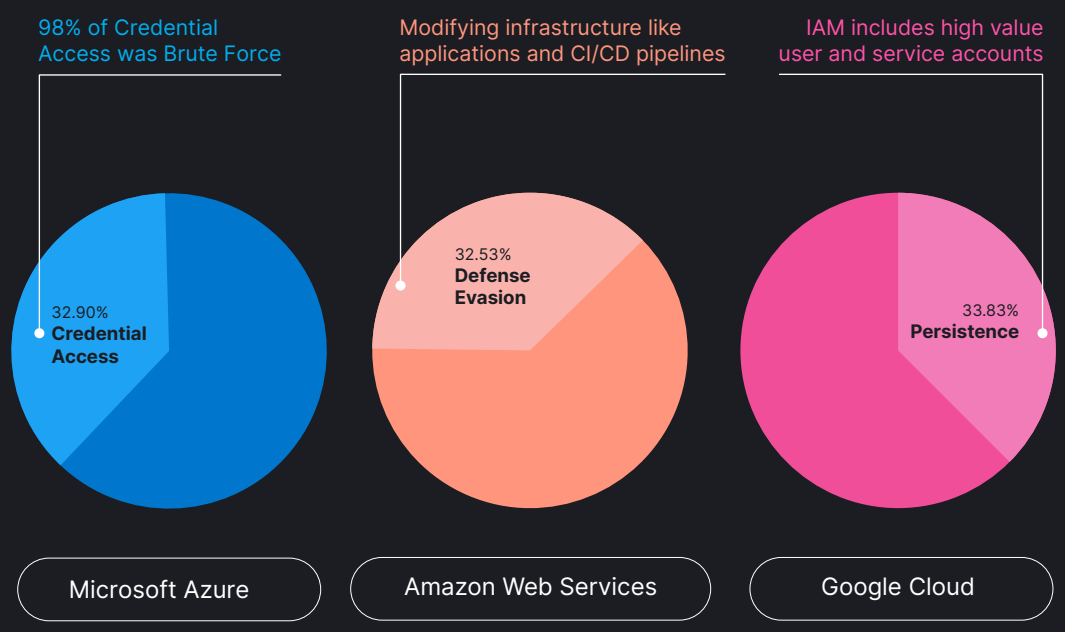
elastic security labs

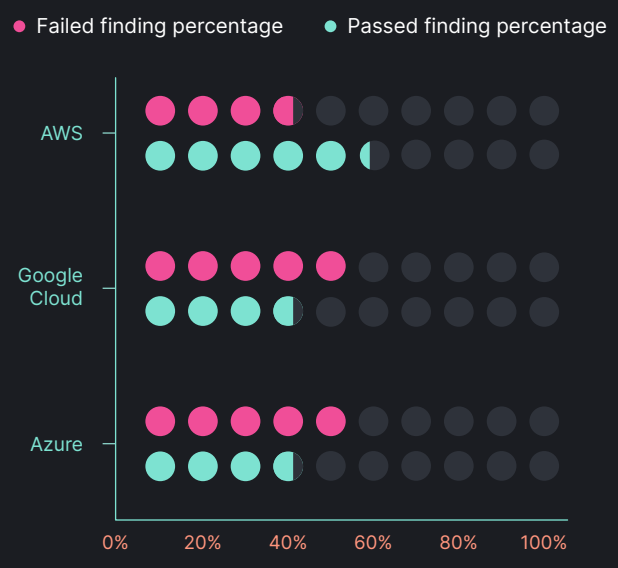
Adversary Methods in the 2024 Elastic Global Threat Report

We're seeing Credential Access, Defense Evasion, and Persistence in cloud environments



Cloud environments can be protected with CIS benchmarks

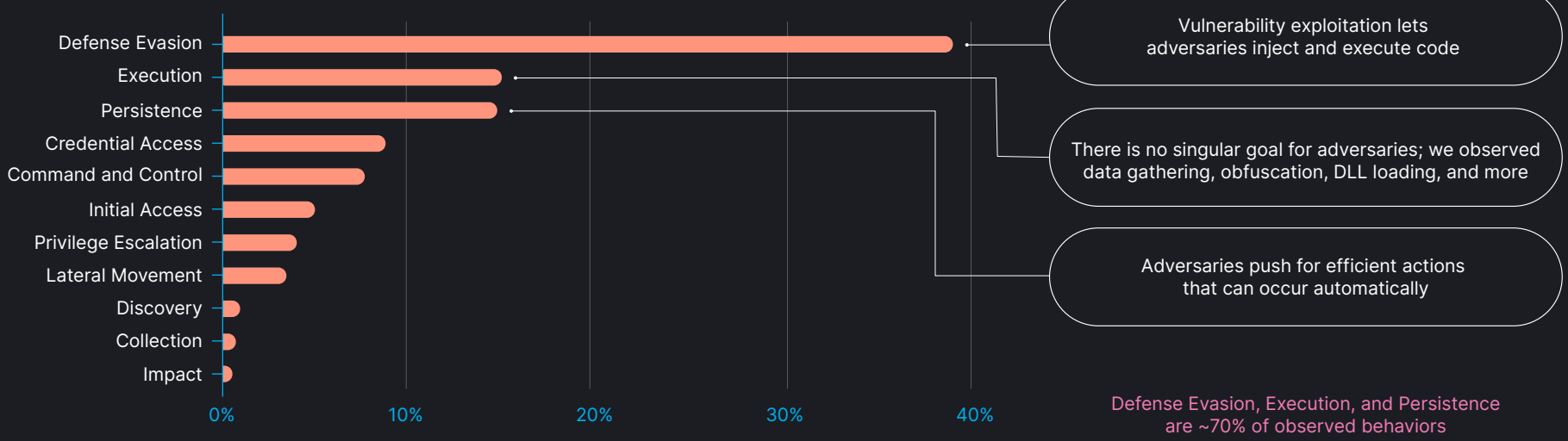
Elastic Security Labs saw failed checks across every major CSP. Check your cloud environment for misconfigurations.



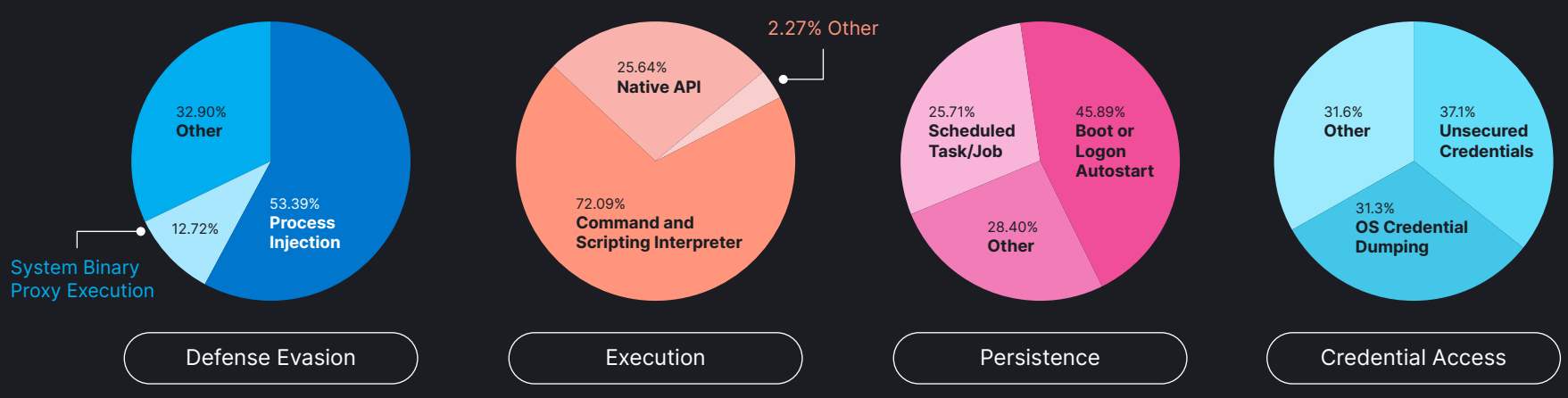
What's changed since last year?

- A **3% increase** in Credential Access techniques — specifically Unsecured Credentials, which **rose 31%**
- A **6% decrease** in Defense Evasion techniques
- Persistence techniques **increased by 8%**

Within endpoints, adversaries are:



Techniques observed in Windows endpoints (92.7% of OS telemetry)



2025

is coming — consider doing the following:

- Calculate your CIS benchmark score and plan how to raise it
- Follow @ElasticSecLabs on X
- Download the full Elastic Global Threat Report
- Audit your protections library with Elastic Security Labs' Detection Engineering Behavioral Maturity Model.

Focus on addressing:

- Defense Evasion
- Execution
- Persistence
- Credential Access