AhnLab

White Paper

AhnLab XDR
통합 보안의 정점을 향하다

AhnLab XDR은 조직 내 시스템으로부터 위협정보를 수집해 분석 · 탐지 · 대응을 제공하는 클라우드 기반 '보안 위협 분석 플랫폼'

개요

AhnLab XDR은 조직 내 수많은 시스템으로부터 위협정보를 수집해 분석 · 탐지 · 대응을 제공하는 클라우드 기반 SaaS형 '보안 위협 분석 플랫폼'이다. 보안 솔루션부터 이메일 등 업무용 시스템까지 다양한 이기종 솔루션으로부터 생성된 데이터를 연계 분석해, 보안 리스크(Risk) 우선순위를 직관적으로 제공하고 연동 솔루션을 활용한 자동 대응까지 제공한다.

AhnLab XDR은 보안 담당자가 실제 업무 과정에서 겪는 어려움을 제품에 적극 반영한 점이 특징이다. ▲사용자와 자산 중심 리스크 지수화 및 관리 ▲안랩이 축적해온 위협대응 노하우가 녹아있는 '시나리오 룰'을 활용한 리스크 분석 · 대응 ▲위협 인텔리전스(TI) 연동으로 위협이 조직에 미치는 영향도 파악 등 보안 업무의 효율성을 높일 수 있는 기능을 제공한다.

> "많은 수의 보안 담당자들은 다양한 보안 솔루션이 탐지한 위협에 개별적으로 대응해왔기 때문에 대응 우선순위 파악에 어려움을 겪고 있다. 광범위한 소스에서 정보를 수집해 연계 분석하고 최적의 대응 방안을 제시하는 XDR 플랫폼이 필요한 시점."
> – 안랩 김창희 제품서비스기획실장

> "최근 디지털전환이 급속하게 진행됨에 따라, 사이버 보안 리스크 관리는 곧 비즈니스 경쟁력이 됐다. AhnLab XDR을 통해 고객에게 조직 내 자산의 보안 리스크에 대한 통합적인 관리를 제공하고, 고객이 보다 효율적인 보안운영 환경을 구축해 비즈니스 경쟁력을 강화할 수 있도록 지원할 것"
> – 안랩 강석균 대표

XDR vs EDR

- 데이터 수집 및 분석 범위의 차이
- XDR은 엔드포인트, 네트워크, 클라우드 등 다양한 영역의 데이터를 수집해 리스크 식별

XDR vs SOAR

- 데이터 수집 및 알림(Alert) 방식의 차이
- SOAR는 SIEM을 통해 데이터를 수집하고 플레이북으로 자동 대응
- XDR은 데이터를 직접 수집, 분석 및 대응

XDR이란 무엇인가?

XDR은 'eXtended Detection and Response'의 약자로, 국문으로는 '확장형 탐지 & 대응'으로 해석된다. 조직에서 운영 중인 여러 이기종 보안 솔루션의 데이터를 수집 및 정규화(normalize)하고, 다양한 이벤트 정보를 종합적으로 분석하여 궁극적으로 리스크(Risk)를 식별, 탐지 및 대응할 수 있도록 한다.

사용자들이 XDR을 접하면 "XDR과 EDR(Endpoint Detection & Response) 및 SOAR(Security Orchestration, Automation and Response)와 무엇이 다른가?"라는 질문을 자주 한다. XDR, EDR, SOAR는 '데이터 수집 > 분석 > 대응'이라는 큰 틀의 프로세스에서는 유사해 보이지만, 그 방식과 초점에 차이가 있다.

우선, XDR과 EDR은 데이터 수집 및 분석 범위에 차이가 있다. EDR은 이름에서 유추할 수 있듯, 엔드포인트 영역의 데이터를 수집하고 해당 데이터를 기반으로 연계 분석을 수행한다. 따라서, 엔드포인트에서 벌어지는 위협 행위 정보를 상세하게 확인할 수 있지만, 그 외 영역에서 발생하는 정보 수집 및 연계에는 한계가 있다. 반면, XDR은 엔드포인트, 네트워크, 클라우드 등 광범위한 영역의 데이터를 수집할 수 있으며, 다양한 데이터를 기반으로 상황정보(Context, 컨텍스트)를 분석하고 리스크를 식별한다.

XDR과 SOAR는 수집 및 알림(Alert) 방식에 차이가 있다. SOAR의 경우 SIEM(Security Information and Event Management)을 활용해 여러 솔루션에서 데이터를 수집한다. 이후, 수집한 데이터 중 위협으로 판단해 생성한 '사건(Incident)'에 대해 플레이북(Playbook)을 통한 자동화 대응 조치를 수행한다. 반면, XDR은 분석에 필요한 데이터를 직접 수집해 분석 및 대응한다. 위험 가능성이 있는 '사건'에 대해 별도 확인이 필요한 SOAR와 달리 XDR은 각 사건의 상황 정보, 우선순위 등을 연계 분석해 사용자가 대응할 수 있도록 한다.

XDR에 대한 관심이 높아지는 이유

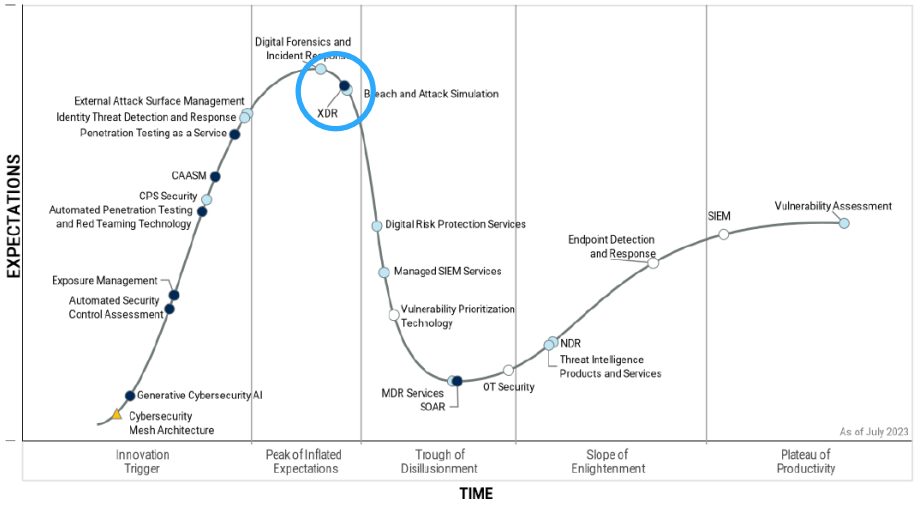
XDR이라는 개념은 지난 2018년 처음 등장했는데, 그 배경에는 기업의 보안 환경과 보안 시장의 급격한 변화가 있었다. 보안 위협이 IT 환경 전반에 걸쳐 전개되고, 공격 기법이 고도화됨에 따라 기업들은 엔드포인트, 네트워크 등 여러 보안 영역에 다양한 보안 솔루션들을 배포해 운영하기 시작했다.

안정기를 향해 가고 있는 XDR, 향후 5년 뒤 약 3조원의 시장 규모 형성 전망

이러한 경향은 코로나19 팬데믹으로 디지털 전환이 빠르게 진행되면서 더욱 가속화되었고, 기업들은 보안 관리 복잡성이라는 도전과제를 마주하게 됐다. 특히, 보안 담당자들은 여러 종류의 고도화된 보안 솔루션들을 운영하면서 업무가 가중되었고, 발생하는 이벤트(Event) 양 증가로 인해 우선순위 판단이 어려워졌다. 이에 따라, '보안 효율화'와 '플랫폼'에 대한 요구가 증가했고 통합된 위협 탐지 & 대응 역량을 제공하는 XDR이 많은 주목을 받게 되었다.

시장조사기관 가트너(Gartner)에서 발행하는 '하이프사이클(Hype Cyle)' 보고서를 보면, XDR을 향한 시장의 기대치를 알 수 있다. 가트너는 매년 분야 별로 기술에 대한 기대와 경험을 정리해 하이프사이클 보고서를 발간하는데, XDR은 보고서를 기준으로 엔드포인트 보안(Endpoint Security)와 보안 운영(Security Operations) 영역에서 중요한 기술로 꼽힌다.

2021년부터 2023년까지의 하이프사이클을 보면, XDR은 2021년 기대치가 빠르게 상승하여 2022년 정점을 찍은 뒤, 2023년에는 하강 곡선에 돌입했다. 하강 곡선을 그린다는 것은 XDR이 만병통치약 혹은 마스터키가 될 것이라는 오해가 해소되고, 사람들이 XDR의 본질을 제대로 이해하면서 기술이 시장에 안착하는 과정에 접어들었음을 의미한다.



[그림 1] 2023 Hype Cycle for Security Operations (출처: 가트너)

기대치 관점에서 안정기를 향해 가고 있는 XDR은 앞으로 큰 폭의 지속적인 성장이 예상된다. 시장조사기관 '마켓 앤 마켓(Markets and Markets)는 글로벌 XDR 시장이 2027년까지 연평균 19.1% 성장해 약 24억 달러(한화 약 3조 2400억원) 규모에 이를 것으로 전망했다. 월드와이드 테크놀로지(World Wide Technology) 역시 XDR 시장 규모가 2028년 20억 6천만 달러(한화 약 2조 7900억원)에 달할 것으로 내다봤다.

고객 요구사항 해결에 중점
·쉽고 효율적인 보안 관리
·위협의 우선순위를 정확하게 판별해 대응

안랩이 파악한 고객의 요구사항

안랩은 지난 3년간 XDR을 준비하면서, 기존 포인트 솔루션의 한계와 플랫폼 접근을 향한 요구사항을 면밀하게 파악했다. 물론, 여러 보고서들을 통해서도 어느정도 파악이 가능한 내용이었지만, 고객들의 요구사항을 보다 면밀하게 파악하기 위해, 수 백개 고객사의 보안 담당자들을 대상으로 인터뷰를 진행했다.

인터뷰에서 고객들은 보안 운영에 대한 다양한 하지만 공통된 어려움들을 호소했는데, ▲사용자 및 자산 추적 ▲모니터링 ▲회복력(Resilience) 확보 ▲너무 다양한 환경 ▲이기종 솔루션 운영 등이 주요 내용이었다. 또한, 전사적으로 보안 수준을 향상시키고 싶지만 인원과 업무량을 고려했을 때 현실적으로 어렵다는 점과 보안 사일로(silo) 해결이 필요하다는 점을 이야기했다.

[그림 2] 보안 담당자 대상 인터뷰 결과

고객들이 직접적으로 XDR을 언급하지는 않았지만, 요구사항들을 종합해보면 자연스럽게 XDR이 제공하는 또 제공해야 할 역량으로 귀결됐다. 안랩은 복잡성 문제를 겪고 있는 기업의 보안 관리자들이 쉽고 효율적으로 보안을 관리하면서도 위협의 우선순위를 정확하게 판별해 대응할 수 있도록 하는 것을 중점에 두고, XDR 플랫폼을 개발했다.

AhnLab XDR의 핵심은 '리스크' 관리

AhnLab XDR을 정의하면, 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 XDR 플랫폼이다. AhnLab XDR은 안정성 및 확장성을 고려하여 클라우드 기반 SaaS(Software-as-a-Service) 형태로 제공된다. 기본적으로는 퍼블릭 클라우드(AWS)에서 운영되며, 프라이빗 클라우드도 지원할 예정이다.

AhnLab XDR은 위협 탐지 & 대응을 넘어 효과적인 '리스크(Risk)' 관리를 통해 조직의 보안 수준 향상

AhnLab XDR의 핵심 지향점은 '효과적인 리스크(Risk) 관리'이다. 개념 설명을 부연하면, 그 동안 대부분의 사이버 보안은 '위협(Threat)'에 대한 탐지와 대응에 초점을 맞춰왔다. 하지만, 위협은 마주하는 조직의 상황에 따라 위험(리스크)의 정도가 다를 수 있다.

실생활의 예시를 들어, 감기라는 위협이 있다고 가정해보자. 똑같은 감기라도 사람의 건강 상태, 나이 등 다양한 요소에 따라 그 위험도는 달라진다. 어떤 사람은 감기가 치명적일 수 있어 즉각적인 대응과 조치가 필요한 반면, 또 다른 사람에게는 시간을 두고 지켜보는 것만으로 충분할 수도 있다. 일차적으로 감기라는 위협에 잘 대응하는 것도 중요하지만, 건강이라는 관점에서 궁극적인 목적은 위험을 잘 관리해 건강한 상태를 유지하는 것이다.

조직의 보안도 마찬가지로, 위협을 많이 탐지하고 대응하는 것을 넘어 우선순위에 따라 리스크를 잘 파악하고 관리하여 보안의 건강한 상태를 지속해 나가야 한다. 그리고 AhnLab XDR은 효과적인 리스크 관리를 통해 조직이 보안 위험을 최소화할 수 있도록 기여한다.

AhnLab XDR은 유연한 연동을 바탕으로 다양한 형태의 이기종 로그를 수집하고, '사용자(User)'와 '자산(Asset)'을 기반으로 리스크를 분석해 대응한다. 이를 통해, 그 동안 개별 솔루션들로 위협을 탐지해 대응해왔던 조직들은 보안에 대한 통합된 가시성을 확보하는 동시에 정확한 우선순위 별로 리스크를 관리하여 조직 전반의 보안 수준을 향상시킬 수 있게 된다.

AI/머신러닝 기술을 기반으로
차별화된 정확성을 확보하고
최적의 대응 방안 제시

[그림 3] AhnLab XDR 개념도

특히, AhnLab XDR은 AI/머신러닝 기술을 적용하여 차별화된 리스크 관리 효율성 및 정확성을 확보했다. 우선, AI와 머신러닝 기술을 기반으로 수 많은 데이터의 행동 특성을 분석하는 '데이터 프로파일링(Data Profiling)' 역량을 갖추고 있다. 이를 통해, 특정 상황이나 영역에서의 행동을 예상하여 선제적으로 대응할 수 있다. 또한, 머신러닝 임계치를 활용하여 사용자의 디바이스의 행동 패턴을 학습하며, 이상 행위 발생 시 최적의 조치 방안을 제시한다.

궁극적으로는 다양한 영역의 이벤트와 데이터를 연계분석(Context) 분석하고, 이를 후술할 '리스크 지수(Risk Score)로 산출한다. 리스크를 지수화는 위험도에 따른 우선순위를 확인하는 것이 목적이며, 확인된 리스크에 대해서는 여러 보안 솔루션들과 연계하여 알림, 분류 혹은 조치할 수 있다.

AhnLab XDR 주요기능

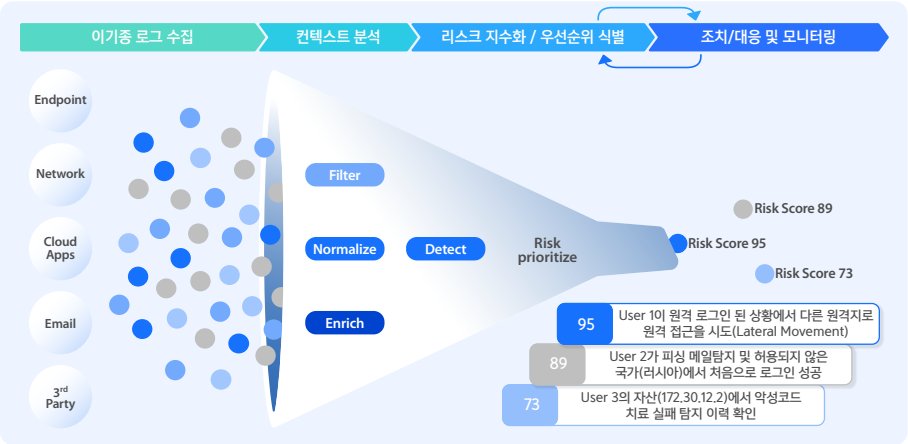
AhnLab XDR은 효과적인 리스크 관리를 위해 ▲리스크 우선순위 식별 및 지수화 ▲고도화된 리스크 시나리오 룰 ▲위협 인텔리전스 기반 내부 영향도 모니터링 ▲이기종 로그 연계분석 및 써드파티 솔루션 연동 등 XDR에 요구되는 핵심적인 역량들을 제공하는 방향으로 설계되었다.

리스크 지수화(Risk Scoring)를 통해 보안 관리자는 우선순위에 따라 리스크를 빠르게 조치하고 잠재적인 리스크까지 확인 가능

1. 리스크 우선순위 식별 및 지수화

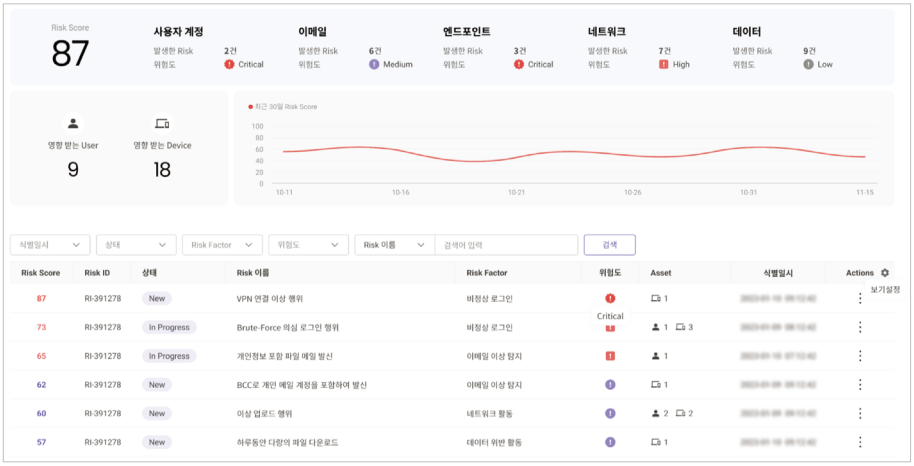
리스크 우선순위 식별과 지수화는 AhnLab XDR의 기반이자 정체성이라고도 할 수 있는 기능이다.

AhnLab XDR은 기본적으로 '로그 수집 > 이벤트 분류 > 이벤트 연계'의 과정을 거쳐 이벤트의 컨텍스트(Context)를 분석한다. 이를 통해, 단편적인 로그와 이벤트만으로는 확인하기 어려운 리스크를 필터링, 정규화 및 보강하여 리스크를 정확하게 식별하고 우선순위를 도출한다. 더 나아가, 분석 결과를 바탕으로 리스크를 지수화하여, 보안 관리자가 우선순위대로 리스크를 빠르게 조치하고 잠재적인 리스크까지 확인할 수 있도록 한다.



[그림 4] A hnLab XDR 리스크 우선순위 식별 및 지수화 과정

AhnLab XDR 화면을 통해 좀 더 자세히 살펴보자.



[그림 5] AhnLab XDR 리스크 지수화

타사들과 달리 0~100점 범위에서 산정되는 리스크 점수를 통해 직관적인 리스크 우선순위 식별 지원

AhnLab XDR의 '리스크(Risk)' 카테고리에서는 조직의 전반적인 리스크 점수와 함께 ▲사용자 계정 ▲이메일 ▲엔드포인트 ▲네트워크 ▲데이터 등 여러 세부 영역에 걸쳐 어떤 리스크가 존재하고 그 위험도는 어느 정도인지 직관적으로 나타낸다. 뿐만 아니라, 사용자(User)와 디바이스(Device) 자산을 기준으로 어느 정도 영향을 받는지 확인할 수 있다. 보안 관리자는 화면 하단의 리스크 내역을 통해 각 리스크의 상세 정보를 확인하고, 이를 해결하기 위한 적합한 조치를 수행할 수 있다.

AhnLab XDR의 리스크 지수는 0~100점의 범위에서 산정된다. 타사 솔루션들을 보면 리스크 점수가 500점 혹은 1,000점을 넘어가는 경우가 있는데 이 경우 리스크의 수준을 제대로 파악할 수 없다. AhnLab XDR은 모든 사람들에게 익숙한 숫자 범위 내에서 리스크 지수를 제공하여 보안 관리자들의 위험의 정도를 직관적으로 파악할 수 있도록 했다.

또한, 정교한 리스크 지수 도출을 위해 고도화된 계산식이 적용되었다. 간단히 설명하면, 자산가치(Asset), 이벤트(Threat), 확률(Likelihood), 가중치(Value) 등의 요소들을 종합적으로 계산하는 것으로 이해하면 된다. AhnLab XDR의 리스크 지수는 이벤트와 자산 가치만 고려하면 리스크를 판단하기 어렵기 때문에 가중치를 함께 고려하며, 위험 확률이 같더라도 자산의 중요도에 따라 다른 점수가 나오게 된다. 이를 통해, 낮은 위험과 높은 위험을 차별화하여 리스크 우선순위를 정확하게 설정할 수 있다.

2. 고도화된 리스크 시나리오 룰

AhnLab XDR의 또 다른 강점 중 하나는 바로 고도화된 리스크 시나리오 룰이다. 보안 관리자 입장에서는 최근 유행하는 리스크 시나리오에 항상 대비하고자 하지만, 이를 직접 반영하는 것은 현실적으로 불가능한 일이다.

이에 대해, AhnLab XDR은 지난 30년 간의 위협 분석 및 대응 경험을 토대로 실제 발생했던 시나리오를 반영하고 새로운 시나리오를 지속적으로 업데이트 한다. 룰(Rule) 역시 안랩이 제공 및 업데이트 하며, 고객에 맞게 세팅하여 최소한의 노이즈(noise)로 최적의 대응 역량을 확보할 수 있다.

AhnLab XDR의 리스크 시나리오를 '내부자 A에 의한 중요자료 외부 유출' 예시를 통해 살펴보자.

고도화된 시나리오 룰을 바탕으로 최신 리스크에 효과적으로 대응하는 동시에 불필요한 '노이즈(noise)' 최소화

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

[그림 6] AhnLab XDR 리스크 시나리오 예시

우선, AhnLab XDR은 앞서 소개한대로 머신러닝을 기반으로 내부자 A의 행동 패턴 분석을 통해 임계치를 산출한다. 파악한 행동 패턴은 출퇴근 시간, 파일 다운로드 및 업로드 빈도, 외부 메일 사용 여부 등이 있다.

어느날, 내부자 A가 중요파일 외부 유출을 시도했다. 이 과정에서, 비 업무시간 근무, 다수 프로젝트 파일 다운로드, 개인 외부메일 접속, 대용량 파일 첨부 등 내부자 A가 평소에 하지 않았던, AhnLab XDR이 산출한 임계치를 초과하는 행위가 다수 탐지된다. 그리고 AhnLab XDR은 적용된 시나리오 룰에 따라, 이를 데이터 유출 행위로 탐지하고 차단한다.

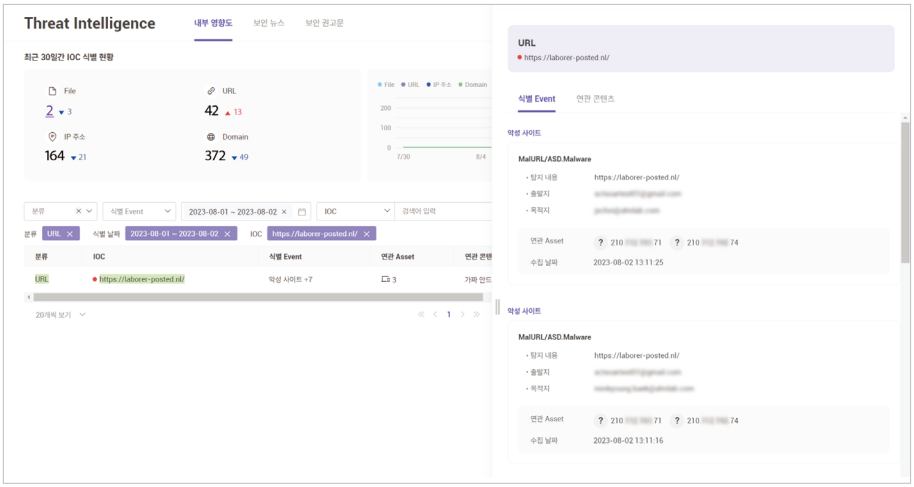
보안 관리자는 다음날 아침에 AhnLab XDR 대시보드를 통해 탐지 및 조치 내역을 보고, 내부 중요파일 유출 행위를 차단했다는 사실을 편리하게 확인할 수 있다.

위협 인텔리전스(Threat Intelligence) 연동을 통해 최신 위협과 내부 영향도를 즉각적으로 확인하여 대응

3. 위협 인텔리전스 기반 내부 영향도 모니터링

최근 사이버 위협이 고도화를 거듭함에 따라, 위협 인텔리전스(Threat Intelligence)의 중요성이 높아지고 있다. 그리고, 보안 플랫폼에도 최신 위협 인텔리전스를 적용해 분석 및 대응 역량을 강화하는 것이 중요한 과제가 되었다.

AhnLab XDR은 자사 위협 인텔리전스 플랫폼 AhnLab TIP 연동을 통해, AhnLab TIP에서 확인된 침해지표(IoC) 정보가 내부 자산에 존재하는지 확인할 수 있도록 모니터링 기능을 지원한다. 모니터링 결과 침해지표에 탐지된 이벤트가 존재하는 사용자와 자산이 있을 경우, 해당 사용자와 자산에 대한 세부 정보를 확인하여 즉각적으로 조치 및 대응할 수 있다.



[그림 7] AhnLab XDR 위협 인텔리전스 화면 – 침해지표 및 영향도

또한, 기본적으로 제공되는 뉴스 클리핑에 더해 보안 권고문 등 최신 위협 정보를 확인할 수 있도록 더욱 풍부한 위협 인텔리전스를 제공하며, 침해지표와 유관한 콘텐츠를 기준으로 내부 자산에서 탐지된 연관 침해지표 정보를 확인할 수 있다.

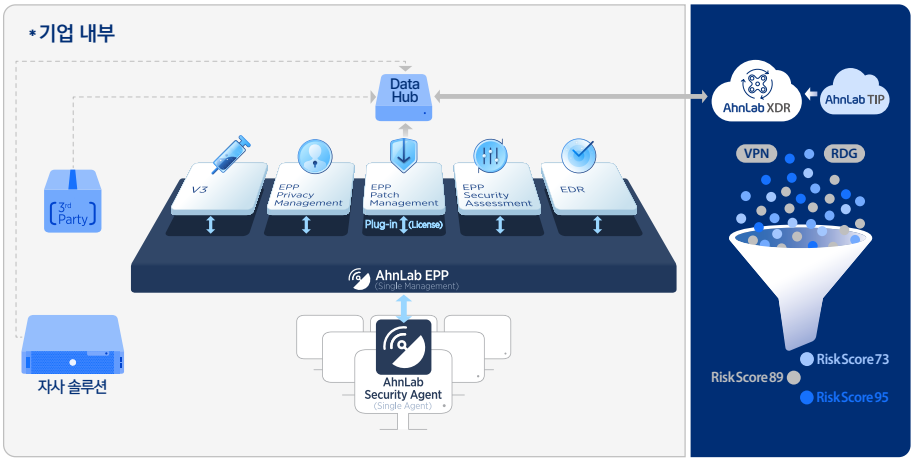
4. 이기종 로그 연계분석 및 써드파티 솔루션 연동

XDR의 방법론으로는 크게 자사 보안 솔루션을 중심으로 이기종 데이터 수집과 분석을 확장하는 개념의 'Native XDR'과 이기종 데이터 수집 및 빅데이터 분석을 기반으로 보안 솔루션 연동을 확장하는 'Open XDR'이 있다. 지금까지 안랩의 방향성은 'Native XDR'에 가까웠지만, AhnLab XDR은 오픈 플랫폼으로 구성했다. 고객이 운영하고 있는 여러 솔루션 간 시너지가 중요하다고 판단했기 때문이다.

자사 뿐만 아니라 써드파티 솔루션 데이터까지 수집 및 연계분석하는 '오픈 플랫폼' 지향

·별도 에이전트 없이 데이터를 수집해 시스템 부하 최소화

이에, AhnLab XDR은 사용자와 자산을 기반으로 엔드포인트, 네트워크, 이메일 등 여러 보안 영역에 걸쳐 자사 솔루션 뿐만 아니라 써드파티 솔루션까지 데이터를 수집해 정규화 및 연계분석을 수행한다. 또한, 자사 엔드포인트 보안 플랫폼 'AhnLab EPP'와 엔드포인트 탐지 & 대응 솔루션 'AhnLab EDR'과 연동해 사용자/자산의 추가적인 데이터를 수집해 대응에 활용할 수 있다.



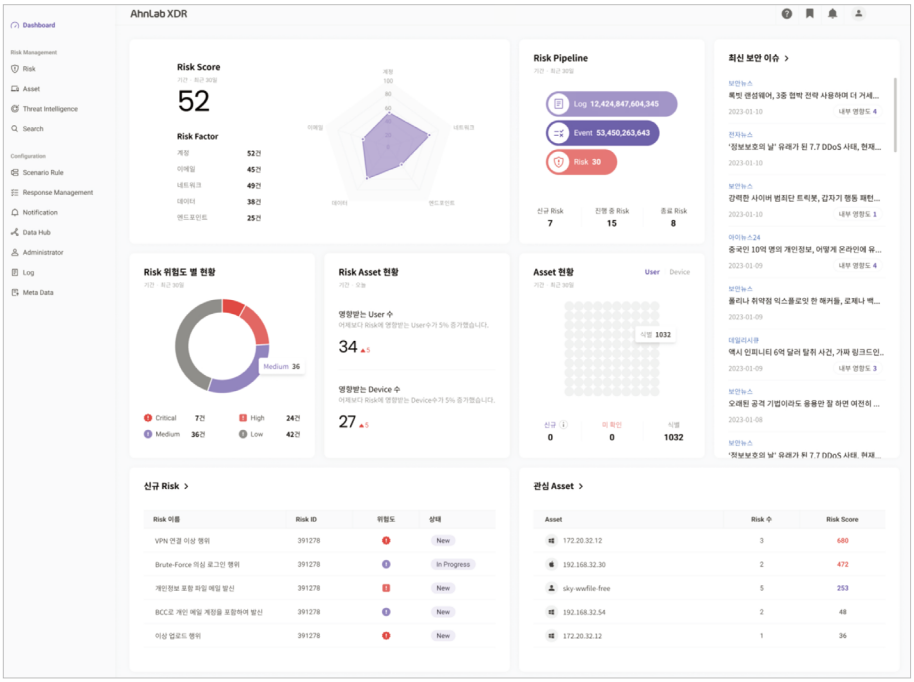
[그림 8] AhnLab XDR 연동 구조도

특히, 별도 에이전트 없이도 AhnLab Data Hub를 통해 기존 운영 중인 보안 솔루션들과 연계해 데이터를 확보하고 위협에 대응하는데, 이는 에이전트 설치로 인한 시스템 부하를 최소화한다는 점에서 운영에 상당한 이점으로 작용한다.

대시보드로 보는 AhnLab XDR

AhnLab XDR의 대시보드는 앞서 소개한 AhnLab XDR의 주요 기능과 역량들을 보안 관리자가 한 눈에 직관적으로 볼 수 있도록 구성됐다.

대시보드에서는 조직의 리스크 현황과 연관된 사용자/자산 정보 등 주요 정보를 직관적으로 확인 가능



[그림 9] AhnLab XDR 대시보드

대시보드에서는 현재 조직의 전체 리스크 수준을 나타내는 리스크 지수와 리스크 점수와 관련 있는 사용자/자산 정보를 직관적으로 확인할 수 있다. 사용자와 자산의 리스크는 '리스크 팩터(Risk Factor)'의 다섯가지 항목으로 구분하며, 각 항목으로 탐지된 세부 내용은 '리스크 상세보기'를 통해 확인할 수 있다.

또한, 최근 30일 내 수집된 로그와 이벤트 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 있다. 최근 발생한 'Top 5 리스크 현황' 및 관심 자산 설정 내역도 모니터링 가능하다. 이 밖에, AhnLab TIP와 연동한 최신 뉴스, 침해지표 정보 및 관련 콘텐츠 등도 대시보드에서 바로 확인할 수 있다.

도입효과

조직이 AhnLab XDR을 도입함으로써 얻을 수 있는 수 있는 효과는 크게 ▲정확한 리스크 우선순위 식별 ▲유연한 연동 기반 체계적인 대응 ▲보안 수준 및 운영 편의성 향상이 있다. 앞서 서술했던 내용들을 요약하는 관점에서 다음과 같이 간략히 정리한다.

1. 정확한 리스크 식별

보안 관리자는 AhnLab XDR을 활용해 사용자와 자산을 기준으로 모니터링을 진행하고 ▲엔티티(entity) 상태 정보 ▲사용자/디바이스 행위 정보를 연계 분석해 리스크를 정확하게 식별할 수 있다. 나아가, AhnLab XDR이 제공하는 리스크 지수를 바탕으로 조치해야 할 우선순위를 판별할 수 있다.

2. 유연한 연동 기반 체계적인 대응

AhnLab XDR은 기존 조직이 운영 중인 이기종 보안 솔루션들의 로그를 안정적으로 수집하고, 데이터 연계 분석을 수행한다. 최종 확인된 침해에 대한 대응은 운영 중인 보안 솔루션들과 연계하여 체계적으로 대응할 수 있어, 기존 포인트 솔루션을 운영하며 마주했던 대응 이슈를 상당 부분 해결할 수 있다.

3. 보안 수준 및 운영 편의성 향상

궁극적으로, AhnLab XDR을 활용해 보안을 효율적으로 관리하고 사내 보안 수준을 향상시킬 수 있다. SaaS 형태로 제공되는 AhnLab XDR은 지속적인 업데이트와 향상된 운영 편의성을 제공하며, 안랩의 위협 인텔리전스 연동을 통해 자산의 최신 위협 영향도를 확인해 대응 가능하다. 그리고, 전용 에이전트 없이 보안 솔루션들의 로그를 수집해 자산 성능에 영향을 미치는 영향을 최소화한다.

결론

AhnLab XDR의 목적을 한 마디로 요약하면 '무조건 많이 탐지해 보여주는 것이 아닌 리스크의 우선순위를 제공하고 지속적으로 관리할 수 있게 하여 조직의 위험도를 낮추는 것'이다.

이러한 AhnLab XDR의 가치를 극대화하기 위해 중요한 것은 더 많은 보안 솔루션들과 연동하여 더욱 다양한 이벤트들을 연계 분석하는 것이다. 안랩은 2023년 RSA 컨퍼런스의 슬로건이었던 'Stronger Together'의 가치에 입각해 고객, 그리고 다른 보안 벤더들과 함께 AhnLab XDR을 계속해서 발전시켜 나갈 계획이다.

AhnLab

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