WHITEPAPER

Messen des ROI von SOAR-Plattformen

splunk>
turn data into doing™

Die Investition in eine SOAR-Plattform (Security Orchestration and Response) ist eine kluge und höchst strategische Entscheidung. Schließlich ist die Wahl der korrekten Plattform, auf der Sie Ihr SOC (Security Operations Center) aufbauen, zweifellos wichtiger als die Wahl eines beliebigen Sicherheitsprodukts, das nur eine Punktlösung darstellt. Die von Ihnen gewählte SOAR-Plattform wird zu einem zentralen Bestandteil Ihrer Sicherheitsinfrastruktur und fungiert im Prinzip als Betriebssystem für Ihre Sicherheitsinvestitionen.

SOAR-Plattformen bieten eine Reihe wirtschaftlicher Vorteile und helfen Ihrem SOC-Team dabei, effizienter zu arbeiten. In diesem Whitepaper werden diese Vorteile quantifiziert, indem eine Vorgehensweise aufgezeigt wird, mit der Sie Ihre Kapitalrendite (Return on Investment, ROI) durch die Investition in eine SOAR-Plattform einschätzen können.

Warum benötigt man SOAR-Plattformen?

Ihr Sicherheitsteam arbeitet dort, wo es brenzlig wird: Bedrohungen für Ihr Unternehmen werden identifiziert, analysiert und ausgeschaltet. Trotz seiner Bemühungen wird der Rückstau von Benachrichtigungen und Fällen wahrscheinlich täglich immer größer. Und dafür gibt es auch eine einfache Erklärung: Es gibt schlichtweg nicht genügend Fachkräfte, die die Menge der täglichen Benachrichtigungen in den meisten der heutigen Unternehmen analysieren können.

Die Angreifer gehören mittlerweile einem ganzen Industriezweig an. Bedrohungen werden immer anspruchsvoller und ihre Zahl steigt. Wahrscheinlich gibt es schon einen neuen Angriff, bevor Sie überhaupt die Gelegenheit hatten, sich um den vorherigen zu kümmern. Die "Dwell Time" für Bedrohungen in Ihrer Umgebung, also die erforderliche Zeit bis zur Erkennung und Behebung von Angriffen, wächst trotz der steigenden Ausgaben für die IT-Sicherheit.

Die Probleme der Sicherheitsteams verschärfen sich noch weiter, wenn man sich die zunehmende Komplexität unserer IT-Umgebungen vor Augen führt. Das gilt auch für die IT-Sicherheit. Es wurden jetzt über drei Jahrzehnte lang Sicherheitsprodukte als Punktlösungen eingesetzt. Die Forschung zeigt, dass es derzeit über 1.500 Hersteller von Sicherheits-produkten und -services gibt. Eine weitere traurige Tatsache ist, dass die meisten Sicherheitsprodukte nicht miteinander funktionieren. Es gibt also Unmengen unabhängiger Lösungen, für deren Wartung eine große Anzahl von Personen erforderlich ist. Trotz gebündelter Lösungen von manchen der größten Sicherheitsunternehmen, entscheiden sich viele Unternehmen verständlicherweise für die individuell jeweils besten Produkte auf dem Markt. Das Endergebnis ist eine heterogene Sammlung individueller Sicherheitsprodukte, die sich weder miteinander verbinden lassen, noch gemeinsam als einheitliche Verteidigungsplattform fungieren können.

Es ist klar, dass sich hier etwas ändern muss. Mit Ihren Ausgaben für Personal und für die bereits vorhandene Technologie haben Sie bereits eine große Sicherheitsinvestition getätigt. Sie möchten diese vorhandenen Ressourcen aber besser nutzen. Das gelingt durch die Bereitstellung von Tools, die Effizienz und Ausmaß optimieren. So entsteht ein einheitliches Verteidigungssystem, das größer ist als die Summe seiner Einzelteile.

SOAR-Plattformen bündeln Kräfte und nutzen so die volle Leistung vorhandener Sicherheitsinvestition eines Unternehmens. Sie sind zur Behebung von Problemen ganz einfach erforderlich. Führende SOAR-Plattformen sind von Grund auf für eine sicherheitsspezifische Automatisierung und Orchestrierung konzipiert. Sie vereinheitlichen Punktlösungen über eine logische Architektur, die abstrakte Produktfähigkeiten in Sicherheitsaktionen umwandelt, die sich leicht über digitale Playbooks automatisieren lassen.

Was sind die Vorteile von SOAR?

SOAR-Plattformen helfen Ihnen dabei, cleverer zu arbeiten, indem Sie repetitive Aufgaben automatisieren. So kann Ihr Team seine ganze Aufmerksamkeit erfolgskritischen Entscheidungen widmen, die sein Können wirklich erfordern. Die Plattformen bieten folgende Funktionen:

- Automatisierte Auswertung von Ereignissen, damit Sie bei Ihrer Arbeit einfacher Wichtiges von Unwichtigem trennen können
- Vorabruf von Bedrohungsinformationen, um bessere Entscheidungen treffen zu können
- Orchestrierung komplexer Workflows, um Effizienz und Präzision zu verbessern

38 % der Unternehmen geben an, dass über die Hälfte ihrer Sicherheitsaktivitäten mit Hilfe von Automatisierung effektiver werden würden.
– ESG Research, 2016

SOAR-Plattformen können auch dazu beitragen, dass Sie schneller reagieren und durch automatisierte Erkennung, Untersuchung und Reaktion einzelne Aufgaben schneller beenden können. Die Plattformen bieten folgende Vorteile:

- Statt Minuten oder Stunden – oder bei manueller Bearbeitung sogar noch länger – führen Sie Aktionen nun in Sekundenschnelle aus
- Sie können komplexe Workflows erstellen und dabei sicherheitsspezifische Aktionen verwenden, die sich auf mehrere Sicherheitsprodukte anwenden lassen
- Sie können über einen visuellen Playbook-Editor schnell und ohne Codierung Playbooks erstellen.

Letztendlich können SOAR-Plattformen dazu beitragen, Ihre Cyber-Abwehr zu stärken, indem sie Ihre gesamte Sicherheitsinfrastruktur gemeinsam integrieren, sodass jeder Teil aktiv zur Verteidigungsstrategie beiträgt.

- Installieren Sie von Drittanbietern bereitgestellte oder benutzerdefinierte App-Integrationen, um alle von Ihnen genutzten Sicherheitstechnologien zu vereinen
- Nutzen Sie die von einer bestimmten Technologie bereitgestellten Sicherheitsdaten, um Downstream-Aktionen mit einer anderen Technologie anzuweisen.
- Verbessern Sie Ihre Cyber-Sicherheit, indem Sie Ihre MTTR (Mean-Time-To-Resolution) senken

Die wichtigste Überlegung bei der Bewertung von Lösungen zur Sicherheitsautomatisierung ist die „Möglichkeit zur Integration unserer Technologien“.
– ESG Research, 2016

Neben den wirtschaftlichen Vorteilen bietet die Nutzung einer SOAR-Plattform auch Vorteile bei Konsistenz, da dieselben Daten für jedes Ereignis erfasst werden und jedes Ereignis immer auf dieselbe Weise untersucht wird.

Der ROI für einen Phantom-Kunden

Viele Kunden denken bei der Bereitstellung einer SOAR-Plattform zunächst an Anwendungsfälle im Bereich „Incident Response (IR)“. Die Automatisierung der Untersuchung von vermeintlichen Phishing-E-Mails ist ein gängiges Szenario. Die Untersuchungen sind sehr repetitiv, folgen einem bekannten Prozess und erfordern ein hohes Arbeitsaufkommen auf Seite der Analysten, wenn sie manuell ausgeführt werden.

Einer der Splunk Phantom-Kunden verwendete die Plattform, um einen Prozess zu automatisieren, der manuell über 90 Minuten Zeitaufwand erforderte. An einem gewöhnlichen Tag gingen bei diesem Kunden ca. 45 Phishing-E-Mails ein, die das Sicherheitsteam untersuchen musste. Die standardmäßige Vorgehensweise bei solch einem Ereignis besteht aus einer Empfangsbestätigung an den Mitarbeiter, der Analyse der E-Mail auf böswillige Anzeichen und dem Ergreifen von Maßnahmen zur Abhilfe, sofern die E-Mail als zu einer Phishing-Kampagne gehörig eingestuft wird. Von Anfang bis Ende, kann dieser Prozess für jede vermeintliche Phishing-E-Mail über 90 Minuten in Anspruch nehmen.

Mit Hilfe der tatsächlichen Daten aus dieser Bereitstellung des Kunden und den geschätzten Lohnkosten für einen Tier-1 SOC-Analysten, können wir die Kosten für die manuelle Untersuchung und Reaktion auf Phishing-E-Mails berechnen:

Ausgangsdaten	
Anzahl von Phishing-E-Mails pro Tag	45
Geschätzter Zeitaufwand für die manuelle Bearbeitung jeder Phishing-E-Mail	90 Minuten
Durchschnittlicher Stundenlohn: Tier-1 SOC-Analyst[1]	39,65 $
Berechnungen:	
Tägliche Kosten für die Bearbeitung von Phishing-E-Mails	2.676 $
Jährliche Kosten für die Bearbeitung von Phishing-E-Mails[2]	695.760 $

1 Quelle: **https://www.glassdoor.com/Salaries/security-analyst-salary-SRCH_KO0,16.htm**

2 Ausgegangen wird von einer Fünftagewoche

Durch die Automatisierung wird der gesamte Prozess jetzt in weniger als einer Minute abgeschlossen. Das Team kann sich nun auch mit anderen Dingen als den routinemäßigen Untersuchungen beschäftigen, bei denen menschliche Eingriffe erforderlich sind. Diese 98 Prozent an Zeiteinsparungen bei der Bearbeitung einer Phishing-E-Mail, bedeuten **Kosteneinsparungen von über 680.000 US-Dollar pro Jahr.**

Womöglich rechtfertigen die potenziellen Einsparungen bei der Bearbeitung der Phishing-E-Mails an einem gewöhnlichen Tag bereits den Erwerb einer SOAR-Plattform – der erwartete ROI liegt jedoch weit höher.

Wie bereits erwähnt bearbeitete das Team routinemäßig täglich 45 Phishing-E-Mails – eine ziemlich hohe Arbeitslast für ein SOC-Team. Manchmal erlebt dieser Phantom-Kunde aber auch Burst-Attacken von bis zu 300 Phishing-E-Mails an einem einzigen Tag. Anhand der obigen Daten können wir auch den ROI bei der Bearbeitung von Burst-Attacken einschätzen.

Ausgangsdaten	
Anzahl von Phishing-E-Mails pro Tag – Burst-Attacke	300
Anzahl von Phishing-E-Mails pro Tag – Normale Bedingungen	45
Zusätzliche Phishing-E-Mails pro Tag – Burst-Attacke	255
Geschätzter Zeitaufwand für die manuelle Bearbeitung jeder Phishing-E-Mail	90 Minuten
Durchschnittlicher Stundenlohn: Tier-1 SOC-Analyst[1]	39,65 $
Berechnungen:	
Tägliche Kosten für die Bearbeitung zusätzlicher Phishing-E-Mails – Burst-Attacke	15.166$
Jährliche[2] Kosten für die Bearbeitung von Phishing-E-Mails – Burst-Attacke	363.984$
Jährliche[3] Kosten für die Bearbeitung von Phishing-E-Mails – Normale Bedingungen	695.760$
Jährliche Kosten für die Bearbeitung von Phishing-E-Mails insgesamt	1.059.744$

1. Quelle: **https://www.glassdoor.com/Salaries/security-analyst-salary-SRCH_KO0,16.htm**
2. Es wird von zwei Burst-Attacken pro Monat ausgegangen.
3. Aus Tabelle 1.

Mit denselben 98 Prozent Zeiteinsparungen bei der Bearbeitung einer Phishing-E-Mail, errechnen sich **Gesamteinsparungen von über 1 Million US-Dollar pro Jahr.** Da es nicht möglich ist, bei Burst-Attacken einfach erforderliche, zusätzliche Analysten einzustellen und das Team nicht über die notwendigen Kapazitäten verfügt, werden die meisten Phishing-E-Mails bei einer Burst-Attacke einfach ignoriert. Die wahren Kosten für ein Phishing-Problem können also viel höher liegen, wenn man die potenziellen Kosten für Sicherheitsverletzungen durch einen ungeprüften Incident mit einkalkuliert.

Dank der Automatisierung mit Phantom können wir E-Mail-Benachrichtigungen aufgrund von Malware in etwa 40 Sekunden verarbeiten, im Gegensatz zu den bisher üblichen über 30 Minuten.
– CISO, Blackstone

Welche anderen Anwendungsfälle sind wichtig?

Obwohl der Bereich „Incident Response“ bei SOAR-Plattformen ein durchaus häufiger Anwendungsfall ist, sind branchenführenden Plattformen wie Splunk Phantom für andere Anwendungsfälle offen und erweiterbar. Durch diese Flexibilität können SOC-Teams ganz einfach eine Vielzahl von Standardvorgehensweisen (Standard Operating Procedures, SOPs) automatisieren.

Teams kümmern sich anfangs häufig eher um Anwendungsfälle, die ihre größten Schmerzpunkte repräsentieren. Die Prozesse in solchen Anwendungsfällen bestehen oft aus vielen manuellen Aufgaben. Häufig ist eine abteilungs- und produktübergreifende Arbeit erforderlich, um ein einzelnes Playbook zu erstellen.

Der Kauf einer SOAR-Plattform lässt sich zwar meist schon mit nur einem einzigen Anwendungsfall rechtfertigen, dennoch ist es wichtig auch andere potenzielle Anwendungsfälle zu betrachten. Hieran sollten die wichtigsten Beteiligten aus Ihrem Security Operations-Team beteiligt sein. Das Entwickeln umfassender Anwendungsfälle für die IT-Sicherheit ist wichtig, um sicherzustellen, dass die Plattform, die Sie heute auswählen, auch künftige Anforderungen erfüllt und Ihren ROI optimiert.

Die folgenden Anwendungsfälle sind ebenfalls sehr geläufig und umfassen die Bereiche Untersuchung, Anreicherung, Schadensbegrenzung und Korrektur:

Alert Triage

Das Ziel von Alert Triage (zu deutsch etwa „Sichtung von Benachrichtigungen“) besteht darin, eingehende Benachrichtigungen zu prüfen und zu priorisieren. Anwendungsfälle, deren Schwerpunkt auf der Sichtung von Benachrichtigungen liegt, beinhalten zudem die Anreicherung von Ereignissen mit zusätzlichem Kontext. Sie können auch Logik umfassen, die die weitere Verarbeitung höchst verlässlicher False Positive-Benachrichtigungen verhindert.

Suche nach Kompromittierungsindikatoren (Indicator of Compromise, IOC)

Durch eine automatisierte Suche nach Kompromittierungsindikatoren können Teams die empfangenen Bedrohungsinformationen voll verwerten, anstatt die gesuchten IOCs aufgrund von Ressourcenbeschränkungen eingrenzen zu müssen. Sie könnten auch eine Informations-Bewertung implementieren, die sie bei der Entscheidung unterstützt, welche Quellen für Bedrohungsinformationen genutzt werden sollen.

Schwachstellenmanagement

Die Automatisierung des Zyklus aus Identifizierung, Klassifizierung, Behebung und Minimierung von Schwachstellen steigert nicht nur die Team-Effizienz, sondern führt auch zu konsistenteren Ergebnissen, indem sichergestellt wird, dass der Prozess jedes Mal auf die gleiche Weise ausgeführt wird.

Netzwerkzugriffsteuerung

SOAR-Plattformen können Strategien für eine dynamische Zugriffskontrolle verbessern. Ein Beispiel dafür ist die Integration eines Erkennungssystems, das bisher nicht Teil der Entscheidungslogik der Netzwerkzugriffsteuerung war.

Benutzerverwaltung

Wenn sichergestellt ist, dass Benutzer präzise, schnell und systematisch aktiviert und deaktiviert werden, kann dies verhindern, dass ein Benutzerkonto böswillig von einem Bedrohungsakteur genutzt wird.

Penetrationstest

Aktivitäten wie Asset-Erkennung, Klassifizierung und Zielpriorisierung können automatisiert werden. Dies steigert die Produktivität des Penetrations-Testteams.

Austausch von IT-Sicherheitsinformationen

Unternehmen mit Programmen zum Austausch von IT-Sicherheitsinformationen können von automatisierten Playbooks enorm profitieren. Die Automatisierung kann auch die Produktivität eines Analysten steigern und zeitkritische Informationen schneller als manuelle Prozesse an eine Community zurückgeben.

Jeder gut dokumentierte SOP, mit dem ein Security Operations-Team die Kriterien für die Automatisierung verschlüsseln kann, eignet sich für SOAR-Plattformen. Letztlich führt eine größere Sammlung automatisierter Playbooks zu einem noch besseren ROI, da die Kosten der Plattform über mehrere Anwendungsfälle amortisiert werden.

Schlussfolgerung

SOAR-Plattformen sorgen für hohe Umsatzzahlen und unterstützen Unternehmen dabei, smarter zu arbeiten. Durch die Automatisierung repetitiver Aufgaben können Teams schneller reagieren und die verwendete Arbeitszeit pro Ereignis durch die automatisierte Erkennung, Untersuchung und Reaktion senken. Die Verteidigung wird optimiert, indem die gesamte Sicherheitsinfrastruktur gemeinsam integriert wird, damit jeder Teil aktiv an der Verteidigungsstrategie teilnimmt.

Ganz egal, ob Sie mit einem gängigen Anwendungsfall aus der Kategorie „Incident Response“ beginnen, oder einen aus einer anderen Kategorie auswählen – in jedem Fall sollten Sie bei der Entscheidung Ihren ROI im Auge behalten.

Wenn Sie mehr über die Phantom-Plattform für die Sicherheitsautomatisierung und -orchestrierung erfahren möchten, **laden Sie die kostenlose** Phantom Community Edition herunter oder **wenden Sie sich an den Vertrieb**, um weitere Informationen zu erhalten.

splunk>

Weitere Informationen: www.splunk.com/asksales www.splunk.com.de

20-13326-SPLK-Measuring-the-ROI-of-Security-Operations-Platforms_DE-103-WP