보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

K 사이버 보안의 인기, 그 현장 속으로

AhnLab 2023-11-06

안랩은 10월 17~19일 3일간 싱가포르 샌즈 & 엑스포 컨벤션 센터(Sands Expo & Convention Center)에서 열린 글로벌 보안 컨퍼런스 'GovWare 2023'에 참가해 현지 보안 산업 관계자에게 ▲XDR ▲위협 인텔리전스 ▲통합 OT 보안에 대한 안랩의 글로벌 전략 솔루션 및 서비스를 소개했다.

컨퍼런스 현장 모습과 이번 행사를 통해 확인한 글로벌 주요 보안 트렌드들을 소개한다.

안랩은 Govware 2023에서 'Detect, Respond and Evolve, Security Powered by AI(탐지, 대응 그리고 진화, AI로 더 강력해진 보안)'를 주제로 ▲SaaS형 XDR(확장된 탐지 및 대응)플랫폼 'AhnLab XDR' ▲차세대 위협 인텔리전스(TI, Threat Intelligence) 플랫폼 'AhnLab TIP' ▲OT 보안 솔루션 'AhnLab EPS' 및 'CEREBRO-XTD' 등 안랩의 글로벌 전략 솔루션을 소개했다.

[사진 1] Govware 2023 안랩 부스 전경

Govware는 '싱가포르 국제 사이버 위크(Singapore International Cyber Week)' 기간 동안 싱가포르 사이버 보안국(Cyber Security Agency of Singapore) 주관으로 매년 개최되는 글로벌 보안 컨퍼런스다. 2022년 행사 기준 65개국 약 10,000명이 이 행사를 방문했다.

[사진 2] Govware 2023 입장을 기다리는 참가자들

[사진 3] Govware 2023에 참가한 기업들의 전시부스

이번 Govware 2023에는 약 300여개의 기업이 참여해 'Fostering Trust Through Collaboration in the New Digital Reality(새로운 디지털 현실에서 협업을 통한 신뢰 증진)'를 주제로 약 28개의 기조 강연 및 트랙 발표, 제품 전시 등을 진행했다.

글로벌 사이버 보안 트렌드, 핵심은 'AI'와 '협력'

행사 둘째 날에는 여러 사이버 보안 업계 리더들이 연사로 나서 기조연설을 진행했다. 각 기조연설에서는 다양한 주제들이 다뤄졌는데, 공통적으로 AI와 협력이 현대 보안의 핵심이라는 점에서 맥을 같이 했다.

[사진 4] 에바 첸(Eva Chen) 트렌드마이크로 CEO

에바 첸(Eva Chen) 트렌드마이크로 CEO는 'Defying Cybercriminals: Trust, Innovation, and Resilience in the Digital Age'를 주제로 한 기조연설에서 급격하게 변화하는 디지털 환경에서의 AI 활용 방안, 공격자와 방어자의 관점 차이, 사이버 리스크 관리의 중요성 및 비즈니스 회복력을 갖추는 방법 등에 대해 설명했다.

에바 첸 CEO는 "공격자들은 사이버 공격을 유기적인 '지도(map)'으로 생각하는 반면, 방어자들은 사이버 보안을 단순 체크 리스트로 생각하는 경향이 있다. 고도화된 최신 공격을 효과적으로 방어하기 위해서는 공격자들의 여러 관점과 기법에 효과적으로 대응할 수 있는 중앙화된 보안 플랫폼이 필요하다."고 강조했다.

이어서, "공격 표면이 늘어나고, 보안 복잡성이 심화되면서, 경영진의 사이버 리스크 관리가 필요해졌다. SaaS 애플리케이션, 공급망, 원격 근무 등으로 인한 공격 표면은 서로 연결되어 있어, 리스크 우선순위를 선별하는 것이 굉장히 중요하다."라며, "이를 사람이 전부 처리할 수 없기 때문에 AI가 필요하다. 또한, 하나의 기업이 모든 보안을 제공하는 것은 불가능하기 때문에 사이버 보안 커뮤니티의 적극적인 협력이 필요하다."고 말했다.

[사진 5] 샘 루빈(Sam Rubin) 팔로알토 네트웍스 Unit 42 글로벌 운영 책임자

샘 루빈(Sam Rubin) 팔로알토 네트웍스 Unit 42 글로벌 운영 책임자는 기조연설 'Navigating the Crossroads of AI and Cybersecurity'에서 공격자들의 동향과 이를 방어하는 기업/기관 입장에서 AI의 역할에 대해 설명했다.

샘 루빈은 "공격자들을 공격의 각 단계에서 더 빠르게 움직여 목표를 달성한다. 조직의 네트워크에 침투하고 나면, 해당 환경을 충분히 정찰 및 학습하여 공격의 성공률을 높인다."며, "AI는 사람의 개입을 최소화 하면서 고도화된 공격을 방어한다. AI를 '올바르게' 활용하면 위협 탐지와 대응 효율성을 개선하고, 보안 부서는 그들이 정말 해야 할 일에 보다 집중할 수 있게 된다."고 말했다.

안랩의 글로벌 전략 솔루션, 참가자들의 이목을 집중시키다

XDR, 위협 인텔리전스 및 OT 보안 솔루션을 소개 및 시연한 안랩의 부스에는 APAC 지역내 고객사, 사이버보안 유관 정부 및 협회 관계자, 시장 조사기관, 파트너 등 수백여 명의 보안업계 관계자들이 방문했다. 참관객들은 안랩의 글로벌 전략제품 전반에 대해 높은 관심을 보였으며, 안랩은 부스 방문 참관객을 대상으로 전시 솔루션의 특장점 등을 소개하고, 시연과 상세한 상담을 제공했다.

#1. AhnLab XDR

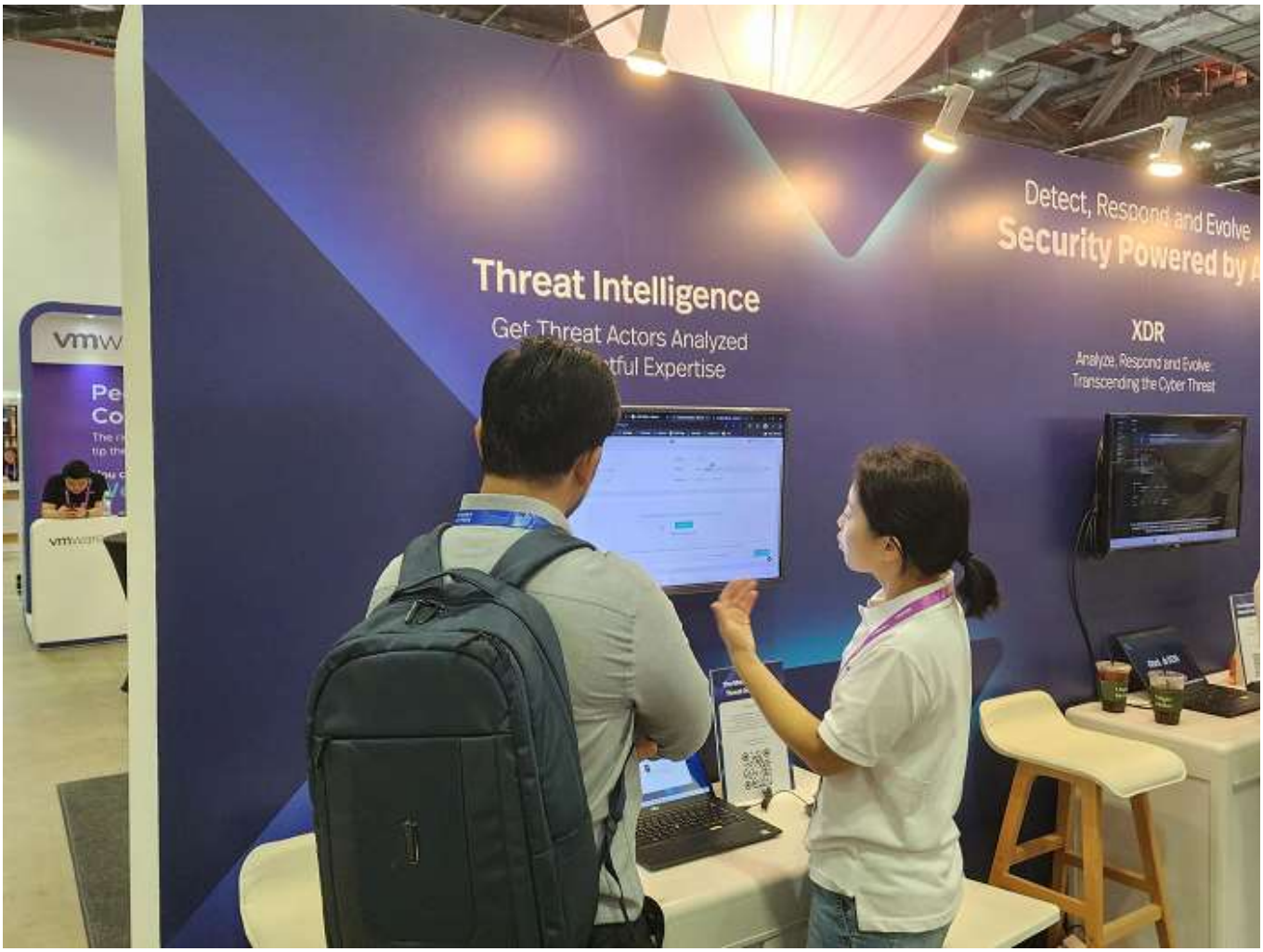
AhnLab XDR은 조직 내 수많은 시스템으로부터 위협정보를 수집해 분석•탐지•대응을 제공하는 SaaS형 '보안 위협 분석 플랫폼'이다. 보안 담당자가 실제 업무 과정에서 겪는 어려움을 제품에 적극 반영한 것이 특징으로, ▲사용자와 자산 중심 리스크 지수화 및 관리 ▲안랩의 축적된 위협대응 노하우가 녹아있는 '시나리오 룰'을 활용한 리스크 분석•대응 ▲위협 인텔리전스 연동으로 위협이 조직에 미치는 영향도 파악 등 보안 업무의 효율성을 높일 수 있는 기능을 제공한다.

[사진 6] AhnLab XDR 부스 시연

부스를 방문한 보안업계 관계자들은 'AhnLab XDR'에 큰 관심을 나타냈다. 특히, 안랩 XDR이 제공하는 '실전형' 시나리오 룰과 이를 고객사에 최적화할 수 있는 커스터마이징 기능, 데이터 허브를 이용한 이기종 데이터 연동 등이 관계자들의 호응을 얻었다.

#2. AhnLab TIP

AhnLab TIP는 안랩이 축적한 보안위협 대응 기술력과 노하우를 집약한 차세대 위협 인텔리전스 플랫폼이다. ▲악성코드 및 취약점, 포렌식 보고서 ▲최신 보안뉴스, 보안권고문 ▲보안 콘텐츠 관련 위협침해지표(IoC, Indicators of Compromise) 기반의 위협 유형, 악성 파일정보, IP, URL ▲DDW(Deep&Dark Web) 모니터링 기능 등 포괄적인 위협 인텔리전스 서비스를 제공한다. 이외에도 사용자가 업로드한 의심 파일/URL에 대해 다차원 행위 분석으로 결과를 제공하는 '클라우드 샌드박스 분석' 기능과 API 제공 기능으로 안랩 제품 외에도 다양한 보안 관리 솔루션과 쉽게 연동이 가능한 점이 특징이다.



[사진 7] AhnLab TIP 부스 시연

부스를 방문해 시연을 본 참가자들은 AhnLab TIP가 제공하는 다양한 글로벌 공격그룹에 대한 분석 정보와 높은 수준의 위협 인텔리전스(위협 유형, 악성 파일정보•IP•URL 등)에 주목했다. 또한, 안랩 TIP의 API(응용프로그램 인터페이스)를 이용한 기존 솔루션과 손쉬운 연동에 대한 발표를 듣고 관련 상담을 이어갔다.

#3. OT 보안 프레임워크

안랩은 지난 2021년 7월 인수한 OT 보안 전문기업 '나온웍스'와 함께 통합 OT 보안 프레임워크를 고도화 해왔다. 안랩과 나온웍스의 솔루션은 보안 프레임워크 하에서 필요한 역할을 수행하며 시너지를 낸다. 사용자 입장에서는 OT 환경 전계층에 걸쳐 '식별 > 탐지 > 대응'으로 이어지는 보안 프로세스를 구축하여 강력한 보안과 관리 효율성을 확보할 수 있다.

[사진 8] OT 보안 부스 시연

이번 행사에서 안랩은 통합 OT 보안 프레임워크의 주축인 AhnLab EPS와 CEREBRO-XTD를 전시 및 시연했으며, 솔루션 도입에 대한 구체적인 상담도 다수 진행했다. 부스를 방문한 OT 업계 관계자들은 안랩과 나온웍스의 OT보안 프레임워크에 대한 설명을 듣고 엔드포인트•네트워크•OT프로토콜 분석기술을 융합한 차별화된 가시성과 보안 위협 탐지 및 대응 역량에 많은 관심을 보였으며, 도입 방안 등에 대한 상담도 진행했다.

안랩 이상국 마케팅본부장은 "이번 행사에서 많은 APAC지역 현지 기업과 기관, 보안업계 관계자들이 안랩 부스를 찾아 자사의 차별화된 보안 역량을 경험했다"며, "안랩은 향후에도 다양한 방식으로 APAC 지역의 고객과 소통을 이어나가 글로벌 시장 확대에 박차를 가할 것"이라고 말했다.

한편, 안랩은 APAC 지역에서 다수의 고객사를 확보하며 입지를 강화하고 있다. 안랩은 △말레이시아 국책은행, 대형보험사 등 금융권에 지능형 위협 대응 솔루션 'AhnLab MDS' 제공 △태국 지역 내 반도체 공장에 OT보안 솔루션 'AhnLab EPS' 제공 △싱가포르 정부기관 재난망 모바일 단말기에 'V3 모바일 엔터프라이즈' 공급 등 APAC 지역 내 다양한 국가에서 공공기관 및 기업을 대상으로 비즈니스를 활발히 진행 중이다.

AhnLab 콘텐츠기획팀 신재만 과장