AhnLab ISF 2024: AI와 통합 보안으로 이루는 혁신

가을이 무르익을 무렵, 안랩은 최신 보안 트렌드를 관통하는 맞춤형 보안 전략을 준비해 고객사 보안 담당자들과 만남의 시간을 가졌다. 지난 9월 26일, 그랜드 인터컨티넨탈 호텔에서 안랩의 통합 보안 컨퍼런스 'AhnLab ISF 2024'가 개최됐다. 올 한 해 안랩은 글로벌 트렌드에 맞춰 보안 솔루션 및 AI 기술 고도화, 플랫폼 기반 연동 강화 등에 집중해왔다. 이번 행사 역시 AI와 통합 보안에 대한 보다 구체적이고 핵심적인 보안 전략을 소개하는 자리로 꾸며졌다. 그 현장의 모습을 함께 들여다보자.

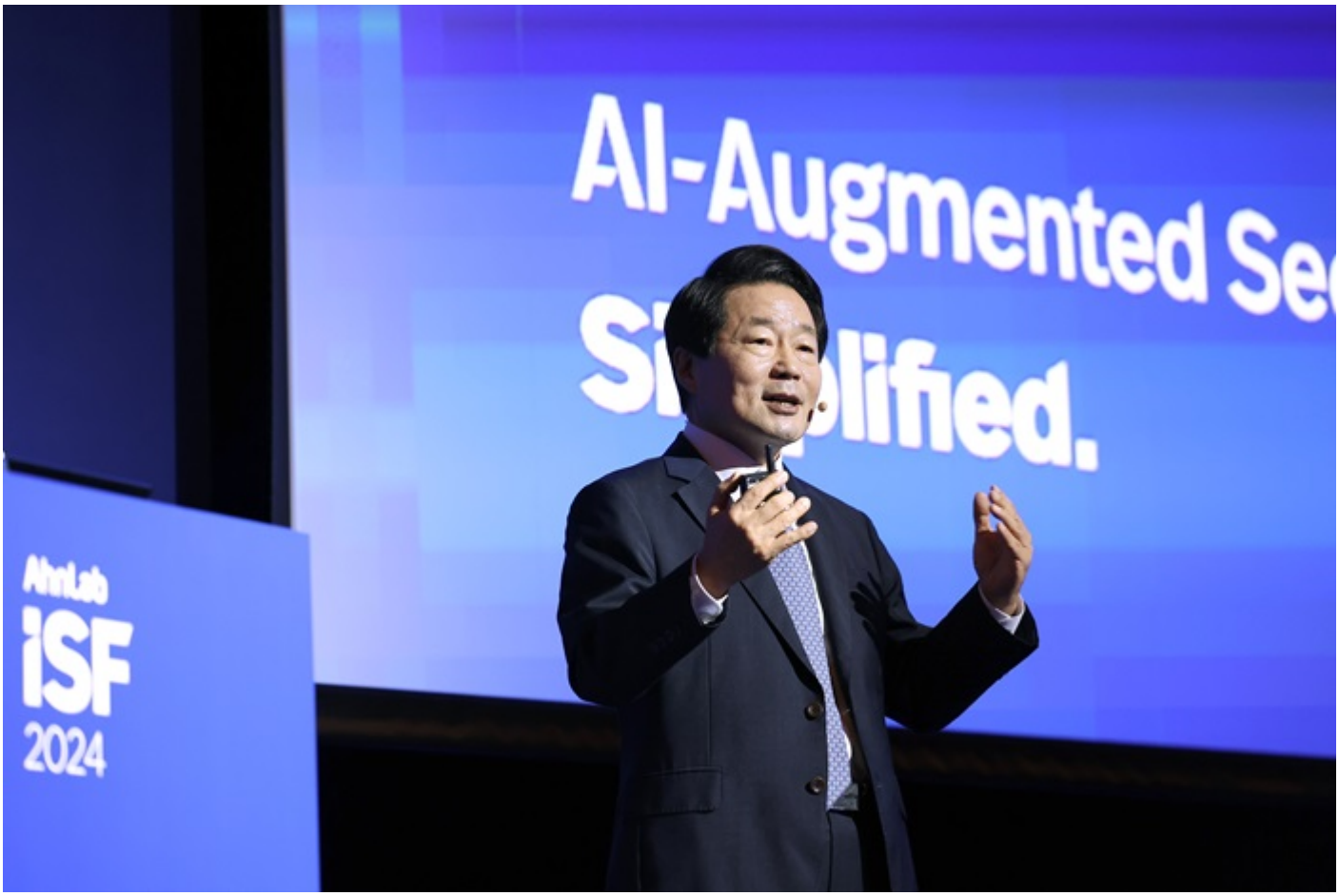
AhnLab ISF 2024에서는 'AI-Augmented Security. Simplified. (AI를 적용해 보안을 단순화한다)'라는 슬로건 아래, AI를 활용해 더 강력하고 단순한 보안을 구현하기 위한 방안을 소개했다. 안랩 강석균 대표의 인사말을 시작으로, 전성학 연구소장, 김창희 제품서비스기획실장의 기조 연설, 그리고 ▲능동적인 위협 예측(**P**roactive) ▲유연한 연동(**L**ow-friction) ▲통합 플랫폼(**U**nified)을 주제로 설명하는 트랙(Track) 발표 세션이 진행됐다.

[사진 1] AhnLab ISF 2024 입장을 기다리는 참가자들

강석균 대표는 인사말에서 안랩이 지난 수 년 동안 자사 제품과 플랫폼에 다양한 방식으로 AI 기술을 적용해 탐지 및 대응 역량을 강화하고 있다고 말했다. 강석균 대표는 "최근 사이버 위협 고도화, 보안 복잡성 심화에 대응하기 위한 핵심 트렌드로 '인공지능(AI)'과 '보안 운영 효율성(Efficiency)'이 주목받고 있다. 안랩 역시 통합을 기반으로 보안 효율성을 강화해 고객의 비즈니스 생산성을 높이는 것을 목표로 삼고, 그 연장선에서 AI 기술을 고도화하고 있다"라고 강조했다.

이어, "오늘 공식 석상에서 처음 소개하는 'AhnLab PLUS'는 엔드포인트와 네트워크, 클라우드, 서비스, 보안 운영, CPS(Cyber-Physical System) 등 총 6개 플랫폼을 융합한 통합 보안 플랫폼으로, ▲능동적인 위협 예측(Proactive)과 ▲유연한 연동(Low-friction) ▲통합 기반 시너지(Unified) ▲강력한 보안(Secure) 등 4가지 지향점에 따라 제품 간, 플랫폼 간 통합을 지속적으로 발전시켜 고객사의 비즈니스 생산성 향상에 기여할 것이다"라고 말했다.

또한, 강석균 대표는 제품과 기술 통합 외에 사람 및 조직 간 협력의 중요성도 강조했다. 강석균 대표는 "하나의 조직이 모든 보안 도전과제를 해결하는 데 한계가 있기에 여러 조직이 힘을 합쳐 진화하는 위협에 대응해야 한다. AhnLab ISF 2024가 이 연대를 이끄는 핵심적인 역할을 하기를 바란다"라고 덧붙였다.



[사진 2] 강석균 안랩 대표는 통합 보안 플랫폼의 필요성과 조직 간 협력의 중요성을 역설했다.

강석균 대표의 인사말이 끝나고, 안랩 전성학 연구소장이 '생성형 AI의 위협과 AI를 활용한 미래의 보안'을 주제로 기조 연설을 진행했다. 전성학 연구소장은 AI 기술, AI를 활용한 공격이 발전하면서, AI를 활용해 미래의 보안을 안전하게 이끌어 가는 방안을 공유했다.

전성학 연구소장은 공격자가 AI를 피싱 메일 유포, 악성코드 제작, 딥페이크 영상 제작 등 AI를 기반으로 하는 보안 위협이 급속도로 증가하고 있으며, 이들 위협을 방어하려면 방어자 관점에서 AI 기술을 탑재한 보안 솔루션으로 공격을 어떻게 탐지할 것인지 지속적으로 고민해야 한다고 조언했다.

전성학 연구소장은 "안랩은 AhnLab EDR, MDS, V3 모바일 시큐리티(V3 Mobile Security), XDR 제품에 AI 기술을 적용해 URL 정보, 이벤트 로그 등을 학습시켜 악성 행위와 피싱 메일, 행위 기반 이상 징후 탐지를 통해 위협 인텔리전스를 제공하고, 선제적으로 대응한다. AhnLab XDR의 경우 AI 시큐리티 어시스턴트(AI Security Assistant)인 생성형 AI 'AhnLab Annie AI'를 활용할 수 있다. AhnLab Annie AI는 프롬프트를 입력하면 퇴근 시간 동안의 보안 이벤트 발생 및 조치, 보고서 출력 여부 등 사용자의 보안 운영을 지원하는 역할을 한다"고 설명했다.

[사진 3] 안랩 전성학 연구소장은 생성형 AI를 활용한 위협에 대응하기 위한 구체적 방안을 공유했다.

두 번째 기조 연설자 안랩 김창희 제품서비스기획실장은 'Empowering the Future of Cyber Security: Everything Everywhere All at Once'에 대해 발표했다. 해당 세션은 급변하는 비즈니스 환경에서 조직이 직면한 도전과제와 안랩이 제시하는 해결 방안에 중점을 뒀다.

김창희 실장은 "사이버 위협이 진화하는 가운데 클라우드 사용 증가, 원격 근무 활성화, 공격 표면 확대 등이 한꺼번에 일어나면서, 대다수 조직이 효율적인 보안 운영, 생산성 향상에 어려움을 겪고 있다. 이를 극복하려면 '통합'이 핵심이다. AhnLab PLUS는 엔드포인트와 네트워크, 클라우드 등 다양한 보안 플랫폼이 중앙 관리 역량을 기반으로 운영되며, AhnLab XDR이 최상위에 위치해 여러 보안 영역의 데이터를 수집하고 분석함으로써 최적의 리스크 관리 방안을 제시한다"라고 말했다.

또한, 김창희 실장은 "이에 더해, 안랩은 엔드포인트와 클라우드, 서비스 영역 각각에 디바이스 제어, 컨테이너 보안, 매니지드 탐지 및 대응(MDR) 등 새로운 제품과 서비스를 추가해 AhnLab PLUS 플랫폼을 발전시켜 나가고 있다. 그리고 제로 트러스트 접근 제어(ZTNA), 공격 표면 관리(ASM) 서비스 등 미래 지향적인 오퍼링을 통해 보안 복잡성을 해소하고, 고객들의 업무 환경을 안전하게 보호할 것이다"라고 밝혔다.

[사진 4] 안랩 제품서비스기획실 김창희 실장은 비즈니스 환경에서 보안 위협에 대응하기 위한 해결책을 제시했다.

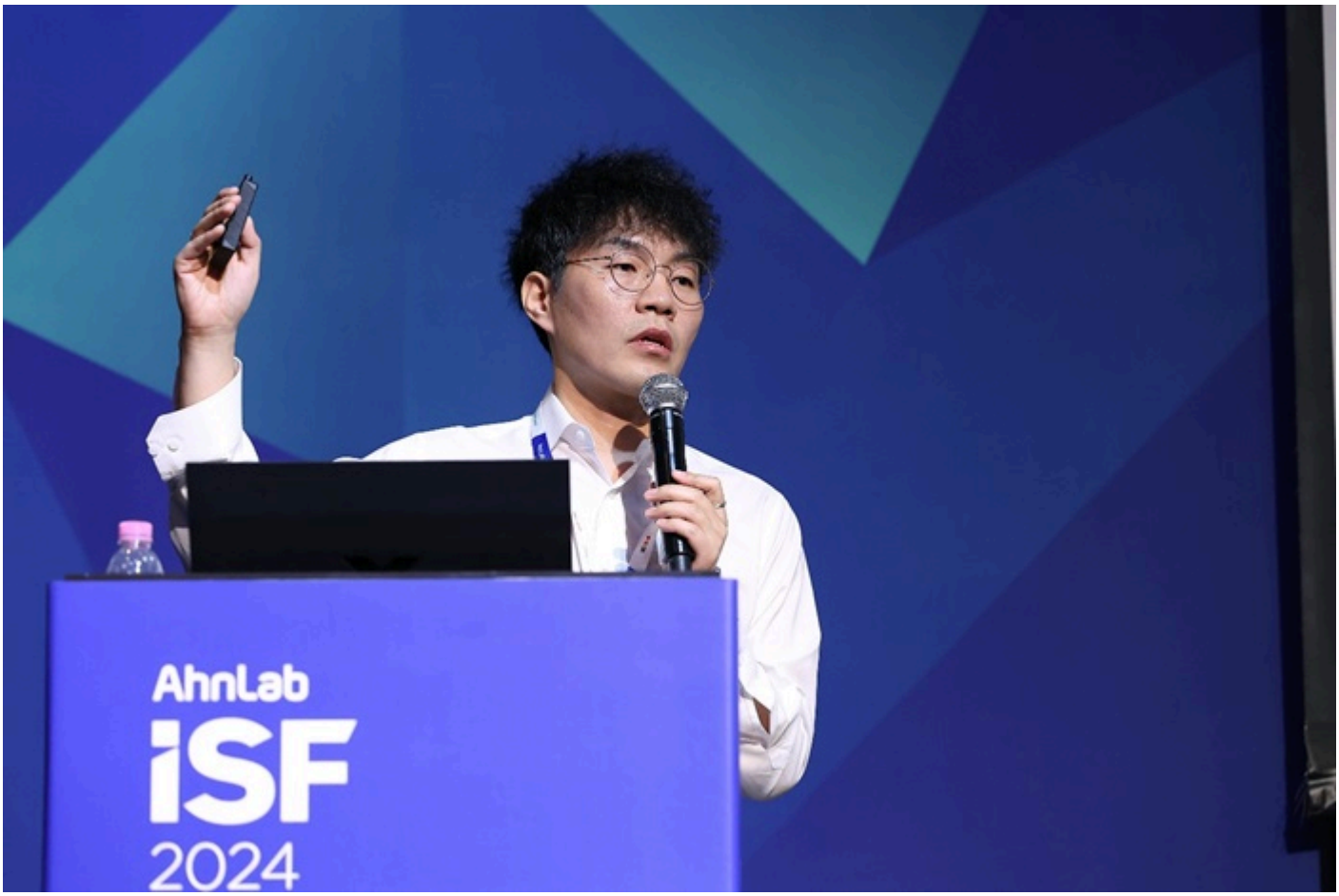
Protect Today for Resilient Tomorrow: 오늘의 안전이 내일의 회복력을 만든다

안랩 A-FIRST팀 이명수 팀장은 'Ransomware ran somewhere'을 주제로 2024년 3분기까지의 랜섬웨어 동향과 침해 사고 사례, 대응 방안에 대해 발표했다.

이명수 팀장은 "최근 취약점을 이용한 랜섬웨어 공격이 급증하고 있는데, 대표적인 사례로는 ESXi, 스크린 커넥트(ScreenConnect), 클릭 센스(Qlik Sense), 윈도우(Windows), PHP 등의 소프트웨어 취약점 공격 등이 있다. 특히 ESXi는 VM웨어에서 만든 가상 머신으로, 랜섬웨어에 감염될 경우 시스템 전체가 동작하지 않게 되어 피해자는 협상에 응할 수밖에 없다. 이런 이유로 많은 공격자가 ESXi를 주요 표적으로 삼고 있다"라고 경고했다.

이명수 팀장은 랜섬웨어에 대응하려면 사전 준비, 실시간 방어, 침해 탐지, 사고 대응 등의 프로세스를 갖추는 것은 물론, 한국인터넷진흥원(KISA)과 안랩에서 제공하는 랜섬웨어 대응 가이드를 참고하고 최신 동향과 대응 방법을 지속적으로 확인해야 한다고 당부했다.

이명수 팀장은 "마크 트웨인의 유명한 격언, '주식 투자는 매월 조심해야 한다'라는 말처럼, 랜섬웨어 보안 역시 항시 경계심을 늦춰서는 안 된다"라고 말했다.



[사진 5] 안랩 A-FIRST팀 이명수 팀장은 올해 3분기까지의 랜섬웨어 트렌드와 랜섬웨어 대응 전략을 소개했다.

'보안에서의 AI: AI-Augmented Security'라는 주제로 발표를 맡은 안랩 인공지능팀 이승경 팀장은 LLM을 비롯한 AI 기술을 접목한 보안 기술이 나아갈 방향을 제시했다. 특히 보안과 AI의 교집합을 통해 AI를 보안에 적용하는 방법, 보안 운영의 어려움을 해소하는 데 있어 AI의 역할을 강조했다.

이승경 팀장은 "보안에서도 데이터 규모와 복잡성이 큰 문제로 작용하는데, 예전 빅데이터 시대처럼이런 문제를 해결하는 데 AI가 대안이 될 수 있다. 보안 운영에서 발생하는 다양한 문제는 AI로 증강된 보안을 통해 해결할 수 있으며, 안랩의 AI는 공통 모델을 기반으로 하는 서비스 플랫폼 형태로 이를 제공하고 있다"라고 말했다.

이승경 팀장은 보안 운영에서 직면하는 두 가지 주요 문제로 '위협 과부하'와 '보안 툴 복잡성'을 꼽았다. 이 문제를 AI로 해결할 수 있는 방안에 대해 "위협 과부하 문제는 AI가 수동적이고 반응적인 탐지 방식에서 벗어나 능동적으로 잠재적 위협을 조기에 발견한다. 데이터를 분석해 이상 행동을 감지하고, 이를 통해 보안 분석가는 더 효과적으로 잠재적 위협에 대응할 수 있다. 보안 툴 복잡성의 경우, AI를 통해 사용자의 프로세스를 단순화할 수 있다. 기존 보안 툴은 복잡한 메뉴를 통해 사용자가 직접 분석해야 했지만, AI 어시스턴트는 필요한 데이터를 자동으로 분석하고 적절한 대응책을 제안할 수 있어, 보안 전문가가 툴 사용에 대한 부담을 줄이고, 본연의 업무에 집중할 수 있다"라고 설명했다.

[사진 6] 안랩 인공지능팀 이승경 팀장은 AI 기술을 접목한 보안 기술이 나아갈 방향을 설명했다.

안랩 융합제품서비스기획팀 이건용 팀장은 'f(X)D+R=0perational Efficiency, AhnLab XDR' 발표 세션에서 AhnLab XDR을 통해 보안 담당자가 보다 효율적인 보안 운영 환경을 구축해 비즈니스 경쟁력을 높일 수 있는 방안을 소개했다.

이건용 팀장은 AhnLab XDR이 ▲로그 통합 연계 분석 ▲리스크 탐지 및 알림 ▲대응 등 크게 세 가지 측면에서 효율화를 지원한다고 밝혔다. 이건용 팀장은 "AhnLab XDR은 다양한 출처의 데이터를 수집하고 통합 분석해 보안 담당자가 잠재 위협을 조기에 발견하도록 하며, 불필요한 알림을 줄이고 ML(Machine Learning) 기반의 행위 탐지 기술을 활용함으로써 더 위험한 알림을 발견한다. 이 밖에, AI 모델을 기반으로 추천 및 자동 대응을 지원하며, 향후 선보일 MXDR(Managed XDR) 서비스를 통해 보안 담당자의 업무 효율성을 향상시키는데 중점을 두고 있다"라고 말했다.

이건용 팀장은 "AhnLab XDR은 모든 리스크를 분석하고 대응함으로써 리스크를 '제로' 상태로 만드는 것을 목표로 한다. 현재 서비스 중인 퍼블릭 클라우드뿐만 아니라 올 하반기에는 프라이빗 클라우드로 지원을 확대할 계획이다"라고 밝혔다.

[사진 7] 안랩 융합제품서비스기획팀 이건용 팀장은 AhnLab XDR을 통해 비즈니스 경쟁력을 높일 수 있는 방안을 소개했다.

실제로 AhnLab XDR을 도입한 안랩 고객사, 골프존 보안 담당자의 발표도 진행됐다. 골프존 정보보안팀 김정훈 팀장은 골프존의 AhnLab XDR 도입 배경과 운영 노하우를 소개했다.

김정훈 팀장은 "AhnLab XDR이 EDR과 쉽게 연계할 수 있고, SaaS 방식으로 신속한 구축이 가능하다는 점에 주목했다. 골프존은 인터넷망, IDC, AWS, 전자금융망 등 다양한 네트워크에 설치된 EDR을 XDR로 통합 관리하고 있으며, 덕분에 보안 위험이 크게 감소했다. 이는 XDR을 활용한 위협 이벤트 연계 분석, 근본적인 원인 해결을 통해 가능했던 것이라고 생각한다"라고 말했다.

김정훈 팀장에 따르면, 골프존은 AhnLab XDR을 도입한 후 악성 의심 IP 차단, VPN 이상 로그인 차단, BruteForce 공격 차단, 방화벽 정책 고도화 외에도 보안 솔루션 로그 상관관계 분석을 통한 직관적이고 유의미한 결과 도출 등의 효과를 경험했다.

김정훈 팀장은 "XDR을 사용한다고 해서 모든 위험이 자동으로 해결되는 것은 아니며, 위험의 우선순위를 설정하고 직접 대응해야 하는 부담은 여전히 존재한다. 이에, 골프존은 AhnLab MDR을 함께 도입해 엔드포인트에서 발생하는 위협을 관리하고 있으며, 외부 전문가의 실시간 모니터링과 대응 지원을 받아 보안 팀의 업무 부담을 줄이고 있다"라고 언급했다.

[사진 8] 골프존 정보보안팀 김정훈 팀장은 자사 시스템에 AhnLab XDR을 도입함으로써 얻은 보안 효과를 소개했다.

안랩 양하영 ASEC 실장은 'Inside Out: The Anxiety(불안) in Cyber Threat Intelligence'를 주제로 발표를 맡았다. 양하영 실장은 우리가 보안에서 불안을 느끼는 이유는 위협이 도사리고 있는 것을 알지만, 언제, 어디서, 어떻게 침해가 일어날지 모르기 때문이라고 설명했다. 이는 위협을 미리 알고 예방할 수 있다면 보안 담당자들이 느끼는 불안도 줄어든다는 것을 의미한다.

해당 관점에서 양하영 실장은 최신 위협 동향을 ▲취약점 공격 ▲피싱 공격 ▲인포스틸러(InfoStealer) 세 가지 분류로 소개했다. 각 공격 유형에 대해 실제 발생했던 사례와 ASEC(AhnLab SEcurity intelligence Center)이 분석한 내용을 공유했다. 또한, 안랩의 위협 인텔리전스 플랫폼 AhnLab TIP가 최신 위협에 대해 어떤 위협 인텔리전스를 제공하는지도 함께 다뤘다.

양하영 실장은 "AhnLab TIP는 위협이 발생한 뒤 대응하는 다른 보안 솔루션들과 다르게 위협을 사전에 식별해 예방하는 사전 대응 관점으로 접근한다. 단순히 분석 보고서 등의 콘텐츠만 제공하는 것이 아니라 ▲침해지표(IOC) 피드 ▲위협 그룹 분석 ▲샌드박스 분석 ▲다크웹 모니터링 등 기업 및 기관이 사이버 위협을 선제적으로 이해하고 예방하는 데 도움이 되는 다양한 기능들을 제공하고 있다"라고 강조했다.

[사진 9] 안랩 양하영 ASEC 실장은 안랩의 CTI(Cyber Threat Intelligence)를 활용해 불안한 사이버 위협에 대비하는 방안을 공유했다.

Simplify and Secure: Seamless Security Solutions: 매끄러운 보안 솔루션으로 구현하는 보안 간소화

안랩 오상언 솔루션컨설팅본부장은 'Why and How to Adopt CTEM(Continuous Threat Exposure Management)' 발표 세션에서 CTEM이 위협 환경 제어, 조직의 보안 강화를 위한 핵심 전략임을 강조했다.

오상언 본부장에 따르면, 재택근무 증가와 클라우드 환경 도입 등으로 보안 관리 영역이 확대됨에 따라, 기존의 데이터센터 및 오피스망 중심 보안에서 벗어나 더 넓은 영역을 포괄하는 보안 관리가 필요하다. CTEM은 이런 환경에 대응하기 위한 새로운 접근법으로, 공격 표면을 사전에 파악하고 우선순위를 정해 지속적으로 관리하는 전략이다.

오상언 본부장은 "CTEM의 핵심은 사전 예방적 보안 관리다. 이는 단순히 보안 솔루션을 도입하는 것을 넘어, 조직의 자산에 대한 노출된 위험을 지속적으로 모니터링하고 관리하는 것을 의미한다. 특히 취약점 관리와 패치 관리 같은 기본적인 조치를 소홀히 해서는 안 된다"라고 당부했다.

또한, "안랩은 CTEM 개념을 AhnLab XDR에 적용하고 있다. 이를 통해 AhnLab XDR은 엔드포인트, 네트워크, 클라우드 등 다양한 영역의 보안 솔루션을 통합하고, 여기에 취약점 정보와 위협 인텔리전스를 연계해 종합적인 위험 관리가 가능하다. 이뿐만 아니라 자동화된 대응과 위험의 우선순위 설정을 통해 보안 팀의 업무 효율성을 높이고, 필요에 따라 MXDR 서비스 형태로 제공해 조직의 보안 역량을 강화할 수 있다"라고 덧붙였다.

[사진 10] 안랩 솔루션컨설팅본부 오상언 본부장은 위협 환경 제어 및 조직 보안 강화에 있어 CTEM이 핵심임을 강조했다.

안랩 원남호 기술지원본부장은 '밤 '새운'거야? 밤새 '운'거야?(feat. Work Diet)'라는 제목으로 세션 발표를 진행했다. 해당 세션에서는 안랩의 엔드포인트 보호 플랫폼, 'AhnLab EPP'를 활용해 보안 위협에 대응하고 업무 효율을 높이는 방안을 다뤘다.

AhnLab EPP는 백신, 패치 관리, 개인정보 보호, 디바이스 제어, EDR 등 다양한 보안 기능을 단일 에이전트로 통합 관리할 수 있는 플랫폼이다. 이를 통해 사용자 PC의 부담을 줄이고 관리 효율성을 향상시킬 수 있다. 특히, '연계 규칙'으로 보안 이벤트에 대한 자동화된 대응을 할 수 있어 보안 관리자의 수동 개입 최소화 및 신속한 대응이 가능하다.

원남호 본부장은 "AhnLab EPP은 취약한 소프트웨어를 자동으로 탐지하고 제거하거나 업데이트함으로써 기업의 전반적인 보안 상태를 개선하는 데 크게 기여한다. 이 외에도 백신의 실시간 검사 상태 확인, 악성코드 탐지 시 자동 격리, 개인정보 유출 의심 행위 탐지 등 다양한 시나리오에 대해 자동화된 대응 규칙을 설정할 수 있다"라고 설명했다.

이에 덧붙여, "AhnLab EPP는 보안 패치나 엔진 업데이트의 안전한 배포를 위한 점진적 배포 기능을 제공한다. 이 기능을 활용하면 패치나 업데이트를 단계적으로 적용해 잠재적인 문제를 미리 파악하고 대응함으로써 기업의 엔드포인트 보안 관리에 안정성을 더할 수 있다"라고 말했다.

[사진 11] 안랩 기술지원본부 원남호 본부장은 AhnLab EPP를 활용한 보안 위협 대응 및 업무 효율성 향상 방안에 대해 발표했다.

안랩 박태환 ACSC 본부장은 'MDR과 함께해요'를 주제로 조직에서 흔히 발생하는 사이버 위협 시나리오와 함께, MDR 도입을 통해 조직이 얻을 수 있는 구체적인 이점을 공유했다.

박태환 본부장은 "그동안 조직에서 확인된 대표적인 사이버 위협으로는 공격자의 무차별 대입 공격에 의한 랜섬웨어 유포 사건, 이메일에 숨겨진 추적 픽셀을 활용한 피싱 공격 시도, 정품 인증 우회 소프트웨어 KMSAuto에 숨겨진 악성코드로 인한 피해 사례 등이 있다. 이처럼 기업은 다양한 사이버 위협에 노출돼 있지만, MDR 서비스를 통해 안랩의 전문 분석 인력의 도움을 받을 수 있다. MDR 팀은 고객사의 곁에서 위협을 분석하고 대응 방안을 제시한다. 더 나아가, MDR 프리미엄 서비스에서는 위협 심층 상세 분석 및 능동적인 위협 헌팅 서비스도 제공한다"라고 밝혔다.

박태환 본부장은 네트워크 연결 불가 환경, 클라우드 환경 등 다양한 사례에서 MDR 서비스 지원이 가능한 점을 강조했다. 박태환 본부장에 따르면, 서비스 도입 검토 시 안랩의 영업 담당자와 상담을 통해 기업 환경에 맞는 서비스 방안을 모색할 수 있다.

박태환 본부장은 "안랩 MDR 서비스를 통해 급변하는 IT 환경을 노린 각종 사이버 위협에 선제적으로 대응하고, 조직의 보안 태세를 한 단계 업그레이드할 수 있을 것이다"라고 제언했다.

[사진 12] 안랩 박태환 ACSC 본부장은 AhnLab MDR 서비스 도입을 통해 조직이 얻을 수 있는 이점을 소개했다.

Manage Less, Defend More: 관리보다 방어에 집중하라

'Endpoint? And Point Security!!'라는 주제로 발표를 진행한 안랩 전략제품서비스기획팀 정광우 부장은 하이브리드 업무 환경에 최적화된 워크스페이스 보안 (Workspace Security) 전략과 엔드포인트 보안 통합 및 연계, 연동 방안을 소개했다.

정광우 부장은 "업무 환경이 확대됨에 따라 엔드포인트 보안의 요구사항도 변화했다. 따라서 이제는엔드포인트와 연결된 인프라 전반에 걸친 포괄적인 보안 제어가 필요하다"라고 지적했다.

정광우 부장은 워크스페이스 보안을 위한 엔드포인트 보안의 필수 요건으로 ▲ Platform-based ▲ User-centric ▲Integration을 제시했다. 이와 관련해, 정광우 부장은 "안랩은 AhnLab EPP를 기반으로 확장된 가시성과 대응, 관리 및 운영 복잡성 감소 등을 구현하며 최적의 엔드포인트 보안을 제공하고 있다. 또한, 이 AhnLab EPP는 사용자 정보가 담긴 서버 및 DB와 연동해 사용자 정보를 기반으로 단말을 식별하는 유연한 접근법을 이용한다. 더 나아가, 다양한 이기종 보안 제품 연계 및 연동이 가능한 syslog와 API도 제공한다"라고 설명했다.

정광우 부장에 따르면, 엔드포인트 보안 측면에서 무엇보다도 중요하게 고려돼야 할 것은 바로 'Consolidation'과 'Integration'이다. 이 두 가지를 사용자 관점에서 어떻게 활용하고 제공할 것인지를 고민해야 할 것이다.

[사진 13] 안랩 전략제품서비스기획팀 정광우 부장은 엔드포인트 보안에 중점을 두고, 하이브리드 업무 환경에 최적화된 워크스페이스 보안 전략을 설명했다.

안랩 융합제품서비스기획팀 윤병성 차장의 'Network PLUS: A to Z AhnLab ZTNA' 발표 세션에서는 제로 트러스트 도입을 위해 알아야 할 기본 개념과 AhnLab ZTNA의 현재와 미래를 중점적으로 다뤘다.

윤병성 차장은 "제로 트러스트 도입을 위한 핵심 요소는 ▲식별자 및 신원 ▲기기와 엔드포인트 ▲네트워크 ▲시스템 ▲응용 및 워크로드 ▲데이터이며, 이들을 관통하는 교차 기능으로는 ▲가시성 및 분석 ▲자동화 및 통합이 있다. 제로 트러스트의 성숙도 단계는 '기존', '향상', '최적화'로 구분되는데, 단기간에 최적화 수준으로 이행하는 것은 불가능하다. 따라서 '준비 – 계획(설계) – 구현(도입) – 운영'의 제로 트러스트 도입 단계를 수 차례 반복해야만 제로 트러스트 고도화가 가능하다."라고 말했다.

또한, 윤병성 차장은 AhnLab ZTNA에 대해 ZTNA 정책과 규칙 설정, 인증, 디바이스 확인을 담당하는 'ZTNA Manager'와 연결 및 접근 제어, 모니터링을 수행하는 'ZTNA Gateway'가 설치돼 있으며, 이 둘은 물리적으로 분리돼 있다고 설명했다. 즉, 제어 영역과 데이터 영역이 완전히 나눠져 있어 더 강력한 보안을 제공한다는 것이다.

윤병성 차장은 "이 두 영역에 안랩의 방화벽 어플라이언스인 XTG를 비롯해 EPP 에이전트(Agent), ESA(EPP Security Assessment), V3를 연동하면 훨씬 더 다양한 디바이스 정보를 수집할 수 있다. AhnLab ZTNA는 향후 하이브리드 클라우드 및 망 분리, 자사 및 원격 접속 환경에 폭넓게 구축될 수 있다"라고 덧붙였다.

[사진 14] 안랩 융합제품서비스기획팀 윤병성 차장은 제로 트러스트 및 ZTNA의 개념과 도입 방안을 소개했다.

안랩 클라우드개발실 노영진 상무는 '컨테이너 중심의 클라우드 보안: SBOM과 eBPF를 활용한 최신 보안 전략'을 주제로 SBOM 및 런타임 보안 전략을 기반으로 안전한 컨테이너 운영 방안을 제시했다.

노영진 상무는 "클라우드의 핵심인 유연한 운영에 가장 중요한 역할을 하는 요소는 바로 '컨테이너'다. 그런데 이 컨테이너는 오픈소스에 대한 가시성이 없고 발견되지 않은 취약점이 존재하며, 도스(DoS) 공격을 통해 무력화될 위험이 있다. 그런 까닭에 컨테이너를 보안을 강화하려면 기존 커널 보안 외에 체계적인 오픈소스 관리를 위한 SBOM(Software Bill of Materials)이 필요하다"라고 강조했다.

또한, 노영진 상무는 "개발 및 공급망 단계에서 막지 못하는 보안 리스크의 경우 런타임 보안으로 해결해야 한다. 런타임 보안은 최신 컨테이너 환경에서의 실시간 모니터링과 제어를 통해 더욱 안전한 환경을 구성한다. 이 밖에, 보안 모듈이 강력한 중앙 통제가 가능하면서도 블루스크린(BSOD) 이슈 없이 안전한 보안 적용을 위해서는 eBPF도 필수적이다. 단, eBPF를 보안 요구사항에 맞춰 다양하게 적용할 수 있어야 할 것이다"라고 제언했다.

[사진 15] 안랩 클라우드개발실 노영진 상무는 안전한 컨테이너 환경 조성을 위한 SBOM과 런타임 보안의 필요성을 강조했다.

안랩 융합제품서비스기획팀 황재훈 부장은 'Continuous Puzzle Games in CPS World'에 대한 발표를 진행했다. CPS(Cyber-Physical System) 환경의 다양한 보안 이슈와 동향을 소개하고, 이에 대한 안랩의 대응 전략을 공유했다.

황재훈 부장에 따르면, CPS 환경에는 많은 기술과 디바이스가 퍼즐 조각처럼 얽혀 있다. 따라서 보안취약점 또한 매우 다양하며, 이에 대한 대응 역량도 아직은 부족한 실정이다. 게다가 최근에는 공격자들이 IT와 OT 환경을 모두 노린 위협과 AI 기술을 활용한 공격도 증가하고 있어, 보안 위험성이 더 가중되고 있다.

황재훈 부장은 CPS 보안은 크게 ▲가시성 ▲탐지 ▲대응 측면에서 고려돼야 한다고 언급했다. 안랩 또한 현재 이 세 가지를 모두 지원한다.

황재훈 부장은 "CPS 환경에서 운영에 영향을 주지 않으면서 가시성을 효과적으로 확보하는 가장 좋은 방법은 네트워크 트래픽을 기반으로 분석하는 것이다. 별도 에이전트를 설치하지 않더라도 패킷만 수집되면 자산을 식별할 수 있기 때문이다. 여기에 더해, 엔드포인트 기반 식별을 병행하면 보다 향상된 가시성을 확보할 수 있다. 그리고, CPS 보안 자산에 대한 엔드포인트 하드닝을 통해 자산에서 사용되는 프로세스와 이동식 매체, 네트워크 통신에 대해 허용 리스트(Allow List)를 기반으로 사전에 등록된 것들만 허용하도록 제어하면 랜섬웨어, APT 공격 등 신□변종 위협으로부터 자산을 효과적으로 보호할 수 있다"라고 조언했다.

[사진 16] 안랩 융합제품서비스기획팀 황재훈 부장은 CPS 환경의 고도화되는 보안 위협에 대응하는 방법을 소개했다.

모든 발표 세션이 끝나고, 안랩은 경품 추첨을 진행하며 한껏 달아오른 행사 분위기를 더욱 고조시켰다. 이와 더불어, 행사장 로비에는 안랩과 안랩 자회사의 글로벌 전략 제품 및 서비스를 직접 체험할 수 있는 시연 부스가 마련됐다. 부스를 방문한 참가자에게는 안랩 보안 솔루션의 효과적인 도입을 위한 맞춤형 상담도 제공했다.

[사진 17] 행사장 로비의 데모 부스에서 제품을 시연하는 모습 (1)

[사진 18] 행사장 로비의 데모 부스에서 제품을 시연하는 모습 (2)

맺음말

올해로 16년차를 맞은 AhnLab ISF 2024는 AI와 통합 보안이라는 키워드를 중심으로 수 많은 참가자들과 보안 인사이트를 공유할 수 있었던 연대의 장이었다. 참고로, AhnLab ISF의 정식 명칭은 AhnLab Integrated Security Fair인데, 안랩은 16년 전부터 통합의 중요성을 강조해 왔으며 앞으로도 AI와 같은 신기술 및 자사 플랫폼을 고도화해 고객들의 비즈니스 생산성 향상에 기여할 계획이다. 서두에 언급한 바와 같이 이제 하나의 기업이 모든 사이버 위협을 해결할 수 없는 상황인 만큼, 안랩을 포함해 더 많은 기업 및 기관들이 함께 협력하여 진화하는 위협에 슬기롭게 대응해 나가길 바란다.

AhnLab

콘텐츠기획팀 서보경 사원