AhnLab

Case Study

AhnLab SOAR로 완성한 스마트 금융 보안 관제

산업

- 종합금융그룹

혜택

- 관제 업무 프로세스 최적화로 분석 및 조치 시간 단축
- 유연한 플레이북(Playbook) 설계를 통한 고객사 맞춤형 보안 로직 구현
- 이벤트 탐지부터 대응까지 전 과정 시각화 및 체계화
- 사용자 중심의 직관적인 워크플로우 설계 지원
- 위협 인텔리전스(Threat Intelligence, TI) 기반 대응 역량 강화

솔루션

- AhnLab SOAR

개요

K사는 11개 이상의 자회사를 기반으로 다양한 금융 상품과 서비스, 솔루션을 제공하는 국내 대표 종합금융그룹이다. 탁월한 리스크 관리 역량과 차별화된 디지털 금융 플랫폼을 바탕으로 금융 혁신을 선도하고 있다.

디지털 전환의 흐름 속에서 K사는 보안 관제 업무의 자동화 구현과 가시성, 효율성 강화를 목표로 AhnLab SOAR를 도입했다. 기존에는 SIEM(Security Information and Event Management)을 통해 이벤트를 수동으로 분석하고 대응했으나, SOAR의 도입을 통해 보안 운영 환경을 체계적으로 개선하고 프로세스 전반을 자동화할 수 있었다. 특히, SOAR는 위협 이벤트에 대한 1차 분석을 자동화함으로써 관제 품질을 높이고, 관제 담당자가 보다 신속하고 정확하게 대응할 수 있도록 지원한다.

SOAR 도입 이후 보안팀의 업무 효율성과 사고 대응 역량은 눈에 띄게 향상됐으며, SIEM, 방화벽, UTM(Unified Threat Management), 사내 메신저 등 다양한 시스템과의 유기적인 통합으로 보안 관제 고도화에 기여하고 있다. 더불어, 계열사 보안 담당자들과의 정보 공유, 공동 대응 등 협업 체계를 강화하는 데에도 중요한 역할을 하고 있으며, 향후 그룹 전체의 보안 업무 자동화와 효율성 확대를 이끄는 핵심 툴로 자리매김할 것으로 기대된다.

> AhnLab SOAR를 통해 악성 IP, Hash 등 TI 정보를 연계해 탐지 이벤트 분석을 고도화하고, 로그 첨부, IP 차단, 보고서 작성, 승인 요청과 같은 반복 작업을 자동화해 관제 대응 시간을 약 10분 단축할 수 있었다. 또한, 다양한 서비스 액션과 조건 분기 기능을 활용해 목적에 맞는 플레이북을 유연하게 설계할 수 있었던 점은 업무 최적화에 도움이 됐다. 아울러, 탐지부터 대응까지 전 과정에 대한 시각화가 가능해 보안 운영 흐름과 개선 지점을 한눈에 파악할 수 있었다.
>
> - K사 보안 운영 담당자

솔루션 도입 배경

AhnLab SOAR를 도입하기 전, K사의 보안 관제 환경은 대부분 수작업에 의존하고 있었다. 별도의 포털이나 자동화 시스템 없이, SIEM을 중심으로 이벤트를 탐지하고 관제 담당자가 직접 로그를 조회하며 분석과 후속 대응을 수행하는 방식이었다. 이런 운영 구조는 위협 이벤트 발생 시 분석부터 대응까지 많은 시간이 소요되는 것은 물론, 반복적인 단순 작업에 관제 인력이 지속적으로 투입되면서 업무 부담과 과부하로 이어지기 쉬웠다. 결과적으로 관제 품질을 유지하기 어려워지고, 대응 누락과 같은 구조적인 리스크가 발생할 가능성도 존재했다.

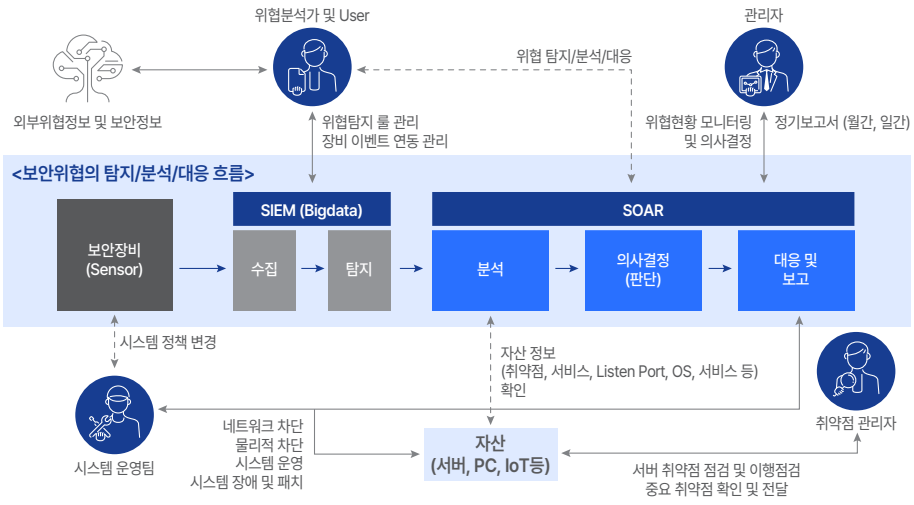
이런 한계 속에서, 관제 업무의 연속성과 효율성을 동시에 확보할 수 있는 시스템의 필요성이 커졌다. 위협 이벤트가 급증하는 상황에서 수작업 위주의 분석 방식은 대응 지연과 과도한 알림 처리 부담으로 이어졌으며, 체계적인 위협 관리와 자동화된 대응 프로세스 수립이 시급한 과제로 부상했다.

이에 따라, K사는 반복 업무를 줄이고 보안 운영의 흐름을 표준화할 수 있는 방안을 모색했으며, 그 대안으로 'AhnLab SOAR'를 채택했다.

AhnLab SOAR는 기존 관제 시스템의 제약을 보완하고, 자동화 기반의 대응 체계를 구축하는 데 핵심적인 역할을 했다. 특히 1차 분석 자동화와 번복 업무의 간소화는 관제 효율을 눈에 띄게 끌어올리는 계기가 됐으며, 실제 현장에서는 관제 담당자의 대응 시간이 단축되고 업무 집중도가 높아지는 등 뚜렷한 개선 효과가 나타났다. 이는 관제 조직이 보다 전략적인 업무에 집중할 수 있는 환경을 마련하는 데 결정적인 기반이 됐다.

운영 사례

AhnLab SOAR는 현재 K사의 다양한 보안 및 업무 시스템과 연동돼 관제 자동화 체계의 중심축을 이루고 있다. 내부 보안 관제 플랫폼인 SIEM을 비롯해 방화벽, 위협 관리 시스템(Threat Management System, TMS), UTM 등 주요 보안 장비와 연계해 악성 IP 탐지 시 자동으로 차단하고, 사내 메신저와 메일 시스템과도 연동돼 신속한 보고 및 커뮤니케이션이 가능한 형태로 구성돼 있다. 이를 통해 탐지부터 대응, 보고까지 전 과정을 유기적으로 자동화한 보안 대응 체계가 구축됐다.



[그림 1] AhnLab SOAR의 대응 프로세스

운영 사례

- 다양한 시스템과의 연동을 통한 관제 자동화 구현
- 80개 이상 플레이북 운영을 통한 위협 대응 자동화
- 선제적 인텔리전스 분석 역량 강화
- 안정적 운영 기반의 관제 효율성 향상

실제 운영 환경에서는 80개가 넘는 플레이북이 가동되고 있으며, 반복적인 이벤트 처리와 다양한 위협 시나리오에 대한 대응을 자동화하고 있다. 아직까지 랜섬웨어나 피싱과 같은 특정 위협에 의한 침해 사고는 발생하지 않았지만, SOAR를 통한 TI 정보 수집과 탐지 이벤트 연계를 통해 악성 IP, 해시 정보 등 위협 인텔리전스를 활용한 선제적 분석 고도화가 이뤄지고 있다. 그 결과, 탐지의 정확도가 향상되고, 관제 조직의 사전 대응 역량도 강화되고 있다.

AhnLab SOAR는 운영 측면에서 전반적으로 안정적인 시스템으로 평가받고 있으며, 사용자 경험 역시 만족스러웠다. 기존에는 'Jupyter' 기능을 활용해 스크립트 노드의 사전 테스트를 수행했으나, 신규 버전으로 업그레이드된 후 해당 기능이 제거된 점은 아쉬움으로 남는다. 그럼에도 불구하고 AhnLab SOAR의 강력한 자동화 기능과 유연한 연동 구조는 관제 업무에 실질적인 도움을 주고 있으며, 향후 지속적인 개선과 확장을 통해 더 높은 수준의 운영 최적화를 기대할 수 있다.

도입 효과

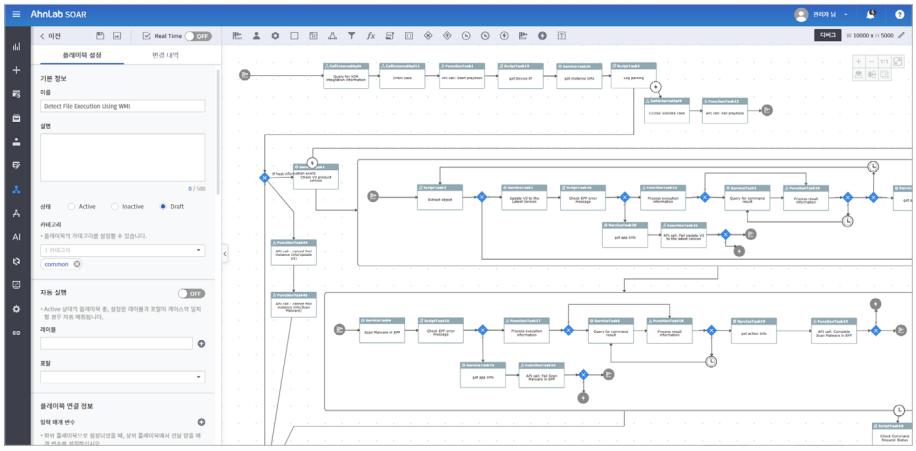
AhnLab SOAR 도입 이후 K사는 탐지부터 대응까지 이어지는 일련의 관제 프로세스를 체계적으로 고도화할 수 있었다. 이벤트 발생 시 SOAR는 자동으로 케이스 이력, 공격자 로그, 자산 정보 등 분석에 필요한 모든 정보를 출력해 관제 담당자가 이를 빠르게 분석하고 IP 차단 및 승인 요청 메시지 발송 등의 후속 조치를 효율적으로 처리할 수 있도록 했다. 그 결과, 이벤트 분석 및 대응 시간이 약 10분 정도 단축됐다.

AhnLab SOAR의 활용 범위를 점차 확대하면서 관제 업무에 큰 개선 효과를 얻을 수 있었으며, 특히 반복적이고 시간이 많이 소모되던 업무들이 자동화됨에 따라 관제팀의 업무 부담이 현저히 감소했다. 또한, 보안 사건에 대한 대응 속도와 정확도가 눈에 띄게 향상돼 더 효과적인 보안 운영이 가능해졌다.

무엇보다 가장 만족스러운 기능은 플레이북이다. 플레이북에서는 다양한 서비스 액션, 사용자 작업, 조건 분기 등을 설정할 수 있어, 보안팀은 특정 위협에 맞는 대응 로직을 유연하게 설계할 수 있었다. 더 나아가, AhnLab SOAR를 통해 계열사의 보안 담당자들에게 외부 동향을 전파하는 업무도 자동화하면서, 다양한 부서에서 SOAR 활용에 대한 만족도가 높아졌다. 일부 계열사에서는 SOAR의 활용 방안을 논의하는 등 긍정적인 반응을 보였다.

도입 효과

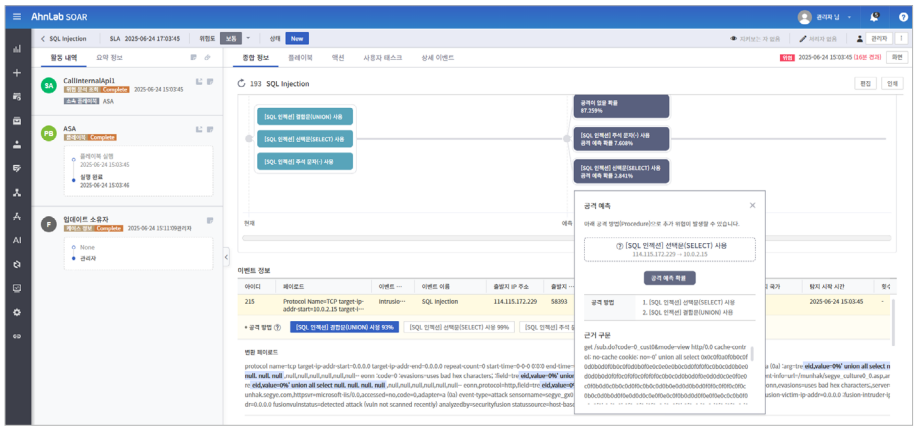
- 평균 분석/대응 시간 10분 단축
- 반복 업무 자동화로 관제 인력 업무 부담 경감
- 플레이북 기반 유연한 대응 로직 설계
- 보안 이벤트 대응의 속도 및 정확도 향상
- 계열사 간 정보 공유 자동화로 협업 강화



[그림 2] AhnLab SOAR에서 제공하는 빌트인(Built-in) 플레이북

향후 계획

K사는 인공지능(AI)/머신러닝(ML)과 SOAR를 결합해 보안 이벤트에 대한 자동 분석 프로세스를 구축하는 것을 목표로 한다. 단순 반복 업무를 줄이는 데 그치지 않고, 이벤트가 발생하면 AI/ML 기반 분석 데이터를 SOAR의 대응 로직과 연동해 관제 인력의 개입을 최소화하고 더욱 정교하고 효율적인 대응 체계를 갖추려는 것이다.



[그림 3] AI 기반 상관분석을 통한 추가 공격 선제 대응

이와 함께, AhnLab SOAR의 활용 범위는 보안 관제를 넘어 확장되고 있다. IP 차단 확대, TI 데이터 수집, 방화벽 차단 관리 시스템 연동 등 관제 업무 전반의 고도화와 더불어, 보안 외 업무의 자동화까지 실현하고자 한다. 궁극적으로는 전사적 IT 운영 전반에서 자동화 기반 효율성을 확보하는 것이 목표이다.

한편, 대시보드의 커스터마이징 기능 향상도 기대하고 있다. 현재 제공되는 위젯을 보다 유연하게 조정하거나 플레이북과 연계해 업무별 맞춤형 시각화를 구현할 수 있다면, 보안 이벤트의 흐름을 한눈에 파악하고 신속하게 조치할 수 있는 기반이 될 것으로 본다. 이런 측면에서 AhnLab SOAR는 직관적인 워크플로우와 확장성 있는 설계가 강점이며, 위협 대응뿐만 아니라 보안 업무의 자동화와 체계화를 고민하는 조직에게 유용한 솔루션이다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901