CROWDSTRIKE

Rapport 2023 sur les risques liés au cloud :

Découvrez les cyberadversaires qui ciblent le cloud et leurs tactiques

95 %
Augmentation de l'exploitation du cloud

X3
Augmentation des cas impliquant des cybercriminels ciblant le cloud

Les cyberadversaires perfectionnent leurs tactiques, techniques et procédures (TTP) dans le cloud

Plusieurs groupes cybercriminels, dont **COZY BEAR** (associé à la Russie), **SCATTERED SPIDER** (cybercriminalité), **LABYRINTH CHOLLIMA** (associé à la Corée du Nord) et **COSMIC WOLF** (associé à la Turquie), font preuve d'une sophistication croissante et se montrent de plus en plus déterminés à cibler le cloud.

COZY BEAR

- **Pays d'origine :** Fédération de Russie
- **Tactiques :** modifie les services cloud au moyen d'outils malveillants

Découvrez-en plus sur ce cyberadversaire prolifique et son impact sur le paysage du cloud mondial.

En savoir plus

SCATTERED SPIDER

- **Pays d'origine :** inconnu
- **Tactiques :** déploie des ransomwares à partir d'un environnement cloud de simulation

Découvrez ce cybercriminel et les techniques qu'il utilise pour cibler les environnements cloud.

En savoir plus

LABYRINTH CHOLLIMA

- **Pays d'origine :** Corée du Nord
- **Tactiques :** utilise des ressources cloud pour distribuer des documents contenant des macros malveillantes

Découvrez-en plus sur les dégâts causés dans le paysage cloud par ce dangereux cyberadversaire.

En savoir plus

COSMIC WOLF

- **Pays d'origine :** Turquie
- **Tactiques :** cible les données stockées par ses victimes dans des environnements cloud

Découvrez comment ce cyberadversaire spécialisé dans les intrusions opère dans le cloud.

En savoir plus

Les identités constituent un point d'accès majeur au cloud

Les cybercriminels cherchent de nouveaux moyens pour exploiter les identités dans le cloud

43 %

Les cyberadversaires s'appuient de plus en plus sur des comptes valides pour obtenir un accès initial. Ceux-ci ont en effet servi dans **43 %** des intrusions dans le cloud observées.*

67 %

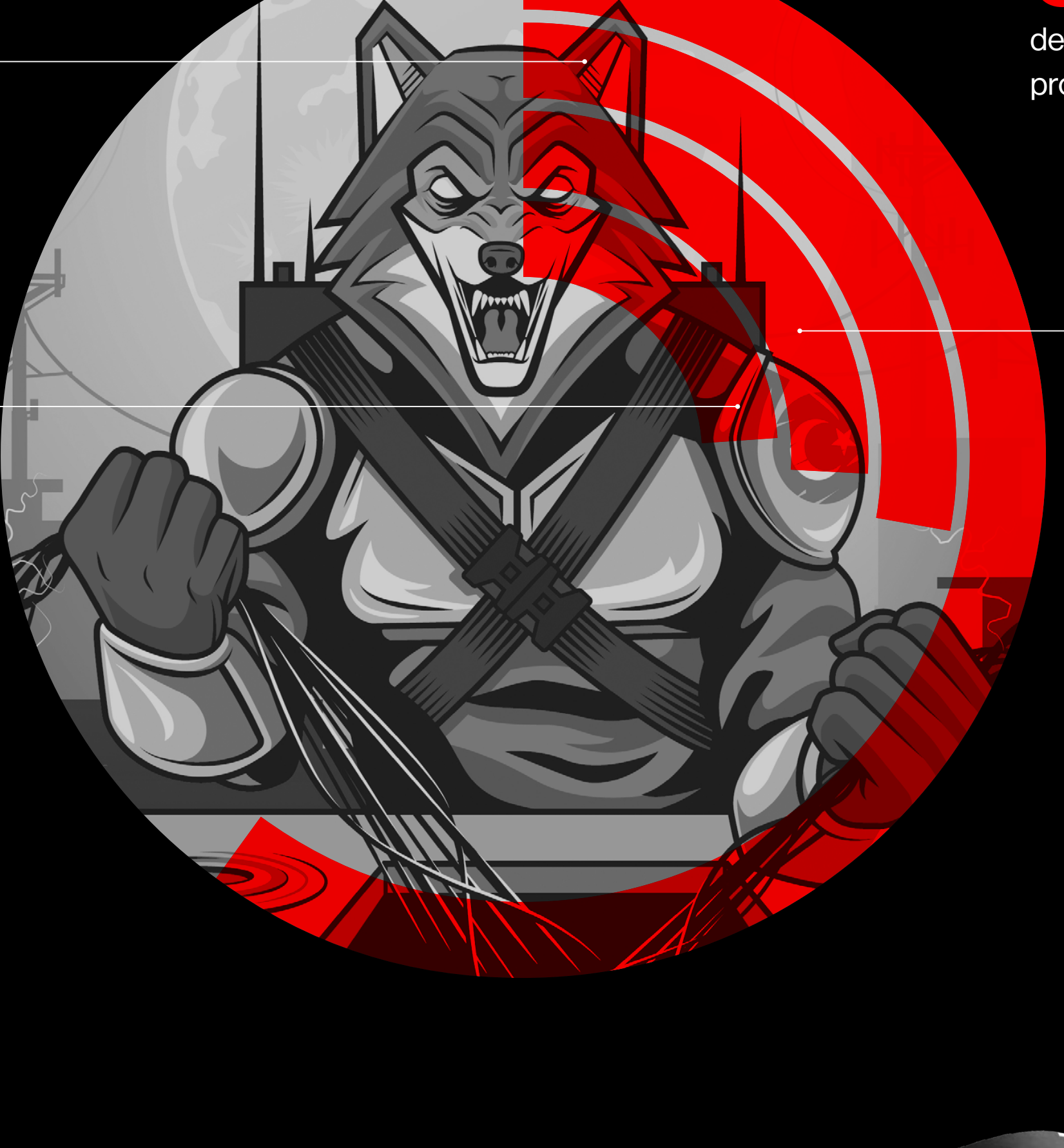
Dans **67 %** des incidents de sécurité dans le cloud, CrowdStrike a mis en évidence des rôles IAM (gestion des identités et des accès) dotés de privilèges excessivement élevés, signe qu'un cyberadversaire avait sans doute détourné le rôle pour compromettre l'environnement et se déplacer latéralement.*

47 %

Près de la moitié (47 %) des erreurs de configuration critiques dans le cloud sont dues à de mauvaises pratiques en matière de gestion des identités et des droits.*

Les erreurs humaines sont une menace pour le cloud

Les erreurs de configuration sont des failles, des erreurs ou des vulnérabilités qui exposent un environnement cloud à divers risques. Elles peuvent résulter de la sélection de paramètres de sécurité inappropriés ou de l'absence d'implémentation de tels paramètres. Compte tenu de la complexité des environnements multicloud, il peut être difficile de repérer les autorisations de compte excessives, les accès publics inappropriés et autres erreurs potentielles.



28 %
des workloads sont exécutés en tant qu'administrateur ou permettent d'obtenir des privilèges administateur*

24 %
des workloads disposent de fonctionnalités de type administrateur*

60 %
des workloads ne disposent pas de protection correctement configurée*

26 %
des workloads présentent un jeton de compte de service Kubernetes monté automatiquement*

Découvrez-en plus sur les menaces qui pèsent sur votre environnement cloud.

Téléchargez le Rapport 2023 sur les risques liés au cloud de CrowdStrike

En savoir plus : https://www.crowdstrike.com/
Suivez-nous : Blog | Twitter | LinkedIn | Facebook | Instagram
Profitez d'une évaluation gratuite : https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you

À propos de CrowdStrike

CrowdStrike (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une intelligence artificielle de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, la recherche de menaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike : prenez les commandes de votre protection.

* Source : incidents de sécurité dans le cloud observés sur une période d'évaluation de 24 heures