# 차세대 솔루션으로 아시아 기업들을 사로잡다

안랩은 10월 9~10일 이틀 간 싱가포르 마리나 베이 샌즈 & 엑스포 컨벤션 센터(Marina Bay Sands Expo & Convention Center)에서 열린 글로벌 IT 전시회 'Tech Week Singapore 2024'에 단독 부스를 열고 참가했다. 또한, 자사 위협 인텔리전스 조직 ASEC 최수진 선임연구원이 실제 침해 사례를 분석한 내용으로 전문가 발표 세션을 진행해 참가자들의 큰 호응을 얻었다.

안랩이 다양한 국가의 참가자들과 만났던 행사 현장을 살펴보자.

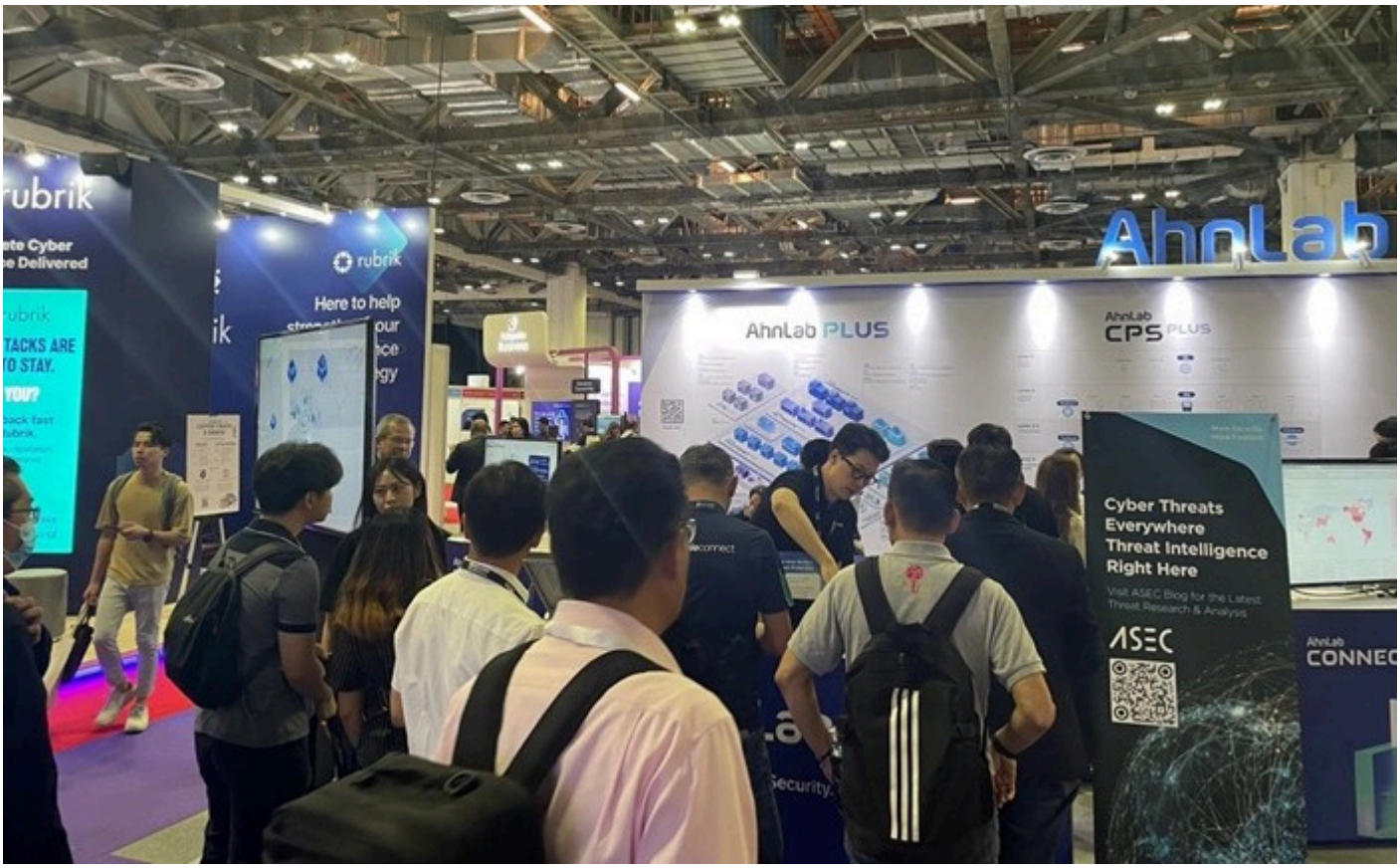
Tech Week Singapore는 동남아시아 지역 최대 규모 IT 전시회 중 하나로 사이버보안, 클라우드, 데이터센터, 빅데이터 & AI, 이커머스 등 총 7개의 IT 영역 별로 전문관을 구성했다. 올해 행사는 1일차에는 'Riding the Wave of Disruptions with Intelligent Technologies(지능형 기술로 혁신의 물결 타기)', 2일차에는 'Reinventing Business in the Digital Age: Leveraging Technologies for Success(디지털 시대의 비즈니스 재창조: 성공을 위한 기술 활용)' 트랙(주제)으로 진행됐다. 참가자 수는 이틀에 걸쳐 약 2만 6천명을 기록했다.


[사진 1] Cyber Security World에서 주요 전시 기업으로 소개된 안랩

안랩은 사이버보안 전문관 'Cyber Security World'에 단독 부스를 운영하고 글로벌 전략 솔루션을 전시 및 시연했다. 안랩이 이번 행사에서 내건 슬로건은 'AI-Augmented Security. Simplified.'였다. AI를 기반으로 강력하고 단순한 보안을 구현한다는 의미다. 안랩은 자사 솔루션 기반 인프라(백엔드)에 AI 기술을 적용해 위협 탐지 및 분류를 고도화 및 자동화하고 있다. 또한, 위협 분석 및 대응 플랫폼 AhnLab XDR에 생성형 AI를 탑재해 고객의 효율적인 리스크 관리를 지원할 계획이다.


[사진 2] 안랩 부스 전경

안랩은 이번 행사에서 ▲AhnLab CPS PLUS(OT-IT 융합 보안 플랫폼) ▲AhnLab TIP(위협 인텔리전스 플랫폼) ▲AhnLab XDR(위협 분석 및 대응 플랫폼)을 소개 및 시연했다. 부스에는 이틀 간 싱가포르, 말레이시아, 인도네시아 등 동남아시아 현지 산업 관계자 600여 명이 방문해 자사 솔루션에 대한 높은 관심을 나타냈다.



[사진 3] 참관객들로 붐비는 안랩 부스

또한, 안랩은 부스 백월에 전체 보안 플랫폼, 제품 및 서비스를 구조화한 '시큐리티 맵'을 함께 전시했다. 안랩은 지난 9월 개최한 AhnLab ISF 2024에서 엔드포인트, 네트워크, 클라우드, 서비스, 보안 운영, CPS(Cyber-Physical System)를 아우르는 통합 보안 플랫폼 'AhnLab PLUS'를 공식적으로 선보인 바 있다. 방문객들은 부스에서 소개 및 시연한 솔루션 외에도 AhnLab PLUS 플랫폼 기반 시큐리티 맵을 보면서 엔드포인트 보안, 모바일 보안, 클라우드 보안 등 안랩의 여러 오퍼링에 대해서도 큰 관심을 보였다.

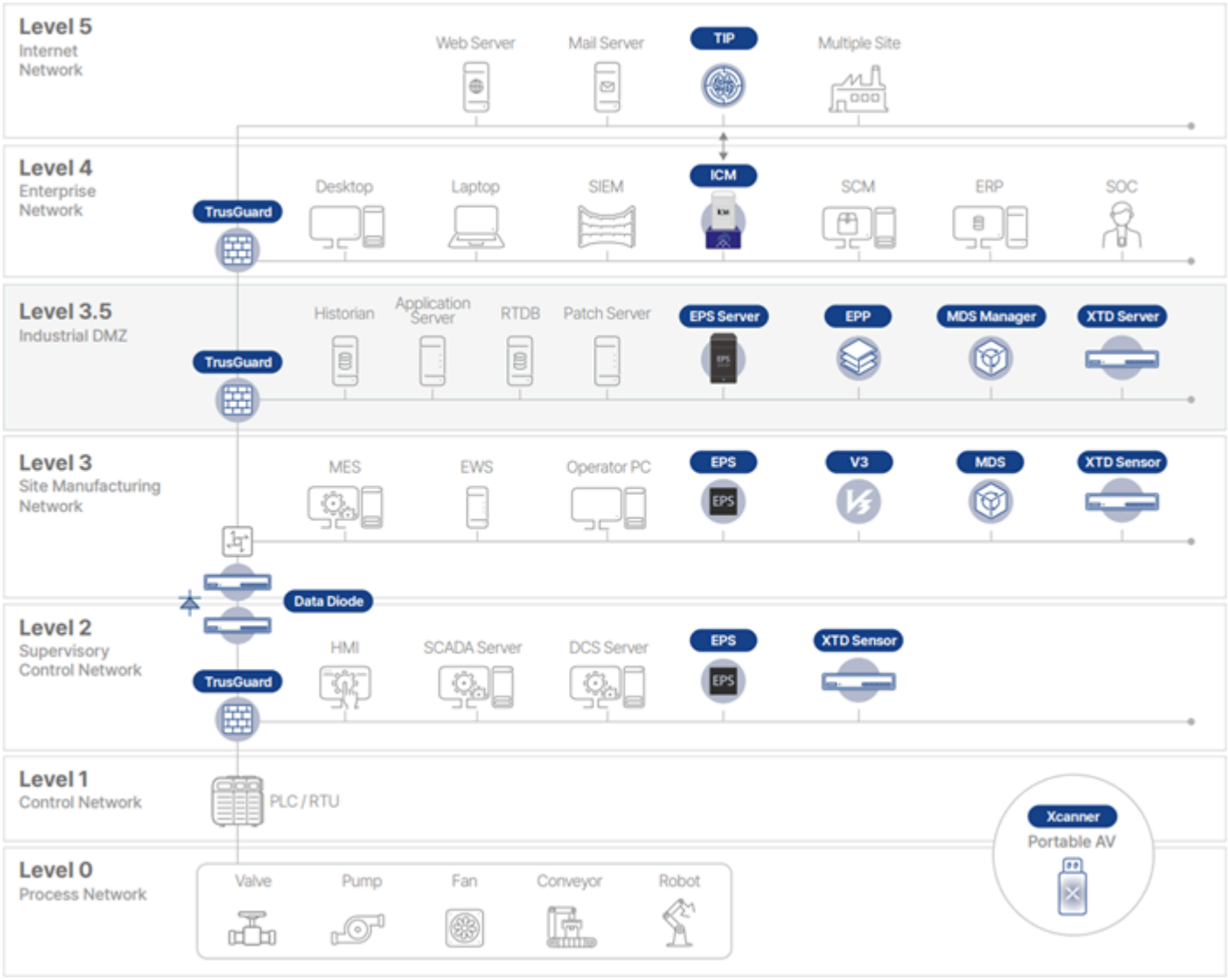

[사진 4] AhnLab PLUS 플랫폼과 시큐리티 맵 설명

다음으로 부스에서 소개 및 시연한 솔루션들에 관한 주요 내용을 소개한다.

## AhnLab CPS PLUS: OT 환경 연결 확대로 주목도 ↑

그 동안, OT 환경은 외부에서의 접근이 엄격히 통제되는 폐쇄성으로 인해 IT 환경과 비교해 상대적으로 안전하다고 여겨져 왔다. 하지만, 디지털화가 빠르게 진행되고 IT 영역과의 접점이 늘어나면서 OT 환경에 대한 사이버 공격도 증가하고 있다. 따라서, OT에 대한 보안의 중요성이 높아진 것은 물론 OT와 IT를 연계한 새로운 통합 보안 접근이 필요한 상황이다.

안랩은 OT 엔드포인트와 네트워크 그리고 OT와 연결된 IT 환경까지 폭 넓게 보호하는 통합 CPS 보안 플랫폼 'AhnLab CPS PLUS'를 통해 최신 보안 요구사항에 대응하고 있다. 특히, AhnLab CPS PLUS는 전 세계적으로도 가장 넓은 보안 커버리지를 제공하며, 제조, 정유, 운송 등 다양한 산업군에서 고객 레퍼런스를 활용하고 있다.




[사진 5] AhnLab CPS PLUS 구조도

안랩은 이번 행사에서 AhnLab CPS PLUS의 전체적인 구조와 개념을 소개하고, 플랫폼을 구성하는 핵심 솔루션인 ▲AhnLab EPS(OT 엔드포인트 보안) ▲AhnLab XTD(OT 가시성 및 위협 탐지) ▲AhnLab ICM(CPS 보안 중앙 관리)에 대한 시연을 진행했다. 참관객들은 OT 환경의 외부 접점이 늘어나면서 새로운 보안 접근이 필요하다는 사실에 깊이 공감했고, 특히 솔루션 중앙 관리를 통해 보안 효율성을 더하는 AhnLab ICM, 시스템 변경을 방지해 운영 안정성을 더하는 AhnLab EPS의 Lock Mode 기능에 주목했다. 또한, 실제 시연한 솔루션 외에도 감염된 설비를 치료하는 'AhnLab Xcanner'와 일방향 데이터 전송 솔루션 'AhnLab Data Diode'에 관해서도 다양한 문의가 이어졌다.


[사진 6] AhnLab CPS PLUS 설명

AhnLab CPS PLUS 소개 및 시연을 들은 방문객과는 플랫폼의 기본적인 내용 뿐만 아니라 제조, 항만, 데이터센터 등 당사자가 속한 조직의 산업군 활용 사례(use case)에 대해서도 구체적인 논의를 이어갔다. 이를 통해, 한국 뿐만 아니라 전 세계적으로도 OT와 IT를 연계한 보안 요구사항이 늘어나고 있음을 확인할 수 있었다. 안랩은 다양한 국가 고객들의 도전과제 해결을 위해 AhnLab CPS PLUS와 구성 솔루션들의 고도화를 지속하고 고객 및 잠재 고객들과의 소통 접점을 확대해 나갈 계획이다.

►AhnLab CPS PLUS 소개 페이지 바로가기

## AhnLab TIP: 안랩만의 차별화된 위협 인텔리전스

고도화된 사이버 위협이 국경을 넘나들면서 각국 기업 및 기관들에게 차세대 위협 인텔리전스 확보가 점점 더 중요해지고 있다. 전 세계적으로 활동하는 공격 그룹의 최신 동향과 이들의 공격 기법을 선제적으로 파악하면, 보안 의사결정을 최적화하고 조직 전체의 보안 태세를 강화할 수 있기 때문이다.

안랩은 부스를 찾은 방문객들에게 자사 위협 인텔리전스 플랫폼 'AhnLab TIP'를 시연하고, AhnLab TIP의 특장점인 아시아권 공격 그룹 분석 역량과 안랩만이 제공하는 침해지표(IOC)의 가치를 강조했다. 안랩은 위협 인텔리전스만 제공하는 타사와 달리 다양한 보안 솔루션을 운영하면서 탐지한 위협 데이터를 바탕으로 안랩만의 IOC를 제공한다. 여기

에 업계 최고 전문가들로 구성된 위협 인텔리전스 조직 ASEC(AhnLab SEcurity intelligence Center)의 전문성을 더해 공격 그룹의 동향과 기법을 정교하게 분석한다.


[사진 7] AhnLab TIP 시연

방문객들은 AhnLab TIP의 대표적인 특장점 외에도 최근 보안 위협의 주요 화두로 떠오른 다크웹에 대한 모니터링, 효과적인 모바일 스캠 대응 역량을 제공하는 클라우드 샌드박스 기능 등 AhnLab TIP가 지원하는 여러 기능들을 높이 평가했다.

►AhnLab TIP 소개 페이지 바로가기

## AhnLab XDR: AI 기반 효율적인 리스크 관리

최근, 조직들의 공격 표면이 확대되고 운영하는 보안 솔루션 수가 늘어나면서 보안 부서가 느끼는 부담도 커지고 있다. 특히, 코로나19 팬데믹 이후 원격 근무 환경까지 보호해야 하는 상황을 맞이하면서 보안 복잡성 문제가 심화되고 있다. 실제로, 많은 조직들이 여러 이기종 솔루션의 관리 분산과 물리적으로 감당하기 힘든 양의 알림(alert)에 대한 피로를 호소하고 있다.

이 문제는 한국 뿐만 아니라 전 세계 조직들이 공통적으로 겪고 있는 사항으로, 안랩은 이번 행사에서 위협 분석 및 대응 플랫폼 'AhnLab XDR'을 소개 및 시연하며 해결 방안을 제시했다. AhnLab XDR은 조직이 보유한 자산을 '사용자(User)'와 '기기(Device)'를 기준으로 식별하고, 다양한 보안 요소들을 반영한 공식을 기반으로 조직의 리스크 지수를 0~100점으로 산출한다. 이를 통해, 사용자는 조직의 리스크 현황을 직관적으로 파악할 수 있다.


[사진 8] AhnLab XDR 시연

또한, 오픈 XDR(Open XDR)을 지향하는 AhnLab XDR은 자사 솔루션 뿐만 아니라 타사의 이기종 솔루션까지 유연하게 연동 가능하다. 이를 통해, 여러 보안 영역에서 데이터를 수집 및 분석하고 최적의 대응 방안을 제시한다. 특히, 플레이북(Playbook)을 활용해 체계적인 대응 과정을 자동화할 수 있다는 점에서 사용자들의 좋은 반응을 얻었다.

이 밖에, 방문자들은 AhnLab XDR에 탑재된 생성형 AI 'AhnLab Annie AI'에도 많은 관심을 보였다. AhnLab Annie AI는 안랩의 고품질 데이터를 학습한 사이버보안 특화 생성형 AI로 조직의 실시간 리스크 현황 파악 등 다양한 영역에서 사용자가 보안을 효율적으로 운영할 수 있도록 지원한다. 안랩은 AhnLab Annie AI를 곧 AhnLab XDR에 정식 탑재해 시장에 선보일 예정이다.

►AhnLab XDR 소개 페이지 바로가기

## 전문가 발표 세션: 실제 사례 분석으로 큰 호응 얻어

행사 2일차에는 ASEC 최수진 선임연구원이 'Leaning from Cyber Incidents: Real-World Attacks(실제 공격 사례로부터 우리가 배워야 할 것)'를 주제로 전문가 스피치 세션을 진행했다.

최수진 선임은 사이버 공격이 단순한 피싱 이메일부터 제로데이 취약점 등 여러 경로를 통해 시작되며, 공격 목적 역시 개인정보를 훔치거나 금전적 이득을 취하는 것부터 국가나 대기업의 정보를 노리는 것까지 다양하다고 설명했다. 그리고, 사이버 공격의 방식과 그로 인한 결과가 각각 다르다는 점을 이해해야 한다고 강조했다.


[사진 9] 최수진 선임연구원 발표 세션

이어서, ASEC에서 분석을 진행한 네 가지 실제 사례의 주요 내용과 시사점을 공유했다.

**#1. 보안 관리가 취약했던 OT 환경이 외부와 연결되면서 발생했던 침해 사례:** 작은 보안 허점도 조직의 방어 체계를 손상시킬 수 있다. 특히, 공장 등 OT 환경은 지속적인 보안 업데이트 적용이 어려워 관리에 더 유의해야 한다.

**#2. 과거 감행되었던 사이버 공격으로 인해 몇 년 후 실제 해킹을 당한 사례:** 사이버 공격은 서로 단절되어 있지 않고 복잡하게 상호 연결되어 있다. 초기 침해가 발생하면, 이후 공격의 가능성을 열어주게 되고, 공격자는 최초 침해를 활용해 TTPs(Tactics, Techniques and Procedures)을 연계할 수 있다.

**#3. 피싱을 통해 다중 인증(MFA)을 우회하여 피해자의 데이터와 자산을 탈취한 사례:** 공격자들은 사용자와 합법적인 서비스 간 통신을 가로채 유효한 세션 정보를 캡처하고 MFA를 우회하는 AITM(Adversary in the Middle) 기법을 사용한다. 예방을 위해서는 장치 기반 인증을 강제하고, 의심스러운 로그인 활동을 모니터링하면서 이상 활동 탐지 시 모든 세션을 종료해야 한다.

**#4. 중앙 관리 솔루션을 해킹해 조직의 엔드포인트를 감염시킨 사례:** 중앙 관리 소프트웨어가 악의적인 목적으로 사용되면 조직 전체가 영향을 받게 된다. 따라서, 신뢰할 수 있는 솔루션과 기능을 사용하고 로그를 정기적으로 감사해야 한다. 또한, EDR과 같은 보안 솔루션을 통해 의심스러운 활동을 지속적으로 모니터링 및 추적해야 한다.


[사진 10] 발표 세션은 가득 메운 참관객들

최수진 선임연구원의 발표는 실제 사례를 상세하게 분석했다는 점에서 참관객들의 깊은 공감을 이끌어냈다. 실제 발표 현장은 순식간에 만원이 되었으며, 발표 후 많은 참관객들이 소셜미디어 포스팅을 통해 해당 세션을 호평했다.

## 맺음말

안랩은 다양한 국가에서 개최되는 주요 컨퍼런스에 참여하며 글로벌 사이버보안 동향을 확인하고 잠재 고객들과의 접점을 넓히고 있다. 또한, 행사를 통해 얻은 인사이트를 자사 제품 및 기술에 반영하여 솔루션을 고도화하고 고객들의 안전한 비즈니스 환경 조성을 위해 지속적인 노력을 기울이고 있다.

이번 행사를 총괄한 안랩 이상국 마케팅본부장은 "이번 행사에서 동남아시아 현지 기업/기관 관계자들과 다수의 미팅을 진행하며 '통합' 관점의 안랩 보안 솔루션과 서비스에 대한 현지의 높은 관심을 확인했다"며, "앞으로도 다양한 방식으로 동남아시아 고객들과 소통하며 글로벌 인지도를 지속적으로 높여갈 것"이라고 말했다.

**AhnLab**

콘텐츠기획팀 신재만 과장