CrowdStrike stellt Humio for Falcon vor

Humio for Falcon bietet eine langfristige, kosteneffiziente Datenspeicherung mit leistungsstarker indexfreier Suche und Analyse von angereicherten Sicherheitstelemetrien in Unternehmensumgebungen

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 Humio for Falcon vorgestellt. Humio for Falcon ist eine neue Funktion, mit der die Datenaufbewahrung von CrowdStrike Falcon-Telemetriedaten für einen Zeitraum von einem Jahr oder mehr verlängert werden kann, wodurch Unternehmen ihre Fähigkeiten zur Analyse von Bedrohungen und zur Bedrohungsjagd verbessern und gleichzeitig Compliance-Anforderungen einhalten können.

Humio for Falcon verbindet die branchenführende Sicherheitsplattform CrowdStrike Falcon mit den leistungsstarken Suchfunktionen von CrowdStrikes zentralem Logging-Angebot Humio. Die neue Funktion gibt Sicherheitsteams die Möglichkeit, Sicherheits- und IT-Telemetriedaten von der Falcon-Plattform zu speichern, die über Endpunkte, Workloads und Identitäten hinweg angereichert und kontextualisiert werden, um die Herausforderung der Operationalisierung der ständig wachsenden Datenmengen zu bewältigen. Humio for Falcon hilft Sicherheitsteams, alle Daten in ihrer Umgebung zu analysieren und darauf zu reagieren, und das sowohl in Echtzeit als auch auf Basis historischer Daten. Dank der längeren Datenaufbewahrung durch die fortschrittliche Komprimierung der aufgenommenen Daten können Sicherheitsteams potenzielle Bedrohungen in ihren Umgebungen mit tiefgreifenden, kontextbezogenen Analysen und Suchergebnissen jeglicher Größenordnung im Sekundentakt durch eine moderne, indexfreie Architektur aufdecken und erkennen.

„Während das Datenvolumen, das Bedrohungsjägern und Incident Respondern zur Verfügung steht, exponentiell wächst, sind sie routinemäßig gezwungen, die Dauer der Speicherung dieser Informationen zu reduzieren“, sagt Michael Sentonas, Chief Technology Officer bei CrowdStrike. „Humio for Falcon löst dieses Problem, indem es eine skalierbare und kosteneffiziente Datenspeicherung bietet, die es Bedrohungsjägern und Incident Respondern ermöglicht, zurückzublicken und zu prüfen, ob und wann ein Angreifer in einer IT-Umgebung aktiv war und jedes System, das er berührt hat, abzugleichen. Das ist wirklich ein Wendepunkt in der Branche.“

Humio for Falcon bietet:

- **Threat Hunting und Fehlerbehebung** in noch nie dagewesenem Umfang: Durch die längere Aufbewahrung von Falcon-Daten können Sicherheitsteams proaktiv nach versteckten Bedrohungen in der Umgebung suchen und diese sekundenschnell aufdecken. Sie können Advanced Persistent Threats (APTs) entfernen, indem sie die Daten durchforsten, um Unregelmäßigkeiten zu erkennen, die auf potenziell

bösartiges Verhalten hindeuten, und Schwachstellen besser priorisieren und beheben, bevor sie gefährlich werden können.

- **Längere Datenaufbewahrung zur Erfüllung von Compliance-Anforderungen bei gleichzeitig geringeren Kosten:** Mit skalierbarem Speicher und fortschrittlichen Komprimierungstechniken können Falcon-Daten je nach Kundenanforderung ein oder mehrere Jahre lang gespeichert und verwaltet werden. Diese Fülle an Echtzeit- und historischen Daten ermöglicht eine vollständige und genaue Untersuchung und Analyse, was zu einer schnelleren Behebung von Bedrohungen führt.
- **Die neue Benutzeroberfläche (UI) des Dashboards ermöglicht eine schnelle und individuelle Suche:** Dank der funktionsreichen Datenbankabfragesprache und der indexfreien Suche können Sicherheitsteams Anfragen an Falcon-Daten stellen und erhalten sofort Antworten. Sie haben zudem die Möglichkeit, umfangreiche Sicherheits- und IT-Telemetriedaten nahtlos zu erfassen, zu aggregieren und zu durchsuchen und wertvolle, kontextbezogene Einblicke mit Suchvorgängen mit einer Latenz von weniger als einer Sekunde zu gewinnen, um reale Sicherheitsanforderungen zu erfüllen, einschließlich fortschrittlicher Bedrohungs- und Schwachstellenuntersuchungen.

„Mit Humio for Falcon konnten wir im ersten Jahr rund 150.000 Dollar einsparen“, sagt Tom Sipes, Direktor für IT-Sicherheit und Compliance bei Tuesday Morning. „Die Möglichkeit, Daten über einen längeren Zeitraum zu speichern, ist von entscheidender Bedeutung. Sobald wir einen Hinweis auf eine Kompromittierung entdecken, können wir zeitlich zurückgehen und die gesamte Angriffskette analysieren, um Untersuchungen zu beschleunigen und Probleme schneller zu erkennen.“

Weitere Informationen zu Humio for Falcon finden Sie in diesem Blog.
Eine Humio for Falcon-Demo können Sie sich hier ansehen.
Wussten Sie schon, dass Humio mehr als ein Petabyte an Daten pro Tag aufnehmen kann? Humio wurde außerdem von den Data Breakthrough Awards für 2022 als „Log Analytics Solution of the Year“ ausgezeichnet.

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