보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

오프라인으로 돌아온 RSAC와 가트너 서밋, 주요 동향은?

AhnLab 2022-07-04

글로벌 보안 컨퍼런스 RSA Conference 2022와 Gartner Security & Risk Management Summit 2022가 지난 6월 첫째 주에 개최됐다. 코로나19 팬데믹 기간 동안 온라인으로 전환된 이후 처음 오프라인으로 돌아온 것이다. 안랩은 두 행사 모두 직접 참관하여 지난 2~3년간 글로벌 보안 시장의 주요 화두와 변화를 확인했다.

이번 글에서는 두 컨퍼런스에서 다뤄진 주요 내용과 인사이트를 공유한다.

세계 최대 사이버보안 컨퍼런스 'RSA Conference 2022(이하, RSAC 2022)'가 지난 6월 6일부터 9일까지 미국 샌프란시스코에서 개최됐다. 2년만에 오프라인으로 개최된 이번 컨퍼런스의 주제는 코로나19 팬데믹 이후 사이버보안의 급격한 변화를 의미하는 'TRANSFORM'이었다. 세계 각지에서 약 2만 6천명의 보안 관계자들과 400여 개 전시업체들이 참가했고, 350여 개 세션이 마련됐다.

[사진 1] RSAC 2022 Moscone Center 전경

글로벌 IT 분야 리서치 전문 기관 가트너가 주최하는 'Gartner Security & Risk Management Summit 2022(이하 가트너 서밋 2022)'도 RSAC 2022와 같은 주에 개최되었다. 6월 7일부터 10일까지 미국 메릴랜드 내셔널 하버에서 진행

된 가트너 서밋 2022는 ▲참가자 약 4천 명 ▲전시 업체 수 224개 ▲세션 수 350여 개를 기록했으며, 여러 가트너 애널리스트들과 보안업계 전문가들이 연사로 나서 최신 보안 인텔리전스를 공유했다.

[사진 2] 가트너 서밋 2022 세션 현장

두 행사에서는 규모에 걸맞게 사이버보안에 관한 폭 넓은 주제들이 깊이 있게 다뤄졌다. 다음은 양 컨퍼런스에서 주요하게 언급된 ▲인공지능(AI) ▲클라우드 보안 ▲제로 트러스트(Zero Trust) ▲XDR & MDR에 관한 내용을 정리한 것이다.

보안에서 AI의 역할

사이버보안 복잡성 심화는 더 이상 새로운 이야기가 아니다. 고도화된 위협 대응과 다양한 보안 솔루션을 사람의 힘으로만 운영하는 것은 이제 한계에 다다랐고, 이와 같은 추세는 앞으로 더 심화될 전망이다. 방대한 데이터를 빠르게 처리할 수 있는 AI는 이 문제에 대한 해결책이 될 것으로 기대를 모으고 있다.

가트너 서밋 2022 오프닝 기조연설에서는 지금으로부터 10년 뒤인 2032년, AI를 활용한 조직의 사이버 위협 대응 협력 모델을 시뮬레이션했다. 조직이 사이버 공격을 당하면, 비즈니스 전문가는 비즈니스 영향에 대한 AI의 분석 결과를 바탕으로 전략 수립에 집중하고, 기술 전문가는 AI 포렌직 서비스를 가동해 공격 방법과 원인을 분석하여 대응 방안을 도출한다. 전략 전문가는 대응 성과를 토대로 AI 활용 보안 체계 강화에 관한 조직의 의사결정과 투자를 이끌어낸다.

[사진 3] 가트너 서밋 오프닝 기조연설 (좌: Katel Thielemann, Gartner VP Analyst, 우: Andrew Walls, Gartner Distinguished VP Analyst, 출처: 가트너)

가트너는 해당 기조연설을 통해 'AI Augmented'라는 개념을 제시했다. 직역하면 증강 AI라는 의미인데, AI를 강화하고 사람과의 시너지를 통해 조직 차원의 사이버보안 협력을 극대화하는 것이 주요 골자다. 추가로, AI는 트레이닝한 데이터만큼 효과를 발휘하므로, 사람은 AI가 한 일을 설명(AI-explainability)하는 부분에서 진화해야 한다는 설명을 더했다.

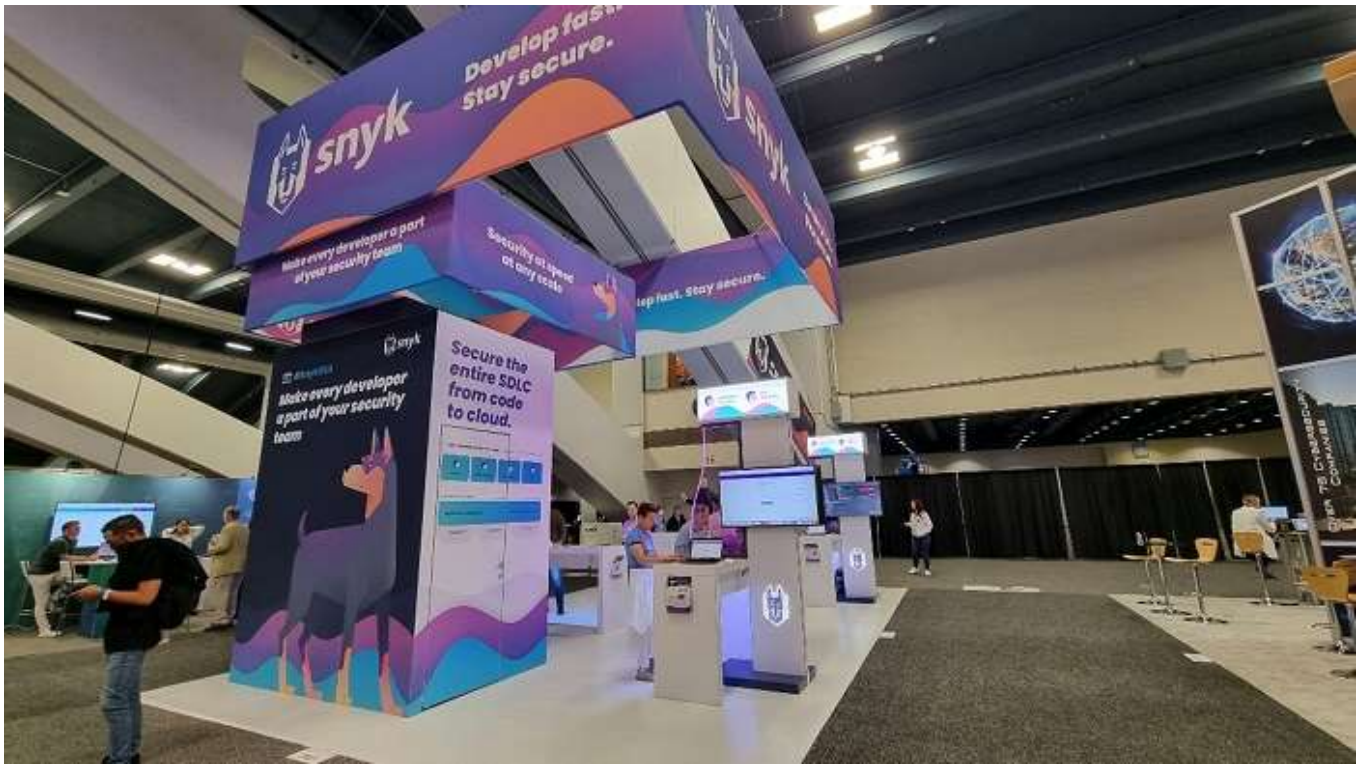
RSAC 2022에서는 바수 자칼(Vasu Jakkal) 마이크로소프트 보안, 컴플라이언스, 아이덴티티 부문 부사장이 발표를 통해 AI를 활용한 보안 혁신의 중요성을 역설했다.

[사진 4] 바수 자칼, 마이크로소프트 부사장 발표 (출처: RSAC)

바수 자칼 부사장은 현재 1초에 921번의 사이버 공격이 일어날 정도로 공격자들이 빠르게 움직이고 있으며, 그에 맞게 대응 속도도 빨라져야 한다고 강조했다. 여기서, 수 많은 데이터를 빠르게 처리할 수 있는 AI는 특히 탐지 영역에서 위협을 분류하는데 두각을 나타내며, 이를 바탕으로 비즈니스 상황과 맥락에 따라 맞춤 대응이 가능하다는 것이다. 더불어, 보안 영역 AI 기술 발전을 위해, 활발한 데이터 공유를 바탕으로 AI의 잠재력을 극대화해야 한다고 촉구했다.

클라우드 네이티브 보안의 핵심은?

지난 수 년간 보안업계의 주요 화두였던 클라우드 보안은 RSAC 2022와 가트너 서밋 2022에서도 단연 주목을 받았다. 두 행사에서는 클라우드 보안을 다각도로 조명하는 여러 세션들이 진행되었고, 많은 보안 기업들이 전시를 통해 당사의 솔루션과 새로운 보안 기능들을 선보였다.



[사진 5] RSAC 2022 DevSecOps 벤더 Snyk 부스

최신 클라우드 보안은 '클라우드 네이티브 서비스의 수명 주기가 점점 짧아지고 있다'는 사실을 전제로 한다. 따라서, 변화에 빠르게 대응하고 운영 효율성을 제고할 수 있는 새로운 보안 접근의 필요성이 대두되고 있다.

대표적인 접근법이 바로 '데브섹옵스(DevSecOps)'다. 데브섹옵스는 개발과 운영을 연계하는 '데브옵스(DevOps)' 파이프라인 전체에 걸쳐 개발 시작 단계부터 보안을 적용하는 프로세스를 의미한다. 이를 통해, 개발 및 운영 시간을 단축하는 데브옵스에 보안을 더해 안전한 개발 결과물을 확보하고, 담당 부서간 협력도 강화할 수 있다.

가트너는 데브섹옵스 파이프라인에서의 보안 방안으로 '클라우드 네이티브 애플리케이션 보안 플랫폼(Cloud Native Application Protection Platform: CNAPP)을 제안한다. CNAPP는 클라우드 워크로드 보안 플랫폼(Cloud Workload Protection Platform: CWPP)과 클라우드 보안 형상 관리(Cloud Security Posture Management: CSPM)이 통합되며, 그 외 부가적인 기능들이 추가된다.

가트너 서밋 2022에서 'Outlook for Cloud Security' 세션 발표를 진행한 찰리 윈클레스(Charlie Winckless) 가트너 시니어 디렉터 애널리스트는 데브섹옵스 보안을 위한 CNAPP의 기본 구성요소로 CWPP가 런타임 보호, CSPM이 클라우드 보안 형상 관리, AST(Application Security Testing)가 아티팩트 스캐닝을 담당한다고 설명했다.

아울러, 클라우드 네이티브 보안 운영의 핵심 요소인 자동화의 중요성도 강조되었다. 핵심은 코드형 인프라(Infrastructure as Code: IaC)와 코드형 정책(Policy as Code)이다. 데브섹옵스 파이프라인을 구성하는 인프라와 적용되는 정책을 코드로 구축해 배포, 제어 및 관리를 자동화하여 빠른 변화 조치와 수정을 가능하게 하는 것이 목적이다.

대세가 된 제로 트러스트

RSAC 2022와 가트너 서밋 2022 모두 '제로 트러스트(Zero Trust)'를 전면에 내세운 부스들을 어렵지 않게 찾아볼 수 있었다. 팔로알토 네트웍스(Palo Alto Networks), 일루미오(Illumio), 아이보스(iboss) 등 다양한 기업들이 부스 슬로건에 제로 트러스트 문구를 활용했다. 사이버 위협이 고도화를 거듭하는 가운데, 제로 트러스트가 보안의 새로운 대세로 자리 잡았음을 확인할 수 있었다.

[사진 6] RSAC 2022 팔로알토네트웍스, 시스코 부스

우선 제로 트러스트는 솔루션이 아니라 보안 접근 방식 혹은 비전이다. RSAC 2022 기조 연설자로 나선 존 크리스 잉글리스(John Chris Inglis) 미국 백악관 국가 사이버 국장은 제로 트러스트를 "정부와 기업의 보안 프로세스를 바꾸는 것"이라고 정의했다. 또한, 가트너 VP 애널리스트 토마스 린테머스(Thomas Lintemuth)는 '암시적(implicit) 신뢰와 컨텍스트 신뢰를 지속적으로 검증하는 비전'이라는 정의를 내렸다.

그럼 제로 트러스트는 구체적으로 어떻게 구성될까? 가트너 서밋 2022 '5 Steps to Start the Zero Trust Journey' 세션에서 토마스 린테머스가 제시한 제로 트러스트 아키텍처는 총 7단계로 구성된다. 간단히 소개하면, 1단계부터 3단계까지는 각각 사용자, 디바이스, 사용자가 연결하고자 하는 애플리케이션을 검증한다. 이후 4단계에서는 사용자, 네트워크, 워크로드, 애플리케이션 등을 모니터링하며, 5단계에서는 위협 인텔리전스 적용 및 애플리케이션 관리 등을 자동화한다. 마지막 6단계와 7단계는 데이터 보안과 세그멘테이션(segmentation)을 진행한다.

RSAC 2022와 가트너 서밋 2022의 다양한 세션들에서 제로 트러스트에 관해 다룬 내용들을 종합해보면, 제로 트러스트는 인증이 완료되기 전까지 그 어떤 것도 신뢰하지 않고 보안을 위해 검증을 계속한다.

제로 트러스트 개념이 각광받게 된 이유는 관리해야 할 계층과 대상이 다양해진 현재 IT 환경에서 기존 네트워크 경계 보안만으로는 안전을 보장할 수 없게 되었기 때문이다. 특히, 동적이고 분산되어 있는 클라우드 네이티브 애플리케이션의 경우 더욱 그렇다. 이에 대해 제로 트러스트 아키텍처는 세분화된 접근 제어를 바탕으로 보안을 강화한다.

XDR & MDR, 어디까지 왔나?

혹자들은 XDR에 대해 아직 현실과는 거리가 있는 마케팅 용어가 아닌지 의구심을 제기하기도 한다. 하지만 이번 RSAC 2022와 가트너 서밋 2022에서는 XDR이 단순히 유행에 그치는 것이 아니라 실제로 보안 업계가 나아가고 있는 방향임을 확인할 수 있었다.

[사진 7] RSAC 2022 XDR, MDR 벤더 부스

XDR에 대해 많은 조직과 기업들이 정의를 내리고 있는데, 정리해보면 '복수의 텔레메트리를 자동으로 수집하고 상호 연결하는 탐지 & 대응 플랫폼'으로 요약할 수 있다. 다양한 포인트로부터의 알림을 침해(incident)로 도출하고, 여러 형태의 탐지 옵션을 제시하며 자동화된 대응을 바탕으로 보안 운영의 효율성과 생산성을 개선하는 것이 XDR의 역할이다.

XDR은 엔드포인트, 네트워크 뿐만 아니라 이메일, 클라우드 등 다양한 영역을 포괄한다. 모든 영역을 완벽하게 보호하는 것이 가장 이상적이지만, XDR을 도입하는 조직 혹은 제공하는 벤더의 상황에 따라 무엇부터 보호해야 할지 우선순위를 정해야 하는 경우가 많다.

데이브 메셋(Dave Messet) 가트너 시니어 디렉터 애널리스트는 가트너 서밋 2022에서 세션을 통해 XDR 구성요소 중 우선순위를 둔다면 ▲엔드포인트(EPP/EDR) ▲이메일(SEG) ▲아이덴티티(IAM)를 먼저 통합할 것을 조언했다. 최근의 고도화된 공격 시나리오를 보면 엔드유저가 피싱 이메일 링크를 눌러 엔드포인트가 침해되고, 이후 ID/PW 등의 자격증명을 탈취당해 피해를 입는 형태로 전개되기 때문이다.

다음으로 MDR은 EDR부터 XDR까지 '탐지 & 대응' 개념이 부상하면서 함께 각광받고 있다. MDR의 정의는 '신속한 탐지, 분석, 조사, 대응을 바탕으로 위협을 완화하고 제어하는 보안 운영 서비스'로 정리할 수 있다. 장소에 구애 받지 않고 제공되며, 전문가의 분석과 조사를 바탕으로 유지/보수를 넘어 실현 가능한 결과물을 내는 것이 특징이다.

MDR 서비스의 구성 요소로는 기본적으로 24시간 모니터링, 침해 탐지, 침해 조사, 침해 억제 및 제어, 위협 사냥이 있다. 여기에 공격 표면 관리와 침해 대응 역량이 더해져 MDR 서비스를 완성한다.

가트너 조사 결과에 따르면 글로벌 MDR 시장은 2020년부터 2021년까지 48.9% 성장한 것으로 나타났다. 이유는 간단하다. 위협이 고도화되고 보호해야 할 영역은 많아지고 있지만, 24시간 보안을 운영하고 위협을 탐지해 대응할 수 있는 역량을 갖춘 조직은 극소수이기 때문이다. 이에 따라, MDR 서비스에 대한 수요는 앞으로도 계속 확대될 것으로 전망된다.

마치며

RSAC 2022와 가트너 서밋 2022에서는 코로나19 팬데믹 기간 동안 일어난 보안 시장의 급격한 변화를 직접 목격할 수 있었다. 두 행사에서 공통적으로 나타난 대표적인 트렌드는 '포인트 솔루션에서 통합 플랫폼으로의 전환'이다. 앞서 주요 주제로 언급한 CNAPP와 XDR 모두 복수의 솔루션을 통합한 플랫폼의 개념이며, 제로 트러스트 역시 같은 지향점을 공유한다. 여기에, 보안 복잡성 심화에 대응하기 위한 AI와 자동화의 역할 확대도 주요 트렌드로 꼽을 수 있다.

이제 올해를 기점으로 잠시 멈췄던 오프라인 행사들이 다시 활기를 띨 것으로 예상된다. 내년에는 기존 트렌드가 어떻게 발전할지, 또 어떤 새로운 트렌드가 부상할지 기대해보자.

AhnLab 콘텐츠기획팀 신재만 대리