AhnLab AI PLUS, AI 보안의 새로운 페이지를 열다

안랩은 최근 자체 구축 AI 플랫폼 AhnLab AI PLUS를 출시했다. AhnLab AI PLUS는 안랩이 30년간 축적한 위협 분석 데이터, 악성코드 및 침해 사고 대응 경험 등 방대한 보안 정보를 기반으로 개발한 자체 AI 플랫폼이다.

이번 글에서는 사이버보안 영역에서 AI의 발전사부터 안랩이 지속해온 AI 혁신과 AhnLab AI PLUS가 고객들에게 제공하는 가치까지 종합적으로 살펴본다.

AI는 어떻게 발전해왔나?

AI 발전의 몇 가지 변곡점들을 생각해볼 때 빼놓을 수 없는 것이 있다. 바로 바둑이다. 지난 2016년 3월, 알파고와 이세돌 9단의 대결을 통해 본격적으로 AI가 세상에 존재를 드러냈고, 이후 10년에 가까운 세월 동안 발전을 거듭해왔다.

AI 관점에서 바둑과 사이버보안을 비교해보면, 두 개 모두 상대방의 전략을 파악하고 대응 전략을 수립해야 한다는 공통점이 있다. 다만 바둑에는 명확한 게임 규칙이 있는 반면, 사이버보안은 공격자와 방어자 간 특정 규칙에 의해 공격과 방어가 이뤄지지 않는다. 한 마디로, 굉장히 불확실하다고 할 수 있다. 이러한 관점에서 사이버보안을 설명하기에 앞서, 사이버보안과 유사하지만 상대적으로 단순한 바둑에서 AI가 어떻게 사람을 이길 수 있었는지 복기해본다.

바둑에서 알파고의 등장은 자동화(Automation)에서 지능화(Intelligentization)로의 전환을 시사한다. 서양 보드게임인 체스(1997년, IBM Deep Blue)와 비교했을 때, 바둑에서 AI가 인간을 넘어서는데 약 20년이 더 걸렸다. 이렇게 오랜 시간이 걸렸던 이유는 바로 패턴 기반 자동화의 한계 때문이었다.

패턴 기반 자동화는 '기보', 즉 정해진 패턴을 토대로 바둑 돌을 기계적으로 두는 방식이다. 바둑은 경우의 수가 너무 많아 패턴 정의가 어렵고, 돌 하나하나의 의미와 전략적 가치가 주변 맥락에 따라 변화한다. 이러한 복잡성 때문에 패턴 기반의 기존 바둑 AI는 인간을 넘어서지 못했다.

이에 반해 알파고는 딥러닝 및 강화 학습을 통해 정해진 패턴에서 벗어나 스스로 상황을 판단하고 바둑 돌을 뒀고 사람이 예측하지 못한 창의적인 수로 인간을 넘어섰다. AI가 지능화된 것이다.

여기서 자동화와 지능화의 차이를 짚고 넘어가보자.

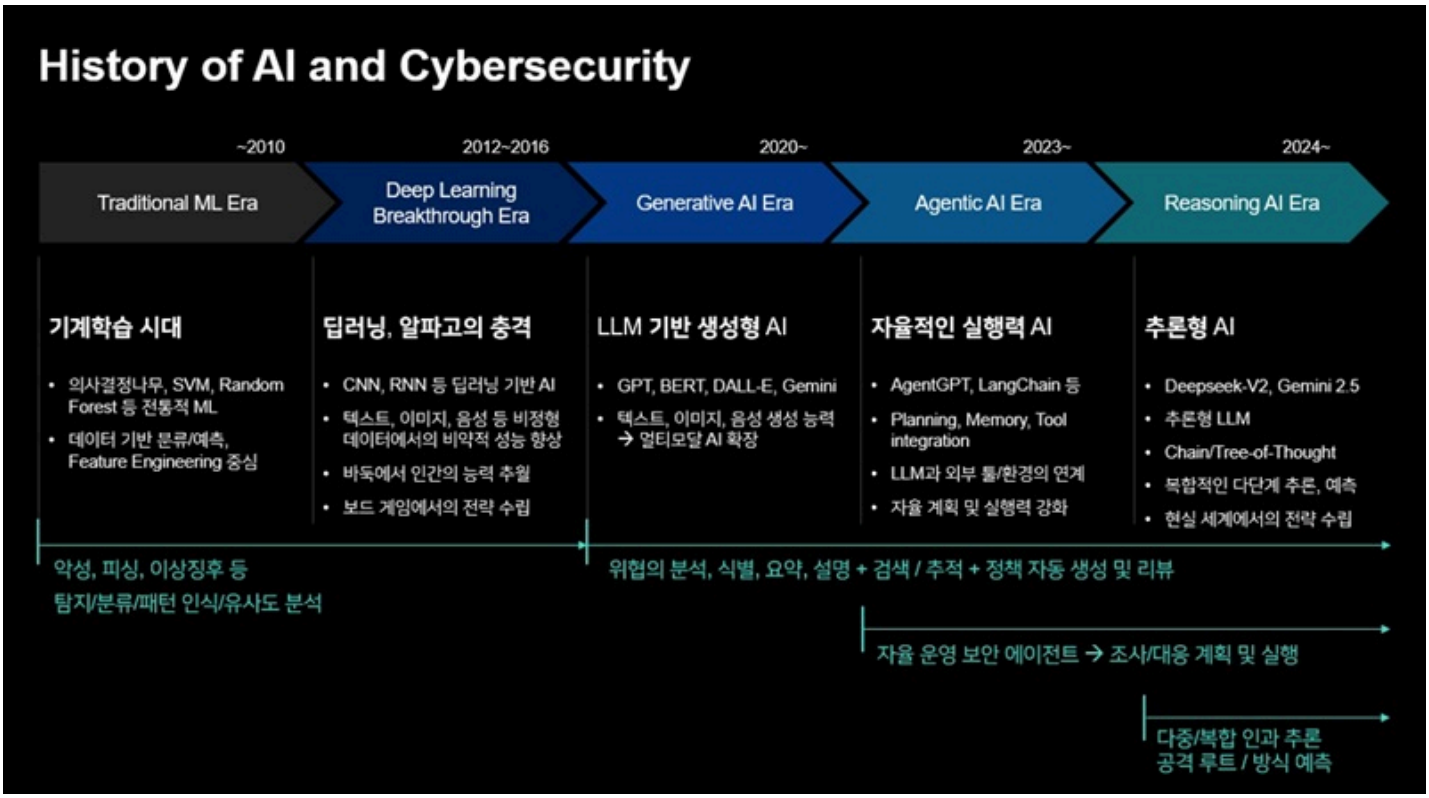
먼저, 자동화는 고정적이고 반복적인 작업 수행을 의미한다. 사람이 정의한 규칙과 흐름대로 작업을 반복 수행하는 개념으로 효율성을 높일 수 있다. 하지만 새롭고 변칙적인 상황에 대한 자체 대응 능력은 없으며, 이런 상황을 인식한 사람이 규칙을 변경한다. 이에 반해, 지능화는 기계가 스스로 상황을 판단해 최적 작업 흐름을 탐색하고 환경 변화에 적응하는 것이다. 따라서 변칙에도 유연하게 대응이 가능하다.

AI 발전사는 곧 지능화의 역사다. 2010년까지는 기계 학습 혹은 머신 러닝(Machine Learning)을 중심으로 학습 능력 확보에 주력했다. 그리고 알파고를 통해 명확한 규칙을 가진 게임에서 상황을 파악하고 적절한 대응 전략을 수립하는 능력에 있어 AI가 인간을 추월했음을 알렸다. 이후 이러한 판단 능력을 불확실성 높은 현실 세계에 적용하기 위한 기술 발전이 시작된다.

그 첫 단계는 언어의 이해였다. 거대 언어 모델(Large Language Model, LLM)으로 대표되는 생성형 AI의 등장과 함께, 언어, 음성, 이미지 등으로 사람과 소통하고 상호작용하는 기반을 만들었다.

그 다음 외부 도구와 연계하며 실행력을 갖추게 됐다. 이를 에이전틱 AI(Agentic AI)라 한다.

더 나아가 바둑에서 다음에 둘 몇 수를 예측하고 대응하는 것과 같이 현실 세계에서도 다단계 추론 능력(추론형 AI)을 활용해 이후 흐름을 예측하고 대응하는 전략 수립 능력을 선보이기 시작했다.



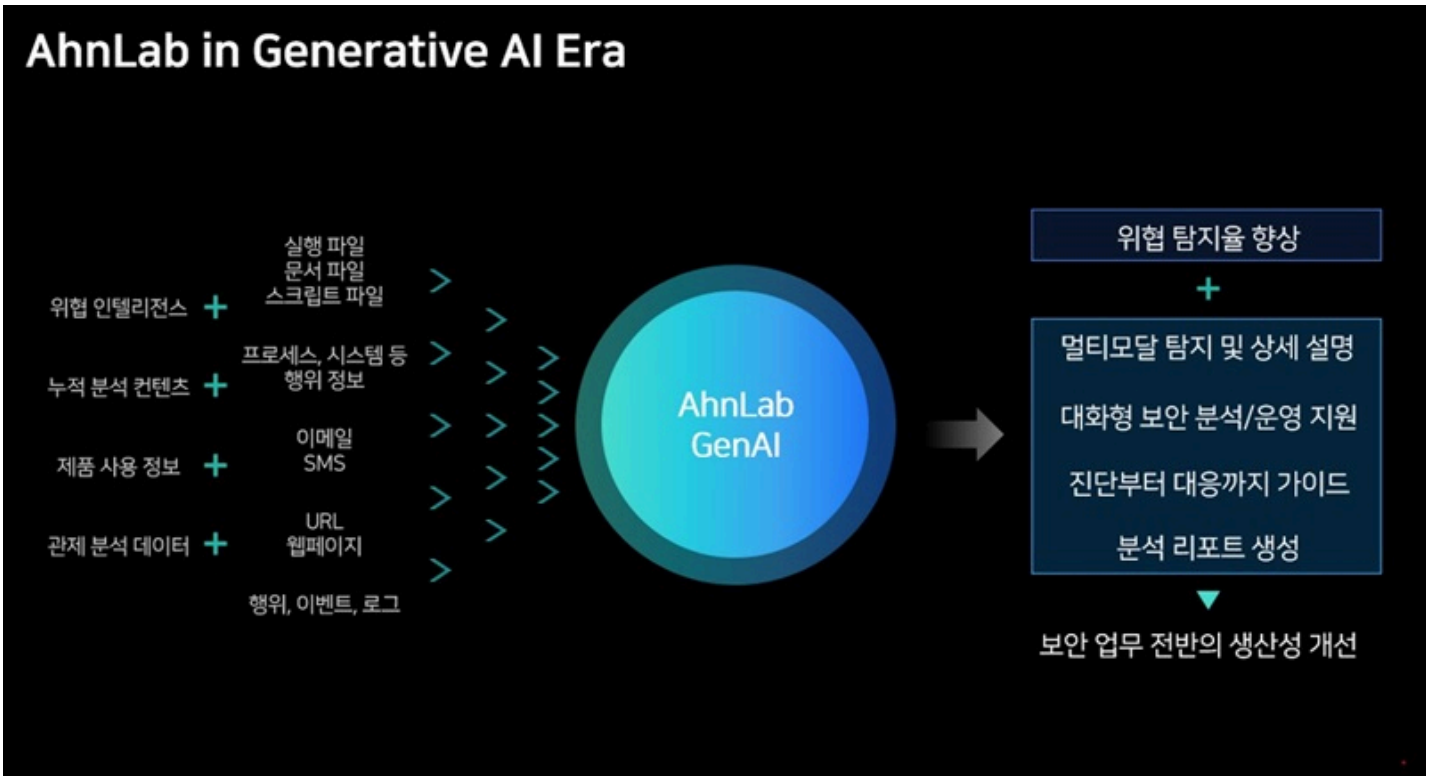
[그림 1] AI와 사이버보안의 발전사

사이버보안에서의 머신 러닝 혹은 AI의 적용 흐름도 AI 발전 흐름과 유사하다. 2010년대까지는 탐지, 분류, 패턴 인식에 중점을 뒀다. 2020년대 들어 위협을 분석, 설명하고 대응 방안을 수립하는 보안 운영 업무를 보조하는 도구로 생성형 AI를 활용하기 시작했다. 그리고 최근에는 실행력을 갖춘 에이전틱 AI 기술을 통해 보안 자율 운영의 방향으로 발전하고 있는 상황이다.

안랩의 AI 혁신, 모든 보안 업무의 생산성 향상

과거 안랩의 AI 기술은 머신 러닝을 통한 위협 탐지 모델 개발에 집중해왔다. 머신 러닝 기술을 활용하여 AhnLab EDR의 악성 행위 탐지, AhnLab MDS의 피싱 이메일 및 URL 탐지 등에 대한 위협 탐지율을 높이는데 주력했다. 탐지 모델별로 개별적인 데이터의 수집, 전처리 및 학습 프로세스를 구축하고, 이러한 프로세스를 통해 개발된 모델들을 제품의 탐지 기능에 활용했다. 다만, 이 방식에는 몇 가지 한계점이 있었다. 다양한 종류의 데이터를 확보하고 교차 활용하는 과정에서 발생하는 시너지 효과의 부재와 AI 활용 영역 확대에 투입되는 비용이 감소하지 않는다는 점 등이었다.

안랩은 이러한 한계를 극복하고자 안랩만이 보유한 위협 인텔리전스와 관제 분석 데이터들을 포함한 각종 데이터를 한 곳에 모으고, 하나의 생성형 AI 모델을 학습시켜 여러 기능을 제공하는 구조로 혁신했다. 안랩만이 보유한 보안 데이터를 포함하기 때문에 일반적인 생성형 AI와 달리 보안에 특화된 AI로 차별화 요소를 갖는다.



[그림 2] 안랩의 생성형 AI 동작 구조

안랩은 AI 적용을 통한 생산성 혁신으로 과거의 위협 탐지 기능뿐만 아니라 ▲컨텍스트 설명을 제공하는 멀티모달 탐지 ▲대화형 분석 및 보안 운영 지원 ▲진단부터 대응까지 종합적인 가이드 제공 ▲분석 리포트 생성 기능까지 보안 업무 전반의 생산성을 개선하는 방향으로 AI의 역할을 확대하고 있다.

AhnLab AI PLUS 출시, 에이전틱 AI로의 혁신

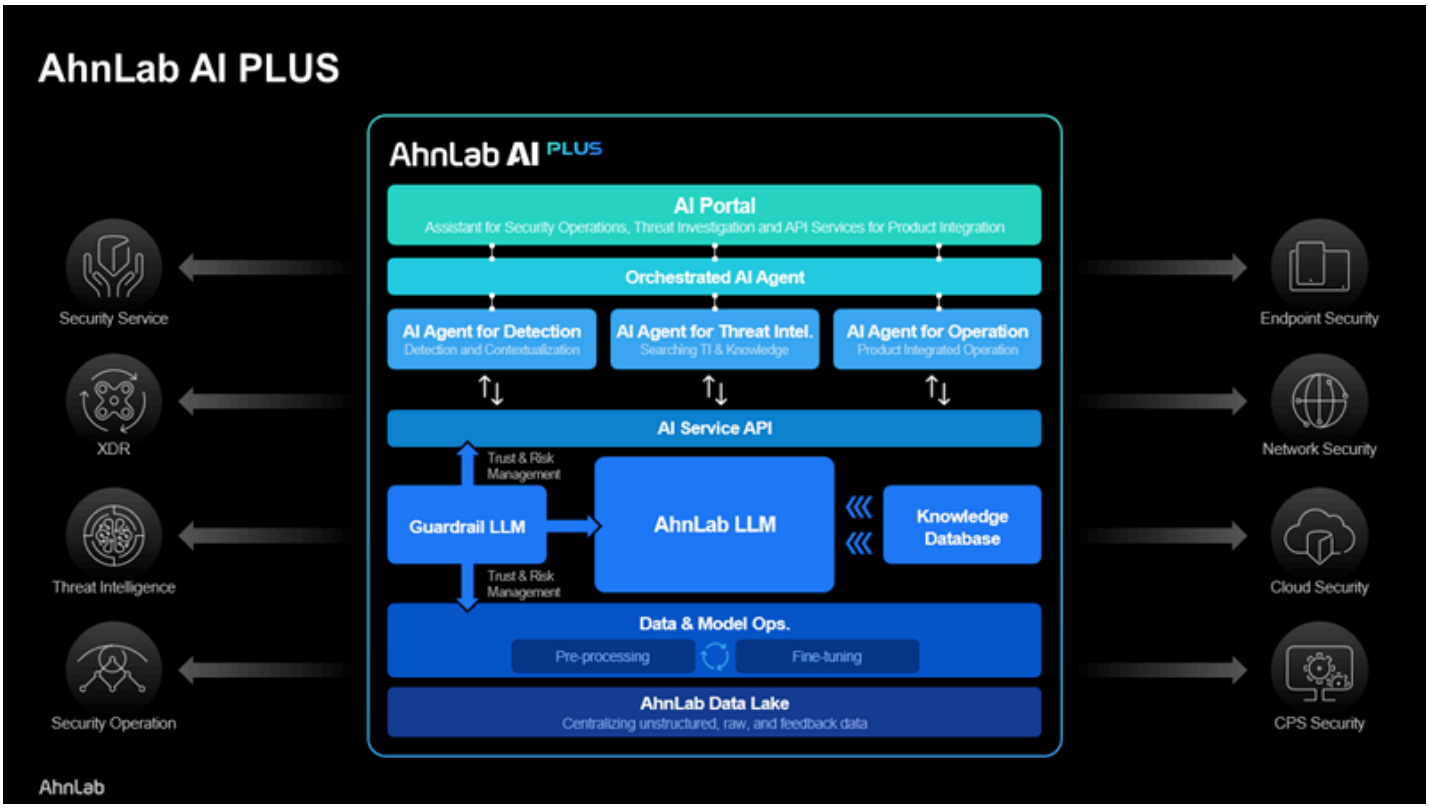
그 일환으로 안랩은 2025년 1분기, 자사의 데이터와 AI 기술을 집대성한 AI 기반 보안 플랫폼 ‘AhnLab AI PLUS’를 출시했다.

AhnLab AI PLUS는 안랩이 30년간 축적한 위협 분석 데이터, 악성코드 및 침해 사고 대응 경험 등 방대한 보안 정보를 기반으로 개발한 자체 AI 플랫폼이다. ▲생성형 AI 및 LLM 기반 지능형 보안 탐지·분석 강화 ▲다양한 제품·서비스 적용으로 AI 기반 운영 확장 ▲자체 수집 데이터 기반 학습 체계로 고도화된 AI 서비스 제공 및 보안성 확보 등으로 자사 제품 및 서비스 전반의 AI 기반 지능화를 이뤄갈 계획이다.

AhnLab AI PLUS의 구조를 살펴보면, 방대한 보안 정보를 내부 데이터레이크(Data Lake)로 중앙화하고 데이터 가공 및 모델 학습 과정을 거쳐 보안 특화 LLM과 지식 데이터베이스를 구축했다. LLM과 지식 검색 기능을 API 서비스로 애플리케이션 계층에 공급한다. 또한, 데이터와 모델의 신뢰성, 리스크 관리, 보안을 고려하여 가드레일(Guardrail)을 적용해 AI로 인해 발생할 수 있는 리스크를 최소화한다.

AI는 어시스턴트(Assistant) 형태로 서비스되며 ▲AI 기반 탐지 & 분석(AI Agent for Detection) ▲위협 인텔리전스 서비스(AI Agent for Threat Intelligence) ▲제품 운영 보조 (AI Agent for Operation)로 역할을 구분하여 제공한다. 그리고 어시스턴트들을 연계하여 통합 보안 운영을 담당하는 Orchestrator AI를 개발 중에 있다.

마지막으로 이 모든 것을 안랩의 AI 포털(AI Portal) 통해 확인할 수 있다.



[그림 3] AhnLab AI PLUS 구조도

고객 입장에서 AhnLab AI PLUS를 처음 접하면, 여러가지 궁금증이 생길 것이라 생각한다. 이에, 가장 기본적인 세 가지 질문에 대한 답변을 다음과 같이 제시한다.

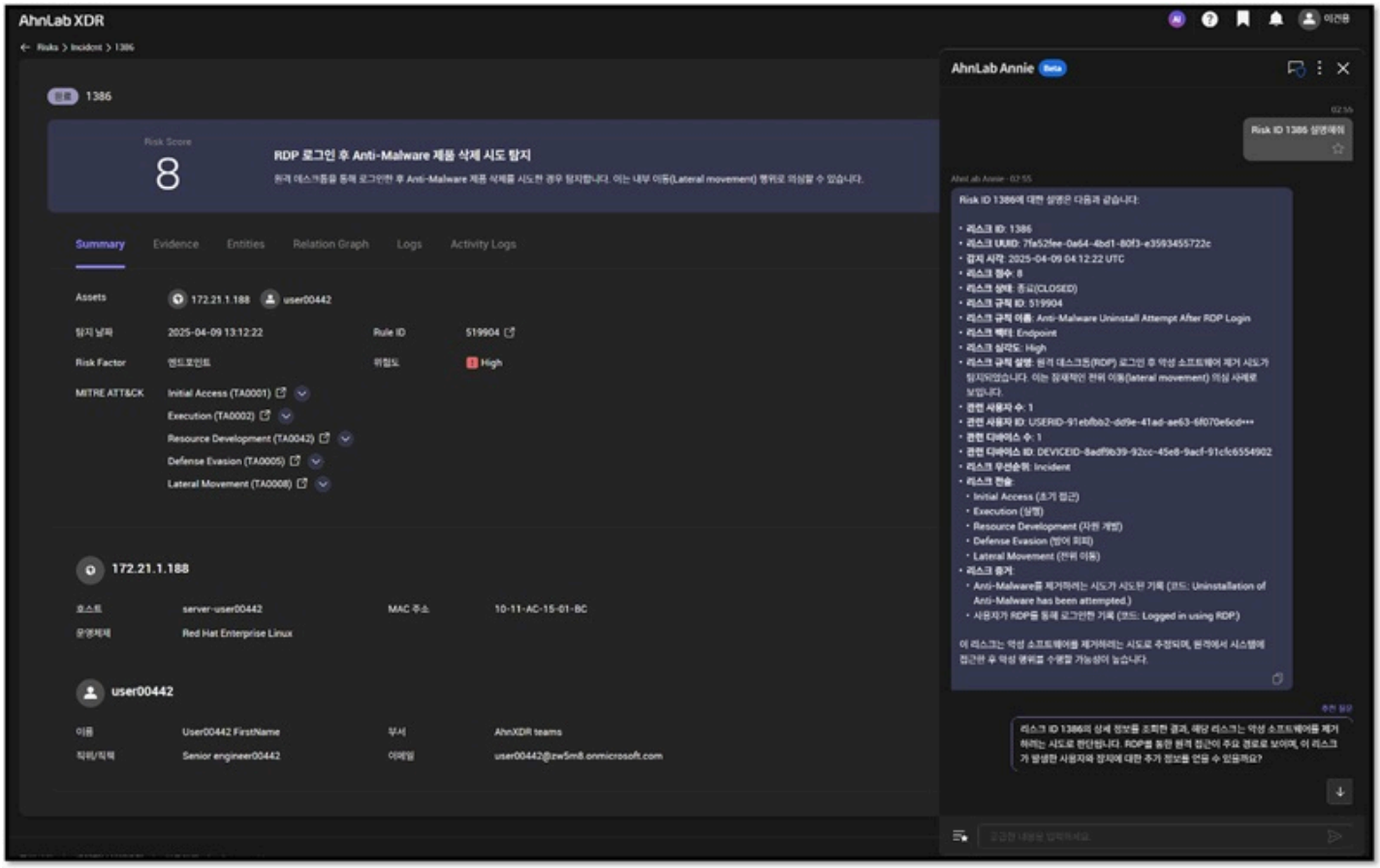
#1. 기존 안랩의 AI와 무엇이 달라진건가?

AhnLab AI PLUS는 생성형 AI와 LLM 기술을 적용해 기존 머신러닝/딥러닝 기반 탐지 기술을 한층 고도화했다. 파일, URL, 행위 정보, 스미싱 문자 등 다양한 형태의 비정형 데이터를 분석하고, 위협 발생 원인과 공격 방식을 심층적으로 파악해 탐지 결과와 대응 가이드를 함께 제공한다.

이로써 보안 담당자는 보안 이벤트를 보다 직관적으로 이해하고, 빠르게 위협 요소를 식별할 수 있다. 또한, 보안 운영의 정확성과 대응 속도가 높아져, 다양한 위협 상황에서도 효율적인 대응이 가능하다.

#2. 보안 솔루션에 어떻게 적용되나?

AhnLab XDR에 AI 보안 어시스턴트 '애니(Annie)'를 연동하며 AhnLab AI PLUS 적용을 시작했다. 제품 UI에서 대화형 AI 보안 어시스턴트를 제공하고, 실시간 위협 탐지, 대응 방안(플레이북) 제시, 추가 질문 추천 등 보안 운영을 지원하는 다양한 기능이 탑재됐다. 이를 통해, 고객은 복잡한 위협 환경에서도 보안 현황을 쉽게 파악하고, 보다 신속하고 체계적인 대응 체계를 구축할 수 있다.



[그림 4] AhnLab XDR에 적용된 AI 보안 어시스턴트

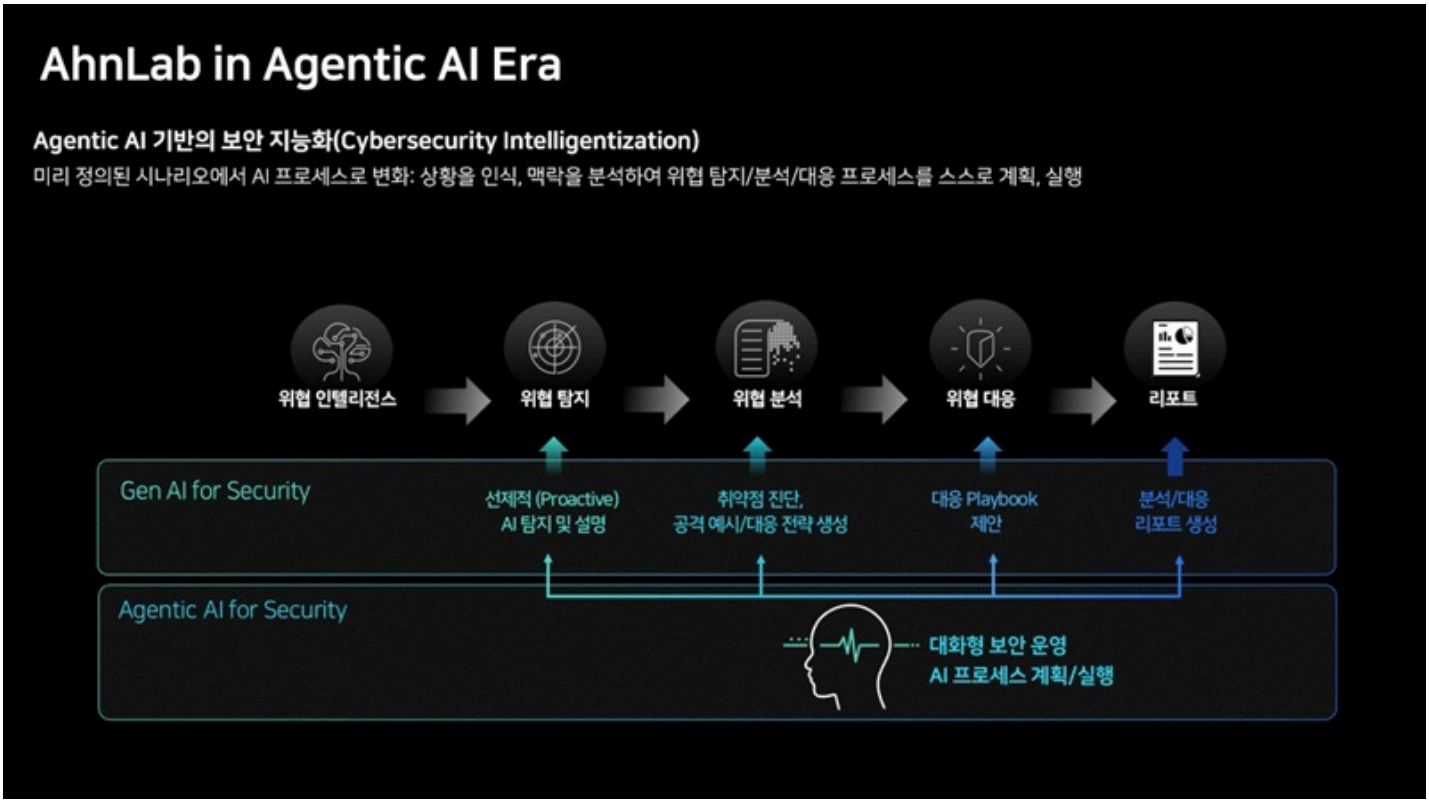
AhnLab AI PLUS는 AhnLab XDR 뿐만 아니라 안랩의 다양한 제품과 서비스에 적용할 수 있도록 설계됐으며, 앞으로 다양한 제품과 서비스로 AI 적용을 확대해 나갈 예정이다.

#3. 모델 학습에 데이터 유출 등 보안 우려는 없나?

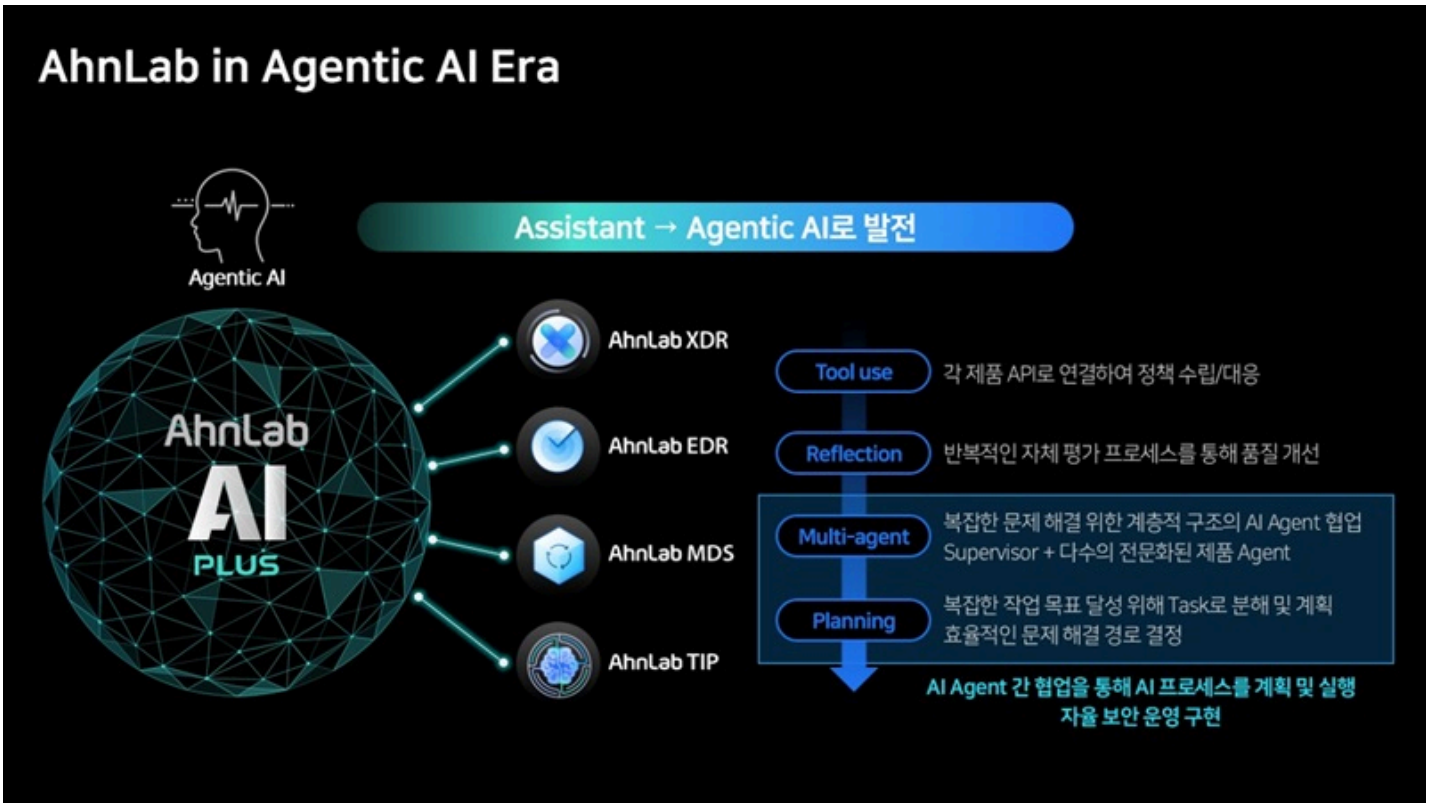
AhnLab AI PLUS는 고객 데이터를 수집하거나 활용하지 않고도, 안랩의 악성코드 분석, 침해 사고 대응 노하우와 AhnLab TIP 및 AhnLab Smart Defense(ASD) 인프라를 통해 수집한 파일, URL, IP, 행위 정보 등의 빅데이터와 보안 인텔리전스를 활용해 학습을 수행하고 AI 서비스의 품질을 높이고 있다. 고객은 보유하고 있는 데이터의 외부 유출 우려 없이, 안랩이 축적한 방대한 위협 인텔리전스를 기반으로 한 높은 수준의 AI 서비스를 제공받을 수 있다.

Next Step, 이제는 보안 지능화

안랩은 AI 고도화를 거듭해 보안 지능화의 완성도를 높이는 것을 목표로 삼고 있다. 사전 정의된 시나리오대로 탐지, 분석 및 대응하는 것을 넘어, AI가 맥락을 파악하고 프로세스를 스스로 계획해 실행하는 개념이다. 보안 업무 전반에 제공하는 여러 생성형 AI 기능들을 통합해 맥락에 맞는 적절한 실행 흐름을 AI가 스스로 설계하고 실행하는 것이 궁극적인 보안 지능화의 모습이다.



[그림 5] 안랩의 생성형 AI 및 에이전틱 AI 기술 활용



[그림 6] 안랩의 Agentic AI 개념도

이를 위해, 앞서 언급한 ▲AI 기반 탐지 & 분석 ▲위협 인텔리전스 서비스 ▲ 제품 운영 보조, 세 가지 역할을 수행하는 AI 에이전트(AI Agent)를 개발 중이다. 지향점은 하나의 통합 에이전트가 계획을 수립하고, 여러 AI 에이전트들과 유기적으로 협업하며 일련의 작업을 수행하는 자율적인 보안 운영 시스템을 구현하는 것이다. AI 에이전트 기반의 보안 운영 시스템의 완성도가 높아지면, 사람을 위한 AI의 지원이 최적화되어 고객의 보안 수준과 비즈니스 생산성 향상으로 이어질 전망이다.

AhnLab

이승경 인공지능개발실장