# 보안 이슈

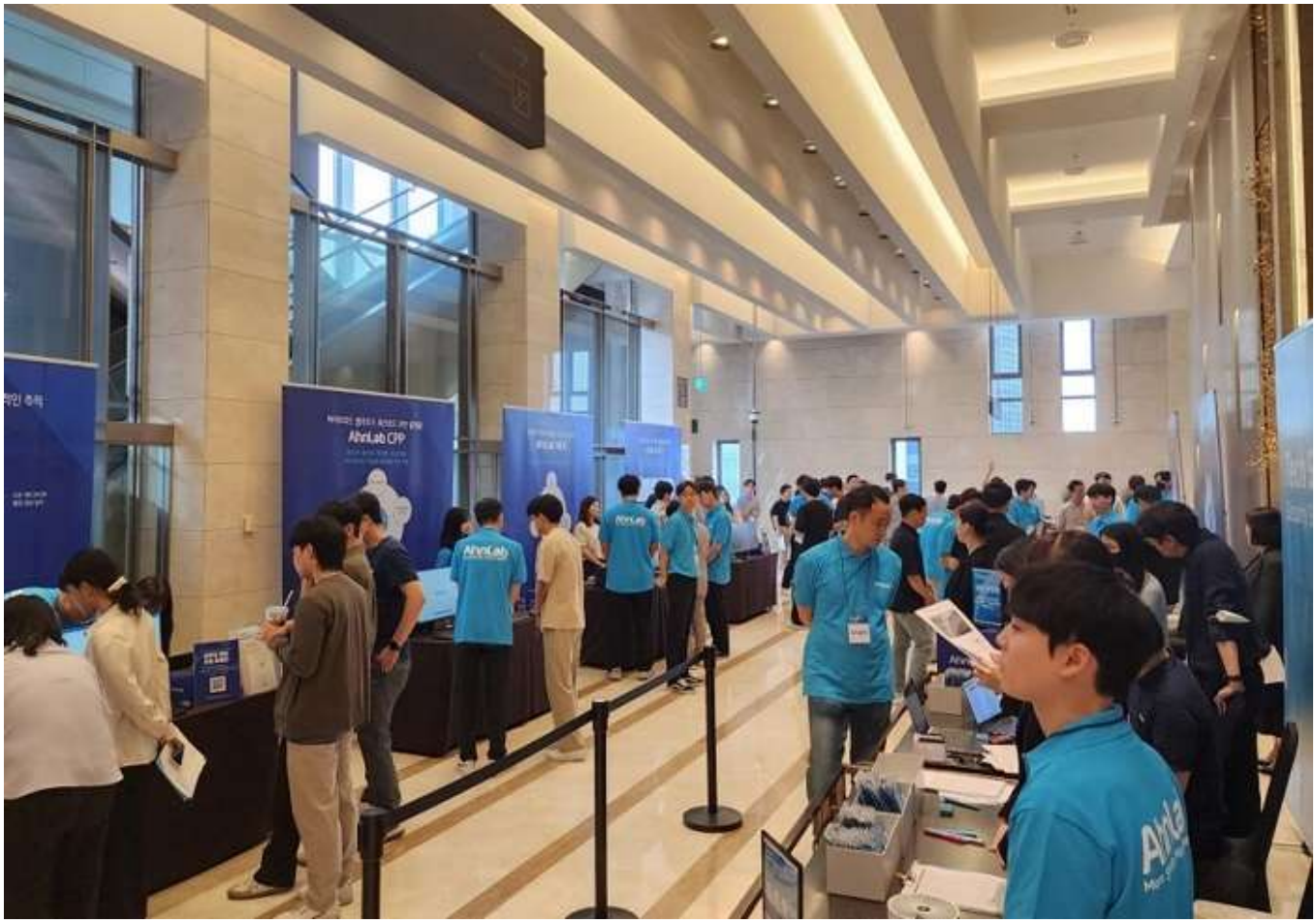
AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

## 보안 실무자라면 꼭 알아야 할 실전 위협 대응 방안

AhnLab 2023-07-03

6월 15일 안랩이 양재 엘타워에서 보안 실무자를 위한 기술 중심 보안 세미나 '안랩 테크 서밋 2023(AhnLab Tech Summit 2023)'을 4년 만에 오프라인으로 개최했다. 이번 행사는 안랩이 고객사 보안 실무자와 팀장 200여 명을 대상으로 실전 위협 대응 전략을 제시하고, 고객 실 사용 사례를 소개하며 자사 제품을 업무에 더 효율적으로 사용하는 방안을 공유하는 자리였다. 그 현장 속으로 가 보자.

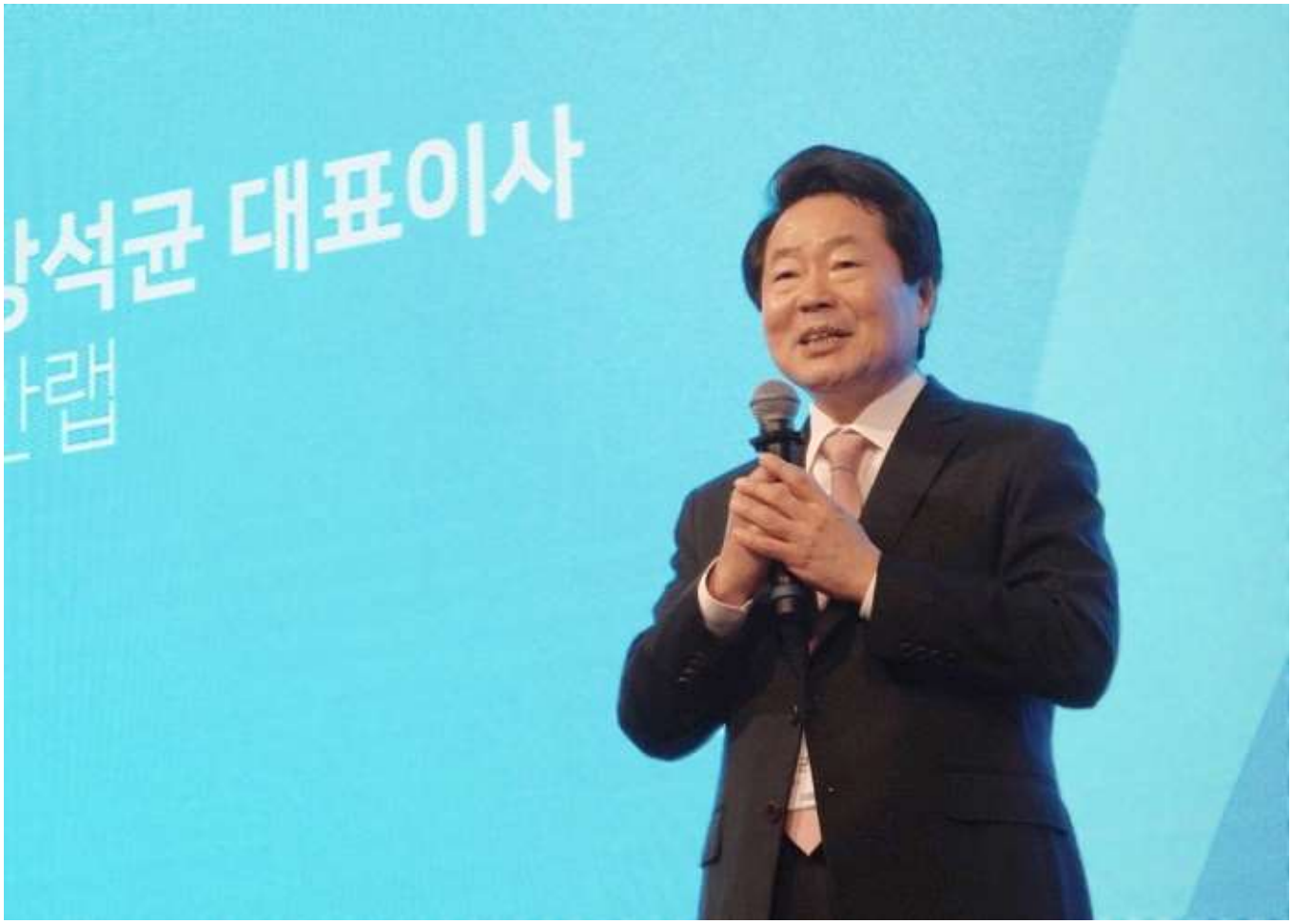

안랩 테크 서밋 2023에서는 ▲침해사고 사례 공유: 누구나 그럴 듯한 계획을 가지고 있다. 침해 당하기 전까지는 ▲최근 언급되고 있는 XDR은 무엇이며, 안랩은 XDR을 준비하고 있을까? ▲바쁘다 바빠 현대사회(Feat. Work Diet) ▲효율적인 정보보호 업무를 위한 EDR 적용 사례 ▲랜섬웨어 이제 그만 ▲최신 DDoS 공격 동향 및 방어 전략 ▲데이터를 통해 알아보는 보안위협 재해석 등 7개 발표 세션을 진행했다.




[사진 1] 안랩 테크 서밋 2023 행사장 로비

행사는 안랩 강석균 대표의 인사말을 시작으로 막을 열었다. 강석균 대표는 최근 안랩이 이룬 성과에 대해 "안랩은 새 버전의 EDR(Endpoint Detection and Response) 제품과 클라우드 보안 솔루션을 시장에 공급하고 고도화를 이루었다. 또, 작년 10월부터 MDR(Managed Detection and Response) 서비스를 EDR과 함께 제공해오고 있으며, 글로벌 보안 평가인 마이터 어택(MITRE ATT&CK) 평가에서도 우수한 성적을 거두며 안랩의 기술력을 증명했다"라고 설명했다.

강석균 대표는 "올해 들어 챗GPT(ChatGPT)와 같은 생성형 AI와 XDR(Extended Detection and Response) 등 새로운 기술이 등장한 가운데, 다양한 형태의 보안 위협에 맞서 강력하고 효과적인 보안 운영을 고민하는 보안 담당자들에게 안랩의 노하우를 전수하는 유익한 시간이 되기를 바란다. 앞으로도 안랩의 축적된 사이버 보안 경험을 공유하는 기회를 지속적으로 마련할 계획이다"라고 말했다.

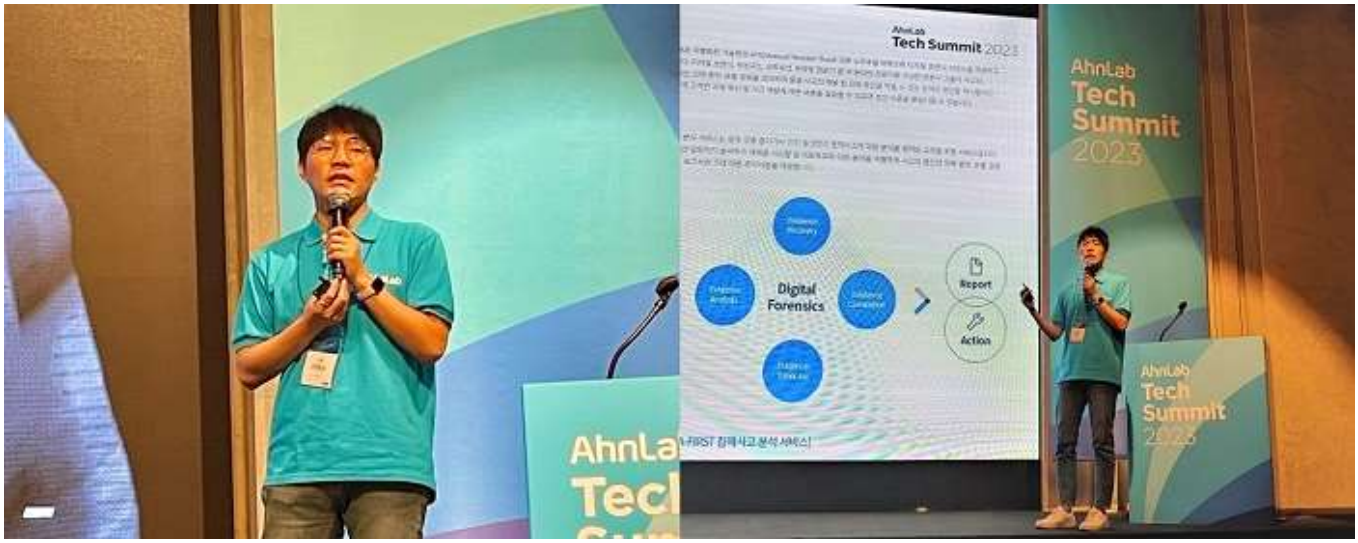


[사진 2] 안랩 강석균 대표가 안랩의 위협 대응 전략과 사용자 경험을 공유할 기회를 지속적으로 마련해 나갈 것이라고 발표했다.

뒤이어 안랩 ASEC 분석팀 이명수 수석 연구원이 안랩의 침해사고 분석 전문 조직 'A-FIRST'가 침해사고를 분석한 최신 사례를 바탕으로 랜섬웨어 피해를 최소화하는 방법을 제시했다.

이명수 수석 연구원은 "최근 랜섬웨어 공격은 APT(Advanced Persistant Threat) 공격과 유사하게 공격자의 사이트 확보 및 시스템 정보 수집을 시작으로 최초 침해 시스템을 거쳐 조직 전체로 피해를 확산시킨 다음, 최종 단계에서 데이터를 유출하고 랜섬웨어에 감염시키는 프로세스를 따른다. 따라서 조직 전체로 피해가 확산되는 시점, 즉, 공격자의 측면 이동(Lateral Movement) 단계에서 위협을 탐지하고 차단해야만 피해를 줄일 수 있다"라고 지적했다.

또한, "최근 들어 라자루스(Lazarus) 공격 그룹의 활동도 심상치 않다. 전체 피해 규모를 파악하기 힘들 정도로 국내 여러 업체가 라자루스의 공격을 받았다. 이에 대비해 소프트웨어 패치 적용 여부와 악성파일 탐지 및 C2 서버 접근 이력 등을 점검하고, 지속적인 모니터링과 분석이 필요하다"라고 강조했다.




[사진 3] 안랩 ASEC 분석팀 이명수 수석이 최신 침해사고 사례와 피해를 최소화하기 위한 보안 담당자의 대응 방법을 제시했다.

안랩 전략제품서비스기획팀 이건용 부장은 작년부터 보안 업계의 주요 키워드로 부상한 XDR의 등장 배경과 함께, 안랩은 XDR을 어떻게 준비하고 있는지에 대해 발표했다.

이건용 부장은 "보안 환경이 기존 경계 중심에서 클라우드 기반으로 변화하면서 보안 사일로(Silo)화가 진행되고 조직이 각 영역에 최고의 제품을 도입하고 있는 가운데, XDR은 다수의 이기종 보안 솔루션을 효율적으로 운영하기 위한 대안으로 등장했다"라고 말했다.

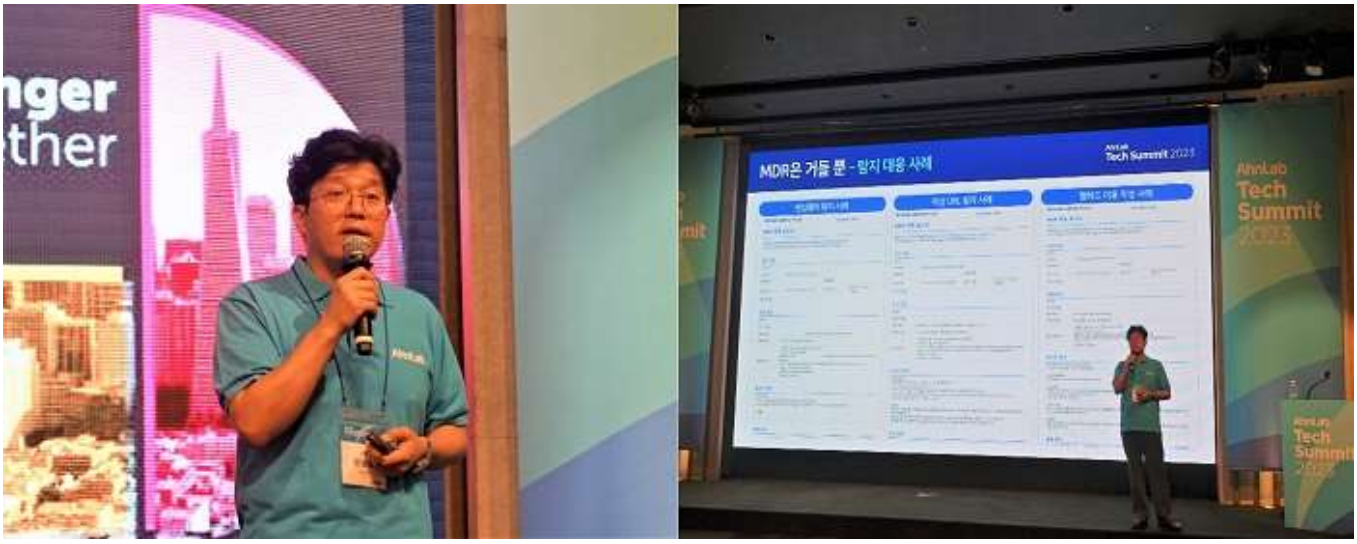
안랩은 'AhnLab XDR' 솔루션 출시를 앞두고 있다. 이건용 부장은 "AhnLab XDR은 SaaS 서비스 형태로 제공되는 리스크 분석 플랫폼으로, 고객사의 엔드포인트, 네트워크, 애플리케이션, 서드파티 등 이기종 시스템에서 수집한 데이터를 통합하고, 공통 스키마 형태로 정규화해 악성 및 이상 행위 탐지, 리스크 스코어링, 연계 솔루션을 통한 자동 대응을 수행한다"라고 설명했다.

[사진 4] 안랩 전략제품서비스기획팀 이건용 부장이 출시 예정인 AhnLab XDR의 기능을 간단히 소개했다.

안랩 기술지원본부 원남호 상무는 안랩 솔루션을 활용해 워크 다이어트를 실현한 고객 사례를 소개했다.

원남호 상무는 "보안 담당자는 여러 솔루션을 운영하는 데 부담을 느끼고 있으며, 통합 보안 관리, 자동화를 통한 업무 간소화 등 효율적인 보안 운영 방안을 고민하고 있다. 이에 안랩은 AhnLab EDR과 AhnLab MDR을 연계해 이슈가 발생한 PC에 대한 상세 정보를 제공하고, 탐지된 로그를 분석해 대응 및 권고 사항까지 제시한다. 악성 URL 탐지

에 있어서는 AhnLab MDS와 AhnLab TrusGuard 간 연동을 통해 차단 룰(Rule)을 자동으로 적용한다. 또한, 최근 안랩이 출시한 'SOAR Basic'은 안랩 제품 간 연동 및 내장된 전용 플레이북을 통해 위협에 통합적으로 대응하고 운영을 자동화한다"라고 말했다.




[사진 5] 안랩 기술지원본부 원남호 상무가 안랩 제품을 도입해 '워크 다이어트'에 성공한 사례를 발표했다.

부산은행의 보안 담당자 김민준 대리는 AhnLab EDR을 도입해 효과적인 정보보안을 달성한 사례를 발표했다.

김민준 대리는 "AhnLab EDR은 다른 프로그램에 우선해 시스템 자원을 확보하고 탐지 및 대응 활동을 수행할 수 있는 권한 확보에 있어 우위를 가지며, 탐지/대응 기법의 적정성과 효율성, 침해사고 대응 조직 여부와 수준 등 다양한 측면에서 악성코드와 싸워 이길 수 있는 요건을 모두 충족한다. 부산은행에서는 AhnLab EDR을 공격 이벤트 교차 분석, APT 공격 시나리오 이해, 탐지 및 대응 자동화 업무에 주로 사용하고 있으며, 추가 활용 포인트로는 사용자 정의 악성행위 차단, PC 침투 및 제어 행위 위험 평가가 있다"라고 설명했다.

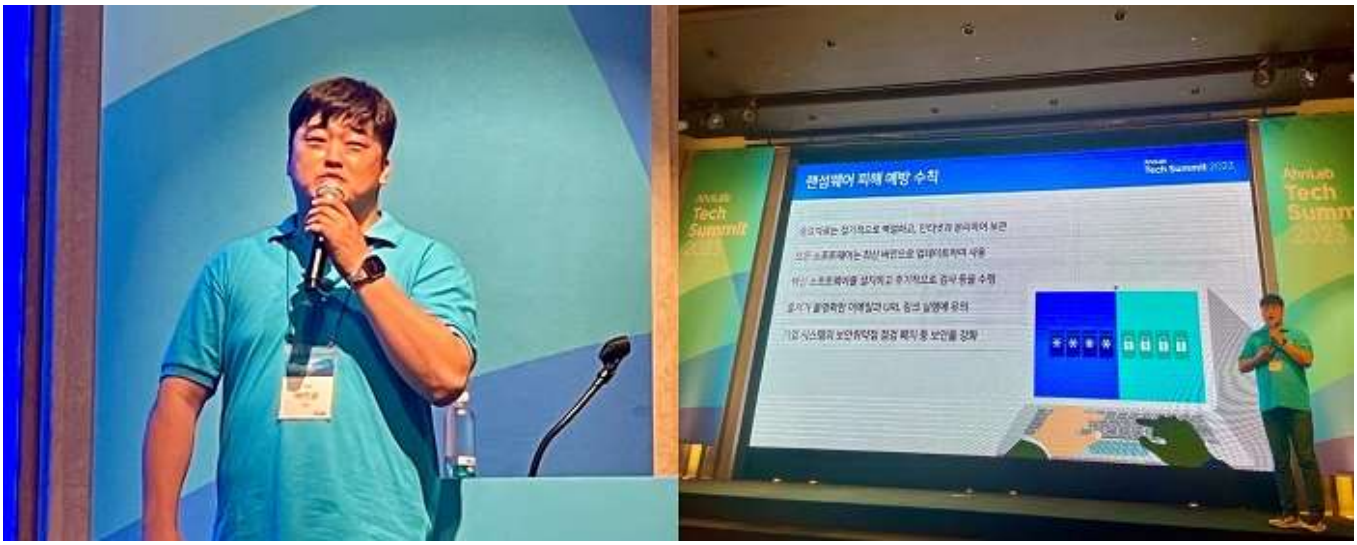
[사진 6] 부산은행 김민준 대리가 AhnLab EDR 도입 및 활용 팁을 공유했다.

그 다음으로, 안랩 EP 기술지원2팀 배연용 차장이 랜섬웨어 공격을 효과적으로 방어하기 위한 AhnLab MDS 및 AhnLab MDR Agent 활용법을 소개했다.

배연용 차장은 "랜섬웨어 침해사고 건수는 매년 증가하는 추세로, 2019년 대비 2022년에는 10배 가까이 늘었다. 또한, 2020년부터 RaaS(Ransomware as a Service)가 본격화됨에 따라, 지난 2년 동안 다크웹에서 활동한 랜섬웨어 그룹 및 그로 인해 피해를 입은 조직의 수가 꾸준히 증가했다"라고 지적했다.

이메일, 네트워크, 엔드포인트, 망연계 등 다양한 경로로 유입되는 랜섬웨어는 AhnLab MDS와 AhnLab MDS Agent로 대응할 수 있다. 배연용 차장은 "예를 들어, 고객사 메일 서버 앞단에 AhnLab MDS를 배치하면 메일이 유입됐을 때 첨부 파일과 메일 본문을 파싱해 별도로 분석하고 행위 분석을 수행한 후, 정상 메일만 수집한다. 악성으로 의심되는 메일은 장비 내부에 격리한 다음, 메일 수신자와 보안 담당자에게 알림을 전송한다"라고 설명했다.

배연용 차장은 "AhnLab MDS Agent는 선택적으로 적용 가능하며, 사용자 PC에 설치돼 AhnLab MDS의 탐지를 우회하는 신규 파일을 수집하고 실행을 보류한다. 악성으로 판단되면 파일을 차단 또는 삭제하며, 해당 PC를 격리한다"라고 덧붙였다.



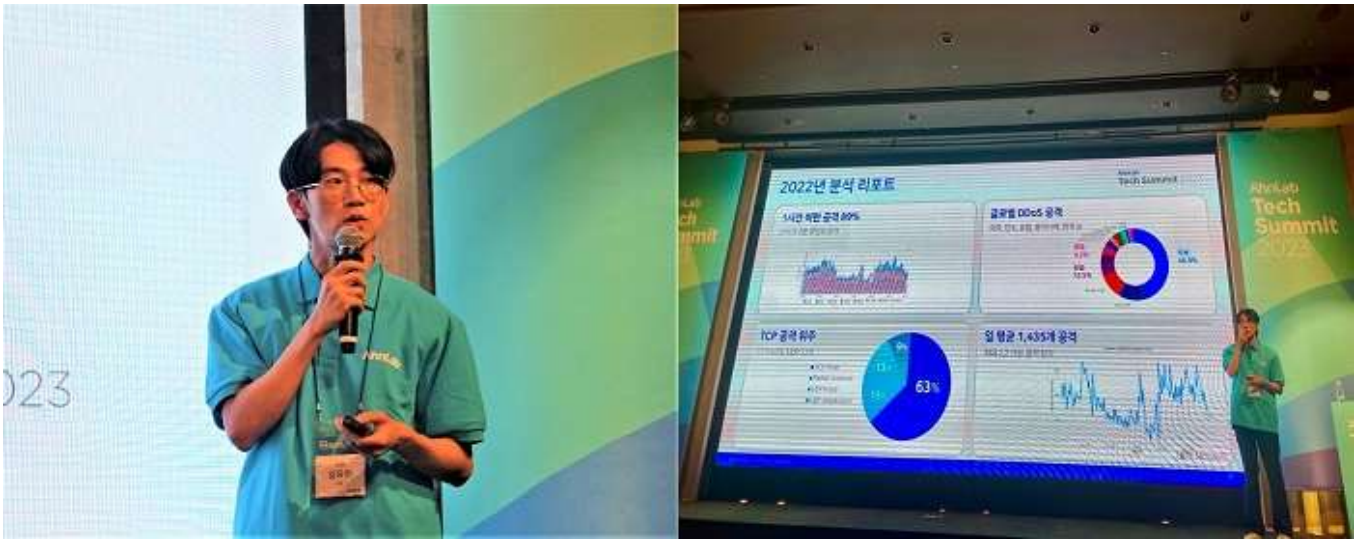
[사진 7] 안랩 EP 기술지원2팀 배연용 차장이 AhnLab MDS와 AhnLab MDS Agent를 활용해 랜섬웨어에 대응하는 방법을 설명했다.

안랩 NW 기술지원2팀 김유헌 차장은 디도스(DDoS) 공격 트렌드의 변화와 대응 전략을 주제로 발표를 진행했다.

김유헌 차장은 "올해 1분기 발생한 초대규모 디도스 공격은 초당 7,100만 이상의 요청(rps)를 기록했으며, 랜섬 디도스 공격이 지속적인 증가 추세를 보이고 있다. 또한, 공격자는 디도스 공격에 고성능 가상 사설 서버(Virtual Private Server, VPS) 봇넷을 사용하고 있는 것으로 확인됐다"라고 경고했다.

김유헌 차장은 "보안 장비를 직접 설치하는 온프레미스(On-Premise) 방식, 공격 트래픽을 차단하는 디도스 클린존(Clean Zone) 및 스크러빙 센터(Scrubbing Center)를 통해 외부로부터 유입되는 디도스 공격에 대응할 수 있지만, 경계 영역에서 디도스 공격을 막아내려면 디도스 대응 전용 솔루션을 사용해야 한다"라고 조언했다.

안랩은 'AhnLab DPX'라는 디도스 대응 솔루션을 보유하고 있다. 김유헌 차장은 "AhnLab DPX는 TCP/HTTP/DNS 인증, 행위 규칙 임계치 학습, 비정상 프로토콜 시그니처 ACL(Access Control List) 규칙 등 여러 단계의 방어 기능을 제공해 디도스 공격을 완화한다"라고 덧붙였다.




[사진 8] 안랩 NW 기술지원2팀 김유헌 차장이 디도스 공격 트렌드의 변화에 대응하는 방법을 설명했다.

마지막 세션의 발표를 맡은 안랩 기술컨설팅팀 조민규 팀장은 보안 솔루션이 생산하는 수많은 데이터 중 유의미한 보안 데이터를 선별하고 해석해 보안 위협에 대응하는 노하우를 소개했다.

조민규 팀장은 "보안 영역에서도 최근 EDR, XDR, ZTNA(Zero Trust Network Access)와 같은 새로운 솔루션이 출시되면서 방대한 양의 데이터가 생산되고 있다. 이런 시대에 필요한 것이 바로 '데이터 리터러시(Literacy)이다"라고 말했다.


[사진 9] 안랩 기술컨설팅팀 조민규 팀장이 데이터 리터러시를 활용해 보안 위협을 선별하고 대응할 수 있는 방법을 설명했다.

조민규 팀장은 "데이터 리터러시를 통해 성공적인 보안 태세를 갖추려면 위협 분석을 위해 데이터를 저장하고 수집해야 하며, 수집된 데이터를 이해하고 분석해야 한다. 더 나아가, 분석 정보의 유형과 위험도를 분류하고, 공격에 대응할 수 있어야 한다"라고 강조했다.

이 밖에, 행사장에는 발표 세션 외에도 안랩의 핵심 보안 솔루션인 AhnLab EDR, AhnLab CPP, AhnLab MDS, AhnLab EPS, AhnLab DPX, AhnLab AIPS를 체험할 수 있는 데모 상담 부스가 마련돼 참석자들에게 생생한 실무 밀착형 정보를 제공했다. 더 나아가, 추첨을 통해 아이패드 프로, 닌텐도 스위치 등 다양한 경품도 제공하며 참석자들의 뜨거운 호응을 얻었다.