AhnLab

Case Study

조선 해양 업계를 위한 EDR 설계 및 구축 방안

국내 조선 해양 업체 A사는 업무망과 인터넷망에 개별적으로 AhnLab EDR을 구축해 안정적인 엔드포인트 위협 탐지 및 대응 체계를 마련했다.

개요

조선 해양 산업군도 정보통신(ICT) 기술 발전에 따른 해킹, 랜섬웨어와 같은 사이버 위협으로부터 자유롭지 못하다. 신・변종 악성코드가 대거 유입되고, 위협이 갈수록 고도화되고 있어 해당 업계의 특수한 작업 환경에 최적화된 선진 침해 사고 대응 시스템이 필요하다. 안랩의 엔드포인트 위협 탐지 및 대응 솔루션 AhnLab EDR은 복잡한 네트워크 및 운영 환경에서 뛰어난 위협 탐지와 대응 역량을 제공함으로써 안전한 비즈니스를 조성하는 데 기여한다. AhnLab EDR을 안티멀웨어 솔루션 AhnLab V3, 샌드박스 기반 지능형 위협 대응 솔루션 AhnLab MDS와 연계해 구축하면 알려진 위협뿐만 아니라 알려지지 않은 위협 및 이상 행위 실시간 탐지, 모니터링, 분석, 대응 등 전방위적인 보안 공조 체계를 구성할 수 있다.

도전과제

(1) 실효적인 엔드포인트 침해 사고 관리 체계 부족

개별 솔루션 중심의 대응으로 인해 발생하는 비효율성을 개선하고, 점차 증가하는 고도화된 침해 위협에 대한 사전 탐지 및 대응의 어려움을 해소한다.

(2) 내·외부 APT 위협 인텔리전스 연계 대응 필요성 대두

악성코드 자체 보호 기술의 발전과 전자 서명을 도용한 악성코드 등 다양한 위협이 지속적으로 확산되고 있어, 복합적인 대응 체계가 필요하다.

(3) 서비스 환경에 최적화된 운영체계의 부재

많은 보안 담당자가 침해사고 발생 시 사전 조사, 분석 관리, 모니터링에 어려움을 겪고 있다. 따라서 침해사고 예방부터 탐지, 분석, 대응, 고급 분석에 이르기까지 체계적인 운영 프로세스가 필요하다.

도전 과제

- 통합 에이전트 기반 알려진 및 알려지지 않은 위협에 대한 가시성 확보
- 성공적인 침해사고 대응을 위한 통합 위협 탐지 및 대응 프로세스 필요
- 사전 방어 체계 구축을 통한 능동적 대응 및 업무 연속성 향상

EDR 구축 방식

A사는 업무망과 인터넷망에 개별적으로 EDR 시스템을 설치했다. 1) 엔드포인트 내 이상 행위 탐지 및 대응을 통한 침해 위협 탐지와 대응 2) 침해사고 사전 탐지 및 대응 3) 침해 위협 발생 시 내부 확산 방지를 위한 통제 체계뿐만 아니라 엔드포인트 이상 행위와 위협 원인, 침투 경로 분석을 위해 로그 중앙 저장 및 분석 서버를 함께 구축했다. 또한, 알려지지 않은 위협 탐지 및 대응을 위해 AhnLab MDS를 연계했다.

A사에 본격적으로 EDR을 구축하기 전, 인터넷망에는 기존 EMS(Enterprise Management System)를 EPP로 마이그레이션하고, EPP Agent 패치를 진행했다. 그리고 업무망과 인터넷망 각각에 EPP 서버를 통해 MDS Agent를 자동으로 배포하고, PC 클린징을 수행했다. PC 클린징의 목적은 은닉된 보안 위협을 사전에 제거하기 위함으로, 다음과 같이 3단계로 진행됐다.

첫 번째, 알려진 또는 알려지지 않은 악성코드에 대한 수집 및 탐지, 분석을 통해 의심스러운 PC와 서버를 선정했다. MDS Agent를 통해 PC 및 서버 내 의심 파일을 추출하고, 알려지지 않은 실행 파일은 위험도를 'High', 'Medium'으로 분류했다. MDS Agent는 의심 파일 추출 시 머신러닝(ML)을 기반으로 하며, 전체 또는 일부 시스템을 대상으로 의심 파일을 자동 및 수동 수집한다. 또한, C&C 및 악성 사이트 접속 행위를 검출하고, 수상한 파일은 삭제하거나 격리 조치했다. EPP 서버는 알려진 악성코드 진단 로그를 분석한다.

두 번째, 안랩의 악성코드 전문가가 악성 행위 및 파일이 탐지된 PC를 대상으로 1단계에서 검출된 의심 파일을 대상으로 상세 분석, 안리포트(AhnReport) 로그 추출, 시스템 분석을 수행했다. 더 나아가, AhnLab V3 패턴 업데이트를 제공하거나 필요 시 전용 백신을 제작해 적용하는 등 신・변종 위협에 대한 대응을 지원하며, 침해사고가 의심되는 단말을 선정했다.

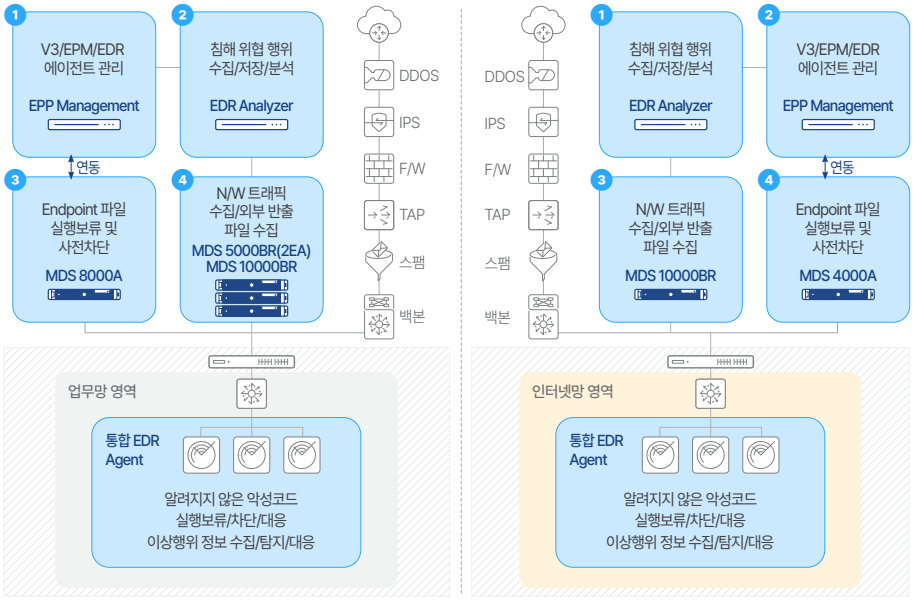
세 번째, 2단계에서 침해사고 흔적이 탐지된 PC가 있는 경우 안랩 TI(Threat Intelligence), 디지털 포렌식 툴 등을 이용해 침해사고 의심 단말 및 연관 시스템에 대한 상세한 포렌식 분석 조치를 시행했다. 분석 결과에 대한 요약 및 조치 방안 가이드를 포함한 상세 보고서를 제공했으며, 추가 확인된 신・변종 위협에 대응했다.

PC 클린징까지 완료한 후에는 EDR Analyzer 서버를 설치하고, 이를 EPP 서버와 연동했다. 그런 다음, EDR 운영 정책, V3 연동 정책을 설정한 후 EDR Agent를 설치해 EDR 배포 정책을 활성화했다.

EDR 기능 테스트 및 호환성 점검을 마친 후 모니터링을 통해 영향도를 검사하고 버그를 수정했다. 이 단계까지 특이사항이 없으면 EDR Agent를 그룹별로 전사에 확대 배포했다.

EDR 구축 핵심 포인트 1.
PC 클린징을 통한 위협 요소 사전 제거 및 시스템 하드닝 후, EDR Analyzer 설치

EDR 구축 핵심 포인트 2.
V3, MDS, PMS, MDR 등 다른 보안 솔루션과의 연계/연동으로 최적의 침해 위협 탐지 및 대응 프로세스 구현



[그림 1] 솔루션 구성도

솔루션 구축 현황과 역할

A사에 구축된 솔루션은 AhnLab EPP Management와 AhnLab EDR Analyzer, AhnLab MDS 분석 및 통합 관리 서버, 통합 EDR Agent로 구성됐다. 제품별 역할은 다음과 같다.

AhnLab EPP Management 서버

EDR과 운용 중인 V3, 패치 관리(Patch Management Sysrem, PMS) 솔루션을 통합 관리하며, MDS와 연동된다. 주로 EDR 정책 관리, 대시보드 및 보고서 제공 등의 역할을 한다.

AhnLab EDR Analyzer 서버

EDR을 통해 수집되는 침해 위협 행위 정보를 저장한다. 침해 정보 조사를 위해 검색을 수행하고 침해 위협 행위를 분석하며, 안리포트 및 아티팩트(Artifact) 수집도 진행한다.

AhnLab MDS 분석 서버(MDS 4000A)

엔드포인트 구간을 통해 유입되는 알려지지 않은 악성코드의 실행을 보류하거나 사전 차단한다. 주로 APT 공격, 사이버 킬 체인(Cyber Kill Chain) 대응을 담당한다.

AhnLab MDS 분석 및 통합 관리 서버(MDS 10000BR)

MDS 제품군을 통합 관리하고 모니터링한다. 또한, 외부로 전송된 파일을 식별하며, 해당 파일의 원본을 저장한다.

통합 에이전트

V3와 MDS, EDR Agent를 모두 포함하며, 탐지된 알려지지 않은 악성코드에 대해 자동 및 수동 삭제, 네트워크 격리 등 사전 대응하고, 실행을 보류한다. 그리고 EDR을 통해 이상 행위 정보를 수집하고, 대응 명령을 수행한다.

도입 효과

(1) 알려지지 않은 위협 탐지 및 자동 대응

AhnLab EDR은 V3와 MDS가 탐지하지 못한 악성 파일 탐지와 분석, 전체 행위 로그 수집을 통한 가시성 확보 및 분석을 수행한다. 또한, 수집된 로그를 기반으로 의심 행위를 분석하고 모니터링함으로써 알려지지 않은 위협에 대해서도 효과적으로 대응할 수 있다. V3와 연동 시 APT 위협에 대한 가시성 확보도 가능하다.

(2) 침해 사고 증적 수집 및 대응

AhnLab EDR은 악성 의심 파일에 대한 전수 검사를 실시할 수 있다. 악성코드 감염이 의심되는 PC 또는 침해사고 상세 분석이 필요한 단말들을 대상으로 아티팩트 수집 명령을 실행하고, 수집된 상세 정보들은 EPP 웹 콘솔 전용 뷰어에서 침해 사고를 상세히 분석하고 검색한다.

(3) 악성코드 사전 대응 및 사후분석 역량 향상

V3+MDS+EDR 위협 대응 아키텍처를 통해 침해 사고 공격 대응 체계를 완성하고, 통합 모니터링 및 관제 대응 체계를 마련할 수 있다. EDR 설치 전 PC 클린징을 통해 위협 요소를 1차적으로 제거하고, 엔드포인트 무결성을 확보함으로써 보안 위협 사전 탐지와 대응이 용이하다.

(4) MDR 연동을 통한 위협 탐지 로그 자동 분석

안랩 악성코드 전문가 분석 서비스인 MDR 서비스 연동을 통해 위협 여부 분석, 위험도 측정이 가능하며, 위험도 분석 보고서를 통해 대응 정책을 설정할 수 있다. 이를 통해 엔드포인트 환경에서 발생하는 보안 위협에 대한 단순 모니터링 및 알림을 넘어, 위협 차단과 억제도 수행한다.

맺음말

조선 해양 업계도 이제 진화하는 사이버 보안 위협으로부터 조직을 안전하게 보호하기 위해 강력한 보안 시스템 도입을 고려해야 할 때다. AhnLab EDR은 복잡한 네트워크와 운영 환경에서도 뛰어난 위협 탐지와 대응을 구현한다. AhnLab EDR은 V3, MDS와 연계해 알려진 위협 뿐만 아니라 새로운 위협과 이상 행위까지 실시간으로 탐지하고 분석한다.

AhnLab EDR을 도입하면 알려지지 않은 위협에 효과적으로 대응하고 악성 의심 파일 전수 검사를 통해 침해 사고를 상세하게 분석할 수 있으며, 통합 에이전트(V3/MDS/EDR) 기반 위협 대응 아키텍처를 통해 보다 안정적이고 견고한 침해 사고 대응 체계를 마련할 수 있다. 그리고, MDR 서비스를 연동함으로써 전문가 중심의 위협 분석 및 차단, 모니터링을 통해 종합적이고 효과적인 보안을 구현할 수 있다. AhnLab EDR은 조선 해양 업계의 사이버 보안 체계를 강화하고, 비즈니스의 안전성을 높이는 데 크게 기여할 것이다.

AhnLab

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