elastic security labs

2024

Elastic 글로벌 위협 보고서

보안 운영 센터(SOC) 리더들이 알아야 할 위협 동향

보안 팀과 최고 정보 보안 책임자(CISO)에게 실행 가능한 인사이트를 제공하기 위해 제작된 2024 Elastic 글로벌 위협 보고서는 공공 및 Elastic 고유의 원격 측정 데이터를 바탕으로 10억 개 이상의 데이터 포인트에 대한 수개월간의 분석을 통해 도출한 주요 결과를 제시합니다. 이러한 결과는 데이터에서 얻은 인사이트와 조직을 위한 권장 조치로 구성되었습니다.

주요 인사이트

01 많은 기업이 클라우드 환경을 잘못 구성하고 있습니다.

클라우드 보안 태세 관리(CSPM)에 대한 새로운 섹션에서는 환경을 인터넷 보안 센터(CIS) 기준과 비교했습니다. 그 결과, 클라우드 서비스 제공자(CSP)에 관계없이 평균적으로 약 50%의 환경이 점검를 통과하지 못한 것으로 나타났습니다.

02 방어 회피는 여전히 가장 흔히 나타나는 엔드포인트 전략입니다.

방어 회피는 엔드포인트 행동의 38%를 차지하며 이는 공격자들이 보안 시스템을 능숙하게 탐색하고 있음을 시사합니다. 특히 이 수치는 작년보다 6% 감소하여 방어 도구가 효과적으로 작동하고 있음을 강조합니다.

03 자격 증명 접근 경고가 계속 증가하고 있으며 특히 클라우드 내에서 두드러집니다.

클라우드 환경 내에서 자격 증명 접근은 전체 활동의 23%를 차지했습니다. 또한 엔드포인트 환경에서는 이러한 기법이 전년 대비 3% 증가한 것으로 나타났습니다. 이는 정보 도용자와 자격 증명 브로커의 증가 및 보안 도구의 가시성이 높아진 사실에 기인할 수 있습니다.

04 공격자는 시스템에 효율적으로 침입하기 위해 방어 도구를 악용합니다.

관찰된 악성 파일의 53%는 공격 보안 도구(OST)로 식별되었으며 이는 기업이 취약점을 발견하기 위해 활용하는 도구이자 공격자가 이를 악용하는 도구입니다. 이러한 OST는 프로세스 주입과 같은 새로운 기능을 만들기 위해 대규모 연구개발(R&D) 팀을 보유하고 있으며, 프로세스 주입은 방어 회피의 한 형태로 올해 Windows 경고 이벤트의 53%를 차지했습니다.

05 생성형 AI는 관찰된 공격의 빈도나 영향에 큰 변화를 주지 않습니다.

보안팀은 GenAI 공격의 급증을 우려해왔습니다. 위협의 규모는 다소 증가했지만 GenAI는 경보 요약 및 작업 자동화와 같은 기능을 통해방어 기술을 크게 강화했습니다.

 |

주요 제안 사항

01 환경을 자주 감사하세요.

공격자들은 허점이나 잘못 구성된 보안 통제를 통해 환경에 침투하고 있으며 침투한 후에는 센서와 데이터를 조작하는 데 집중합니다. 벤치마킹 및 위험 평가를 통해 모범 사례와 업계 표준을 활용하여 기업 내 액세스를 효과적으로 통제하고 있는지 파악할 수 있습니다.

02 보안 통제를 조정하여 생성형 AI에 대비하세요.

GenAI의 증가는 소셜 엔지니어링 시도의 증가로 이어질 것입니다. 사용자들에게 이러한 시도를 식별하는 법을 교육하는 것도 중요하지만 보안 팀은 통제와 권한 설정을 확인해 피싱 공격이 성공하더라도 장기적인 피해를 막을 수 있도록 해야 합니다.

03 방어 회피 공격을 무력화하기 위해 대화형 엔드포인트 에이전트를 구현하세요.

방어 회피 공격은 몇 년간 주요 전술로 사용되었습니다. 감소 추세에 있지만, 공격자들은 여전히 이를 통해 환경에 침투하고 있습니다. Elastic Agent와 같은 엔드포인트 기술은 필요한 도구의 수를 줄이면서도 가시성과 기능을 제공합니다.

04 노출된 자격 증명에 대한 강력한 대응 계획을 수립하세요.

무차별 대입 및 의심스러운 메모리에서 브라우저 자격 증명에 접근하는 등의 기법이 자주 사용되는 것이 관찰되었습니다. 노출된 자격 증명을 교체하고 침해 대응을 위한 신속한 워크플로를 구성하면 큰 차이를 만들 수 있습니다. 아직 다중 인증을 도입하지 않았다면 보안팀은 다중 인증을 의무화해야 합니다.

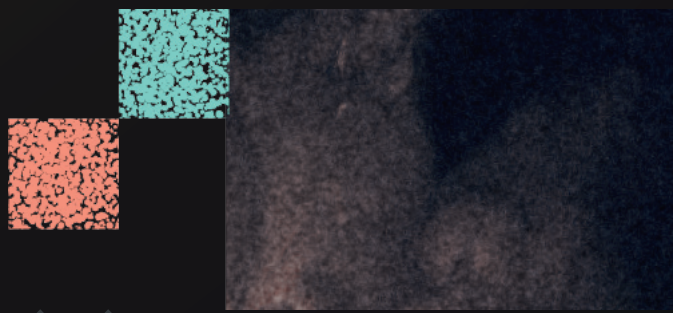
05 클라우드 환경을 CIS 벤치마크와 비교하세요.

The CIS 벤치마크는 업계 표준이며 주의가 필요한 영역을 빠르게 식별하는 데 도움이 됩니다. 팀은 점수를 모니터링하고 향상시키기 위한 계획을 수립해야 하며, 이는 장기적으로 위협 감지 능력을 향상시키고 위험을 줄이는 데 도움이 될 것입니다.

위협 환경을 마스터하세요

진화하는 위협에 대비하고 더 많은 정보를 얻으세요. 2024 Elastic 글로벌 위협 보고서에서 오늘날의 위협 환경에 대한 전체 분석과 모든 제안을 확인할 수 있습니다. @ElasticSecLabs 에서 전문가들을 팔로우해보세요 .

Elastic Security가 보안 운영을 현대화하는방법을 알아보세요.



 |

elastic security labs