글로벌 시장은 AI를 어떻게 바라보고 있을까?

글로벌 IT 리서치 기관 가트너(Gartner)는 지난 6월 3일부터 5일까지 사흘간 미국 메릴랜드주 내셔널 하버의 게일로드(Gaylord) 컨벤션 센터에서 'Gartner Security & Risk Management Summit 2024(이하 가트너 서밋 2024)'를 개최했다. 본 컨퍼런스에서는 가트너 애널리스트 포함 수십 여명의 보안 전문가들이 각 세션을 통해 다양한 보안 인텔리전스를 공유했다.

이번 글에서는 컨퍼런스를 통해 확인한 주요 보안 트렌드들을 공유한다.

[사진 1] 가트너 서밋 2024 현장 사진

북미 포함 전 세계 보안 관계자들이 참석한 가트너 서밋 2024은 ▲참가자 약 5000여 명 ▲전시 업체 수 240여 개 ▲세션 수 250여 개 규모로 치뤄졌다. AI가 전 세계 보안 시장을 수놓고 있는 가운데, 이번 컨퍼런스에서도 AI가 주요한 주제로 다뤄졌다. 이 밖에도, 진화하는 엔드포인트 보안, 지속적인 위협 표면 관리(Continuous Threat Exposure Management, CTEM), 최신 랜섬웨어 동향 및 대응 방안 등 글로벌 최신 보안 트렌드들을 확인할 수 있었다.

보안을 강화하고 복잡성 극복하기

RSAC 2024의 메인 테마는 'The Art of Possible'이었다. 국문으로는 '가능성의 미학'이라는 뜻으로, 데이터와 인공지능(AI)을 기반으로 협력을 통해 '사이버 보안의 무한한 가능성을 연다' 정도로 해석될 수 있다. 사이버 보안 커뮤니티의 협력에 중점을 두는 것은 지난해 RSAC 2023의 메인 슬로건 'Stronger Together'와도 맥을 같이한다.

가트너 서밋 2024 오프닝 기조연설은 'Augmented Cybersecurity: How to Thrive Amid Complexity'를 주제로 가트너 VP 애널리스트 크리스토퍼 믹스터(Christopher Mixter)와 데니스 추(Dennis Xu)가 함께 진행했다. 기조연설 제목을 국문으로 옮기면, '사이버보안 강화: 복

잡성을 극복하고 성공하기' 정도로 해석할 수 있다.

[그림 2] 가트너 서밋 2024 오프닝 기조연설 (출처: 가트너)

두 연사는 기조연설을 통해 현재의 복잡한 환경에서 보안을 완벽하게 수행하는 'Zero Tolerance' 접근은 불가능한 미션이라 강조했다. 이제, 위협을 완벽하게 차단(Prevention)하는 것이 아닌 대응하고 회복하는(Response and Recovery) 접근법을 지향해야 하며, 이를 위해 허용(Tolerate)하는 개념을 받아들여야 한다고 말했다.

해당 개념을 안착시키기 위해 가트너에서 제시한 것이 바로 '사이버보안 강화(Augmented Cybersecurity)'다. 사이버보안 강화는 조직을 지속가능한 방법으로 보호하고, 대응 및 회복을 차단의 수준까지 끌어올리는 것을 의미한다. 성공적인 사이버보안 강화를 위해서는 다음 세 가지 방법론이 요구된다.

#1: 조직 차원에서 실패를 허용하자 (Fault Tolerant Organization)

이제 보안에서 실패는 필연적이며, 조직들은 이를 받아들일 수 있어야 한다. 다만, 그 과정에서 ▲생성형 AI(Gen AI)와 써드파티 툴(Third-party Tools)을 적극 활용해야 한다. 먼저, AI의 파도는 이제 거스를 수 없게 되었다. 조직들은 생성형 AI 플레이북을 만들고 보안 요소 중 무엇이 '허용 가능(Tolerable)'한지 판단할 수 있어야 한다. 또한, 써드 파티와의 협력을 계속해 상호간 리스크 관리 역량을 향상시키고 공생 관계를 형성하는 것도 중요하다.

#2: 적은 보안으로 최대한의 효과 내기 (Minimum Effective Toolset)

Minimum Effective Toolset은 지난해 컨퍼런스에서 소개된 개념으로, 적은 보안 툴로 최대한의 효과를 보는 것을 의미한다. 이에 대해, 기조연설 연사들은 ▲통합 플랫폼 사용을 통한 중복 및 갭 제거 ▲리스크, 기술 호환성, 비용에 대한 지속적인 검증 ▲생성형 AI 사용을 통한 보안 형상 및 효율성 개선을 해답으로 제시했다.

#3: 사이버 보안 조직에 회복력 더하기 (Resilient Cyber Workforce)

지난 5월 열린 RSA Conference 2024에서 지목된 최신 보안 트렌드 중 하나가 바로 보안 전문가들의 '번아웃(Burnout)' 이었다. 이번 기조연설에서도 연사들은 번아웃이 주요한 문제라고 지적했으며, 보안 부서 전체적으로 '회복력(Resilience)'를 갖추는 것이 중요하다고 강조

했다. 이어서, 문제 해결을 위한 방안으로 직원 케어 프로그램 마련, 회복력을 조직의 경쟁력으로 받아들일 것, 번아웃을 고려해 워크플로우를 재구성할 것을 권고했다.

[그림 3] 가트너 서밋 2024 세션 주제

오프닝 기조연설이 끝난 뒤, [그림 2] 주제들에 대해 3일 동안 250개 이상의 세션들이 진행됐다. 세션을 맡은 전문가들은 각 대주제를 다양한 영역과 시각에서 바라보며, 심도 있는 인사이트를 공유했다. 아래에서는 여러 주제 중에서도 핵심이라 할 수 있는 ▲AI 보안 ▲워크스페이스 보안 ▲리스크 관리 ▲CPS(Cyber Physical System) 보안에 관한 주요 발표 내용을 소개한다.

AI, 보안을 어떻게 바꿀까?

AI는 올 한해, 보안 업계를 뜨겁게 달구고 있는 키워드로 단연 첫 손에 꼽힌다. 이처럼 높은 관심을 대변하듯, 가트너 서밋 2024에서도 AI에 관한 세션들이 상당한 비중을 차지했다. 특히, 전 세계적으로 주목 받고 있는 생성형 AI에 관한 세션들이 많았다. 보안에서 생성형 AI를 제대로 사용하려면 어떻게 해야 하는지 또 주의해야 할 점은 무엇인지, 전문가들의 발표 내용을 살펴보자.

리차드 바틀리(Richard Bartley) 가트너 VP 애널리스트는 'Technical Insights: 5 Ways GenAI Can Help Build Better Security Architecture' 세션에서 생성형 AI를 활용한 보안 아키텍처 구축 방안 5가지를 다음과 같이 제시했다.

1. 관계 식별(Identify relationship): 보안 프레임워크, 제어 및 정책을 매핑해 기반 구축

2. 맥락화(Contextualize): 보안 이벤트의 전후관계 파악

3. 분석 향상(Analysis uplift): 보안 현황 분석, 갭 식별 및 취약점 파악, 개선 방향 설정

4. 생성(Create): 보안 요구사항을 생성하고 처리 최적화

5. 관리(Manage): 보안 기능을 제안하고 작업 우선순위 결정

이어서, 보안 아키텍트는 생성형 AI에 대한 효과적인 프롬프트 엔지니어링 기술을 습득해 정확하고 유용한 결과를 얻을 수 있어야 한다고 강조했다. 또, 오픈되어 있는 생성형 AI 서비스에 지나치게 의존하지 말고 목적에 따라 트레이닝된 사설 생성형 AI를 사용하는 것이 좋으며, 생성형 AI가 출력한 답은 사람이 항상 검토하고 검증해야 한다고 당부했다.

피트 쇼어드(Pete Shoard) 가트너 VP 애널리스트는 'Generative AI and the SOC: The Good, the Bad and the Ugly' 세션에서 생성형 AI를 SOC에 적용할 때 얻을 수 있는 장점과 도전과제들을 소개했다.

장점		도전과제	
분석 자동화	반복 작업을 자동화해 분석 속도 향상	데이터 품질	정확하고 일관성 있는 데이터 유지 필요
위협 탐지	더 빠르고 정확한 위협 탐지	알고리즘 편향성	알고리즘의 편향성 최소화 및 공정성 유지 필요
대응 시간 단축	자동화된 대응 시스템으로 신속한 위협 대응	인적 역	생성형 AI를 효과적으로 사용할 수 있도록 교육

[표] 생성형 AI의 장점과 도전과제

피터 쇼어드는 생성형 AI가 반복적인 작업을 자동화하고, 대규모 데이터를 효율적으로 분석하며, 보안 인텔리전스를 강화할 수 있는 잠재력을 가지고 있다고 강조하는 동시에, 성공적인 생성형 AI 활용을 위해서는 기술을 단계적으로 도입해 리스크를 관리해야 한다고 말했다.

엔드포인트와 제로 트러스트, 그리고 워크스페이스 보안

가트너에서 이번 컨퍼런스를 통해 새롭게 소개한 개념 중 하나가 바로 '워크스페이스(Workspace) 보안'이다. 워크스페이스 보안은 엔드포인트 보안에서 진일보한 개념으로, 엔드포인트 뿐만 아니라 사용자, 협력 툴, 데이터 등의 요소들도 '업무 환경(워크스페이스)'에 포함된다. 기존, '기기'에 집중하는 엔드포인트 보안에 다양한 요소들이 추가된 포괄적 개념으로 이해할 수 있다.

크리스 실바(Chris Silva) 가트너 VP 애널리스트는 'How to Apply Zero Trust to Strengthen Endpoint Security' 세션을 통해 워크스페이스 보안 강화를 위한 방안 중 하나로 엔드포인트 보안과 제로 트러스트 패러다임의 통합을 제시했다. 간단히 하면, 엔드포인트, 네트워크, 아이덴티티를 통합해 생각하고 관리해야 한다는 것이다.

[그림 4] 크리스 실바 가트너 VP 애널리스트

크리스 실바는 제로 트러스트 패러다임이 공격 표면을 줄이고 조직 전체의 보안 형상을 강화하는데 의미가 있다며, 안전한 엔드포인트가 제로 트러스트+엔드포인트 통합의 핵심이라고 강조했다. 이어서, 최신 업무 환경에서 엔드포인트는 취약해지고 공격 표면은 넓어지는 가운데, 인증된 애플리케이션과 사용자만 접근을 허용하고, 디바이스 제어 역량을 적극 활용하며, EDR을 통한 지속적인 엔드포인트 모니터링이 필요하다고 말했다.

또한, 보안 침해의 74%는 '사람'과 연관이 있다며, 업무 환경에서 기기들이 계속 바뀌면서 접근 제어가 느슨해지는 경우가 많으므로, 지속적인 조건부 접근 정책을 적용해 사람으로 인한 리스크를 줄여야 한다고 짚었다.

리스크 관리, CTEM과 XSPM

CTEM(Continuous Threat Exposure Management)과 XSPM(eXtended Security Posture Management)은 리스크 관리라는 측면에서 주목받고 있는 개념이다. CTEM은 기존 공격 표면 평가와 취약점 관리를 결합한 지속적인 위협 표면 관리를 뜻하며, XSPM은 기존 클라우드 보안 형상 관리(CSPM)에서 시작된 보안 형상 관리 개념을 SaaS, 데이터, 아이덴티티, 생성형 AI까지 넓게 확장시킨 것이다.

닐 맥도날드(Neil MacDonald) 가트너 수석 VP 애널리스트는 'Emerging Technologies in Security and Risk Management, 2024'에서 보안 리스크 관리 신기술 다섯 가지를 소개했는데, 이 중 CTEM과 XSPM이 각각 선정되었다.

[그림 5] 닐 맥도날드 가트너 수석 VP 애널리스트

닐 맥도날드는 CTEM이 공격 표면 매핑, 취약점 식별 및 리스크 완화를 포함하는 '프로세스'이며, 제품이 아니라고 강조했다. 그리고, 공격 표면 및 취약점의 우선순위를 선정하고 보안 제어의 유효성을 검증해야 하며, 공격 표면을 써드 파티와 OT/ICS 시스템을 포함해 포괄적으로 관리해야 한다고 말했다. CAASM(Cyber Asset Attack Surface Management)과 같은 도구들이 디지털 자산을 관리하는 데 도움이 될 수 있다고 조언했다.

XSPM에 대해서는 공격자가 미흡한 형상 관리를 악용하기 전에 리스크를 사전 식별하는 방향으로 패러다임이 전환되고 있다고 밝혔다. XSPM 도구들은 클라우드, SaaS, 데이터, 심지어 생성형 AI까지 여러 도메인에서 취약점 우선순위를 정하고 리스크를 완화하는데 도움을 주지만, 무조건적으로 새로운 솔루션을 도입하기 보다는 기존 운영 중인 솔루션을 잘 활용하는 것이 더 중요하다고 말했다.

OT는 왜 CPS로 바뀌나?

토마스 린테머스(Thomas Lintemuth) 가트너 VP 애널리스트는 'Outlook for Cyber-Physical System (CPS) Security 2024' 세션에서 OT와 CPS의 개념적 차이와 보안 접근법 변화에 대해 소개했다.

CPS(Cyber Physical System)는 OT(Operation Technology)에서 진일보한 개념이다. CPS는 OT 뿐만 아니라, 사물 인터넷(IoT), 산업제어시스템(ICS), 물리 보안 등을 포괄하며, 사이버 위협의 진화와 기존 OT 환경의 연결성 확대에 대응하는 관점에서 등장했다. 예를 들어, OT 시스템이 제조 공장의 컨베이어 벨트 제어 시스템을 일컫는다면, CPS는 장비 뿐만 아니라 이를 실시간으로 모니터링 및 제어할 수 있는 디지털 네트워크와 소프트웨어까지 통합해서 보는 것이다.

토마스 린테머스는 이 때문에, CPS와 OT 보안은 접근법에 차이가 있다고 말했다. OT 보안은 표준화된 보안 방식과 접근 제어를 따르는 반면, CPS 보안은 다양한 연결 지점을 노린 사이버 공격과 물리적 보안에도 신경을 써야 한다는 것이다. 스마트 공장, 전기차 충전소 등 다양한 CPS 환경이 생겨나는 상황에서, 조직들은 표준화된 보안 모델 뿐만 아니라 당사 활용 사례(Use Case)를 확인하고 이에 맞춘 보안 아키텍처를 개발해야 한다고 제언했다.

전시장에도 이어지는 AI 열풍

지난 5월, 안랩이 부스를 열고 참가한 RSA Conference 2024에서는 기업들이 그 동안 집중해오던 보안 영역의 메시지를 AI라는 주제로 통합하는 트렌드를 확인할 수 있었다. 이러한 흐름은 가트너 서밋 2024 전시장에서도 확인할 수 있었다. 약 240개 기업들이 참여한 이번 전시에는 상당수 기업들이 AI에 관한 메시지를 전면에 내세우고 제품 혹은 플랫폼을 시연했다.

[그림 6] 가트너 서밋 2024 전시장

[그림 7] 가트너 서밋 2024 행사장 메시지

마지막으로, 이번 행사를 총평하면 AI가 주를 이뤘지만, 그 외에도 리스크 관리(Risk Management)와 회복력(Resilience)이라는 주제도 굉장히 비중 있게 다뤄졌다. 특히, 현재의 복잡다단한 보안 환경에서 허용 가능한 실패는 받아들이고 빠르게 회복해야 한다는 기조연설 키 메시지는 수 많은 참가자들의 공감을 얻었다. 또한, 보안 플랫폼을 기반으로 솔루션 활용성을 극대화해야 한다는 메시지도 보안 기업과 고객사들의 방향성을 다시 한 번 확인시켰다는 점에서 의미가 있었다.

또한, 컨퍼런스에서 확인한 주요 트렌드들이 안랩의 지향점과 일치한다는 점은 상당히 고무적이었다. 안랩은 각 영역의 보안 솔루션들을 플랫폼 기반으로 통합해 활용성을 극대화하고 있으며, 플랫폼에 AI 기술을 적용해 탐지, 분석 및 대응 효율성을 높였다. 또한, 워크스페이스 보안과 CPS 보안에 대해서도 각각 엔드포인트 & 네트워크 보안 솔루션 연동과 IT-OT 통합 보안 플랫폼을 바탕으로 최신 트렌드에 발맞춰 나아가고 있다. 그리고, 앞으로도 기술 개발 및 고도화에 매진해 고객들이 마주한 보안 복잡성과 도전과제를 보다 효과적으로 해결해 나갈 계획이다.

안랩

콘텐츠기획팀 신재만 과장