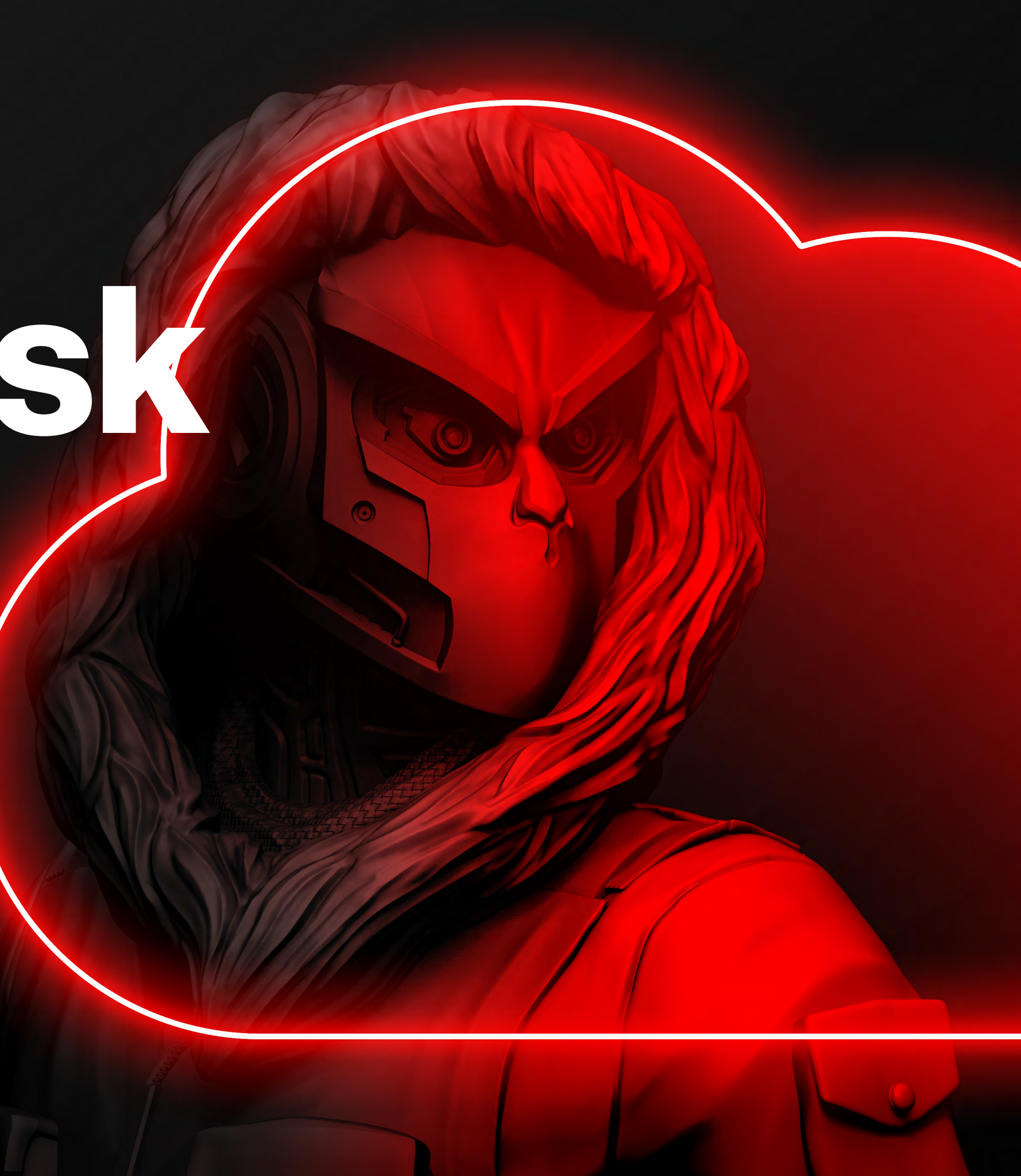
CROWDSTRIKE

Cloud Risk Report 2023

Scopri gli avversari e le tattiche che prendono di mira il cloud



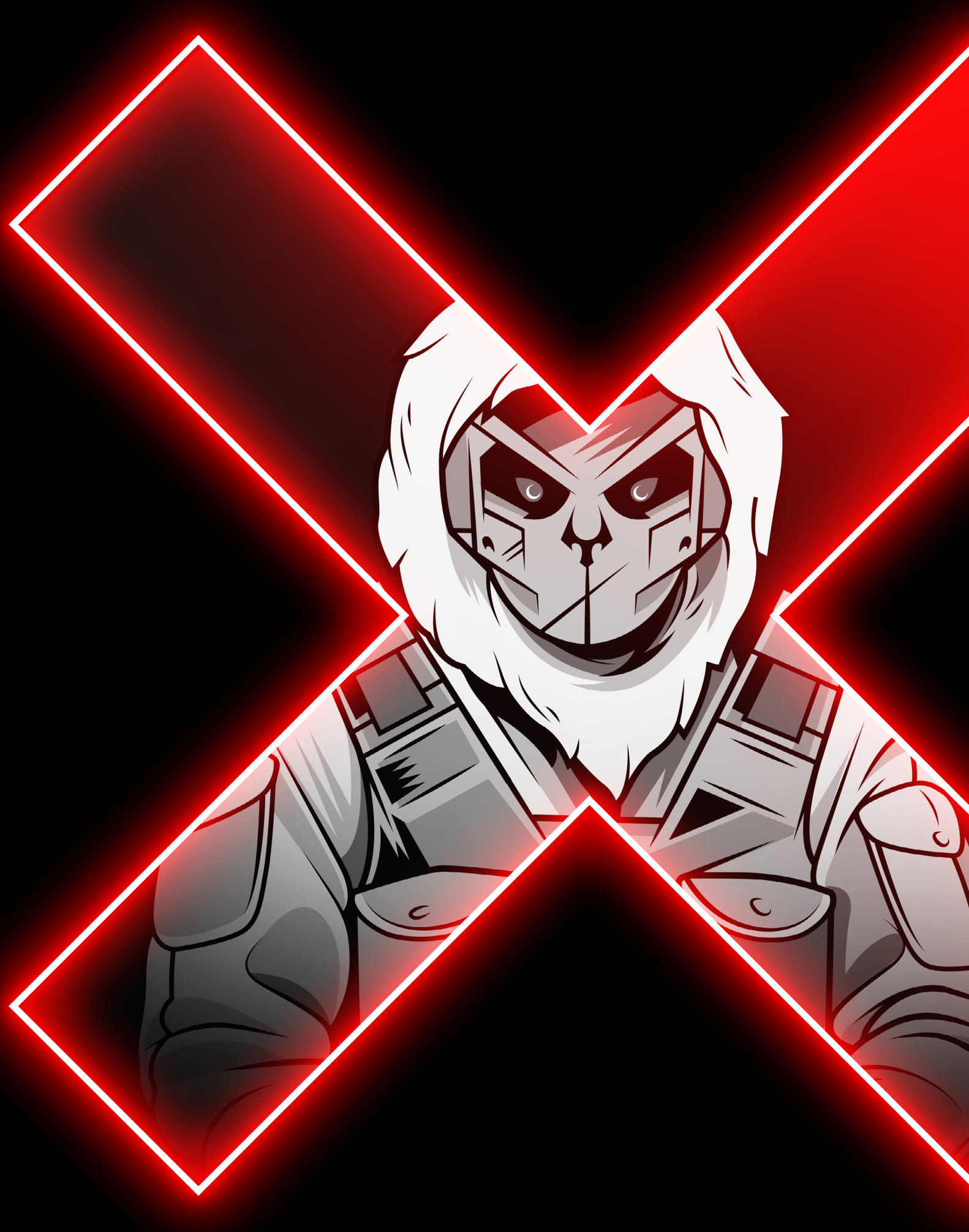
95%
di incremento nello sfruttamento del cloud

3X
il numero dei casi che coinvolgono i cybercriminali cloud conscious

Gli avversari stanno affinando le TTP del cloud

Diversi gruppi avversari, tra cui **COZY BEAR** (Russia-nexus), **SCATTERED SPIDER** (eCrime), **LABYRINTH CHOLLIMA** (DPRK-nexus) e **COSMIC WOLF** (Turkey-nexus) stanno diventando sempre più sofisticati e determinati nel prendere di mira il cloud.

COZY BEAR

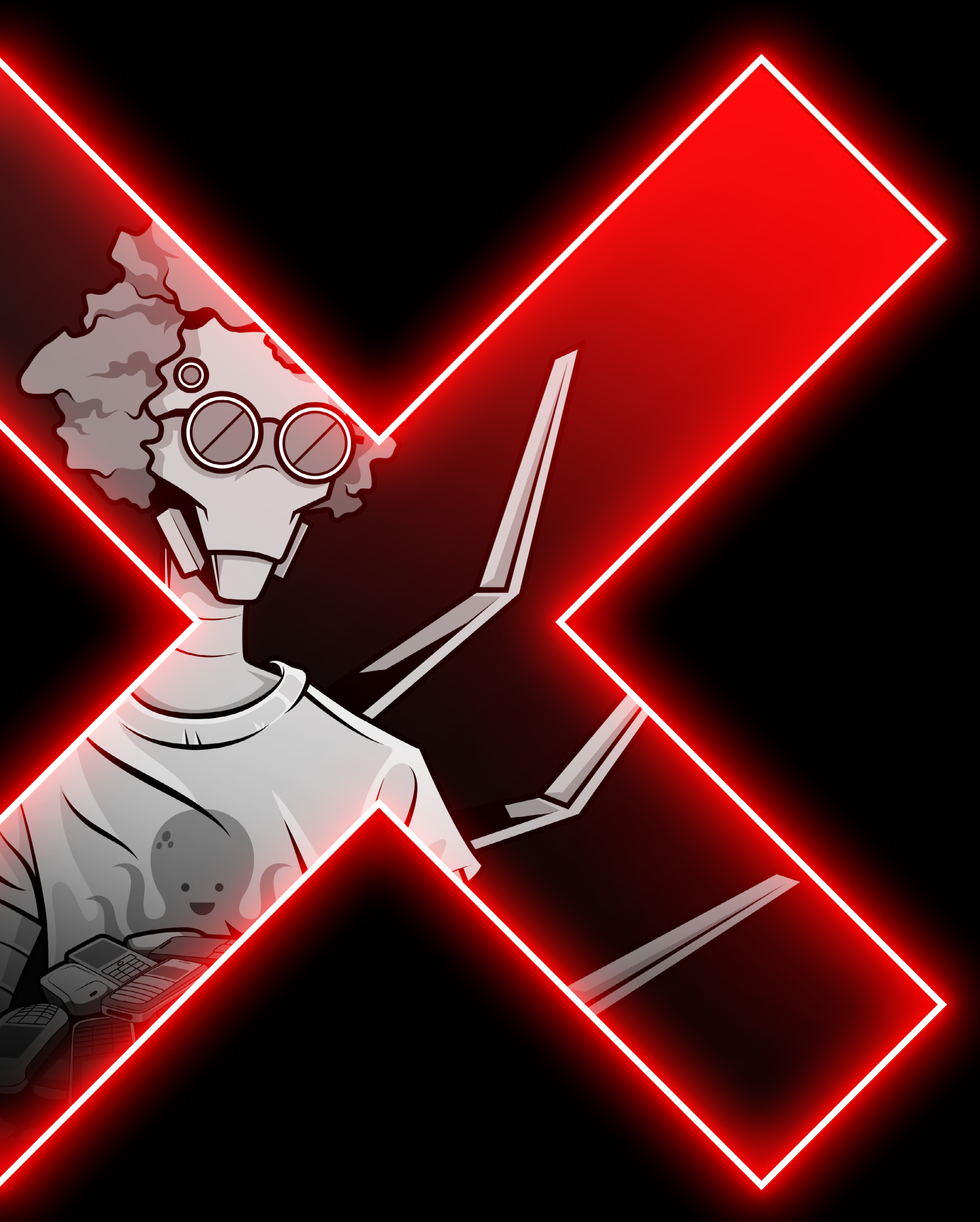


- **Paese di origine:** Federazione Russa
- **Tattiche:** uso di strumenti dannosi per modificare i servizi cloud

Scopri di più su questo avversario e su come influisce sul panorama globale del cloud.

Ulteriori informazioni

SCATTERED SPIDER

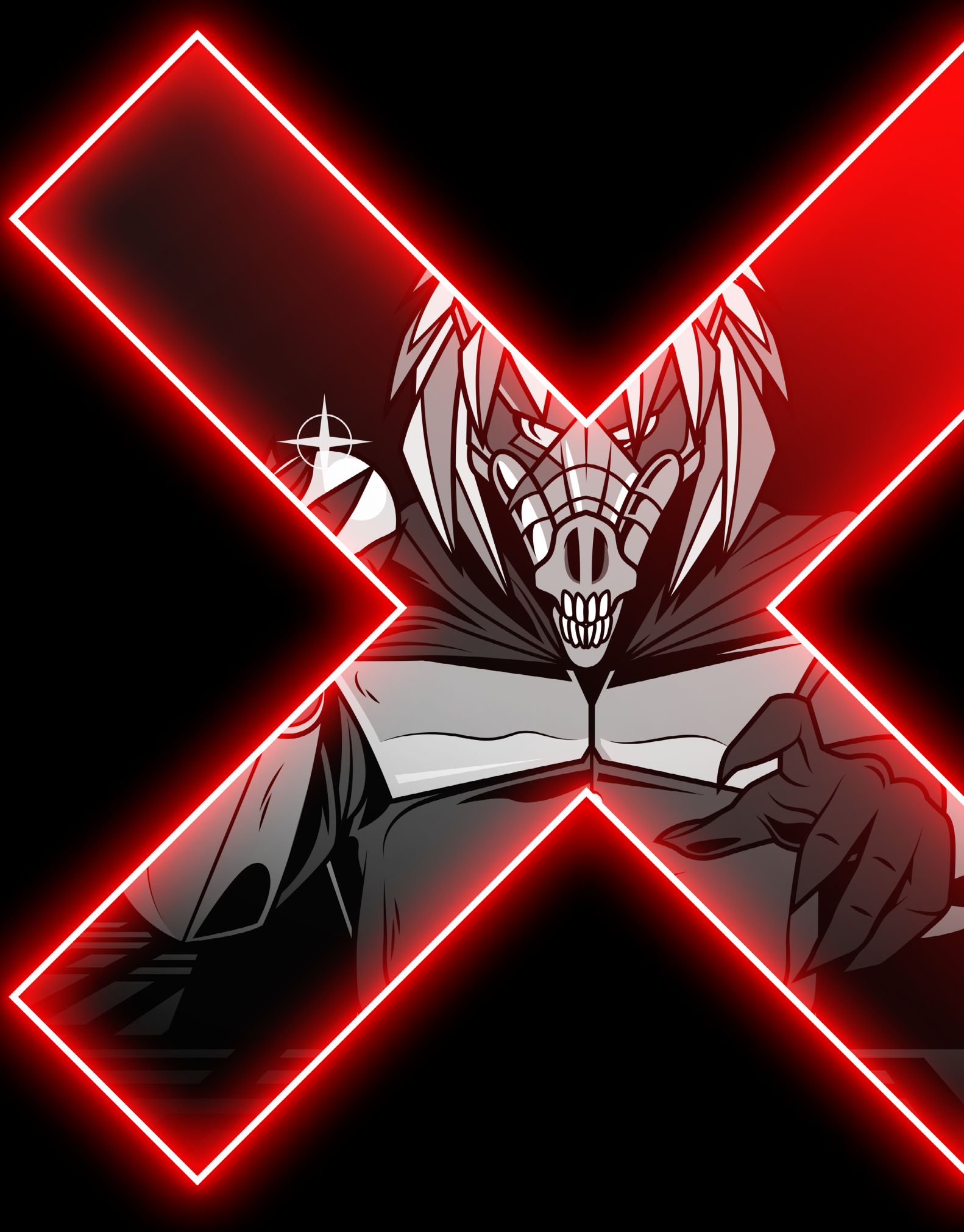


- **Paese di origine:** sconosciuto
- **Tattiche:** distribuisce il ransomware da un ambiente di staging al cloud

Impara a conoscere questo avversario dell'eCrime e il modo in cui prende di mira gli ambienti cloud.

Ulteriori informazioni

LABYRINTH CHOLLIMA



- **Paese di origine:** Corea del Nord
- **Tattiche:** utilizza le risorse cloud per diffondere documenti con macro dannose

Scopri come questo pericoloso avversario sta causando danni in tutto il panorama del cloud.

Ulteriori informazioni

COSMIC WOLF

- **Paese di origine:** Turchia
- **Tattiche:** prende di mira i dati delle vittime archiviati in ambienti cloud

Scopri come questo avversario esperto delle intrusioni mirate opera nel cloud.

Ulteriori informazioni

L'identità è il punto di accesso chiave al cloud

I cybercriminali cercano nuovi modi per sfruttare le identità nel cloud

43%

Gli avversari stanno intensificando l'uso di account validi, che sono stati utilizzati per ottenere l'accesso iniziale nel **43%** delle intrusioni al cloud osservate.*

67%

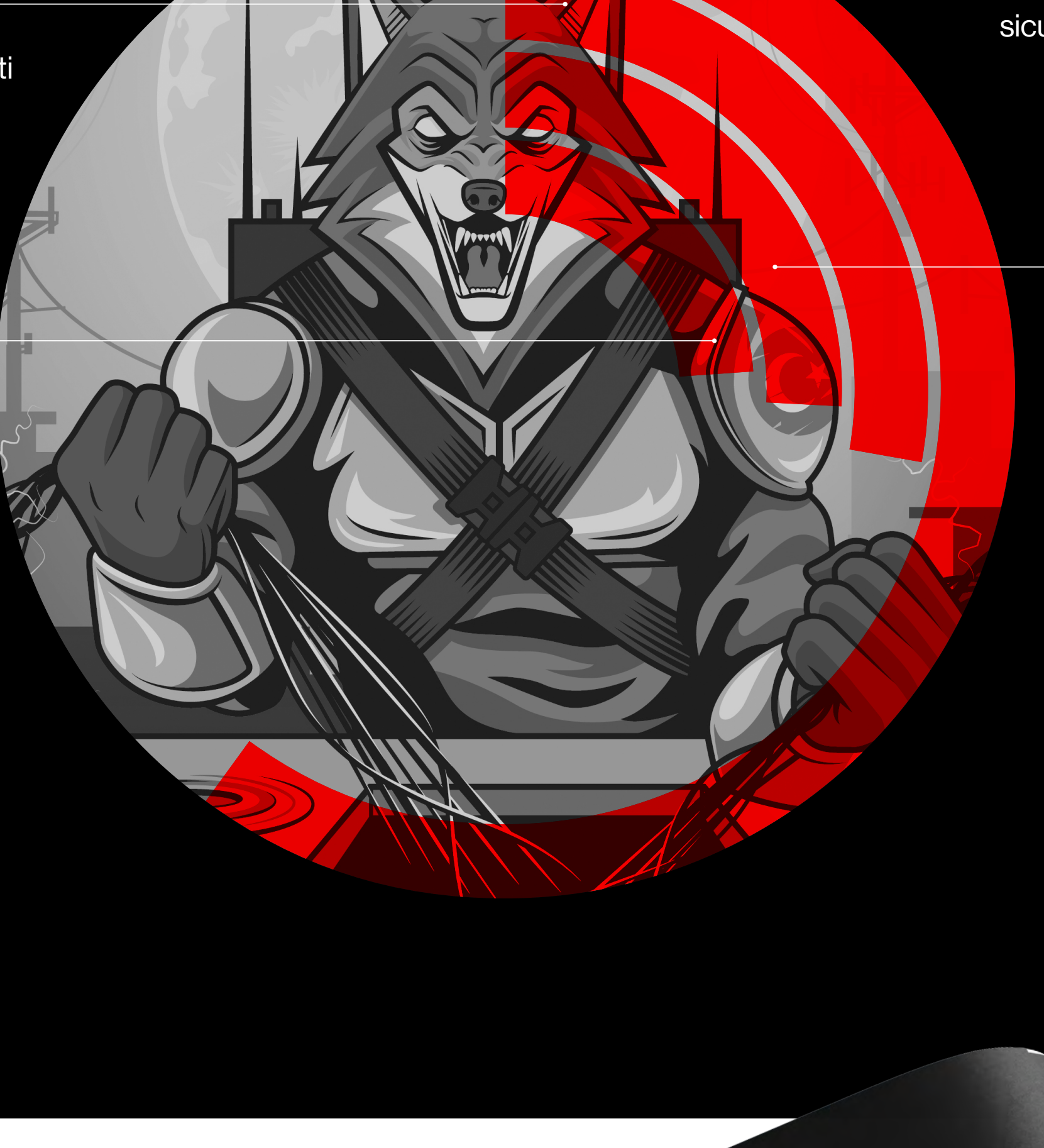
Nel **67%** degli incidenti di sicurezza riguardanti il cloud, CrowdStrike ha riscontrato ruoli di gestione dell'identità e dell'accesso con privilegi elevati al di là di quanto richiesto, il che indica che un avversario potrebbe aver sovvertito il ruolo per compromettere l'ambiente e spostarsi lateralmente.*

47%

Quasi la metà (47%) delle configurazioni errate critiche nel cloud era legata all'integrità insufficiente di identità e diritti.*

L'errore umano genera il rischio cloud

Le configurazioni errate del cloud sono lacune, errori o vulnerabilità che espongono un ambiente cloud al rischio. Possono verificarsi quando le impostazioni di sicurezza sono scelte in modo non idoneo o non vengono implementate affatto. Gli ambienti multi-cloud possono essere complessi e può risultare difficile capire se vengono concessi permessi eccessivi agli account, se viene configurato un accesso pubblico improprio o se vengono commessi altri errori.



28%
i workload che vengono eseguiti come root o consentono l'escalation a root*

24%
i workload che hanno funzionalità simili a root*

60%
i workload privi di protezioni di sicurezza correttamente configurate*

26%
i workload dove il token dell'account Kubernetes Service si installa automaticamente*

Scopri di più sulle minacce al tuo ambiente cloud.

Scarica il Cloud Risk Report 2023 di CrowdStrike

Ulteriori informazioni: https://www.crowdstrike.com/
Seguici: Blog | Twitter | LinkedIn | Facebook | Instagram
Inizia oggi una prova gratuita: https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della cybersecurity, ha ridefinito la sicurezza moderna con la piattaforma cloud native più avanzata al mondo per la protezione delle aree critiche del rischio aziendale: endpoint e workload cloud, identità e dati.

Basata sulla tecnologia CrowdStrike Security Cloud e sulla migliore intelligenza artificiale, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, la threat intelligence, lo spionaggio degli avversari in evoluzione e la telemetria arricchita proveniente da tutta l'azienda per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'élite e osservabilità delle vulnerabilità.

Costruita appositamente nel cloud con una singola architettura di lightweight-agent, la piattaforma Falcon assicura una distribuzione rapida e scalabile, protezione e prestazioni superiori, una complessità ridotta e un time-to-value immediato.

CrowdStrike: Protection that powers you.

*Fonte: dati sulla sicurezza del cloud osservati per un periodo di valutazione di 24 ore