Case Study

AhnLab

대응 속도와 효율을 동시에 **자동화**로 완성한 보안 관제

업종
정보통신업

규모
대기업

도입제품
AhnLab MDS +
API 자동화

M사는 통합 보안 관제 센터를 운영하며 사이버 위협 대응, 개인정보 보호, 보안 솔루션 운영을 담당하고 있다. 특히 신·변종 악성코드 및 랜섬웨어 대응을 위해 다양한 보안 솔루션과 안랩 위협정보 신고센터를 연계한 분석·대응 체계를 운영해왔다.

그러나 고도화되는 위협과 제한된 인력 환경 속에서, 기존의 수작업 중심 분석 체계는 대응 속도와 효율성 측면에서 한계를 드러내기 시작했다.

이에 M사는 AhnLab MDS와 API 기반 자동화 체계를 도입해 분석 프로세스를 고도화했으며, 그 결과 위협 대응 속도 향상과 분석 정확성 확보, 그리고 운영 효율 극대화라는 성과를 동시에 달성했다.

위협 데이터 통합 분석으로 대응 범위 확장

M사는 안랩 위협정보 신고센터와 연계한 분석 프로세스를 운영한다. 이를 통해 기존 보안 솔루션에서 탐지되지 않는 신·변종 악성코드와 랜섬웨어 의심 파일의 정·오탐 여부를 확인함으로써 탐지 공백을 최소화하고 정밀한 분석 기반을 확보하고 있다.

이를 통해 M사는 다양한 위협 데이터를 일관된 기준으로 수집·분석할 수 있는 체계를 구축하고, 신·변종 위협까지 포괄하는 대응 기반을 마련했다.

분석 자동화로 수작업 감소 및 대응 속도 향상

기존에는 위협정보 신고센터의 분석 결과를 확인하기 위해 웹 기반 데이터 수집 방식을 활용해 정보를 자동으로 수집했다. 그러나 이 과정에서 불필요한 정보가 함께 수집되거나 추가적인 데이터 가공이 필요해 운영 효율에 한계가 있었다.

게다가 일부 샘플은 분석가가 직접 확인해야 하는 구조로 인해 반복적인 수작업이 발생하고, 대응까지의 시간이 지연되는 문제가 있었다.

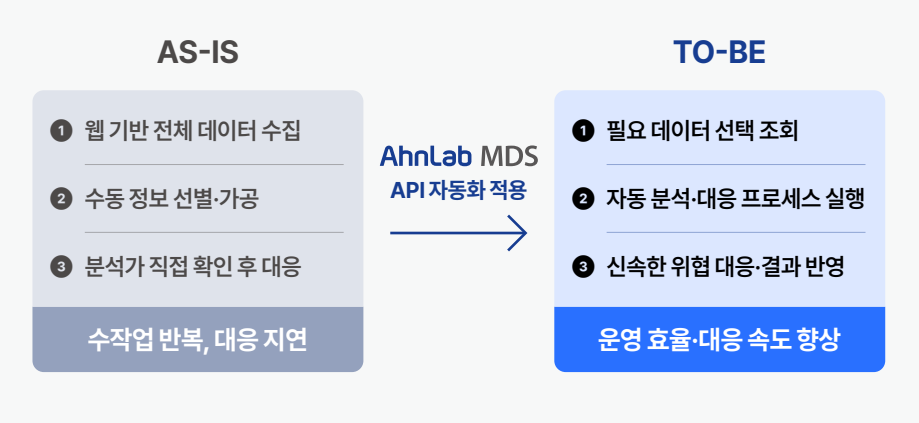
Results

위협 탐지 범위 확대·공백 감소

API 기반 자동화 체계 구축

분석 효율·대응 속도 향상

이에 M사는 AhnLab MDS와 연계된 분석 체계를 기반으로 자동화 프로세스를 단계적으로 적용함으로써, 분석부터 대응까지의 흐름을 효율적으로 개선했다.
그 결과 반복적인 확인 작업이 줄어들고, 분석 결과를 보다 신속하게 활용할 수 있는 환경이 구축되면서 전반적인 대응 속도가 향상됐다.



"API 기반 연계를 통해 분석 과정 전반에 자동화를 적용하면서 반복적인 확인 작업이 줄었고, 보안 운영 효율도 함께 개선됐습니다."
- M사 보안 운영 담당자

API 기반 자동화로 데이터 정확성과 운영 안정성 확보

기존 웹 기반 데이터 수집 방식은 웹페이지 전체 데이터를 수집한 뒤 필요한 정보를 선별해야 하는 구조로, 처리 시간이 길고 불필요한 트래픽이 발생하는 한계가 있었다. 또한, 데이터 정확성과 무결성 측면에서도 개선이 필요한 상황이었다.
이를 개선하기 위해 M사는 안랩 CSM(Customer Success Manager)과의 협업을 통해 요구사항을 구체화하고, 안랩이 제공하는 공통 API를 활용해 관제 환경에 적합한 자동화 체계를 구축했다.
특히 보안관제 시스템과 안랩 위협정보 신고센터 간 API 연계를 통해 필요한 데이터만 선택적으로 조회할 수 있도록 구성했다. 이를 통해 웹페이지 로딩 없이 서버 간 직접 통신이 가능해지면서 응답 속도와 데이터 처리 효율성이 함께 개선됐다.
그 결과 M사는 데이터 정확성과 처리 효율을 동시에 확보하고, 안정적인 자동화 기반의 보안 운영 환경을 구축했다.

"안랩 CSM과의 협업을 통해 API와 관제 시스템을 지속적으로 고도화하면서, 보다 안정적인 보안 운영 환경을 구축할 수 있었습니다."
- M사 보안 관제팀 관계자

AhnLab MDS는 네트워크, 이메일, 엔드포인트 등 여러 경로로 유입되는 위협을 통합적으로 탐지·분석하고 대응을 지원하는 샌드박스 기반 지능형 위협 대응 솔루션이다.
다양한 분석 기술을 기반으로 알려진 악성코드 외에도 신·변종 위협과 APT 공격 등 고도화된 위협까지 정밀하게 식별한다. 의심 파일은 가상 환경에서 실행해 실제 위협 여부를 검증하고, 메모리 분석 및 익스플로잇 탐지 기술을 더해 탐지 정확도를 높인다.
이와 함께 메일 위협 대응과 CDR 기반 문서 무해화 기능을 통해 피싱 메일과 문서 기반 위협까지 대응 범위를 확장하며, 기업의 업무 연속성과 보안 운영 효율을 높이는 데 기여한다.