IBM Security

IBM Security 위협 관리 서비스

지속적인 탐지.

지속적인 예방.

내장된 대응 기능.

24X7 침해 신고 직통 전화

국내: 한국IBM 임귀빈과장

010-4995-6380

해외: (+001) 312-212-8034

IBM

과제

엔드포인트에 대한 위협이 증가하면서 EDR(Endpoint Detection and Response, 엔드포인트 탐지 및 대응) 툴이 널리 사용되기 시작했습니다. EDR 솔루션 시장(SW)은 2026년까지 미화 71억 5천만 달러 규모로 성장할 것으로 예측되며 이 예측 기간 중 CAGR은 24.9%입니다. 이러한 복잡한 툴은 SOC 통합을 요구하며 방대한 양의 알림을 생성할 수 있습니다. 적절한 튜닝이 이루어지지 않으면 이러한 알림 중 대부분이 오탐(false positive)일 수 있으나, 그럼에도 이 모든 알림을 조사해야 합니다. 하지만 과도한 업무에 시달리는 보안 팀은 연중무휴(24x7) 보안 운영을 위해 이러한 알림을 철저하게 조사할 시간이나 숙련된 시스템 관리 인력이 부족할 수 있습니다. 취약점 관리 서비스(Vulnerability Management Services)를 포함하는 IBM Security의 매니지드 탐지 및 대응 서비스(Managed Detection and Response Services)는 선도적인 EDR 플랫폼을 활용하여 기존 검사 툴을 배포, 튜닝 및 최적화하고, 가장 중요한 알림을 우선적으로 처리하며, 오탐을 줄이고, 지능적인 최신 공격을 신속하게 탐지, 조사 및 대응하도록 지원할 수 있습니다.

멀티벡터 탐지. 우선 순위별 대응.

- 멀티벤더 시나리오를 포함, 선도적인 EDR 플랫폼이 제공하는 알림을 통해 위협을 통합, 튜닝, 관리
- IBM Security X-Force Threat Intelligence를 활용하여 지능형 공격 탐지
- 위협 추적 팀은 IBM의 독자적인 위협 추적 라이브러리를 활용하여 악의적인 TTP를 찾아낼 수 있으며, 이를 통해 지능형 보안 위협에 대한 가시성 제공
- 위협의 성공에 기여할 중대한 취약점을 찾아내어 가장 긴급한 알림을 우선적으로 처리
    - 해커가 구축한 IBM Security의 자동화된 순위 지정 엔진은 취약점이 인더와일드(in the wild)에서 악용되는지 여부, 자산 가치, 기타 공격자 관련 인텔리전스와 같은 주요 위험 요인을 기반으로 취약점의 우선 순위를 정함
- 5곳의 글로벌 통합 SOC에서 모니터링 분석가, 인시던트 대응자, 위협 추적 전문가로 구성된 조사 팀이 최신 지능형 위협에 대해 상시적으로 탐지 및 대응을 수행
- 전문가가 주도하지만 자동화된 조치를 통해 대응 속도를 높여 위협 통제

지속적인 예방. 지속적인 보호.

- 문제 해결 노력을 집중할 대상을 알 수 있도록 지속적인 취약점 관리를 통해 가장 위험도가 높은 취약점을 파악하여 우선 순위 지정
- 전체 자산 소유자에 대해 문제 해결 프로세스를 촉진하고 패치 적용이 불가능하거나 실용적이지 않을 경우에 대한 대응책 제공
- 지속적인 예방 정책 튜닝 및 관리
- 어떠한 검사 툴이든 배포 및 관리 가능
- X-Force Threat Intelligence는 새로운 위협에 선제적으로 대응할 수 있도록 심층적인 연구 분석 및 글로벌 위협 인텔리전스를 제공

IBM Security MDR에 대해 자세히 알아보기
IBM Security VMS에 대해 자세히 알아보기

감소된 공격 표면에 대한 지속적인 탐지 및 예방

심층적 가시성 제공, 상세한 조사 수행

인텔리전스 기반으로 24/7 알림 모니터링과 분석이 제공되며, 이러한 정보를 X-Force 분석가, 인시던트 대응자, 위협 추적 전문가가 공유

위협 추적 전문가의 지원으로 일관된 성과 달성

TTP에 집중하여 정적 IOC보다 위협을 더욱 일관성 있게 찾아내고 위협 환경의 변화에 상관없이 성과 달성

빠른 대응 및 적극적 차단

전문가가 주도하는 자동화된 조치를 통해 대응 속도를 높임으로써 위협을 통제

해커들이 이끄는 집중적 취약점 관리

툴에 상관없이 검사를 관리하고 자동으로 우선 순위를 지정하며 위험도가 높은 취약점을 먼저 해결하도록 지원