AI와 함께하는 우리의 5년 후 모습은?

글로벌 IT 리서치 기관 가트너(Gartner)는 지난 6월 9일부터 11일까지 미국 메릴랜드주 내셔널 하버 게일로드 컨벤션 센터에서 ‘Gartner Security & Risk Management Summit 2025(이하 가트너 서밋 2025)'를 개최했다. 이번 컨퍼런스에서는 가트너 애널리스트 포함 수십 여명의 연사들이 AI를 포함한 다양한 영역의 트렌드와 인사이트를 공유했다.

이번 글에서는 가트너 서밋 2025에서 확인한 주요 보안 트렌드들을 공유한다.

전 세계 보안 관계자들이 참석한 가트너 서밋 2025은 ▲참가자 5000여 명 ▲전시 업체 수 250여 개 ▲세션 수 360여 개 등 큰 규모로 진행됐다. 그리고, 전 세계 사이버 보안을 관통하고 있는 AI를 포함해 제로 트러스트 보안, 보안 운영 최적화, CPS 보안, 워크스페이스 보안 등 다양한 주제들이 다뤄졌다.

기조연설: 기대감을 기회로 만들자

가트너 서밋 2025 오프닝 기조연설 ‘Harness the Hype: Turning Disruption Into Cybersecurity Opportunity’은 가트너 Distinguished VP 애널리스트 레이 맥뮬런(Leigh McMullen)과 카텔 틸레만(Katell Thielemann)이 진행했다. 이 연설은 다양한 신기술에 대한 기대감을 사이버 보안의 실질적인 기회로 만들자는 의미다.

[사진 1] 가트너 서밋 2025 오프닝 기조연설 (출처: 가트너)

두 연사는 보안 환경이 복잡하고 예측 불가능한 방향으로 전개되는 가운데, CISO(Chief Information Security Officer)들이 신기술에 대해 높아지는 기대감과 보안 요구사항을 해결하기 위해 다음 세 가지를 갖춰야 한다고 강조했다.

#1. 조직의 미션과 사이버보안 연결(Be Mission-Aligned)

CISO는 보호(Protection) 강화와 공격 노출(Exposure) 감소라는 관점에서 커뮤니케이션을 해야 한다. 그래야 신기술에 대한 과도한 기대감(Hype, 하이프)에 휘둘리지 않을 수 있다. 하이프의 흐름을 이해하고 활용할 줄 아는 CISO는 변화로부터 조직을 보호하고 혁신에 앞장설 수 있다. 또, 이러한 CISO의 접근은 사이버 보안에 대한 노력을 조직의 비즈니스 미션과 일치시키는 데 기여한다.

#2. 항상 혁신할 준비하기(Be Innovative-Ready)

CISO는 조직의 AI 역량(AI literacy)을 키워 부서 전체가 AI를 이해하고 실험할 수 있도록 해야 한다. 또한, 사이버 보안 분야에서 AI를 적극적으로 실험하고 실제 활용 사례(Use Case) 적용을 통해 업무 혁신을 보호해야 한다. AI 보안 강화와 리스크 대응 체계도 마련하여 조직이 투자한 AI 자산을 보호해야 한다. AI, 사이버 보안, 조직의 변화는 모두 연결되어 있으며, 이 셋을 연결 짓는 능력이 CISO 리더십의 핵심 자질이다.

#3. 변화에 빠르게 대응하기(Be Change-Agile)

CISO는 팀이 문제 해결의 주체가 되고, 주도성을 가질 수 있도록 지원해야 한다. 구성원들이 주도성을 갖게 되면 AI를 활용해 반복 작업을 자동화하여 새로운 기술을 개발하는 데 집중할 수 있게 된다. 이는 CISO뿐 아니라 팀 모두의 성장으로 이어지고, 어떤 변화를 맞이하더라도 회복력 있게 헤쳐 나갈 수 있는 역량을 길러준다.

끝으로 두 연사는 항상 배우는 자세로 새로운 기술 하이프를 분석하여 변화를 기회로 전환하는 리더가 되길 바란다는 메시지와 함께 기조 연설을 마무리했다.

향후 10년을 이끌어갈 AI, 어떻게 접근해야 할까?

사이버 보안의 핵심으로 자리한 AI. 이번 가트너 서밋 2025에서도 AI에 관한 수 많은 세션들이 진행되었다. 이 중 'Future-Ready: Security Implications of Emerging GenAI Technologies' 세션을 발표한 가트너 Distinguished VP 애널리스트 피터 퍼스트브룩(Peter Firstbrook)은 "향후 10년은 AI의 시대가 될 것이며, 큰 기회와 리스크를 동반할 것"이라고 강조했다.

#1. AI 혁신과 도전과제

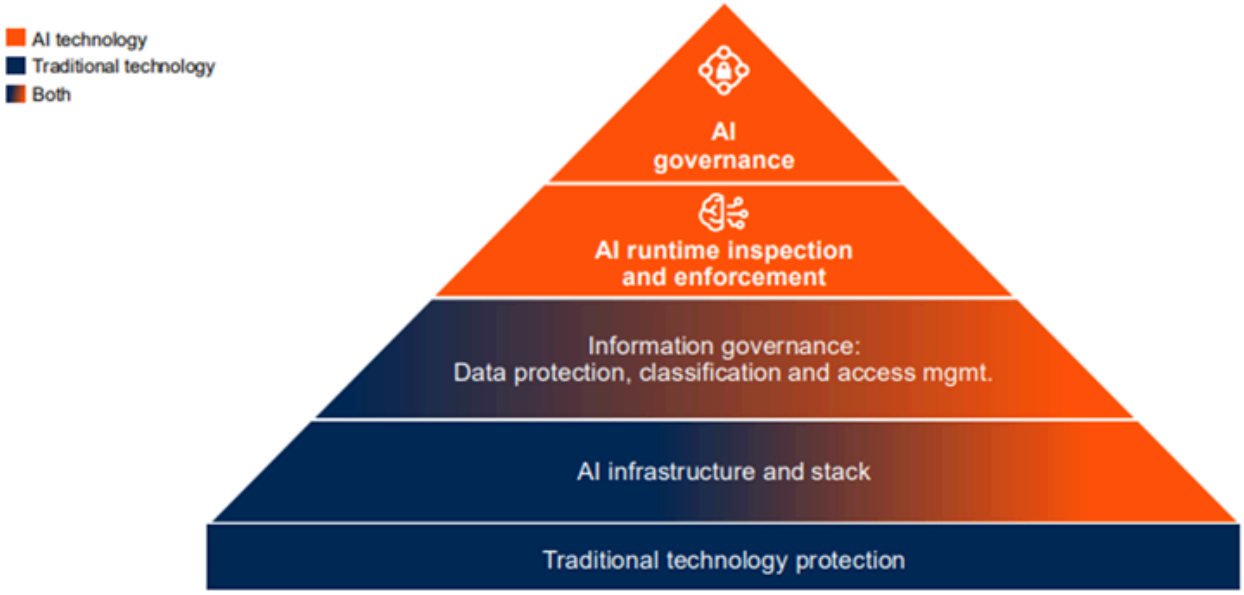
이 세션에서 피터 퍼스트브룩은 ▲눈 앞에 다가온 AI 혁신 ▲AI로 인한 리스크 ▲장기적인 리스크 해결 방안 등 세 가지 관점에서 AI 보안의 현재와 미래를 짚었다.

먼저 가시적인 AI 혁신의 키워드는 바로 '에이전틱 AI(Agentic AI)'다. 에이전틱 AI는 특정 분야에 특화된 AI 에이전트가 자율적으로 작업을 수행하는 개념이다. 현재의 AI 어시스턴트는 큰 자율성 없이 규칙을 기반으로 작업을 수행하지만, 에이전틱 AI 혁신이 가속화되면 여러 특화된 에이전트들이 작업을 조율하고 AI 에이전트 생태계를 구축해 나갈 전망이다.

피터 퍼스트브룩은 보안 운영에서도 위협 탐지, 분석, 대응 등 영역 별로 특화된 AI 에이전트가 필요하다고 강조했다. 예를 들면, 침해 분석 에이전트는 로그 분석과 코드 설명을 담당하고, 침해 대응 에이전트는 대응 워크플로우 관리 및 계획을 수립한다. 공격 표면 관리에 최적화된 에이전트는 공격 표면을 식별하고 검증 및 감소시키는 역할을 맡게 된다.

AI 혁신의 혜택을 넘어 AI 도입으로 인한 리스크까지 함께 짚었다. 우선, 생성형AI를 사용하는 과정에서 데이터 유실, 공격자들의 프롬프팅 공격, 허용되지 않은 정보 검색 등에 대한 주의를 당부했다. 또한, 공격자들 역시 생성형AI를 사용하고 있으며 피싱 캠페인, 딥페이크 공격, 악성코드 개발 등이 더욱 정교해지고 있다고 말했다. 더 나아가, 에이전틱 AI가 수반하는 리스크의 예시로 'LLM-as-a-judge'를 함께 소개했다. LLM이 다른 LLM 혹은 사람이 만든 콘텐츠를 평가하게 되고, 이 과정에서 오류로 인해 정확한 평가가 이뤄지지 않을 수 있다는 개념이다.

AI 리스크에 대해 피터 퍼스트브룩이 제안한 해결 방안은 'AI TRiSM 프레임워크'였다.



[사진 2] 가트너의 AI TRiSM Framework (출처: 가트너)

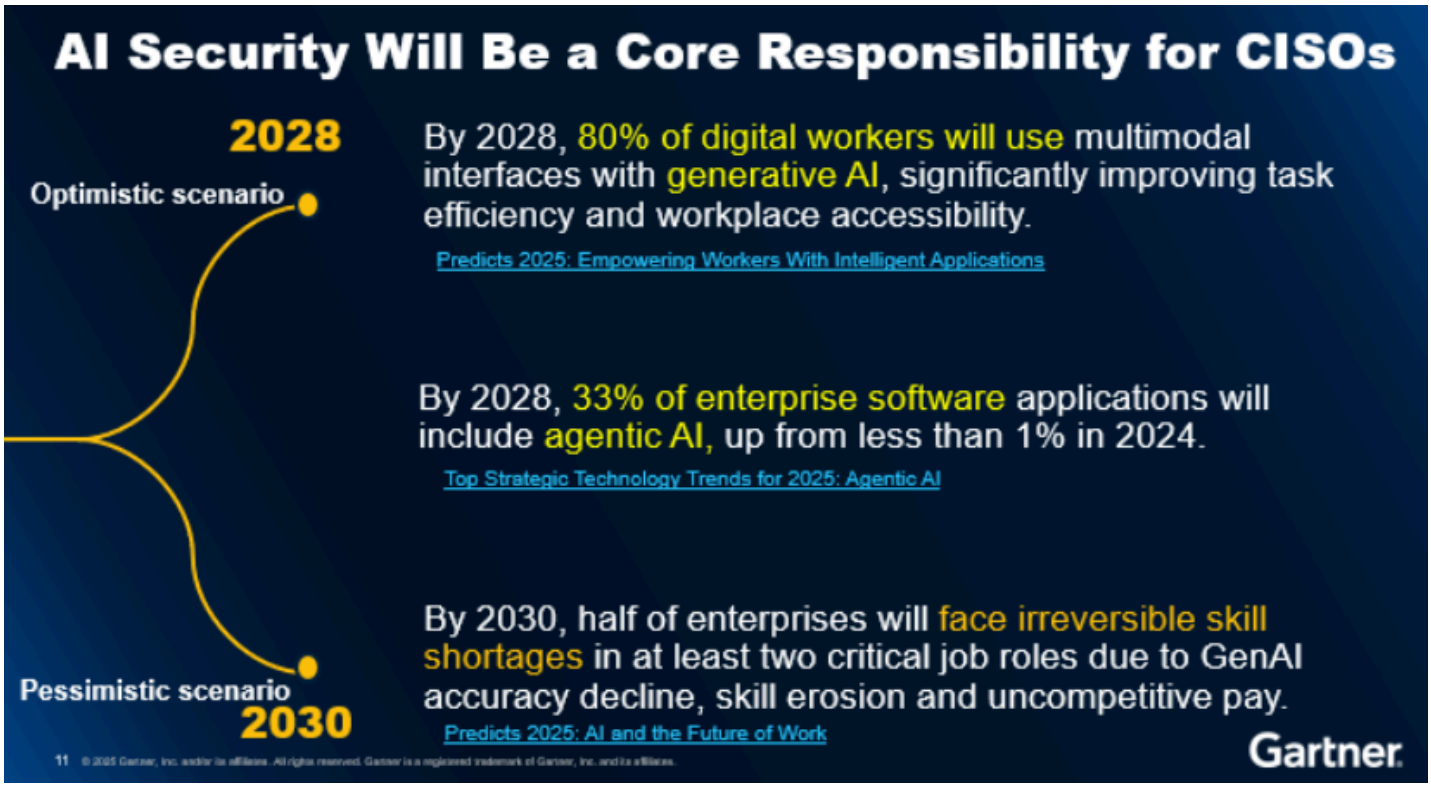
AI TRiSM은 Artificial Intelligence Trust, Risk and Security Management를 의미한다. 보안 관점에서 보면 먼저 조직에서 운영 중인 기존 기술에 대한 보안이 이뤄지고, AI 인프라에 대한 보안이 뒤따른다. 이후, 데이터 보안 등 정보 거버넌스를 수행한 뒤 AI 런타임 검사 및 AI 거버넌스를 진행하는 프레임워크다. 그는 AI 기반 공격이 사람의 대응을 쉽게 능가할 수 있기 때문에 AI TRiSM을 토대로 공격 표면 관리 자동화 등 공격자들을 어렵게하는 선제적 사이버보안의 중요성을 강조했다.

#2. 2030년 AI를 사용하는 모습은?

이처럼 AI는 우리에게 혜택과 리스크를 동시에 가져다준다. 그럼 5년 뒤인 2030년, AI를 사용하는 우리는 어떤 모습일까? 가트너 Distinguished VP 애널리스트 제레미 듀혼(Jeremy D'Hoinne)은 'Future of AI in Cybersecurity: AI Predictions and Roadmap Challenges for 2025-2028' 세션을 통해 AI 보안의 미래를 조망했다.

[사진 3] 제레미 듀혼((Jeremy D’Hoinne) 가트너 Distinguished VP 애널리스트 (출처: 가트너)

먼저, 제레미 듀혼은 현재 상황에 대해 AI 기술 성숙도에 비해 기대치가 앞서가면서 과열과 냉각이 반복되고 있다고 짚었다. 또한, 일각에서 거론되는 범용 인공지능(Artificial General Intelligence, AGI) 조기 도래에 대해서도 2040년 이후가 될 가능성이 높다는 의견을 피력했다. 기술의 가능성을 과장하기보다는 현재 할 수 있는 일과 없는 일을 구분하여 접근해야 함을 거듭 강조했다.



[사진 4] 가트너가 제시한 AI 보안 전망 (출처: 가트너)

이어서 그는 2030년까지 AI에 대한 낙관적인 전망과 부정적인 전망을 모두 제시했다. 낙관적 전망은 전체 디지털 노동자의 약 80%가 생성형AI를 활용해 업무 효율성을 높일 것으로 봤다. 다만, 2030년에는 약 절반의 조직들이 생성형AI에 과도하게 의존하면서 보안 역량이 약화될 것이라는 부정적인 전망도 내놓았다.

제레미 듀혼은 AI 기술이 빠르게 변화하는 가운데, 조직들이 3년 단위의 전통적 로드맵이 아닌 6개월 단위의 유연한 실험 중심 전략으로 전환해야 한다고 강조했다. 또한, AI를 목표(objective)로 삼기보다 활동(activity)으로 정의해야 하며, 'AI를 도입한다'는 개념이 아닌 'AI로 탐지 정확도를 개선한다' 등 구체적이고 측정 가능한 목표 설정이 필요하다고 했다. 결론적으로, AI 활용은 ▲측정 가능한 결과 ▲실패를 허용할 수 있는 실험 설계와 새로운 시도 ▲유연한 전략이 뒷받침되어야 진정한 가치를 실현할 수 있다고 당부했다.

차세대 네트워크 보안 플랫폼, SASE의 미래는?

SASE(Secure Access Service Edge)는 현대적인 트래픽 패턴에 맞춰 성능과 관리 효율성을 높이고, 제로 트러스트 원칙을 적용하는데 중점을 둔 접근 방식이다. 기능 관점의 구성요소는 ▲SD-WAN ▲방화벽 ▲SWG ▲ZTNA ▲CASB가 있다. SASE는 현존하는 네트워크 보안 플랫폼 중 가장 큰 개념을 지향한다고도 할 수 있다.

그렇다면 조직들은 SASE에 대해 어떻게 접근해야 할까? 가트너 VP 애널리스트 앤드류 러너(Andrew Lerner)는 'Technical Insights: Which SASE Operating Model Is Right for Me?' 세션에서 가트너 조사 결과를 인용하며, 기업들이 SASE에서 보안 기능(70%)을 가장 중요시한다고 설명했다. 편리한 관리(51%)와 통합된 정책(44%)이 뒤를 이었고 네트워킹 기능은 19%에 그쳤다.

그는 기업들의 SASE 플랫폼 도입 목적을 ▲VPN 대체 ▲관리 복잡성 해소 ▲지점(Branch) 오피스 현대화 ▲제로 트러스트 확보 ▲분산된 네트워킹 환경 대응 등으로 꼽았다. 그리고, 방대한 SASE 플랫폼 구축을 위해 단일 벤더 혹은 복수 벤더와 협업이 가능한데, 일반적으로 기능을 중시하는 대기업들은 복수 벤더를 편의성에 초점을 두는 중소기업들은 단일 벤더 접근을 선호하는 경향이 있다고 설명했다.

이어서, 다음과 같이 SASE 플랫폼의 발전 방향을 제시하며 조직의 특성을 고려해 SASE 플랫폼을 고려 및 도입하는 것이 중요하다고 강조했다.

- 플랫폼 가속화: 각 기능들이 SASE 플랫폼으로 통합되는 추세 가속화

- 민감 데이터 탐지 및 제어 확장: 위협 인텔리전스만큼 중요성 부각

- AI 적용: 생성형 AI 어시스턴트, 생성형 AI 기반 제어, 에이전틱 AI의 도입 확대

- 활용 사례 확대: 범용 ZTNA, 공공장소 네트워킹, LAN 및 IoT 디바이스로의 확장

- 인접 솔루션과의 통합: EPP, DSPM, SSPM, XDR 영역으로의 확장성

CPS 보안은 시스템이 아닌 사회를 지키는 것

가트너가 정의하는 CPS(Cyber-Physical System)은 센싱, 연산, 제어, 네트워킹, 분석 기능을 조율하여 물리적 세계(인간 포함)와 상호작용하는 엔지니어링된 시스템을 뜻한다. 과거에는 퍼듀 모델(Purdue Model)을 기준으로 외부와 분리된 OT 보안의 개념이 통용되었다. 하지만, 이제 OT와 IT가 상호 연결되어 보안 복잡성이 심화되고 있는 상황이다.

가트너 VP 애널리스트 왐 보스터(Wam Voster)는 Outlook for Cyber-Physical Systems Security 2025 세션을 통해 CPS 보안의 현재와 미래를 조망했다.

[사진 5] 왐 보스터(Wam Voster) 가트너 VP 애널리스트

먼저, 왐 보스터는 2023년 약 50개였던 랜섬웨어 그룹이 2024년 120개로 증가했는데, 이 중 40개는 제조업을 목표로 공격을 감행했다고 말했다. 그리고, CPS를 향하는 공격 중의 약 절반은 '표적형 공격(Targeted Attack)이라며, 공격자들이 공격 대상을 오랜 기간 관찰한 뒤 공격을 감행한다고 밝혔다.

그는 이러한 상황에서 기업들이 대체로 CPS와 IT의 연결을 이해하고는 있지만, 아직 효과적으로 구현하지 못하고 있다고 지적했다. CPS 보안에서 가장 큰 이슈는 바로 오너십과 거버넌스로, CPS 자산 보유 부서와 보안 부서 및 IT 부서가 서로 책임을 미루는 경우가 많다고 했다. 이어서, CPS 보안에서는 책임 분담이 중요하고, 자산을 소유하게 되면 리스크와 책임이 따른다는 사실을 유념해야 한다고 강조했다.

끝으로 왐 보스터는 우리 사회에는 지켜야 할 인프라가 굉장히 많고 이들은 서로 연결되어 있으며, CPS 보안은 시스템을 지키는 것이 아닌 사회를 지키는 것이라는 메시지를 전했다. 그리고, 효과적인 CPS 보안을 위해 다음과 같은 사항들을 권고했다.

- CPS의 선제적 관리를 통해 공격자가 침투할 수 있는 기회를 줄여야 한다.

- MITRE ATT&CK for ICS 프레임워크를 활용하여 공격자의 TTPs를 확인해야 한다.

- CPS 보안 플랫폼이 기업 환경에서 그대로 작동할 것이라 단정하지 말고, 사전 검증(POC)을 통해 가장 적합한 플랫폼을 선택해야 한다.

- AI 기반 CPS 보안 기능에 대한 레퍼런스와 실제 활용 사례를 확인해 과장된 이야기와 실제 운영 가치를 구분해야 한다.

- 조직 내 보안 인식 제고를 위한 교육을 실시하고 역할과 책임을 명확히 해야 한다.

- 사고 대응 계획을 수립하고 그 계획을 지속적으로 테스트해야 한다.

워크스페이스 보안, 핵심은 '효율성'

워크스페이스 보안(Workspace Security)은 최근 가트너에서 제시하는 새로운 보안 개념으로 하이브리드 환경에서 근무하는 직원을 보호하기 위한 사람, 프로세스 및 기술의 통합이다. 주요 보호 대상은 디바이스, 애플리케이션, 데이터, 자격 증명(credential) 및 ID 시스템 등이 있다.

피터 퍼스트브룩은 Strategic Roadmap for Workspace Security 2025 세션을 통해 아직까지도 많은 조직들이 보안 인프라를 제대로 통합하지 않아 침해 대응에 어려움을 겪는다고 했다. 공격자들은 이미 AI를 활용해 공격을 고도화하고 있지만 대부분의 방어자들은 인력과 자동화 부족에 시달리고 있다는 것이다.

[사진 6] 피터 퍼스트브룩(Peter Firstbrook) 가트너 Distinguished VP 애널리스트

가트너가 제시하는 워크스페이스 보안 구성요소를 보면 ▲엣지 보안(인터넷 및 이메일 보안) ▲엔드포인트 탐지 & 대응(EDR) ▲아이덴티티 접근 관리(IAM) ▲데이터 유출 방지(DLP) ▲사용자 행동 인식(Security behavior and culture) ▲그 외 서비스(자산 탐지, 보안 형상 평가, 취약점 탐지 & 대응) 등이 있다.

다만, 피터 퍼스트브룩은 워크스페이스 보안의 최종 목표는 모든 보안 툴을 갖추는 것이 아니라, 통합되고 관리 가능한 최소 포트폴리오(Minimally Effective Portfolio)를 운영하는 것이라 강조했다. 그리고, CTEM(Continuous Threat Exposure Management)와 같이 자동화를 중심으로 한 보안 구조를 통해 효율성을 갖출 것을 당부했다.

이에 관해, 가트너 VP 애널리스트 크리스 실바(Chris Silva)는 Forget the Hype: 5 Key Things You Should Be Doing to Secure Your Endpoints 세션에서 최근 조직들이 신기술의 하이프에 쫓겨 정작 보안의 기본기를 소홀히 하고 있다고 지적했다. 그리고, 조직들이 워크스페이스 보안을 위해 즉시 실천할 수 있는 5가지 핵심 요소들을 소개했다.

5가지 핵심 요소

- EDR: 실시간 공격 탐지 및 사전 대응을 가능하게 하는 핵심 보안 기술

- 애플리케이션 제어: 엔드포인트에서 실행되는 프로그램 식별 및 위험 행위 제한

- 보안 형상 관리: 설정 관리는 그 자체로 하나의 방어 계층

- 패치 관리: 중간 위험도 취약점이 많이 악용되는 가운데 증거 기반(evidence-based) 패치 우선순위화 필요

- 사고: 분리된 영역 간 연계 관점 전환

크리스 실바는 EDR, 애플리케이션 제어, 보안 형상 관리, 패치 관리라는 기술적 기반에 보안과 운영의 사고방식을 통합하는 조직 구조적 전환이 함께 이뤄져야 비로소 지속 가능하고 효율적인 보안 운영이 가능하다고 조언했다.

맺음말: 현재는 효율적으로 미래는 담대하게

이번 가트너 서밋 2025의 키메시지는 ‘Engage. Innovate. Lead’였다. 한글로 풀면 ‘협력하라. 혁신하라. 주도하라’ 정도로 해석된다. 최근 AI, 제로 트러스트 등 새로운 개념과 기술이 빠르게 등장하면서 협력과 혁신의 가치가 지속적으로 주목 받고 있다. 이러한 트렌드는 사이버보안 벤더들이 참가한 행사 전시장에서도 확인할 수 있었다.

[사진 7] 가트너 서밋 2025 전시장

다만, 워크스페이스 보안 내용 중 다룬 바와 같이 운영 중인 보안 솔루션의 효율성을 높여 현재를 잘 지켜내는 것도 굉장히 중요하다. 안랩도 이 점을 항상 인지하고 AI와 같은 미래지향적 기술 개발에 매진하는 동시에 현재 고객들에게 제공하는 솔루션과 서비스의 사용성을 높이는 데에도 지속적인 노력을 기울이고 있다.

월간안 독자 여러분도 맺음말의 부제처럼 '현재는 효율적으로 미래는 담대하게' 임하여 당사의 비즈니스를 안전하게 보호해 나가길 바란다.

AhnLab
콘텐츠마케팅팀 신재만 과장