RSAC 2026 Insight Report
Security Operations & MDR Landscape

AI SOC 시대, MDR은 어떻게 달라지는가

RSAC 이후, AI 보안 위협과 운영 기준의 재정의

기술을 넘어, 속도와 판단이
보안 경쟁력을 결정하는 시대

pago

The Global MDR Frontline
Owning the Decisions That Matter Most

본 리포트는 RSAC 2026에서 확인된 보안 시장의 구조적 변화에 대한 분석을 출발점으로 삼는다. 그러나 이러한 변화는 컨퍼런스 현장에서 끝나지 않았다.

RSAC 종료 이후, Mythos AI를 중심으로 한 새로운 변수와 논의가 빠르게 확산되며, AI 기반 보안 위협과 대응에 대한 시장의 인식 역시 다시 한 번 크게 흔들리고 있다.

이에 본 리포트는 RSAC에서 확인된 방향성에 더해, 최근 발생한 Mythos 관련 이슈와 그에 따른 시장 반응까지 함께 반영함으로써, 현재 보안 환경을 보다 입체적으로 조망하고자 한다. 특히 AI 기반 위협에 대한 과도한 공포와 실제 위험 사이의 간극을 짚고, Security Operations 관점에서 조직이 무엇을 준비해야 하는지를 중심으로 분석을 전개한다.

목차

MDR
in the
AI SOC
Era

AI SOC의 부상, MDR의 재정의, 그리고 PAGO가 서 있는 위치

RSAC 2026은 단순히 "AI가 화두였다"는 수준으로 정리하기에는 부족한 행사였다. 올해 RSAC는 보안 업계가 더 이상 개별 제품 중심의 경쟁만으로는 시장을 설명할 수 없으며, 운영 중심의 보안 모델(Security Operations)로 무게중심이 확실히 이동하고 있음을 보여준 무대였다.

RSAC 2026은 샌프란시스코 모스콘 센터에서 3월 23일부터 26일까지 열렸으며, 700명 이상의 연사, 31개 트랙, 570개 이상의 세션, 600개 이상의 전시 부스가 운영됐다. 행사 전반의 문제의식 역시 "AI가 사이버 리스크와 방어를 동시에 가속하는 시점"에 맞춰져 있었다.

이번 행사에서 가장 선명하게 드러난 흐름은 세 가지였다.

- 첫째, MDR이 더 이상 일부 전문 사업자의 차별화 서비스가 아니라 시장의 기본 언어가 되었다는 점이다.
- 둘째, AI가 보안 운영에 깊숙이 들어오면서 SOC 자체가 'AI SOC' 혹은 'Agentic SOC'로 재정의되고 있다는 점이다.
- 셋째, 그럼에도 불구하고 최종 승부는 여전히 누가 더 정확하게 판단하고, 더 책임 있게 대응하느냐에 달려 있다는 사실이다.

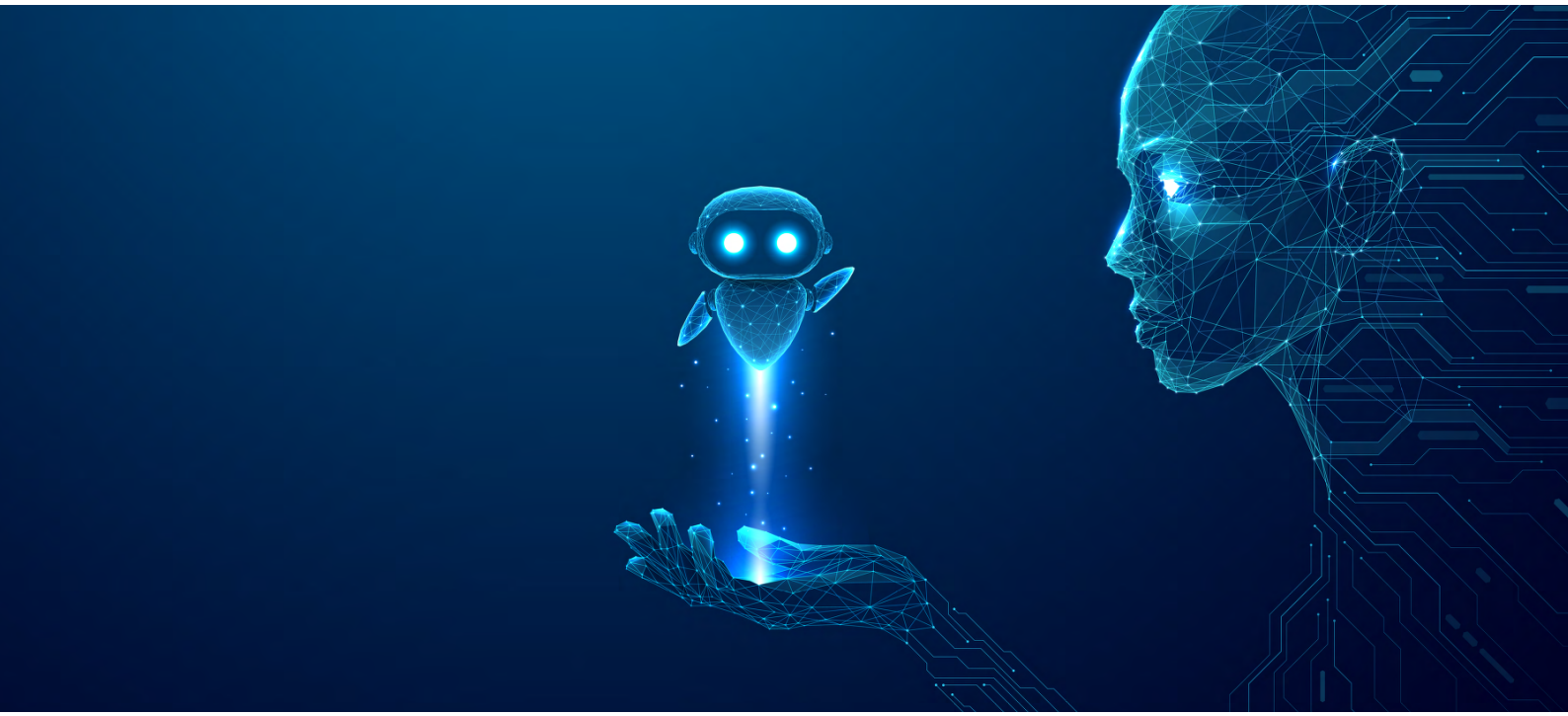
이러한 흐름은 최근 보안 업계 전반에서 나타나고 있는 방향성과도 맞닿아 있다. 단순한 기술 트렌드의 변화가 아니라, 보안 운영 모델 자체가 'Security Operations Platform + MDR' 구조로 재편되고 있으며, 이번 RSAC 현장에서는 이러한 변화가 이미 빠르게 현실화되고 있음을 확인할 수 있었다.

1. RSAC 2026의 핵심: AI는 기능이 아니라 운영

올해 RSAC를 관통한 가장 큰 키워드는 단연 AI였다. 그러나 중요한 것은 "AI가 많았다"는 사실이 아니라, AI가 어떤 역할로 들어오고 있었는가이다. RSAC 측도 사전 콘텐츠를 통해 AI security, cloud attacks, emerging threats가 2026년 주요 세션과 논의의 중심이 되고 있음을 강조했으며, 실제 현장에서도 AI는 더 이상 부가 기능이 아니라 보안 운영 구조 자체를 재설계하는 요소로 제시됐다.
특히 눈에 띈 점은, 'AI가 분석가를 완전히 대체한다'는 단순한 주장보다는 초기 분석·분류·조사 과정을 얼마나 빠르게 수행할 수 있는지에 초점이 맞춰졌다는 것이다.

이번 RSAC에서 부상한 AI SOC 플랫폼 사업자들은 레벨 1 분석가가 수행하던 초기 triage 업무를 agentic AI로 자동화하거나 최소화하는 방향을 강조하고 있었으며, 최종 판단과 책임은 여전히 사람의 역할로 남겨두고 있었다. 이 부분은 매우 중요하다. 시장은 "Autonomous"라는 표현을 강하게 사용하고 있지만, 실제로는 완전 무인화보다는 '분석가 증강'에 더 가까운 방향으로 진화하고 있다. 다시 말해, AI는 보안 운영의 앞단을 가속하고 정리하는 엔진으로는 빠르게 자리잡고 있으나, 사고의 의미를 규정하고 실제 대응을 결정하는 마지막 단계는 여전히 인간의 영역으로 남아 있다.

이는 MDR 서비스의 본질이 자동화가 아니라, 최종 판단과 대응 책임에 있음을 분명히 보여준다.



2. 올해 RSAC가 보여준 진짜 변화: “누구나 MDR”에서 “누가 제대로 운영하느냐”로

몇 년 전만 해도 MDR은 제한된 범위에서 활용되던 보안 운영 모델이었으나, 이제는 시장 전반으로 빠르게 확산되고 있다. RSAC 2026은 그 다음 단계로의 전환을 보여준다. 이제는 대형 벤더, 플랫폼 기업, 전문 서비스 업체를 막론하고 거의 모든 플레이어가 MDR를 이야기하는 상황이다. 그러나 중요한 것은 그 이후다. **누구나 MDR을 말하는 시대에서는 ‘진짜 MDR’과 ‘Managed EDR’ 수준의 서비스가 보다 명확하게 구분되기 시작한다.**

일반적으로 Managed EDR은 엔드포인트 중심의 탐지와 알림, 그리고 기본적인 대응 권고에 초점을 맞추는 반면, MDR은 위협의 맥락을 종합적으로 분석하고 우선순위를 판단하며, 필요 시 격리·차단·정책 변경 등 실제 대응까지 포함하는 운영 모델이다. 또한 MDR은 단일 솔루션에 국한되지 않고, EDR, NDR, XDR, 네트워크, 계정, 이메일 등 다양한 보안 영역에서 수집된 이벤트를 통합적으로 분석해 공격의 흐름을 이해하고 대응하는 데 목적을 둔다.

결국 두 모델의 차이는 ‘무엇을 탐지하느냐’보다, ‘탐지 이후 무엇을 결정하고 어디까지 대응하느냐’에 있다. 이러한 변화는 고객의 평가 기준에도 그대로 반영되고 있다. 이제 단순히 **“24x7 모니터링을 제공한다”**는 설명만으로는 충분하지 않다. 고객이 실제로 확인하고자 하는 것은 보다 구체적이다.

- 실제 위협 발생 시 누가 판단하는가
- 분석 결과에 대한 책임은 누구에게 있는가
- 대응은 어디까지 수행되는가
- 기존에 운영 중인 다양한 보안 솔루션을 통합적으로 운영할 수 있는가

이러한 기준에서 보면, RSAC 2026은 MDR의 대중화를 보여준 행사라기보다, MDR의 기준이 한 단계 높아졌음을 보여준 행사로 해석할 수 있다. 이는 MDR의 경쟁력이 단순한 기술이나 기능이 아니라, 운영의 깊이와 의사결정 구조에 의해 결정된다는 점을 시사한다.

> **누구나 MDR을 말하는 시대에서는 ‘진짜 MDR’과 ‘Managed EDR’ 수준의 서비스가 보다 명확하게 구분되기 시작한다.**

3. 벤더별 RSAC 2026 포인트: 무엇을 말했고, 무엇을 노렸는가

CrowdStrike: Agentic SOC를 중심으로 한 플랫폼 전략의 구체화

공식 RSAC 2026 발표에서 CrowdStrike는 “Securing the AI Era Together”라는 메시지와 함께, 보다 직접적으로는 “the future of the agentic SOC”를 핵심 방향으로 제시했다. 조지 커츠 CEO의 키노트 역시 AI 보안과 거버넌스를 중심으로 구성되었으며, Falcon 플랫폼 Spring ’26 릴리스를 통해 AI, 통합 데이터, 플랫폼 기반 보안 전략을 강조했다. 특히 “엔드포인트를 AI 보안의 중심축으로 삼는다”는 메시지는, 기존 엔드포인트 보안을 넘어 AI 시대의 보안 운영 구조를 재정의하려는 의도를 보여준다.

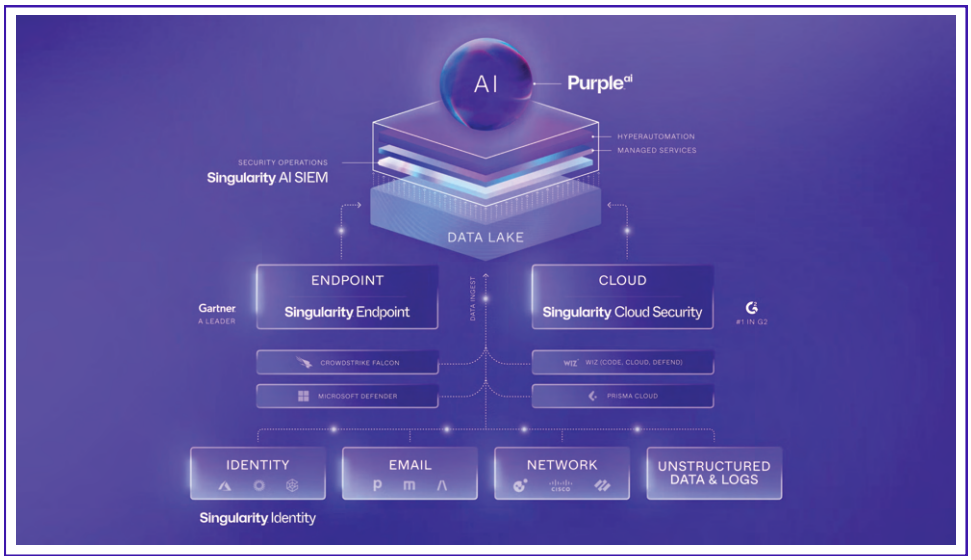
이번 RSAC에서 CrowdStrike는 단일 제품 중심 접근을 넘어, 플랫폼 기반 보안 전략을 한층 구체화한 모습을 보였다. MDR를 별도의 서비스가 아닌 기본 제공 모델로 포함하고, AI 기능, 데이터 통합, 운영 자동화, 그리고 유연한 소비 모델을 결합한 구조를 통해 보안 운영 전반을 하나의 플랫폼 안에서 제공하는 방향을 강조했다.

특히 SMB 및 미드마켓을 포함한 다양한 고객군을 대상으로 MDR를 기본 옵션처럼 제공하는 구조와, 고객 환경 및 예산에 따라 기능을 유연하게 조합할 수 있는 소비 모델은 주목할 만한 변화로 해석된다. 이는 보안 솔루션 도입 방식이 단일 제품 선택에서 벗어나, 운영 중심의 통합 플랫폼 기반으로 재편되고 있음을 보여주는 사례로 볼 수 있다.

이러한 흐름은 보안 시장 전반이 제품 중심 경쟁에서 벗어나, 플랫폼과 운영을 결합한 구조로 이동하고 있음을 시사한다. 특히 AI를 기반으로 한 SOC 운영 모델이 현실화되면서, 개별 기능보다 이를 어떻게 통합하고 운영할 것인가에 대한 중요성이 더욱 커지고 있다.

SentinelOne: Purple AI를 중심으로 한 '설명 가능한 자동화'의 진전

SentinelOne은 RSAC 2026에서 Purple AI를 중심으로 한 AI 기반 보안 운영 전략을 보다 구체화했다. 공식 발표에 따르면, Purple AI Auto Investigation은 일반 제공(GA) 단계에 진입했으며, 분석가는 단일 인터페이스에서 자동화된 조사(agentic investigation)를 수행할 수 있다. 이 기능은 플랫폼 전반에서 증거를 수집하고 위협 데이터를 종합해 실시간 공격 타임라인을 구성하며, Hyperautomation과 연계해 대응까지 이어지는 구조를 갖추고 있다.



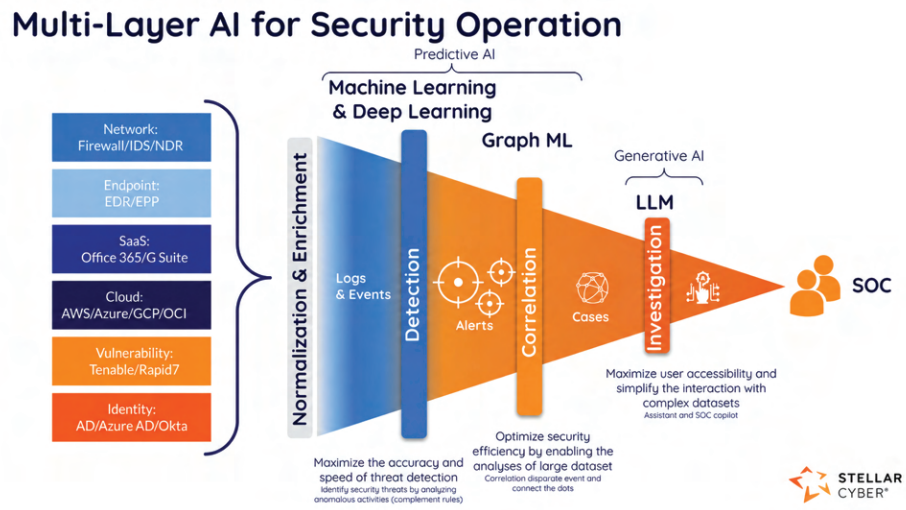
특히 SentinelOne은 이러한 자동화 기능과 함께 'analyst-in-the-loop governance'를 강조하고 있다. 이는 AI를 통해 조사와 분석 과정을 가속화하되, 최종 판단과 운영 통제는 여전히 사람의 역할로 남겨두는 접근 방식이다.

이러한 흐름은 AI 기반 보안 운영이 단순한 자동화를 넘어, '설명 가능성과 통제 가능성'을 함께 요구하는 방향으로 발전하고 있음을 보여준다. 즉, 보안 운영에서 중요한 것은 자동화의 수준 자체보다, 자동화된 결과를 어떻게 해석하고 의사결정으로 연결할 수 있는가에 있다.

또한 SentinelOne의 접근은 EDR 중심에서 벗어나, 조사·분석·대응을 통합한 운영 플랫폼으로의 확장을 시사한다. 이는 보안 시장이 개별 기능 중심에서 벗어나, AI와 자동화를 기반으로 한 통합 운영 구조로 이동하고 있음을 보여주는 사례로 볼 수 있다.

Stellar Cyber: Open XDR에서 Human-Augmented Autonomous SOC로의 확장

Stellar Cyber는 RSAC 2026에서 "Human-Augmented Autonomous SOC"라는 메시지를 전면에 내세우며, AI와 사람의 역할을 결합한 보안 운영 모델을 강조했다. 공식 행사 페이지에서도 "GenAI + Human Expertise = The Future of SecOps"라는 표현을 사용하며, Multi-Layer AI와 보안 전문가의 결합을 통해 alert noise와 false positives를 줄이고, cloud와 on-prem 환경 전반의 triage를 자동화하며, 실행 가능한 고충실도(high-fidelity) 케이스를 제공한다고 설명했다.



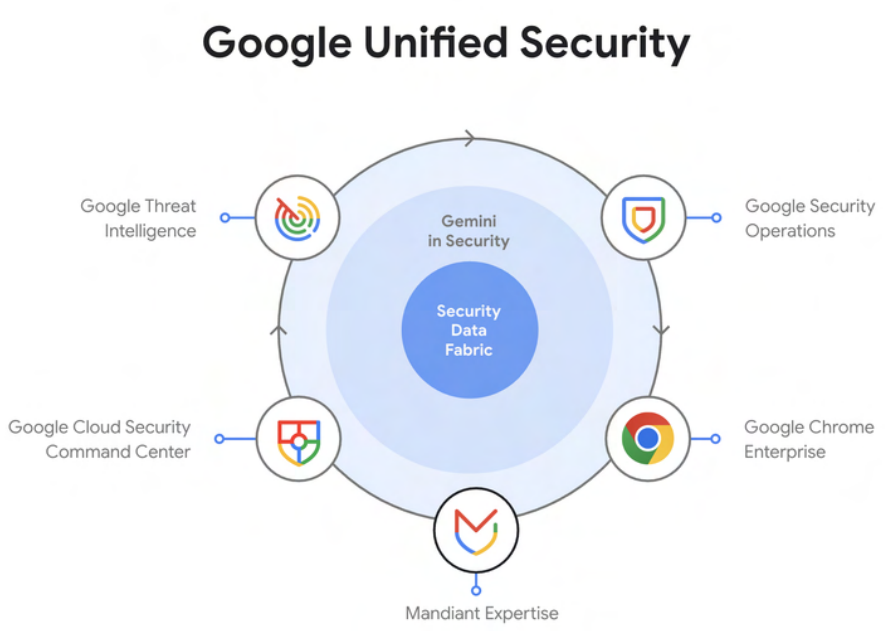
이와 함께 Stellar Cyber는 Open XDR, AI-driven SIEM, NDR/OT, ITDR, UEBA를 하나의 운영 구조 안에서 통합하는 방향을 제시하고 있다. 특히 MSSP와 MDR 사업자 친화적 구조를 함께 강조하고 있다는 점은, 단일 제품 판매보다는 다양한 환경을 묶어 운영 효율을 높이는 플랫폼 전략에 무게를 두고 있음을 보여준다.

이러한 접근은 보안 운영 시장이 폐쇄형 단일 제품 구조보다, 다양한 데이터와 기능을 연결할 수 있는 개방형 운영 모델로 이동하고 있음을 시사한다. 또한 AI 기반 자동화가 확대되더라도, 최종적으로 의미 있는 케이스를 만들고 운영 판단으로 연결하는 과정에서는 사람의 역할이 여전히 중요하다는 점을 분명히 하고 있다.

결국 Stellar Cyber가 보여준 방향은, 향후 MDR 시장에서 경쟁력이 단일 탐지 기능보다 개방형 구조 위에 얼마나 정교한 운영 체계를 구축할 수 있는가에 달려 있음을 보여주는 사례로 볼 수 있다.

Google Security: SecOps와 Threat Intelligence의 결합이 보여준 새로운 가능성

Google Security는 RSAC 2026에서 AI-powered defense, cloud security, active defense를 중심으로 한 보다 선명한 보안 운영 청사진을 제시했다. 공식 요약 페이지와 관련 발표에서는 M-Trends 2026, agentic SOC, Gemini 기반 reasoning, frontline threat intelligence, Wiz 통합, Mandiant 리서치 등을 유기적으로 묶으며, 단순한 제품 전시를 넘어 보안 운영 전반을 아우르는 구조를 부각했다.



특히 주목할 부분은 Security Operations와 Threat Intelligence가 별개의 기능으로 제시되는 데 그치지 않고, 실제 운영 과정에서 상호 보완적으로 연결되는 구조를 보여줬다는 점이다. 이는 보안 운영에서 단순히 많은 데이터를 보유하는 것보다, 그 데이터를 얼마나 빠르게 해석하고 의사결정에 연결할 수 있는가가 점점 더 중요해지고 있음을 보여준다.

이러한 흐름은 앞으로의 SOC가 단순히 이벤트를 수집·상관 분석하는 체계를 넘어, AI와 TI를 결합해 위협의 의미를 더 빠르게 해석하고 판단 품질을 높이는 방향으로 진화하고 있음을 시사한다. 특히 클라우드 환경과 하이브리드 인프라가 복잡해질수록, SecOps와 Threat Intelligence의 결합은 선택이 아니라 필수 요소에 가까워질 가능성이 크다.

Google Security가 이번 RSAC에서 보여준 방향은 결국 하나로 요약된다. 향후 보안 운영의 경쟁력은 단순 탐지 기술이 아니라, 위협 인텔리전스와 운영 플랫폼을 얼마나 긴밀하게 연결해 실질적인 판단 체계로 전환할 수 있는가에 달려 있다는 점이다.

그 외 주목할 벤더들: 운영 철학과 플랫폼 전략의 다변화

RSAC 2026에서는 대형 플랫폼 벤더 외에도, 각기 다른 방식으로 보안 운영의 미래를 제시하는 기업들이 눈에 띄었다. 공통점은 분명했다. 더 이상 단순한 탐지 기능이나 개별 솔루션만으로는 차별화가 어렵고, 결국은 운영 구조와 서비스 모델을 어떻게 설명하느냐가 핵심 경쟁 요소가 되고 있다는 점이다.

Expel은 자사의 접근 방식을 "human-powered, AI-accelerated approach to security operations"로 표현했다. 이 문구는 AI를 전면에 내세우면서도, 궁극적으로는 사람 중심 운영 철학을 유지하겠다는 메시지에 가깝다. 이는 보안 운영 시장에서 AI가 분석가를 완전히 대체하기보다는, 운영 효율과 대응 속도를 높이는 방향으로 활용되고 있음을 보여준다.

eSentire는 Atlas 기반 Security Operations Platform을 내세우며, AI를 활용하되 expert validation을 강조하는 방향을 취하고 있다. 이는 순수 MDR 사업자 역시 더 이상 서비스 자체만을 설명하지 않고, 운영 플랫폼을 브랜드화해 시장에 제시하고 있음을 의미한다. 다시 말해, 전문 서비스 기업들도 이제는 "사람이 잘한다"는 설명만으로는 충분하지 않으며, 어떤 운영 체계 위에서 그 서비스를 수행하는가를 함께 증명해야 하는 단계에 들어선 것이다.

Rapid7은 최근 메시지를 Preemptive Security Operations, Preemptive MDR 방향으로 확장하고 있다. 이는 사고 발생 이후 대응에 머무르지 않고, 노출 관리와 사전 준비까지 포함하는 구조를 강조하는 접근이다. 이러한 흐름은 MDR가 탐지 이후 대응 서비스에서 벗어나, 사전 예방과 노출 관리까지 포함하는 더 넓은 운영 모델로 확장되고 있음을 보여준다.

Securonix는 "Breach Ready. Board Ready. AI-Powered."라는 문구를 통해 자신을 소개하며, 전통적인 SIEM 계열 사업자 역시 탐지 도구를 넘어 운영 준비도가 높은 플랫폼으로 포지셔닝을 바꾸고 있음을 보여줬다. 이는 SIEM 시장조차 더 이상 로그 수집과 분석에 머무르지 않고, 운영-ready 구조와 AI 기반 활용성을 강조하는 방향으로 이동하고 있음을 의미한다.

이들 벤더의 접근은 서로 다르지만, 공통된 메시지는 분명하다. 향후 보안 운영 시장의 핵심은 개별 제품의 성능 경쟁이 아니라, AI, 플랫폼, 서비스, 운영 철학을 어떤 방식으로 결합해 실제 고객 환경에 적용 가능한 구조로 만드는가에 있다.

RSAC 2026이 보여준 3가지 구조적 변화

전체적으로 보면, 이번 RSAC에서 확인된 변화는 세 가지로 정리할 수 있다.

첫째, 보안 운영은 점점 더 개방형 구조(Open Architecture)를 중심으로 재편되고 있다.

둘째, AI는 분석가를 대체하기보다는, 분석과 대응 속도를 높이는 방향으로 활용되고 있다.

셋째, MDR는 단일 기능이나 서비스가 아니라, 플랫폼과 운영 체계를 기반으로 설명되는 모델로 진화하고 있다.

4. RSAC 이후의 새로운 변수: Mythos AI와 AI 보안 위협 논의

RSAC 2026은 보안 운영의 방향성을 제시한 행사였지만, 그 직후 등장한 Mythos AI 관련 이슈는 그 방향에 대한 해석을 다시 한 번 복잡하게 만들었다. 컨퍼런스가 제시한 것은 구조적 변화였고, Mythos는 그 변화가 실제 시장에서 어떻게 인식되고 받아들여지는지를 보여주는 사례에 가깝다. 현재 시장에서 Mythos는 "차세대 공격형 AI(Offensive AI)"로 빠르게 확산되며 강한 인식을 형성하고 있다. 일부에서는 이를 보안 패러다임을 근본적으로 뒤흔드는 기술로 해석하기도 한다. 그러나 현재까지 확인된 사실을 기준으로 보면, 이 이슈는 실제 공격 사례보다는 제한된 정보와 그 해석 과정에서 비롯된 불확실성이 크게 작용하고 있다.

발표 자료에 따르면 Mythos는 일반 공개된 상용 모델이 아니라, 제한된 환경에서 운영되는 Preview 형태의 시스템이다. 또한 현재까지 해당 모델을 활용한 실제 공격 사례나 침해 사고가 확인된 바는 없다. 그럼에도 불구하고 시장에서는 이 기술이 이미 실질적인 공격 도구로 활용되고 있는 것처럼 인식되고 있으며, 이러한 인식은 개발사의 메시지와 미디어 확산을 통해 빠르게 강화되고 있다. 이 지점에서 중요한 것은 단순히 '위협이 존재하는가'가 아니라, 그 위협이 어떤 방식으로 정의되고 확산되는가이다. Mythos 사례는 AI 보안 영역에서 기술적 사실보다 '인지된 리스크(perceived risk)'가 먼저 형성되고 확대되는 구조를 단적으로 보여준다.

일부 내부 문서 노출과 제한적 프리뷰 공개를 통해 모델의 존재가 알려지면서, '자율적으로 취약점을 탐지하고 공격 코드를 생성할 수 있다'는 메시지가 빠르게 확산됐다. 그러나 실제로는 전체 기능이 공개된 것이 아니라 제한된 범위의 기능만 제공되는 초기 단계였으며, 접근 역시 통제된 환경에서만 가능했다. 그럼에도 불구하고 시장에서는 이 모델이 이미 현실적인 공격 수단으로 활용 가능한 것처럼 인식되기 시작했고, 이는 검증된 사실보다 가능성과 시나리오가 먼저 확산되는 전형적인 패턴을 보여준다. 실제로도 "공격이 이미 시작된 것인가"라는 질문이 반복적으로 제기되었지만, 명확한 검증보다 공포가 앞서는 양상이 나타났다.

PROJECT GLASSWING

이러한 상황 속에서 Anthropic은 Project Glasswing을 출범시킨다. Glasswing은 특정 AI 모델이나 공격 기술이 아니라, AI 시스템의 취약점을 사전에 탐지하고 보완하기 위한 협력 기반의 검증 이니셔티브로, Mythos를 둘러싼 논란과 시장의 불확실성에 대응하기 위한 구조적 시도로 해석할 수 있다. 즉, Mythos가 '위협 인식'을 촉발한 사건이라면, Glasswing은 그로 인해 증폭된 불확실성을 통제하고 신뢰를 회복하기 위한 대응 프레임에 가깝다.

다만 Glasswing은 폐쇄형 협력 구조로 운영되며, 내부에서 어떤 취약점이 발견되고 어떻게 검증되는지에 대한 정보는 제한적으로만 공개된다. 이로 인해 방어를 위한 구조임에도 불구하고, 외부에서는 오히려 불확실성을 확대시키는 요인으로 작용하는 역설적인 상황이 발생한다.

결국 Mythos와 Glasswing은 별개의 이벤트가 아니라 '위협 인식 → 시장 반응 → 대응 구조'로 이어지는 하나의 흐름 안에서 이해할 필요가 있다. 이는 AI 보안 영역에서 기술 자체보다 정보의 공개 방식과 해석 구조가 시장에 더 큰 영향을 미칠 수 있음을 보여준다. 그러나 이러한 현상을 단순히 과장된 공포로만 해석하는 것은 적절하지 않다. 이 이슈가 보여주는 보다 본질적인 변화는 공격과 방어의 속도가 동시에 가속되고 있다는 점이다.

이번 발표에서도 반복적으로 강조된 부분은, AI가 공격 방식을 근본적으로 바꾸고 있다기보다 기존 공격을 실행하는 속도를 비약적으로 끌어올리고 있다는 점이다. 다시 말해 공격의 본질(TTPs)은 크게 달라지지 않았지만, 탐지와 대응이 허용되는 시간 창이 급격히 줄어들고 있다. 이는 보안 운영의 문제를 기술의 문제가 아니라 '시간과 판단의 문제'로 전환시키고 있다. 이와 동시에 방어 측면에서도 유사한 변화가 나타나고 있다. GPT 기반 보안 모델과 같은 Defensive AI는 탐지, 이벤트 정리, 초기 분석 속도를 크게 단축시키며 보안 운영의 효율성을 높이고 있다. 결국 현재의 보안 환경은 AI 기반 공격과 AI 기반 방어가 동시에 진화하는 구조로 재편되고 있으며, 여기에 인간 분석가의 판단이 결합되는 형태로 발전하고 있다.

이러한 변화는 RSAC 2026에서 확인된 Agentic SOC 흐름과도 맞닿아 있다. 초기 분석과 triage는 AI가 담당하고, 최종 판단과 대응은 인간이 책임지는 구조가 점점 더 명확해지고 있다. Mythos 논의 역시 이러한 방향성을 부정하기보다, 오히려 그 필요성을 강화하는 사례로 작용하고 있다.

결국 이 이슈에서 도출할 수 있는 핵심은 다음과 같다.

첫째, AI 기반 공격은 분명히 현실화되고 있지만, 현재 시장에서 인식되는 수준과 실제 적용 수준 사이에는 여전히 간극이 존재한다.
둘째, 보안의 핵심 변수는 공격 방식 자체가 아니라 공격과 대응의 속도다.
셋째, 이러한 환경에서는 자동화만으로 충분하지 않으며, 최종 판단과 대응을 수행하는 운영 체계가 더욱 중요해진다.

Mythos는 하나의 기술이나 사건이 아니라, 보안 운영이 어떤 방향으로 이동하고 있는지를 보여주는 신호에 가깝다. 그리고 그 방향은 명확하다. 기술이 고도화될수록 보안의 경쟁력은 더 이상 탐지 기능 자체에 있지 않으며, 얼마나 빠르고 정확하게 판단하고 대응할 수 있는가에 의해 결정된다.

5. AI SOC 플랫폼의 부상: 새로운 운영 레이어의 등장

RSAC 2026에서 주목할 만한 또 하나의 변화는, 기존 대형 벤더 외에도 AI 기반 SOC 플랫폼을 중심으로 한 신생 플레이어들이 가시적으로 등장하기 시작했다는 점이다. Early Stage Expo를 포함한 전시 전반에서는 AI 에이전트, AI 자율성, SOC 자동화, 대응 자동화와 관련된 다양한 기업들이 눈에 띄었으며, 관련 세션에서도 AI agents, AI autonomy, reasoning-based security와 같은 주제가 다수 다뤄졌다.

이러한 흐름은 보안 운영 시장이 기존의 제품·플랫폼·서비스 구조를 넘어, 새로운 운영 레이어를 형성하고 있음을 시사한다. 특히 최근에는 이를 크게 두 가지 방향으로 구분해 볼 수 있다.

하나는 AI SOC Platform으로, 기존 SOC에서 레벨 1 분석가가 수행하던 triage, 정리, 1차 조사 업무를 agentic AI를 통해 자동화하거나 압축하는 구조다.

다른 하나는 AI MDR로, 플랫폼을 넘어 서비스, 온보딩, 과금 구조, 운영 전달까지 포함한 형태로 확장된 모델이다.

이 두 흐름은 공통적으로 보안 운영의 초기 단계, 즉 이벤트 정리와 1차 분석 영역을 빠르게 자동화하는 데 초점을 맞추고 있다. 그러나 동시에, 이러한 자동화가 보안 운영 전반을 완전히 대체하는 구조로 이어지고 있는 것은 아니다.

오히려 중요한 시사점은 그 반대에 가깝다. AI 기반 플랫폼이 발전할수록, 자동화된 결과를 해석하고 실제 대응으로 연결하는 과정에서 숙련된 운영 조직의 역할이 더욱 중요해지고 있다는 점이다. 특히 다양한 환경과 복잡한 공격 흐름을 고려할 때, 최종 판단과 실행은 여전히 사람의 책임 영역으로 남아 있다.

이는 향후 보안 운영이 '툴 중심'이 아니라, 플랫폼과 운영 역량의 결합 구조로 재편될 가능성이 높다는 점을 보여준다. 또한 AI SOC 플랫폼은 기존 서비스를 대체하기보다는, 오히려 고도화된 운영을 가능하게 하는 기반으로 작동할 가능성이 크다.

운영 중심 MDR의 중요성: 기술을 넘어 '판단과 책임'으로

RSAC 2026은 AI 중심의 기술 변화가 빠르게 진행되고 있음을 보여주는 동시에, 보안 운영의 본질이 여전히 '판단과 책임'에 있다는 점을 다시 한 번 드러냈다.

표면적으로는 AI, 자동화, 플랫폼이 전면에 등장하고 있지만, 실제 고객 환경에서는 여전히 탐지 이후 무엇을 결정하고 어떻게 대응할 것인가가 핵심 과제로 남아 있다. 이는 보안 운영이 기술의 문제가 아니라, 의사결정 구조와 운영 체계의 문제에 가깝다는 점을 보여준다.

이러한 흐름 속에서 MDR 역시 단순 탐지 서비스에서 벗어나, 보다 확장된 운영 모델로 진화하고 있다. 특정 벤더 기술에 종속된 형태보다는, 다양한 보안 솔루션과 환경을 유연하게 통합하고 운영할 수 있는 구조가 점점 더 중요해지고 있다.

또한 MDR의 역할은 탐지 이후 대응에 머무르지 않고, 위협 노출을 사전에 식별하고 관리하는 영역까지 확장되고 있다. 이는 공격 발생 이후 대응뿐 아니라, 사전 예방과 노출 관리까지 포함하는 보다 입체적인 보안 운영 모델로의 전환을 의미한다.

결국 RSAC 2026이 보여준 가장 중요한 메시지는 분명하다. 보안의 경쟁력은 더 많은 기능이나 더 강력한 탐지 기술에 있는 것이 아니라, 그 기술을 어떻게 연결하고, 해석하고, 실제 대응으로 이어지게 하는가에 있다.

6. RSAC 2026이 보여준 기준에서 바라본 MDR의 경쟁력

RSAC 2026을 통해 확인된 가장 중요한 변화 중 하나는, MDR의 경쟁 기준이 명확해지고 있다는 점이다. 이제 시장은 단순히 어떤 기술을 보유하고 있는가보다, 그 기술을 어떻게 운영하고, 어떻게 판단으로 연결하며, 어디까지 책임질 수 있는가를 중심으로 평가하기 시작했다.

이러한 기준에서 보면, 최근 MDR 시장에서 경쟁력으로 평가되는 요소는 몇 가지 공통된 특징으로 정리할 수 있다.

첫째, 단일 제품 중심이 아닌 다층 구조 기반의 운영 모델이다.

EDR, NDR, XDR를 넘어 ASM, DRP, 취약점 점검 등 다양한 영역을 통합적으로 연결하고, 이를 개별 이벤트가 아닌 공격 흐름 관점에서 해석할 수 있는 구조가 중요해지고 있다. 이는 RSAC 2026에서 다수의 플랫폼 사업자들이 강조한 방향과도 일치한다.

둘째, 탐지 이후의 판단과 대응까지 포함하는 운영 범위다.

단순 알림이나 분석 리포트 제공을 넘어, 실제로 어떤 조치를 취할 것인지에 대한 판단과 실행까지 연결되는 구조가 MDR의 핵심 요소로 자리잡고 있다. 이는 고객이 기대하는 MDR의 역할이 점점 더 '모니터링'에서 '의사결정 지원 및 실행'으로 이동하고 있음을 보여준다.

셋째, AI를 활용하되, 운영 통제와 판단 구조를 유지하는 접근 방식이다.

RSAC 2026에서 확인된 바와 같이, AI는 초기 분석과 조사 과정을 가속하는 데 중요한 역할을 하고 있지만, 최종 판단과 책임까지 완전히 대체하는 방향으로는 아직 발전하지 않았다. 따라서 AI를 어떻게 운영에 통합하고, 사람과의 역할을 어떻게 설계하는지가 중요한 차별화 요소로 작용하고 있다.

넷째, IT를 넘어 다양한 환경까지 확장 가능한 운영 모델이다.

특히 제조, 에너지, 인프라 환경을 포함한 OT 영역까지 고려한 보안 운영 구조는 점점 더 중요한 요소로 부각되고 있다. 이는 단순한 기술 확장이 아니라, 환경별 리스크와 운영 특성을 이해할 수 있는 역량을 요구한다.

다섯째, 글로벌 환경과 다양한 기술 스택을 포괄할 수 있는 유연성이다.

단일 벤더 중심 구조에서 벗어나, 다양한 보안 솔루션과 환경을 유연하게 통합하고 운영할 수 있는 구조는 글로벌 시장에서 MDR 서비스가 확장되기 위한 필수 조건으로 자리잡고 있다.

이러한 기준은 특정 기업에 국한된 것이 아니라, RSAC 2026 전반에서 공통적으로 확인된 시장의 방향성이다. 그리고 이 기준에 부합하는 MDR는 단순한 서비스 제공을 넘어, 실제 보안 운영을 책임지는 구조로 진화하고 있다.

7. 결론: 보안 운영의 본질로 돌아가다

RSAC 2026은 AI와 플랫폼 중심의 기술 변화가 빠르게 진행되고 있음을 보여준 행사였다. 동시에, 보안 운영의 본질은 여전히 '판단과 책임'에 있다는 점을 다시 한 번 확인시켰다.

시장에는 다양한 AI 기반 솔루션과 자동화 기술이 등장하고 있지만, 실제 고객 환경에서는 여전히 누가 더 빠르게 상황을 이해하고, 더 정확한 결정을 내리며, 그 결정에 책임을 질 수 있는가가 핵심 기준으로 작용하고 있다.

이러한 흐름은 MDR의 역할이 단순한 탐지 서비스에서 벗어나, 조직의 보안 운영을 실질적으로 담당하는 구조로 진화하고 있음을 의미한다. 특히 기술과 플랫폼이 고도화될수록, 이를 실제 환경에 맞게 연결하고 운영할 수 있는 역량의 중요성은 더욱 커지고 있다.

결국 RSAC 2026이 보여준 메시지는 분명하다. 보안의 경쟁력은 더 많은 기능이나 더 강력한 기술에 있는 것이 아니라, 그 기술을 어떻게 운영하고, 어떻게 판단으로 연결하며, 어떻게 책임지는가에 있다.

이러한 관점에서 볼 때, 앞으로의 MDR 시장은 단순한 기능 경쟁이 아니라, 운영의 깊이와 의사결정 구조를 중심으로 재편되는 국면에 들어섰다고 볼 수 있다.

그리고 이 변화는 하나의 방향으로 수렴하고 있다.

기술을 넘어 운영을 설계하고, 판단을 내리며, 그 결과에 책임지는 역량을 갖춘 조직만이, 앞으로의 보안 운영을 실질적으로 이끌어가게 될 것이다.

www.pagonetworks.com

www.pagonetworks.com