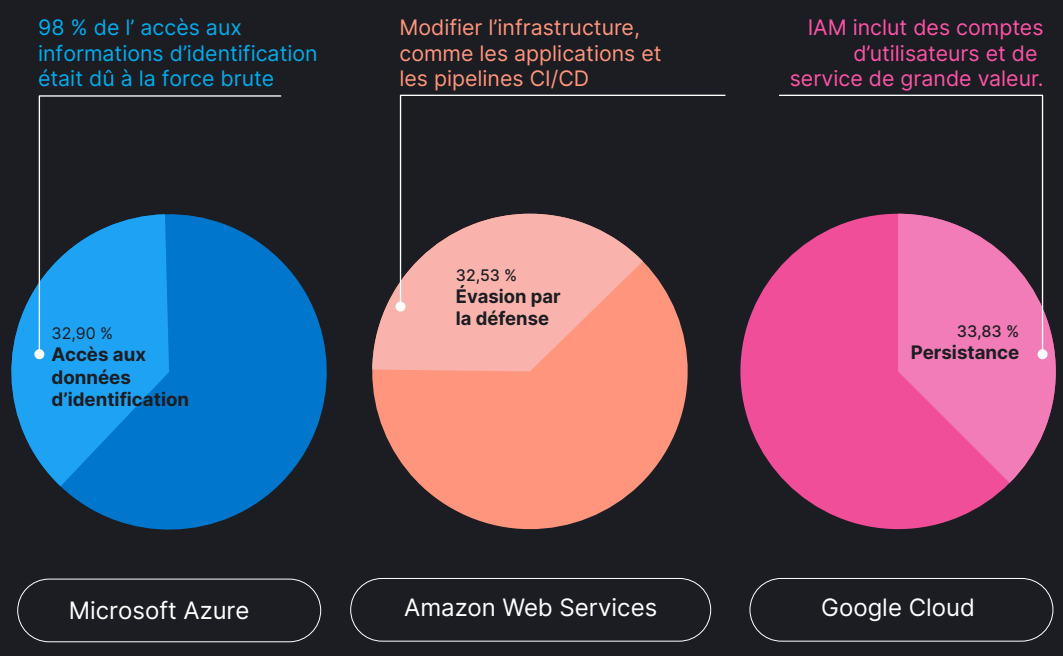
elastic security labs

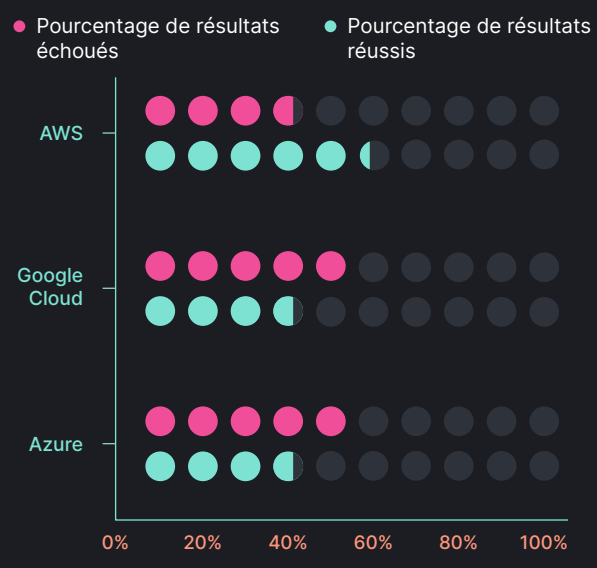
Méthodes des utilisateurs malveillants décrites dans le Rapport 2024 sur les menaces mondiales d'Elastic

Nous assistons à l'accès aux informations d'identification, à l'évasion par la défense et à la persistance dans les environnements cloud



Les environnements cloud peuvent être protégés par les benchmarks CIS

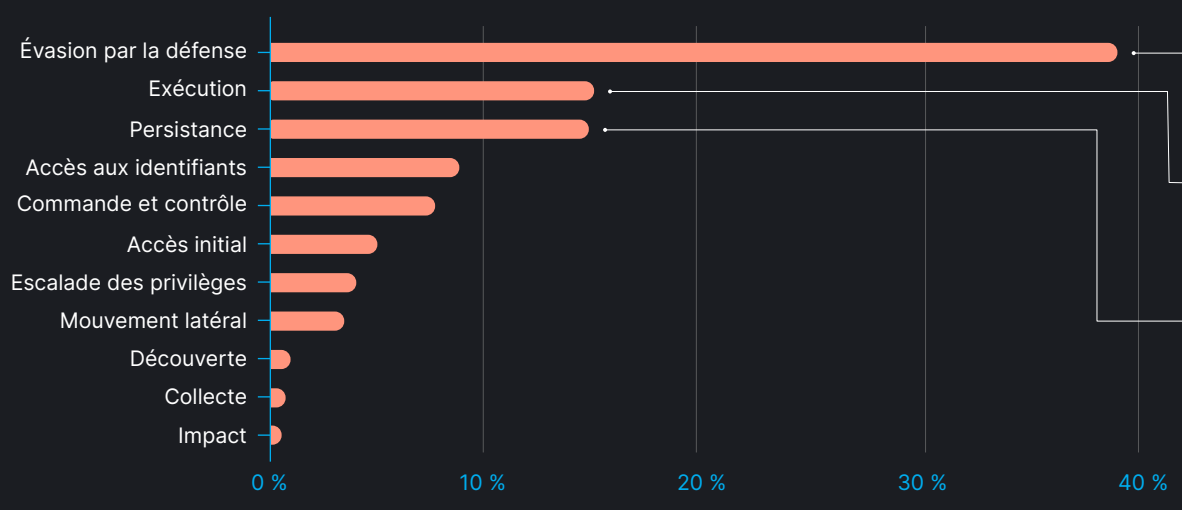
Elastic Security Labs a constaté des échecs dans toutes les principales politiques de sécurité du contenu (CSP). Vérifiez que votre environnement cloud ne présente pas d'erreurs de configuration.



Qu'est-ce qui a changé depuis l'année dernière ?

- Une **augmentation de 3%** in des techniques d'accès aux données d'identification, en particulier les données d'identification non sécurisées, qui **ont augmenté de 31 %**
- Diminution **de 6 %** des techniques d'évasion par la défense
- Les techniques de persistance **ont augmenté de 8 %**

Au sein des terminaux, les adversaires sont :



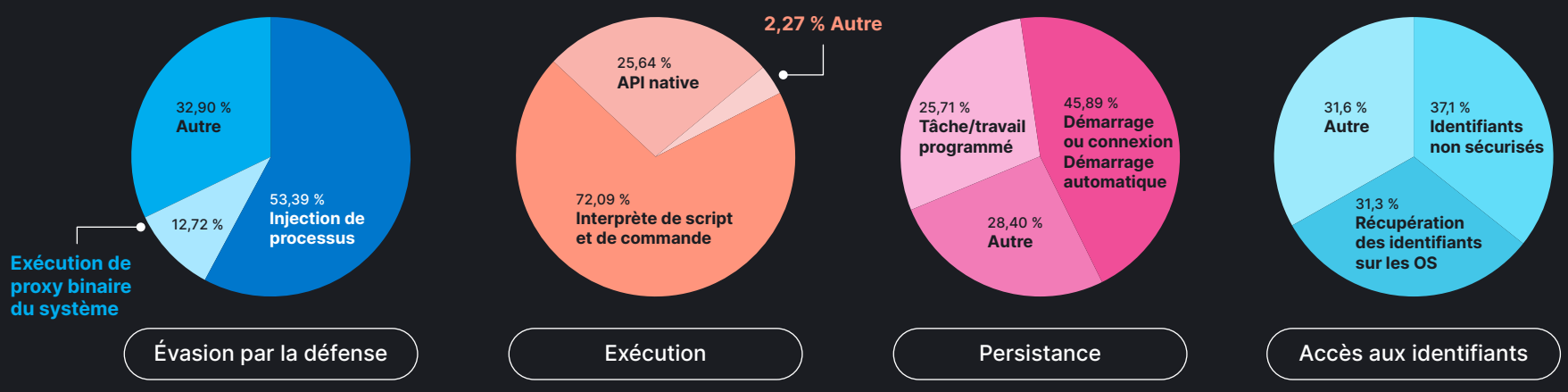
L'exploitation des vulnérabilités permet aux adversaires d'injecter et d'exécuter du code.

Il n'y a pas d'objectif unique pour les adversaires. Nous avons observé la collecte de données, l'obscurcissement, le chargement de DLL, etc.

Les adversaires recherchent des actions efficaces qui peuvent se produire automatiquement.

Défense, évasion, exécution et persévérance représentent environ 70 % des comportements observés.

Techniques observées sur les terminaux Windows (92,7 % de la télémétrie du système d'exploitation)



2025 approche : envisagez de faire ce qui suit :

- Calculez votre score de benchmark CIS et planifiez comment l'augmenter
- Suivez @ElasticSecLabs sur X
- Téléchargez le rapport complet d'Elastic sur les menaces mondiales
- Auditez votre bibliothèque de protections avec le modèle de maturité comportementale de l'ingénierie de détection d'Elastic Security Labs.

  Concentrez-vous sur la résolution de :

  - Évasion par la défense
  - Exécution
  - Persistance
  - Accès aux identifiants