IBM QRadar Advisor with Watson

AI를 활용한 SOC 자동화

주요 특징

- 분석가와 기술 간의 새로운 파트너십 실현
- 인시던트 분석 자동화, 팀의 업무 생산성 및 역량 극대화
- 일관성 있는 심층 조사 활성화
- 더 신속하고 결단력 있게 인시던트 에스컬레이션 수행
- 체류 시간 단축

오늘날 SOC의 과제

귀사의 보안 팀원이 2명이건 100명이건 간에, 궁극적인 목표는 비즈니스 성공을 뒷받침하는 것입니다. 그러기 위해서는 중요 시스템, 사용자, 데이터를 보호하고 위협을 탐지하여 대응하며 선제적으로 사이버 범죄에 대처해야 합니다. 그러나 오늘날 보안관제센터 (Security Operation Center, SOC)가 당면한 수많은 중대 과제가 이러한 목표 달성에 걸림돌이 될 수 있습니다.

미해결 위협

분석가가 정보의 연관성을 파악하지 못해 방치되는 정보가 너무 많습니다. 실행 가능한 인사이트를 찾아내기가 쉽지 않기 때문에 분석가가 확실히 알고 있는 사례만 다룰 가능성이 있으며, 그로 인해 일부 조사가 누락되면서 조직이 위험에 노출되기도 합니다.

인사이트 과부하

분석해야 할 인사이트가 너무 많고 다양하며 빠르기 때문에 작업의 우선순위를 정하고 근본 원인을 규명하는 데 어려움이 있습니다. 이는 크고 작은 기업 모두가 겪고 있는 상황입니다. 국지적인 컨텍스트를 결합하여 시급한 문제를 빠르게 파악하려면 어디서 출발해야 하는지를 정확하게 알고 있는 분석가가 없습니다. 이들 대다수가 반복적인 작업과 피로감에 시달립니다. 그 결과, 정의된 프로세스는 어긋나고 중요한 IoC(Indicator of Compromise)를 놓치기 쉽습니다. 연관성 있는 모든 위협을 분류하지 못하는 조직이 전체의 93%[1]에 달합니다. 또한 1/4[2]가까이는 이러한 경고를 조사하지 않고도 비즈니스에 큰 타격 없이 지나간 것을 다행으로 여깁니다.

더 심각해지는 체류 시간

보안 전문가가 데이터 보호 및 방어의 성공을 평가할 때 많이 쓰는 지표 중 하나가 체류 시간(dwell time)인데, 주로 MTTD(Mean Time To Detect)와 MTTR(Mean Time To Respond)을 사용합니다. 체류 시간은 어떤 위협 주체가 완전히 제거될 때까지 들키지 않고 네트워크에서 액세스 권한을 행사한 기간을 말합니다.

그 어느 때보다 많은 솔루션과 데이터가 있음에도 불구하고, 현재 평균 체류 시간은 50일에서 200일까지 매우 다양합니다. 이 지표가 왜 중요할까요? Ponemon Institute에 따르면, 100일 이내에 보안 침해를 찾아낸 기업은 100일 넘게 걸린 기업보다 100만 달러 이상 비용을 절감했습니다. 이외 비슷하게, 30일 이내에 보안 침해를 차단한 곳은 문제 해결에 30일 넘게 걸린 곳보다 100만 달러 이상을 절감했습니다.[3] 일관성, 품질, 컨텍스트의 삼박자를 모두 갖춘 조사가 이루어지지 않으면, 기존 프로세스는 무너지고 핵심 인사이트를 놓칠 가능성이 증가하여 결국 조직이 위험에 노출될 수 있습니다.

사이버 보안 인력 부족과 업무 피로감

여느 보안 분석가와 마찬가지로, 귀사의 팀도 부족한 인력으로 과중한 업무를 처리하느라 지친 상태일 것입니다. 그들의 잘못이 아닙니다. 사람의 힘만으로는 날로 확대되는 위협 환경을 다룰 수 없습니다. 게다가 SOC는 일상적인 보안관제 업무로 눈코 뜰 새 없이 바쁩니다.

사이버 보안 팀이 겪는 피로감은 귀사만의 문제가 아닙니다. 2018년에 실시된 ESG Research의 조사에서 사이버 보안 "전문 인력 부족이 큰 문제"라고 밝힌 곳이 51%에 달했습니다. 이는 2017년의 45%에서 증가한 것입니다.[4] 사이버 보안 인력의 업무 피로감은 현실적인 문제입니다. ESG에 따르면, 이미 사이버 보안 전문가의 38%가 인력난으로 기존 팀의 피로도가 극에 달하고 인력 이탈이 심화되었다고 지적합니다. 앞으로 데이터는 계속 급증하고 스킬 갭이 점점 더 벌어지면서 상황은 악화일로를 거듭할 것입니다. 2022년에는 충원하지 못한 보안 일자리가 180만 개에 이를 것으로 예상됩니다.[5] 티어 1, 즉 최일선의 분석가들 중에는 보안 업종 및 보안 팀에서 일한 경험이 없는 경우가 많습니다. 이들이 실력과 자신감을 키우면서 어엿한 전문가로 성장하려면 시간이 걸립니다.

빠르게 더 많이 도입되는 포인트 솔루션

CISO들은 더 정교해지는 새로운 위협을 차단하기 위해 더 많은 포인트 솔루션을 도입하고 있습니다. 중요 데이터 보호, 내부자 위협 차단, 신원 및 액세스 관리, 자격 증명 오용 방지 등 어떤 활용 사례에서든 곧 온갖 솔루션에 둘러싸이게 됩니다. 결국 솔루션 간 통합 문제, 확장성 부재, 까다로운 사용법 등으로 어려움을 겪게 됩니다.

최고의 위기 상황

어려움을 호소한다고 해서 문제가 해결되지는 않으며, 감정이 상한 고객의 신뢰를 회복하기도 어렵습니다. Ponemon Institute에 따르면, 데이터 유출 사고로 인해 발생하는 총비용이 2017년의 평균 362만 달러에서 386만 달러로, 6.4% 증가했습니다. 6 보안 책임자는 경영진, 고객, 직원, 투자자, 감독 기관, 보험사, 감시 단체 등 다방면에서 더 촘촘해지는 감시의 눈 아래 있습니다. 귀사는 이처럼 전례 없이 위태로운 상황을 아무런 준비 없이 견뎌낼 수 있습니까?

분석가와 기술 간의 새로운 파트너십 실현

인공 지능은 이러한 빈틈을 채우고 보안 분석가와 이들이 사용하는 기술 간의 새로운 파트너십을 가능하게 합니다. 사람인 분석가는 상식적인 판단이 가능하고, AI는 편향을 해소할 뿐만 아니라 플러스/마이너스 요인을 분석하는 등 저마다 장점이 있습니다. 하지만 이들이 하나의 팀을 이룬다면 더 효과적으로 위협을 차단하고 체류 시간을 단축할 수 있습니다.

AI를 접목한 SOC의 이점

인시던트 분석 자동화, 팀의 업무 생산성 및 역량 극대화

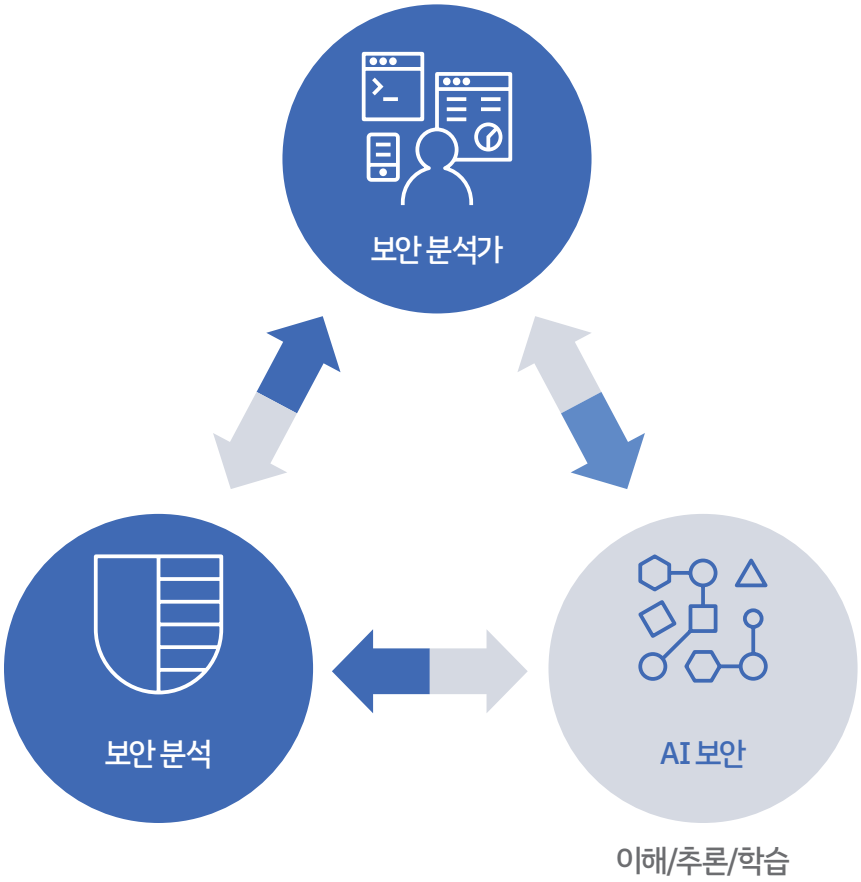
일상적인 분석에 인적 자원을 낭비할 필요가 없습니다. 반복적인 SOC 업무는 AI에 맡겨 자동화하고, 분석가들은 조사에서 더 중요한 요소에 집중하면서 더 효율적으로 일할 수 있습니다.

일관성 있는 심층 조사 활성화

분석가들이 업무 수행에 필요한 정보의 8%만 감당할 수 있다는 사실을 알고 계십니까? 이제 SOC를 업그레이드할 차례입니다. AI를 도입하여 인지 추론(cognitive reasoning)을 통해 여러 인시던트의 공통점을 발견하고 실행 가능한 피드백을 컨텍스트와 함께 제공할 수 있습니다. AI는 분석가를 위한 맞춤형 어드바이저라 할 수 있습니다. AI가 현장에서 외부 위협에 관한 인텔리전스를 수집해오면 그것을 토대로 분석가가 분석 작업에 컨텍스트를 추가합니다. 그러면 전혀 다른 듯 보였던 인시던트들의 연관성을 파악하면서 시간을 절약할 수 있습니다. 금요일 오후 4:30이든 월요일 오후 10:00든 언제나 분석 팀은 일관성 있는 철저한 조사에 집중해야 합니다.

체류 시간 단축

더 신속하고 결단력 있는 에스컬레이션 프로세스로 MTTD와 MTTR을 줄여야 합니다. MITRE ATT&CK 모델과 같은 동적 플레이북을 활용하여 공격을 분석함으로써 근본 원인을 밝혀내고 자신 있게 다음 단계를 진행할 수 있습니다.



AI는 보안 분석가와 이들이 사용하는 기술 간의 새로운 파트너십을 가능하게 합니다.

IBM QRadar Advisor with Watson – 최일선의 보안 분석가를 위한 AI 기반 솔루션

IBM QRadar Advisor는 보안 분석가가 인시던트에 대해 일관성 있는 조사, 신속하고 결단력 있는 에스컬레이션을 수행하여 체류 시간을 줄이고 분석 업무의 효율성을 높이도록 지원합니다.

팀의 업무 생산성 및 역량 극대화

- 위험도 순으로 조사의 우선순위 결정
- 중요도를 기준으로 더 빨리 데이터 필터링/정렬 수행
- 사내외 위협 인텔리전스 피드를 활용하여 더 유익한 IBM Watson 피드백 실행

일관성 있는 심층 조사 활성화

- 교차 조사 분석을 통해 연관된 관찰 지표를 찾아내 자동으로 조사 연계, 이미 파악한 잠재적 인시던트 이외의 영역까지 확장하여 분석
- 작업 중복 방지
- 같은 이벤트에 의해 여러 차례 중복 조사가 실행될 경우, 추가 조정의 필요 여부 결정

체류 시간 단축

- MITRE의 ATT&CK 모델을 통해 공격의 경위 및 진행 상황, 진행 단계별 신뢰도, 이미 시도한 전술, 앞으로 시도 가능한 전술을 시각화
- Easy Incident Scoring을 활용하여 분석가에게 더 신속하고 결단력 있는 에스컬레이션 프로세스 제공
- 분석의 효율성 제고, MTTD 및 MTTR 단축

직접 확인해 보십시오. 이미 AI를 활용하여 여러 효과를 누리고 있는 IBM 고객의 사례가 입증합니다. Sogeti Luxembourg의 분석 팀은 두세 시간 걸리던 조사 작업을 2~3분 만에 완료할 수 있게 되었습니다. 이제는 실제 위협을 조사하고 더 의미 있는 컨텍스트를 추가하는 데 이 값진 시간을 사용합니다. 그 밖의 많은 고객사에서 AI를 적용하여 훨씬 더 생산적이고 유능한 팀으로 거듭나고 있습니다. 아울러, AI 덕분에 상대적으로 숙련도가 떨어지는 인력도 티어 1 분석가 직무에 투입할 수 있습니다. 기존 티어 1 분석가는 티어 2 임무에 집중하면서 생산성과 역량을 획기적으로 향상시킬 수 있습니다.

AI와의 새로운 파트너십에 관한 다른 성공 사례와 자세한 정보를 ibm.biz/learnAI에서 확인하실 수 있습니다.

1 McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-quarterly-threatsdec-2016.pdf)

2 McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-quarterly-threatsdec-2016.pdf)

3 Cost of a Data Breach. Ponemon, 2018.(https://www.ibm.com/security/data-breach)

4 Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/com_hsd/report/213/document/ESG-Research-Insights-Paper-Spirent-2018.pdf)

5 Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/com_hsd/report/213/document/ESG-Research-Insights-Paper-Spirent-2018.pdf)

6 Cost of a Data Breach. Ponemon, 2018.(https://www.ibm.com/security/data-breach)

왜 IBM인가?

IBM Security는 가장 발전되고 통합된 엔터프라이즈 보안 제품 및 서비스 포트폴리오를 제공합니다. 세계적 명성의 IBM X-Force® 연구소가 뒷받침하는 이 포트폴리오는 기업이 효과적으로 위험을 관리하고 새로운 위협으로부터 조직을 보호하도록 지원합니다. IBM은 전 세계에서 가장 광범위한 보안 연구, 개발, 서비스 조직을 운영하면서 매일 130여 개국에서 350억 건 이상의 보안 이벤트를 모니터링합니다. 아울러 8,000여 개에 달하는 보안 특허를 보유하고 있습니다. 자세한 내용은 ibm.com/security에서 확인하세요. 또한 Twitter에서 @ibmsecurity를 팔로우하거나, IBM 보안 인텔리전스 블로그를 참조하실 수 있습니다.

자세한 정보

QRadar Advisor with Watson에 대한 자세한 내용은 IBM 영업대표에게 문의하거나 ibm.com/us-en/marketplace/cognitive-security-analytics를 참조하세요.