IBM Security 매니지드 탐지 대응 서비스(MDR)

AI 기반 연중무휴(24/7) 매니지드 예방, 탐지, 대응 체계를 통한 신속한 위협 차단

노트북, 데스크탑, 그리고 원격 근무자가 점점 더 늘어나는 가운데, 귀사를 노리는 지능적인 사이버 범죄자의 잠재적 공격 경로도 많아졌습니다. 사이버 범죄자들은 그러한 진입 지점을 통해 은밀하게 깊은 곳까지 침투하곤 합니다. 설상가상으로, 이와 같은 지능형 공격으로부터 귀사를 보호할 사내 보안 인력의 부족은 문제를 더 복잡하게 만듭니다.

이처럼 확대되는 공격 범위에 맞서려면, 시그니처 기반의 사후 대응 중심 위협 관리 솔루션에서 벗어나 인텔리전스 기반의 선제적 방식으로 전환해야 합니다. 즉, 상시적으로 모니터링과 분석을 실시하면서 지능형 공격에 신속히 대처할 수 있도록 뛰어난 역량을 가진 보안 전문 팀을 활용해야 합니다. 기술만으로는 지능형 공격을 막아낼 수 없습니다. 기업이 각종 공격을 성공적으로 방어하려면 신뢰할 수 있는 파트너가 필요합니다. 네트워크 및 엔드포인트를 상시 모니터링하고 가시성을 제공하면서 대응 조치를 자동화하고 위협을 추적하여 악성 활동을 파악하고 인시던트 대응(IR) 경험을 근간으로 한 첨단 위협 인텔리전스를 활용하는 파트너가 필요합니다.

주요 특징

- IBM Security의 매니지드 탐지 대응(Managed Detection and Response, MDR) 서비스는 위협 관리 라이프사이클의 전 범위를 관리하는, 업계에서 가장 포괄적인 솔루션 포트폴리오인 IBM Security X-Force Threat Management의 구성 요소입니다.
- AI를 활용하고 위협 인텔리전스를 기반으로 하는 탐지, 위협 추적, 대응 방식으로 각종 공격을 방어합니다.
- 벤더 중립적인 솔루션으로 고객의 기존 보안 기술 투자를 보호합니다.
- IBM의 독자적인 위협 추적 라이브러리를 활용하여 악의적인 TTP를 선제적으로 찾아냅니다.

IBM Security 매니지드 탐지 대응 서비스(MDR)

IBM Security의 매니지드 탐지 대응 서비스(MDR)에서는 연중무휴 하루 24시간 위협을 탐지하고 신속하게 대응합니다. 이를 위해 위협 인텔리전스 및 선제적 위협 추적 기술을 활용하여 발견되지 않은 위협을 더 빨리 밝혀내고 SOC 생산성도 향상시킵니다. IBM의 AI 기반 자동화 기술과 전문가가 주도하는 분석의 시너지를 통해 하이브리드 멀티클라우드 환경의 모든 네트워크와 엔드포인트에서 더 신속하게 위협에 대응합니다.

IBM Security MDR은 엔드포인트 탐지 대응(Endpoint Detection and Response, EDR) 툴과 네트워크 탐지 대응(Network Detection and Response, NDR) 툴로 구성되어 면밀한 조사를 수행합니다. 여기에는 IBM의 독자적인 TTP(Tactics, Techniques and Procedures) 위협 추적 라이브러리, 그리고 행동 기반 차단 및 상시 정책 관리를 지원하는 차세대 안티바이러스가 포함됩니다. 이 종합 위협 관리 서비스에서는 IBM의 글로벌 SOC(Security Operations Centers) 네트워크, 통합형 인프라, 높은 전문성 및 위협 인텔리전스를 활용합니다. 그 결과, 우수한 가시성 및 실행 가능한 인사이트를 확보하여 제로데이 위협을 비롯한 각종 위협을 효과적으로 차단할 수 있습니다.

IBM Security MDR의 주요 특징과 이점

뛰어난 가시성, 면밀한 조사

IBM의 세계 정상급 X-Force 위협 인텔리전스 및 인시던트 대응 팀에서는 유기적 특성의 위협 인텔리전스에 분석 기술을 접목하여 여러 공격 벡터와 그 상황을 파악하는 방식으로 모든 네트워크 및 엔드포인트를 대상으로 연중무휴 하루 24시간 위협을 차단합니다.

미래의 위협까지 차단할 수 있는 일관성 있는 결과

IBM Security MDR에서는 IBM의 독자적인 TTP 위협 추적 라이브러리를 활용하면서 정적 침해 지표(Indicators of Compromise, IOC)보다 더 일관성 있게 위협을 찾아내고, 변화무쌍한 위협 환경에서도 유의미한 결과를 제공합니다.

복잡성 없는 포괄적인 보안

IBM Security MDR의 통합된 역량이 고객의 기존 엔드포인트/네트워크 보안 기술을 지원하므로, '걷어내고 바꿔야 하는' 부담이 없고 특정 벤더에 종속될 염려도 없습니다.

빠른 대응, 능동적 차단

IBM Security MDR은 AI 기반 자동화, 통합형 SOAR 역량, 상시 플레이북 라이프사이클 관리를 통해 자동화된 대응, 또는 사람에 의한 대응으로 위협을 미리 차단할 수 있게 합니다.

글로벌 위협 인텔리전스 + AI 기반 자동화의 조합으로 전사적 범위의 강력한 보호 실현

우수한 인텔리전스가 있어야 신속한 탐지가 가능합니다. IBM 보안 전문가 팀은 IBM Security MDR의 신뢰도 높은 24시간 탐지 기술과 IBM Security X- Force 지능형 위협 인텔리전스 피드 및 세부 분석을 통합하여 활용합니다. 이렇게 확보하는 추가 컨텍스트, 맞춤형 탐지 정보와 인사이트를 바탕으로 상시 위협 추적 체제를 마련할 뿐만 아니라, 숙련된 위협 분석을 통해 고객이 더 빨리, 선제적으로 위협을 탐지하도록 지원합니다.

IBM Security MDR의 AI 기능은 기존 방어 시스템의 틀에 머무르지 않는 혁신을 보여줍니다. IBM의 AI 스택에서 모든 네트워크와 엔드포인트에서 발생하는 알림을 자동 필터링하여 오탐(false positive)으로 인한 불필요한 정보를 없애므로, 고객은 우선순위가 높은 위협에 집중할 수 있습니다. 게다가 IBM Security MDR은 독자적인 희소 이벤트 탐지(Rare Event Detection) 알고리즘을 적용하여 고객 환경에서 제로데이 취약점을 찾아냅니다. 더 나아가 IBM은 SOAR 기능을 통합하여 운영 효율성을 확보하는 것은 물론 협업 및 상시 플레이북 라이프사이클 관리까지 지원합니다.

숙련된 IBM Security 전문가와 IBM 위협 인텔리전스 및 첨단 AI 역량이 만나 진정한 시너지 효과를 발휘하는 IBM Security MDR 위협 관리 솔루션은 차별화된 방식으로 엔터프라이즈 보호를 극대화합니다. IBM 글로벌 SOC의 분석 및 인시던트 대응 팀은 소위 '해가 지지 않는(follow-the-sun)' 상시 운영 모델에 따라 근무합니다. IBM Security X-Force 위협 인텔리전스를 적용하고 다양한 업종에서 수천 건의 IR 조사를 수행한 경험을 살려 가장 중대한 알림을 신속 탐지하고 우선순위에 따라 처리합니다. 이처럼 IBM Security MDR 전문가는 해박한 IR 지식을 바탕으로 조사 보고서를 제출하고 IR 권장 사항을 제안하며, 리스크 평가, 컴플라이언스 검토 등의 컨설팅으로 보안 태세 강화를 지원합니다.

전문가가 주도하는 선제적 위협 추적으로 기존 예방 범위 확대

선제적 위협 추적은 IBM Security MDR의 핵심 구성요소 중 하나이며, 기존 보안 솔루션을 완벽하게 보완하면서 기업 환경 내 이상 활동을 밝혀냅니다. 이 선제적 위협 추적을 담당하는 IBM 팀은 고객과 함께 가장 귀중한 자산 및 중대 과제를 식별합니다. 위협 추적 팀은 이 정보를 바탕으로 완전 맞춤형 위협 추적 리포트를 작성하고 맞춤 탐지 정보를 생성합니다.

IBM의 추적 전문가 팀은 MITRE ATT&CK 프레임워크 및 독자적인 TTP 위협 추적 라이브러리도 활용합니다. 수백 개의 위협 추적 시스템에서 텔레메트리 수집을 자동화하므로, IBM 추적 전문가는 가시성 향상을 위한 분석에 집중하면서 잠재적 위협과 고도로 지능적인 공격자까지 밝혀냅니다. 사람이 주도하지만 고도로 자동화된 IBM 위협 추적 인텔리전스가 IBM의 글로벌 위협 인텔리전스, 데이터 및 기능에 쓰이면, 빠르고 결단력 있는 공격 대응이 가능해집니다.

IBM Security MDR + X-Force 인시던트 대응 + 위협 인텔리전스 = 강력한 위협 방어 체계

IBM Security 매니지드 탐지 대응 서비스(MDR)에서는 단일 통합 위협 관리 전략을 통해 다양한 엔드포인트/네트워크 보안 기술과 위협 인텔리전스는 물론 글로벌 분석가 수천 명의 전문성까지 활용합니다. 따라서 탁월한 가시성으로 전사적 범위에서 효과적으로 위협을 탐지하고 대응하면서 보호할 수 있습니다.

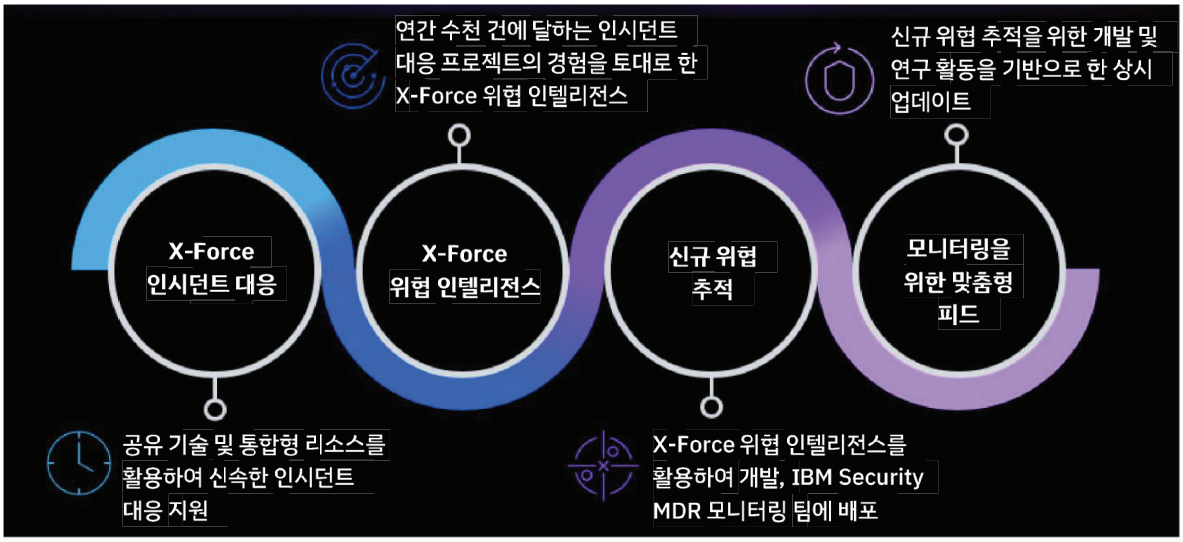

그림 1: 인시던트 대응, 위협 인텔리전스, 매니지드 탐지 대응의 팀워크

왜 IBM인가?

IBM Security는 가장 진일보한 통합 엔터프라이즈 보안 제품/서비스 포트폴리오를 제공합니다. 세계적 명성의 IBM Security X-Force® 연구소가 뒷받침하는 이 포트폴리오는 기업이 비즈니스의 기본 구성요소로 보안을 적용하여 불확실성을 극복하고 성공을 누리는 데 필요한 보안 솔루션을 제공합니다.

IBM은 가장 광범위하면서 수준 높은 보안 연구, 개발, 서비스 조직을 운영하면서 130여 개국에서 월 1조 건 이상의 이벤트를 모니터링하고 있으며, 3,000개 이상의 보안 특허를 보유하고 있습니다. 자세한 내용은 ibm.com/security를 참고하시기 바랍니다.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

자세한 정보

IBM Security 매니지드 탐지 대응 서비스에 대한 자세한 내용은 IBM 영업대표 또는 IBM 비즈니스파트너에 문의하시거나, 다음 웹사이트에서 확인하시기 바랍니다.
https://www.ibm.com/security/services/managed-detection-response

한국IBM: 임귀빈과장
010-4995-6380
gwibin.im@ibm.com