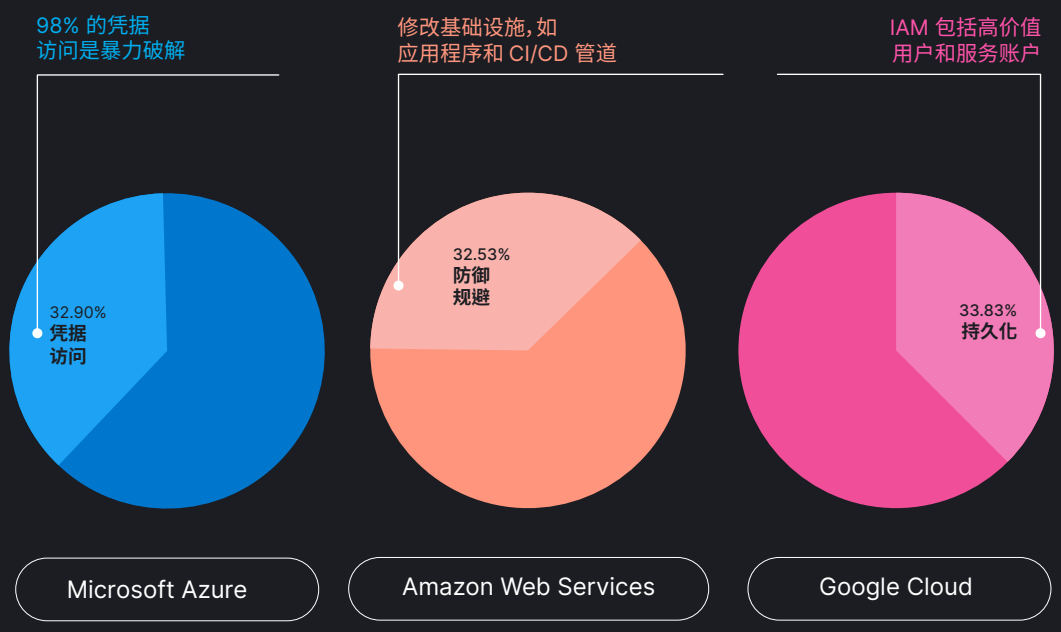
elastic security labs

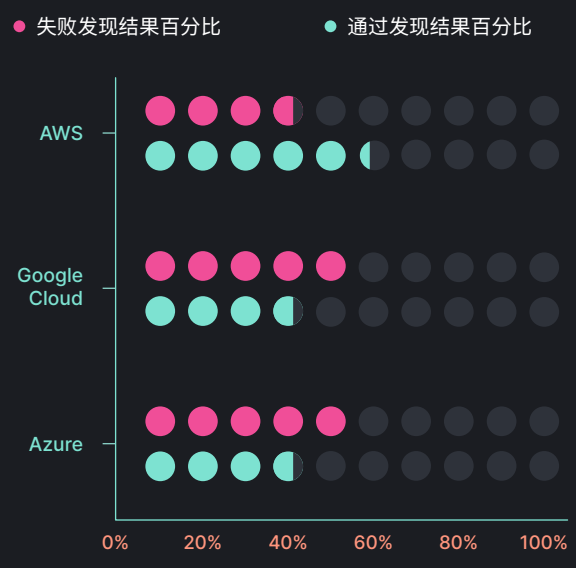
2024 年 Elastic 全球威胁报告中的

我们看到了云环境中的凭据访问、防御规避和持久性



可以使用 CIS 基准来保护云环境

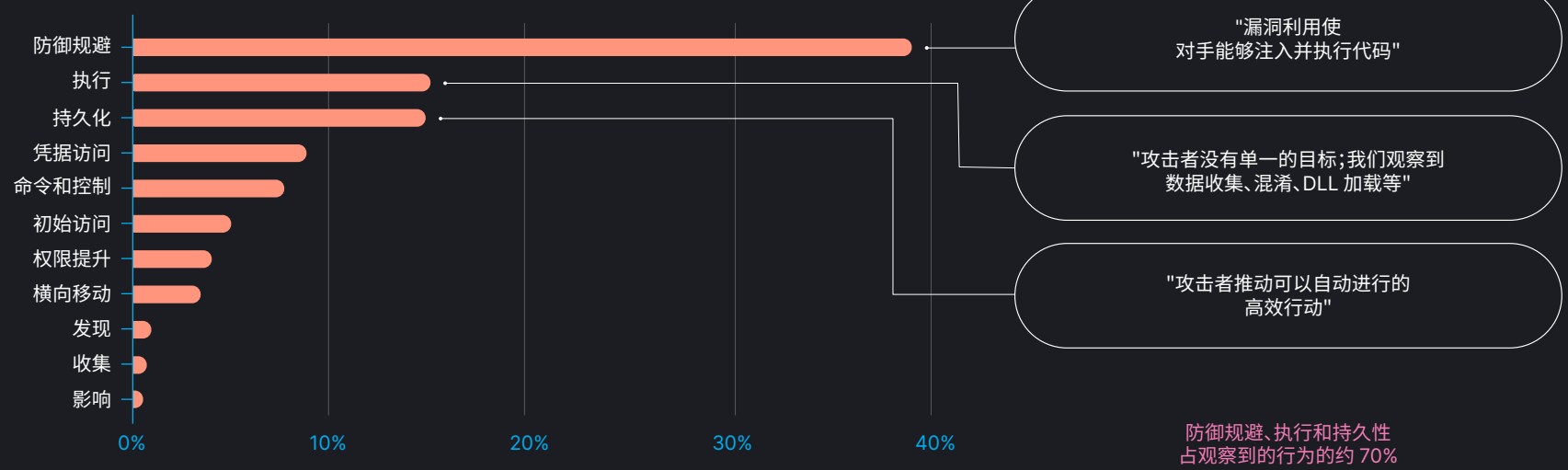
Elastic Security Labs 在每个主要 CSP 中都发现了检查失败的情况。检查您的云环境是否存在错误配置。



自去年以来发生了什么变化?

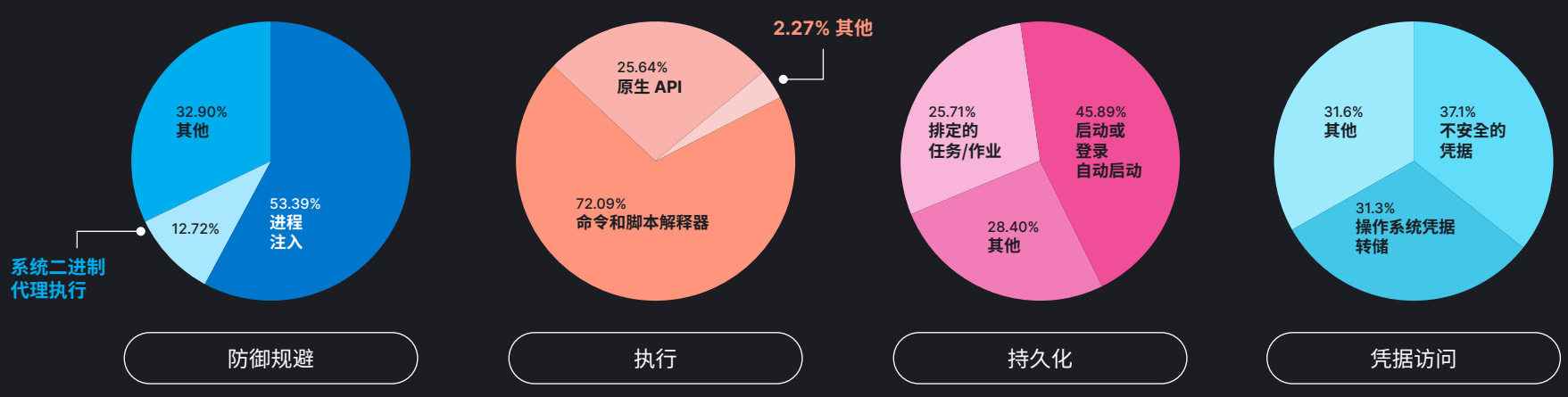
- 凭据访问技术**增加了 3%**，特别是不安全凭据**，增加了 31%**
- 防御规避技术**减少 6 %**
- 持久化技术**增加了 8%**

在终端内，攻击者：



防御规避、执行和持久性
占观察到的行为的约 70%

在 Windows 终端中观察到的技术（占操作系统遥测的 92.7%）



2025

年即将到来——请考虑采取以下行动:

- 计算您的 CIS 基准分数并规划如何提高它
- 在 X 上关注 @ElasticSecLabs
- 下载完整的 Elastic 全球威胁报告
- 使用 Elastic Security Labs 的检测工程行为成熟度模型审核您的保护库。

重点解决:

- 防御规避
- 执行
- 持久化
- 凭据访问