AhnLab

White Paper

"탐지 그 이상의 대응" EDR을 활용한 보안 전략

Contents

- EDR의 이해 1
- EDR 도입의 필요성 2
- AhnLab EDR의 공격 대응 방법 3
- AhnLab EDR 실전 활용 방안 7
- 맺음말 12

EDR의 이해

엔드포인트는 사이버 공격자의 최종 목표다. 엔드포인트의 취약점은 연간 수만 건에 달하며, 하루에 발견되는 신종 악성코드는 수십 만 개나 된다. 게다가 최근에는 기존 보안 솔루션 탐지 우회, 내부 이동을 통한 서버 탈취, 침입 흔적 삭제 등의 고도화된 공격 유형도 등장하고 있다. 이를 해결하기 위해 상시 감시 및 사후 조사 체계를 수립하는 방향으로 보안 패러다임이 변화했으며, 그렇게 등장한 것이 바로 'EDR(Endpoint Detection and Response)'이다.

2013년 가트너(Gartner)에 의해 처음 소개된 EDR은 엔드포인트에서 지속적인 모니터링과 위협 정보 수집 및 분석을 통해 위협에 대한 적절한 가시성을 확보하고, 대응력을 강화하는 보안 솔루션이다. 이를 통해, 위협의 잠복 기간(Dwell Time)을 최소화하고, 잠재적 피해를 방지하는 것이 목적이다. 또한, 가트너에 따르면, EDR이 ▲보안 침해 탐지(Detect security incident) ▲보안 침해 조사(Investigate Security incident), ▲엔드포인트 영역에서의 침해 억제(Contain the incident at the endpoint) ▲감염 전 상태로의 치료/회복(Provide remediation guidance) 등 4가지 기능을 모두 제공해야 한다.

더 쉽게 설명하면, EDR은 CCTV와 역할이 유사하다. 엔드포인트에서 발생하는 모든 행위를 탐지해 엔드포인트 로깅을 강화하고, 침해사고 조사에 필요한 정보를 상시적으로 수집한다. 수집한 행위 정보를 바탕으로 위협을 능동적으로 추적·분석하며, 장기적인 위협 대응 체계를 수립하는 데 기여한다.

참고로, EDR은 엔드포인트 보안을 보완하기 위한 툴로, 보안 환경을 완벽하게 만드는 만능 솔루션은 아니다. 이 점을 이해하고, 안티바이러스(Anti-Virus, AV) 등 기존 보안 제품과 연계해 사용하는 것이 바람직하다.

EDR 도입의 필요성

EDR은 '수집할 수 없는 대상은 분석할 수 없고, 분석하지 못하면 악성 여부를 판별할 수 없으며, 악성코드를 확인하지 못했다면 대응도 할 수 없다'를 기본 전제로 한다.

이 전제를 충족하기 위해, EDR은 단말에서 발생한 모든 행위를 지속적으로 모니터링하고 가시화하며, 기존 솔루션과의 연계를 통해 위협 잠복 기간을 최소화하는 것을 목표로 작동한다. 위협 잠복 기간이란 외부로부터 유입된 위협 확인부터 샘플링 및 분석, 엔진 등록 및 업데이트까지 소요되는 시간을 말한다. 이 기간 동안 발생할 수 있는 보안 취약점을 EDR을 활용해 대응할 수 있다.

공격자가 악성코드를 전달하는 대표적인 경로는 이메일 또는 웹이다. 공격자는 취약점이 있는 특정 PC를 확보해 공격을 수행한 다음, 백도어를 설치하고 외부에 있는 C&C 서버를 통해 추가 악성파일을 다운로드한다. 또한, 내부에 접근 가능한 서버를 찾아 해당 서버에 연결 가능한 PC에 대해 측면 이동(Lateral Movement)을 수행한다. 이를 통해, 서버의 데이터를 유출한 후, 그 흔적을 모두 없앤다.

이런 유형의 공격은 기존 보안 솔루션으로 추적이 불가능하다. 이를 보완하기 위해서는 EDR 도입이 필요하다. EDR은 타임라인을 기반으로 엔드포인트에서 발생하는 파일이나 프로세스 등의 행위 이력을 로깅해 필요 시 능동적으로 위협을 추적하는 위협 헌팅(Threat Hunting)을 수행할 수 있다.

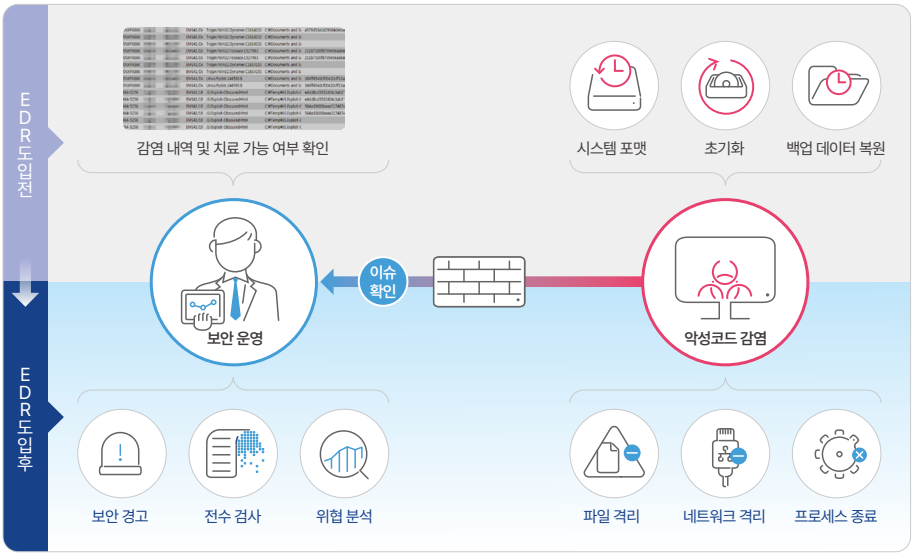
이 밖에, 위협 확산을 방지하기 위한 네트워크 격리, 프로세스 실행 차단, 파일 수집 및 복원 등 다양한 대응 방안을 제공해 기업의 사전 예방 및 재발 방지 체계 구축에 도움을 준다.

EDR이 필요한 이유:

·알려지지 않은 위협 대응의 한계
·높은 수준의 포렌식 분석 기술 필요
·침해 원인 분석을 통한 재발 방지 전략 도출

더 나아가, EDR에 마이터어택(MITRE ATT&CK) 프레임워크를 적용하면 다양한 공격 기법을 더 효과적으로 탐지하고 식별하는 데 도움이 된다. 공격의 특정 단계와 사용된 기술을 참고해 위협이 어디에서 시작됐고, 어떻게 진행됐는지 확인할 수 있으며, 향후 발생할 수 있는 공격 방식도 예측할 수 있다. 따라서 보안 담당자는 위협을 더 잘 이해하고 신속하게 대응하는 등 조직의 전반적인 보안 태세를 강화할 수 있다.

기존에는 위협 대응이 일회성에 그치고, 위협 고도화에 따른 분석 및 대응 한계가 있었다면, 이제는 EDR을 활용해 알려지지 않은 위협도 전방위적으로 관리·대응하고, 종합적인 분석을 통해 원인을 파악함으로써 재발 방지 전략까지 도출할 수 있다.



[그림 1] EDR 도입 전과 후 비교

이에, 안랩은 'AhnLab EDR'을 2018년에 처음 출시했다. 2022년에는 사용성과 위협 가시성을 한층 더 강화한 업그레이드 버전인 'AhnLab EDR 2.0'을 발표하기도 했다.

AhnLab EDR의 공격 대응 방법

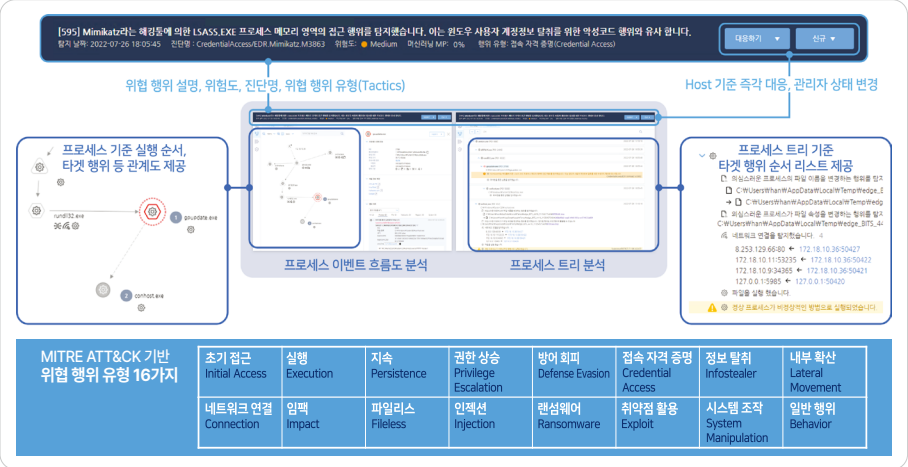
AhnLab EDR은 다음 7가지 핵심 기능을 바탕으로 엔드포인트 위협에 대응한다.

(1) 다이어그램 및 타임라인 분석

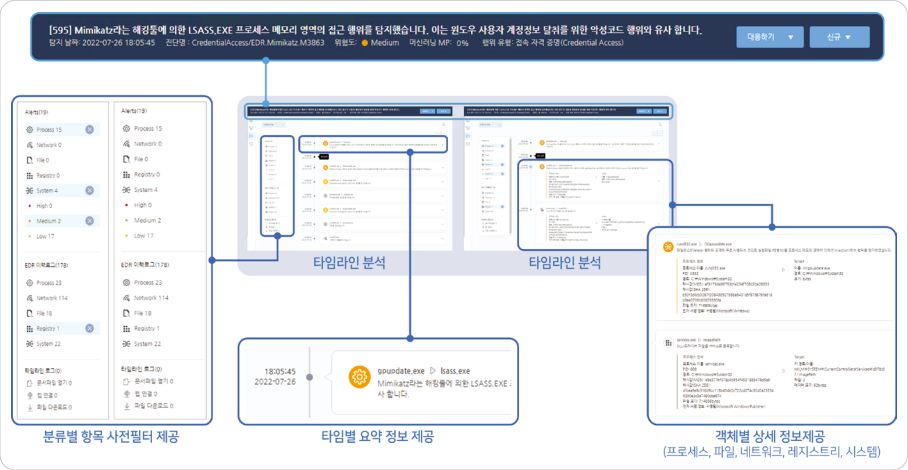
마이터어택(MITRE ATT&CK) 기반 위협 유형 16종과 위협 유입 경로, 주요 행위, 연관관계, 위험도, 위협 정보 링크 등에 대한 분석 내용과 프로세스, 파일, 시스템, 레지스트리, 네트워크 타겟별 행위 및 상세 정보를 제공하고, 실시간으로 대응한다. 또한, 탐지된 위협 분석 정보를 주요 행위별(객체 종류/위험도), 일반 행위별(객체 종류), 아티팩트(Artifacts) 정보를 기준으로 사전 분류할 수 있는 필터와 이들의 필요조건들을 조합해 타임라인별로 정보를 제공한다.

AhnLab EDR 주요 기능 (1):
다이어그램 및 타임라인 분석을 통한 위협 정보 제공

AhnLab EDR 주요 기능 (2):
위협 인텔리전스 플랫폼과 연동한 전용 콘솔 지원



[그림 2] 다이어그램 분석



[그림 3] 타임라인 분석

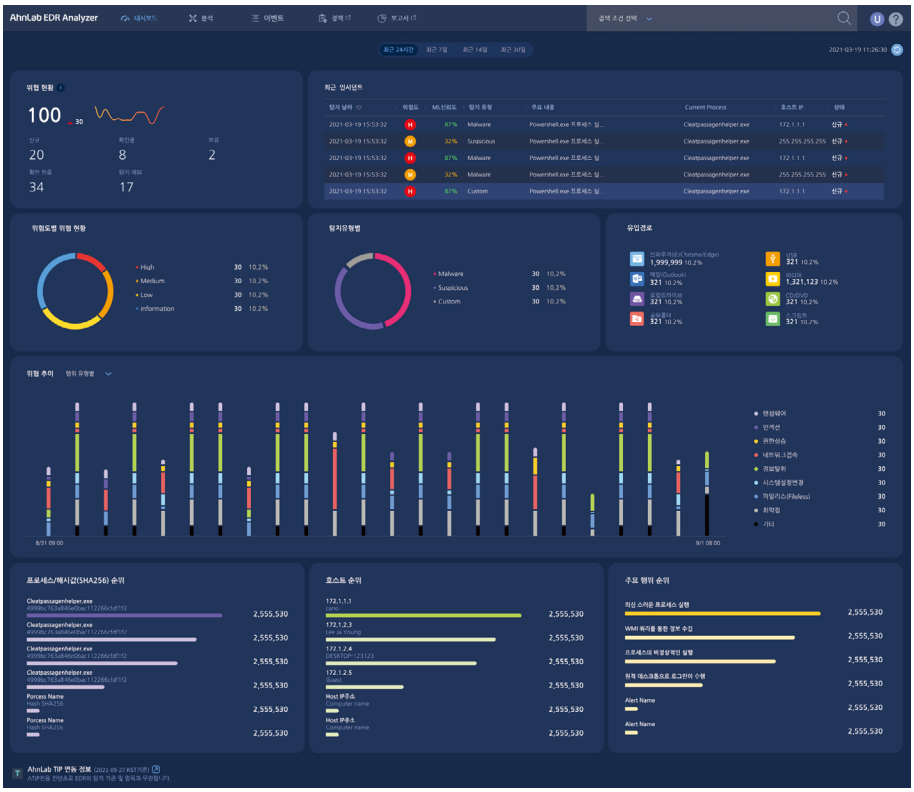
(2) 전용 콘솔 기반 위협 정보 및 통계 제공

AhnLab EDR은 운영 편의성과 안랩의 전문 기술력을 탑재한 전용 콘솔 'EDR Analyzer'를 제공한다. EDR Analyzer는 탐지 및 분석, 대응 관점에서 사용자가 위협을 정확히 인식하고 조건을 설정하도록 구성됐다. AhnLab EDR은 의심스러운 행위 관련 유형별 정보를 상시로 수집해 EDR Analyzer 중앙 서버에 저장하며, 고객사 환경 및 모니터링 그룹의 중요도에 따라 행위 수집 레벨을 다르게 조정함으로써 관리를 최적화하고 용량 부담을 줄인다.

또한, EDR Analyzer를 안랩 위협 인텔리전스 플랫폼 AhnLab TIP와 연동해 최신 IoC(파일, IP, URL) 현황 정보와 최신 보안 권고문을 제공하고, 고객의 EDR에서 탐지된 이벤트에 대한 평판도 조회할 수 있다.

AhnLab EDR 주요 기능 (3):
머신러닝 기반 고도화된 탐지 및 분석

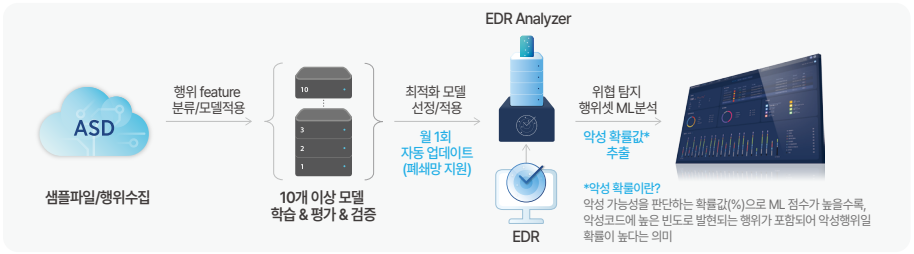
AhnLab EDR 주요 기능 (4):
사용자 정의 규칙 및 자동 대응 설정



[그림 4] EDR Analyzer 대시보드

(3) 머신러닝(ML) 기반 위험도 분석

AhnLab EDR에는 '지도학습 ML'이 적용돼 있어 안랩 클라우드 서버 ASD(AhnLab Smart Defense)에 수집된 수백억 개 대용량 데이터를 기반으로 학습을 진행한다. 학습 시 10개 이상의 모델을 사용하며, 이 중 최적화 모델을 선정해 제품에 반영한다. EDR에 적용된 ML은 EDR이 탐지한 의심 및 위협 행위에 대한 악성 확률을 제공해 보안 담당자가 EDR 분석 결과에 대한 우선순위 및 중요도를 파악하는 데 도움이 된다.



[그림 5] ML 적용 프로세스

(4) 사용자 정의 규칙 설정을 통한 자동 대응

AhnLab EDR은 다양한 종류의 사용자 정의 규칙(IoC/Yara/행위 기반 규칙)과 네트워크 및 파일 격리, 프로세스 차단 등의 자동 대응 설정 기능을 제공한다. 특히, 행위 기반의 사용자 정의 규칙은 조직 환경에 맞게 중점적으로 모니터링해야 하는 의심 행위를 정의할 수 있어, 조직 환경에 특화된 위협 관리를 지원한다.

AhnLab EDR 주요 기능 (5):
랜섬웨어에 감염된 PC의 중요 데이터 복구

AhnLab EDR 주요 기능 (6):
침해사고 상세 분석 및 추가 증적 수집

[그림 6] 사용자 정의 규칙 설정 방법

(5) 롤백(Roll back) 기능

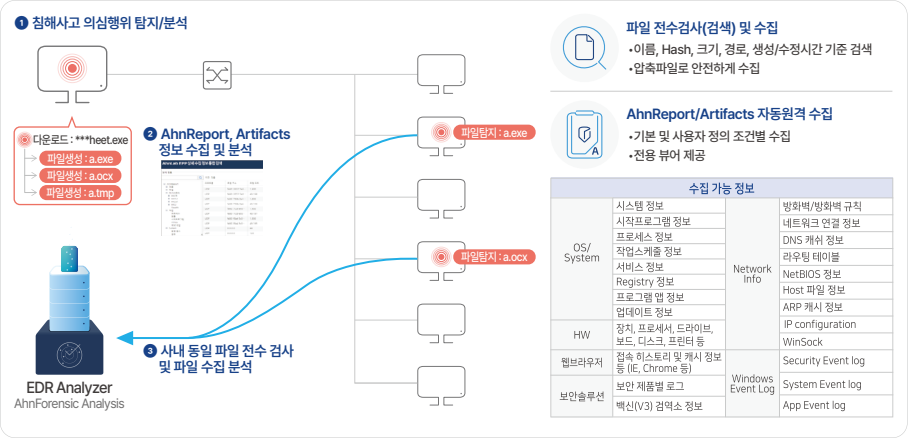
롤백 기능도 AhnLab EDR의 중요한 기능 중 하나다. AhnLab EDR은 윈도우의 VSS 기술을 활용해 랜섬웨어로 암호화된 파일을 이전 상태로 복원한다. 또한, 악성 행위와 VSS 기능 무력화, 스냅샷 삭제 행위를 원천 차단한다. 이를 통해, 사용자는 PC 데이터를 피해 이전의 상태로 안전하게 복원할 수 있다.

[그림 7] 롤백 기능 적용 프로세스

(6) 침해사고 증적 수집 및 대응

AhnLab EDR은 상세 분석이 필요한 단말들을 대상으로 추가 증적 정보를 수집해 대응한다. 기본 및 사용자 정의 조건별로 아티팩트 정보를 수집해 분석하고, 파일 전수 검사를 실시한다. 그런 다음, 다수 단말에서 수집된 상세 정보들을 바탕으로 통합 검색 시스템을 통해 침해사고 상세 분석 및 검색을 수행한다.

AhnLab EDR 주요 기능 (7):
EDR 운영과 활용을 돕는 MDR 서비스 기본 제공

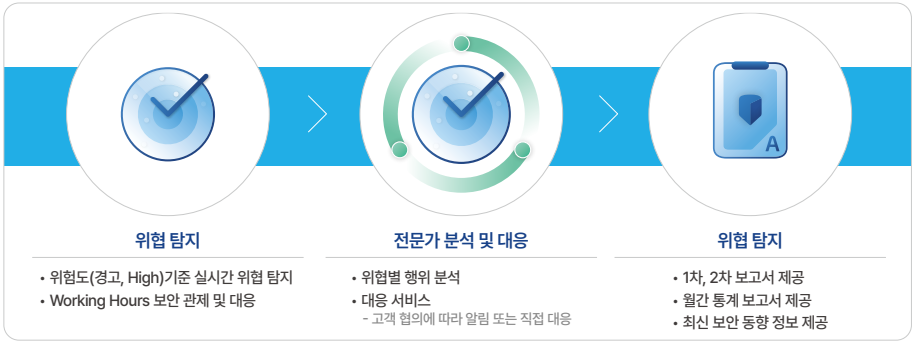


[그림 8] 침해사고 증적 수집 및 대응 프로세스

(7) EDR 운영과 활용을 돕는 MDR 서비스 제공

AhnLab EDR은 안랩의 보안 전문가가 EDR의 운영과 활용을 지원하는 'MDR 서비스'를 기본으로 제공한다. 기업에 설치돼 운영되는 EDR을 활용해, 위협에 대한 티켓(Ticket)을 발생시켜 평판 정보, 악성코드 행위 분석 등 안랩의 위협 대응 프로세스에 맞게 체계적으로 처리하며, 위협 분석 보고서, 월간 통계 보고서뿐만 아니라 위협 완화 및 복구를 위한 조치 가이드도 함께 제공한다.

보다 더 전문적인 맞춤형 MDR 서비스를 원하는 기업은 추가 비용을 지불해 위협 전체에 대한 모니터링 및 분석, 대응 서비스를 제공하고, 분기별로 전문가의 의견이 담긴 리뷰 보고서를 발행하는 'EDR Premium'을 이용할 수 있다.



[그림 9] MDR 서비스 개요

AhnLab EDR 실전 활용 방안

AhnLab EDR은 독자적으로 구축하면 그 진가를 제대로 발휘할 수 없다. 다른 보안 제품과 연계해 통합 보안을 실현해야 더 강력한 보안 체계를 마련할 수 있다.

AhnLab EDR 실전 활용 방안 (1) : EP(V3/MDS/EPP) 솔루션 연동을 통한 엔드포인트 통합 보안 실현

AhnLab EDR은 안랩의 AV 솔루션인 V3 제품군과 샌드박스 솔루션 MDS, 엔드포인트 통합 보안 플랫폼 EPP(Endpoint Protection Platform)과 같은 EP 전용 솔루션뿐만 아니라 SIEM(Security Information and Event Management), SOAR(Security Orchestration, Automation, and Response) 등의 원격 관제 시스템, 그리고 다양한 연계 시스템과 함께 사용하면 보안 강화의 시너지 효과를 발휘할 수 있다.

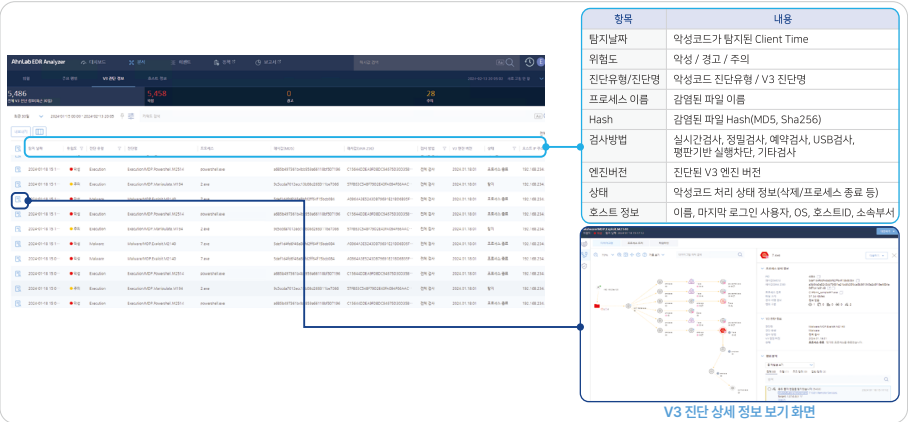
(1) EP 솔루션 연계 – 엔드포인트 통합 보안 실현

먼저, AhnLab EDR은 AhnLab V3, AhnLab MDS와 유기적으로 연동돼 엔드포인트 영역에 대한 통합 보안을 실현할 수 있다. V3와 연계하면 이미 발생한 위협과 의심스러운 위협을 악성/경고/주의 3단계로 분류해 분석 정보를 제공한다. MDS와 연동할 경우, 의심스러운 파일에 대해 추가 동적 및 정적 분석을 수행한다.

더 구체적으로 설명하면, AhnLab V3를 설치한 서버에 AhnLab MDS와 AhnLab EDR을 추가하면, 에이전트에 악성 파일 삭제, PC 격리, 공지사항 전달 등의 대응 명령을 내리고, ML 및 빅데이터 기반 위협 탐지 기능을 통해 APT 공격 등 알려지지 않은 위협을 효과적으로 탐지하고 대응할 수 있다. 또한, 파일 실행부터 종료까지의 행위를 상세 분석한 결과 보고서를 제공하며, 바이러스토탈(VirusTotal)과의 연동을 통해 사용자가 악성 판단 여부를 판단할 수 있도록 지원한다.

AhnLab EDR은 알려지지 않은 위협과 더불어, AhnLab V3와 AhnLab MDS를 우회하는 공격도 차단한다. 엔드포인트에서 발생하는 모든 프로세스 및 파일, 네트워크, 레지스트리, 시스템 행위를 수집하고, 안랩의 노하우와 마이터 어택(MITRE ATT&CK) 프레임워크를 이용한 탐지 패턴 및 규칙(Rule)으로 위협을 모니터링하고 탐지한다. 여기에 더해, 고객사 환경에 맞는 IoC, YARA, 행위 규칙 생성을 통한 위협 탐지 및 대응도 가능하다.

또한, V3가 진단한 악성코드의 유입 경로, 주요 행위 마이터 어택 정보, 프로세스 이벤트 흐름도, 프로세스 트리, 타임라인 정보 등 향후 발생할 수 있는 동일한 위협을 선제적으로 방어할 수 있는 다양한 분석 정보를 제공한다. EDR에서 수집된 의심스러운 프로세스 또는 파일은 MDS를 통해 샌드박스 분석이 가능하며, 분석 결과 및 추가 증적도 확인할 수 있다.

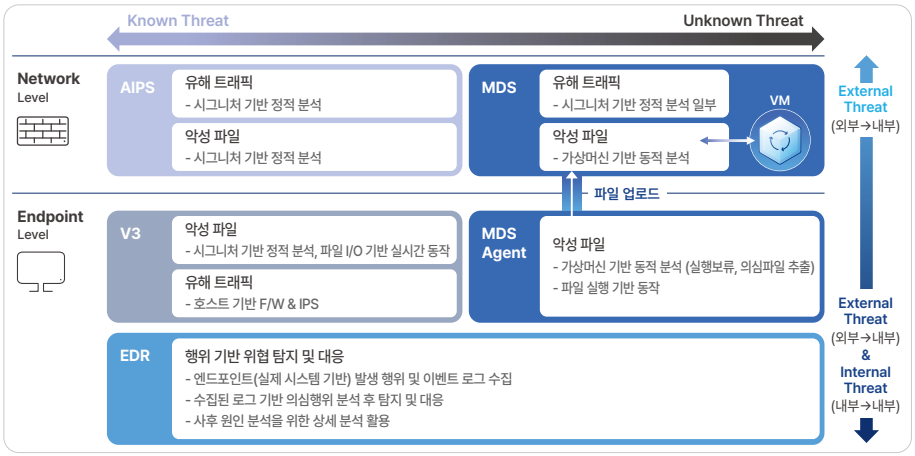


[그림 10] V3 진단 정보 제공

AhnLab EDR과 V3, MDS 간 연동 효과 : 알려진/알려지지 않은 악성코드 탐지와 샌드박스 기반 동적 분석, 행위 정보 수집 및 모니터링을 통한 전방위적 보안 역량 확보

[그림 11] AhnLab EDR과 AhnLab MDS 간 연동

정리하면, AhnLab V3가 시그니처 및 패턴 기반 악성코드 탐지와 악성 파일 또는 URL 차단·삭제·치료 등의 사전 대응을 수행하고, AhnLab MDS가 샌드박스 기술을 기반으로 알려지지 않은 위협을 정확히 탐지한다면, AhnLab EDR은 최종적으로 엔드포인트에서 위협 가능성이 있는 모든 행위를 모니터링 및 탐지하고, 위협을 추적해 분석한다는 점에서 더 고차원적인 기능을 담당한다. 이들 3가지 솔루션을 연계해 구축하면 복잡다단한 엔드포인트 시스템 환경을 안전하게 보호할 수 있다.



[그림 12] 엔드포인트 통합 에이전트 기반 위협 대응 아키텍처

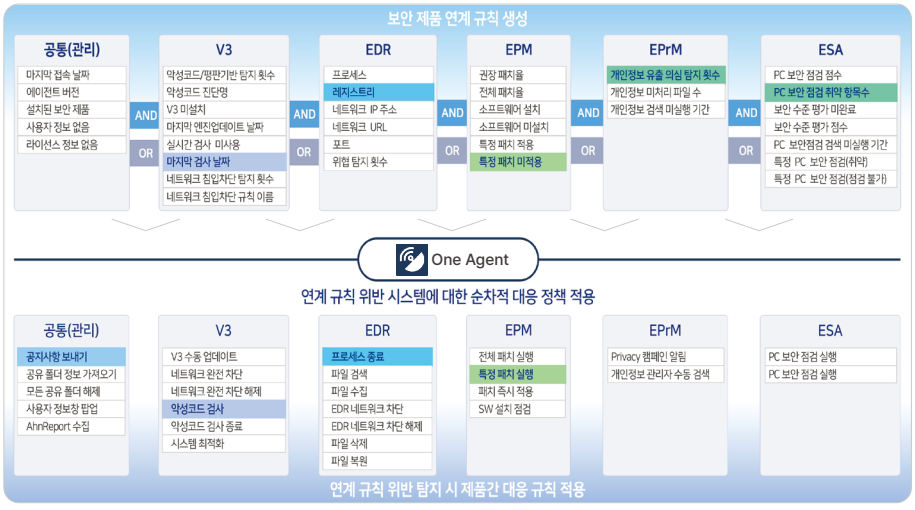
AhnLab EDR과 EPP의 통합:
기존 엔드포인트 제품 대비 신속한 위협 탐지 및 자동 대응 가능

이 외에도, AhnLab EDR은 AhnLab EPP와 통합돼 위협을 더 빠르게 탐지하고 대응한다. EPP에 포함된 솔루션들이 엔드포인트 하드닝(Endpoint Hardening)을 위한 보안 기능을 제공하고, 위협을 직접 탐지·대응한다면, EDR은 EPP가 탐지·대응한 결과를 분석해 보안 담당자에게 알려주고, 침해사고 발생 및 진행 여부, 대응 필요성에 대한 인사이트를 제공한다.

엔드포인트 하드닝: 다양한 보호 조치를 통해 엔드포인트 영역의 공격 표면을 최소화하는 것

또한, EPP와 연계한 AhnLab EDR은 엔드포인트 취약 상태 여부, 의심 행위 등에 대한 개별 및 연계 정책 설정을 제공하며, 보안 관리자가 보안 정책을 위반한 시스템에 대해 알람, 네트워크 격리, 악성코드 치료, 패치 적용 등을 주도적·능동적으로 조치할 수 있도록 지원한다.

[그림 13] AhnLab EPP 제품군과의 상호 보완적 운용



[그림 14] EPP 솔루션 연계 규칙 설정

AhnLab EDR 실전 활용 방안 (2): SIEM 및 SOAR와의 연동으로 보안 위협 대응 자동화

(2) SIEM & SOAR 연계 – 보안관제(SOC) 운영 효과 극대화

AhnLab EDR은 SIEM, SOAR와 Syslog, API 연동 기능을 제공한다. 따라서 보안 관리자는 위협 탐지 유형, 위험도, 행위 유형 등 연동 정보를 선택적으로 지정해 위협을 확인할 수 있으며, 네트워크 격리 또는 해제, 파일 격리 및 복원, 공지사항 보내기, 프로세스 종료, 아티팩트 수집, 안리포트 수집 등의 API를 연동해 자동 대응이 가능하다. 또한, 호스트 정보 및 데이터베이스(DB) 정보 쿼리(Query)를 제공받을 수 있다.

[그림 15] AhnLab EDR과 SIEM & SOAR 연동

또한, SIEM은 네트워크 정보 또는 단순 AV 진단 정보 만으로 경보 조건을 설정해 엔드포인트의 다양한 정보와의 상관 분석 진행 및 연계 조건 수립에 한계가 있다. 하지만 AhnLab EDR을 SIEM과 연계하면, 이슈 이벤트 경보 조건을 다양화하고, 심각도 기준을 세분화해 위협 및 대응 우선순위에 대한 판단이 용이하며, 엔드포인트 위협에 실시간으로 대응할 수 있어 조치 평균 응답시간(MTTR) 및 운영 리소스를 줄인다.

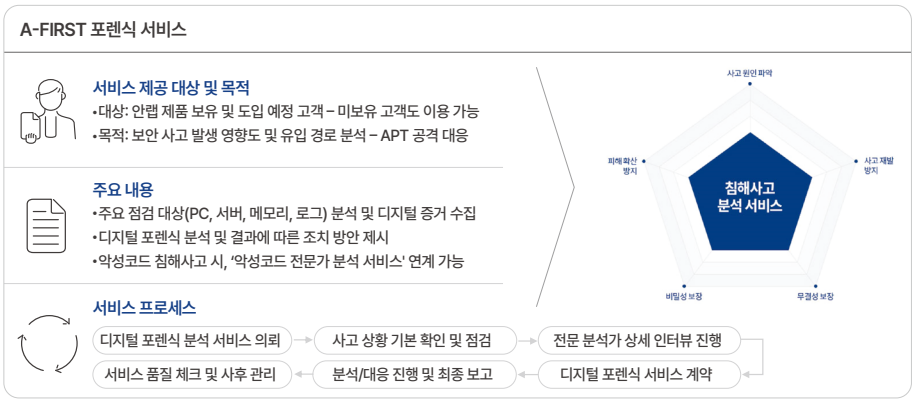
(3) 안랩 전문가 서비스 연계 – 최적의 대응 방안 제시

AhnLab EDR을 MDR 서비스와 함께, '안랩 프로페셔널 서비스(Professional Service)'와 연계하면 국내 최고의 악성코드 전문 분석가가 기업 및 기관에 유입된 악성코드(파일)의 다운로드 및 복제, 생성, 네트워크 등의 기능과 특성을 상세 분석해 의심 행위 정보에 따른 대응 방안을 제시한다. 또한, 내부로 유입된 악성코드의 기본 정보, 악성 여부, 행위 정보 등을 정리한 분석 보고서도 제공한다.

더 나아가, 침해사고에 따른 영향도와 유입 경로를 디지털 포렌식 기술로 분석해 리스크를 관리하고, APT 공격 등의 보안 사고 재발을 방지한다.

AhnLab EDR 실전 활용 방안 (3): 안랩 프로패셔널 서비스 연계를 통한 침해사고 분석 및 위협 대응 방안 도출

[그림 16] AhnLab EDR 연계 서비스 – 악성코드 전문가 분석 서비스



[그림 17] AhnLab EDR 연계 서비스 – A-FIRST 포렌식 서비스

맺음말

AhnLab EDR은 악성코드 감염이나 침해사고 예방을 위한 기술적 보호 조치가 필요한 모든 기업과 기관에 필수적인 보안 솔루션이다. 다만, AhnLab EDR을 도입할 때 획일적인 관점으로 접근해서는 안 된다. EDR 자체가 탐지 및 분석 정보가 많은 무거운 솔루션이기 때문에, 현 조직의 규모와 IT 인프라 현황, 비용, 구체적인 활용 방안 등 여러 가지 요소를 고려해야 한다. 또한, 단독으로 운영하는 것보다 다른 제품과 연계했을 때 더 큰 보안 가치를 제공한다는 점을 염두에 둬야 할 것이다. 기존 IT 환경에서 EDR로 보완 가능한 영역을 적극적으로 검토하고, 그에 맞게 EDR을 '맞춤형'으로 구축하는 것이 바람직하다. 필요시, 안랩과 같은 전문 업체의 컨설팅을 받는 것도 좋은 방법이다.

AhnLab EDR에 관한 자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인할 수 있다.

▶AhnLab EDR 제품 소개 페이지 바로가기

▶AhnLab EDR 도입 사례 소개 동영상 바로가기

AhnLab

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