| 2025년 상반기

정보보호 인적자원개발위원회

Issue Report

2025 정보보호 트렌드: 사람과 AI, 새로운 협력의 시대

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

정보보호 인적자원개발위원회

Issue Report

CONTENTS

목 차

보고서 내용에 대한 문의는 아래의 연락처로 주시기 바랍니다.

정보보호 인적자원개발위원회 사무국 TEL. 02-6748-2011, 2039 E-MAIL. mhr0327@kisia.or.kr

본 이슈리포트는 지니언스(주) 이대효 전략마케팅실장이 작성하였습니다.

01 서론

정보보호(안) 환경은 인공지능(AI), 특히 생성형 AI(Gen AI)의 급격한 발전과 함께 패러다임의 전환을 맞이하고 있다. 과거 사람 중심의 보안 운영에서 이제는 사람과 AI가 긴밀하게 연동하고 협업하여 지능화·고도화되는 사이버 위협에 맞서야 하는 새로운 시대가 도래한 것이다. 본 보고서는 이러한 변화를 가장 잘 확인할 수 있는 'RSAC (RSA Conference) 2025'의 주요 내용을 정리하고 정보보호 솔루션의 동향 및 협업 사례를 분석함으로써 미래 정보보호 환경에서 사람과 AI가 어떻게 시너지를 창출하고 새로운 보안 협력 시대를 열어갈 수 있을지에 대한 의견을 제공하고자 한다.

이번 행사는 '다양한 목소리, 하나의 커뮤니티 (Many Voices. One Community)' 라는 주제 아래 (생성형) AI가 가져올 가능성과 동시에 내재된 위험을 집중적으로 조명했다. 특히 자율적으로 판단하고 행동하는 에이전틱 AI(Agentic AI)의 등장은 보안 운영의 효율을 극대화할 수 있는 기회임과 함께 AI 모델 자체의 보안과 거버넌스라는 새로운 과제를 제시했다. 이와 함께 신원(Identity) 보안의 중요성이 재차 강조되었으며 XDR(eXtended Detection and Response), SASE(Secure Access, Service Edge), CNAPP(Cloud Native Application Protection Platform) 등 플랫폼 기반 솔루션으로의 통합의 추세는 더욱 가속화되는 모습을 보였다.

본 보고서는 먼저 RSAC 2025의 개요와 주요 키노트 발표 내용을 통해 현재 사이버 보안 산업의 화두를 살펴본다. 이어서 전시회에서 확인할 수 있었던 주요 기술 트렌드와 시장의 변화를 살펴보고 Microsoft, Cisco, Google 등 주요 산업 리더(Big Brother)들이 제시하는 AI 통합 및 플랫폼 확장 전략을 들여다본다. 마지막으로 정보보호 솔루션 간의 연동 및 협업의 발전과 이 과정에서 사람과 AI가 각각 어떤 역할을 수행하고 어떻게 상호작용하여 보안 역량을 극대화할 수 있는지 기술적, 전략적 관점에서 살펴본다.

결과적으로 본 보고서를 통해 정보보안이 더 이상 사람의 능력만으로는 대응하기 어려운 시대로 진입했음을 다 같이 인지하고 생성형 AI를 포함한 인공지능 기술과의 공존을 통해 미래 위협에 선제적으로 대비해야 한다는 핵심 메시지를 전달하고자 한다.

02 RSAC 2025: 사이버 보안의 현재와 미래를 조망

RSA Conference(RSAC)란?

- **주최기관** RSA Conference, LLC
- **주 개최지** 미국(샌프란시스코)
- **주요 참가자** 글로벌 보안 기업, 연구기관, 학계, 정부기관, 보안 전문가 등
- **행사 구성** 기조연설, 기술세션, 워크숍, 제품 및 기술 전시 부스, 네트워킹 행사 등
- **주요내용** RSAC는 1991년 미국 캘리포니아에서 처음 개최된 세계 최대 규모의 사이버 보안 컨퍼런스로, 글로벌 정보보안 기술과 정책을 선도하는 대표적인 행사로 자리매김

2.1. RSAC 2025 개요 및 주요 특징

올해 4/28 ~ 5/1까지 샌프란시스코 모스콘 센터에서 개최된 RSA Conference (RSAC) 2025는 전 세계 사이버 보안 전문가, 리더, 혁신가들이 모여 최신 위협 동향을 공유하고 미래 보안 전략을 논의하는 중요한 자리였다. 올해 행사는 '다양한 목소리, 하나의 커뮤니티 (Many Voices. One Community)' 라는 주제 아래 7백여명의 발표자, 650여개의 전시업체 그리고 4만명 이상의 참관객이 함께했다.

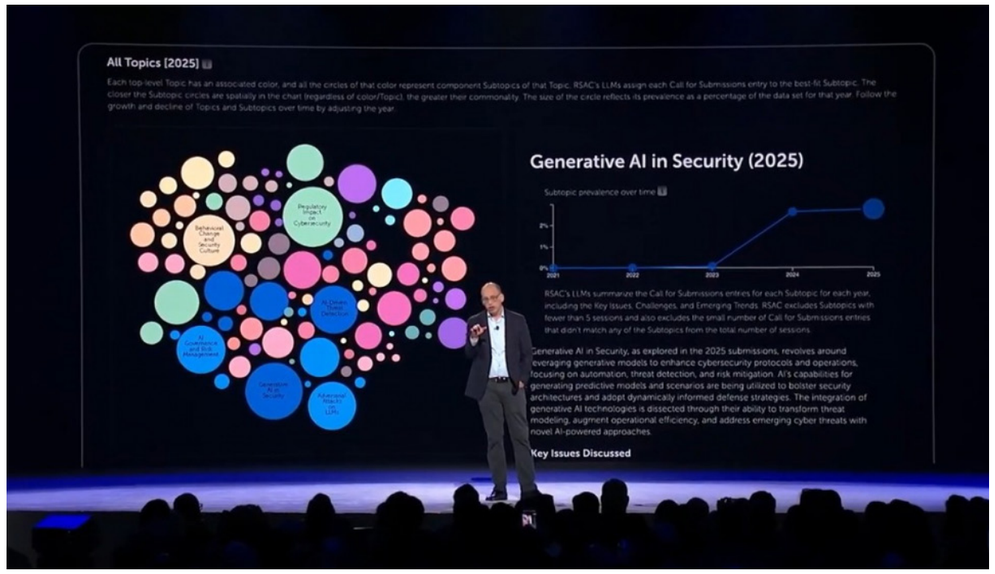
올해의 주제는 사이버 보안에 대한 공동의 목표인 사고 예방, 위협 대응 그리고 끊임없이 진화하는 위협에 보다 효과적으로 대처하기 위해 다양한 배경과 전문성을 가진 구성원들의 협력이 필수적임을 강조하는 메시지다. 오늘날 AI 기반 공격의 증가, 국가 지원 해킹 그룹(Nation Backed)의 활동 그리고 공급망 공격과 같은 위협은 단일 조직이나 솔루션만으로는 대응하기 어렵다는 현실을 반영한 메시지라 볼 수 있다. 이는 사이버 보안이 특정 기업이나 보안 부서만의 역할이나 책임이 아니며 나아가 공공 또는 민간 부문의 적극적인 정보공유 및 협력이 그 어느 때보다 중요해지고 있음을 시사한다. 따라서 다양한 구성원들의 커뮤니티와 협력은 생존을 위한 필수 전략이 되었다. 더불어 사이버 보안 인력과 역량의 부족 문제는 공유와 협업의 필요성을 가속화하고 있다.

2.2. RSAC 2025 키노트 핵심 메시지

RSAC 2025의 기조연설에서는 NBA 명예의 전당(Hall of Fame)에 두번이나 오른 매직 존슨부터 전 미국 국가사이버국장 크리스 잉글리스, 암호학 전문가 휘트필드 디피 등 각계의 저명인사들이 참여하여 심도 있는 통찰을 제공했다. 이들 연설에서 반복적으로 강조된 세 가지 주요 주제는 '에이전틱 AI(Agentic AI), 암호화(Cryptography) 그리고 공공-민간 협력(Public-Private Collaboration)' 이었다.

2.2.1. 에이전틱 AI(Agentic AI): 보안의 새로운 패러다임

인공지능(AI)은 이번 행사의 가장 뜨거운 화두였다. RSAC 집행위원장 휴 톰슨(Hugh Thompson)은 기조연설에서 "AI는 모든 곳에 있으며 사이버 보안의 거의 모든 측면에 스며들고 있다" 고 언급하며 그 중요성을 강조했다. 특히 기존의 규칙 기반 자동화 및 구조화된 데이터에 의존하는 시스템을 넘어 대규모 언어 모델(LLM)을 활용하여 자율적으로 동작하는 에이전틱 AI가 주목받았다. 이는 사용자와 상호작용을 통해 스스로 학습하고 분석가의 업무를 지원하며 상황에 기반해 결정을 내릴 수 있는 잠재력을 가진다.



[AI 시대, 보안의 미래는 기술이 아니라 '공동체' 와 '적응', 데일리시큐]

SANS 연구소의 롭 리(Rob Lee)는 AI가 보안팀의 생산성 향상에 기여하는 동시에 공격자들 또한 동일한 목적을 위해 AI를 활용하고 있다고 지적하며 AI의 양면성을 강조했다. 시스코(Cisco)의 부사장인 지투 파텔(Jeetu Patel)은 "AI 자체를 보호하고, 그 다음 AI를 방어에 사용해야 한다" 고 역설하며 사람의 방어는 기계의 공격에 불충분할 것이라고 말했다. 그는 시스코가 보안에 특화된 AI 모델을 공개한 사실을 언급하며 업계가 범용 AI 모델에 지나치게 의존하는 경향이 있어 보안에 특화된 모델이 필요하다고 주장했다. RSA(회사)의 CEO 로힛 가이(Rohit Ghai) 역시 공격자들이 진보된 AI 기술을 사용하여 사람을 사칭하고 워크플로우를 표적으로 삼고 있다고 경고하며 AI가 ID 수명 주기 전반에 걸쳐 위협이 될 수 있음을 시사했다.

2.2.2 암호화(Cryptography): 신뢰 기반 강화

암호화 역시 행사의 핵심 논의 주제였다. 인공지능(AI)이라는 거대한 화두 속에서 디지털 신뢰의 근간을 이루는 암호화(Cryptography) 기술에 대한 중요한 논의가 비중 있게 언급되었다. 특히 차세대 암호·인증 기술, 그 중에서도 양자내성암호(PQC, Post-Quantum Cryptography) 와 패스워드리스(Passwordless) 인증의 중요성이 강조되었다. 많은 세션에서 "양자 컴퓨터가 등장하지 않았더라도, 데이터를 훔쳐 미래에 해독하려는(Harvest Now, Decrypt Later) 공격에 대비해야 한다"는 경고가 이어졌다. 패스키(Passkey)와 같은 공개키 기반의 혁신적인 인증기술이 기존의 피싱공격에 매우 강력한 저항력을 갖추고 탁월한 편의성을 제공할 수 있음이 강조되었다.

2.2.3. 공공-민간 협력: 강력한 방어 체계 구축

수많은 세션에서 보안 강화를 위한 협력의 중요성이 큰 화두로 제시되었다. 매직 존슨은 기조연설을 통해 '어시스트의 기술(The Art of Assist)'을 언급하며 농구 코트에서 배운 협력과 팀워크에 대한 가치를 감동적으로 전달하였다. 그는 '동료와의 경쟁, 자기 스스로의 인식 그리고 신뢰'를 언급하며 왜 우리가 협력해야 하는가에 대한 동기를 부여했다. 그는 "래리 버드가 나를 더 나은 농구 선수로 만들었다" 고 언급하며 사이버 보안이라는 복잡하고 어려운 문제를 해결하기 위해 우리 모두가, 심지어 경쟁자여도 서로에게 훌륭한 팀원이 되어야 한다는 강력한 메시지를 남겼다.

[Earvin Magic Johnson 의 키노트 스피치, @Magicjohnson]

03 RSAC 2025 전시회 트렌드: AI와 플랫폼, 사람과의 새로운 협력

컨퍼런스와 함께 열리는 전시회(Exhibition)는 컨퍼런스에서 언급된 주제들이 산업현장에 적용되는 모습을 확인하고 솔루션과 시연을 통해 체감하는 자리였다. 특히 AI, 신원 보안, 플랫폼 통합이라는 세 가지 큰 흐름이 전시장을 관통하며 미래 정보보호 시장의 방향을 제시했다. 더불어 AI가 사람의 결정(Decision)과 행동(Response)을 대체할 수 있는가에 대한 판단 이전에 AI와 효율적인 협업의 필요성을 강조하는 계기가 되기에 충분했다.

3.1. AI의 영향력과 에이전틱 AI의 부상

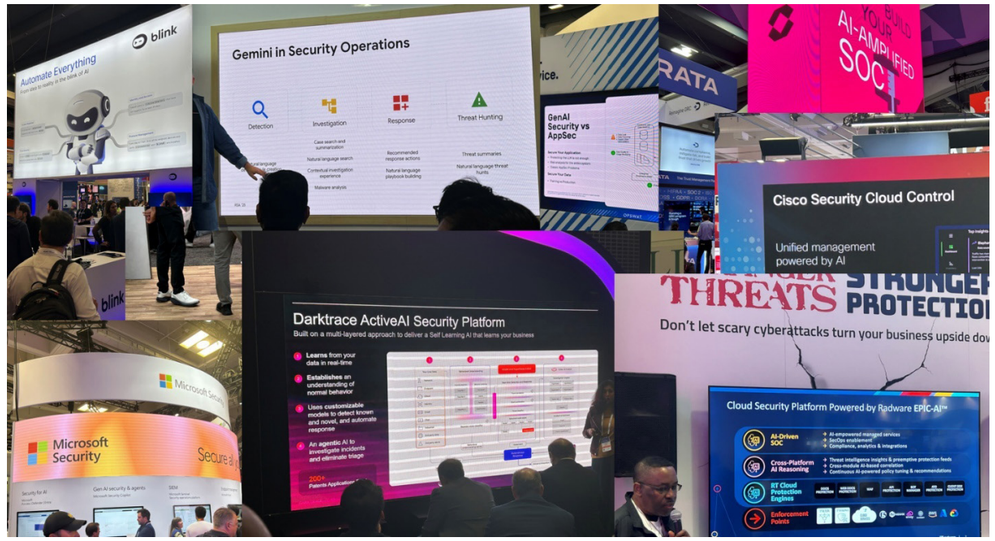
전시회장 역시 가장 두드러진 주제는 단연 인공지능(AI)이었다. 특히 생성형 AI(GenAI)와 더 나아가 자율적인 판단과 행동이 가능한 에이전틱 AI(Agentic AI)는 행사의 거의 모든 세션과 부스에서 핵심적인 위치를 차지했다.

그러나 AI는 양날의 검이다. 보안 운영 센터(SOC)의 효율성을 높이고 위협 탐지 및 대응을 자동화하여 분석가의 역량을 강화하는 강력한 도구임에 분명해 보인다. 하지만 다른 한편으로 AI는 공격자들에게도 강력한 힘을 제공한다. 더욱 정교하고 규모가 큰 공격(예: 딥페이크를 이용한 사회 공학, 지능형 피싱, LLM 자체의 취약점 공격)을 감행할 수 있다는 우려가 커지고 있다.

주요 기업들은 이러한 흐름에 맞춰 AI 에이전트를 선보였다. Microsoft의 Security Copilot, SentinelOne의 Purple AI Athena, Cisco의 Foundation AI, CrowdStrike의 Charlotte AI 등이 대표적이다. 이들 에이전트는 SOC 업무 자동화, 위협 헌팅, 분석가 역량 강화 등을 목표로 개발되었으며 사람과 협업을 통해 보안 운영의 효율성과 정확성을 높일 수 있을 것으로 기대된다.

그럼에도 AI 도입은 새로운 과제도 안겨주었다. AI 모델 자체 취약성(프롬프트 인젝션, 데이터 포이즈닝, 모델 탈취 등)의 대응, AI 거버넌스 수립('Shadow AI' 문제 해결) 그리고 AI 시스템의 보안 상태를 지속적으로 관리하는 AI 보안 상태 관리(AI-SPM, Security Posture Mgmt.) 등의 필요성이 대두되었다. 특히 에이전틱 AI가 자율적으로 동작함에 따라 AI 에이전트 자체의 행동을 모니터링하고 의사결정 과정을 감사(Audit)하며 잠재적인 오작동이나 악의적인 행위로부터 보호하는 새로운 프레임워크, 즉 '기업을 보호하는 AI를 보호해야 하는' 순환적 보안 문제가 발생하는 것이다. 이는 향후 AI 에이전트의 행동과 무결성에 초점을 맞춘 특화된 'AI SecOps' 역할과 관련 도구 시장의 성장을 예고하며 AI가 보안 운영의 신뢰 모델 자체를 근본적으로 변화시킬 수 있음을 암시한다.

궁극적으로 에이전틱 AI의 부상은 보안 전문가와 AI 간의 역할 재정의를 요구한다. AI는 반복적이고 정형화된 작업을 자동화하고 방대한 데이터를 신속하게 분석하여 사람의 판단을 돕는 강력한 조력자가 될 수 있지만 최종적인 의사결정과 책임은 여전히 사람에게 있다. 더불어 AI의 행동을 감독하고 통제하는 것 또한 사람의 중요한 역할이 될 것이다. 사람 참여형(Human-in-the-loop) AI 모델이 미래 SecOps의 가장 현실적인 모습이라고 제안되는 이유이다.



[전시장을 점령(?) 한 AI 관련 내용들, 지니언스]

3.2. 신원 중심 보안(Identity Centric Security)의 지속적 중요성

AI와 함께 가장 중요하게 다뤄진 주제는 신원(Identity) 보안이었다. 이는 신원 정보 탈취 및 오용이 여전히 주요 침해 사고의 핵심 원인이자 가장 효과적인 공격 경로로 활용되고 있기 때문이다. 행사 전 발간된 2025년 Verizon 데이터 침해 조사 보고서(DBIR)에서도 초기 침투 벡터로서 크리덴셜 오용의 심각성이 재확인되었다.

강력한 신원 보안 체계 구축의 중요성은 늘 강조된다. 복잡하고 고유하며 충분히 긴 암호(16자리 이상 등)를 사용하고 엔터프라이즈 암호 관리자(EAM) 도입, 다중 인증(MFA) 체계 적용 등이 그것이다. 그러나 이러한 작업 만으로 충분치 않다는 인식이 확산되면서 신원 위협 탐지 및 대응(ITDR), 권한 있는 접근 관리(PAM) 그리고 제로 트러스트 원칙 기반의 신원 중심 접근 통제의 중요성이 부각되었다.

AI 기술은 신원 보안의 중요성을 더욱 증가시키고 있다. 공격자는 AI를 이용해 암호 해독의 속도를 높이고 더욱 정교한 딥페이크 기술로 사회 공학적 공격을 감행하며 피싱 공격의 성공률을 높이고 있다. 또한 API 토큰, 키(Key), 시크릿 및 AI 에이전트와 같은 '사람이 아닌 신원(Non-Human ID)'에 대한 관리 및 보안 문제도 새로운 과제로 떠올랐다.

[ID 분야 다양한 보안솔루션과 메시지, 지니언스]

이러한 위협에 대응하기 위해 ITDR(Id Treat Detection & Response), 패스워드리스(Passwordless) 및 ISPM(ID Security Posture Management) 등 신원 보안에 특화된 솔루션이 다수 선보였다. 특히 ITDR과 PAM은 크리덴셜 침해에 완벽하게 대응하는 것이 (사실상)불가능해짐에 따라 대응의 초점이 (침해를 가정하고) 침해 이후의 악의적인 행동을 신속하게 탐지하고 권한 상승 및 내부 확산(lateral movement)을 차단하는 방향으로 이동하고 있음을 보여준다. 이는 제로 트러스트의 핵심 원칙인 '지속적 검증'과 '최소권한'으로 침해 사고 발생 시 피해를 최소화는 회복탄력성(resilience)을 중점에 둔 전략으로의 전환을 의미한다.

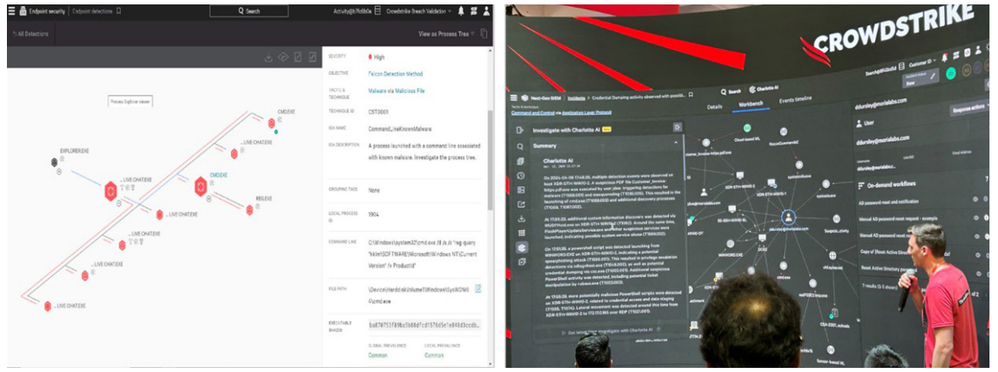
신원 중심 보안은 사용자와 AI 에이전트를 포함한 모든 행위자의 신원을 정확히 식별하고 상황에 맞는 적절한 접근 권한을 부여하며 의심스러운 활동을 지속적으로 모니터링하는 것을 목표로 한다. 그리고 이것은 사람과 AI가 안전하게 협업하고 시스템에 접근하기 위한 기본적인 전제 조건이 된다.

3.3. 플랫폼 가속화(Platform Acceleration): XDR, SASE, CNAPP 중심의 통합

단위 보안 솔루션의 한계를 극복하고 보안 시너지를 높이려는 목적의 통합은 언제나 중요한 화두 중에 하나이다. 작년에 이어 엔드포인트 탐지 및 대응(EDR)을 넘어 확장된 탐지 및 대응(XDR) 등이 핵심 개념으로 부상하며 많은 논의를 이끌었다.

XDR은 단말 뿐만 아니라 네트워크, 클라우드, 이메일 등 다양한 이 기종 솔루션에서 데이터를 수집하고 분석하여 개별 솔루션의 한계를 넘는 가시성과 자동화된 대응 역량을 제공하는 것을 목표로 한다. XDR은 기존 EDR 솔루션의 한계인 단말에 국한된 가시성, 과도한 경보(Alarm), 컨텍스트 부족 등의 한계를 극복함과 동시에 SIEM(Security Information and Event Mgmt.)에서 지적되는 시스템 복잡성, 높은 오탐율 그리고 자동 대응의 한계 등을 개선하려는 목적이 강하다. 따라서 XDR 플랫폼 내에서 AI 기술은 방대한 데이터의 자동 분석, 위협 상관관계 분석, 지능형 위협 탐지 그리고 자동화된 대응 등 핵심적인 역할을 수행하며 그 중요성이 더욱 커지고 있다.

XDR과 SIEM 그리고 SOAR(Security Operation, Automation and Response)의 관계는 지속적인 통합과 발전으로 점점 모호해지고 있다. XDR이 SIEM과 SOAR의 일부 기능을 통합하거나 강화하는 형태로 발전하고 있지만 로그 관리 및 컴플라이언스 중심의 SIEM이나 복잡한 워크플로우 자동화에 특화된 SOAR를 완전히 대체하기보다는 상호 보완적인 역할을 수행할 것으로 보인다. 특정 벤더에 종속(Native XDR)되지 않고 다양한 솔루션을 통합할 수 있는 개방형 XDR(Open XDR) 방식 역시 주목할 만하다.



['22, Chain of Event Vs '24, Next SIEM + Charlotte AI, Crowdstrike]

클라우드 환경, 특히 멀티 클라우드 및 하이브리드 환경에서 보안은 더욱 중요하며 복잡한 환경을 효과적으로 보호하기 위한 통합 솔루션으로 CNAPP(Cloud Native Application Protection Platform)의 중요성이 커지고 있다. CNAPP은 클라우드 보안 형상 관리(CSPM), 클라우드 워크로드 보호(CWPP), 클라우드 인프라 권한 관리(CIEM) 등 다양한 보안 기능을 단일 플랫폼에 통합하여 제공하는 것을 목표로 한다. 특히 클라우드 환경에서 AI 워크로드 대상 보안이 새로운 과제로 떠오르면서 AI 모델과 데이터 저장소에 대한 보안 상태 관리 및 위협 탐지 기능이 향후 CNAPP의 중요한 요소로 자리매김하게 될 것이다.

이러한 플랫폼 통합의 가속화는 분석가와 AI 에이전트가 단일화된 환경에서 정보를 공유하고 분석 결과를 교환하며 공동으로 대응 조치를 수행할 수 있는 기반을 마련한다는 점에서 중요하다. 통합 플랫폼은 사람과 AI간의 원활한 워크플로우 연동을 지원하고 보안 운영의 효율성과 효과성을 극대화하는 데 기여할 것이다.

3.4. 주요 산업 리더들의 전략: AI 통합과 플랫폼 확장

이번 행사에서 Microsoft, Cisco, Google 등 주요 선도 기업들은 AI 통합, 플랫폼 확장, 신원 및 클라우드 보안 강화라는 공통된 흐름 속에서도 각자의 강점과 비전을 바탕으로 차별화된 접근 방식을 제시했다. 이들 기업의 기술과 전략을 통해 미래 정보보호 시장에서 사람과 AI가 어떻게 협력해 나아갈 수 있는지를 예상해 보는 것은 의미 있는 일이라 생각한다.

3.4.1. Microsoft: AI 기반 SecOps 혁신 주도, 모든 곳에 Copilot을

Microsoft는 자사의 통합 보안 플랫폼(Microsoft Defender XDR + Microsoft Sentinel)을 중심으로 AI 기술을 접목하여 보안 운영(SecOps)을 혁신하겠다는 메시지를 강력하게 전달했다. 핵심 전략은 '보안을 위한 AI(AI for Security) 와 AI 자체의 보안(Security for AI)'을 동시에 추구하는 것으로 Microsoft Security Copilot을 필두로 자율적인 AI 에이전트 기능을 대거 선보이며 AI가 주도하는 미래의 SOC 비전을 제시했다.

Microsoft의 전략은 자사의 광범위한 클라우드 및 엔터프라이즈 소프트웨어 생태계를 기반으로 AI 기술을 보안 포트폴리오에 깊숙이 통합하고 Security Copilot 에이전트를 통해 단순한 보조 도구를 넘어 자율적인 보안 운영으로 나아가려는 의지를 보여준다. 이는 분석가가 AI 에이전트와 협력하여 방대한 데이터를 처리하고 신속하게 대응하는 모델을 지향하면서 AI의 자율성과 사람의 감독 및 신뢰 사이의 균형이 중요한 과제가 될 것임을 암시한다.

3.4.2. Cisco: 단말부터 네트워크/클라우드까지, AI 보안 생태계를

Cisco는 네트워킹 분야의 강점과 최근 인수한 Splunk의 역량을 결합하여 AI 시대의 보안 과제에 대응하겠다는 전략을 발표했다. 특히 AI 보안 기술의 보편화를 위해 보안에 특화된 추론 모델인 Foundation AI를 오픈소스로 공개하는 등 오픈소스 이니셔티브를 강조하며 업계 전반의 협력을 촉구하는 모습을 보였다.

Cisco의 전략은 강력한 네트워크 인프라와 Splunk의 데이터 분석 역량을 결합해 포괄적인 AI 기반 보안 플랫폼 구축을 목표로 하며 Foundation AI 공개를 통해 자사의 AI 보안 접근 방식에 대한 영향력을 확대하고 생태계를 구축하려는 의도로 해석된다. 이는 개발자와 분석가들이 Cisco의 AI 프레임워크를 통해 다양한 보안 솔루션을 개발하고 연동하여 활용할 수 있는 기반을 제공하며 개방형 협력을 통한 AI 보안 발전을 추구하는 모델을 염두에 둔 것이라고 볼 수 있다.

3.4.3. Google: 다 가지고 있는데, 더 잘 하기까지

Google Cloud Security는 Mandiant의 위협 인텔리전스와 Google의 AI(Gemini) 및 클라우드 기술력을 결합하여 인텔리전스 기반의 선제적 방어 체계를 구축하는 데 주력하는 모습을 보였다. Google Unified Security 플랫폼을 중심으로 Chronicle(SecOps), Security Command Center(클라우드 보안) 등 핵심 솔루션 전반에 걸쳐 Mandiant의 통찰력과 Gemini AI의 분석 능력을 통합하는 데 중점을 두었다.

Google은 최상위 위협 인텔리전스 및 사고 대응 전문성과 강력한 AI/클라우드 인프라를 결합하여 위협 탐지부터 대응까지 전 과정을 지능화·자동화하려는 목표를 분명히 보여준다. 특히 AI 자동화와 함께 Mandiant의 전문가 서비스를 확대하는 것은 AI가 대규모 데이터 처리와 신속한 초기 대응을 담당하되 복잡하거나 새로운 유형의 위협 분석 및 최종 판단에는 사람의 개입과 검증을 활용하는 '사람 참여형(Human-in-the-loop)' AI 모델을 제시하려는 의도로 보인다. 이는 AI의 효율성과 사람 전문가의 신뢰성을 결합한 공존의 모델을 추구하는 것으로 해석될 수 있다.

3.4.4. 기타 주요 경쟁사 동향

기타 주요 업체들의 방향 역시 크게 다르지 않았다. PaloAlto Networks는 Cortex XSIAM 3.0 과 Prisma Access Browser 출시를 언급하였으며, Protect AI의 인수를 통하여 SASE 플랫폼을 포함해 AI가 애플리케이션 환경과 보안을 근본적으로 변화시킬 것을 강조했다. CrowdStrike는 자사의 AI 플랫폼인 Charlotte AI 기반의 에이전틱 AI 기능(Agentic Response, Agentic Workflows)을 출시하고 Falcon 플랫폼 전반의 기능을 강화했다. SentinelOne은 SOC 분석가의 추론 및 조율 능력을 모방하는 에이전틱 AI 기능인 Purple AI 'Athena'를 선보이며 외부 데이터 소스와의 연동을 통한 통합을 강조했다.

이들 기업 모두 저마다의 사업영역과 강점을 보유하고 있으나 'AI 기반 SOC' 라는 공동의 목표를 향해 나아가면서 각 기업의 강점과 시장 전략에 따라 서로 다른 사람-AI 협력 모델을 제시하고 있음을 보여준다.

3.5. 시장 환경 및 미래 방향 예측

이번 행사의 트렌드는 향후 사이버 보안 시장의 몇 가지 중요한 변화를 명확하게 보여준다.

첫째, AI는 더 이상 미래 기술이 아닌 현재 시장을 주도하는 핵심 동력으로 자리 잡았다. 벤더들의 제품 로드맵과 고객들의 투자 우선순위 모두가 AI를 중심으로 재편되고 있으며 특히 에이전틱 AI는 사람과 AI의 협업을 기반으로 하는 차세대 보안 패러다임을 예고하기에 충분하다.

둘째, 경제 불확실성에도 불구하고 사이버 보안 지출은 지정학적 긴장 고조와 위협의 진화로 필수 투자 영역으로 인식되고 있으며 상대적으로 견조한 흐름을 유지할 것으로 예상된다. 특히 통합 플랫폼을 제공하는 기업들은 시장 성장률을 상회하는 성과를 보이고 있다.

셋째, XDR, SASE, CNAPP 등 플랫폼 기반 솔루션으로의 통합 및 전환이 가속화되고 있다. 이는 다양한 보안 기능을 단일 플랫폼에서 관리하고 분석가와 AI 에이전트가 원활하게 협력할 수 있는 환경을 제공한다.

넷째, 투자자들은 AI 우선 전략을 가진 혁신 기업에 높은 관심을 보이며 이는 시장의 가치 평가와 인수합병에도 영향을 주고 있다. Google의 Wiz 인수, Palo Alto Networks의 Protect AI 인수, CyberArk의 Venafi 인수 등은 AI 및 클라우드 보안, 신원 관리 분야의 중요성을 보여주는 사례라고 할 수 있다.

인수 기업	피인수 기업	시기(E)	주요 분야 / 목표
Google	Wiz	25년 3월	클라우드 보안 (CNAPP), 멀티 클라우드 경쟁력 강화
Palo Alto Networks	Protect AI	25년 4월	AI 보안 (모델, 데이터, 에이전트), Prisma AIRS 플랫폼 가속
Mastercard	Recorded Future	24년 9월	위협 인텔리전스 통합 사기 방지 및 ID 서비스 강화

인수 기업	피인수 기업	시기(E)	주요 분야 / 목표
CyberArk	Venafi	24년 10월	머신 아이덴티티 관리, 엔드투엔드 보안 플랫폼 구축
Sophos	Secureworks	24년 4분기	매니지드 보안 운영 (MSO) 확장
CrowdStrike	Adaptive Shield	24년 11월	SaaS 보안 상태 관리 (SSPM) 강화
N-able	Adlumin	24년 11월	MSP를 위한 SIEM/XDR 플랫폼
Wiz	Dazz	24년 11월	애플리케이션 보안 (AppSec) 및 CNAPP 내 교정 역량 강화
Cisco	Robust In telligence	24년 8월	AI 모델 보안 및 거버넌스 Cisco Security Cloud 통합
Armis Security	OTORIO	25년 3월	운영 기술 (OT)/산업 제어 시스템 (ICS) 보안 역량 확장

[사이버 보안 분야 주요 인수합병 (2024년 하반기 ~ 2025년 상반기)]

마지막으로, 사이버 보안 역량(사람 등)의 부족은 관리형 서비스(MDR, Managed XDR 등) 등의 성장을 촉진하고 있다. AI와 자동화가 이러한 문제의 해결사로 제시되는 동시에 위협 헌팅(Threat Hunting) 및 사고대응(Incident Response) 등의 영역에서 여전히 전문가의 중요성이 강조되는 현상은 흥미롭다. 이는 AI가 사람의 역할을 완전히 대체하는 것이 아닌 업무 방식을 변화시키고 있음을 시사한다. 미래의 보안 전문가는 AI를 효과적으로 활용하고 AI 시스템 자체의 보안을 관리하며 AI가 처리하기 어려운 고도의 분석 및 전략 수립 그리고 AI의 의사결정을 감독하는 역할을 수행하게 될 것이다. AI는 분석가의 업무를 지원하고 반복적인 작업을 자동화하는 동시에 AI 보안, 프롬프트 엔지니어링 등 새로운 기술에 대응하며 자연스럽게 업무 효율화를 이끌게 될 것이다.

04 연동과 협업: 솔루션간 연동을 넘어 AI시너지를 향하여

위협의 지능화·고도화와 더불어 공격 표면(Attack Surface)의 확대로 개별 정보보호 솔루션의 대응 한계는 분명해졌으며 솔루션 간 연동과 협업을 통해 통합적인 보안 체계를 구축하는 것이 필수 과제로 떠오르고 있다. 여기에 보안 전문가의 역량과 AI 기술이 더해져 각자의 강점을 바탕으로 상호 보완적인 역할을 수행하며 운영의 효율성과 위협 대응 역량을 높이는 방향으로 나아가야 한다.

4.1. 정보보호 환경 변화와 통합의 필요성 증대

최근 사이버 공격은 특정 시스템을 감염시키는 것을 넘어 다양한 경로로 침투 및 장기간 잠복하며 지능적 방식으로 목표를 달성하도록 진화하고 있다. 공격자들은 생성형 AI 기술을 사용해 더욱 정교한 스피어피싱 이메일을 작성하거나 악성코드를 제작하는 등 공격의 성공률과 파급력을 높이고 있다. 이러한 위협에 대응하기 위해서는 단일 보안 솔루션의 탐지 능력을 넘어 여러 보안 계층에서의 정보를 종합적으로 분석하고 연계 대응하는 체계가 필수적이다.

효율적인 위협 탐지 및 대응의 시작은 다양한 보안 이벤트를 통합하고 분석하여 위협에 대한 가시성을 확보하는 것이다. 단말, 네트워크, 클라우드, 이메일 등 다양한 계층의 이벤트를 한 곳에 모으고 분석을 통해 미래 공격의 징후 또는 장기간 진행된 공격의 전체적 맥락을 파악할 수 있다. 그러나 다수의 보안 솔루션을 개별적으로 운영하는 방식은 비효율성을 야기한다. 분석가는 다수의 개별 콘솔(대시보드)을 오가며 수동으로 데이터를 취합하고 분석한다. 이는 많은 시간과 노력이 필요할 뿐 아니라 중요한 위협을 놓칠 가능성도 증가한다. 더불어 관리의 복잡성과 너무 많은 이벤트에 의한 '경고 피로(Alert Fatigue)'는 오히려 중요한 이벤트의 대응 역량을 낮추거나 심지어 간과되기 일쑤다.

이러한 문제를 해결하기 위하여 보안 솔루션 간의 연동 및 자동화는 효과적인 보안 운영을 가능하게 하고 반복적이고 소모적인 작업에서 벗어나 고도의 분석 및 위협 헌팅과 같은 업무에 집중할 수 있도록 지원함으로써 인력 및 역량 문제에 대한 대안을 제시할 수 있다.

4.2. 통합의 시작 SIEM, SOAR 그리고 XDR 과 AI의 역할

정보보호 솔루션 간의 통합은 각 솔루션이 가진 고유한 강점을 극대화하고 상호 보완을 통해 전체적인 보안 수준을 향상시키는 것을 목표로 한다. 이러한 통합 보안 생태계에서 SIEM, SOAR, XDR은 기존 레거시 솔루션을 대상으로 통합의 토대를 제공하고 AI 등 미래 기술과의 협업을 위한 출발점을 제공할 수 있다.

- **SIEM(Security Information and Event Management, 보안 정보 및 이벤트 관리)**
  SIEM플랫폼은 조직 IT 인프라 전반에 걸쳐 다양한 시스템 및 보안 장비로부터 로그 및 이벤트 데이터를 수집하고 분석하는 대표적인 솔루션이다. SIEM은 데이터의 1차 저장소이자 분석 엔진의 역할을 수행한다. AI 기술은 수집된 방대한 데이터를 분석하여 알려지지 않은 위협이나 잠재적 위협 등을 발견하는데 도움을 줄 수 있다.

- **SOAR(Security Operation, Automation and Response, 보안 오케스트레이션, 자동화 및 대응)**
  SOAR플랫폼은 보안 운영 센터(SOC)의 업무 효율을 높이고 사고 대응 시간(MTDD, MTDR 등)을 단축하기 위한 솔루션으로 다양한 보안 도구와 프로세스를 통합하고 사전에 정의된 규칙(Playbook)에 따라 반복적 업무를 자동화하며 협업을 지원한다. AI는 SOAR 플랫폼에서 플레이북을 최적화하고 탐지된 위협의 특성, 범위 및 영향 등 다양한 컨텍스트를 고려하여 최적의 대응 방식을 추천하거나 조정할 수 있다. 분석가는 AI가 제안하는 자동화된 대응 조치를 검토하고 승인하며 복잡하거나 새로운 유형의 위협에 대해서는 직접 플레이북을 수정하거나 새로운 플레이북을 개발할 수 있다.

- **XDR(eXtended Detection and Response, 확장된 탐지 및 대응)**
  XDR은 엔드포인트, 네트워크, 클라우드 등으로 위협탐지 및 대응 범위를 확장하여 개별 보안 영역에서 발생하는 단일한 정보를 통합하고 상호 연관 분석하여 보다 정교하고 광범위한 공격 탐지 및 대응기능을 제공한다. 특히 XDR 플랫폼에서 AI 에이전트는 다양한 로그 및 데이터의 상관관계 등을 분석하여 알려지지 않은 위협을 탐지하고 최적화된 대응 조치를 제안할 수 있다. 분석가는 AI 에이전트에 의한 분석의 결과를 검토하고 제안된 내용을 확인하여 최종 의사결정을 내리고 이를 수행할 수 있다. 이러한 결정 및 조치는 다시 AI 에이전트의 성능 개선을 위한 데이터로 활용된다.

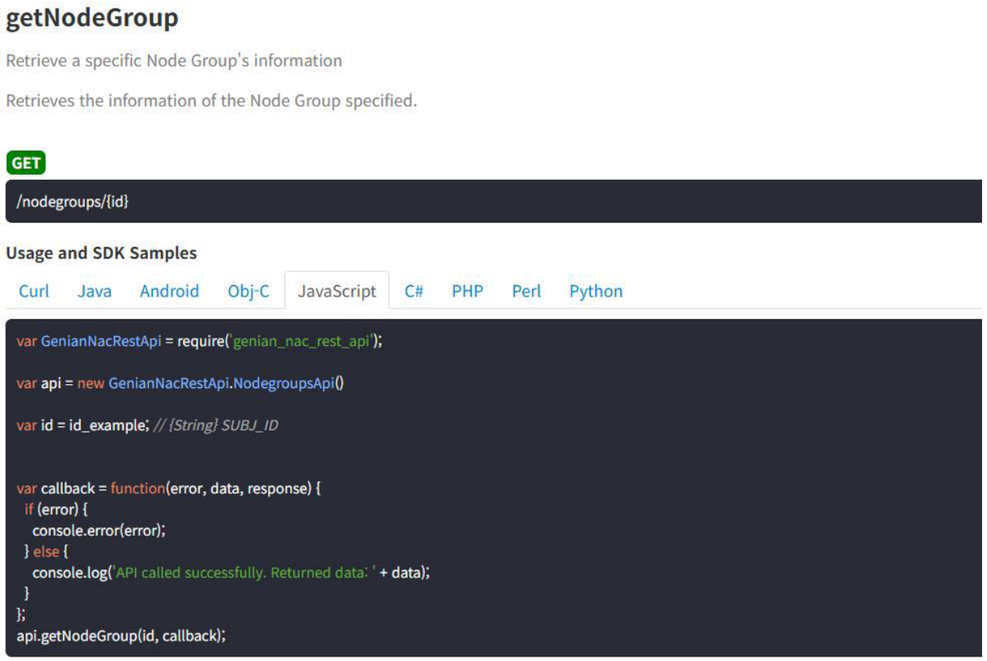
최근 이러한 솔루션 간의 협업 또는 통합이 가속화되고 있다. EDR이 네트워크 등 다양한 데이터를 수집·분석하기 위해 SIEM을 통합하여 위협 대응의 범위를 넓히고 XDR과 SOAR가 통합해 탐지된 위협에 대해 시나리오 기반으로 강력한 대응 기능을 제공한다. 이러한 가운데 AI는 대량의 데이터 처리, 반복적인 작업 자동화, 신속한 초기 분석 등에 적합하다. 이는 분석가의 업무를 경감시키고 AI의 분석 결과를 바탕으로 복잡한 의사결정, 창의적인 문제 해결, 전략 수립 등 보다 가치 있는 업무에 집중할 수 있게 도와준다.

4.3. 연동과 협업을 위한 열쇠, API(Application Programming Interface)와 로그(Log)

위에서 언급한 정보보호 솔루션 간의 효과적인 연동 및 협업, 그리고 더 나아가 사람과 AI 간의 원활한 상호작용을 위해서는 기술적인 상호 운용성 확보가 필수적이다. 이를 위해 다양한 표준 기술과 프로토콜이 활용된다.

- **API (Application Programming Interface, REST API, SOAP API 등)**
  API는 서로 다른 애플리케이션이 상호 작용하고 데이터를 교환할 수 있도록 하는 인터페이스 규약(칙)이다. 보안 솔루션 간의 연동 뿐 아니라 AI 에이전트가 다른 시스템의 데이터를 조회하거나 특정 기능을 호출할 때 역시 필요하다. 분석가가 AI 시스템과 상호작용하기 위해서도 API는 핵심적인 역할을 수행한다.

  - **REST API (Representational State Transfer):** 현재 연동을 위한 가장 대표적인 방식이다. (상대적으로)유연한 데이터 형식(주로 JSON), 경량화, 우수한 성능, 확장성, 개발 용이성 등 많은 장점으로 다양한 보안 솔루션 및 AI 시스템 연동에 가장 널리 사용된다. AI 에이전트는 REST API를 통해 위협 정보를 조회하고 분석 결과를 전송하며 대응을 위한 조치를 수행할 수 있다. 분석가 역시 REST API 기반의 대시보드나 인터페이스를 통해 AI의 분석 결과를 확인하고 중요한 의사결정 및 전략적 대응이 가능하다.



[Genian NAC의 API, NodeGroup정보를 요청하면 JSON 형태로 리턴 받는다]

  - **SOAP API (Simple Object Access Protocol):** XML(eXtensible Markup Language) 기반의 메시지 프로토콜로 구조화된 정보의 전송을 통해 높은 신뢰성과 강력한 기능을 제공할 수 있어 특정 환경(금융, 레거시 시스템 등)에서 주로 사용된다. REST 와 SOAP는 웹(Web) 기반의 통신이라는 점에서 유사하나 SOAP이 XML 기반 메시지를 사용하는 데 반해 REST는 HTTP 기반을 사용한다는 데 차이가 있다. 이러한 특성으로 SOAP은 REST와 대비해 보안과 트랜젝션 등 복잡한 기능을 지원할 수 있다.
  - **기타 API (gPRC, WebSocket 등):** 이 외에도 TCP 기반의 양방향 통신이 필요한 경우 WebSocket을 사용할 수 있다. HTTP 기반 REST와 달리 클라이언트와 서버가 연결되어 있어 실시간으로 데이터를 주고받을 수 있다. gRPC는 구글에서 개발한 RPC의 일종으로 원격지의 프로시저를 선택하고 매개변수를 전달하면 실행할 수 있다. 다양한 언어를 지원해 호환성이 좋고 타 프로토콜에 비해 빠르게 동작한다.

- **표준 로그 포맷 (Syslog, CEF, LEEF)**
  다양한 보안 솔루션에서 생성되는 로그는 각기 다른 형식을 가질 수 있다. 그 결과로 이를 통합하여 분석하고 이해하는 데 어려움이 있을 수 있다. 이는 AI 에게도 동일하다. 표준화된 로그 포맷은 이러한 문제를 해결하고 데이터의 상호 운용성을 높여 사람과 AI 모두에게 분석을 용이하게 한다.

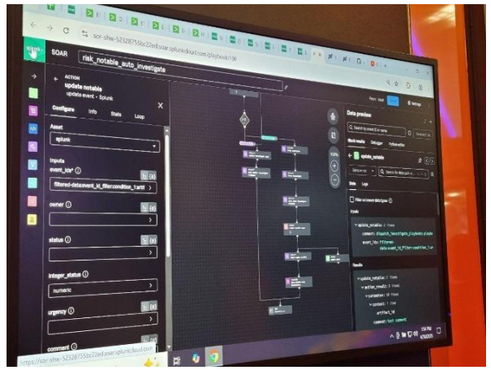
  - **Syslog:** IP 네트워크를 통해 이벤트, 알림 메시지 등을 중앙 로그 수집 서버로 전송하기 위한 가장 대표적인 프로토콜이다.
  - **CEF (Common Event Format) 및 LEEF (Log Event Extended Format):** 다양한 보안 솔루션 및 애플리케이션에서 생성되는 로그 및 이벤트를 표준화하여 상호 운용성을 높이기 위한 개방형 로그관리 표준이다. 둘 다 syslog 기반의 표준 로그 포맷으로 주로 SIEM과 연동하기 위해 사용된다. AI는 수집된 로그 데이터를 학습하여 위협 패턴을 식별하고 이상 징후를 탐지하는 데 활용할 수 있다.

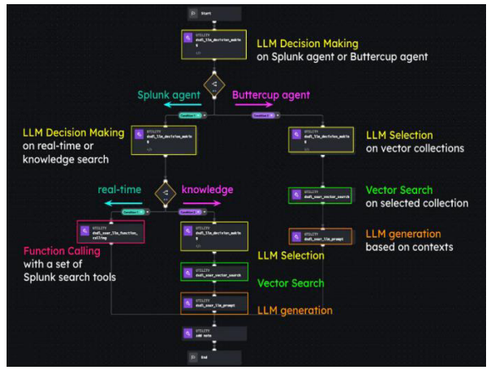
이러한 기술적 기반 위에서 사람과 AI는 데이터를 공유하고 분석 결과를 교환하며 공동으로 대응 조치를 수행할 수 있는 환경을 구축할 수 있다. 특히 AI가 다양한 소스로부터 정형/비정형 데이터를 효과적으로 수집하고 이해하기 위해서는 개방형 표준과 잘 정의된 API가 필수적이다.

4.4. 워크플로우(Workflow)의 부상: 사람과 AI 협업 프로세스 고도화

최근 XDR 및 SOAR 솔루션에서 기존 플레이북에 더하여 워크플로우를 적용하는 사례가 증가하고 있다. 이는 날로 고도화되는 위협에 보다 빠르고 정확하게 대응하기 위해 사람과 AI가 협력하여 보안 운영의 효율과 대응 효과를 극대화하려는 전략으로 예상된다.

- **워크플로우(Workflow)와 플레이북(Playbook)**
  워크플로우는 특정 작업이나 사고 등에 대응하기 위해 사전에 정의된 일련의 자동화(또는 반자동화)된 단계와 의사결정 지점의 집합을 의미한다. 플레이북은 특정 보안 이벤트나 경고에 대응하기 위해 수행해야 할 조치 순서를 구체적으로 명시한 것으로 조직의 보안 대응 절차, 모범 사례 그리고 축적된 지식 등을 코드화 한 것이다. 워크플로우와 플레이북은 비즈니스와 IT에서 서로 연관된 개념이지만 그 범위와 목적이 서로 다르다. 워크플로우는 반복적인 작업과 프로세스를 관리하기 위한 보다 광범위한 시스템인 반면, 플레이북은 특정 시나리오나 이벤트를 처리하도록 설계된 구체적이고 세부적인 절차이다.





[AI Agent Workflow, SPLUNK]

워크플로우와 플레이북에는 각 단계별로 분석가의 역할과 AI 에이전트의 역할을 명확하게 정의될 수 있다. 예를 들어 초기 경고 및 1차 분석은 AI가 담당하고 추가·심층 분석 및 최종 대응 결정은 사람이 담당하는 형태로 협업 프로세스를 설계하는 것이 가능하다.

- **워크플로우 도입의 주요 동인**

  자동화된 워크플로우 도입의 궁극적인 목적은 평균 탐지 시간(MTTD) 및 평균 대응 시간(MTTR)의 단축이라고 할 수 있다. 이를 위해 반복 작업의 자동화와 일관되고 표준화된 대응 절차를 제공하여 분석가의 번아웃을 예방하고 보안팀의 운영 효율 및 사고대응 역량을 강화할 수 있다. 결국 AI는 워크플로우의 각 단계에서 분석가의 업무를 보조하거나 자동화하여 분석가가 보다 전략적이고 가치 있는 업무에 집중할 수 있도록 지원한다.

- **자동화된 워크플로우 사례: 피싱 대응, 악성코드 확산 방지 등**

  - 피싱 이메일 분석 및 대응: AI가 피싱 의심 이메일을 1차 분석하고(첨부파일, URL, 샌드박스 분석, 평판 조회 등), 악성으로 판단 시 자동으로 차단하거나 사용자에게 경고를 보낸다. 분석가는 AI의 판단 결과를 검토하고 필요한 경우 추가 조치를 취하거나 오탐 여부에 대응한다.

  - 악성코드 감염 확산 방지: AI가 EDR/XDR로부터 악성코드 감염 이벤트를 수신하면 자동으로 감염 단말을 격리하고 (방화벽 등) C&C 서버 통신을 차단하며(샌드박스 등) 악성코드 샘플을 분석 시스템으로 전송한다. 분석가는 AI의 대응 상황을 모니터링하고 치료/복구 절차를 지휘하거나 AI가 탐지하지 못한 추가적인 확산 경로를 조사할 수 있다.

이처럼 워크플로우 기반의 보안 운영은 사람과 AI, 각자의 강점을 최대한 발휘하며 시너지를 창출할 수 있는 협업의 장을 제공한다. AI는 속도와 확장성을 제공하고 사람은 통찰력과 최종 판단력을 제공하여 보다 효과적이고 효율적인 보안 대응 체계를 구축할 수 있다.

4.5. 자동화된 보안운영: Autonomous SOC(Security Operation Center)

이제 인공지능(AI), 머신러닝(ML), 생성형(Gen) AI 등의 기술은 현대의 정보보호 분야에서 없어서는 안 될 핵심 요소로 자리매김하고 있다. 특히 해당 기술들은 복잡한 IT 환경에서 보안 솔루션 간, 또는 사람과의 협업을 위해 워크플로우와 함께 위협 대응 역량을 확장하고 보완하는 역할을 수행할 것으로 예상한다.

- **AI 기반 위협 탐지 및 분석: 분석가 능력 강화**

  AI/ML 알고리즘은 방대한 양의 보안 데이터를 분석하여 분석가가 수동으로 식별하기 어려운 미묘한 이상 행위, 알려지지 않은 신종 악성코드, 그리고 복잡하게 얽힌 공격의 초기 징후를 탐지하는 데 탁월한 능력을 발휘한다. AI는 수많은 보안 경고 중에서 실제 위협과 오탐을 구분하고 위험도에 따라 경고의 우선순위를 지정함으로써 분석가가 가장 시급하고 중요한 위협에 집중할 수 있도록 지원한다.

- **워크플로우 및 AI 활용: 분석가의 전략적 판단 지원**

  AI는 SOAR 플랫폼의 플레이북 실행 과정에도 적용되며 단순한 자동화를 넘어 보다 지능적인 의사결정을 내리고 상황에 따라 대응 방식을 조정하는 데 기여할 수 있다. AI는 탐지된 위협의 특성, 자산의 중요도 등 컨텍스트(Context)를 종합적으로 고려하여 가장 적절한 플레이북을 선택하거나 또는 플레이북 내의 특정 조치 순서나 범위를 동적(Dynamic)으로 조절하여 분석가의 전략적 판단 및 대응을 지원한다.

- **분석가를 위한 생성형 AI: 사람과 AI의 상호작용 및 협업 기반**

  생성형 AI는 분석가의 업무를 직접적으로 지원하는 강력한 도구로 활용될 수 있다. LLM 기반 AI 어시스턴트를 이용하면 자연어 질의를 통해 방대한 데이터를 검색하여 (복잡한) 보안 사고의 원인과 영향을 확인할 수 있다. 위협인텔리전스(Threat Intelligence)와 교차분석이 가능하며, 보고서 초안이나 대외 커뮤니케이션을 위한 문서를 작성하는 데에도 도움을 줄 수 있다. 이는 사람과 AI가 직접 상호작용하며 지식을 공유하고 공동으로 문제를 해결하는 새로운 협업 모델을 제시한다.

- **설명 가능성(Explainability)과 신뢰성(Trustworthiness)**

  AI가 자동화된 의사결정, 특히 XDR/SOAR 워크플로우 내에서 중요한 역할을 수행함에 따라 AI 모델의 판단 근거를 사람이 이해하고 신뢰할 수 있도록 하는 설명 가능성과 신뢰성이 매우 중요한 과제로 부각된다. 분석가가 AI의 판단을 이해하고 신뢰할 수 있어야 진정한 협업이 가능하며 자동화의 이점을 최대한 활용할 수 있다.

이처럼 인공지능(AI)은 단순한 보조 및 지원의 역할을 넘어 대응의 전 단계에 깊이 관여하며 '두뇌' 로서 역할의 가능성을 보여주고 있다. 향후 AI는 보안 전문가의 역량을 확장하고 반복적인 업무로부터 해방시키며 보다 창의적이고 전략적인 업무에 집중할 수 있도록 지원함으로써 사람과 AI가 함께 만들어가는 새로운 보안의 미래에 중추적 역할을 할 것으로 기대된다.

05 결론 및 제언: 사람과 AI, 새로운 보안 협력 시대를 열다

이번 RSAC 2025에서 보여준 다양한 트렌드와 보안 솔루션의 연동 및 협업은 명확한 메시지를 전달하고 있다. 정보보안은 이제 사람의 역량에 의한 범위를 넘어 생성형 AI를 포함한 인공지능(AI) 기술과의 상생을 통해 새로운 차원으로 발전해야 한다는 점이다. 사이버 위협의 고도화·지능화와 공격 표면의 확대로 전통적인 보안 방식은 한계에 직면했으며 사람과 AI가 각자의 강점을 최대한 발휘하고 상호 보완하여 더욱 강력하고 지능적인 보안 체계를 구축하는 것이 필수적인 시대가 된 것이다.

본 보고서에서 살펴본 바와 같이 에이전틱 AI의 부상, 신원 중심 보안의 지속적인 중요성, XDR·SASE·CNAPP 중심의 플랫폼 통합 가속화는 모두 사람과 AI의 협력을 기반으로 더욱 효과적인 보안을 달성하려는 노력의 일환이다. AI는 방대한 데이터 분석, 신속한 위협 탐지, 반복 업무 자동화 등에서 사람을 보조하고, 사람은 AI의 분석 결과를 바탕으로 최종 의사결정을 내리고 복잡한 문제를 해결하며 AI 시스템을 감독하고 개선하는 역할을 담당해야 할 것이다. 이러한 '사람-AI' 공존의 시대를 성공적으로 맞이하기 위해 조직은 다음과 같은 사항에 대하여 적극적으로 고려하고 준비할 것을 제안한다.

1. **전략자산 및 AI 거버넌스 확립:** AI를 보안 전략의 핵심 요소로 인식하고 AI 도입 및 활용에 대한 명확한 로드맵과 함께 AI 모델의 보안, 데이터 프라이버시, 윤리적 사용 등을 포괄하는 AI 거버넌스 체계를 수립해야 한다.

2. **프로세스 우선 정의 및 표준화:** 자동화 및 AI 도입에 앞서 기존 보안 운영 프로세스를 명확하게 정의하고 표준화 하여 사람과 AI가 협업할 수 있는 기반을 마련해야 한다.

3. **통합 플랫폼 구축 및 개방형 생태계 활용:** XDR, SOAR, SIEM 등 기반 솔루션들을 효과적으로 통합하고 필요에 따라 개방형 표준 및 API 등을 활용하여 다양한 AI 기술 및 외부 인텔리전스와의 연동을 위해 노력해야 한다.

4. **분석가의 AI 활용 역량 강화:** 분석가는 AI를 효과적으로 활용하고 AI의 분석 결과를 비판적으로 검토하며 AI 시스템을 관리하고 개선할 수 있는 기술과 지식을 습득해야 한다. AI 프롬프트 엔지니어링, AI 모델의 이해 및 데이터 분석 역량 등이 미래 보안 전문가의 중요한 능력이 될 것이다.

5. **단계적 접근 및 지속적인 검증:** AI 기반 자동화 및 협업 모델의 적용을 위해 유의미하며 작은 성공사례(Small Success)를 발굴할 필요가 있다. 여기서 얻은 교훈과 시행착오를 바탕으로 점진적으로 확대해야 한다. 지속적으로 AI의 판단과 결과에 대한 검증 및 감독체계를 갖출 필요가 있다.

미래의 보안 운영은 단순한 '자동화(Automated)'를 넘어 사람과 AI가 유기적으로 결합해 새로운 위협을 발견하고 스스로 위협에 대응하며 근본적인 재발을 방지하고 최적화하는 '자율적인(Autonomic)' 형태로 발전할 가능성이 높다. 이러한 과정에서 분석가의 역할은 일상적인 운영에서 벗어나 AI시스템 감독, 최상위 전략의 수립 그리고 복잡하고 새로운 예외 상황 처리에 집중하도록 변화될 것으로 예상된다.

결론적으로 정보보호의 미래는 사람과 AI의 성공적인 파트너십에 달려있다. 기술의 발전은 계속될 것이며 위협은 더욱 교묘해질 것이다. 끊임없는 창과 방패의 싸움에서 승리하기 위해서는 사람의 창의성과 직관력, 그리고 AI의 분석력과 속도를 결합하여 함께 배우고, 함께 대응하며 함께 진화하는 새로운 보안 협력 시대를 적극적으로 만들어가야 할 것이다.

정보보호ISC가 바라본 RSAC 2025를 통해 조망한 ISC의 역할과 시사점

- **AI 도입에 따른 정보보호 직무 변화와 역량의 재정립**

  AI 시대의 도래로 정보보호업계의 업무환경과 요구되는 직무역량이 빠르게 변화하고 있다. 특히 AI 기술을 기존 업무에 접목해 활용하는 능력은 필수 역량으로서 자리잡을 것으로 보인다. 산업 전반의 업무 프로세스나 수행행위의 변화가 불가피할 것으로 예상되기에, 정보보호 인력이 변화하는 환경에 적응하고 향후 등장할 새로운 직무에 대비할 수 있도록 AI 도입에 따른 직무 및 역량의 변화 양상을 분석하여 전망을 도출할 필요가 있다. 또한 연구결과를 활용하여 산업현장에 맞는 인재를 양성·확보하기 위해 국가직무능력표준 개발·개선과 이에 기반한 교육과정 개발 등을 추진해야 할 것이다.

- **안전한 AI 활용을 위한 AI '보안' 리터러시 확산**

  AI의 자동화·최적화·예측 기능 고도화는 산업 전반의 생산성을 크게 향상시키는 한편, 새로운 유형의 보안 위협을 초래한다. 이러한 상황에서 '정보보호'는 더 이상 특정 산업이나 기술에 국한된 과제가 아닌, 사회 전체가 공동으로 대응해야 할 이슈로 부상하고 있다. 이와 같은 변화에 효과적으로 대응하기 위해, 향후 AI를 실질적으로 활용하는 모든 산업 종사자가 기본적인 보안역량을 갖출 수 있도록 'AI 보안 리터러시' 교육의 개발과 확산에 나서야할 것이다. 또한 AI의 안전하고 윤리적인 활용을 보장할 수 있도록 관련 거버넌스 구축을 정책적으로 뒷받침하는 역할에 집중할 필요가 있다.

보안역량을 사회 전반에 내재화하고 정책-산업현장–일자리 간 유기적 연계를 통해 급변하는 인력수요에 체계적으로 대응할 수 있는 기반을 마련함으로써, 안전하고 지속가능한 AI 활용 환경 조성에 기여해야 할 시점이다.

정보보호 인적자원개발위원회

Issue Report

2025 정보보호 트렌드: 사람과 AI, 새로운 협력의 시대

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

(05717) 서울특별시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회