THREATQUOTIENT™

AUFBAU ODER KAUF?
Die ewige Technologiefrage

Ryan W. Trost, Mitbegründer und CTO

Die ewige Technologiefrage *„Aufbau oder Kauf?“* stellt sich meist dann, wenn für eine technologische Funktion bereits Open-Source-Optionen angeboten werden und eine gewisse Marktnachfrage besteht, der Reifegrad jedoch nicht groß genug ist, dass sich bereits sich über viele Jahre eine eigene Disziplin entwickeln konnte, in der von mehreren Herstellern verschiedene Lösungen angeboten und von Branchenexperten bewertet werden.

Threat Intelligence-Plattformen (TIPs) sind an einem Punkt angelangt, an dem sich Sicherheitsteams fragen, ob sie eine TIP selbst aufbauen oder kaufen sollten. Die Frage sollte jedoch vielmehr lauten: *„Wir könnten eine TIP aufbauen, aber sollten wir das auch tun?“*

BESCHREIBUNG EINER OPTIMALEN TIP

Eine Threat Intelligence-Plattform unterstützt Security Operations Center (SOC), 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 zentrale Informationsquelle für alle Bedrohungsdaten aus externen sowie internen Quellen. Dadurch werden die Zusammenarbeit, fundierte Entscheidungen, proaktive Maßnahmen sowie schnellere Erkennung und Reaktion vereinfacht. Ganz gleich, ob Sie diese Plattform kaufen oder aufbauen: Sie muss Sie dabei unterstützen, die relevantesten Bedrohungen für Ihr Unternehmen zu erkennen, zu priorisieren und angemessen zu handeln. Im Zuge der Veränderungen der Bedrohungslandschaft und Ihrer internen Umgebung kann die TIP außerdem dazu beitragen, dass Sie über potenzielle Gefahren auf dem aktuellen Stand bleiben, diese vorhersagen und dank kontinuierlicher Bedrohungsbewertungen Ihre Abwehrmaßnahmen verstärken können.

Zur Optimierung der Bedrohungsabwehr und Verwaltung sollte eine TIP die Möglichkeit bieten, interne Bedrohungsinformationen (z. B. Sicherheitsereignisdaten sowie Analysen von Malware und böswilligen Akteuren) schnell zusammenzuführen und mit externen Erkenntnissen zu korrelieren. Auf diese Weise erhalten Sie den wichtigen Bedrohungskontext: Wer, was, wann, wie und warum. Eine TIP sollte außerdem die Priorisierung unterstützen, damit Sie automatisch das Rauschen herausfiltern können und verstehen, welche Informationen für Ihr Unternehmen relevant sind. Hierfür legen Sie entsprechende Parameter fest. Durch Koordinierung, Automatisierung und Synchronisierung der Threat Intelligence sollte eine TIP Sie dabei unterstützen, die Konfiguration und Richtlinien Ihrer Sicherheitsinfrastruktur proaktiv zu optimieren und die Erkennungs- und Reaktionsmaßnahmen zu beschleunigen. Regelmäßige Aktualisierungen mit vorverarbeiteten, kontextbezogenen und priorisierten Daten sowie die Möglichkeit, Feedback und Erkenntnisse zu erfassen, bieten Teams die Möglichkeit, Bedrohungen neue Prioritäten zuzuweisen und vorherzusehen. So lässt sich das Risiko zum aktuellen Zeitpunkt und für die Zukunft reduzieren.

WICHTIGE ÜBERLEGUNGEN BEI DER ENTSCHEIDUNG ÜBER AUFBAU ODER KAUF

Unabhängig davon, wie viele dieser Fähigkeiten von Ihren Sicherheitsteams und der Verwaltung als wichtige technische oder geschäftliche Anforderungen eingestuft werden, müssen Sie folgende Aspekte beachten.

RESSOURCEN

Verfügt Ihr Unternehmen über ein dediziertes Entwicklungsteam?

Es ist äußerst schwierig, eine Person (oder gar ein kleines Team) mit den nötigen Kenntnissen für den Aufbau zentraler Software-Komponenten zu finden. Noch schwieriger ist es, diese Ressource langfristig zu halten, damit sie die kontinuierliche Wartung gewährleisten sowie neue Funktionen und Integrationen einbinden kann. Das gilt vor allem dann, wenn dieses Projekt nicht direkt zur Umsatzsteigerung beiträgt. Vermeiden Sie es, Mitarbeiter aus anderen Abteilungen zu „borgen“ oder einen Ringtausch vorzunehmen. Das führt vor allem in Umgebungen zu Problemen, in denen Entwicklern je nach Bedarf neue Aufgaben zugewiesen werden. Der „Ersatz“-Entwickler müsste sich vor dem Weiterarbeiten erst mit dem vorhandenen Code vertraut machen, was zu Verzögerungen führt oder gar den Stopp des Projekts verursachen kann.

FINANZIELLE HERAUSFORDERUNGEN

Haben Sie alle Vorab- und Wartungskosten einkalkuliert?

Der Aufbau eines internen Teams zur Unterstützung kleiner unternehmenseigener Anwendungen erfordert mindestens vier Vollzeitmitarbeiter: zwei Entwickler, einen dedizierten Experten für Datenbanken/Big Data und einen Verantwortlichen für Qualitätssicherung. Möglicherweise denken Sie, dass sie keinen dedizierten Experten für Datenbanken/Big Data benötigen. Doch wenn Sie berücksichtigen, dass externe Quellen aggregiert und interne Analysen von Malware-Daten, Schwachstellendaten sowie Risikomanagementfaktoren durchführt und alle diese Objekte miteinander verknüpft werden müssen, wird der Bedarf schnell klar. Wenn Sie auf eine dedizierte Ressource verzichten und nur einen Teil dieser Funktionen nutzen, wird das Endergebnis Ihr eigentliches Ziel deutlich verfehlen. Auch wenn die jährlichen Kosten für die Einstellung eines solchen Teams von der Region abhängen und auf dem Papier angemessen scheinen, ist es in den meisten Unternehmen deutlich einfacher, ein neues Tool einzuführen, als neue Mitarbeiter einzustellen. Das gilt besonders dann, wenn ein vergleichbares Tool 85 bis 90 Prozent der Anforderungen erfüllt und die Kosten bereits Support und Upgrades abdecken.

OPERATIVE DISKREPANZEN

Verfügen Ihre Ressourcen über Kompetenzen in den Bereichen Software-Entwicklung und Bedrohungsabwehr?

„Echte“ Software-Entwicklung und Sicherheitsprozesse sind sehr unterschiedliche Disziplinen. Ein geeigneter Entwickler muss sich mit Software-Architekturen, Entwicklungsprozessen (DevOps), Sicherheitsprozessen (SecOps) und Sicherheitstechnologien auskennen. Diese Kombination ist extrem selten. Daher benötigt er wahrscheinlich einen Kollegen, der sich mit Sicherheit bzw. Intelligence auskennt und bei der Konzeption und Entwicklung helfen sowie als „finaler Verantwortlicher“ agieren kann. Das bedeutet jedoch, dass dieser Kollege seinen Kernaufgaben als Sicherheits- und Intelligence-Analyst oder Sicherheitsverantwortlicher nicht mit voller Produktivität nachgehen kann.

INNOVATION

Sind Sie bereit, kontinuierlich Ressourcen für neue Funktionen und Problembehebungen zur Verfügung zu stellen?

Wenn die TIP intensiver genutzt wird, werden natürlich auch die Funktionswünsche der Analysten zunehmen – ganz besonders dann, wenn die TIP Intelligence von mehreren Teams oder Abteilungen aggregieren soll. Können Sie das Entwicklerteam auch für längere Zeit aufrechterhalten, damit die Plattform erweitert werden kann? Was passiert, wenn die Funktionswünsche aufgrund konkurrierender Prioritäten nur mit Verzögerung umgesetzt werden können? Verfügen Sie über die Ressourcen, um Innovationen wirklich zu fördern, oder werden Sie eher versuchen, mit den TIP-Lösungen Schritt zu halten, die von Unternehmen angeboten werden? Bedenken Sie, dass Sie bei Anbietern (und besonders bei solchen mit Jahresabonnements) einen Hebel haben und damit gewährleisten können, dass das Produkt stets zu Ihren Anforderungen und Erwartungen passt. Es gibt genügend TIP-Anbieter, sodass Sie Ihren Anbieter bei Bedarf wechseln können. Obwohl ein solcher Wechsel nie einfach ist, geben sich Anbieter meist größte Mühe, den Wechsel von einem Mitbewerber so einfach und reibungslos wie möglich zu gestalten.

QUALITÄTSSICHERUNG

Kann Ihr Team alle erforderlichen System-, Regressions- und Integrationstests durchführen?

In der Anfangsphase genügt es möglicherweise, wenn die Entwickler den Code gegenseitig prüfen. Diese Vorgehensweise ist jedoch nicht endlos skalierbar. Wenn Ihre Plattform Ihren Anforderungen entsprechen soll, benötigen Sie einen formalisierten Qualitätssicherungsprozess, einschließlich standardisierter Komponententests, Simulationstests, Regressionstests und aufwändiger manueller Tests. Zudem müssen Sie verschiedene Umgebungen für Entwicklung, Produktion und Staging pflegen. Machen Sie sich bewusst, dass der Code-Umfang mit der zunehmenden TIP-Nutzung durch Analysten verschiedener Teams wachsen und der technische Aufwand für „schnelle Code-Korrekturen“ enorm zunehmen wird. Dieser Zeitaufwand geht von der Zeit ab, die für die lange Warteliste für neue Funktionen zur Verfügung steht. Das führt zu Spannungen zwischen Teams. In dieser Phase müssen Sie sich bewusst machen, dass der ursprüngliche Entwickler bereits über stark nachgefragte Kompetenzen im Bereich Sicherheits-Intelligence-Entwicklung verfügen wird und für andere Unternehmen äußerst interessant ist. Daher ist es sinnvoll, einen dritten Entwickler und zweiten Verantwortlichen für Qualitätssicherung abzustellen, damit Sie auch bei erfolgreichen Abwerbeversuchen immer noch über Redundanz verfügen.

INTEGRATION

Verfügt Ihr Team über die Kompetenz, alle aktuellen und zukünftigen Integrationen zeitnah durchzuführen?

Die meisten Unternehmen handhaben Millionen bedrohungsorientierte Datenpunkte aus kommerziellen und Open-Source-Quellen sowie von verschiedensten Sicherheitsanbietern plus umfangreiche Protokoll- und Ereignisdaten aus jedem Einzelprodukt innerhalb Ihres Abwehrsystems bzw. SIEM. Die Aggregation dieser Daten in Ihre TIP und deren Umwandlung in ein einheitliches, verarbeitbares Format ist eine gewaltige und komplexe Aufgabe, für die ein Vollzeit-Datenbanktechniker erforderlich ist. Zudem müssen die entscheidungsrelevante Threat Intelligence angewendet und die entsprechenden Technologien in Ihrem Sensornetz bereitgestellt werden. Das schließt die Integration in Firewall, IPS, IDS, NetFlow und Endgeräteschutz mit ein. Dieser Aufwand entwickelt sich schnell zu einem Vollzeitjob.

ZEIT

Verfügen Sie über realistische Einschätzungen zu dem Zeitraum, der für Entwicklung und Bereitstellung erforderlich ist?

Berücksichtigen Sie den Zeitaufwand für die korrekte Gestaltung, Ausarbeitung und Entwicklung einer Plattform im Vergleich zum Aufwand für die Implementierung einer Drittanbieterlösung: Bewertung potenzieller Lösungen, Eingrenzung der Auswahl, Proof-of-Concept-Prozesse und die eigentliche Implementierung. Zu berücksichtigen ist auch der Aufwand für die Anpassung der internen Anwendung, wenn bisher verborgene Hindernisse auftreten oder sich mehrere Monate nach dem Projektstart herausstellt, dass sich Konzepte und theoretische Pläne nicht in operative Routinen umsetzen lassen. Jede nötige Anpassung verlängert die Zeit, in der Ihr Bedrohungsabwehrprogramm nicht wie erforderlich arbeitet, und vergrößert das Fenster, in dem Gegner Angriffe starten können.

RISIKO

Wie viel Risiko sind Sie bereit, für eine interne Entwicklung in Kauf zu nehmen?

Letztendlich geht es darum, das Cyberrisiko zu minimieren. Der Vergleich der Performance und Risikominimierungsleistung zwischen einer selbstentwickelten Lösung und einer kommerziellen Plattform ist schwierig. Da proprietäre Lösungen nicht von Dritten validiert werden, gibt es keine etablierte Erfolgsbilanz. Dadurch fehlen unabhängige Prüfungen zur Leistung, zu den Best Practices für sicheren Code und zu eingebetteten Open-Source-Tools. Außerdem fehlen häufig SLAs. Wenn ein Gegner in eine intern erstellte Anwendung eindringen kann, ist die Beseitigung der Folgen zudem deutlich zeitaufwändiger, da Sie nicht nur die Incident Response handhaben, sondern auch Sicherheitslücken in den Funktionen schließen müssen, die möglicherweise zu dem erfolgreichen Angriff geführt haben.

ANBIETERVERWALTUNG

Bevorzugen Sie einen zentralen Ansprechpartner für Plattformaktualisierungen und Produkt-Roadmaps?

Es ist immer einfacher, mit einem Anbieter zusammenzuarbeiten – ganz gleich, ob es um eine innovative Funktion oder die Behebung eines Problems geht. Bei einer internen Lösung lautet die Frage eher, ob ein Mitarbeiter entlassen oder neu eingestellt werden muss. SOC-Manager sind meist die Hauptverantwortlichen für eine TIP, und sie verbringen 60 Prozent ihrer Zeit als Sachverständiger und Schiedsrichter, 20 Prozent als Übersetzer für die Geschäftsführung und 20 Prozent mit der Behebung technischer Probleme. Bei zusätzlichen Personalproblemen genügen diese 60 Prozent nicht, sodass noch weniger Zeit für andere Aktivitäten mit hoher Priorität zur Verfügung steht.

FAZIT

Ihre Möglichkeit zur Beschleunigung der Sicherheitsprozesse mithilfe eines optimierten Programms für Bedrohungsabwehr und Verwaltung hängt von dem Tool ab, mit dem Bedrohungsdaten, Analysen und Aktionen zusammengeführt werden. Wenn Sie die zuvor erläuterten Überlegungen durchgehen, stellen Sie die voraussichtlichen Kosten für Vollzeitmitarbeiter den Kosten für den Kauf einer Software gegenüber. Berücksichtigen Sie zudem die Opportunitätskosten und Risiken durch die Umlenkung der Sicherheitsressourcen von der Frontlinie zu Entwicklungsarbeiten. Ganz gleich, für welchen Ansatz sich Ihr Unternehmen entscheidet, sollten Sie sich an einer Strategie orientieren, die sich mit Ihrem Unternehmen und der Bedrohungslandschaft weiterentwickelt.

ÜBER DEN AUTOR

Als CTO und Mitbegründer von ThreatQuotient kann Ryan Trost auf mehr als 15 Jahre Erfahrung im Bereich Sicherheit zurückblicken. Dabei konzentriert er sich auf Eindringungserkennung und Cyber Intelligence, um die Vordenkerposition zu stärken und innovative Produkte zu konzipieren. Ryan Trost ist in der Cyberbranche als Experte anerkannt und häufiger Redner auf Branchenkonferenzen wie BlackHat, DEFCON, SANS, HTCIA (High Technology Crime Investigation Association) und FIRST. Er ist Autor des Buches „Practical Intrusion Analysis“ (Praktische Eindringungsanalyse) und hat einen der ersten raumbezogenen Eindringungserkennungsalgorithmen entwickelt, mit dem standortbezogene Angriffsmuster identifiziert werden können. Vor seiner Tätigkeit bei ThreatQuotient verwaltete Ryan Trost verschiedene USG und kommerzielle Security Operations Center (SOC), zudem war er Leitender Sicherheitsdirektor und Datenschutzbeauftragter eines mittelständischen Gesundheitsunternehmens in Nord-Virginia (USA). Ryan Trost ist außerdem Vorsitzender des Beirats des Cyber-Studiengangs am Northern Virginia Community College.

ÜBER THREATQUOTIENT™

ThreatQuotient ist sich bewusst, dass Menschen die Grundlage für Intelligence-basierte Sicherheit darstellen. Dank ThreatQ™, unserer offenen und erweiterbaren Threat Intelligence-Plattform, steht den Verteidigern die richtige Threat Intelligence zur Verfügung – mit den richtigen Tools sowie zum richtigen Zeitpunkt. Führende globale Unternehmen verwenden ThreatQ als Grundpfeiler für ihre Threat Intelligence-Abläufe sowie -Verwaltungssysteme und steigern so die Effektivität und Effizienz ihrer Sicherheitsmaßnahmen.

Weitere Informationen finden Sie unter threatq.com.

TQ_Build-vs-Buy_Rev1