CrowdStrike bietet eine vollständig integrierte Plattform zur Verhinderung von Sicherheitsverletzungen für Cloud-Workloads in AWS Cloud- und Edge-Umgebungen

CrowdStrike erweitert die Unterstützung für AWS Outposts und Amazon EKS Anywhere, um eine konsistente Sicherheit vom Edge bis zur Cloud zu gewährleisten, und führt neue AWS-Integrationen mit Humio ein

Aachen – 2. Dezember 2021 – CrowdStrike Inc., ein führender Anbieter von Cloud-basiertem Endpunkt- und Workload-Schutz, gibt neue Produktintegrationen und Zertifizierungen bekannt, die Schutz vor Sicherheitsverletzungen und Streaming-Erkennung bieten. Diese Lösungen bieten konsistente Sicherheit und vereinfachtes Betriebsmanagement über Amazon Web Services, Inc. (AWS) Cloud-to-Edge- und kundenverwaltete Infrastrukturen und brechen Silos zwischen IT-Sicherheits- und DevOps-Teams auf.

„Vielen Unternehmen fehlt es an Transparenz und optimierter Sicherheit, um ihre Cloud-Workloads präzise von Ende zu Ende zu schützen“, sagt Matthew Polly, Vice President of World Wide Alliances, Channels and Business Development bei CrowdStrike. „Mit diesen neuen Zertifizierungen und Integrationen erhalten gemeinsame Kunden einen konsistenten Sicherheitszustand und eine ganzheitliche Beobachtbarkeit ihrer Edge-Workloads, On-Premises-Rechenzentren und Cloud-nativen Implementierungen und schließen so die Lücke zwischen IT-Sicherheit und DevOps.“

Der erweiterte CrowdStrike-Support umfasst neue Produktintegrationen, AWS-Zertifizierungen und die Teilnahme als Launch-Partner für die folgenden AWS-Programme:

- **EKS Anywhere Support -** CrowdStrike bietet kontinuierliches Posture Management und Schutz vor Sicherheitsverletzungen für Amazon Elastic Kubernetes Service (EKS), Amazon EKS mit AWS Fargate und jetzt auch Amazon EKS, das über Amazon EKS Anywhere auf der lokalen Infrastruktur der Kunden läuft. Kunden profitieren von höherer Transparenz, Compliance und einer der branchenweit schnellsten Bedrohungserkennung und -reaktion, um Angreifer zu überlisten.

- **AWS Outposts Launch Partner -** IDC prognostiziert, dass bis 2024 aufgrund der explosionsartigen Zunahme von Edge-Daten 65 Prozent der Forbes Global 2000-Unternehmen Edge-First-Data-Stewardship-, Sicherheits- und Netzwerkpraktiken in ihre Datenschutzpläne einbinden werden.[1] CrowdStrike ist stolz darauf, Launch Partner von AWS Outposts zu sein, das die Formfaktoren 1U, 2U und 42U umfasst. Den Kunden wird ein einheitliches Sicherheitserlebnis über AWS-unterstützte On-Premise Edge-, Rechenzentrums- und Cloud-native Services hinweg geboten.

[1] *IDC FutureScape: Worldwide Future of Digital Infrastructure 2022 Predictions* (IDC #US47441321, October 2021)

- **AWS Quick Starts für Humio -** Kunden können Humio-Cluster über AWS Quick Starts-Vorlagen initiieren. Dadurch werden Dutzende von manuellen AWS-Verfahren auf wenige Schritte reduziert, so dass Kunden innerhalb weniger Minuten die konsistente Streaming-Erkennung von Humio in großem Umfang erreichen können.

- **Humio-Integration mit AWS FireLens -** Kunden können nun AWS-Service- und Ereignisdaten über AWS FireLens, den Container-Log-Router für Amazon Elastic Container Service (Amazon ECS) und AWS Fargate, in Humio einlesen. Humio-Kunden haben nun umfassendere Erweiterungsmöglichkeiten, um die Breite der AWS-Dienste zu nutzen, um die Weiterleitung von Protokollen an Humio zu vereinfachen, was eine beschleunigte Bedrohungsjagd und Suche nach neuartigen und fortgeschrittenen Cyber-Bedrohungen in ihrer AWS-Umgebung ermöglicht.

- **AWS Well Architected ISV-Zertifizierung erreicht -** CrowdStrike wurde erfolgreich von AWS geprüft und hat damit die Zertifizierung als AWS Well Architected ISV erhalten. Damit hat CrowdStrike bewiesen, dass es die Best Practices von AWS anwendet, verbesserte Sicherheits- und Leistungsergebnisse erzielt, Cloud-native Architekturen einsetzt und die Branchenkonformität im großen Maßstab erreicht.

Weitere Informationen finden Sie im AWS Marketplace oder auf der Website von CrowdStrike.

Über CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Plattform zum Schutz von Workloads und Endgeräten die Sicherheit im Cloud-Zeitalter neu. Die schlanke Single-Agent-Architektur der CrowdStrike Falcon®-Plattform nutzt Cloud-skalierte Künstliche Intelligenz und sorgt unternehmensweit für Schutz und Transparenz. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit täglich und in Echtzeit circa 1 Billion endpunktbezogene Ereignisse. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cybersicherheit.

Mit der Cloud-nativen Falcon-Plattform von CrowdStrike können sich Kunden umfassender schützen, ihre Performance steigern und eine sofortige Wertschöpfung erreichen.

Das Motto von CrowdStrike lautet: Wir verhindern Sicherheitsvorfälle.

Berechtigte Organisationen können vollständigen Zugang zu Falcon Prevent™ erhalten, indem sie eine kostenlose Testphase starten.

Mehr Informationen finden Sie unter: https://www.crowdstrike.de

Folgen Sie uns: Blog | Twitter

Pressemitteilung

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