AI 공격에는 왜 AI 보안이 필요한가

공격자가 AI를 활용하는 시대, 방어도 AI의 속도를 갖춰야 한다

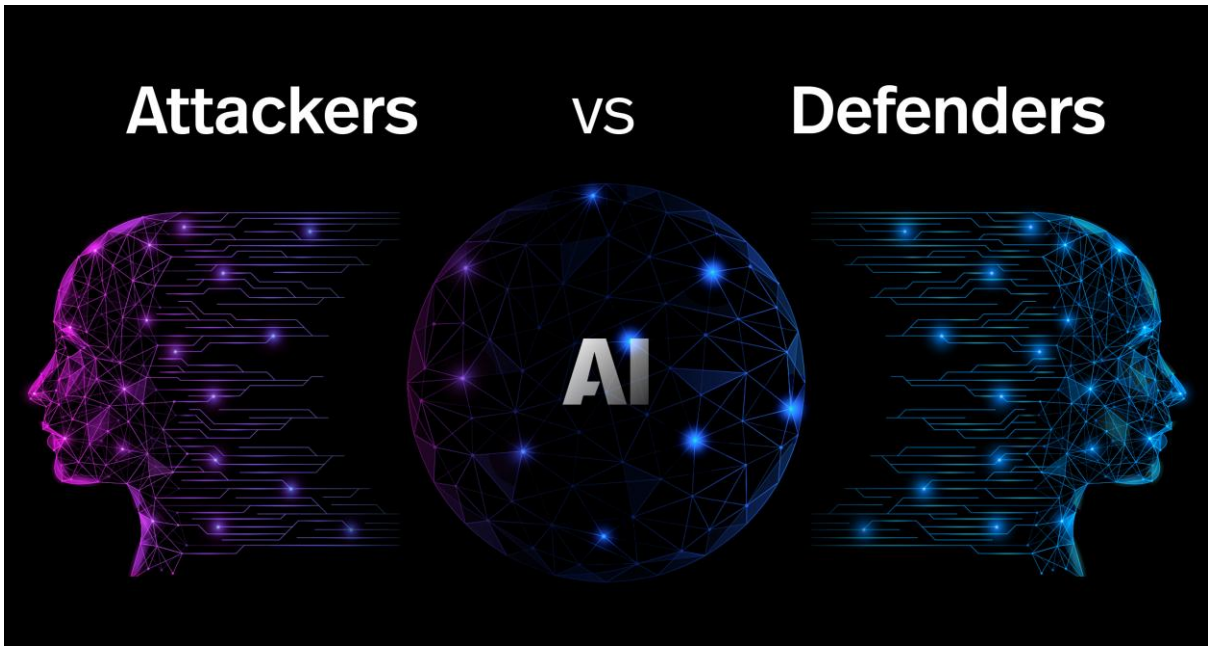
최근 클로드 미토스 (Claude Mythos)와 같은 차세대 AI가 취약점 탐색과 공격 시나리오 생성 등 사이버 공격에 활용될 가능성이 주목받으면서, AI가 공격 방식을 어떻게 변화시킬지에 대한 관심이 커지고 있다.

생성형 AI의 등장은 업무 방식에 큰 변화를 가져왔고, 이제는 스스로 계획을 세우고 작업을 수행하는 에이전틱 AI(Agentic AI) 시대로 빠르게 전환되고 있다. 이러한 변화는 기업의 생산성뿐 아니라 사이버 공격과 보안 운영 방식에도 큰 영향을 미치고 있다.

과거 사이버 공격은 공격자가 직접 취약점을 찾고 공격 코드를 작성해 단계별로 수행하는 방식이 일반적이었다. 하지만 AI의 발전으로 공격 준비와 실행 과정이 자동화되면서 공격은 더 빠르고, 더 많은 대상을 향해, 더 반복적으로 이루어질 수 있는 환경으로 변화하고 있다.

이는 방어 측에도 새로운 과제를 던진다. AI 기반 공격을 기존의 사람 중심 보안 운영만으로 대응하기에는 속도와 규모 측면에서 한계가 있기 때문이다. 이제 기업은 AI를 단순히 보호하거나 통제해야 할 대상으로만 볼 것이 아니라, 보안 운영 역량을 높이는 핵심 기술로 활용해야 한다.

결국 AI 시대의 보안 경쟁력은 새로운 위협을 얼마나 빠르게 탐지하고 분석하며 대응할 수 있는가에 달려 있다.



AI 기반 공격은 무엇이 달라졌는가

AI 기반 사이버 공격(AI-powered Cyber Attack)이란?

AI 기반 사이버 공격은 인공지능을 활용해 취약점 탐색, 공격 시나리오 생성, 피싱, 악성 코드 작성, 공격 실행 등 사이버 공격 과정을 자동화하는 공격 방식이다. AI가 새로운 공격 기법을 만드는 것이 아니라, 기존 공격을 더 빠르고 반복적으로 수행할 수 있도록 한다는 점이 가장 큰 특징이다.

생성형 AI에서 Agentic AI로

생성형 AI는 질문에 답하거나 텍스트, 코드, 이미지를 생성하는 역할을 한다. 반면 Agentic AI는 주어진 목표를 바탕으로 스스로 계획을 세우고, 필요한 도구를 활용해 여러 단계의 작업을 수행할 수 있다. 예를 들어 보안 운영에서는 단순히 로그를 요약하는 수준을 넘어, 관련 정보를 수집하고 위협을 분석한 뒤 대응 방안을 제안하는 일련의 과정을 하나의 흐름으로 수행할 수 있다. 즉, AI는 '답을 생성하는 도구'에서 '업무를 수행하는 주체'로 진화하고 있다. 이러한 변화는 사이버 공격에도 그대로 적용되고 있다.

AI 공격의 핵심은 자동화와 속도

AI가 등장했다고 해서 사이버 공격의 기본 원리가 바뀐 것은 아니다. 취약점 악용, 악성 코드 실행, 계정 탈취, 권한 상승, 내부 확산과 같은 공격 방식은 여전히 기존 공격 기법의 연장선에 있다. 달라진 것은 공격을 수행하는 방식이다. AI는 방대한 정보를 빠르게 분석하고, 반복적인 작업을 자동으로 수행하며, 실행 결과를 바탕으로 다음 행동을 결정할 수 있다. 공격자는 이를 활용해 취약점을 더 빠르게 찾고, 다양한 공격 시나리오를 생성하며, 동일한 공격을 대규모로 반복 실행할 수 있다.

결국 AI 기반 공격의 본질은 새로운 공격 기법이 아니라 기존 공격의 자동화와 고속화라고 할 수 있다.

AI는 공격을 어떻게 고도화하는가

AI는 공격의 효율성과 규모를 크게 높일 수 있다. 대표적인 변화는 다음과 같다.

① 취약점 탐색과 공격 준비의 자동화

AI는 공개된 취약점 정보와 기술 문서를 분석해 공격에 활용할 수 있는 정보를 빠르게 정리한다. 공격 준비에 필요한 시간이 줄어들면서 새로운 취약점이 공개된 이후 실제 공격으로 이어지는 시간도 짧아질 수 있다.

② 대규모 공격의 반복 실행

AI는 휴식 없이 동일한 작업을 반복할 수 있다. 다양한 공격 전략을 동시에 시도하고, 실패한 결과를 바탕으로 새로운 방법을 적용해 공격을 지속적으로 수행할 수 있다.

③ 맞춤형 공격의 고도화

AI는 공개된 정보를 활용해 특정 조직이나 사용자를 겨냥한 피싱 메시지를 생성하거나, 상황에 맞는 공격 시나리오를 구성하는 데 활용될 수 있다. 향후에는 공격 대상의 반응에 따라 대화를 이어가는 형태로 발전할 가능성도 있다.

AI는 새로운 공격 표면이 되기도 한다

AI는 공격을 자동화하는 도구인 동시에 새로운 공격 대상이 되기도 한다.

기업이 AI 에이전트를 업무에 활용하기 시작하면, AI가 어떤 시스템에 접근하고 어떤 권한을 가지며 어떤 작업을 수행하는지가 새로운 보안 관리 대상이 된다. 예를 들어 공격자는 AI에게 잘못된 명령을 입력해 의도하지 않은 행동을 유도하거나, AI 에이전트의 권한을 탈취해 정상 사용자처럼 시스템에 접근할 수 있다.

따라서 앞으로는 AI를 활용하는 것뿐 아니라, AI 자체를 안전하게 운영하기 위한 보안 체계도 함께 갖춰야 한다.

왜 AI 공격에는 AI 보안이 필요한가

AI 보안(AI Security)이란?

AI 보안은 AI 모델, 학습 데이터, 입력값과 출력값, AI가 연결된 시스템을 공격과 오남용으로부터 보호하는 보안 체계를 의미한다. 기존 보안이 네트워크, 단말, 서버, 사용자 계정 보호에 초점을 맞췄다면, AI 보안은 여기에 모델과 데이터, AI의 의사결정 과정까지 포함한다는 점이 특징이다.

사람 중심 보안 운영의 한계

기존 보안 운영은 사람이 보안 이벤트를 확인하고, 위협 여부를 분석한 뒤 대응하는 방식으로 이루어져 왔다.

하지만 AI 기반 공격으로 공격 속도와 규모가 커질수록 사람이 처리해야 하는 보안 이벤트도 함께 증가한다.

보안 담당자는 수많은 로그를 확인하고, 여러 보안 시스템에서 정보를 수집하며, 공격 여부를 판단하고 대응 우선순위를 결정해야 한다. 이러한 과정은 높은 전문성을 요구하지만 동시에 많은 시간과 노력이 필요하다.

공격은 AI를 통해 자동화되는데, 방어가 사람의 속도에 머문다면 공격과 방어 사이의 격차는 점점 커질 수밖에 없다.

AI 보안은 새로운 운영 방식이다

AI 보안은 기존 보안 제품에 생성형 AI 기능을 추가하는 것을 의미하지 않는다. 핵심은 AI를 활용해 보안 운영 전반의 속도와 효율성을 높이는 것이다. AI는 방대한 보안 데이터

를 분석하고, 위협 인텔리전스와 연계해 공격의 맥락을 파악하며, 대응 우선순위를 제시할 수 있다. 반복적인 분석과 조사 업무를 AI가 지원하면 보안 전문가는 더 중요한 판단과 전략 수립에 집중할 수 있다.

이처럼 AI 보안은 개별 기능이 아니라 보안 운영 체계 자체를 변화시키는 기술이다.

탐지에서 AI 기반 보안 운영으로

앞으로의 보안은 알려진 위협을 탐지하는 수준을 넘어, 새로운 위협을 얼마나 빠르게 식별하고 대응할 수 있는지가 더욱 중요해질 것이다. 이를 위해서는 엔드포인트, 네트워크, 클라우드, CPS 등 다양한 영역의 데이터를 통합하고, AI가 이를 분석해 공격의 흐름과 영향 범위를 빠르게 파악할 수 있어야 한다. 또한 AI가 제시한 분석 결과와 대응 방안을 보안 전문가가 검증하고 최종 의사결정을 내리는 구조가 함께 마련되어야 한다.

결국 AI 시대의 보안은 사람과 AI가 각자의 강점을 결합해 운영 효율성과 대응 속도를 높이는 방향으로 발전하고 있다. 공격자가 AI를 활용하는 시대에는 방어 역시 AI를 활용해야 한다. AI 보안은 더 이상 선택적인 기능이 아니라, 새로운 보안 운영 방식으로 자리잡고 있다.

AI 보안 운영은 어떻게 달라지는가

AI 기반 보안 운영은 단순히 분석 속도를 높이는 것이 아니다. 보안 운영 방식 자체를 사람 중심에서 AI와 전문가가 협업하는 구조로 변화시키는 데 의미가 있다.

AI SOC (AI Security Operations Center)이란?

AI SOC는 AI를 활용해 탐지, 분석, 조사, 대응 등 보안 운영 전반을 지원하는 차세대 보안 운영 체계다.

반복적인 분석 업무는 AI가 수행하고, 보안 전문가는 최종 판단과 의사결정을 담당하는 Human-in-the-Loop 구조를 지향한다.

Agentic AI는 보안 운영을 어떻게 바꾸는가

기존 AI는 보안 담당자의 질문에 답하거나 로그를 요약하는 등 분석을 지원하는 역할에 머물렀다.

반면 Agentic AI는 하나의 목표를 수행하기 위해 필요한 작업을 스스로 계획하고 실행할 수 있다. 보안 운영에서는 위협을 탐지하고 관련 정보를 수집·분석한 뒤 대응 방안을 제시하는 일련의 과정을 하나의 흐름으로 수행하는 형태로 발전하고 있다. 예를 들어 새로운 보안 이벤트가 발생하면 AI는 관련 로그와 위협 정보를 수집하고, 공격 흐름과 영향 범위를 분석한 뒤 대응 우선순위를 제안할 수 있다. 보안 담당자는 AI가 제공한 분석 결

과를 검토한 뒤 최종 대응 여부를 결정한다. 이처럼 AI는 반복적인 운영 업무를 지원하고, 보안 전문가는 판단과 의사결정에 집중하는 방향으로 역할이 변화하고 있다.

에이전틱 AI(Agentic AI)이란?

Agentic AI는 사용자의 지시에 따라 답변을 생성하는 것을 넘어, 목표를 달성하기 위해 스스로 계획을 세우고 여러 도구를 활용해 작업을 수행하는 AI를 의미한다. 보안 분야에서는 탐지, 분석, 조사, 대응 등 여러 업무를 하나의 흐름으로 수행하는 AI 기술로 발전하고 있다.

여러 AI 에이전트가 함께 보안을 운영한다

앞으로의 보안 운영은 하나의 AI가 모든 업무를 수행하기보다, 서로 다른 역할을 담당하는 여러 AI 에이전트가 협업하는 구조로 발전할 것으로 예상된다. 예를 들어 한 에이전트는 보안 이벤트를 분석하고, 다른 에이전트는 위협 인텔리전스를 확인하며, 또 다른 에이전트는 대응 방안을 제안하는 방식이다. 각 AI 에이전트의 결과는 하나의 운영 흐름으로 연결되어 보다 빠르고 일관된 보안 대응을 지원한다.

이러한 구조는 사람의 업무를 대체하기 위한 것이 아니라, 반복적인 업무를 AI가 수행함으로써 보안 전문가가 더 중요한 판단과 전략 수립에 집중할 수 있도록 하기 위한 것이다.

[그림] 한눈에 보는 AI 공격과 AI 보안: 공격이 AI의 속도로 진화한다면, 방어도 AI의 속도를 갖춰야 한다.

AI와 전문가의 협업이 핵심이다

AI가 빠르게 발전하고 있지만, 보안 운영의 최종 책임은 여전히 사람에게 있다.

실제 보안 대응은 기술적인 위험뿐 아니라 업무 영향도, 시스템 중요도, 규제와 컴플라이

언스 등 다양한 요소를 함께 고려해야 한다. 이러한 판단은 AI만으로 수행하기 어렵다.

따라서 앞으로의 AI 보안은 AI가 분석과 대응을 지원하고, 보안 전문가가 이를 검증해 최종 의사결정을 내리는 Human-in-the-Loop 구조가 핵심이 될 것이다.

AI의 역할은 사람을 대신하는 것이 아니라, 사람이 더 빠르고 정확하게 판단할 수 있도록 지원하는 것이다.

안랩은 AI 공격 시대를 어떻게 준비하고 있는가

안랩은 AI를 기존 제품에 추가되는 하나의 기능이 아니라, 보안 운영 전반을 연결하고 고도화하는 핵심 기술로 보고 있다. 이를 위해 자체 AI 플랫폼인 AhnLab AI PLUS를 중심으로 AI 기반 보안 운영 체계를 발전시키고 있다.

AhnLab AI PLUS, 보안 운영을 위한 AI 플랫폼

AhnLab AI PLUS는 하나의 독립적인 보안 제품이 아니다. 안랩이 보유한 엔드포인트, 네트워크, 클라우드, CPS 등 다양한 보안 제품과 서비스를 AI로 연결하고, 보안 운영 전반을 지능화하기 위한 공통 AI 플랫폼이다.

안랩은 30년 이상 축적해 온 악성코드 분석 정보, 위협 인텔리전스, 침해사고 대응 경험을 AI가 활용할 수 있도록 체계화하고 있다. 이를 기반으로 AI는 보안 이벤트를 분석하고, 위협의 맥락을 이해하며, 대응 방안을 제안하는 역할을 한다. 즉, AhnLab AI PLUS의 핵심은 최신 AI 모델을 도입하는 것만이 아니라 안랩이 축적한 보안 데이터를 AI가 효과적으로 활용할 수 있도록 만드는 것이다.

AI가 보안 운영을 지원하는 방식

AhnLab AI PLUS에서는 하나의 AI가 모든 업무를 수행하지 않는다.

보안 이벤트 분석, 위협 인텔리전스 활용, 대응 지원 등 서로 다른 역할을 담당하는 AI가 협업해 하나의 보안 운영 흐름을 구성한다.

예를 들어 새로운 보안 이벤트가 발생하면 AI는 다음과 같은 과정을 지원할 수 있다.

- 이벤트와 로그 분석
- 관련 위협 인텔리전스 확인
- 공격 흐름과 영향 범위 분석
- 위험도 평가
- 대응 우선순위와 대응 방안 제안

이러한 분석 결과를 바탕으로 보안 전문가는 보다 빠르게 대응할지 여부를 결정할 수 있다.

AhnLab AI PLUS는 제품 전반으로 확장되고 있다

AhnLab AI PLUS는 하나의 제품에만 적용되는 AI가 아니라, 안랩의 다양한 보안 제품과 서비스에 AI 기능을 연결하는 공통 AI 플랫폼이다.

현재는 AI 기반 보안 운영을 위해 여러 제품에서 AI 기능을 확대하고 있으며, 대표적인 사례로 AhnLab XDR의 AI 보안 어시스턴트 'Annie'와 AhnLab EDR의 'AI Insight'를 들 수 있다.

Annie는 보안 담당자가 자연어로 위협 정보를 질의하고, 관련 이벤트와 분석 정보를 빠르게 확인할 수 있도록 지원하는 대화형 AI 보안 어시스턴트다. 반복적인 정보 검색과 분석 시간을 줄여 보안 담당자가 위협 분석과 대응에 더욱 집중할 수 있도록 돕는다.

AI Insight는 AhnLab EDR에서 탐지된 이벤트를 AI가 종합적으로 분석해 공격 의도와 위협 맥락, MITRE ATT&CK 기반 TTP, 위협 인텔리전스, 대응 방향 등을 하나의 분석 보고서 형태로 제공하는 AI 기반 분석 기능이다. 이를 통해 보안 담당자는 복잡한 이벤트의 의미를 빠르게 이해하고, 보다 효율적으로 대응 우선순위를 판단할 수 있다.

이처럼 안랩은 AI 기능을 특정 제품에 한정하지 않고, AhnLab AI PLUS를 중심으로 다양한 보안 제품과 서비스에 지속적으로 확대 적용하며 AI 기반 보안 운영 체계를 발전시켜 나가고 있다.

안랩 AI 경쟁력의 핵심은 보안 도메인 전문성이다

AI 보안의 성능은 AI 모델 자체만으로 결정되는 것이 아니다. 실제 보안 환경을 얼마나 깊이 이해하고 있는지, 즉 도메인 특화 데이터(Domain-specific Data)와 운영 경험이 AI의 정확성과 활용도를 좌우한다.

안랩은 30년 이상 축적한 보안 전문성과 위협 분석 경험을 바탕으로, 보안 도메인에 특화된 AI(Domain-specific AI)를 발전시키고 있다. AI가 실제 보안 위협의 맥락(Context)을 이해하고 보다 정확한 탐지·분석·대응을 수행할 수 있도록 하는 것이 안랩 AI 전략의 핵심이다. 이러한 AI 경쟁력은 다음의 4가지 기반 위에서 구축된다.

① 보안 도메인 전문성: 안랩은 30년 이상 축적한 악성코드 분석 정보와 침해사고 대응 경험, 보안 운영 노하우를 AI 학습과 분석의 기반으로 활용하고 있다. 이를 통해 AI가 단순히 데이터를 분석하는 수준을 넘어, 실제 보안 환경의 맥락을 이해하고 보다 정교한 판단을 내릴 수 있도록 지원한다.

특화 도메인 AI(Domain-specific AI)와 보안 도메인 전문성이란?

특화 도메인 AI(Domain-specific AI)는 특정 산업이나 업무 분야에 필요한 데이터와 전문 지식을 기반으로 학습하거나 최적화된 AI를 의미한다. 이러한 AI는 해당 분야의 전문 용어와 업무 규칙, 데이터 구조, 운영 맥락(Context)을 이해해 범용 AI보다 더 정확하고 실질적인 결과를 제공할 수 있다.

보안 도메인 전문성(Security Domain Expertise)은 악성코드 분석, 위협 인텔리전스, 침해사고 대응, 보안 운영 경험 등 사이버 보안 분야에서 축적된 전문 지식과 데이터를 의미한다. 안랩은 이러한 보안 도메인 전문성을 AI에 결합해 실제 위협의 맥락을 이해하고, 보다 정확한 탐지·분석·대응을 지원하는 AI 플랫폼을 발전시키고 있다.

② **위협 인텔리전스:** 안랩이 지속적으로 축적해 온 위협 인텔리전스는 AI가 공격 기법과 위협 행위, 위험도를 보다 정확하게 분석하고 대응 우선순위를 판단할 수 있도록 지원하는 핵심 자산이다.

③ **통합 보안 플랫폼:** 엔드포인트, 네트워크, 클라우드, CPS 등 다양한 보안 영역의 데이터를 하나의 운영 흐름으로 연결함으로써, AI가 개별 이벤트가 아닌 공격의 전체 흐름과 영향 범위를 분석할 수 있는 환경을 제공한다.

④ **신뢰할 수 있는 AI 운영:** AI의 활용 범위가 넓어질수록 정확성과 신뢰성은 더욱 중요해진다. 안랩은 AI의 자율성을 높이는 동시에 가드레일과 전문가 검증 체계를 적용해 신뢰할 수 있는 AI 기반 보안 운영 환경을 구축하는 데 중점을 두고 있다.

결국 안랩 AI 경쟁력의 핵심은 최신 AI 모델을 적용하는 데 있지 않다. 보안 도메인 전문성과 위협 인텔리전스, 통합 보안 플랫폼, 그리고 신뢰할 수 있는 AI 운영 체계를 결합해 AI가 실제 보안 환경을 이해하고 활용할 수 있도록 만든 것이 안랩의 차별화된 경쟁력이다.

AI 시대, 새로운 보안 경쟁력이 만들어지고 있다

AI는 사이버 공격의 속도와 규모를 빠르게 변화시키고 있다. 앞으로의 공격은 더욱 자동화되고 지능화될 것이며, 이에 따라 보안 운영 역시 새로운 방식으로 진화할 수밖에 없다.

이제 기업은 AI를 단순히 보호하거나 통제해야 할 대상으로만 바라볼 것이 아니라, 보안 운영 역량을 높이는 핵심 기술로 활용해야 한다. 공격자가 AI를 활용하는 시대에는 방어 역시 AI를 활용해 탐지·분석·대응 속도를 높여야 한다.

물론 AI가 보안 전문가를 대체하는 것은 아니다. AI는 방대한 데이터를 빠르게 분석하고 반복적인 업무를 지원하는 데 강점이 있으며, 최종 판단과 의사결정은 여전히 보안 전문가의 역할이다. 앞으로의 보안 운영은 AI와 사람이 각자의 강점을 결합하는 휴먼인더루프(Human-in-the-Loop) 방식으로 발전할 가능성이 높다.

안랩은 이러한 변화에 맞춰 AI를 개별 기능이 아닌 보안 운영 전반을 연결하는 플랫폼 기술로 발전시키고 있다. AhnLab AI PLUS를 중심으로 보안 도메인 전문성과 위협 인텔리전스, 통합 보안 플랫폼을 결합해 AI가 실제 보안 운영에서 실질적인 가치를 제공할 수 있도록 연구개발을 이어가고 있다.

결국 AI 시대의 보안 경쟁력은 AI를 얼마나 안전하게 관리하는지와 AI를 얼마나 효과적으로 활용하는가를 함께 고민하는 데 있다. 안랩은 AI와 보안 전문성이 결합된 Agentic AI 기반 보안 운영 환경을 통해 기업이 더 빠르고 정확하게 위협에 대응할 수 있도록 AI 보안 역량을 지속적으로 발전시켜 나갈 것이다.

AhnLab의 AI 기반 보안을 직접 확인해 보세요

AI 공격 시대에는 AI 기반 보안이 어떻게 작동하는지 이해하는 것도 중요합니다. 데모 영상을 통해 AhnLab AI PLUS와 다양한 AI 기반 보안 기능을 직접 확인해 보세요.

[Demo] AhnLab AI PLUS - AI 에이전트가 수행하는 이벤트 및 영향도 분석

[Demo] AhnLab XDR – 실제 공격 시나리오 탐지 & 대응

[Demo] AhnLab TIP – AI를 활용한 Lazarus 공격 그룹 분석

FAQ: AI 공격과 AI 보안에 대한 주요 질문

Q1. 기존 사이버 공격과 AI 공격의 차이는 무엇인가?

가장 큰 차이는 자동화와 속도이다. 기존 공격은 공격자가 각 단계를 직접 수행해야 했지만, AI 기반 공격은 여러 작업을 자동화하고 반복적으로 수행할 수 있다. 이에 따라 동일한 시간 안에 더 많은 시스템과 취약점을 대상으로 공격을 시도할 수 있다.

Q2. 생성형 AI와 Agentic AI의 차이는 무엇인가?

생성형 AI는 사용자의 질문이나 지시에 따라 텍스트, 코드, 이미지 등의 결과물을 생성한다. Agentic AI는 사용자가 목표를 제시하면 필요한 작업을 계획하고 외부 도구를 활용해 여러 단계의 업무를 수행한다.

즉, 생성형 AI가 답을 만드는 AI라면 Agentic AI는 목표를 달성하기 위해 행동하는 AI라고 할 수 있다.

Q3. AI 공격은 기존 보안 제품으로 막을 수 없나요?

기존 보안 기술은 여전히 중요하다.

AI 공격 역시 취약점 악용, 악성코드 실행, 계정 탈취와 같은 기존 공격 행위를 기반으로 하기 때문이다. 다만 공격의 속도와 규모가 커지면 개별 보안 제품의 탐지 기능만으로는

충분하지 않을 수 있다. 여러 보안 영역의 데이터를 통합하고, AI를 활용해 위협을 빠르게 분석·대응하는 운영 체계도 함께 필요하다.

Q4. AI 보안이란 무엇인가?

AI 보안은 인공지능을 활용해 보안 데이터와 위협을 분석하고, 탐지·조사·대응 과정을 자동화하거나 지원하는 보안 체계를 의미한다. 대량의 이벤트 분석, 위협 간 상관관계 파악, 이상 행위 탐지, 대응 우선순위 결정과 보고서 작성 등에 활용할 수 있다.

Q5. AI 공격에는 반드시 AI로 대응해야 하나?

AI만으로 모든 공격을 방어할 수 있는 것은 아니다. 기존 보안 기술과 보안 전문가의 판단도 반드시 필요하다.

그러나 공격자가 AI를 활용해 공격 속도와 규모를 높이는 환경에서는 방어 측도 AI를 활용해 탐지·분석·대응 시간을 줄여야 한다. AI 보안은 기존 보안과 전문가를 대체하는 기술이 아니라, 기존 보안 체계와 전문가의 역량을 강화하는 수단이다.

Q6. Agentic SOC란 무엇인가?

Agentic SOC는 탐지, 위협 인텔리전스, 포렌식, 대응 및 보고 등 서로 다른 역할을 담당하는 AI 에이전트들이 협업해 보안 운영을 수행하는 구조이다. 각 에이전트의 업무를 오케스트레이션 에이전트가 조율함으로써 보안 담당자가 수작업으로 처리하던 업무를 줄이고 분석과 대응 속도를 높일 수 있다.

Q7. AI가 보안 전문가를 대체하게 되나?

AI가 보안 전문가를 완전히 대체하기는 어렵다.

AI는 반복적인 분석과 운영 업무를 빠르게 수행할 수 있지만, 사업 영향도, 시스템 중요도, 규제와 조직 상황을 고려한 최종 판단에는 전문가의 경험과 책임이 필요하다. 따라서 AI가 업무를 지원하고 전문가가 최종 판단과 통제를 담당하는 휴먼인더루프(Human-in-the-Loop) 구조가 중요하다.

Q8. AhnLab AI PLUS는 무엇인가?

AhnLab AI PLUS는 안랩이 축적한 보안 데이터와 위협 분석 경험을 기반으로, 안랩의 다양한 보안 제품과 서비스에 AI 기능을 연결하고 고도화하는 에이전틱 AI 보안 플랫폼이다. 보안 특화 LLM과 지식 데이터베이스, AI 에이전트, 오케스트레이션과 가드레일을 기반으로 보안 운영 전반의 AI 지능화를 지원한다.