Best Use Case

AhnLab

확장자 변경을 통한 망간 자료 반입 탐지

업종
첨단 제조업

규모
대기업

도입제품
AhnLab EDR

C사는 망간 자료 전송 시스템을 통해 실행 파일이 확장자 변경 방식으로 내부망에 우회 반입된 뒤 사용된 사례를 확인했다. AhnLab EDR은 파일 변경과 망간 자료 전송, 내부망 실행 이력을 연계 분석해 관련 사용자와 장비를 특정했으며, 분석 결과는 현장 확인과 내부 규정에 따른 후속 조치에 활용됐다.

내부망에 들어온 실행 파일, 어떻게 반입됐을까?

C사는 외부망과 내부망 사이의 자료 이동을 위해 망간 자료 전송 시스템을 운영하고 있었다. 그러나 파일의 실제 형식이나 실행 가능 여부보다 확장자를 중심으로 반입 여부를 확인하는 과정에서 실행 파일의 확장자를 변경해 첨부 제한을 우회할 가능성이 있었다.

실제로 윈도우 권한을 변경하는 실행 파일의 확장자를 .exe에서 .txt로 변경한 뒤, 망간 자료 전송 시스템을 통해 내부망으로 반입하고, 내부망에서 다시 .exe로 변경해 사용한 정황이 확인됐다.

파일 변경, 망간 자료 전송, 내부망 유입 및 실행 기록은 서로 다른 이벤트로 남기 때문에 개별 로그만으로는 전체 행위의 흐름을 파악하기 어려웠다. AhnLab EDR은 이들 기록을 시간순으로 연계 분석해 외부망에서 이루어진 확장자 변경부터 내부망 반입과 실제 사용까지 이어진 흐름을 가시화했다.

[그림 1] 파일 확장자 변경을 통한 망간 자료 우회 반입 및 AhnLab EDR 증적 확보 과정

Results

파일 유입 흐름 가시화
확장자 변경부터 내부망 실행까지 흐름 확인

조사 대상 신속 특정
사용자 · 장비 · 파일 및 발생 시점 확인

현장 대응 근거 확보
현장 확인과 후속 조치 근거 확보

사용자·장비·파일 이력 추적으로 조사 근거 확보

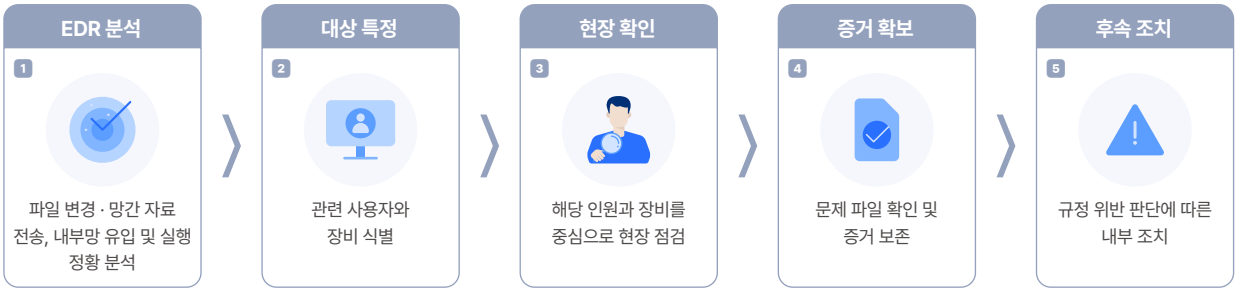
보안 운영 과정에서는 의심스러운 이벤트를 발견하는 것뿐만 아니라, 해당 행위가 누구에 의해 어떤 장비에서 발생했는지 구체적으로 확인하는 것이 중요하다. 관련 기록이 여러 시스템과 시점에 분산돼 있으면 실제 행위자를 특정하고 규정 위반 여부를 판단하기 어렵다.

AhnLab EDR은 파일 변경과 실행 기록을 사용자 및 엔드포인트 정보와 연계해 분석할 수 있도록 지원한다. C사는 이를 바탕으로 해당 파일을 변경하고 사용한 사용자와 장비, 주요 발생 시점을 구체적으로 식별했다.

이를 통해 조사 대상과 범위를 좁히고, 현장에서 우선 확인해야 할 사용자와 장비, 파일 정보를 명확히 설정할 수 있었다.

"기존에는 여러 시스템에 흩어진 기록을 수작업으로 수집하고 분석해야 해 조사에 많은 시간이 필요했습니다. AhnLab EDR을 활용하면 관련 행위 이력을 하나의 흐름으로 확인할 수 있어 초기 분석과 조사 범위 설정에 드는 시간을 줄일 수 있었습니다."

- C사 정보보안 담당자



[그림 2] AhnLab EDR 분석 기반 현장 확인 및 후속 조치 과정

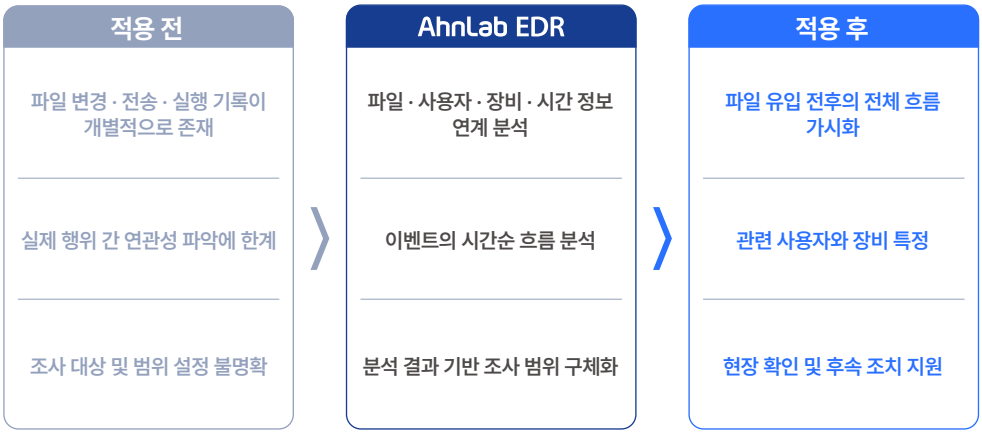
정확한 대상 식별로 현장 대응과 후속 조치 지원

AhnLab EDR 분석을 통해 조사 대상이 구체화되면서 보안 담당자는 해당 인원과 장비를 중심으로 현장 점검을 진행했다. 현장에서는 내부망으로 반입된 윈도우 권한 변경 프로그램의 존재와 사용 여부를 확인하고 관련 자료를 확보 · 보존했다.

이후 AhnLab EDR 분석 이력과 현장 자료를 종합해 내부 규정 위반 여부를 판단하고, 조직의 보안 정책에 따른 후속 조치를 진행했다.

"분석 결과와 현장 자료를 함께 대조할 수 있어 정황에 의존하지 않고 사실관계를 판단할 수 있었습니다. 확인해야 할 대상과 항목이 명확해지면서 현장 점검과 후속 조치도 보다 체계적으로 진행할 수 있었습니다."

- C사 보안 운영 담당자



[그림 3] AhnLab EDR 적용에 따른 현장 대응 지원 효과

보이지 않던 우회 반입 경로 추적 및 현장 대응 근거 확보

AhnLab EDR은 분산돼 있던 파일 변경·전송·실행 기록을 하나의 흐름으로 연결해 우회 반입 경로를 가시화했다. 이를 통해 C사는 관련 사용자와 장비, 파일 및 발생 시점을 신속하게 특정하고, 현장 확인과 후속 조치에 필요한 객관적인 근거를 확보할 수 있었다.