
CrowdStrike gewinnt weitere strategische Partner für die CrowdXDR Alliance und baut die Falcon XDR-Funktionen aus

- *Menlo Security, Ping Identity und Vectra AI sind neue CrowdXDR-Allianzpartner*
- *Zu den neuen Funktionen von Falcon XDR gehört unter anderem die native Integration mit Falcon Fusion SOAR-Workflows zur Rationalisierung und Vereinfachung von Sicherheitsoperationen*

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, gab die Erweiterung der [CrowdXDR Alliance](#) um wichtige strategische Partner in den Bereichen Web- und E-Mail-Sicherheit (Menlo Security), Identitäts- und Zugriffsmanagement (Ping Identity) sowie Netzwerkerkennung und -reaktion (Vectra AI) bekannt. CrowdStrike stellte außerdem neue Funktionen für das [Falcon XDR](#)-Modul (Extended Detection and Response) vor, um die Erkennung für Sicherheitsteams zu beschleunigen. Dazu gehört auch eine Integration mit ServiceNow, einem bestehenden CrowdXDR Alliance-Partner, um die Arbeitsabläufe im Sicherheitsbereich durch die automatische Erstellung von Tickets stark zu vereinfachen.

Falcon XDR bietet folgende neue Funktionen:

- **Auf XDR-Erkennung basierende Falcon Fusion-Workflows:** [Falcon Fusion](#) (das SOAR-Framework von CrowdStrike) ist nativ in Falcon XDR integriert und automatisiert nun zahlreiche Arbeitsabläufe direkt auf Basis der Falcon XDR-Erkennung, darunter:
 - Ticket-Erstellung über ServiceNow, einem CrowdXDR Alliance-Partner.
 - Benachrichtigungen per E-Mail, Slack oder Webhook.
 - Incident-Details von Statusänderungen bis hin zu Teamzuweisungen und Kommentaren.
- **Zeitstrahl für XDR-Ereignisse:** Beschleunigung der Triage und Untersuchung mit einer Zeitstrahlansicht, die die wichtigsten Ereignisse einer Erkennung in chronologischer Reihenfolge anzeigt, um den Verlauf einer Aktivität leicht zu verstehen.
- **Grafische Visualisierung von benutzerdefinierten XDR-Erkennungen:** Erstellung benutzerdefinierter XDR-Erkennungen aus Abfragen, die zur Suche nach Bedrohungen in der Umgebung geschrieben wurden. Der Falcon XDR Graph Explorer visualisiert, wie die Ereignisse und Entitäten in einer benutzerdefinierten XDR-Erkennung zusammenhängen, sodass Sicherheitsanalysten sich schnell orientieren und Verbindungen in domänenübergreifenden Daten untersuchen können.

„CrowdStrike vereint weiterhin das Beste aus [offenen und nativen Ansätzen für XDR](#)“, sagt Michael Sentonas, Chief Technology Officer bei CrowdStrike. „Für Unternehmen, die einen offenen Ansatz bevorzugen, bauen wir die Unterstützung von Drittanbietern für die CrowdXDR

Alliance weiter aus, deren Ziel es ist, ein standardisiertes Schema für den Datenaustausch zur Anreicherung von XDR-Erkennungen bereitzustellen. Wir begrüßen Menlo Security, Ping Identity und Vectra AI in der CrowdXDR Alliance und freuen uns darauf, mit ihnen zusammenzuarbeiten, um Integrationen von Drittanbietern bereitzustellen. Für Unternehmen, die einen nativen Ansatz suchen, erweitern wir Falcon XDR um neue Funktionen, die die Erkennung von und Reaktion auf Bedrohungen über Datenquellen und Umgebungen hinweg beschleunigen. Damit bieten wir eine Lösung an, die es den Kunden ermöglicht, einen XDR-Ansatz zu wählen, der ihren Anforderungen am besten entspricht.“

Partnerzitate:

Poornima DeBolle, Mitgründerin und Chief Product Officer von Menlo Security: „Das Internet sollte für alle Arbeitnehmer sicher, nahtlos und effektiv sein. Cyberkriminelle erschweren dies jedoch, indem sie immer raffiniertere Malware einsetzen, darunter auch Ransomware, die von Highly Evasive Adaptive Threats angetrieben wird. Wir müssen verhindern, dass solche Malware und Zero Day Exploits jemals auf die Endgeräte gelangen. Menlo Security freut sich, der CrowdXDR Alliance von CrowdStrike beizutreten. Unsere Integration mit CrowdStrike Falcon XDR wird es Unternehmen ermöglichen, ein sicheres Online-Erlebnis zu bieten, ohne die Produktivität für die Sicherheit opfern zu müssen.“

Loren Russon, Vice President of Product Management bei Ping Identity: „Wir freuen uns, der CrowdXDR Alliance von CrowdStrike beizutreten und unsere gemeinsamen Lösungen weiter auszubauen. Kunden fordern ein umfangreiches Partner-Ökosystem mit einfach zu implementierenden Integrationen, und diese Partnerschaft bietet genau das durch unternehmenserprobte Identitätssicherheit zusammen mit umfassender Transparenz und Schutz vor Bedrohungen.“

Michael Porat, Senior Vice President, Corporate and Business Development bei Vectra AI: „Das Ausmaß und die Intensität von Cyberangriffen nehmen immer weiter zu und erinnern uns daran, dass Prävention allein Unternehmen nicht vor den heutigen kultivierten Angriffen schützen kann. Um moderne Sicherheitsbedrohungen erfolgreich abwehren zu können, müssen Unternehmen fortschrittlichere Mechanismen zur Erkennung von Bedrohungen und zur Reaktion darauf implementieren, die das Verhalten von Angreifern genau bestimmen und sie daran hindern, durch hybride Clouds zu navigieren. Wir freuen uns, der CrowdXDR Alliance von CrowdStrike beizutreten und unser Fachwissen im Bereich Bedrohungserkennung und -reaktion mit anderen angesehenen Sicherheitsanbietern zu teilen, da wir alle mit einem gemeinsamen Ziel zusammenarbeiten - bösartige Akteure zu erkennen und zu stoppen.“

Weitere Informationen über die CrowdXDR Alliance und Falcon XDR finden Sie [hier](#).

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/>

© 2022 CrowdStrike, Inc. Alle Rechte vorbehalten. CrowdStrike, das Falken-Logo, CrowdStrike Falcon und CrowdStrike Threat Graph sind eingetragene Marken von CrowdStrike, Inc. und beim Patent- und Markenamt der Vereinigten Staaten und in anderen Ländern registriert. CrowdStrike ist Eigentümer anderer Marken und Dienstleistungsmarken und kann die Marken Dritter zur Kennzeichnung ihrer Produkte und Dienstleistungen verwenden.

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