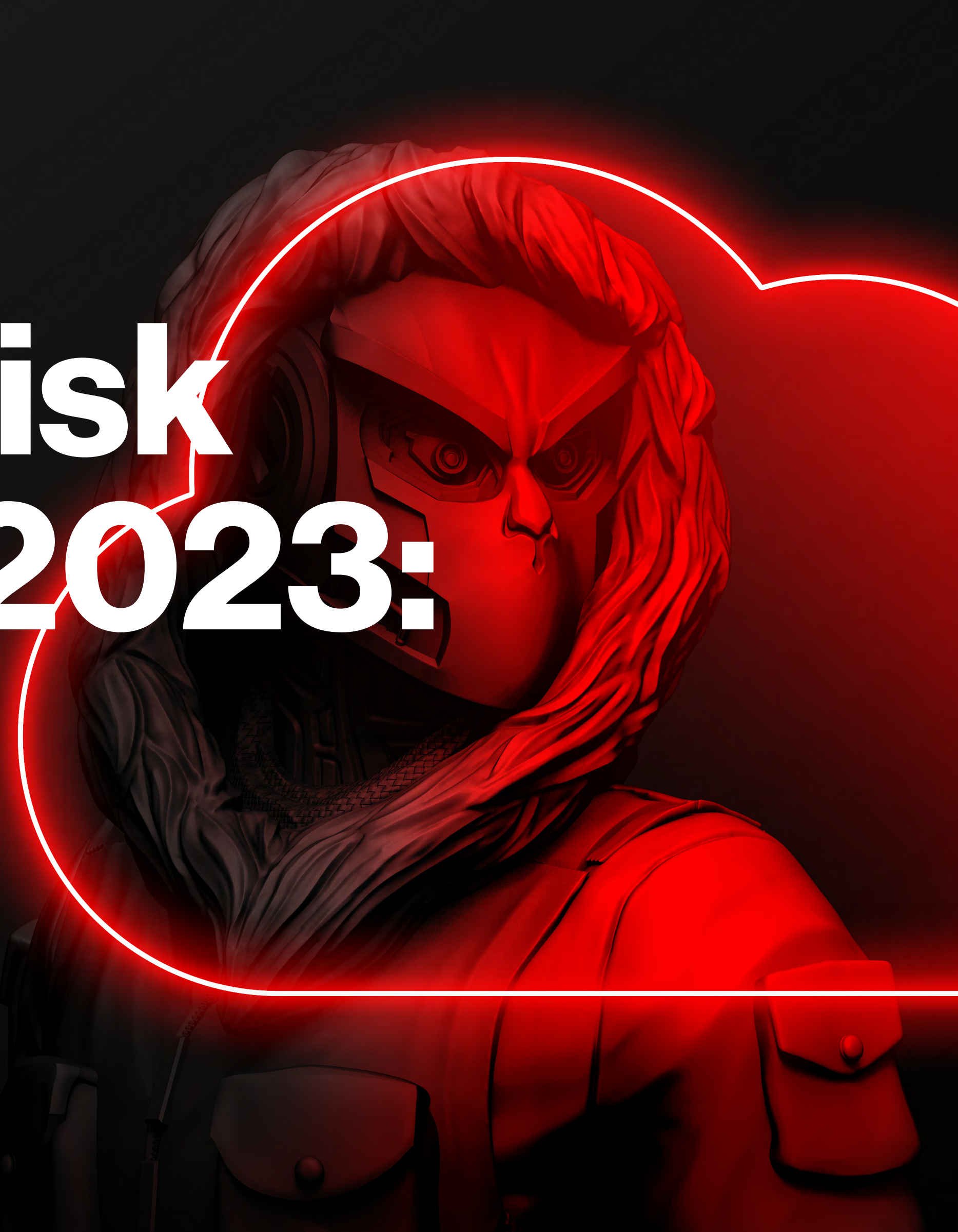
CROWDSTRIKE

Cloud Risk Report 2023:

Lernen Sie Angreifer und ihre Taktiken für Cloud-Angriffe kennen



95 %

Zunahme von Cloud-Exploits

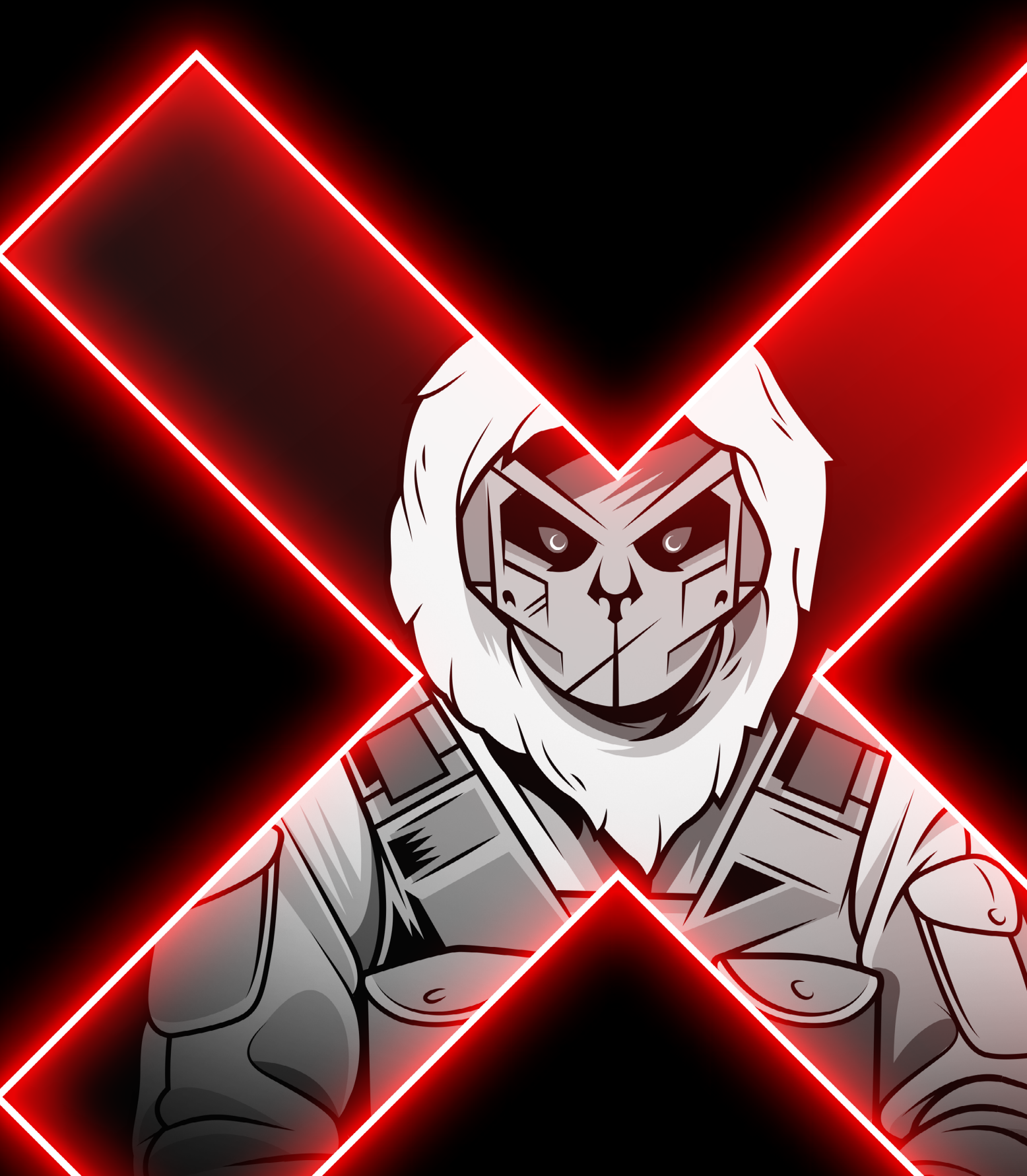
300 %

Steigerung bei Vorfällen mit cloudorientierten Bedrohungsakteuren

Angreifer optimieren ihre cloudbezogenen TTPs

Zahlreiche Angreifergruppen, darunter **COZY BEAR** (mit Verbindung nach Russland), **SCATTERED SPIDER** (Cyberkriminalität), **LABYRINTH CHOLLIMA** (mit Verbindung nach Nordkorea) und **COSMIC WOLF** (mit Verbindung zur Türkei) starten immer raffiniertere sowie aggressivere Angriffe gegen Ziele in der Cloud.

COZY BEAR

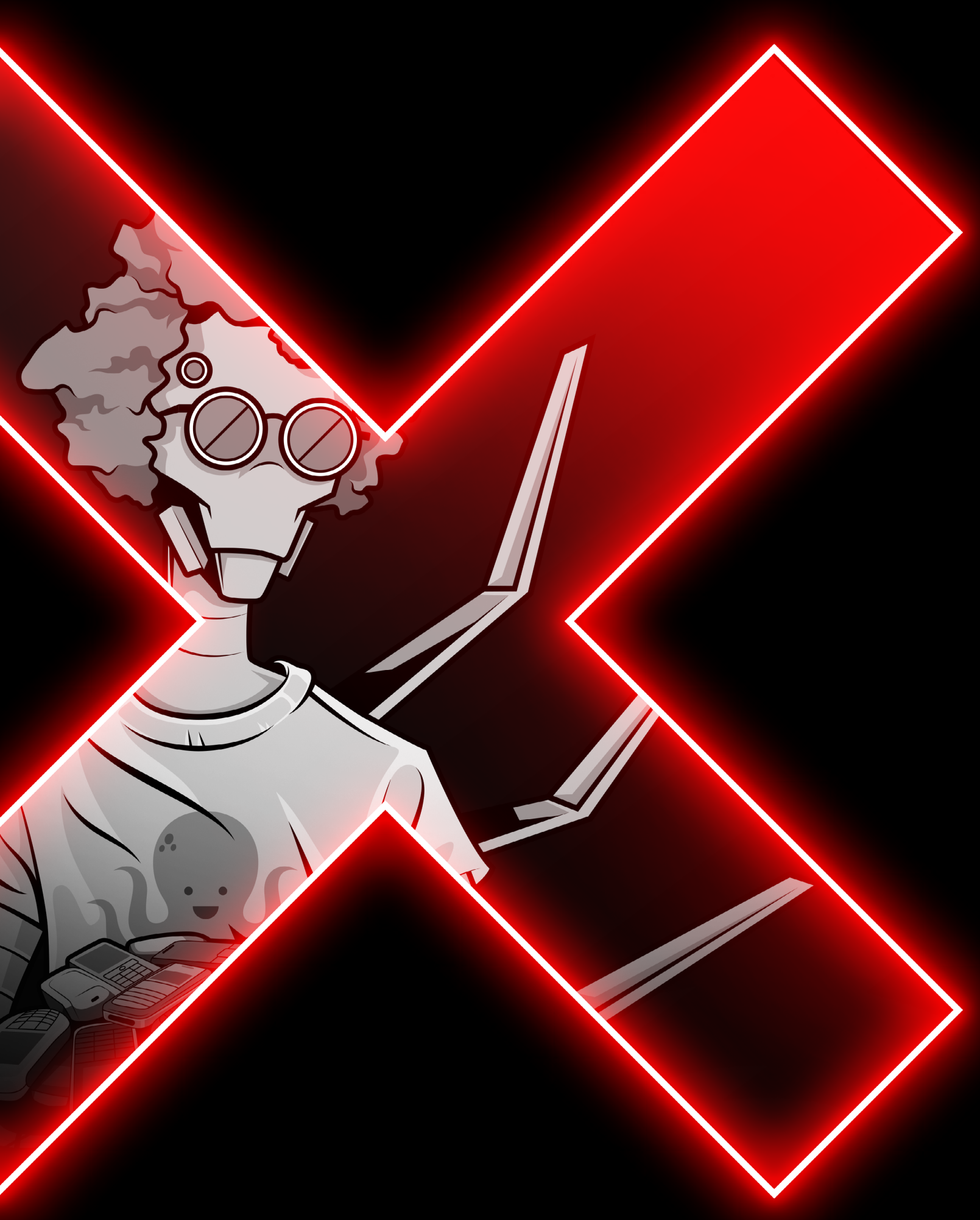


- **Herkunftsland:** Russische Föderation
- **Taktik:** Verwendet schädliche Tools, um Cloud-Services zu manipulieren

Erfahren Sie mehr über diesen aktiven Angreifer und darüber, wie er sich weltweit auf Cloud-Umgebungen auswirkt.

Weitere Informationen

SCATTERED SPIDER

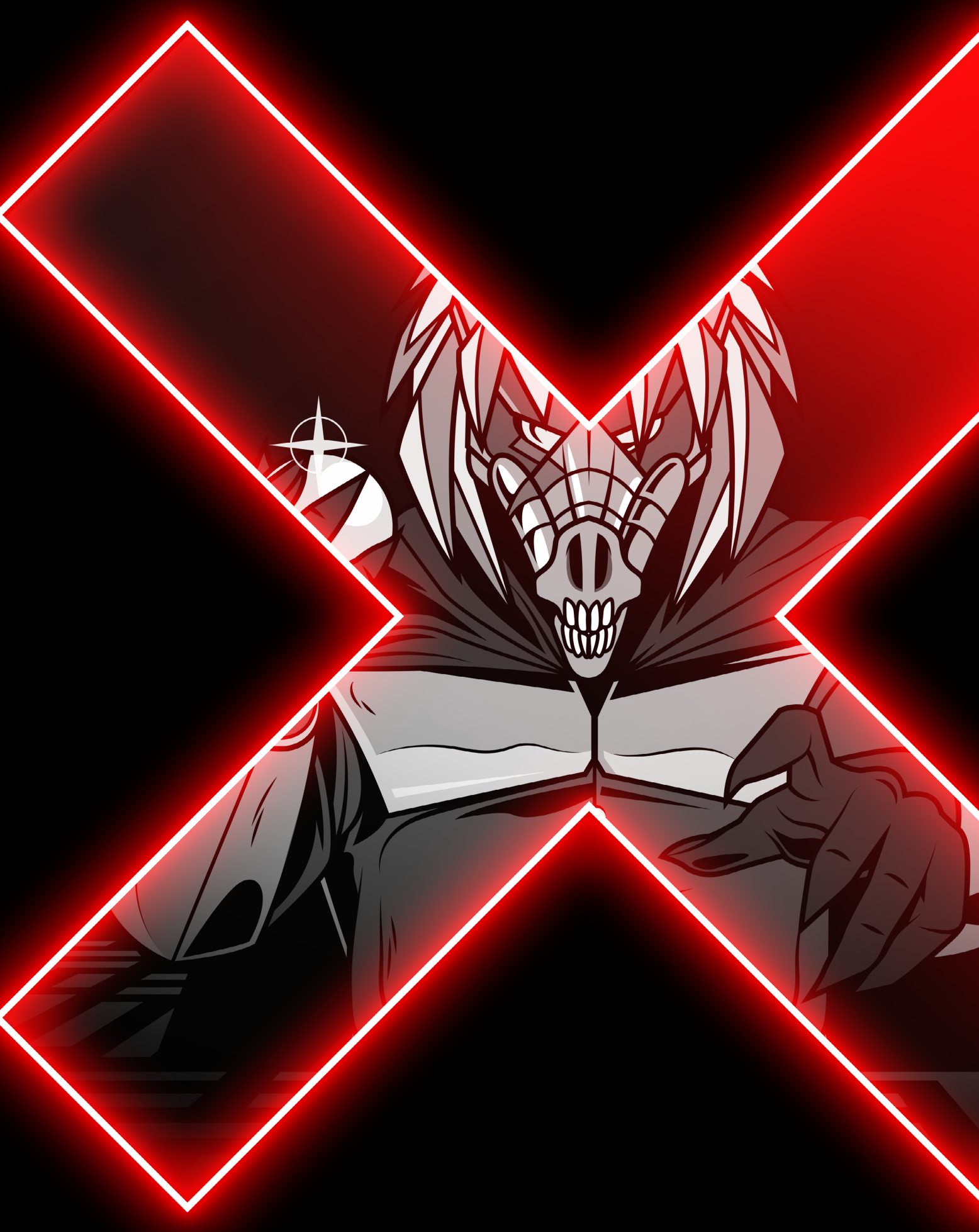


- **Herkunftsland:** Unbekannt
- **Taktik:** Bezieht Ransomware aus einer Cloud-Staging-Umgebung

Lernen Sie diesen Cybercrime-Akteur kennen und erfahren Sie, wie er Cloud-Umgebungen angreift.

Weitere Informationen

LABYRINTH CHOLLIMA



- **Herkunftsland:** Nordkorea
- **Taktik:** Verwendet Cloud-Ressourcen, um Dokumente mit schädlichen Makros zu verteilen

Erfahren Sie, wie dieser gefährliche Akteur in Cloud-Umgebungen Schäden verursacht.

Weitere Informationen

COSMIC WOLF

- **Herkunftsland:** Türkei
- **Taktik:** Greift Daten an, die in Cloud-Umgebungen gespeichert sind

Erfahren Sie, wie dieser Angreifer gezielt in der Cloud agiert.

Weitere Informationen

Identität ist ein wesentlicher Zugangspunkt zur Cloud

Bedrohungsakteure suchen nach neuen Möglichkeiten, Identitäten in der Cloud auszunutzen.

43 %

Die Angreifer nutzen zunehmend gültige Konten. Bei **43 %** der beobachteten Cloud-Angriffe erfolgte der Erstzugriff auf diese Weise.*

67 %

Bei **67 %** der Cloud-Sicherheitsverletzungen fand CrowdStrike IAM-Rollen (Identitäts- und Zugriffsverwaltung) mit mehr Berechtigungen, als erforderlich waren. Ein Hinweis auf einen Angreifer, der versucht hat, die Rolle zu untergraben, um die Umgebung.*

47 %

Fast die Hälfte (47 %) der kritischen Cloud-Konfigurationsfehler entsteht durch unzureichende Identitäts- und Berechtigungsverwaltung.*

Menschliche Fehler verstärken Cloud-Risiken

Cloud-Konfigurationsfehler sind Sicherheitslücken, Fehler und Schwachstellen, die eine Cloud-Umgebung gefährden können. Sie entstehen, wenn Sicherheitseinstellungen schlecht gewählt oder gar nicht erst implementiert werden. Multi-Cloud-Umgebungen sind häufig komplex und es lässt sich mitunter nur schwer erkennen, ob übermäßige Kontoberechtigungen gewährt, öffentliche Zugriffe falsch konfiguriert oder andere Fehler gemacht wurden.

28 %

der Workloads werden mit Root-Berechtigungen ausgeführt oder erlauben die Erweiterung auf Root-Zugriffsrechte*

24 %

der Workloads verfügen über Root-ähnliche Funktionen*

60 %

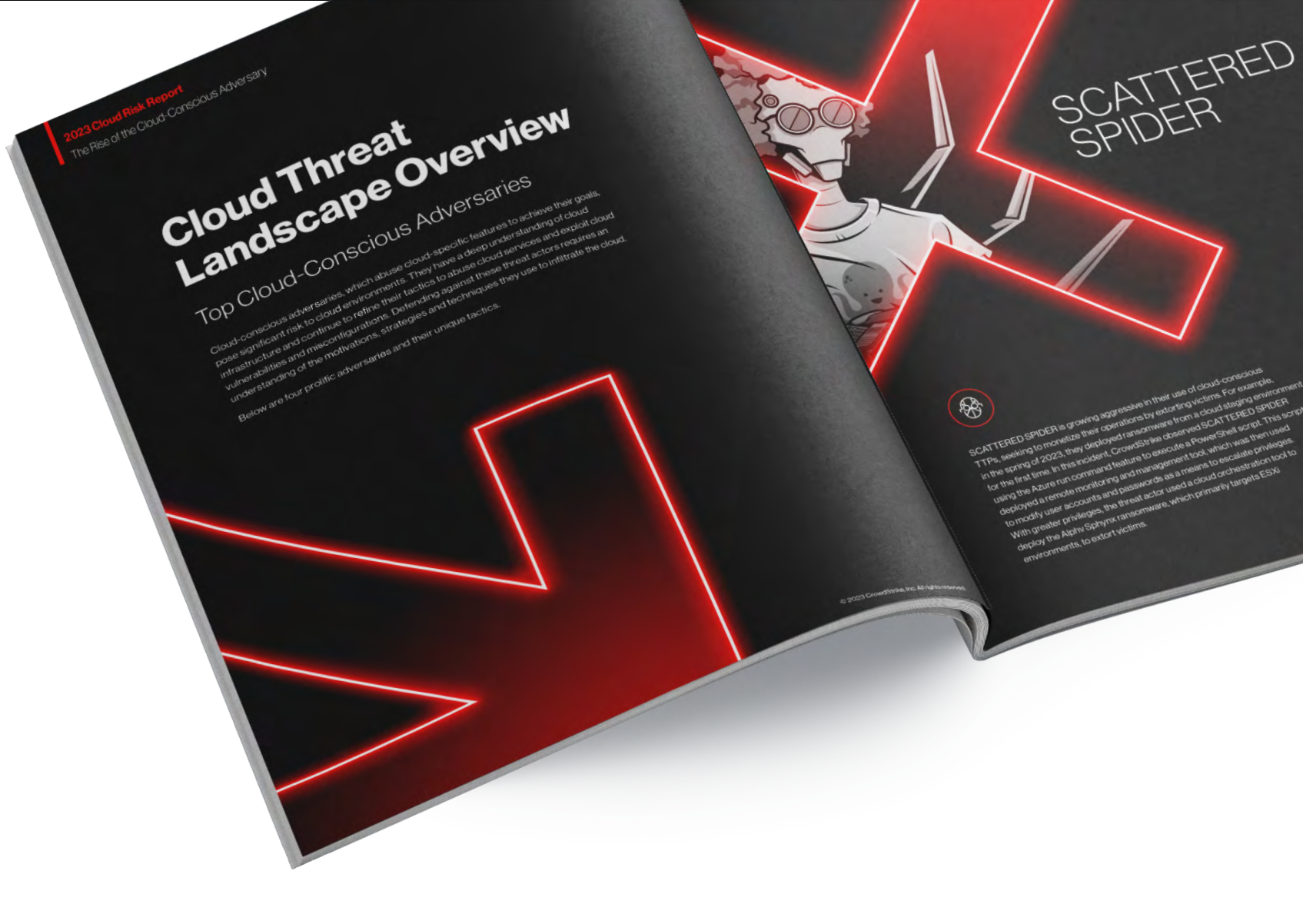
der Workloads verfügen nicht über ordnungsgemäß konfigurierte Sicherheitsfunktionen*

26 %

der Workloads verfügen über automatisch bereitgestellte Kubernetes Service Account Token*

Erfahren Sie mehr über Bedrohungen für Ihre Cloud-Umgebung.

CrowdStrike Cloud Risk Report 2023 herunterladen



Weitere Informationen: https://www.crowdstrike.com/
Folgen Sie uns: Blog | Twitter | LinkedIn | Facebook | Instagram
Kostenlose Testversion starten: https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you

Über CrowdStrike

CrowdStrike (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit einer der weltweit fortschrittlichsten cloudnativen Plattformen für Endgeräte- und Workloadschutz sowie Identität und Daten die Sicherheit geschäftskritischer Unternehmensbereiche neu.

Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform auf äußerst präzise Weise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde für den Cloud-Einsatz entwickelt und nutzt einen einzigen schlanken Agenten, um schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite zu ermöglichen.

CrowdStrike: Schutz, der Sie weiter bringt.

---

* Quelle: Beobachtete Cloud-Sicherheitsvorfälle innerhalb eines 24-stündigen Analysezeitraums