splunk>

CASE STUDY

7 Minuten MTTD bei Phishing-Angriffen im Splunk-SOC mit Splunk Attack Analyzer und Splunk SOAR

Zentrale Herausforderungen

Jeden Monat überfluteten Hunderte von Phishing-Warnmeldungen die Splunk-SOC-Analysten. Dies zog die MTTR in die Länge und ließ wenig Zeit für eingehendere Untersuchungen.

Wichtige Ergebnisse

Mit Splunk Attack Analyzer hat das Incident-Response-Team nun mehr Kontext für Untersuchungen, sodass es Phishing-Meldungen 90 % schneller lösen und die Bedrohungsabwehr deutlich beschleunigen kann.

splunk>

Branche: Technologie

Lösungen: Security

Produkte: Splunk SOAR, Splunk Attack Analyzer

Splunk gehen alle Phishe ins Netz.

Phishing ist einer der häufigsten und finanziell schädlichsten Angriffsvektoren. 88 % der Unternehmen, die wir für unseren neuesten Lagebericht Security befragt haben, gehen davon aus, dass sich das Phishing-Problem durch generative KI in puncto Umfang und Effektivität noch weiter verschärfen wird. Wenn Mitarbeitende von Splunk eine verdächtige E-Mail erhalten, können sie diese dem Detection- und Response-Team von Splunk melden, um das Unternehmen vor Sicherheitsverletzungen zu schützen. Von den Hunderten Warnmeldungen, die das Team monatlich erhält, sind viele jedoch Fehlalarme. Nur wenige sind tatsächlich gefährlich. Um False Positives von echten Risiken unterscheiden zu können, muss das Team aber zunächst jede einzelne Meldung untersuchen.

Angesichts dieser Flut von Warnmeldungen brauchte das Splunk-Team eine praktikable Lösung und entschied sich für Splunk SOAR. Damit automatisierte es die Ticketerstellung und Informationsextraktion für eingehende E-Mail-Meldungen – ein guter Anfang, aber noch nicht gut genug, denn das Team wollte die Mean Time to Detect (MTTD) auf unter 7 Minuten senken. Dazu mussten auch Untersuchungen automatisiert werden. Und hier kam Splunk Attack Analyzer als zweite Lösung ins Spiel.

Ergebnisse

- 90 % schnellere Lösung von Phishing-Warnmeldungen
- Präzisere Phishing-Erkennung
- Schnellere Eindämmung von Cybersecurity-Bedrohungen

Früher stauten sich derart viele Phishing-bezogene Tickets, sodass das Erkennungs- und Incident-Response-Team mit der Bearbeitung kaum hinterherkam. Attack Analyzer beschleunigte den Untersuchungs- und Behebungsvorgang um sage und schreibe 90 %. Wird heute ein potenzieller Phishing-Angriff gemeldet, erstellt SOAR automatisch ein Ticket und leitet die verdächtige E-Mail zur Analyse an Attack Analyzer weiter. Attack Analyzer untersucht die gesamte Angriffskette und stuft den Schweregrad der Bedrohung auf einer Skala ein. Anschließend lädt es das Analyseergebnis und die dazugehörigen forensischen Daten ins Ticket hoch. Schon nach wenigen Minuten ist der ganze Prozess abgeschlossen. Dadurch können die Analysten in Splunks SOC-Team viel schneller auf Bedrohungen durch Phishing reagieren und das Risiko von Sicherheitsverletzungen und Ausfällen eindämmen.

Reaktion auf besonders schwerwiegende Vorfälle

Wer im Bereich Incident Response arbeitet, darf sich keine Fehltritte erlauben. Das und nicht weniger erwarten Unternehmen von ihren Cybersecurity-Profis. Umso mehr gilt dies für das Advanced-Threat-Response-Team von Splunk, das für die Abwehr der größten und schwerwiegendsten Angriffe auf das Unternehmen zuständig ist. Um Splunk vor Ungemach zu bewahren, arbeitet das zehnköpfige Team eng mit dem SOC und anderen internen Beteiligten zusammen. Wenn etwas schiefläuft, muss das Team die Auswirkungen auf Betrieb, Finanzen und Ansehen des Unternehmens minimieren und dafür sorgen, dass die gesamte Splunk-Belegschaft weiterarbeiten kann.

Um profundere Incident-Untersuchungen und mehr Analysen durchführen zu können, führte das Team kürzlich Splunk Attack Analyzer ein. Es ist mittlerweile zum Tool der Wahl für die Analyse verdächtiger Dateien und Domains avanciert. Mit Splunk Attack Analyzer kann das Team Vorfälle schneller erkennen und Risiken für das Unternehmen reduzieren. „Es hat uns bei den allerschwierigsten Vorfällen weitergeholfen“, sagt Tony Iacobelli, Senior Manager im Advanced-Response-Team von Splunk.

> Attack Analyzer ist eines der wenigen Tools, die unser Response-Team wirklich gerne nutzt. Das Team weiß, dass das Tool auch an der Belastungsgrenze noch funktioniert. Und wenn wir mit nebulösen, obskuren Problemen zu tun haben, gehört Attack Analyzer zu den ersten Tools, mit denen wir versuchen, Licht ins Dunkel zu bringen.“
>
> **Tony Iacobelli,** Senior Manager, Splunk Advanced Response

Seitdem das Advanced-Threat-Response-Team mit Splunk Attack Analyzer über ein starkes, automatisiertes Tool zur Bedrohungsanalyse verfügt, hat sich sein Erkennungsradius deutlich erweitert. Zuvor musste es sich ganz auf seine EDR-Lösung verlassen, um verdächtige Aktivitäten automatisch an der weiteren Ausführung zu hindern. Mit Attack Analyzer haben Analysten nun auch die Möglichkeit, Muster zu analysieren und nähere Informationen über die Angriffsquelle (z. B. Gefährdungsindikatoren und hostbasierte Artefakte) zu erhalten. Auf diese Weise lassen sich weitere verdächtige Aktivitäten aufspüren, die das EDR-System womöglich übersehen hätte. Mithilfe der interaktiven Detonationsmodi des Tools kann das Team zudem Malware untersuchen, ohne Gefahr zu laufen, die eigenen Geräte zu infizieren.

Diese neuen Funktionalitäten kamen für Splunk genau zur richtigen Zeit. „Wir waren gerade dabei, neue Anwendungsfälle einzuführen und zusätzliche Bereiche zu durchleuchten“, so Tony Iacobelli. „Leider können wir nicht ohne Weiteres unser Personal aufstocken, nur weil wir mehr Einblicke haben. Wir mussten also effizienter werden, um die Produktivität des Teams zu steigern. Und mithilfe von Attack Analyzer haben wir genau das erreicht.“ Attack Analyzer sorgte für effizientere Abläufe, sodass die Incident-Response-Teams von Splunk ihr ursprüngliches Ziel erreichen konnten: eine MTTD von unter 7 Minuten in kritischen Use Cases.

24-643263-Splunk-SOC-CS-103__DE