THREATQUOTIENT

KUNDEN-FALLSTUDIE

Weltweit tätiges Software-Unternehmen konzentriert sich mit ThreatQ auf 5 Anwendungsszenarien

Ein weltweit tätiges Software-Unternehmen mit Hauptsitz in den USA, das Cloud Computing, Virtualisierung und Sicherheits-Software anbietet, benötigte eine zentrale Plattform, um die Sicherheitsüberwachung zu verbessern und die Erkennung und Reaktion zu beschleunigen.

Herausforderung

Das global agierende Software-Unternehmen benötigte eine effizientere und effektivere Möglichkeit, die zahlreichen Bedrohungs-datenquellen zu verstehen und basierend darauf Angriffsrisiken zu verringern. Beim Durchsuchen aller Bedrohungsinformationen war es bisher schwierig und zeitaufwändig, die beobachteten Aktivitäten mit den für die Unternehmensumgebung relevanten Bedrohungen zu korrelieren. Das Unternehmen musste schneller feststellen können, welche Angreifer hinter den Kampagnen steckten, welche Schwachstellen mit hoher Priorität gepatcht werden müssen und welche Angriffe gegen die Partner die eigenen Kunden, Mitarbeiter und Infrastruktur gefährdeten.

- Erfassung der Daten aus internen, kommerziellen und Open-Source-Feeds
- Fokus auf aktive Bedrohungen in der eigenen Umgebung
- Priorisierung und Verwaltung von Schwachstellen

„Unsere Bedrohungsdaten-Analysten benötigten eine zuverlässige Plattform, mit der sie Cyber-Sicherheitsbedrohungen gegen das Unternehmen schneller einschätzen und darauf reagieren können“, erklärte der Leitende Analyst für Bedrohungsdaten. „Dabei waren Automatisierung und Zusammenarbeit entscheidend, da unser Team klein ist und weltweit verteilt arbeitet.“

Lösung

Der Kunde benötigte eine Plattform, die als zentrales Repository für alle Bedrohungs-informationen fungieren und das Team dabei unterstützen konnte, in den fünf Phasen des Threat-Intelligence-Zyklus – Planung, Erfassung, Verarbeitung, Anreicherung und Verteilung – effizient und effektiv zu arbeiten. Hierfür identifizierte das Unternehmen die folgenden Erfolgskriterien:

- Aggregation der Feed-Daten aus den verwendeten Open-Source- und Premium-Services, einschließlich Berichte und Bedrohungsindikatoren
- Datenanreicherung einschließlich der Möglichkeit, Beziehungen zwischen Indikatoren herzustellen und Kontextinformationen aus internen Systemen hinzufügen
- Priorisierung der Bedrohungen basierend auf den Tools, Techniken und Prozeduren (TTPs) der Angreifer und korreliert mit den Schwachstellen und dem Risikoprofil des Unternehmens
- Reporting-Funktionen, mit denen Analysten schnell fertige Berichte für Führungskräfte erstellen können, die die Relevanz innerhalb der Bedrohungslandschaft aufzeigen
- Zentrale Bibliothek aller Daten, Berichte, Digests und Zusammenfassungen zu internen und externen Bedrohungen und Ereignissen als durchsuchbare zentrale Informationsquelle
- Funktionen zur einfachen Zusammenarbeit mit internen Teams, einschließlich Überwachung und Koordinierung der Aktivitäten, um Untersuchungen und die Erstellung von Berichten zu unterstützen
- Möglichkeit zum Austausch von Indikatoren (einschließlich Kontext) mit externen Gruppen bei Bedarf

Nach einer umfassenden Evaluierung von drei Anbietern stellte das Unternehmen fest, dass ThreatQ alle Erfolgskriterien erfüllt. ThreatQ wird derzeit für alle wichtigen

ÜBERSICHT

BRANCHE: Globales Technologieunternehmen

KUNDE SEIT: 2018

MITARBEITER: Mehr als 24.000

UMSATZ: Über 8 Milliarden

STANDORT: Hauptsitz in den USA

HERAUSFORDERUNG

Untersuchung und Priorisierung von Bedrohungs-daten für Threat Hunting, Bedrohungsverwaltung, Untersuchung von Spear-phishing-Angriffen, Reaktion auf Zwischenfälle und Schwachstellenverwaltung.

LÖSUNG

Durch Automatisierung und Zusammenarbeitsfunktionen unterstützt die ThreatQ-Plattform die schnelle Bewertung und Abwehr von Bedrohungen sowie die Erfassung, Korrelation, Evaluierung und Verteilung von Bedrohungsinformationen für eine breite Palette an Quellen und Technologien.

ERGEBNIS

- ✔ Höhere Effizienz und Effektivität von Teams und Technologien
- ✔ Beschleunigte Prozesse für fünf wichtige Anwendungsszenarien
- ✔ Fertige Berichte für Führungskräfte zu wichtigen Kennzahlen
- ✔ Höhere Rendite der bestehenden Sicherheitsinfrastruktur

www.threatquotient.com

Anwendungsszenarien eingesetzt: Bedrohungsverwaltung, Threat Hunting, Untersuchung von Spearphishing-Angriffen, Reaktion auf Zwischenfälle und Schwachstellenverwaltung.
Da Bedrohungsdaten basierend auf von Analysten festgelegten Parametern ausgewertet und gefiltert werden können, werden die relevanten Bedrohungen für ihre Umgebung sichtbar, was die Bedrohungsverwaltung und Priorisierung von Aktivitäten wie Patch-Installationen vereinfacht. Die Bedrohungsdaten werden automatisch neu priorisiert, wenn neue Daten und Erkenntnisse zur Plattform hinzugefügt werden. Durch das Zusammenführen von Bedrohungsdaten, Nachweisen und Benutzern können alle Teammitglieder für die Untersuchung zusammenarbeiten und Spearphishing-Kampagnen abwehren, nach Bedrohungen suchen oder die Reaktion auf Bedrohungen beschleunigen. Mit den Kollaborationsfunktionen für die Untersuchung wird gewährleistet, dass das Team effizient zusammenarbeiten und schnelle effektive Behebungsmaßnahmen ergreifen kann. Die Datenweitergabe zwischen Analysten, Teammitgliedern und Zeitzonen ist nahtlos möglich, was besonders für geografisch verteilte Teams wichtig ist.

„ThreatQ kann unsere Threat Intelligence- und Untersuchungsprozesse unterstützten, sodass wir unsere Vorgehensweise nicht ändern mussten. Dazu standen standardmäßig vorhandene Integrationen für eingehende Feeds, zusätzliche Sicherheitstools und Schutzkontrollen zur Verfügung. Durch die Automatisierung und Zusammenarbeit an wichtigen Stellen im Threat-Intelligence-Zyklus konnten wir unsere Sicherheitsüberwachung sowie die Erkennung von und Reaktion auf Bedrohungen deutlich verbessern."

– Leitender Analyst für Bedrohungsdaten

Ergebnis

Beschleunigte Prozesse

Die Kombination aus automatisierter Datenaggregation, Korrelation, Priorisierung und Verteilung von Bedrohungsdaten für alle Systeme und Teams sowie die Zusammenarbeit während der Untersuchung ermöglichen schnellere die Erkennung von und Reaktion auf Bedrohungen.

Standardisierte Berichtsvorlagen

ThreatQ optimiert das Reporting für Führungskräfte dank Vorlagen, die sich in Wirtschaftssprache auf Kennzahlen und Erkenntnisse konzentrieren.

Zentrale Informationsquelle

Alle Daten werden in einem zentralen Repository aggregiert, das Analysten anhand von Beobachtungen, Erkenntnissen und Dokumentationen zu Untersuchungen aktualisieren können, damit die Threat Intelligence aktuell und relevant bleibt und die Produktivität und Effizienz der Analysten verbessert wird.

Unterstützung für fünf Anwendungsszenarien

Das Sicherheitsteam verwendet ThreatQ zur Verbesserung der Sicherheitsprozesse für fünf Anwendungsszenarien: Bedrohungsverwaltung, Threat Hunting, Untersuchung von Spearphishing-Angriffen, Reaktion auf Zwischenfälle und Schwachstellenverwaltung.

Integration mit der Infrastruktur für höhere Rendite

Mit einem SDK (Software Development Kit) und benutzerfreundlichen APIs (Application Programming Interfaces) integriert ThreatQ die bestehenden Tools und Technologien des Kunden vollständig und erhöht damit den Wert der bestehenden Sicherheitsinvestitionen.

Arbeiten mit eigenen Prozessen statt Anpassung an ein Tool

Analysten können auf die Threat Intelligence zugreifen, die sie für ihre Arbeit benötigen. Dazu können sie die ihnen vertrauten Workflows und Tools beibehalten. Dies ist nahtlos in einer Umgebung möglich, in der sie mit anderen Spezialisten zusammenarbeiten und so Untersuchungen beschleunigen können.

Durch den Einsatz von ThreatQ kann der Kunde zusätzliche Tools für Anreicherung und Analyse integrieren, die in der bestehenden Sicherheitsinfrastruktur vorhanden sind. Das erweitert zudem die Threat Hunting-Möglichkeiten um proaktives Threat Hunting, d. h. der Kunde erhält aus einem externen Bericht Informationen zu einer Bedrohung und sucht in seiner Umgebung nach den zugehörigen Indikatoren. ThreatQ bietet den erforderlichen Kontext, um False Positives zu vermeiden. Außerdem können die Teams zusammenarbeiten, um jeden Winkel des Unternehmens zu überprüfen und so die TTPs der Angreifer und ihre böswilligen Aktivitäten zu finden. Dadurch lassen sich Bedrohungen vollständig beheben.

ThreatQuotient hat sich das Ziel gesetzt, die Effizienz und Effektivität von Sicherheitsabläufen mithilfe einer bedrohungsbasierten Plattform zu verbessern. Durch die Integration der bestehenden Prozesse und Technologien eines Unternehmens in eine zentrale Sicherheitsarchitektur beschleunigt und vereinfacht ThreatQuotient die Untersuchungen sowie die Zusammenarbeit innerhalb von und zwischen Teams und Tools. Dank Automatisierung, Priorisierung und Visualisierung verringern die Lösungen von ThreatQuotient die Menge nicht relevanter Informationen und heben Bedrohungen mit hoher Priorität hervor, damit begrenzte Ressourcen ihren Schwerpunkt auf diese Gefahren legen können und bei Entscheidungen unterstützt werden. ThreatQuotient hat seinen Hauptsitz in Nord-Virginia (USA) sowie internationale Zweigstellen in Europa, im APAC- und im MENA-Raum. Weitere Informationen finden Sie unter **www.threatquotient.com**.

© ThreatQuotient, Inc.