Fragen an Anbieter von Threat Intelligence-Plattformen

Eine Threat Intelligence-Plattform (TIP) unterstützt SOCs, Threat Intelligence-Analysten sowie die für Incident Response, Risiko-Management und Schwachstellen verantwortlichen Teams, damit sie nicht nur auf Ereignisse und Warnmeldungen reagieren müssen, sondern Bedrohungen vorhersehen und proaktiver agieren können. Um dies leisten zu können, dient die TIP als zentrales Repository für alle Bedrohungsdaten aus externen sowie internen Quellen. Dadurch werden die Zusammenarbeit, fundierte Entscheidungen, proaktive Maßnahmen sowie schnellere Erkennung und Reaktion vereinfacht. Die Plattform muss Sie dabei unterstützen, die relevantesten Bedrohungen für Ihr Unternehmen zu erkennen, zu priorisieren und angemessen zu handeln.

Hier finden Sie die wichtigsten Fragen, die Sie einem Threat Intelligence-Plattform-Anbieter vor dem Kauf stellen sollten. Sie können die Liste als Schnellreferenz nutzen. Laden Sie außerdem den Buyer's Guide to Threat Intelligence Platforms (Käuferleitfaden für Threat Intelligence-Plattformen) mit weiteren Informationen herunter.

Datenerfassung

Wie viele kommerzielle und Open-Source-Feeds sind standardmäßig enthalten?

Können Kunden einzelne Feeds aktivieren/deaktivieren?

Können Kunden Komponenten eines Feeds aktivieren/deaktivieren (z. B. wenn sie nur Intelligence im Zusammenhang mit bestimmten Branchen importieren möchten)?

Kontext

Werden von Kunden initiierte oder definierte IoCs an die anderen Kunden des Anbieters weitergegeben?

Wenn ein Indikator mehrmals erfasst wurde, haben die nachfolgenden Indikator-Sichtungen Priorität gegenüber den vorherigen?

Kann ich benutzerdefinierte Attribute (z. B. Bitcoin-Adressen, Twitter-Benutzernamen, SWIFT-Code) definieren, um den Anforderungen unseres Unternehmens Rechnung zu tragen?

Scoring

Können Kunden das Scoring basierend auf ihrem eigenen Unternehmen, Team, Ressourcen und Funktionen anpassen, ohne dass diese Anpassungen mit anderen Kunden geteilt werden?

Kann ich den Scoring-Algorithmus anpassen, damit er auf für mein Unternehmen relevanten Informationen basiert?

Unterstützen Sie negative Score-Werte?

Kann ich den Score-Wert für die verschiedenen Feeds anpassen?

Ablaufdaten für Intelligence

Welchen Ansatz verfolgt der Anbieter in Bezug auf Ablaufdaten für Intelligence?

Kann ich die Ablaufmethodik an mein benutzerdefiniertes Scoring und die Möglichkeiten meiner Sensornetz-Technologien anpassen?

Kann das TIP das Ablaufdatum automatisch basierend auf von mir festgelegten Parametern anpassen?

Korrelation interner und externer Daten

Muss ich mehr bezahlen, um APIs für die Integration interner sowie externer Daten nutzen zu können?

Wenn bidirektionaler Datenaustausch aktiv ist, besitzt Ihr Unternehmen Eigentumsrechte an den Daten meines Unternehmens innerhalb des Systems?

Muss ich für die Umsetzung der benötigten Integrationen zusätzliche Ports in der Firewall öffnen?

Integrationen

Ist die Nutzung von APIs für Integrationen mit Zusatzkosten verbunden?

Bieten Sie bidirektionale Integration in alle SIEM-Systeme, Ticket-Systeme und Lösungen zur Schwachstellenverwaltung?

Welche anderen Tools unterstützen Sie mit bidirektionaler Integration?

Muss ich Professional Services engagieren, um Integrationen nutzen zu können?

Werden SIEM-Informationen geteilt?

Benachrichtigungen

Kann ein Analyst zu beliebigen Objekten im System über Ihr Dashboard eine Warnungsliste erstellen?

Erfolgt die Warnbenachrichtigung in der Benutzeroberfläche, per E-Mail oder in einem Drittanbieter-Client (z. B. Slack, HipChat, per RSS-Feed)?

Exportmöglichkeiten

Werden Exports in die häufigsten Standardformate (z. B. CSV, JSON, CIF) unterstützt?

Kann ein Analyst beliebige Objekte und ergänzenden Kontext exportieren?

Unterstützt der Export eine Skriptsprache, die umfassende Kontrolle über Typ und Format der exportierten Informationen erlaubt (d. h. kann ein Analyst die exportierte Intelligence definieren und sie in einem bestimmten Technologie-spezifischen Format in einer zentralen Benutzeroberfläche ausgeben)?

Kann ein Analyst mehrere Export-Feeds konfigurieren (z. B. nach Sensortechnologie, geografischem Standort oder zur Unterstützung täglicher Suchvorgänge)?

Datenaustausch und Zusammenarbeit

Kann das TIP als gemeinsamer Arbeitsbereich für alle Mitglieder des Sicherheitsteam fungieren?

Kann ich Zusammenarbeitsfunktionen in unsere vorhandenen Arbeitsabläufe integrieren? Wenn ja, wie muss ich dazu vorgehen, und ist diese Integration mit Zusatzkosten verbunden?

Kann ich den Datenaustausch mit einem Anbieter oder einer Community aktivieren bzw. deaktivieren?

Werden die geteilten Daten anonymisiert, und wenn ja, wie?

Wenn Daten weitergegeben werden, wie werden sie vom Anbieter verwendet?

Beansprucht der TIP-Anbieter Eigentumsrechte an allen Daten, die auf seiner Plattform ausgetauscht werden?

Bereitstellungsoptionen

- Bin ich der alleinige Eigentümer meiner Daten?
- Werden meine Daten mit denen anderer Kunden in einer mandantenfähigen Umgebung zusammengeführt?
- Welche Funktionen stehen nur zur Verfügung, wenn ich einen lokalen Integrations-Server bereitstelle?
- Wenn die Infrastruktur eines Cloud-Anbieters offline geht, welche Funktionen sind dann nicht verfügbar?
- Können Sie Kopien Ihres vierteljährlich durchgeführten Penetrationstests zur Verfügung stellen?

Preismodelle

- Fallen Kosten pro Integration oder API für jedes Schutzsystem an? Wenn ja, wie hoch sind diese Kosten?
- Ist die Integration kundenspezifischer Daten oder IoCs mit Kosten verbunden?
- Wie hoch sind die Gesamtbetriebskosten bei meinen geschäftlichen Anforderungen?
- Ist eine private Instanz einer Cloud-basierten Bereitstellung mit Zusatzkosten verbunden?
- Kann ich die Anzahl der Benutzerlizenzen ohne zusätzliche Gebühren anpassen?
- Gibt es eine Lizenz für eine unbegrenzte Anzahl von Benutzern?
- Gelten Sonderpreise für MSSPs (Managed Security Services Provider)?

Support

- Gibt es verschiedene Möglichkeiten, sich mit dem Support in Verbindung zu setzen?
- Welche SLAs werden in Bezug auf Support-Tickets angeboten?
- Wie aktualisiere ich Support-Tickets?
- Wie kann ich ein Problem eskalieren?
- Wie werden Funktionswünsche behandelt und wie schnell werden sie erfüllt?
- Wie werden Fehlerberichte behandelt und wie schnell werden Fehler üblicherweise behoben?
- Welche RMA-Richtlinien bestehen (sofern zutreffend)?

ÜBER THREATQUOTIENT™

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 und im APAC-Raum. Weitere Informationen finden Sie unter https://threatquotient.com.

TQ_Vendor-Question-List-for-TIPs_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • Allgemeine Fragen sowie Fragen zum Vertrieb: +1 703 574-9885