사이버 보안 리스크 & 취약점 진단

트렌드 비전 원™
통합 보안 플랫폼으로
현재 보안 취약점 진단과
사이버 보안 리스크를
무료로 알아보세요.

Use case
인터넷과 연결된 자산의 취약점과 리스크가 궁금하다면

Use case
조직의
클라우드 보안 상태 점검이 필요하다면

Use case
이메일 데이터와 관련된 알려지지 않은 위협이 궁금하다면

Use case
엔드포인트의 위협 요소를 발견하고 보호하는 방법이 궁금하다면

Use case
모의 피싱 공격을 통해 보안 인식을 개선하고 싶다면

Use case
최신 글로벌 보안 위협에 얼마나 노출되어 있는 지 궁금하다면

클라우드 보안 설정 점검

필요성
복잡한 하이브리드 클라우드 환경을 보호하기란 쉽지 않습니다. 포인트 솔루션으로 구성된 보안 환경은가시성의 사일로를 야기하므로, 컴플라이언스 준수와 거버넌스가 매우 어려워지기 때문입니다.

혜택
보안 표준 지침 및 베스트 프랙티스에 따라 클라우드 인프라의 잘못된 구성, 총 규칙 검사 수, 규정 준수 요약 및 보안 위험을 식별할 수 있으며, 진단 결과에 따른 수정 지침을 적용해 공격 표면 위험 관리(ASRM)로 발전시킬 수 있습니다.

엔드포인트 취약점 분석

필요성
모든 엔드포인트는 잠재적인 해커들의 진입 관문입니다. 39초마다 발생하는 요즘의 사이버 공격에 대응하기 위해, 엔드포인트 위협을 선제적으로 탐지하고 분석하며, 방어해야 합니다.

혜택
트렌드마이크로의 고도화된 글로벌 위협 인텔리전스로 수집된 위협 지표가 엔드포인트 취약점 진단에 활용됩니다. 엔드포인트 스캔을 통해 악의적인 활동을 확인하고 최적의 조치를 취할 수 있습니다.

글로벌 보안 취약점 분석

필요성
사이버 공격 시 해커들이 취약점을 악용할 수 있는 모든 경우의 수를 고려해야 하는 것이 보안의 어려운 점입니다. 발견되지 않은 취약점은 네트워크와 시스템에 침투하는 사이버 공격의 성공률을 높이기 때문입니다.

혜택
엔드포인트에 특화된 스캔 및 진단으로 Log4Shell, Samba, OpenSSL과 같은 글로벌 오픈소스 위협의 영향을 확인하고 진단 받은 환경이 영향을 받았다면 필요한 단계별 조치를 선택할 수 있습니다.

*본 진단 서비스는 전세계 영향 수준의 취약점이 발견된 경우에만 제공 가능합니다.

외부 공격 표면 취약점 분석

필요성
사용자가 알려지지 않은 공격이나 관리되지 않는 사이버 자산을 모두 파악하기는 어렵습니다. 따라서 위험을 자체적으로 평가하고 소통하기란 거의 불가능합니다.

혜택
호스트 및 인터넷 포트에서 악용되기 쉬운 CVE 위험과 SSL 인증서 만료/취약 등 안전하지 않은 연결 문제를 확인할 수 있습니다. 트렌드 비전 원을 활용하면 사용자, IP, 클라우드 앱, 스토리지, 컨테이너 및 워크로드 전반의 공격 표면 가시성 관리도 가능합니다.

이메일 보안 취약점 분석

필요성
사이버 공격의 90% 이상이 피싱 이메일*로 시작됩니다. 가장 널리 쓰이는 소통 수단인 이메일은 이미 맬웨어, 랜섬웨어, 이메일 사기(BEC) 공격으로 몸살을 앓고 있습니다.

혜택
M365와 구글워크스페이스 이메일 사서함을 검사하여 최근 30일간의 악성 파일, URL, 피싱 및 랜섬웨어 공격 여부와 이력을 확인합니다. 내부적으로 가장 표적이 되는 사용자를 파악하여 이메일 공격을 차단하고 사서함을 보호합니다.

*출처: 딜로이트

이메일 모의 피싱 훈련

필요성
사이버 범죄자들의 피싱 공격과 이메일 사기 기법은 끊임없이 발전하고 있습니다. 이메일 피싱 공격을 인식하고 즉각 신고하는 임직원 행동 습관이 소셜 엔지니어링 공격을 예방하는 핵심입니다.

혜택
기존 템플릿으로 이메일 모의 피싱 공격을 실행해 본 후, 조직의 인적 위험 요소에 대한 상세한 인사이트가 제공됩니다.

진단 서비스를 신청하시는 모든 분께

진단 영역 별로 취약한 보안 상태의 범위, 진단을 통해 발견된 정보, 추천 대응 방안 및 단계별 조치 방법까지 한 눈에 볼수 있는 **결과 리포트**를 제공해 드립니다.

지금 진단해 보세요