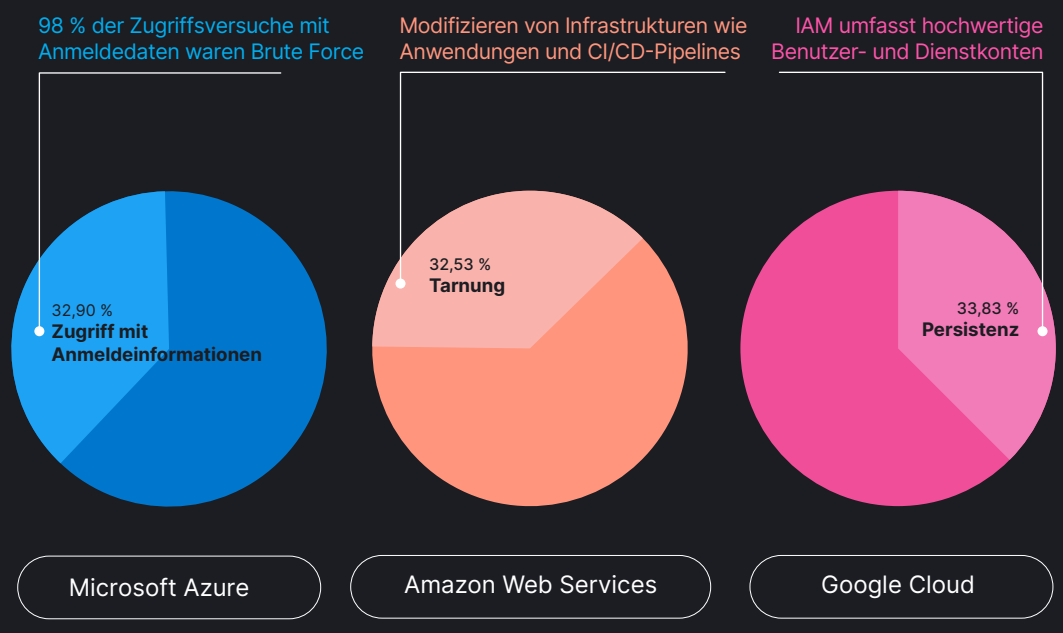
elastic security labs

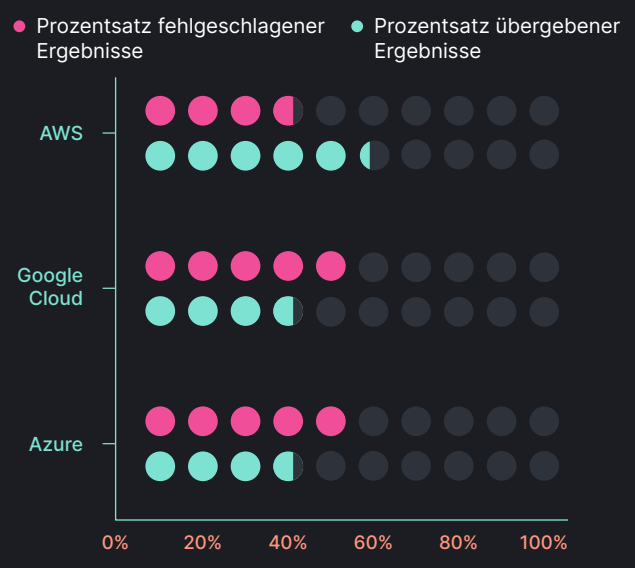
Angreifertechniken im Elastic Global Threat Report 2024

Wir sehen Zugriff mit Anmeldedaten, Tarnung und Persistenz in Cloud-Umgebungen



Cloud-Umgebungen können mit den CIS-Benchmarks geschützt werden

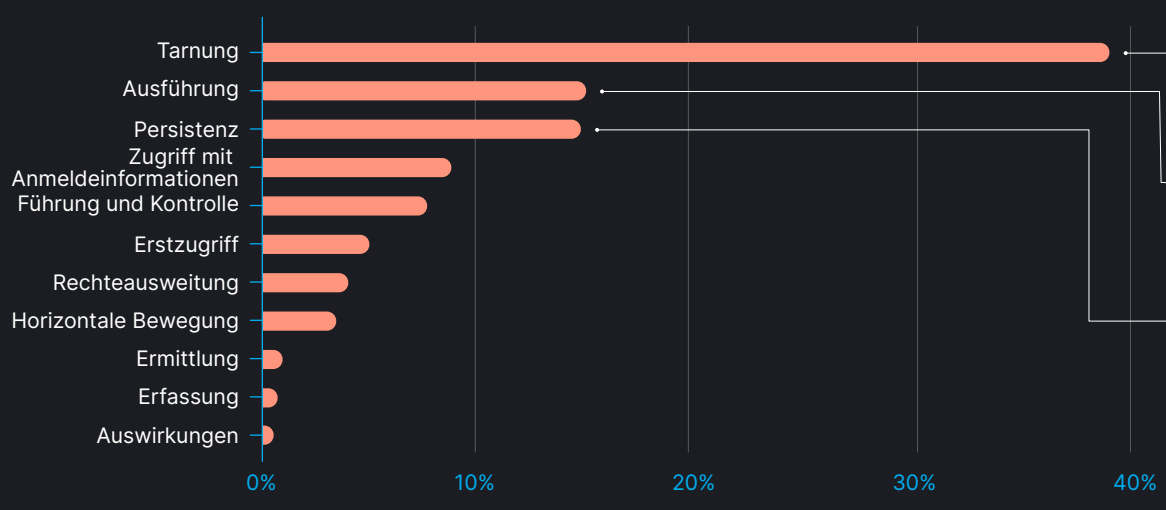
Elastic Security Labs stellte bei allen großen CSPs fehlgeschlagene Prüfungen fest. Überprüfen Sie Ihre Cloud-Umgebung auf Fehlkonfigurationen.



Was hat sich seit letztem Jahr geändert?

- Ein **Anstieg von 3 %** bei den Techniken zum Zugriff mit Anmeldeinformationen – insbesondere bei ungesicherten Anmeldeinformationen, die **um 31 % zunahmen**
- Ein **Rückgang um 6 %** der Techniken zur Tarnung
- Die Persistenztechniken **nahmen um 8 % zu**

Innerhalb der Endpunkte sind die Gegner:



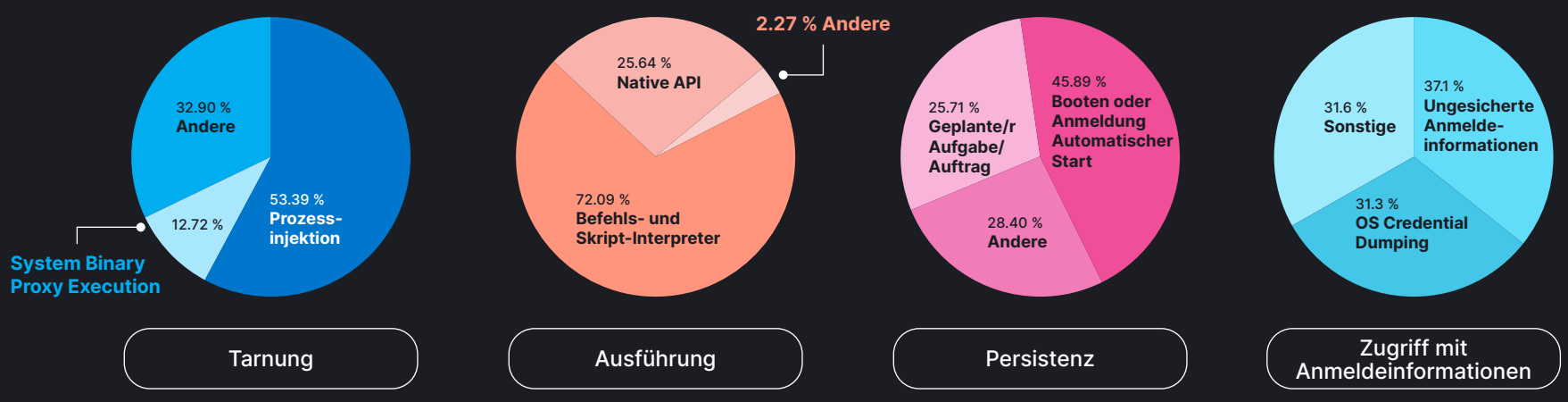
Die Ausnutzung von Schwachstellen ermöglicht Angreifern, Code einzufügen und auszuführen.

Es gibt kein einzelnes Ziel für Gegner. Wir stellten fest, dass Datenerfassung, Verschleierung, Laden von DLL und mehr möglich sind.

Gegner drängen auf effiziente Maßnahmen, die automatisch erfolgen können

Tarnung, Ausführung und Persistenz sind ca. 70 % der beobachteten Verhaltensweisen

In Windows-Endpunkten beobachtete Techniken (92,7 % der OS-Telemetrie)



Das Jahr

2025

kommt – überlegen Sie, das Folgende zu tun:

- Berechnen Sie Ihren CIS-Wert und planen Sie, wie Sie ihn erhöhen können
- Folgen Sie @ElasticSecLabs auf X
- Laden Sie den vollständigen Elastic Global Threat Report herunter
- Prüfen Sie Ihre Schutzbibliothek mit dem Detection Engineering Behavioral Maturity Model von Elastic Security Labs.

  Konzentrieren Sie sich auf die folgenden Punkte:

  - Tarnung
  - Ausführung
  - Persistenz
  - Zugriff mit Anmeldeinformationen