

# RSAC 2026, 에이전틱 AI 시대 사이버 보안은 어떻게 재편되나

지난 3월 23일부터 26일까지 미국 샌프란시스코 모스콘 센터에서 세계 최대 규모 사이버 보안 전시회 ‘RSAC 2026’이 개최되었다. 약 4만 명 이상이 참가한 올해 행사에서는 ‘Power of Community(공동체의 힘)’ 슬로건 아래, AI 시대 사이버 보안에서 사람과 커뮤니티 및 협업의 중요성이 강조되었고, 최신 보안 트렌드에 대한 스피치 세션과 기관·기업의 부스 전시로 구성되었다.

안랩은 올해 3년 연속으로 단독 부스를 운영하며, 에이전틱 AI 보안 기술을 중심으로 XDR, 위협 인텔리전스, CPS 보안에 대한 데모를 진행하며 전 세계 참가자들의 높은 관심을 받았다.

이번 행사에서 나타난 최신 사이버 보안 트렌드와 안랩의 전시 내용을 소개한다.



[사진 1] RSAC 2026 행사장 전경 (출처: RSAC)

## RSAC 2026 슬로건: ‘Power of Community’가 의미하는 보안의 미래

이번 RSAC 2026의 공식 슬로건은 ‘Power of Community’였다. 초고도화되는 사이버 위협 대응을 위해, 개별 기업의 독자적 방어를 넘어 글로벌 보안 커뮤니티의 정보 공유와 협력이 필수가 되어가고 있다. 이에, 기업에서 운영 중인 보안

솔루션을 폐쇄적으로 운영하는 것이 아니라, 다양한 솔루션 간 원활한 연동과 파트너십을 통해 ‘통합 보안 체계’를 구축하는 취지다.

한 발 더 나아가 ‘커뮤니티’는 사람 중심의 협업을 넘어, 사람 & AI & 시스템이 유기적으로 동작하는 보안 생태계를 의미한다. 에이전틱 AI(Agentic AI)의 등장으로 AI가 자율적인 보안 의사결정을 내리는 주체로 인식되기 시작했고, 기존 인간 중심 보안 모델을 근본적으로 변화시키고 있다. 이제 보안은 단순히 기술을 배포하는 것을 넘어, 각 주체들이 어떻게 상호작용하고 신뢰를 형성하는지가 핵심이 되었다.

이러한 맥락에서 ‘Power of Community’는 보안이 나아가야 할 방향을 제시하는 선언에 가깝다고도 볼 수 있다. 앞으로의 사이버 보안은 다양한 주체들이 연결된 환경에서 얼마나 효과적으로 협력하는가, 또 그 협력 관계를 얼마나 안전하게 유지할 수 있는가에 의해 달렸다. 그 중심에는 인간과 함께 상호작용하기 시작한 에이전틱 AI가 있다.

## RSAC 2026 Keynote 핵심 정리: AI 시대, ‘통제 가능한 AI’가 경쟁력이다

RSAC 2026의 주요 키노트들은 AI의 확산을 전제로 하면서, AI 기술의 ‘도입’을 넘어 ‘통제’까지 개념을 확장시켰다. 이제 AI는 선택의 개념이 아니라 모든 보안의 근간을 이루고 있다. 이 가운데, 기업들은 AI를 얼마나 안전하게 잘 활용할 것인가를 고민하고 있다. 이제 보안 전략이 AI의 기능 중심에서 운영 중심으로 이동하고 있다. 이러한 개념의 확장은 주요 기조연설에서도 잘 드러났다.

### 휴 톰슨 RSAC 회장 – 안전한 AI 활용, 기술이 아닌 사람이 핵심

휴 톰슨(Hugh Thompson), RSAC 회장(Executive Chairman)은 오프닝 기조연설 ‘What’s Your Why?’에서 AI의 변화를 수동적으로 겪는 것을 넘어, 방어를 위해 AI를 주도적으로 활용해야 할 책임이 있다고 강조했다.



[사진 2] 휴 톰슨(Hugh Thompson) RSAC 회장 (출처: RSAC)

그는 AI가 보안 환경을 근본적으로 변화시키는 가운데, 공격자들도 동일한 수준의 혜택을 얻고 있다고 언급했다. 미래의 보안은 더 이상 기술 경쟁이 아니라 AI를 얼마나 안전하고 책임 있게 운영해 보안을 실현할 수 있는가에 달려 있다고 말했다.

안전한 AI 활용의 핵심은 이를 설계하고 운영하는 사람이라는 점을 강조했다. 그 연장선에서 AI는 보안 조직의 역할을 줄이는 것이 아니라 오히려 보안의 범위와 책임을 확장시킨다고 했다. 보안 조직이 단순히 위협에 대응하는 조직이 아니라 AI 기반 시스템 전체를 설계하고 관리하는 전략 조직으로 진화한다는 뜻이기도 하다.

### **바수 자칼 마이크로소프트 시큐리티 부사장 - 보안은 신뢰를 기반으로 지속 운영되어야**

바수 자칼(Vasu Jakkal), 마이크로소프트 시큐리티 부사장(Corporate Vice President, Microsoft Security)은 기조연설 'Ambient and Autonomous Security: Building Trust in the Agentic AI Era'에서

AI가 스스로 계획하고 실행하는 에이전틱 AI 시대가 도래함에 따라 AI가 사람의 개입 없이 자율적으로 위협에 대응하는 형태로 진화하고 있다고 말했다.

위협 행위자들이 AI를 활용해 피싱, 멀웨어 생성 등 전술적 해킹 작업의 80~90%를 자동화해 대규모 자율형 공격 전개하고 있다고 밝히며, 보안 역시 특정 시점에 작동하는 기능이 아니라 에이전트를 중심으로 지속적으로 작동하는 환경

(ambient)으로 전환되어야 한다고 강조했다. 즉, 보안은 더 이상 사용자가 인식하는 순간에만 발현되는 것이 아니라, 시스템 전반에 자연스럽게 녹아들어야 한다는 것이다.

자율적인 보안(autonomous security)으로의 변화는 전에 없던 새로운 리스크를 동반한다. 바수 자칼 부사장은 AI를 이해하고 통제할 수 있는 가시성(visibility)과 거버넌스(governance)가 반드시 함께 구축되어야 한다고 강조했다. AI 시대 보안의 본질을 ‘신뢰 구축’으로 정의하며, 특히 AI가 내리는 결정과 근거를 지속적으로 검증할 수 있는 체계가 신뢰 확보의 핵심이라고 설명했다.

## 산드라 조이스 구글 위협 인텔리전스 부사장 - 연대를 통해 최신 위협에 반격

2022년 8시간에서 2025년 22초로 급감. 공격자가 침투 후 공격 전개까지 걸리는 시간의 변화다.

산드라 조이스(Sandra Joyce) 구글 위협 인텔리전스 부사장(Vice President, Google Threat Intelligence)은 공격자들이 AI를 활용해 속도, 규모, 정교함을 모두 강화하여 공격을 굉장히 빠르게 전개하고 있다고 말했다.

이에 대응하기 위해 방어자들도 필연적으로 AI를 사용해야 하며, 위협 헌팅, 패칭 등 보안의 여러 요소들도 AI가 주도하는 모델 구축이 필요하다고 밝혔다. 이어서, 방어자들이 더 이상 수동적인 위협 탐지와 집계(Counting)에 머물러서는 안되며, 업계 전체가 연대를 통해 강력한 보안을 확립하고 사이버 복원력(Resilience)을 구축해야 한다고 강조했다.

기조연설 내용들을 종합하면, RSAC 2026은 분명한 방향성을 보여준다. 이제 보안의 핵심 경쟁력은 AI를 얼마나 신뢰 가능한 형태로 안전하게 운영할 수 있는가에 달려 있다. 특히 에이전틱 AI의 확산은 이러한 변화를 더욱 가속화하며, 보안 조직이 AI 기반 운영을 설계하는 핵심 역할을 수행해야 함을 분명히 한다.

## Innovation Sandbox 2026: Agentic AI 시대, ‘AI를 통제하는 보안’의 부상

RSAC의 이노베이션 샌드박스(Innovation Sandbox)는 매년 보안 산업의 미래를 가장 빠르게 보여주는 무대다. 2026년에는 AI와 관련된 기술들이 중심을 이루었으며, 앞서 기조연설과 유사한 흐름이 이노베이션 샌드박스에서도 관찰되었다. AI를 활용해 보안을 강화하는 기술 뿐만 아니라, AI의 행동을 설명 가능하게 만들고, 정책적으로 통제할 수 있는 기술이 많은 관심을 받았다.

올해 우승 기업인 Geordie AI는 조직이 사용하는 AI 에이전트의 행동을 분석하고 통제하는 AI 거버넌스 플랫폼을 선보였다. 특히, AI 에이전트의 의사결정 과정과 행동 패턴을 지속적으로 모니터링하고, 정책 기반으로 이를 제어할 수 있는 기능을 제공한다는 점에서 높은 평가를 받았다.





[사진 3] RSAC 2026 이노베이션 샌드박스를 우승한 Geordie AI (출처: RSAC)

Geordie AI의 우승은 보안의 중심이 위협을 탐지하고 차단하는 것에서 AI가 무엇을 하고 있는지 이해하고 통제하는 것으로 비중이 옮겨감을 시사한다. 보안의 대상이 전통적인 IT 자산에서 AI 자체로 확장되고 있다는 의미이기도 하다.

## RSAC 2026 전시 트렌드: AI-enabled부터 AI security & governance까지

RSAC 2026 엑스포 현장에서 가장 두드러진 특징은 거의 모든 기업이 AI를 중심으로 메시지를 구성하고 있었다는 점이다. 다만, 접근 방식은 각 벤더의 전략에 따라 차이를 보였다. AI는 더 이상 차별화 요소가 아니라, 보안 시장의 기본 전제이자 전략의 구조를 나누는 기준이 된 것이다.



[사진 4] RSAC 2026 엑스포 현장 (1)





[사진 5] RSAC 2026 엑스포 현장 (2)

현장에서 보이는 AI에 대한 접근법은 크게 ▲AI-powered ▲AI-native ▲AI security & governance가 있었다.

먼저, AI-powered 접근은 EDR, XDR 등 보안 솔루션에 AI 역량을 통합한 모델이다. 보안 솔루션의 백엔드에 AI 기술을 적용하고, AI 어시스턴트 혹은 AI 에이전트를 활용해 위협 탐지, 분석, 대응을 자동화하고 보안 의사결정을 지원한다. 현재 사이버 보안 업계에서 보편적으로 사용되는 형태이며, 이번 행사 엑스포에서도 가장 흔하게 찾아볼 수 있는 접근 방식이었다.

AI-native는 제품 설계부터 AI를 중심으로 재구성한 모델로, 데이터 수집, 분석, 대응까지 전 과정이 하나의 흐름으로 연결된다. 이 접근법은 보안 아키텍처 자체를 재정의하며, 자동화와 확장성 측면에서 강력한 경쟁력을 가진다. 이번 행사 현장에서는 일부 벤더들이 기존 솔루션을 유지하면서, AI-native 플랫폼을 구축하는 전략을 병행하는 모습을 보였다. 다만, 진정한 AI-native 에이전트 기반 보안 운영이라는 관점에서는 일부 역량들만 구현하는 단계로 아직 과정 중에 있었다.

이와 함께 AI security & governance 영역도 빠르게 부상하고 있다. 에이전틱 AI의 확산으로 AI가 새로운 보호 대상이자 공격 표면이 되었기 때문이다. 앞서, 이노베이션 샌드박스를 통해 살펴봤던 흐름과 유사하게 AI의 행동을 모니터링하

고 통제하는 기술들도 확인할 수 있었다. AI security & governance는 AI-native가 확산될수록 AI에 대한 신뢰(Trust)와 안전한 사용이 중요해지기 때문에, 함께 성장하는 관계로 볼 수 있다.



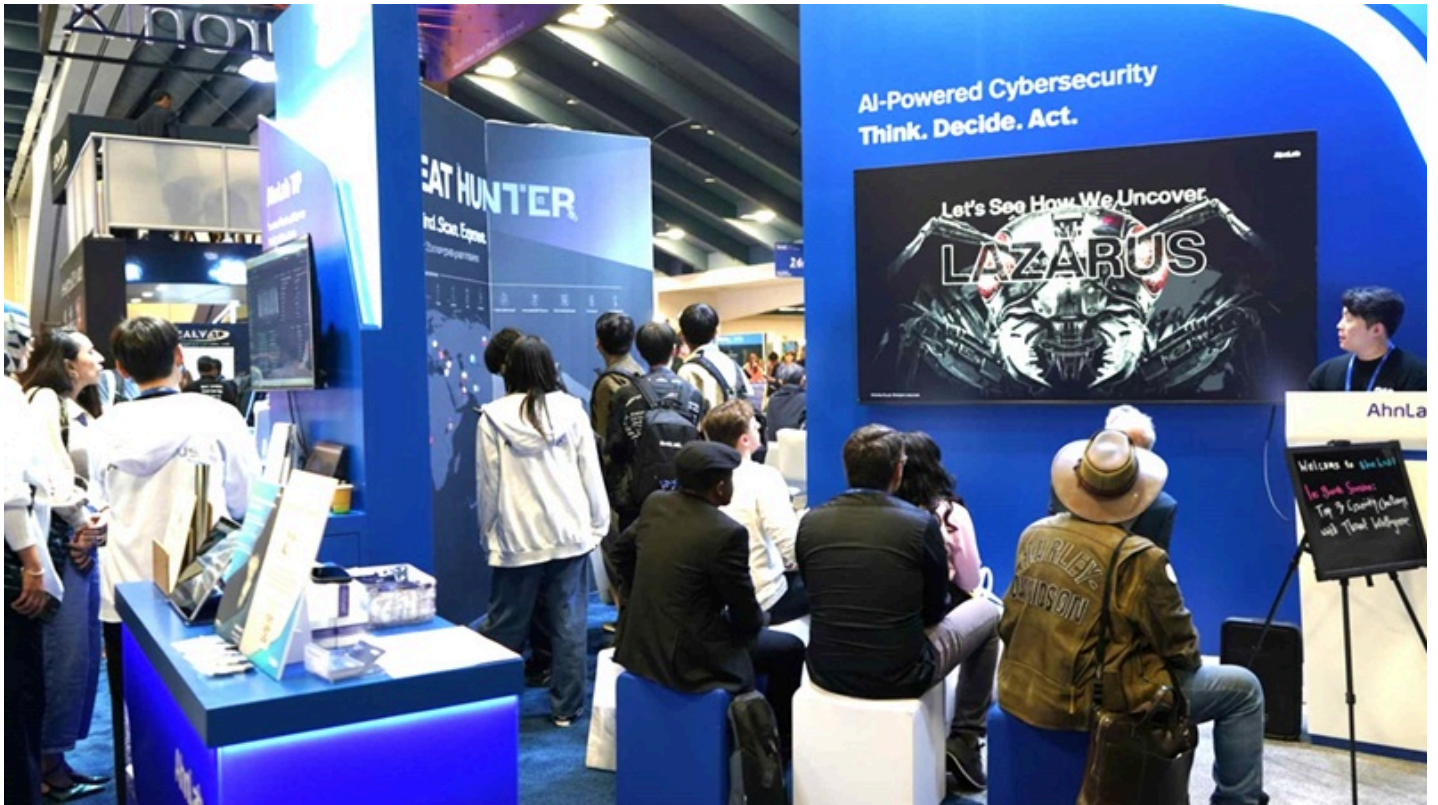
[사진 6] RSAC 2026 엑스포 현장 (3)

AI 트렌드의 연장선에서 아이덴티티(Identity) 영역의 중요성이 높아지는 것도 확인했다. 기존에는 사용자 계정 중심의 접근 제어가 핵심이었다면, 이제는 AI 에이전트와 클라우드 워크로드까지 포함하는 아이덴티티 관리 체계가 필요하기 때문이다. 이 밖에, 공격자들이 시스템 뿐만 아니라 AI의 입출력, 맥락 등 의사결정 과정 전체를 노리면서, 모델 컨텍스트 프로토콜(Model Context Protocol, MCP) 등 새로운 인터페이스를 지원하는 기업들의 모습도 볼 수 있었다.

## 안랩의 AI-Powered Security, 참가자들의 시선을 사로잡다

RSAC 2026에서 안랩은 ‘AI-Powered Cybersecurity: Think, Decide, Act(AI 기반 사이버 보안: 생각하고, 판단하고, 행동하다)’라는 슬로건과 함께 AI 기술이 통합된 XDR, 위협 인텔리전스, 그리고 전 세계 CPS 보안 시장을 선도하는 CPS 보안 플랫폼을 선보였다.

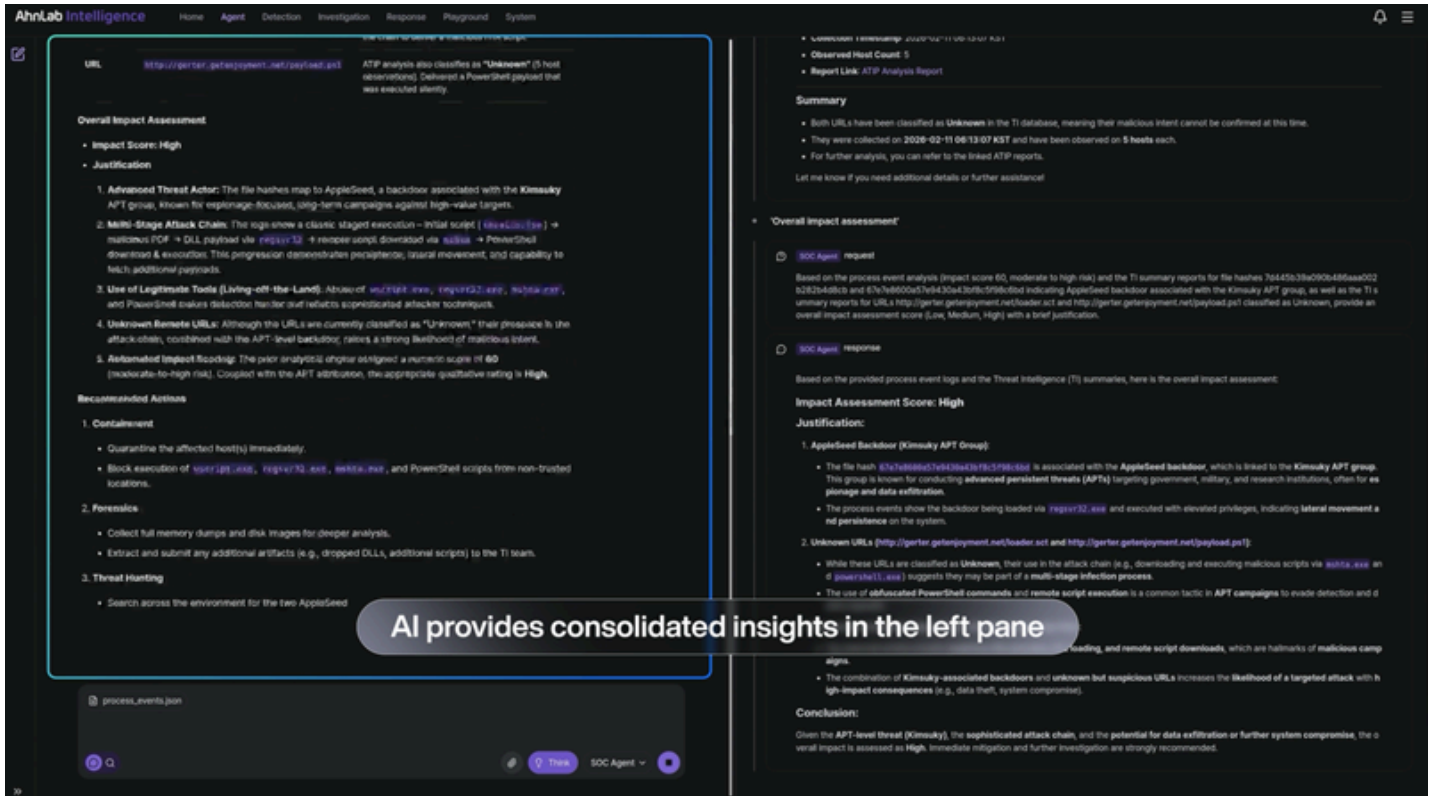




[사진 7] RSAC 2027 안랩 부스 전경

안랩 부스에는 북·남미, 아시아, 중동, 유럽 등 전 세계 보안 업계 관계자가 방문해, 안랩이 통합 보안 플랫폼 체계에서 제공하는 다양한 제품에 대한 체험과 상담을 이어갔다.

또한, 참관객들은 안랩의 AI 보안 플랫폼 AhnLab AI PLUS가 위협 식별부터 분석, 대응까지 수행하는 ‘에이전틱 AI 기반 자율 보안 운영’을 보며 안랩의 AI 보안 전략을 이해하고 공감했다.



[사진 8] AhnLab AI PLUS 데모 영상 중 일부 ([영상 시청하기](#))

안랩이 이번 RSAC 2026에서 선보인 주요 내용은 다음과 같다.

## AhnLab XDR: 마이터어택 평가를 통해 검증된 AI 기반 위협 탐지 & 대응

먼저 안랩 XDR은 마이터어택 평가(MITRE ATT&CK® Evaluations) 등 주요 글로벌 보안 제품 평가에서 입증한 통합 위협 탐지·대응 역량으로 주목을 받았다. AI 보안 어시스턴트 ‘애니(Annie)’, 머신러닝 기반 탐지 룰 등의 기능을 강화하며, 위협 탐지·분석·대응 전 과정에 AI를 적용하고 있다. 참관객은 이 같은 AI 기반 XDR 플랫폼을 활용해 위협을 조기 식별하고, 위험도를 신속하게 판단함으로써 보안 운영을 효율화 할 수 있다는 점에 관심을 보였다.

## AhnLab CPS PLUS: OT-IT를 융합한 글로벌 리딩 CPS 보안 플랫폼

안랩은 글로벌 제조 환경을 중심으로 강화되고 있는 보안 규제에 대응하려는 다양한 국가의 수요도 확인했다. 안랩의 CPS 보안 플랫폼 AhnLab CPS PLUS는 다양한 산업 현장에서의 레퍼런스를 기반으로 운영 중단 없는 안정적인 시스템 보호 역량과 위협 탐지 역량을 제공한다는 점에서 긍정적인 반응을 얻었다. 특히 OT 전용 네트워크 보안 솔루션 ‘AhnLab XTD’와 OT 엔드포인트 보안 솔루션 ‘AhnLab EPS’ 연동을 통해 타사 대비 탁월한 자산 가시성을 제공한다는 점에 높은 관심이 이어졌다.

실제로 안랩은 폭 넓은 CPS 보안 커버리지와 강력한 고객 레퍼런스를 바탕으로 시장조사기관 프로스트 앤 설리번(Frost & Sullivan)의 2025 프로스트 레이더(Frost Radar) CPS 보안 글로벌 리더로 선정된 바 있다.



## AhnLab TIP: 실제 적용 가능한 위협 인텔리전스, 글로벌 도입 사례 이어져

안랩의 위협 인텔리전스 플랫폼 AhnLab TIP는 즉시 활용 가능한(Actionable) 고도화된 위협 인텔리전스를 제공한다는 점에서 높은 관심을 받았다. 특히 침해지표(IoC), 다크웹, 위협 행위자 정보 등 다양한 영역에서 안랩 분석가들이 직접 수집·분석한 독점 정보가 주요 차별점으로 꼽혔다. 또한 자체 LLM 기반의 AI 어시스턴트로 보안 담당자가 필요한 위협 정보를 편리하게 확인할 수 있는 기능도 호응을 얻었다. 이 같은 위협 정보는 안랩의 다양한 제품과 연동돼 실제 의사결정 및 대응에 즉시 활용 가능하다.

아시아권 공격 그룹들에 대한 독보적인 분석 역량을 자랑하는 AhnLab TIP는 일본, 싱가포르 등 다양한 국가의 고객들이 연이어 도입하고 있다.

## ASEC 전문가가 발표한 실제 위협 사례와 동향

안랩의 위협 인텔리전스 전문 조직 ASEC(AhnLab SEcurity intelligence Center) 소속 이정욱 매니저는 RSAC 공식 브리핑 세션의 연사로 나서 'Abusing Legitimate Platforms: Real-World Threat Cases and Trends(정상 플랫폼 악용 공격: 실제 위협 사례와 동향)'을 주제로, 최신 위협에 대한 안랩의 심층 분석 결과를 공유했다.



[사진 9] ASEC 이정욱 매니저 브리핑 세션

이 매니저는 실제 공격 사례를 중심으로, 게임·개발·메신저 서비스 등 정상 플랫폼을 악용한 최신 공격 기법을 분석하고 대응 방안을 제시했다. 이에 안랩이 수십 년간 자체 축적한 글로벌 위협 정보와 정교한 분석 및 추적 역량에 대한 현지 보안 업계 관계자들의 질의가 이어졌다.

## AI 중심의 사이버 보안, 글로벌 영향력을 확대하는 안랩

RSAC 2026의 핵심은 단연 에이전틱 AI였다. 그리고, 전 세계 다양한 보안 기업들이 AI-powered부터 AI-native, AI security & governance 등 각자에 맞는 전략을 바탕으로 AI 보안의 미래를 준비하고 있었다. 특히, 기존 IT 자산 중심의 보안에서 AI 자체를 보호하는 방향으로 보안의 무게 중심이 옮겨가고 있으며, 효과적인 보안을 위해서는 조직들의 연대가 중요하다는 것이 가장 큰 시사점이었다.

안랩은 자체 개발한 AI 보안 플랫폼을 중심으로 보안 솔루션들의 탐지, 분석, 대응 역량을 강화해 고객들의 보안 운영 생산성을 높이고 있다. 앞으로도, AI 보안 기술 고도화에 박차를 가해 전 세계 고객들의 보안 도전과제 해결을 위해 앞장 설 계획이다.

안랩 강석균 대표는 이번 행사에 대해 “RSAC에서는 안랩의 보안 기술력을 집약한 솔루션과 AI 중심 플랫폼 보안 전략의 청사진을 선보이며 글로벌 시장에서의 경쟁력을 다시 한번 입증했다”며, “빠르게 변화하는 시장 환경 속에서 글로벌 고객과의 꾸준한 소통으로 안랩의 새로운 도약을 가속해 나가겠다”고 말했다.

안랩의 AI 보안 플랫폼 AhnLab AI PLUS에 대한 자세한 내용은 안랩 홈페이지에서 확인할 수 있다.

▶ [AhnLab AI PLUS 자세히 알아보기](#)

**AhnLab**

콘텐츠마케팅팀 신재만 매니저