

CrowdStrike Falcon XDR ab sofort verfügbar

Falcon XDR vereint erstklassiges Threat Hunting, maschinelles Lernen (ML), künstliche Intelligenz (KI) und Angriffsindikatoren (IOAs) mit Datenquellen von Drittanbietern, um Ereignisse zu korrelieren und Echtzeit-Erkennung zu bieten.

Aachen – 7. Februar 2022 – [CrowdStrike Inc.](#), ein führender Anbieter von Cloud-basiertem Schutz von Endgeräten, Workloads, Identitäten und Daten, gibt die allgemeine Verfügbarkeit des [Falcon XDR](#)-Moduls bekannt. Es erweitert die [branchenführenden](#) Endgeräteerkennung und Reaktion (EDR)-Funktionen von CrowdStrike, um unternehmensweit die Transparenz von Bedrohungen zu verbessern, Sicherheitsabläufe zu vereinfachen und die benötigte Zeit für Reaktion, Eindämmung und Behebung der raffiniertesten Angriffe drastisch zu beschleunigen.

„Eine der Möglichkeiten, die Lücke bei den Cybersecurity-Fähigkeiten zu schließen, besteht darin, Sicherheitsteams in die Lage zu versetzen, effektiver zu arbeiten“, sagt Amol Kulkarni, Chief Product and Engineering Officer bei CrowdStrike. „Falcon XDR hilft, dieses Problem zu lösen, indem es schwache, isolierte Bedrohungssignale in priorisierte Warnungen von einer zentralen Konsole für Sicherheitsteams umwandelt, um sicherzustellen, dass ihre Untersuchungen sinnvoll und effizient sind.“

Falcon XDR bietet Sicherheitsteams folgende Fähigkeiten:

- **Vereinheitlichung von Sicherheitsdaten zur Erkennung und Reaktion.** Falcon XDR nimmt Daten von Drittanbietern (inklusive Netzwerksicherheit, E-Mail-Sicherheit, Websicherheit, Cloud-Sicherheit und Cloud Access Security Broker [CASB]), einschließlich der Partner der [CrowdXDR Alliance](#), auf und korreliert sie mit Daten aus der CrowdStrike Security Cloud, um die Echtzeiterkennung, die Untersuchung, Reaktion und Jagd nach Bedrohungen zu optimieren.
- **Schnelles Finden der richtigen Antworten.** Falcon XDR beschleunigt die Triage und Untersuchung für Security Operations Center (SOC)-Analysten und Threat Hunter, indem es eine zentrale Konsole für die genaue Priorisierung von Alarmen, eine flexible Suchplanung und Erkennungsanpassung, einen vollständigen Angriffskontext und eine interaktive Graphen-Visualisierung bereitstellt.
- **Umsetzung von XDR-Erkenntnissen in konkrete Maßnahmen.** Zur Orchestrierung und Automatisierung von Reaktionen über Sicherheits-Workflows hinweg ist [Falcon Fusion](#), ein SOAR-Framework (Security Orchestration, Automation and Response), nativ in die [Falcon-Plattform](#) integriert. Sicherheitsteams können die SOC- und IT-Effizienz verbessern, indem sie Echtzeit-Benachrichtigungs- und Reaktionsfunktionen zusammen mit anpassbaren Auslösern auf der Grundlage von Erkennungs- und Vorfallskategorien aufbauen. Falcon Fusion ist für CrowdStrike-Kunden kostenlos.
- **Effizientere SOC-Operationen.** Falcon XDR korreliert und liefert automatisch hochwertige Erkennungsdaten über den gesamten Security Stack hinweg. Durch die

Bereitstellung einer gemeinsamen Suchoberfläche direkt aus der CrowdStrike Security Cloud werden die Untersuchung und die Suche erheblich beschleunigt.

- **Verbesserung des ROI bestehender Sicherheitsinvestitionen.** Falcon XDR deckt verwertbare Erkenntnisse aus Daten auf, die zuvor in getrennten, nicht verbundenen Sicherheitsprodukten aus dem gesamten IT Stack enthalten waren.

„CrowdStrike hat jahrelang an der Entwicklung und Verfeinerung seiner Automatisierungsfunktionen für Erkennung und Reaktion gearbeitet“, erklärt Dave Gruber, Principal Analyst bei der Enterprise Strategy Group (ESG). „Da das Marktinteresse an XDR weiter zunimmt, ist CrowdStrike gut positioniert, um in den Bereich XDR zu expandieren und von seiner bestehenden, ausgereiften und skalierbaren EDR-Infrastruktur zu profitieren. Gleichzeitig investiert das Unternehmen in neue Datenerfassungs-, Analyse- und fortschrittliche Erkennungsfunktionen für Bedrohungen, die erforderlich sind, um auf eine immer komplexere Bedrohungslandschaft zu reagieren. CrowdStrikes auf Allianzen basierende XDR-Strategie sollte es CrowdStrike ermöglichen, Telemetriedaten aus einer breiten Palette von Sicherheitslösungen von Drittanbietern problemlos in seine Security Cloud aufzunehmen, was den Sicherheitsteams Flexibilität bei der Auswahl anderer zentraler Sicherheitskontrollen bietet.“

Weitere Informationen zu Falcon XDR finden Sie in unserem [Blog](#).

Um sich eine Falcon XDR-Demo anzusehen, klicken Sie bitte [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