CrowdStrike Asset Graph hilft Unternehmen bei der proaktiven Identifizierung und Beseitigung von blinden Flecken auf der Angriffsfläche

CrowdStrike Asset Graph bietet eine einzigartige Übersicht über die Ressourcen in einer IT-Umgebung, um Cyber-Abwehrstrategien zu optimieren und Risiken zu verwalten

AUSTIN, Texas und RSA Conference 2022, SAN FRANCISCO – 8. Juni 2022 – CrowdStrike Holdings, Inc., ein führender Anbieter von Cloud-basiertem Schutz von Endgeräten, Workloads, Identitäten und Daten, hat CrowdStrike Asset Graph vorgestellt. Dabei handelt es sich um eine neue Graph-Datenbank, die auf der CrowdStrike Security Cloud basiert und IT- und Sicherheitsverantwortlichen einen 360-Grad-Blick auf alle Assets (sowohl verwaltete als auch nicht verwaltete) sowie einen einzigartigen Einblick in die Angriffsfläche von Geräte, Benutzer, Konten, Anwendungen, Cloud-Workloads, Betriebstechnologie (OT) und vieles mehr bietet, um den IT-Betrieb zu vereinfachen und Sicherheitsverletzungen zu verhindern.

Angesichts des beschleunigten digitalen Wandels in Unternehmen vergrößert sich auch deren Angriffsfläche exponentiell. Somit steigt auch das Risiko eines Angriffs durch Akteure an, die diese weichen Ziele und Schwachstellen mitunter schneller entdecken und ausnutzen, als IT- und Sicherheitsteams sie aufspüren können. Visibilität ist eines der Grundprinzipien der Cybersicherheit. Schließlich kann man keine Ressourcen schützen und verteidigen, von denen man nicht weiß, dass sie existieren. Dies wiederum führt zu einem Wettlauf zwischen Angreifern und den IT- und Sicherheitsteams von Unternehmen, mit dem Ziel, diese blinden Flecken zu finden. Laut eines Berichts der Enterprise Strategy Group (ESG) aus dem Jahr 2022 „haben 69 % der Unternehmen einen Cyberangriff erlebt, bei dem der Angriff selbst durch die Ausnutzung eines unbekannten, nicht oder schlecht verwalteten Internet-Assets begann."

CrowdStrike Asset Graph löst dieses Problem, indem es die komplexen Interaktionen zwischen Assets dynamisch überwacht und nachverfolgt, sodass ein einziger, ganzheitlicher Überblick über die von diesen Assets ausgehenden Risiken entsteht. Während andere Lösungen lediglich eine Liste von Assets ohne Kontext liefern, visualisiert Asset Graph grafisch die Beziehungen zwischen allen Assets wie Geräten, Benutzern, Konten, Anwendungen, Cloud-Workloads und OT, zusammen mit dem umfassenden Kontext, der für eine angemessene Sicherheitshygiene und ein proaktives Sicherheitsmanagement erforderlich ist, um das Risiko im Unternehmen zu reduzieren.

„Die digitale Transformation hat zu einer ebenso deutlichen Beschleunigung der Sicherheitstransformation in modernen Unternehmen geführt. In den Unternehmen, die auf diesem Weg am weitesten fortgeschritten sind, nähern sich die IT-Betriebs- und Sicherheitsteams - einst getrennte Silos - einander an und schaffen eine weitaus proaktivere Haltung, wenn es um Sicherheit und Risikomanagement geht", sagt Amol Kulkarni, Chief

Product and Engineering Officer bei CrowdStrike. „CrowdStrike Asset Graph wurde speziell für diese neue Dynamik entwickelt und gibt Unternehmen einen Überblick über ihre Assets und deren Interaktion untereinander. So können sie fundierte, risikobasierte Entscheidungen treffen, um ihre IT-Umgebung proaktiv zu schützen und zu verwalten - angefangen bei der Sicherheit bis hin zu IT-Performance, Auslastung, Kapazität, Lizenzmanagement und vieles mehr."

Die Kluft zwischen IT-Betrieb und Sicherheit überbrücken

Die CrowdStrike Falcon-Plattform wurde speziell mit einer Cloud-nativen Architektur entwickelt, um enorme Mengen an hochgradig zuverlässigen Sicherheits- und Unternehmensdaten zu nutzen und Lösungen über einen einzigen, schlanken Agenten bereitzustellen, damit Kunden den raffinierten Angreifern von heute einen Schritt voraus sind.

CrowdStrikes innovative Graphen-Technologien, die ihren Ursprung im renommierten Threat Graph haben, bilden eine leistungsstarke, nahtlose und verteilte Datenstruktur, die zu einer einzigen Cloud - der Security Cloud - verbunden ist und die Falcon-Plattform sowie die branchenführenden Lösungen von CrowdStrike antreibt. Dank einer Kombination aus künstlicher Intelligenz (KI) und Techniken zum Abgleich von Verhaltensmustern (Behavioral Pattern Matching) zur Korrelation und Kontextualisierung von Informationen in der riesigen Datenstruktur bieten die Graphen von CrowdStrike einen Ansatz zur Lösung der größten Probleme, mit denen die Kunden konfrontiert sind. Mit dem neu eingeführten Asset Graph setzt CrowdStrike auf den gleichen Ansatz, um die schwierigsten, ungelösten Herausforderungen seiner Kunden mit Blick auf proaktive Sicherheit sowie beispiellose IT-Transparenz und Risikomanagement zu lösen.

Folgende drei hochentwickelte Graphentechnologien bilden die Grundlage der Falcon-Plattform:

- **Threat Graph:** Der branchenführende Threat Graph von CrowdStrike nutzt Billionen von Sicherheitsdatenpunkten von Millionen von Sensoren, angereichert mit Bedrohungsdaten und Quellen von Drittanbietern, um Bedrohungsaktivitäten zu identifizieren und miteinander zu verknüpfen, um einen vollständigen Einblick in Angriffe zu gewährleisten und Bedrohungen automatisch und in Echtzeit für den weltweiten Kundenstamm von CrowdStrike zu verhindern.
- **Intel Graph:** Durch die Analyse und Korrelation enormer Datenmengen über Angreifer, ihre Opfer und ihre Tools bietet Intel Graph einzigartige Einblicke in die Veränderungen von Taktiken und Techniken und ergänzt so den auf Angreifer ausgerichteten Ansatz von CrowdStrike mit erstklassigen Bedrohungsdaten.
- **Asset Graph:** In diesem Release löst CrowdStrike eines der komplexesten Kundenprobleme von heute: Die genaue Identifizierung von Assets, Identitäten und Konfigurationen über alle Systeme - einschließlich Cloud, On-Premise, Mobile, Internet of Things (IoT) und andere - und deren Verknüpfung in Form eines Graphen. Die Vereinheitlichung und Kontextualisierung dieser Informationen wird zu neuen leistungsstarken Lösungen führen, die die Art und Weise verändern, wie Unternehmen ihre Sicherheitshygiene umsetzen und ihre Sicherheitslage dynamisch verwalten.

CrowdStrike Asset Graph ermöglicht neue Falcon-Module und darauf aufbauende Funktionen zur Definition, Überwachung und Erkundung der Beziehungen zwischen Assets innerhalb einer Organisation. Das erste Modul von Falcon, das Asset Graph nutzt, ist Falcon Discover (Sicherheitshygiene), das die folgenden Erweiterungen umfasst:

- **Verbesserte Dashboards, hochgradig anpassbare Filter und Freigabeoptionen:** Mit Hilfe von Asset Graph können IT-Teams die Kartenvisualisierung und die leistungsstarken Suchfunktionen individuell anpassen, die alle bequem in der Falcon Discover-Konsole dargestellt werden.
- **Neue Integration von Drittanbieterdaten mit ServiceNow:** Durch die Kombination dieser Integration mit Asset Graph und Falcon Discover erhalten IT-Teams eine weitere Ebene der Asset-Transparenz für Geräte in einer einzigen Konsole, die eine verbesserte Überwachung von nicht verwalteten und nicht unterstützten Assets ermöglicht.

„Nicht ohne Grund heißt es, man kann nicht schützen, was man nicht sieht. Der erste Schritt bei der Bekämpfung von Schatten-IT oder dem Aufdecken blinder Flecken besteht darin, zu verstehen, welche Assets man sichern muss und wie diese mit unvorhergesehenen unsicheren Assets interagieren“, sagt Juan Jose Chang, CISO bei Bladex. „Wir glauben, dass Falcon Discover in Kombination mit CrowdStrike Asset Graph den Unterschied zwischen einem Taschenlampenlicht und einer ganzen Straßenbeleuchtung ausmacht, um zu erkennen, wohin man geht.“

Weitere Informationen zu CrowdStrike Asset Graph und den Erweiterungen von Falcon Discover finden Sie in diesem Blog.

Über CrowdStrike
CrowdStrike Holdings Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Plattform zum Schutz von Workloads, Endgeräten, Identitäten und Daten die Sicherheit im Cloud-Zeitalter neu.

Dank der CrowdStrike Security Cloud und erstklassiger künstlicher Intelligenz kann die CrowdStrike Falcon®-Plattform Echtzeit-Angriffsindikatoren, Bedrohungsdaten, sich ständig weiterentwickelnde Methoden der Gegner sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen nutzen, um hochpräzise Detektionen, eine automatisierte Schutz- und Abhilfemaßnahme, erstklassiges Threat Hunting und eine nach Prioritäten geordnete Beobachtung von Schwachstellen zu ermöglichen.

Die speziell für die Cloud entwickelte Falcon-Plattform verfügt über einen einzigen, schlanken Agenten und bietet eine schnelle und skalierbare Implementierung, ausgezeichneten Schutz und Leistung bei geringerer Komplexität und schneller Wertschöpfung.

Das Motto von CrowdStrike lautet: Wir verhindern Sicherheitsvorfälle.

Mehr Informationen finden Sie unter: https://www.crowdstrike.de
Folgen Sie uns: Blog | Twitter | LinkedIn | Facebook | Instagram
Jetzt kostenlos testen: https://www.crowdstrike.com/free-trial-guide/

Für weitere Informationen kontaktieren Sie bitte:
HARVARD ENGAGE! COMMUNICATIONS GMBH
Oliver Salzberger / Ava Dühring
Tel: +49 89 53 29 57 23
E-Mail: crowdstrike@harvard.de