CrowdStrike stellt den branchenweit ersten Cloud Threat Hunting Service vor, um fortschrittliche Cloud-basierte Angriffe zu stoppen

Mit Falcon OverWatch Cloud Threat Hunting erhalten Unternehmen Zugang zu einem Eliteteam von Threat Huntern, um Vorfälle in Cloud-Umgebungen zu verhindern.

AUSTIN, Texas und AWS re:inforce 2022, Boston – 26. Juli 2022 – CrowdStrike, ein führender Anbieter von Cloud-basiertem Schutz von Endgeräten, Workloads, Identitäten und Daten, hat heute Falcon OverWatch Cloud Threat Hunting vorgestellt. Dabei handelt es sich um den branchenweit ersten eigenständigen Threat Hunting Service für versteckte und hochentwickelte Bedrohungen, die in Cloud-Umgebungen entstehen, operieren oder bestehen. Ausgestattet mit den branchenweit ersten Cloud-orientierten Angriffsindikatoren (Indicators of Attack, IOAs) für die Steuerungsebene und detaillierte gegnerische Vorgehensweisen, bietet OverWatch Cloud Threat Hunting einen einzigartigen Einblick in Cloud-Umgebungen, um die raffiniertesten Cloud-Bedrohungen zu beobachten und letztendlich zu stoppen.

Die rasche Einführung von Cloud-nativen Architekturen hat neue, breitere Angriffsflächen geschaffen, die Sicherheitsteams oft im Dunkeln tappen lassen, da sie weder den Überblick haben noch über die erforderlichen Fähigkeiten verfügen, um rund um die Uhr nach fortschrittlichen Bedrohungen in diesen komplexen Cloud-Umgebungen zu suchen. Folglich können Angreifer Cloud-Ressourcen schneller finden und ausnutzen, als Sicherheitsteams sie entdecken können.

Durch den Einsatz der agentenbasierten und agentenlosen Cloud Native Application Protection Platform (CNAPP) von CrowdStrike können Falcon OverWatch Cloud Threat Hunter verdächtige und anormale Verhaltensweisen sowie neuartige Angriffstechniken untersuchen. Falcon OverWatch Cloud Threat Hunting ist rund um die Uhr und an 365 Tagen im Jahr im Einsatz und kann Vorfälle und Sicherheitsverletzungen verhindern, indem es Kunden proaktiv vor Cloud-basierten Angriffen warnt, einschließlich:

- Angriffsaktivitäten, die innerhalb und über die Cloud-Infrastruktur von Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure und anderen Cloud-Service-Anbietern stattfinden.
- Anspruchsvolle Hands-on-Keyboard-Aktivitäten und Zero-Days, die Cloud-Workloads und Container in der Produktion ausnutzen und kompromittieren.
- Cloud-basierte IOAs, wie z.B. Schwachstellen in der Steuerebene sowie serverlose Schwachstellen, Fehlkonfigurationen, Anomalien im Anwendungsverhalten, Container-Ausbrüche, Privilegieneskalation, Kompromittierung von Knoten und mehr.
- Angriffspfade, die zunächst traditionelle IT-Ressourcen ausnutzen, um sich einen ersten Zugang zu verschaffen und dann auf Anwendungen, Systeme und Daten in der Cloud überzugehen.

„CrowdStrike hat Pionierarbeit geleistet, indem es branchenführende Technologie mit proaktivem Threat Hunting kombiniert hat, um einen wirklich umfassenden Schutz zu bieten, der die Lücke zwischen Erkennung und Reaktion schließt“, sagt Shawn Henry, Chief Security Officer and President of CrowdStrike Services. „Wir setzen diese Vorreiterrolle auch bei Falcon OverWatch Cloud Threat Hunting ein und bieten damit einen neuen Cloud-spezifischen Service, den kein anderer Anbieter leisten kann. Auf diese Weise erhalten Unternehmen einen rund um die Uhr Zugang zur Cloud-Expertise, ohne die hohen Gemeinkosten oder die erforderlichen Investitionen in Personal, Schulungen und Tools, die für die erfolgreiche Bekämpfung von Angreifern erforderlich sind. Wir glauben, dass Falcon OverWatch Cloud Threat Hunting ein starker Multiplikator für Unternehmen ist, die einen dedizierten Service zum Schutz ihrer Cloud-Umgebungen suchen.“

„Hervorragende Threat Hunting-Expertise ist schwer zu finden und zu halten. Falcon OverWatch stellt daher eine nahtlose Erweiterung unseres Sicherheitsteams dar, um anspruchsvolle Cloud-Bedrohungen zu erkennen und zu stoppen“, sagt Michael Sherwood, CIO der Stadt Las Vegas. „Da wir uns von physischer Hardware wegbewegen und zunehmend auf virtuelle und Cloud-basierte Systeme setzen, suchen wir nach Partnern, die über die Fähigkeiten und Technologien verfügen, um diesen Übergang zu unterstützen. CrowdStrike hat es uns ermöglicht, diese Umstellung sicher zu vollziehen. Durch die Kombination von Automatisierung und menschlicher Intelligenz können wir Bedrohungen effektiv und in Echtzeit abwehren.“

„Die Komplexität der Cloud nimmt nicht ab und die Angriffsfläche wächst exponentiell, was sich die Angreifer zunutze machen“, sagt Craig Robinson, Research Vice President, Security Services bei IDC. „Die richtige Technologie und die richtigen Prozesse sind zwei zentrale Säulen der Cybersicherheit, aber Unternehmen brauchen zugleich auch die richtige Expertise, um anspruchsvolle Cloud-Bedrohungen zu bekämpfen.“

Für weitere Informationen zu Falcon OverWatch Cloud Threat Hunting besuchen Sie bitte unsere Website.

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 Angreifer sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen nutzen, um hochpräzise Detektionen, automatisierte Schutz- und Abhilfemaßnahmen, 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