der Dashboards von Splunk kann Check Point den aktuellen Status seiner Systeme visualisieren. Automatisierte Warnmeldungen informieren über bösartige Aktivitäten oder Schwachstellen im Netzwerk. Laut Fischbein kann sein Team dank Splunk außerdem rasch und wirksam Probleme mit Schadenspotenzial untersuchen, bevor tatsächlich Schäden eintreten, zum Beispiel wenn Entwickler Quellcode mit aus dem Büro nehmen oder eine neue Schwachstelle in einem eingesetzten Produkt auftaucht.

„Wir wissen jetzt, was wir untersuchen müssen und ob wir das Problem gelöst haben. Dabei verlassen wir uns nicht auf ein Bauchgefühl, sondern auf solide Daten“, so Fischbein.

Sicheres Arbeiten während der Pandemie

Splunk gab Check Point die Möglichkeit, aussagekräftige Erkenntnisse aus Daten abzuleiten und auch während der COVID-19-Pandemie sicher und produktiv zu arbeiten.

Als ein Mitarbeiter positiv auf COVID-19 getestet wurde, griff das IT-Team von Check Point auf Splunk zurück, um anhand von Aufzeichnungsdaten der Zugangsausweise zu ermitteln, welche Mitarbeiter besonders exponiert waren und in den letzten 14 Tagen Kontakt zu der betreffenden Person hatten. Mitarbeiter mit einem Infektionsrisiko wurden umgehend benachrichtigt und aufgefordert, von zu Hause aus zu arbeiten und sich in Selbstisolation zu begeben.

„Das wäre mit keiner anderen Lösung möglich gewesen“, so Fischbein.

> Wir sind ein datengestütztes Unternehmen. Die größte Herausforderung besteht im Aggregieren der enormen Datenmengen, die wir erfassen, und die Umwandlung dieser Daten in nützliche Informationen.”
>
> **Jony Fischbein,** Global Chief Information Security Officer, Check Point

Dank Splunk konnte Check Point während der Pandemie außerdem dafür sorgen, dass die Sicherheit auch bei der Remote-Arbeit nicht zu kurz kam. Als die Unternehmensführung neue Sicherheitsmaßnahmen für die Arbeit im Homeoffice festlegte, ließ sich mit Splunk nachverfolgen, welche Mitarbeiter die Maßnahmen einhielten. Innerhalb von zwei Wochen konnte Fischbein seinem CEO eine Security-Compliance von 100 Prozent vorweisen. „Das hat unserem Führungsteams wirklich vor Augen geführt, wie wertvoll Splunk ist. Die Daten waren ein Beleg dafür, dass die Mitarbeiter von zu Hause aus produktiv und sicher arbeiten konnten.“

> Wir wissen jetzt, was wir untersuchen müssen und ob wir das Problem gelöst haben. Dabei verlassen wir uns nicht auf ein Bauchgefühl, sondern auf solide Daten.”
>
> **Jony Fischbein,** Global Chief Information Security Officer, Check Point

Mit Blick auf die Mitarbeiter im Homeoffice nutzte Check Point Splunk auch, um Sicherheitsrisiken zu erkennen und zu minimieren. Ein Entwickler nutzte beispielsweise einen BYOD-Laptop, um auf das Darknet zuzugreifen, und ein Mitglied des Finanzteams gewährte einem anderen Mitarbeiter Zugriff auf seinen Firmenlaptop. Nachdem sie über diese Probleme in Kenntnis gesetzt worden waren, wiesen die Manager ihre Mitarbeiter an, sich an die Richtlinien zu halten, um Unternehmensdaten und sensible Informationen zu schützen.

Zukunftssicheres Wachstum mit Splunk

Check Point ist sehr zufrieden mit den Vorzügen, die Splunk bietet, und plant eine Ausweitung der Nutzung.

„Wir wollen keine Lösung, die nur unsere aktuellen Anforderungen erfüllt. Wir wollen auch Unterstützung bei Aufgaben, die wir noch gar nicht kennen und die vielleicht in sechs Monaten oder einem Jahr anfallen“, erklärt Fischbein. „Bei denLösungen von Splunk haben wir festgestellt, dass sie mitwachsen.”

Check Point plant, Splunks Automatisierungsfunktionen für Aufgaben wie das Isolieren eines potenziell anfälligen Geräts und die Verbesserung des Geheimhaltungsmanagements der Mitarbeiter einzusetzen. Darüber hinaus findet das Unternehmen Möglichkeiten, Splunk auch von Mitarbeitern außerhalb des SOC nutzen zu lassen. Beispielsweise können Helpdesk-Mitarbeiter Warnmeldungen herausfiltern und entsprechende Maßnahmen ergreifen.

„Mit Splunk haben wir das gesamte Unternehmen im Blick“, so Fischbein. „Außerdem ist die Plattform nützlich für so ziemlich alles, was wir tun.“

21-19735-Splunk-Tier2-Check Point-CS-A4-101