CrowdStrike stellt neue, Gegner-fokussierte CNAPP-Funktionen vor

Die Falcon-Plattform bietet Unternehmen dank agentenbasierter und agentenloser Cloud-Sicherheit die notwendige Flexibilität zur Sicherung ihrer Cloud-Umgebungen

Aachen – 27. April 2022 – CrowdStrike (Nasdaq: CRWD), ein führender Anbieter von Cloud-basiertem Schutz von Endgeräten, Workloads, Identitäten und Daten, stellt neue, Gegner-fokussierte Cloud Native Application Protection Platform (CNAPP)-Funktionen vor, um das Threat Hunting für Cloud-Umgebungen und -Workloads zu beschleunigen und die durchschnittliche Reaktionszeit zu verkürzen. Die neuen Funktionen werden über die Falcon-Plattform bereitgestellt und führen die CrowdStrike-Module Falcon Horizon (Cloud Security Posture Management oder CSPM) und Falcon Cloud Workload Protection (CWP) innerhalb eines gemeinsamen Dashboards zusammen. Dadurch werden Sicherheits- und DevOps-Teams dabei unterstützt, die wichtigsten Cloud-Sicherheitsprobleme zu priorisieren, Runtime-Bedrohungen zu bekämpfen und das Threat Hunting innerhalb der Cloud zu ermöglichen. Die Updates umfassen auch neue Möglichkeiten zur Verwendung von Falcon Fusion (CrowdStrikes SOAR-Framework) zur Automatisierung von Behebungen für Amazon Web Services (AWS), neue benutzerdefinierte Indikatoren für Fehlkonfigurationen (IOMs) für Google Cloud Platform (GCP), neue Möglichkeiten zur Abwehr von identitätsbasierten Bedrohungen für Microsoft Azure und vieles mehr.

CrowdStrikes Gegner-fokussierter CNAPP-Ansatz bietet sowohl agentenbasierte (Falcon CWP) als auch agentenlose (Falcon Horizon) Lösungen innerhalb der Falcon-Plattform. Dadurch erhalten Unternehmen die notwendige Flexibilität, zu entscheiden, wie sie ihre Cloud-Anwendungen über die Continuous Integration/Continuous Delivery (CI/CD)-Pipeline und die Cloud-Infrastrukturen von AWS, Azure und GCP am besten absichern können. Ein zusätzlicher Vorteil der CWP-Lösung ist die Ermöglichung von Pre-Runtime- und Runtime-Schutz, im Gegensatz zu rein agentenlosen Lösungen, die nur eingeschränkte Transparenz und keine Abhilfemöglichkeiten bieten.

„Der Unterschied zwischen CrowdStrike und anderen Anbietern ist, dass wir sowohl agentenbasierte als auch agentenlose Optionen anbieten, die Unternehmen umfassende Transparenz, Erkennungs- und Abhilfemöglichkeiten bieten, um ihre Cloud-Infrastrukturen abzusichern“ so Amol Kulkarni, Chief Product and Engineering Officer bei CrowdStrike. „Zusätzlich bieten wir Unternehmen, dank Echtzeit-Warnungen und Berichten zu mehr als 150 Cloud-Angreifern, Schutz vor Sicherheitsverletzungen für Cloud-Workloads, Container und Kubernetes in Multi-Cloud- und Hybrid-Cloud-Umgebungen. Unser auf Angreifer fokussierter CNAPP-Ansatz, der auf unserer branchenführenden Threat Intelligence basiert, stellt sicher, dass Unternehmen bestens gerüstet sind, um Cloud-Angriffe zu stoppen.“

Die auf Angreifer fokussierten CNAPP-Funktionen von CrowdStrike umfassen folgendes:

Neue zentralisierte Konsole für Falcon Horizon und Falcon CWP

- **Dashboard für Cloud-Aktivitäten.** Vereinigen Sie die CSPM-Einblicke von Falcon Horizon mit dem Workload-Schutz von Falcon CWP in einer zentralen Benutzererfahrung, um die wichtigsten Probleme zu priorisieren, Runtime-Bedrohungen zu adressieren und die Suche nach Cloud-Bedrohungen zu ermöglichen. So werden Untersuchung und Reaktion beschleunigt.

Neue Funktionen für Falcon Horizon

- **Benutzerdefinierte Indikatoren für Fehlkonfigurationen (IOMs) für AWS, Azure und GCP.** Stellen Sie sicher, dass jede Cloud-Bereitstellung mit benutzerdefinierten Richtlinien versehen ist, die auf die Unternehmensziele abgestimmt sind.

- **Identitätszugriffsanalyse für Azure.** Verhindern Sie identitätsbasierte Bedrohungen und stellen Sie sicher, dass Azure AD-Gruppen, -Benutzer und -Apps über Berechtigungen verfügen, die nach dem Prinzip der geringsten Berechtigung durchgesetzt werden. Diese Funktion erweitert die bestehende Identity Access Analyzer-Funktion von Falcon Horizon für AWS.

- **Individuelle IOMs für GCP.** Stellen Sie mit auf die Unternehmensziele abgestimmten individuellen Richtlinien sicher, dass Security Teil jeder Cloud-Bereitstellung ist. Diese Funktion erweitert die bestehenden benutzerdefinierten IOM-Funktionen von Falcon Horizon für AWS und Azure.

Neue Fähigkeiten für Falcon CWP

- **Falcon Container-Erkennung.** Schützen Sie sich automatisch vor Malware und fortschrittlichen Bedrohungen, die auf Container abzielen, dank maschinellem Lernen (ML), künstlicher Intelligenz (KI), Angriffsindikatoren (IOAs), umfassender Kernel-Transparenz, benutzerdefinierten Kompromissindikatoren (IOCs) und Verhaltensblockierung.

- **Erkennung von Rogue-Containern.** Halten Sie Ihr Inventar aktuell, wenn Container bereitgestellt und außer Betrieb genommen werden. Scannen Sie Rogue-Images und identifizieren und stoppen Sie Container, die als privilegiert oder beschreibbar gestartet wurden, da diese als Einstiegspunkte für Angriffe genutzt werden können.

- **Verhinderung von Drift-Containern.** Entdecken Sie neue Binärdateien, die zur Laufzeit erstellt oder geändert werden, um Unveränderlichkeit des Containers zu schützen.

„Einer der großen Vorteile ist, dass CrowdStrike seine Cloud-Sicherheitsangebote wie Falcon Horizon, mit dem wir unsere Cloud-Umgebung überwachen und Fehlkonfigurationen,

Schwachstellen und Sicherheitsbedrohungen erkennen, ständig erneuert und verbessert“, so Dave Worthington, General Manager of Digital Security and Risk bei Jemena. „CrowdStrikes CNAPP bietet einen tiefgehenden und genauen Einblick in die Cloud-Bedrohungslandschaft, wodurch sie sich von der Konkurrenz abhebt.

„Wir sind von CrowdStrikes Leistung überwältigt, da die CPU-Auslastung minimal ist und die Systemleistung nur geringfügig beeinträchtigt wird. Mit Falcon Horizon sind wir in der Lage, Sicherheitslücken zu eliminieren indem wir unsere Cloud-Umgebung kontinuierlich auf Fehlkonfigurationen überprüfen“, so Jason Waits, Director of Cyber Security bei Inductive Automation. „Wir glauben, dass CrowdStrike durch die Erweiterung der Falcon-Plattform zur Unterstützung von CNAPP eine umfassende Cloud-Sicherheit mit Funktionen bietet, die kein anderer Anbieter bieten kann.“

„CrowdStrikes Fähigkeit, eine gegnerische Perspektive auf Cloud-Angriffsketten zu liefern unterstützt die strategische Notwendigkeit für Unternehmen, ihr Bedrohungsmodell zu aktualisieren und ihren Cloud-Footprint zu berücksichtigen“, so Doug Cahill, Vice President, Analyst Services and Senior Analyst bei der Enterprise Strategy Group (ESG). „Zusätzlich erfordert die Zunahme von Cloud-Bedrohungen einen umfassenden Ansatz für die Cloud-Sicherheit. CrowdStrike ist gut positioniert, diesen Bedarf mit der Falcon Plattform zu bedienen, die agentenbasierte und agentenlose Lösungen umfasst und eine durchgängige Sicherheit vom Code bis zur Laufzeit bietet.“

Alle CNAPP-Fähigkeiten stehen ab Mai Kunden zur Verfügung.

Zusätzliche Informationen

- Weitere Informationen über CrowdStrikes Gegner-fokussierten CNAPP-Ansatz finden Sie in unserem Blog.
- CrowdStrike wurde kürzlich im Bericht „The Forrester Wave™: Cloud Workload Security, Q1 2022“ als „Strong Performer“ 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