AhnLab XDR

위협 탐지 & 대응의 끝없는 진화

AhnLab XDR은 정교한 위협 탐지, 상관관계 분석, 리스크 지수화를 통해
한 차원 높은 위협 탐지 & 대응을 구현합니다.

AhnLab XDR 소개

최근 업무 환경이 변화하고 사이버 위협이 고도화되면서 조직에서 도입하는 보안 솔루션 수도 증가하고 있습니다. 각 보안 솔루션에서 동시에 많은 양의 이벤트 정보를 생성하기 때문에, 보안 관리자는 위협 우선순위 판단에 어려움을 겪게 됩니다. 이에 따라, 다양한 보안 영역의 탐지 정보를 수집해 연계 분석하여 최적의 위협 대응 방안을 제시할 수 있는 XDR(eXtended Detection and Response) 플랫폼이 필요한 시점입니다.

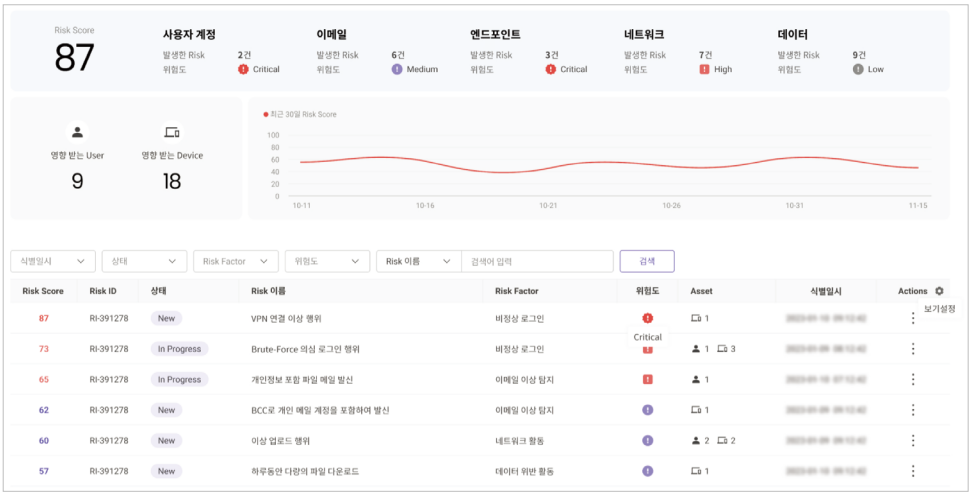
AhnLab XDR은 보안 솔루션, 이메일 등 사내에 구축하여 운영 중인 시스템에서 생성되는 로그를 기반으로 조치가 필요하거나 확인이 필요한 리스크(Risk)에 대한 우선순위를 파악하고 관리할 수 있도록 하는 클라우드 기반 XDR 플랫폼입니다.

그 동안, 조직들은 보안 영역 별로 개별 솔루션을 통해 위협을 탐지해 대응해 왔습니다. AhnLab XDR은 유연한 연동을 바탕으로 다양한 형태의 이기종 로그를 수집하고, AI/ML 학습 기능을 적용해 사용자와 자산을 기반으로 리스크를 분석 및 대응하여 조직의 보안 수준을 향상시킵니다.

주요 기능

리스크 지수화

AhnLab XDR은 최초 수집한 로그 데이터를 정규화 및 보강하여 연계 분석 및 상관관계 분석을 수행합니다. 분석 결과를 바탕으로 리스크를 도출해 지수화하여 사용자가 직관적으로 위협의 우선순위와 영향도를 파악해 대응 전략을 수립할 수 있도록 합니다.



최신 시나리오 룰

AhnLab XDR에는 기존 발생했던 리스크와 최근 유행하는 리스크 시나리오를 사전 정의한 시나리오 룰이 적용되어 있습니다. 또, 시나리오 룰을 실시간으로 지속 업데이트 하여 사용자가 최신 위협에 대응할 수 있도록 합니다.

*** 시나리오 예시: 내부자에 의한 중요자료 외부 유출**

최근 1달 내 해당 사용자 행동 패턴 분석을 통해 임계치 산출

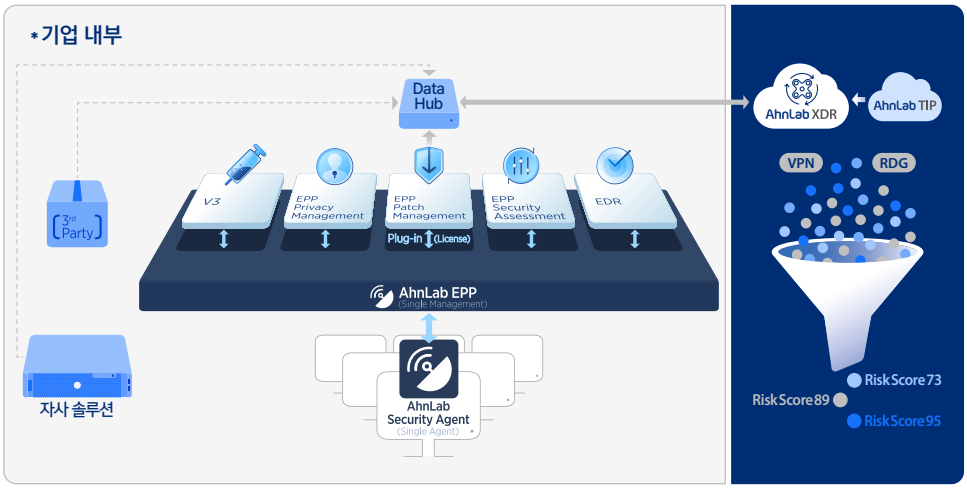
✓ 9시 출근/6시 퇴근
✓ 1시간 내 10개 미만의 파일 다운로드
✓ 작업 파일을 사내 서버로 업로드함. 1달 이내 300MB 미만
✓ 외부 메일 사용하지 않음
✓ 외부 메일 첨부 용량이 1달 이내 10MB 미만

수집정보	행동	타임라인
계정	내 계정으로 정상 로그인	AM 9:00
시간/위치	저녁 9시 근무중, 회사	
접속시스템	내부 문서관리 시스템 (예: Docs) 접속	PM 9:00
	파일 다운로드 크기 증가	
다운로드 이력	다수 프로젝트 파일 다운로드(200 files)	PM 9:01 – 9:30
파일 압축 이력	다수 프로젝트 파일을 압축	PM 9:31
	최초 수신자, 외부 개인메일	
외부시스템접속	외부 웹 메일 접속	PM 9:35
	발송 메일 첨부 파일의 크기 증가	비 업무 시간
대용량 첨부 이력	메일에 대용량 파일 첨부	PM 9:36
None	AhnLab XDR 데이터 유출 의심 탐지/차단	PM 9:37
None	보안팀 출근, XDR 대시보드 확인	다음날 AM 10:00

주요 기능

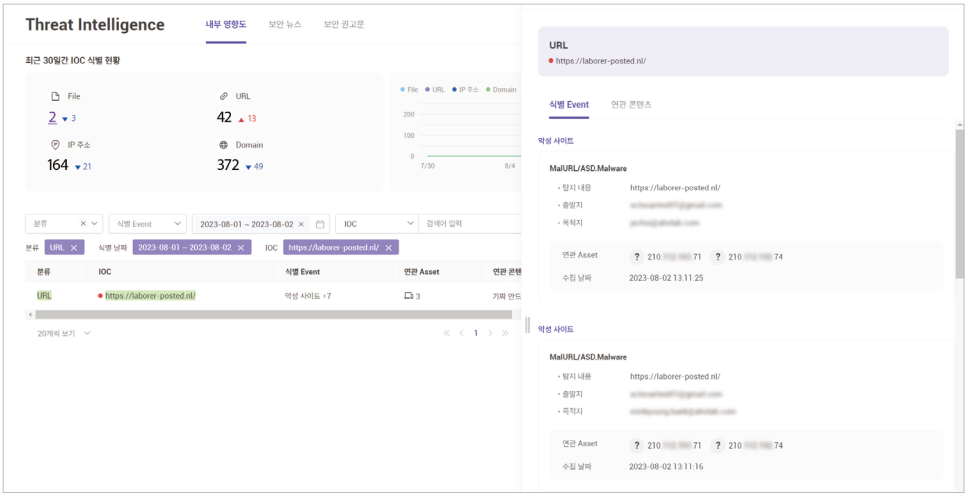
로그 수집 및 연계 대응

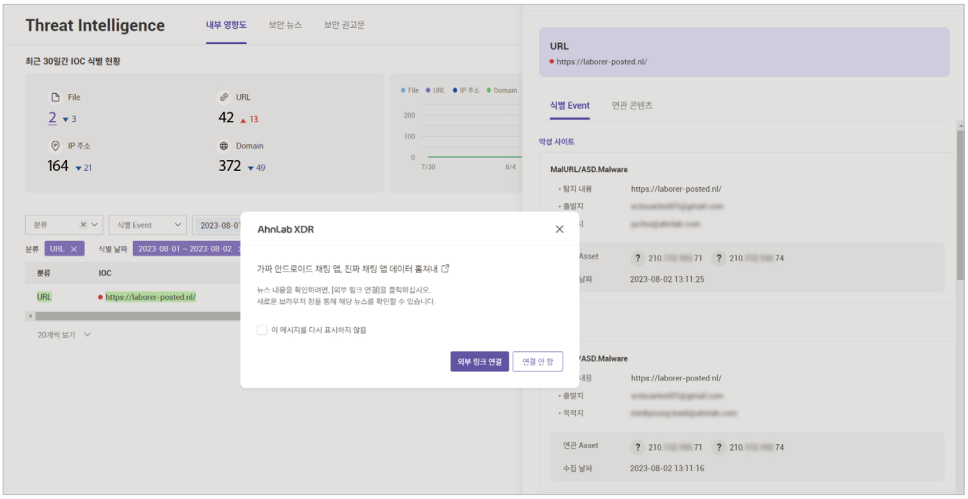
AhnLab XDR은 AhnLab EPP, EDR과 연동해 사용자와 자산의 추가 데이터를 수집해 대응에 활용할 수 있습니다. 또한, 별도 에이전트 없이도 AhnLab Data Hub를 통해 기존 운영 중인 보안 솔루션들과 연계해 데이터를 확보하고 위협에 대응할 수 있습니다.



안랩 TI 기반 내부 영향도 모니터링

안랩의 위협 인텔리전스 플랫폼 AhnLab TIP에서 확인된 침해지표(IoC) 정보가 내부 자산에 존재하는지 확인할 수 있도록 모니터링 기능을 지원합니다. 모니터링 결과 내부에 존재하는 것으로 확인된 침해지표와 유관한 콘텐츠가 있을 경우 바로 연결 가능합니다. 또한, 기본적으로 제공되는 뉴스 클리핑과 보안 권고문 등 최신 위협 정보를 확인할 수 있도록 더욱 풍부한 위협 인텔리전스를 제공합니다.

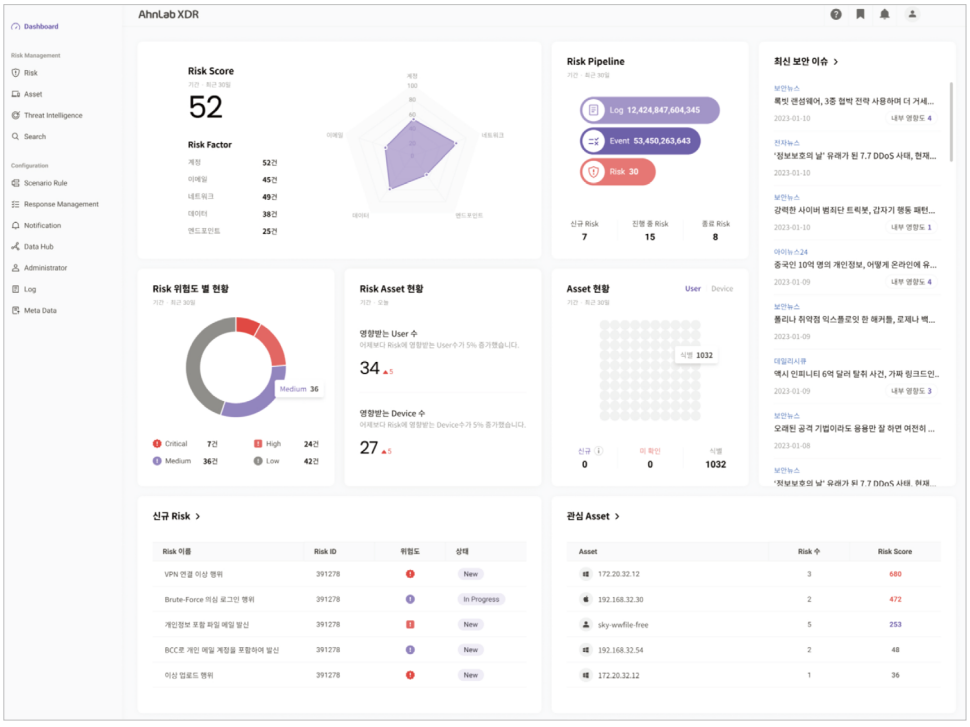




대시보드

AhnLab XDR 대시보드에서는 현재 조직의 전체 리스크(Risk) 수준을 리스크 점수(Risk Score)로 제공하고, 리스크 점수와 관련 있는 사용자(User)와 자산(Asset) 정보를 직관적으로 확인할 수 있습니다. 사용자와 자산의 리스크는 '리스크 팩터(Risk Factor)'의 다섯가지 항목으로 구분하며, 각 항목으로 탐지된 세부 내용은 '리스크 상세보기'를 통해 확인할 수 있습니다.

또한, 최근 30일 내 수집된 로그(Log)와 이벤트(Event) 수준을 확인하고 ▲새롭게 확인된 리스크 ▲조치 진행 중인 리스크 ▲완료된 리스크 현황 정보를 볼 수 있으며, 신규 확인 및 미확인 사용자와 자산정보 현황도 확인할 수 있습니다. 아울러, 최근 발생한 'Top 5 리스크 현황' 및 관심 자산 설정 내역도 모니터링 가능합니다. 이 밖에, AhnLab TIP와 연동해 최신 뉴스, IoC 정보 및 관련 콘텐츠 등을 확인할 수 있습니다.



도입효과

보안 관리자는 AhnLab XDR을 통해 리스크를 정확하게 식별하고, 리스크 지수(Risk Score)를 바탕으로 조치해야 할 우선순위를 판별할 수 있습니다. 또한, 확인 및 조치가 필요한 리스크에 대해서는 유연한 연동을 통해 다양한 방법으로 체계적인 대응이 가능합니다. 궁극적으로, 사내 보안 수준을 향상시키고 보안을 효율적으로 관리할 수 있게 됩니다.

정확한 리스크 식별

사용자(ID, 회사명, 부서명, 이름, 이메일 주소 등)가 보유한 자산(디바이스 ID, 호스트 이름, IP, Mac 등)을 기준으로 모니터링을 진행하고 ▲엔티티(entity) 상태 정보 ▲사용자/디바이스 행위 정보를 연계 분석해 리스크를 정확하게 식별할 수 있습니다.

유연한 연동 기반 체계적인 대응

AhnLab XDR은 기존 고객이 운영 중인 이기종 보안 솔루션들의 로그를 안정적으로 수집하여 데이터 연계 분석을 수행합니다. 최종 확인된 침해(Incident)에 대한 대응(Response)은 운영 중인 보안 솔루션들과 연계하여 체계적으로 대응 가능합니다.

보안 수준 및 운영 편의성 향상

SaaS 형태로 제공되는 AhnLab XDR은 지속적인 업데이트와 향상된 운영 편의성을 제공합니다. 또, 안랩의 위협 인텔리전스 연동을 통해 자산의 최신 위협 영향도를 확인해 대응할 수 있으며, 전용 에이전트 없이 보안 솔루션들의 로그를 수집해 자산 성능에 영향을 미치지 않습니다.

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901
© 2023 AhnLab, Inc. All rights reserved.

AhnLab