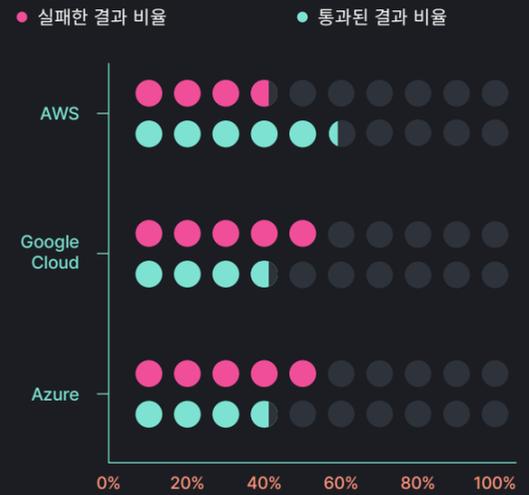
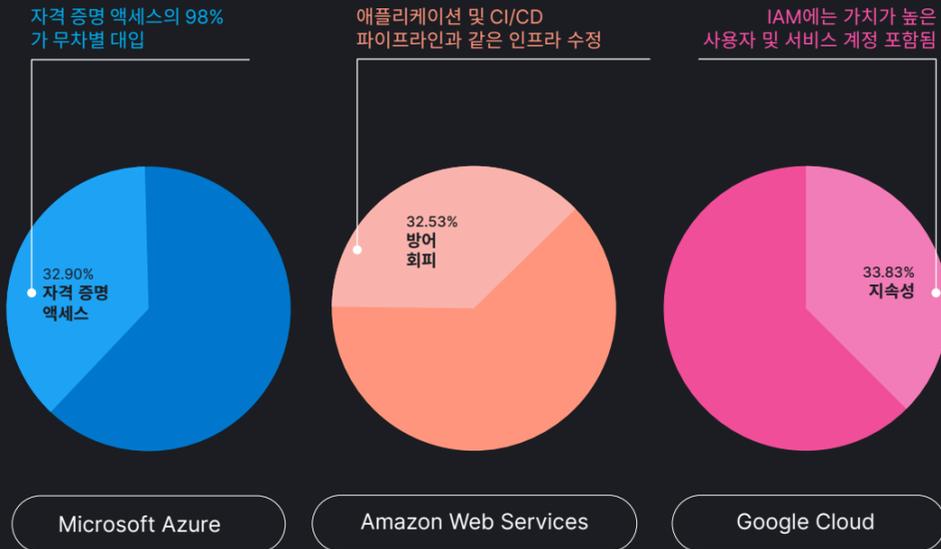


2024년 Elastic 글로벌 위협 보고서에서 살펴본 공격 방식

클라우드 환경에서 자격 증명 액세스, 방어 회피, 지속성 발견

CIS 벤치마크를 통해 클라우드 환경을 보호할 수 있습니다

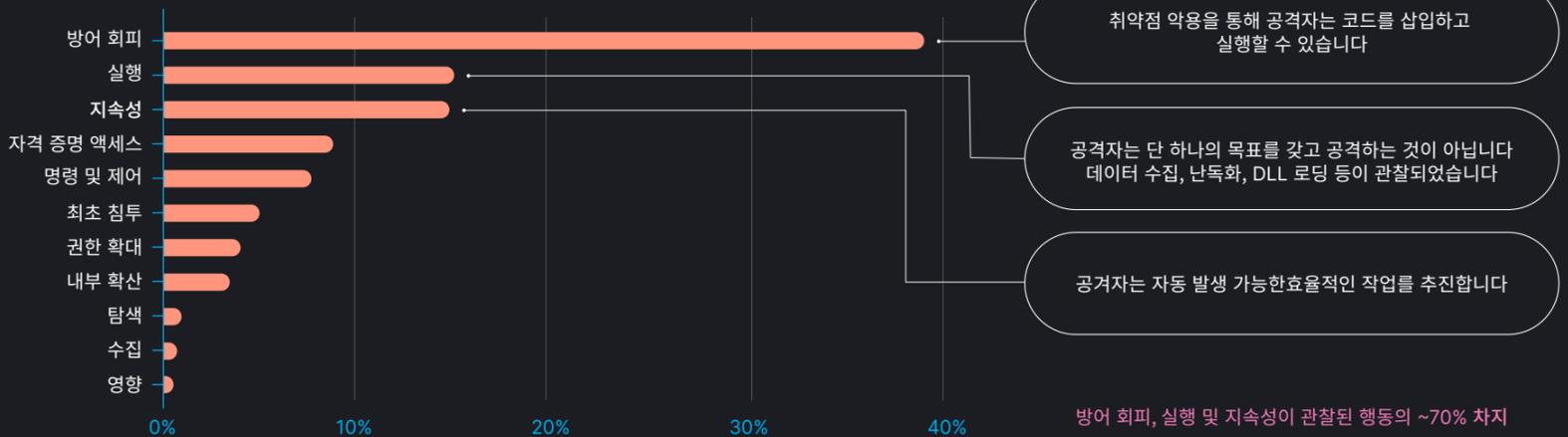
Elastic Security Labs는 모든 주요 CSP에서 점검 실패를 확인했습니다. 클라우드 환경에 잘못된 구성이 있는지 확인하세요.



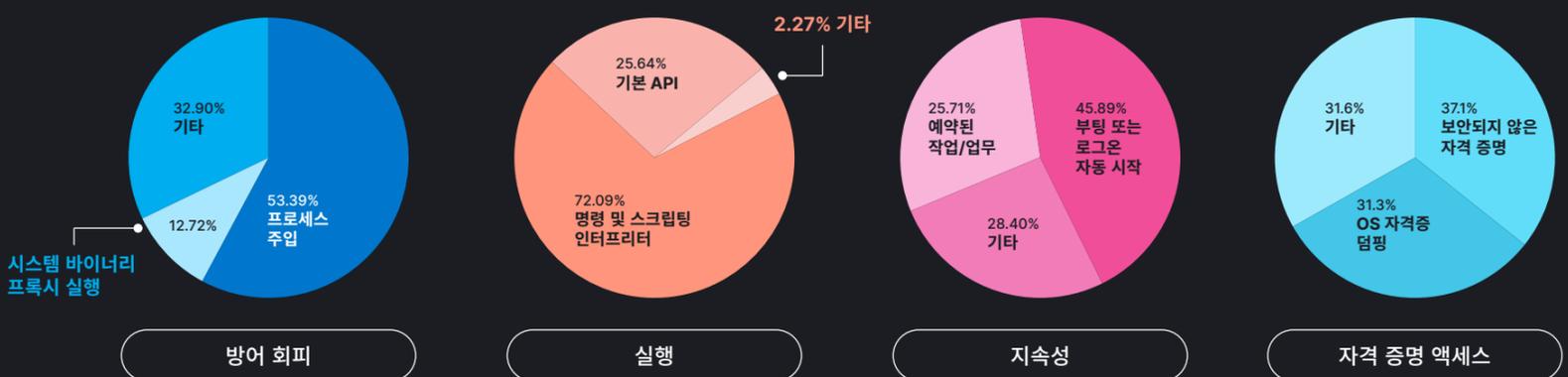
작년과 비교해 무엇이 달라졌나요?

- 자격 증명 액세스 기법 3% 증가, 특히 보안되지 않은 자격 증명의 경우 31% 증가
- 방어 회피 기법 6% 감소
- 지속성 기법 8% 증가

엔드포인트 내에서 공격자는 다음과 같은 기법을 사용합니다.



Windows 엔드포인트에서 관찰된 기법(OS 원격 측정의 92.7%)



2025
년을 준비하기 위해

- CIS 벤치마크 점수를 계산하고 점수를 높이는 방법 계획
 - X에서 @ElasticSecLabs 팔로우하기
 - Elastic 글로벌 위협 보고서 전문 다운로드
 - Elastic Security Labs의 Detection Engineering Behavioral Maturity Model로 보호 라이브러리 감사
- 다음 문제에 중점을 두세요.
- 방어 회피
 - 지속성 유지
 - 실행
 - 자격 증명 액세스