DATENBLATT

THREATQ DATA EXCHANGE

Effizienter Austausch gezielter und kuratierter Threat Intelligence mittels ThreatQ-Plattform und ThreatQ Data Exchange

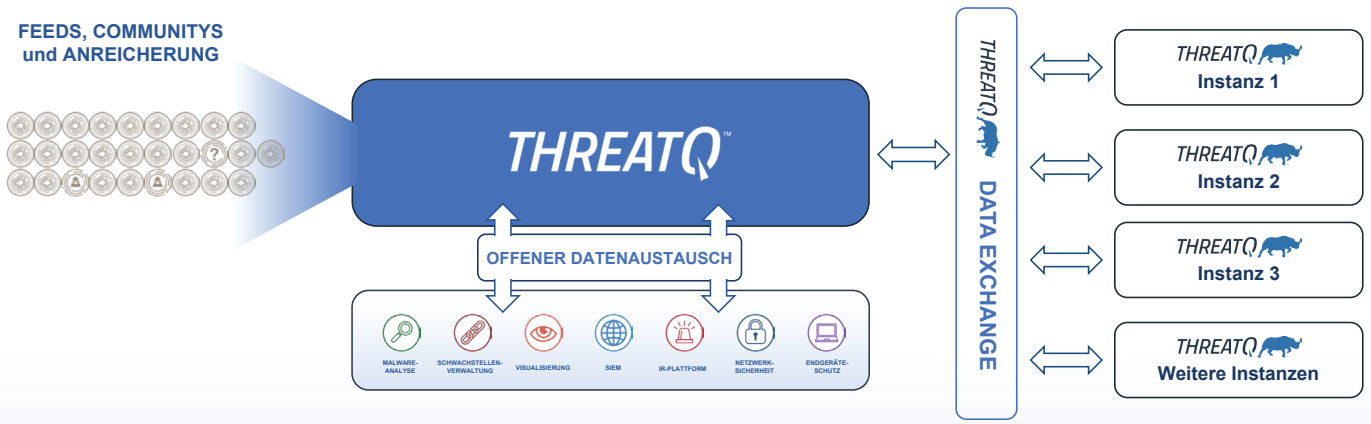
Mit ThreatQ Data Exchange können Sie den Informationsaustausch innerhalb oder zwischen Unternehmen jeder Größe und Komplexität optimal unterstützen und verwalten. ThreatQ Data Exchange vereinfacht nicht nur die Einrichtung eines bidirektionalen Austauschs von Bedrohungsinformationen in der ThreatQ-Plattform, sondern auch den skalierten Austausch zwischen mehreren Teams und Unternehmen jeder Größe.

Die Lösung setzt auf dem flexiblen Datenmodell von ThreatQuotient auf und unterstützt offene Standards für den Datenaustausch. Damit ist sie für die Anpassung an die jeweiligen Anforderungen und optimale Zusammenarbeit ausgelegt. Das bedeutet, dass Teams entsprechend ihren spezifischen Anforderungen und Zielen handeln und mit Partnern zusammenarbeiten können, ohne den Datenaustausch einschränken oder Daten ungewollt offenlegen zu müssen.

Hauptvorteile

- Intuitive Benutzeroberfläche für die unkomplizierte Herstellung uni- oder bidirektionaler Verbindungen zu externen Systemen
- Interaktives Topologie-Diagramm mit allen verbundenen Systemen für einfache und leicht skalierbare Verwaltung und Überwachung
- Einfache Installationsabläufe, die Verbindungskonfigurationspakete zum einfachen und reproduzierbaren Hinzufügen mehrerer verbundener Nodes nutzen
- Zuverlässiges Aktivitätenprotokoll zum Status der Verbindungen, einschließlich Details zu den ausgetauschten Daten für Überwachung und Berichterstellung

DATENÜBERTRAGUNG MIT THREATQ DATA EXCHANGE



Wer profitiert von ThreatQ Data Exchange?

Mehrstufige Netzwerke zum Austausch von Threat Intelligence, bei denen einem globalen Administrator Kontroll- und Überwachungsrechte gewährt werden müssen, können Bedrohungsinformationen mithilfe von ThreatQ Data Exchange schneller und einfacher nutzen. Davon profitieren zum Beispiel:

- Große staatliche Stellen mit individuellen Datenteams und -zielen, die permanent zusammenarbeiten und relevante Daten austauschen.
- MSSPs, die mehrere Vektoren oder geografische Regionen abdecken.
- Große oder mittelständische Unternehmen mit weltweiter Präsenz oder segmentierten Geschäftseinheiten (multinationale Unternehmen, Großkonzerne und Entitäten, die in mehreren Regionen tätig sind und auf Datentrennung achten müssen).

ANWENDUNGSSZENARIO

Die unternehmensweiten Security Operations Center (SOC) eines Unternehmens befinden sich an den Hauptsitzen. Aufgrund der Art des Geschäfts sind Zweigstellen auf der ganzen Welt verteilt und müssen kuratierte Threat Intelligence mit den Sicherheitsteams dieser Zweigstellen austauschen. Das CTI-Team (Cyber Threat Intelligence) an den Hauptsitzen ist verantwortlich für die Erfassung, Analyse und Priorisierung der relevanten Threat Intelligence. Ein Teil dieser Informationen muss an jede Zweigstelle gesendet werden, um weltweit einheitliche Erkennung und Schutz vor globalen Sicherheitsrisiken zu gewährleisten.

Mit ThreatQ Data Exchange kann das zentrale Team die ThreatQ-Plattform als primäre Quelle für Threat Intelligence in der Umgebung konfigurieren. Es ist ganz einfach, Entitäten den Abruf von Daten aus der primären Quelle zu ermöglichen. Sie generieren dazu ein Verbindungspaket auf der primären ThreatQ-Plattform und exportieren es in jeden einzelnen Node der Zweigstelle. Sobald diese Pakete implementiert sind, kann die Kommunikation beginnen.

Wenn Analysten die primäre ThreatQ-Plattform verwenden, können sie die Threat Intelligence kuratieren, sodass die Zweigstellen nur für ihre Umgebung relevante und priorisierte Daten erhalten und verarbeiten. Das zentrale CTI-Team kann die Suche speichern, sodass die Daten bei jeder Erstellung und Weiterleitung einer Datensammlung für die lokale Nutzung bereits basierend auf den festgelegten Parametern kuratiert sind. Datensammlungen sind nicht auf technische Indikatoren beschränkt, sondern können auch Kontextinformationen sowie Informationen zu Malware, konkreten Kampagnen und Taktiken, Techniken und Prozeduren (TTPs) sowie Motiven von Bedrohungsakteuren enthalten. Durch die Aktivierung der Datenübertragung wird an jede Zweigstelle kuratierte Threat Intelligence weitergeleitet.

Ein bidirektionaler Austausch

Für das zentrale CTI-Team ist es außerdem wichtig, Feedback von Zweigstellen auf der ganzen Welt zur verteilten Threat Intelligence zu erfassen. ThreatQ Data Exchange bietet bidirektionale Integration, sodass festgelegt werden kann, dass dieselbe Transportebene Feedback von jeder Zweigstelle zurück an das zentrale CTI-Team liefert. Dadurch kann das zentrale CTI-Team die Sicherheitslage des globalen Unternehmens in Bezug auf konkrete nachverfolgte Bedrohungen besser verstehen, Trenddaten hervorheben und Bereiche mit schwacher Abdeckung aufzeigen.

Darüber hinaus kann dank der bidirektionalen Kommunikation ein globaler Bedrohungsdatenspeicher aufgebaut werden. Sobald Zweigstellen Sicherheitsvorfälle verwalten, neue Bedrohungen aufdecken oder zusätzlichen Kontext zu bekannten Bedrohungen finden, können diese Daten im zentralen Repository gespeichert werden. Die Transportebene kann so konfiguriert werden, dass alle Informationen zum Zwischenfall oder lokal erstellte Informationen automatisch zurück an die zentrale ThreatQ-Plattform gesendet werden und eine zentrale Informationsquelle aufgebaut wird, die Teams auf der ganzen Welt zur Verfügung steht.

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

Sales@ThreatQ.com • +1 703.574.9885

© ThreatQuotient, Inc.