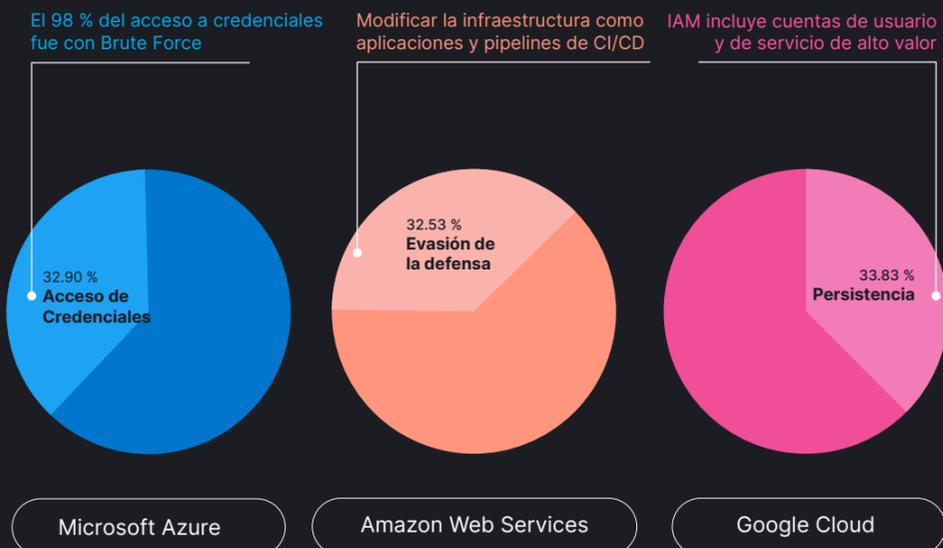


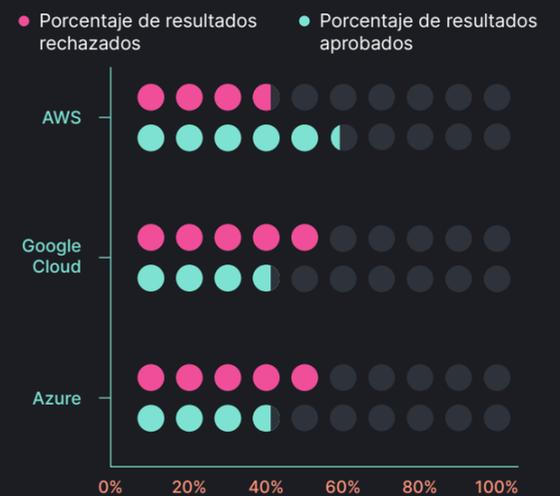
Métodos de adversarios en el Reporte global de amenazas de Elastic 2024

Estamos viendo acceso a credenciales, evasión de la defensa y persistencia en entornos del cloud



Los entornos en la nube pueden protegerse con puntos de referencia CIS

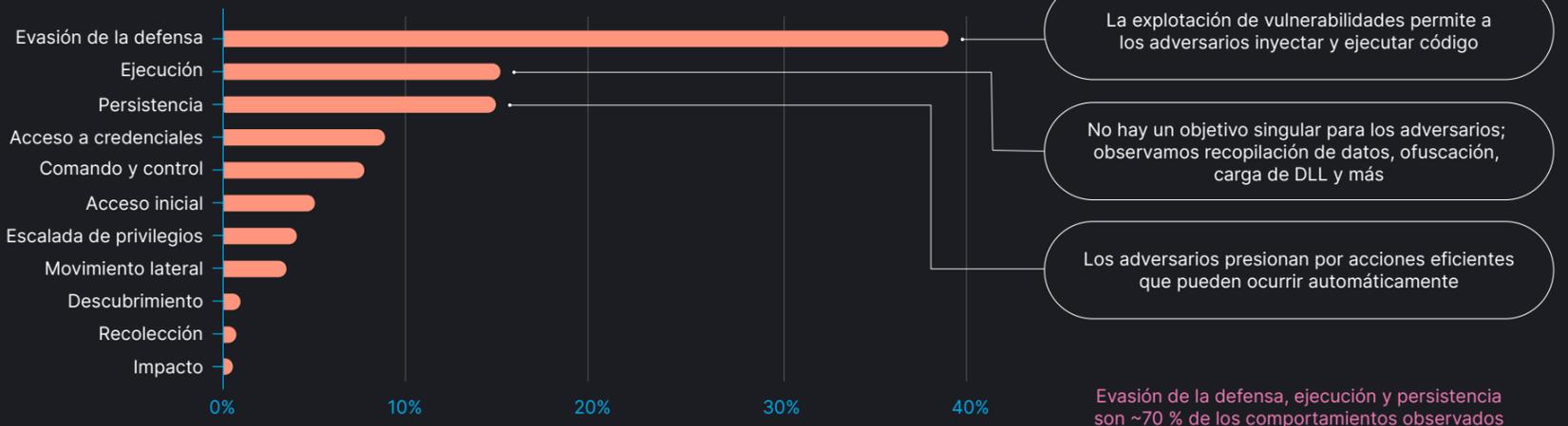
Elastic Security Labs detectó comprobaciones fallidas en todos los principales CSP. Comprueba si hay errores de configuración en tu entorno en la nube.



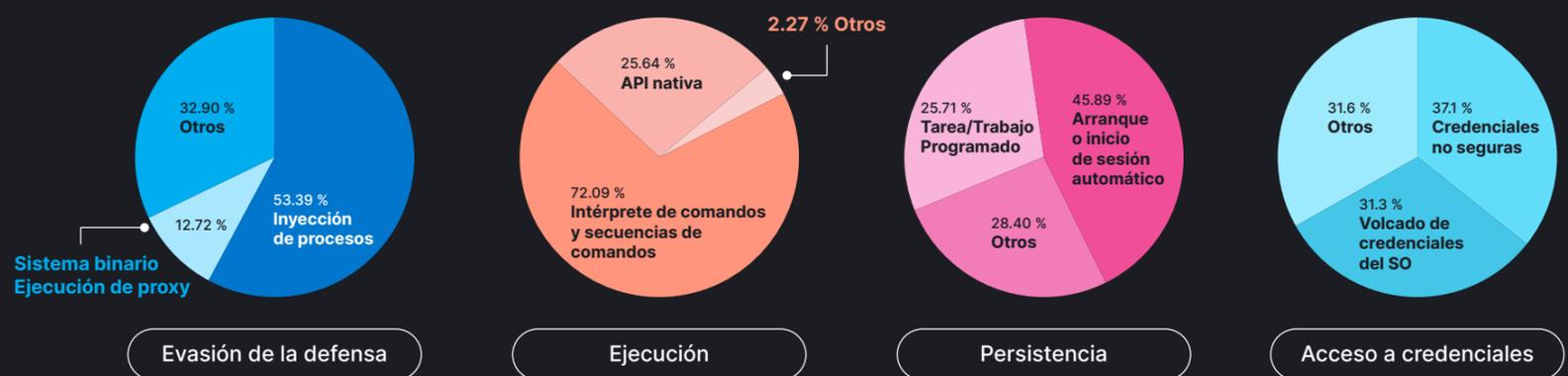
¿Qué ha cambiado desde el año pasado?

- Un aumento del 3 % en las técnicas de acceso a credenciales, específicamente credenciales no seguras, que aumentaron un 31 %
- Una reducción del 6 % en las técnicas de evasión de la defensa
- Las técnicas de persistencia aumentaron en un 8 %

Dentro de los endpoints, los adversarios son:



Técnicas observadas en los endpoints de Windows (92.7 % de la telemetría del sistema operativo)



Se acerca el **2025**
Piensa en hacer lo siguiente:

- Calcula tu puntaje de referencia CIS y planea cómo aumentarlo
 - Sigue a [@ElasticSecLabs](#) en X
 - Descarga todo el [Reporte sobre amenazas globales de Elastic](#)
 - Audita tu biblioteca de protecciones con [el modelo de madurez del comportamiento de ingeniería de detección de Elastic Security Labs](#).
- Concéntrate en abordar:
- Evasión de la defensa
 - Persistencia
 - Ejecución
 - Acceso a credenciales