pago



2026 PAGO Security Summit Insight Report

Defining the Future of Security Operations

By PAGO Networks in collaboration with reporter Jang Doohwan from SharedIT

www.pagonetworks.com

목차

01 조찬 세션과 기자 간담회 5

PAGO Security Summit 2026 CISO 대상 조찬 세션

01 공격자만 강해진 게 아니다: 오펜하이머 모멘트로 바라보는 AI의 양면성 6

02 완전 자율 SOC는 아직 어렵기에 증강이 필요하다 9

03 숫자로 평가하는 AI 성과: KPI 다섯 개와 하이브리드 조직도 11

PAGO Security Summit 2026 기자 간담회

01 하나의 플랫폼, 세 개의 브랜드: PAGO DeepACT 13

02 MDR이라는 용어를 버리고 한 단계 더 도약하다 16

02 오후 세미나: 키노트와 파고 세션 18

Keynote 세션

LG U+ 함께 만들어가는 Security Operations의 미래 19

Stellar Cyber Open, Intelligent & Unified Security Operations for the AI Era 21

SentinelOne Autonomous AI Meets Human Expertise: The Future of Modern Security Operations 24

파고네트웍스 세션

Hybrid SecOps in Action · Two Teams, One Security Operation **권영목 대표** 26

Proactive SecOps · Reducing Risk Before the Attack with CTEM & Exposure Validation **이시우 주임** 28

AI-Powered SecOps · Accelerating Alert Triage with AI Investigator **김재근 주임** 30

Advanced SecOps · Human-led Threat Hunting & Detection Engineering in the AI Era **권표 이사** 32

03 권영목 대표 단독 인터뷰 36

소수 의견을 지우지 않는다는 것의 의미 37

AI 보안에서 봐야 할 것과 보지 말아야 할 것 39

똑똑해 보이는 건 AI지만, 판단하는 몫은 결국 사람에게 주어진다 41

결론: AI 시대, 여전히 시스템이 아니라 사람이 중요한 이유 43

pago

SentinelOne Wayfinder 위협 헌팅과 함께

HYBRID MDR

Two MDR Teams. One Security Operation.

AI의 속도, 사람의 판단.

TEAM 1
SentinelOne Wayfinder MDR

AI와 Threat Hunting 전문가 협업 / 새로운 위협의 선제적 탐지 / Google Threat Intelligence 기반

+

TEAM 2
PAGO MDR Operations

검증된 24×7 MDR 운영 노하우 / 탐지 · 조사 · 대응 / 전문 보안 분석가 운영

ONE OPERATION: 더 빠른 탐지 · 더 깊이 있는 조사 · 더 효과적인 대응

운영 범위

24/7/365 위협 모니터링.
엔드포인트, 클라우드 워크로드, ID 전반을 지속적으로 탐지합니다. 확인된 위협이 조치를 요구할 때만 고객 팀에 연락드립니다.

Wayfinder 위협 헌팅.
Google Threat Intelligence 기반 자동화 헌팅이 분석가가 찾아 나서기 전에 위협을 드러냅니다. 사후 대응이 아닌 선제 대응입니다.

대기 없는 위협 차단.
EDR이 고객 승인을 기다리지 않고 즉시 디바이스를 격리하고, 악성 프로세스를 종료하며, 변경 사항을 롤백합니다.

Why PAGO

3.3분
Wayfinder 평균 탐지 소요 시간(MTTD)

2년 연속
SentinelOne APJ MSSP Partner of the Year

DeepACT를 통해 제공됩니다.
PAGO의 AI 기반 운영 플랫폼으로, 한국과 APJ 전역의 24×7 분석가가 운영합니다.

추가 비용 없이 제공.
PAGO를 통해 SentinelOne Singularity Complete 이상을 사용하는 고객 대상.
제품 변경 없이, 기존 가격 정책 그대로.

시작은 HYBRID MDR로. 확장은 필요에 맞게.

NDR | CTEM | AI-SIEM | SOAR

무료 상담 신청하기
위협 준비 상태 평가 포함

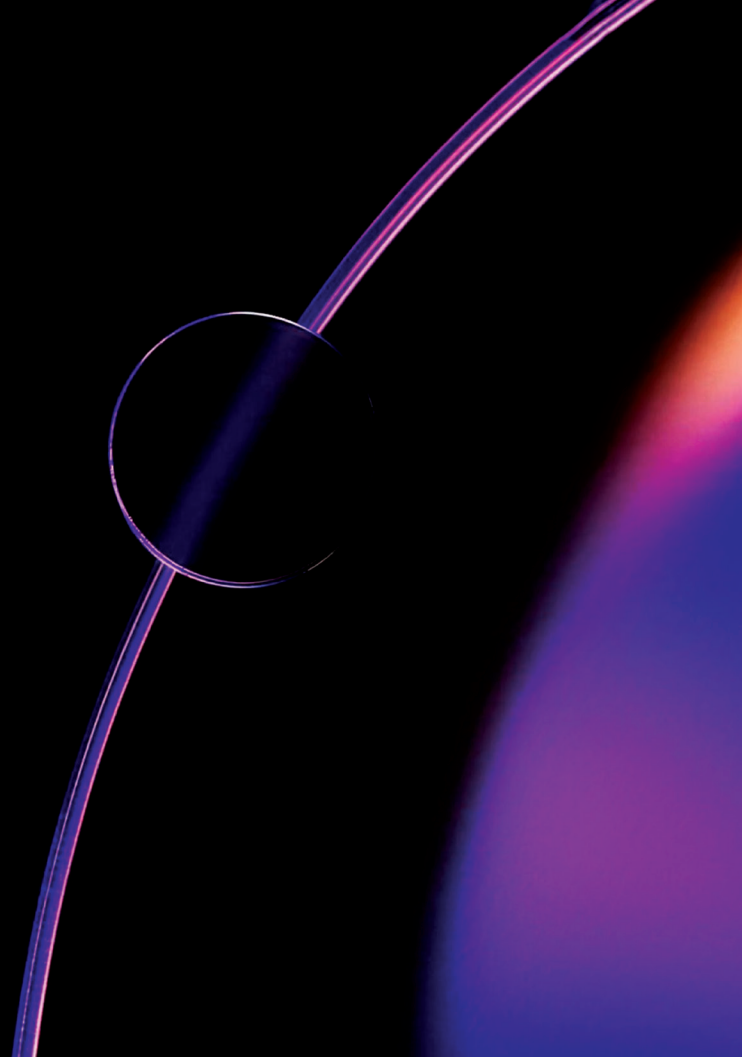
PAGO Networks Inc Korea
PAGO Networks Pte Ltd Singapore
Hybrid MDR for Korea and APJ

PART

01

조찬 세션과 기자 간담회

9월 1일, PAGO SECURITY SUMMIT 2026



CISO 조찬 세션 · 기자 간담회

“ 2026년 상반기, 무엇이 그토록 우리를 두려워하게 했습니까?

지난 9월 1일 파고네트웍스가 CISO들을 초청해 진행한 PAGO Security Summit 2026 조찬 세션의 시작은 이 질문이었습니다. 발표자로 나선 권영목 대표는 AI로 무장한 공격자가 우리보다 먼저 취약점을 찾아낸다는 것, 그리고 그 속도를 방어 쪽에서 도무지 따라잡을 수 없다는 것을 답변으로 내놓았는데요.

이어서 권 대표는 이 현상을 공격의 속도(Speed of Attack)라고 부르며, 공격자는 이제 AI를 이용해 우리가 미처 발견하지 못한 설정 오류나 제로데이 취약점을 찾아내고, 발견과 거의 동시에 실제 공격이 가능한 형태로 만들어 낸다고 언급했습니다. 그리고 이 공격 속도를 방어하는 쪽이 따라가지 못하는 현상은 대응 격차(Response Gap)라고 했고요.

머신 기반 공격은 기하급수적으로 늘어나는데, 사람 중심 SOC의 대응력은 인력을 충원하는 만큼만 선형적으로 늘어납니다. 두 선은 어느 시점부터 벌어지기 시작하고, 그 뒤로는 좀처럼 좁혀지지 않습니다. 이 벌어진 틈, 즉 대응 타이밍의 상실을 사람을 더 뽑는 방식으로 메울 수 있을까요? 권 대표의 답은 명확히 아니오였습니다. 구조적인 결함이라는 겁니다.

이번 칼럼의 1부는 지난 9월 1일에 있었던 PAGO Security Summit 2026 조찬 모임과 기자 간담회 내용을 정리한 것입니다. 2부에서는 PAGO Security Summit 2026의 주요 세션 내용을, 3부에서는 권영목 대표와의 단독 인터뷰 내용을 소개하겠습니다.

그럼, 제가 서두에 언급한 질문에 대한 해결책을 파고네트웍스는 어떻게 제시하고 있는지, CISO 대상 조찬 세션과 기자 간담회의 주요 내용에서 확인해 봅시다.

PAGO Security Summit 2026
CISO 대상 조찬 세션

01 공격자만 강해진 게 아니다: 오펜하이머 모멘트로 바라보는 AI의 양면성

■ 원자폭탄에서 프레임을 빌려오다

조찬 세션 내용으로 다시 돌아가 봅시다. 권 대표는 이 위기 앞에서 원자폭탄 개발의 역사를 꺼냈습니다. 오펜하이머가 원자폭탄을 연구하기 시작한 원동력은 방어적 목적과 과학적 사명감이었죠. 하지만 결과는 히로시마와 나가사키라는, 의도치 않은 파괴 행위였다는 것을 우리는 잘 알고 있습니다. 지금 실리콘밸리에서 벌어지는 일도 다르지 않다는 게 그의 진단입니다. 강력한 기술의 등장이 인류사적 위기이자 전환점을 동시에 몰고 오는, 소위 오펜하이머 모멘트에 우리가 도달했다는 겁니다.

AI는 현실이고 오펜하이머 모멘트, 파멸적 혁신이라는 양면성을 지니고 있습니다. 공격자가 AI로 무장해 불가능해 보였던 규모의 공격을 자동화하는 것도 이 양면성의 한쪽 면이라고 봐야합니다. 그럼 반대편 방어자 쪽은 어떨까요? 동일한 효과가 적용되고 있다는 것이 참 다행이긴 합니다. 그래서 권 대표는 이를 "AI로 무장한 공격 vs AI로 대응하는 방어"라는 대칭 구도로 정리합니다. 전자가 Speed of Attack이라면, 후자는 그가 이름 붙인 Security at the Speed of Attack입니다.



AI는 현실이고,
오펜하이머 모멘트이며,

인류의 역사를 뒤바꾸는
파멸적 혁신 양면성을
지니고 있다





AI는 공격자만 키우지 않습니다. 우리도 함께 키웁니다.
충분히 이길 수 있는 싸움이니, 두려워하지 않으셔도 됩니다!

Gartner
Security & Risk Management Summit

■ 위협을 키워놓고 두려워하지 말라는 이유는 해결책이 있기 때문

권 대표는 이 대칭을 뒷받침하는 근거로 Gartner Security & Risk Management Summit 2026에서 나온 발언을 인용했습니다. AI는 공격자의 역량만 키우는 게 아니라 방어자의 역량도 똑같이 키운다는, 그래서 이건 우리가 이길 수 있는 싸움이고 두려워할 필요가 없다는 내용입니다.

앞서 오펜하이머 모먼트라는 비유를 언급했는데 곧바로 "This is a fight we can win."이라고, 그래도 우리가 이길 수 있다는 결론으로 넘어가는 구성 자체가 청중인 CISO들을 의도적으로 겨냥한 것 아닐까 싶습니다. 위협을 실제보다 축소해서 안심시키려는 게 아니라, 위협의 크기를 인류사적 사건에 비견될 만큼 키워놓고도 "두려워하지 말라"고 말하려면, 그 뒤에 반드시 구체적인 해법이 따라와야 신뢰가 생기지 않을까요?

그래서 권대표는 질문의 프레임을 바꿔야 한다고 강조합니다. Security at the Speed of Attack이라는 표현은 단순한 슬로건이 아니고, 보안 조직이 스스로에게 던져야 할 질문을 바꾸라는 겁니다. "얼마나 많이 탐지했는가"가 아니라 "공격자와 같은 속도로 판단하고 있는가"라고 말이죠. 이 발상의 전환이 왜 앞으로의 SOC 운영 방향성을 바꿔야 하는가에 대한 당위성을 제공해 줄겁니다.

"얼마나 많이 탐지했는가"가 아니라 "공격자와 같은 속도로 판단하고 있는가

02 완전 자율 SOC는 아직 어렵기에 증강이 필요하다

2025 Autonomous SOC 는 불가능하다

2026 Autonomous SOC 는 불가능하다
당분간은 ...
Augmented SOC with Agentic AI

Gartner

Security & Risk Management Summit

■ "당분간은 불가능하다"는 표현의 이면에 숨은 뜻

조찬 세션 후반부는 자연스럽게 "그럼 SOC는 어디로 가야 하는가"라는 질문에 대한 답을 찾는 여정으로 넘어갑니다. 권 대표가 인용한 가트너 Gartner Security & Risk Management Summit 2026의 담당자 발언에 따르면, 사람의 개입이 전혀 없는 완전 자율형 SOC, 즉 Autonomous SOC는 당분간 불가능하다는 게 Gartner의 입장인데요. 대신 2030년까지 현실적인 방향은 Agentic AI가 결합된 Augmented SOC, 줄여서 Augmented SOC with Agentic AI라는 겁니다.

용어가 좀 복잡한데, 간단히 말하면 AI로 강화된 SOC라고 봐도 됩니다. 하지만 단순히 SOC에 AI가 접목됐다고 하는건 아닙니다. Gartner의 발언을 통해 유추해 보면 완전 자율화로 가는 여정의 속도가 생각보다 빠르지 않다는 것으로 읽히지만, 동시에 그 방향 자체는 바뀌지 않았다는 신호이기도 합니다. 즉 "언젠가는 간다, 다만 아직은 아니다"라는 잠정적 결론이라는 건데, 이걸 곧이곧대로 "AI가 SOC를 완전히 대체할 일은 없다"로 결론내리는 것은 다소 성급한 판단입니다.

Gartner 견해: 2030년까지의 방향

당분간은 불가능

Autonomous SOC

사람의 개입이 전혀 없는 완전 자율형

→

2030년까지 현실적 방향

Augmented SOC with Agentic AI

보안 인력 대체가 아니라 증강과 자동화.
최종 판단과 책임은 사람에게 남음.

■ 왜 증강에 주목해야 하는가

그래서 권 대표는 이걸 "보안인력 대체가 아니라, 증강과 자동화 (Augmentation/Automation)"라는 문장으로 요약했습니다. 겉보기엔 무난해 보이지만, 실무자 입장에서 보면 이건 예산 배분과 채용 계획에 직결되는 이야기죠. AI에 맡길 영역과 사람이 남아야 할 영역의 경계를 어디에 그을 것인가라를 따져봐야 하기 때문입니다.

그래서, AI 기반 방어 전략에서도, 최종 판단과 책임은 운영조직에 남아 있다는 것이 핵심입니다. 탐지와 분석의 상당 부분은 AI로 넘어가더라도, "이 판단을 근거로 무엇을 할 것인가"를 결정하고 그 결과에 책임지는 주체는 여전히 사람이라는 겁니다. 즉, Gartner가 말하는 증강은 AI로 SOC의 운영 역량을 강화하는 것 뿐만 아니라, SOC의 운영 주체인 사람의 역량을 증강, 강화시켜야 한다는 것으로 이해해야 합니다.

■ AI를 기술이 아니라 팀원으로 바라봐야

많은 기업들이 AI 도입을 새로운 기술을 들여오는 것으로 여깁니다. 하지만 AI 에이전트로 인해 패러다임이 바뀌었죠. AI 도입은 단순한 신기술 도입이 아닌 새로운 팀원을 채용하는 것으로 여겨야 한다는 것이 권 대표의 주장입니다. 왜냐, AI는 너무나도 방대한 지식을 갖췄고, 업무 처리가 빠르며, 자동화가 가능한 엄청난 팀원거든요.

생각해 봅시다. 기업이 새로운 인력을 뽑으면 뭘 제공하나요? 어떤 일을 하게 되는지, 무엇은 하면 안되는지, 어떻게 평가할 것인지 등에 대한 지침을 제공합니다. AI도 똑같습니다. 명확한 직무 설명서, 철저한 가이드라인, 측정 가능한 성과지표, 그리고 명확한 해고 사유(Guardrails)까지, AI 도입이 사람 채용과 크게 다르지 않다는 겁니다.

AI 도입 패러다임 전환 in Cybersecurity

AI 도입은 단순한 기술선택이 아님 → **AI 도입은 새로운 팀원을 채용하는 과정**

- 방대한 지식 소유,
- 업무처리가 빠르고
- 자동화가 가능한 엄청난 팀원이 들어옴

- 명확한 직무 설명서
- 철저한 가이드라인
- 측정 가능한 성과지표
- 명확한 해고 사유(Guardrails)

> **AI 도입은 단순한 신기술 도입이 아닌 새로운 팀원을 채용하는 것으로 여겨야 한다**

실제로 많은 조직에서 AI 보안 도구 도입이 기술 검토에서 끝나고 운영까지 이어지지 못하는 것 역시 AI를 기술로써 취급하기 때문입니다. 신규 팀원에게 업무 범위도, 평가 기준도, 문제가 생겼을 때의 퇴출 기준도 정해주지 않고 자리에 앉히면 어떻게 되나요? 그 팀원은 아무런 성과를 낼 수 없을겁니다. 물론 일부러 그런 기간을 갖는 조직도 있긴 하지만(저는 그랬습니다만 매우 비효율적이라고 생각합니다.), 그런데 정작 AI 도구 역시 이렇게 일단 도입해서 "그래, AI가 얼마나 똑똑한지 한 번 볼까? 에이 뭐야, 생각보다 별론데? 내 업무엔 못쓰겠다."라며 그냥 방치하는 경우도 많죠.



그래서 Augmented SOC가 작동하려면 채용 프로세스에 준하는 관리 체계가 먼저 갖춰져야 합니다. 팀원이 구석에서 놀고 있으면 관리자 입장에선 속터지잖아요. AI도 마찬가지입니다. 방치되는 AI가 가져올 비효율성을 사전에 제거할 수 있는 체계 마련이 선행돼야 합니다.

03 숫자로 평가하는 AI 성과: KPI 다섯 개와 하이브리드 조직도

성공적인 AI 채용, 평가 기준

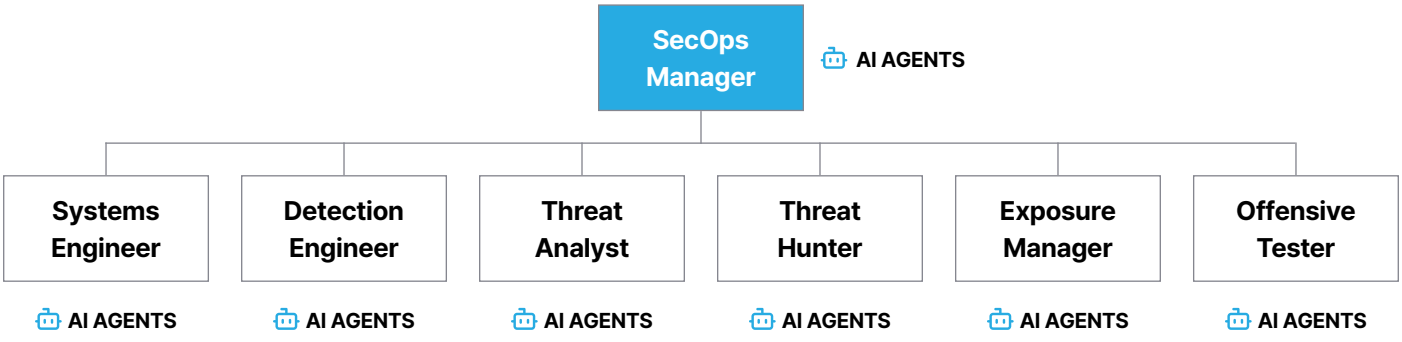
AI 채용 평가 영역	기존 대비	개선 효과 (예시)
효율성 (Efficiency)	분석 업무, 2시간 → 5분으로 단축
오류율 (Error Rate)	경고알림분류(Triage) 오류율, 20% → 5%로 감소
성과 향상 (Performance Improvement)	평균 탐지 시간(MTTD), 2시간 → 30분으로 단축
요구 기술 수준 (Skills Required)	주니어 분석가가 시니어 업무 수행 가능하도록 진화 가능 여부
프로그램 성장 (Program Growth)	테레메트리 조사 가능 비율, 기존 80% 수준 → 100% 수준

■ AI를 평가할 수 있는 기준을 마련해야

증강과 자동화라는 원칙이 제대로 작동하려면 AI의 성과를 측정할 수 있는 지표, KPI가 있어야 합니다. 이를 위해 권 대표는 성공적인 AI 채용의 평가 기준으로 다섯 가지를 제시했는데요. 분석 업무 처리 시간(2시간 → 5분), 경고 알림 분류 오류율(20% → 5%), 평균 탐지 시간(2시간 → 30분), 요구 기술 수준(주니어 분석가가 시니어 업무를 수행할 수 있도록 진화하는지), 그리고 텔레메트리 조사 가능 비율(기존 80% → 100%)입니다.

이 다섯 지표를 나란히 놓고 보면 눈에 띄는 공통점이 있습니다. 속도(2시간 → 5분, 2시간 → 30분)와 정확도(20% → 5%)만 다루는 게 아니라, 사람의 역량이 성장하고 있는가와 조사 가능한 범위 자체가 넓어지고 있는가 까지 함께 측정한다는겁니다. 앞서 언급한, AI를 사람으로 봐라봐야 한다는 것과 일맥상통하죠? 단순히 "AI를 도입했더니 업무가 빨라졌어요." 같은 식의 효율 지표에서 멈추지 않고, AI 도입이 조직의 역량 자체를 어떻게 바꿔놓는지까지 KPI에 포함시킨 겁니다.

Augmented SOC with Agentic AI - 하이브리드 조직도



■ 여섯 개의 직무, 여섯 개의 AI 에이전트

이 원칙이 조직도로 구체화된 형태가 Augmented SOC with Agentic AI 하이브리드 조직도입니다. SecOps Manager 아래 Systems Engineer, Detection Engineer, Threat Analyst, Threat Hunter, Exposure Manager, Offensive Tester까지 여섯 개 직무가 있고, 이 각각에 AI 에이전트가 짝지어져 있는데요. 단순히 직무마다 AI를 붙인 것이 아닌, 같은 직무 안에서도 역할이 명확히 구분되고 있습니다.

예를 들어 Detection Engineer는 탐지룰의 방향성과 프롬프트 설계를 맡고, 짝을 이루는 AI는 실제 탐지 코드 생성과 테스트, 업데이트 자동화를 맡습니다. Threat Hunter는 헌팅을 주도하고 Offensive 프로그램을 기획하는 반면, AI는 과거 기록 조사와 지표 수집을 바탕으로 헌팅 가설을 자동 생성합니다. Offensive Tester도 마찬가지입니다. 사람은 테스트의 조정과 범위 설정을 맡고, AI는 실제 모의침투 테스트 실행과 코드 리뷰 자동화를 맡습니다.

여섯 개 직무 전체에 걸쳐 이 패턴이 반복 적용됩니다. 사람은 전략과 관리(방향성 설정, 조정, 범위 설정, 우선순위 판단), AI는 실행과 전술(코드 생성, 자동 조사, 실행, 자동화)을 맡는 식입니다. 직무 이름이 무엇이든, 그 직무 안에는 항상 판단이 필요한 부분과 반복 가능한 실행 부분이 섞여 있고, 하이브리드 SOC는 그 경계를 직무 단위가 아니라 업무 단위로 그거야 한다는 뜻입니다.

따라서, "이 직무는 사람이, 저 직무는 AI가"가 아니라, 모든 직무 안에서 "이 일은 사람이, 저 일은 AI가"로 잘게 쪼개는 방식이 필요합니다. 앞서 나온 다섯 가지 KPI 중 요구 기술 수준(주니어가 시니어 업무를 할 수 있게 되는것)이 평가 기준으로 적용해도 되는 이유도 여기에 있습니다. 반복적인 전술 실행을 AI가 흡수해주면, 사람은 판단력을 요구하는 상위 업무에 더 빠르게, 더 많이 경험할 수 있기 때문입니다.

여기까지 CISO 대상 조찬 세션 내용을 정리했습니다. 뒤이어 이어진 기자간담회에서도 같은 내용이 소개되었는데요. 참석 대상이 CISO에서 IT 기자 분들로 바뀌었기 때문입니다. 하지만 세션 내용이 전부 같지는 않았기에, 조찬 세션에서 소개되지 않은 내용 위주로 기자 간담회 내용을 정리해 보겠습니다.

하이브리드 조직도: 여섯 개 직무, 여섯 개 AI 에이전트

SecOps Manager

↓

직무	사람	짝을 이루는 AI 에이전트	
Detection Engineer	탐지를 방향성과 프롬프트 설계 (uncertain)	탐지 코드 생성, 테스트, 업데이트 자동화	발표에서 소개
Threat Hunter	헌팅 주도, Offensive 프로그램 기획 (uncertain)	과거 기록과 지표로 헌팅 가설 포함 생성 (uncertain)	발표에서 소개
Offensive Tester	테스트 조정과 범위 설정	모의침투, 코드 리뷰 자동화	발표에서 소개
Systems Engineer	전략과 관리: 방향성 설정, 조정, 범위 설정, 우선순위 판단	실행과 전송: 코드 생성, 자동 조사, 실행, 자동화	동일한 패턴
Threat Analyst	전략과 관리: 방향성 설정, 조정, 범위 설정, 우선순위 판단	실행과 전송: 코드 생성, 자동 조사, 실행, 자동화	동일한 패턴
Exposure Manager	전략과 관리: 방향성 설정, 조정, 범위 설정, 우선순위 판단	실행과 전송: 코드 생성, 자동 조사, 실행, 자동화	동일한 패턴

직무가 아니라 업무 단위로 나눕니다. 모든 직무 안에서 판단은 사람이, 반복 가능한 실행은 AI가 맡습니다. 그래서 주니어가 시니어 업무에 더 빨리 다가갈 수 있습니다.

PAGO Security Summit 2026 기자 간담회

01 하나의 플랫폼, 세 개의 브랜드: PAGO DEEPACT

같은 날 오후, 기자간담회에서 권 대표는 조찬에서 설명한 하이브리드 SOC 구조를 실제 제품 라인업으로 공개했습니다. PAGO DeepACT 플랫폼 아래에 아래 세 개의 브랜드를 발표한 것인데요. DeepACT DEFENSE, DeepACT ATTACK, 그리고 DeepACT Detection-Engineering입니다. 앞서 조찬 세션에서 언급한 공격이 일어나기 전 단계 → 공격이 일어난 이후 → 그리고 이 둘을 연결하는 제품들인데요. 하나씩 좀 더 자세히 살펴봅시다.

PAGO DeepACT Platform									
3 DeepACT Detection-Engineering									
1 DeepACT DEFENSE						2 DeepACT ATTACK			
EPP	EDR	NDR	XDR	AI Sec.	ID Sec.	ASM	AEV	Red Teaming	DRP

Threat Validation	Threat Investigation	Threat Hunting	Threat Containment	Threat Disruption	Live Forensic	Preemptive Response	Threat Intelligence	Sharing TI	Incident Response	Compromise Assessment



출시 1. PAGO DeepACT DEFENSE

① DeepACT DEFENSE					
EPP	EDR	NDR	XDR	AI Sec.	ID Sec.

능동적 BLUE TEAM 서비스 제공

- 실제적 대응 : 위협 통보에 그치지 않고, 차단/격리 수행
- 위협 우선 순위화 : AI 기반 자동 처리 및 우선순위 처리

All-in-One 탐지 및 대응 역량 제공

- 다차원 보안 커버리지 : EDR, NDR, XDR 등
- 24×7 지속적 대응 / 보안운영 자동화

■ 통보에 그치지 않는다, DEEPACT DEFENSE

DeepACT DEFENSE는 기존의 EDR, NDR, XDR에 AI Sec, ID Sec까지 더한 통합형 블루팀 서비스입니다. 여기서 강조된 표현은 "능동적 블루팀"으로, 위협을 통보하는 데서 그치지 않고 실제로 차단하고 격리까지 수행한다는 뜻입니다. 언뜻 당연한 이야기처럼 들리지만, 그동안 다수의 MDR 서비스가 "이상 징후를 알려드립니다"까지만 하고 실제 조치는 고객사 몫으로 남겨뒀던 관행을 생각하면, 서비스 범위 자체를 한 단계 넓힌 것으로 이해가 됩니다. 이번 칼럼에서 다루진 않았지만, 조찬 세션 때 패널 토의 시간이 있었습니다. 그 때 언급된 내용 중에 "탐지는 보안팀, 조치는 다른 팀"이라는 조직 간 마찰 문제가 언급됐는데요. 이 DeepACT DEFENSE가 통보를 넘어 차단 및 격리까지 직접 수행하겠다는 건 그 마찰 지점 자체를 파고네트웍스가 대신 떠안겠다는 뜻으로 봐도 되지 않을까요?

출시 2. PAGO DeepACT ATTACK

② DeepACT ATTACK			
ASM	AEV	Red Teaming	DRP

통합 RED TEAM 서비스 제공

- AI 공격자 관점 빠른 분석, 사전 위험 식별
- ASM, AEV, AI Red-Teaming, Dark-web Intelligence

공격 가능성 검증 및 우선순위화

- 실제 인프라 대상, 공격지점 및 타격지점 검증
- 취약점 수정 우선순위 확실히 제공

■ 비 정기적 검증에서 365일 상시 검증 체계로, DEEPACT ATTACK

DeepACT ATTACK은 ASM(Attack Surface Management, 공격 표면 관리), AEV(Adversarial Exposure Validation, 공격 경로 검증), AI Red-Teaming, 다크웹 인텔리전스를 묶은 통합 레드팀 서비스입니다. 기존에 기업들이 1년에 한두 번, 많아야 네 번 정도 실시하던 모의해킹을 상시 검증 체계로 바꾸겠다는 게 핵심입니다.

DeepACT ATTACK이 중요한 이유는 앞서 조찬 세션의 핵심 메시지로 언급된, 공격의 속도와 맞물리기 때문인데요. 공격자가 AI를 등에 업고 몇 시간 단위로 취약점을 무기화하는 시대에, 방어 쪽에서 1년에 몇 번 점검하는 방식으로는 애초에 속도 경쟁이 되지 않기 때문입니다. 그래서 파고네트웍스는 DeepACT ATTACK을 상시 활성화된 형태로 제공해, 방어뿐 아니라 검증의 빈도 자체도 공격자의 속도에 맞출 수 있도록 지원하겠다는 계획입니다.



이미지 출처: IT조선, AI가 바꾸는 보안관제... 파고네트웍스 "MDR 넘어 'AI SOC'로 진화"

출시 3. PAGO DeepACT Detection-Engineering

3 DeepACT Detection-Engineering		
Google Threat Intelligence	**Frontier AI**	**PAGO Hunting Framework**

능동적 자동 위협헌팅 로직으로 전환

- DEFENSE 및 ATTACK 의 위협헌팅 정책 지속적 업데이트
- 위협헌팅 탐지 로직의 자산화 및 고객 보안솔루션 공유

글로벌 인텔리전스 내재화 및 Frontier AI 결합 엔진

- 글로벌 연동 (GTI 내재화 및 글로벌 TI 연동)
- Frontier AI 연동

■ DEFENSE와 ATTACK의 심장을 무상 제공, DETECTION-ENGINEERING

세 번째로 발표된 브랜드인 DeepACT Detection-Engineering은 Google Threat Intelligence, Sentinel Laps, CrowdStrike Falcon Intelligence에 AI 모델을 결합해, DEFENSE와 ATTACK 양쪽의 위협 헌팅 정책을 지속적으로 업데이트하는 내부 엔진입니다. 특징은 무상으로 제공한다는 것인데, DeepACT DEFENSE와 ATTACK이 고객에게 판매하는 제품이라면, Detection-Engineering은 그 두 제품이 계속 최신 상태를 유지하도록 뒤에서 돌아가는 인텔리전스 엔진입니다. 전면에 내세운 핵심 제품 2개가 상시 안정적으로 최상의 성능을 제공할 수 있도록 돕는 엔진을 무상으로 제공함으로써, 고객들에게 제품에 대한 신뢰를 뒷받침해줄 수 있는 근거를 제시한 것으로 저는 해석했습니다.



02 MDR이라는 용어를 버리고 한 단계 더 도약하다

이후에도 기자 간담회에서는 많은 내용과 질의응답이 오갔는데요. 그 중 핵심만 정리해 보겠습니다.

■ MDR이라는 용어를 더 이상 쓰지 않기로 한 이유

국내 보안관제 서비스 시장은 2024년 4364억원으로 전년 대비 16.2% 늘었고, 정보보안 관련 서비스 시장 전체는 같은 기간 1조 7491억원에서 2조136억원으로 커졌습니다. 글로벌 MDR 시장도 2026년 66억달러에서 2030년 153억달러로 연평균 23.5% 성장할 전망이고, AI가 결합된 AI SOC 시장은 2026년 181억달러에서 2031년 470억7000만달러로 더 빠르게 크고 있다고 합니다.

이런 흐름 속에서 권 대표는 MDR이라는 용어를 2026년 12월까지만 쓰고 내년부터 SOC-as-a-Service로 전환하겠다고 밝혔습니다. 시장이 커지는 와중에 파고네트웍스의 상징이라고도 할 수 있는 용어를 더 이상 쓰지 않겠다는 과감한 결정인데, 앞서 소개한 DeepACT 플랫폼의 3개 브랜드 출시 발표와 연관지어 생각해보면 이해가 가는데요.

MDR은 원래 탐지 후 대응을 위한 서비스죠. 하지만 파고네트웍스가 발표한 DeepACT DEFENSE는 고객이 취해야 할 조치를 대신 하고, DeepACT ATTACK은 공격 이전 단계 담당하며, DeepACT Detection-Engineering은 이 두 제품을 후방에서 지원합니다. 탐지되지 전부터 서비스가 시작되기 때문에 이제 더 이상 MDR이라는 용어에 파고네트웍스의 역량을 가둬 둘 필요가 없다는 것, 아닐까요?

이에 발맞춰 인력 운용도 크게 변화합니다. 초급 분석가 신규 채용을 중단하고 대응 전문 직무를 신설했으며, 특정 업무에서는 AI 70%, 사람 30%가 개입하는 구조로 운영한다고 밝혔습니다. 대량 알림을 1차로 걸러내던 초급 업무가 AI로 넘어가면서, 사람에게 남은 역할은 처음부터 판단이 필요한 업무에 집중하는 쪽으로 옮겨간 겁니다. 타겟 고객군도 보안운영인력 3~10명 규모, 연매출 500억 원~5조 원 사이의 중견기업, 특히 제조업으로 구체화됐습니다. 자체 SOC를 구축할 여력은 없지만 단순 탐지 및 통보 수준의 MDR로는 부족한 규모를 노리겠다는 계획으로 보입니다.



이미지 출처: 파고네트웍스, 센티넬원 위협분석 역량 결합한 '하이브리드 MDR' 출시 "AI 기술과 속도로 보안운영"

■ 관리 사각지대를 없애는 전략, FOLLOW THE SUN

파고네트웍스는 지난 6월 30일 캐나다 토론토에 지사를 설립했고, 아웃소싱 없이 자사 MDR센터 위협분석가를 주재원 방식으로 현지에 파견했습니다. 시차를 활용해 24시간 어느 시간대는 대응할 수 있게 만드는 전략으로, 파고네트웍스의 표현을 빌리면 Follow the Sun 전략입니다. 해가 지지 않는 방향으로 근무지를 배치해, 어느 시간대든 사람이 대응할 수 있는 체계를 만들겠다는 뜻입니다.

그럼 왜 이런 전략이 필요할까요? 어찌 보면 당연합니다. AI는 24시간 쉬지 않고 동작하죠. 그 AI를 활용해 전 세계에서 시차 구분없이 해커들은 공격합니다. 하지만 우리나라 시차를 기준으로 대응한다면, 새벽 시간대에는 대응이 어려울 거잖아요? 즉, 최종 판단과 책임은 사람이 몫이라는 원칙을 지키려면, 사람이 자리를 비우는 시간대 자체를 없애야 한다는 겁니다.

이에 대한 일환으로 파고네트웍스는 지난 7월 SentinelOne과 Wayfinder Threat Hunting 팀과 파트너쉽을 맺으며 Hybrid MDR 서비스를 발표 했습니다. 24시간 상시 감시 체계를 위해 서비스 지역과 시간대를 넓혀가는 과정 자체가, DeepACT ATTACK에서 강조한 상시 검증이라는 메시지를 위한 인력 운영 체계를 갖춰 나가는 과정이라고 봐도 되지 않을까요?

여기까지 조찬 세션과 기자 간담회의 주요 내용을 정리했습니다. 사실 이번 칼럼에서 정리한 내용은 메인 이벤트인 PAGO Security Summit 2026의 예고편 겸으로 봐야합니다. 보다 자세한 내용은 당일 오후에 진행된 8개의 세션에서 소개됐는데요. 그 내용 역시 준비했습니다. 조찬 세션과 기자 간담회와 겹치지 않는 내용 위주로 정리했으니 많은 관심 부탁드립니다. 끝!

PART

02

오후 세미나: 키노트와 파고 세션

PAGO SECURITY SUMMIT 2026 · 오후 1시 30분–5시 10분

8개의 세션 중 7개

지난 칼럼에서 PAGO Security Summit 2026의 조찬 세션과 기자 간담회 주요 내용을 정리했다면, 이번엔 이번 행사의 메인 이벤트인 오후 세미나에서 발표된 내용을 살펴볼 차례입니다. 오후 1시 30분부터 5시 10분까지, 총 8개의 세션이 이어졌는데, 오전 세션들에서 발표된 핵심 개념들이 좀 더 구체적으로 소개되는 자리였습니다.

그래서 이번 칼럼에서는 키노트 세션과 더불어 오전 세션에서 소개된 내용과 겹치지 않는 선에서 7개의 세션 내용을 정리해 보겠습니다. 파고네트웍스의 AI와 함께 변모하는, 보다 발전된 SOC의 구체적인 모습을 확인해 봅시다.

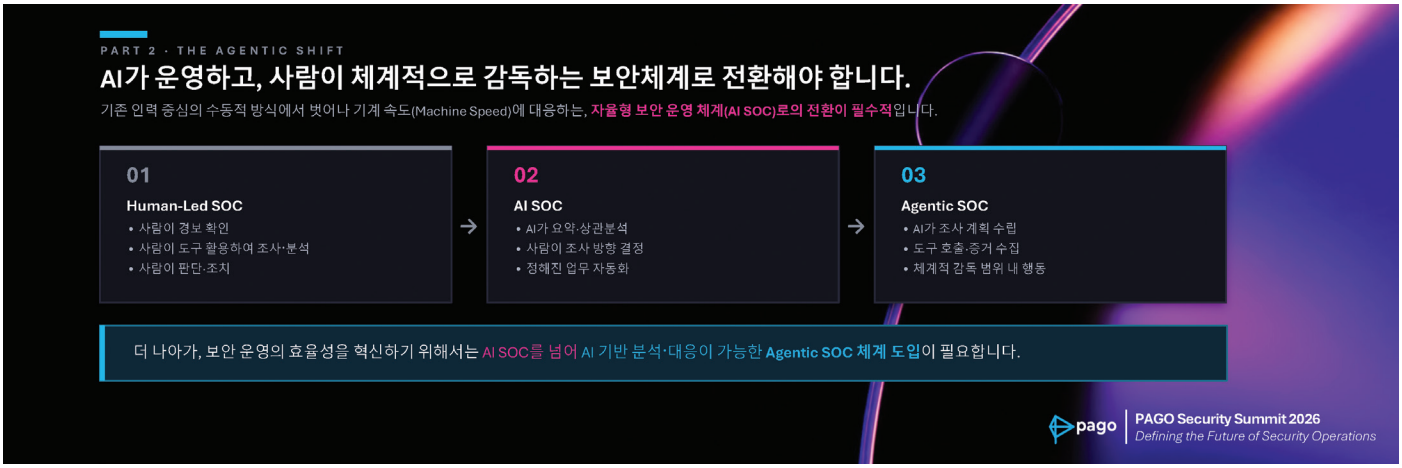


KEYNOTE 세션



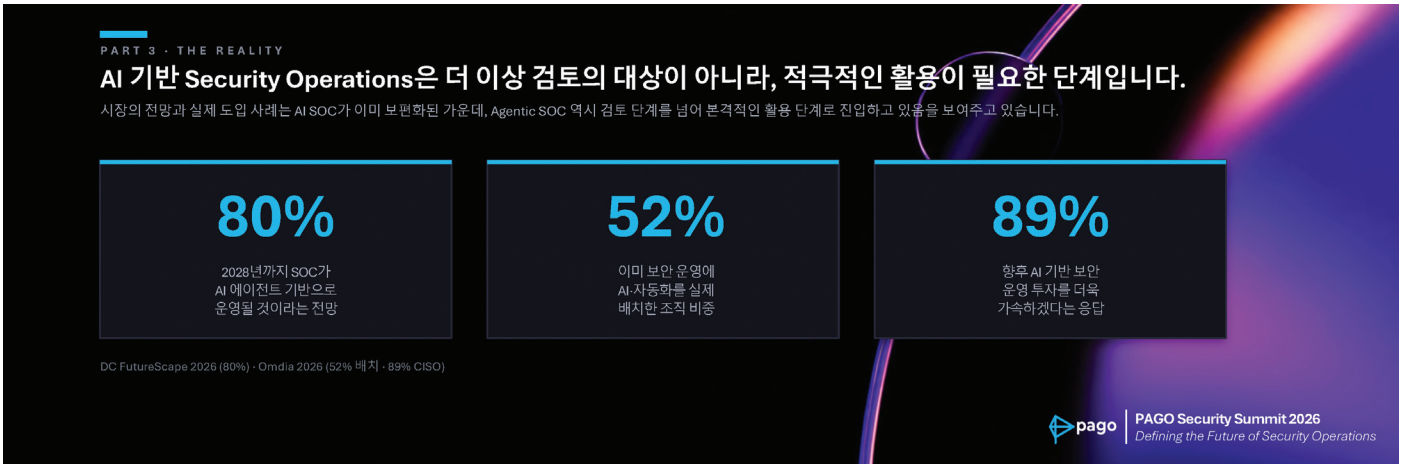
LG U+
함께 만들어가는 Security Operations의 미래

PAGO Security Summit 2026의 오후 세미나는 LG U+ 홍관희 전무의 발표로 시작됐습니다. 조찬 세션의 패널 토의 시간에 언급했던 대응 격차,Decision Gap을 보다 자세히 설명했는데요. 공격하는 쪽은 정찰, 취약점 분석, 경로 변경을 AI로 자동화시켜서 반복적으로 수행하고 있지만, 방어하는 쪽은 경보 → 티켓 → 분류 → 분석 → 승인 → 조치라는 순서를 밟아 나가고 있어 이 지리한 대기열에 갇혀 있다고 진단했습니다.

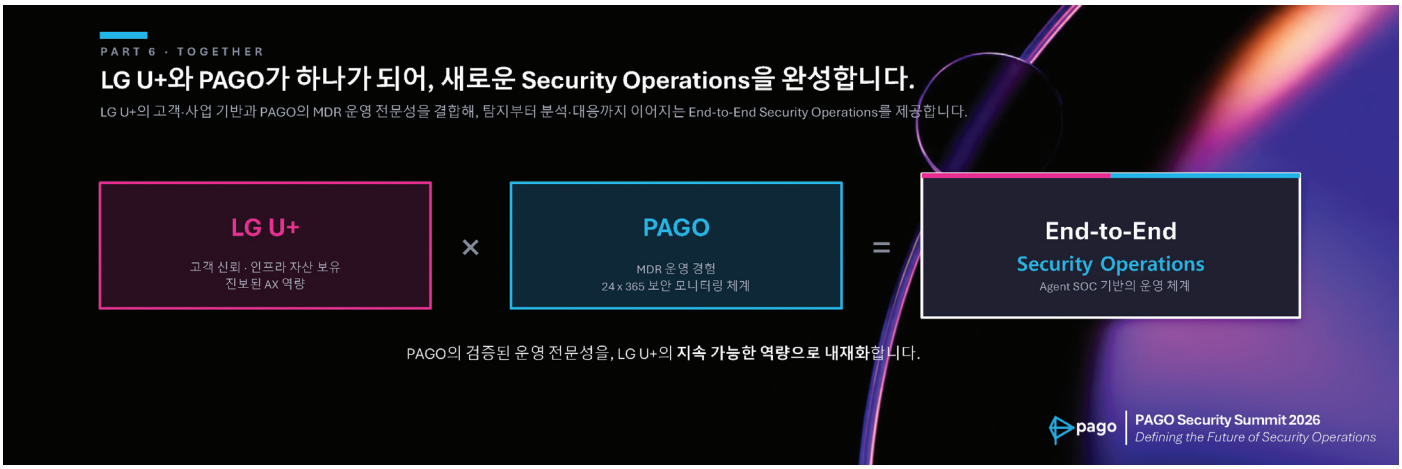


그리고 이어서 이 격차를 메우기 위한 방안으로 Human-Led SOC(사람이 직접 조사) → AI SOC(AI가 요약, 사람이 방향 결정) → Agentic SOC(AI가 계획 및 수집까지, 사람은 판단만) 3단계 프레임워크를 제안했습니다.

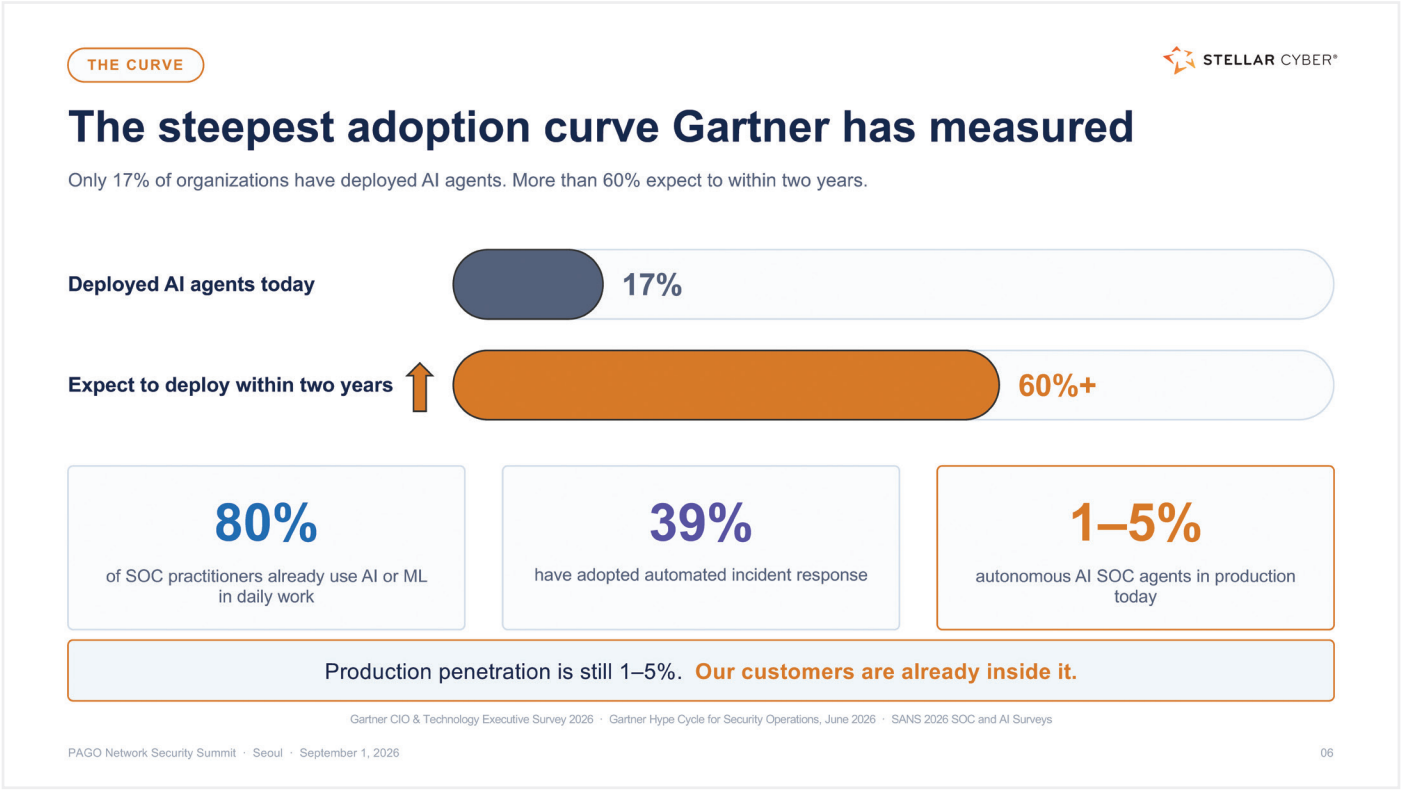
다만 완전 자동화의 위험(오탐 확산, 근거 불가 설명, 되돌릴 수 없는 조치, 불분명한 책임 소재)도 함께 짚었는데요. 그래서 Observe - Understand - Plan - Act - Learn 순환 구조에서 Act 직전에 사람의 승인해야 하는 관문(HITL Gate)을 추가했습니다. 실제로 IDC FutureScape 2026은 2028년까지 SOC의 80%가 AI 에이전트 기반으로 운영될 것으로, Omdia 2026은 이미 52%가 AI와 자동화를 실제 배치했고 89%가 투자를 가속하겠다고 한 점도 함께 언급했고요.



결국 이러한 3단계 프레임워크가 제대로 작동하기 위해 LG U+는 파고네트웍스와의 협업이 필요하다고 강조했습니다. LG U+의 인프라와 AX 역량에 파고네트웍스의 MDR 운영 전문성을 얹어 End to End 보안 운영을 제공하는 것이라고 보시면 되겠습니다.



Stellar Cyber
Open, Intelligent & Unified Security Operations for the AI Era



Aimei Wei CTO는 Gartner의 CIO 서베이 결과를 인용해 지금 시장이 어느 위치에 있는지를 숫자로 짚었습니다. AI 에이전트를 이미 실제 업무에 배치한 조직은 17%뿐이지만, 60% 이상의 조직이 앞으로 2년 안에 도입할 계획이라고 답했고, SOC 실무자의 80%는 이미 일상적으로 AI 도구를 쓰고 있다는 응답도 나왔습니다. 그런데 이 중 사람의 개입 없이 완전히 자율적으로 작동하는 AI SOC 에이전트가 실제 운영 환경에 들어간 비율은 고작 1~5%에 불과한 것이 인상적인데요. "AI를 써보고 있다"는 응답과 "AI에게 실제 판단을 맡기고 있다"는 응답 사이에 여전히 큰 간극이 있다는 뜻입니다.

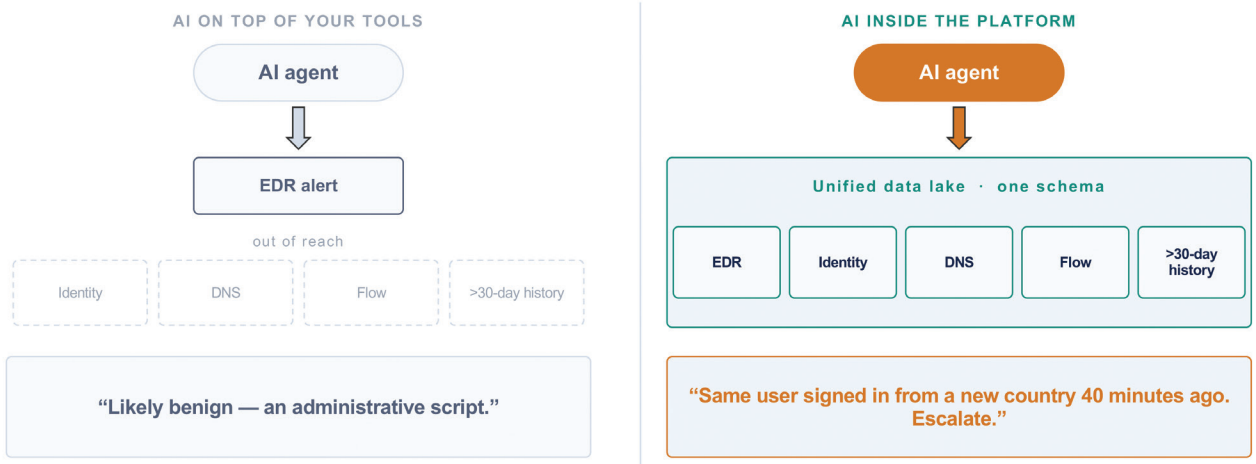


Wei CTO는 실제 경보 상황 하나를 예로 들었습니다. 새벽 3시 4분, 재무팀 워크스테이션에서 "의심스러운 파워셸 실행"이라는 경보가 발생했다고 가정했는데요. 이걸 판단하는 두 가지 AI 아키텍처를 나란히 보여줬는데, 결과가 정반대였습니다. 여러 개의 개별 보안 도구 위에 AI를 별도로 얹은 구조는 EDR이 갖고 있는 경보 정보만 보고 "관리 목적의 정상 스크립트로 보임, 양호"라고 판단했거든요.

Q1 · EVIDENCE

STELLAR CYBER®

Same alert. Two architectures.



The standalone answered the alert. The platform asked a better question.

PAGO Network Security Summit · Seoul · September 1, 2026 13

반면 여러 도구의 로그를 하나의 데이터 레이크에 미리 모아두고 그 안에 AI를 내장한 구조는 조금 달랐습니다. 같은 시각의 아이덴티티 로그와 DNS 기록까지 함께 조회해서 "같은 사용자 계정이 40분 전 평소와 다른 국가에서 로그인한 기록이 있음, 에스컬레이션 필요"라는 정반대 결론을 냈습니다. 두 구조 모두 AI가 판단한다는 점은 같지만, 차이는 그 AI가 얼마나 넓은 범위의 데이터를 한 번에 놓고 볼 수 있느냐에 달려있다는 겁니다.

이 차이가 어디서 나오는지에 대해 구체적인 숫자를 확인할 수 있었는데요. Stellar Cyber는 600개 이상의 보안, 인프라 제품들과 연동하고 있는데, 이걸 단순히 로그를 받아 쌓아두는 수준이 아니라 하나의 공통 스키마로 정규화해왔다고 강조했습니다. CrowdStrike, Okta, AWS 같은 제품들은 로그 형식과 필드명이 제각각인데(사용자 필드 하나만 해도 벤더마다 다른 이름을 쓰죠.), 이걸 전부 통일된 형식으로 변환해둬야 서로 다른 제품의 로그를 시간과 사용자 기준으로 엮어볼 수 있습니다.

Q1 · EVIDENCE

STELLAR CYBER®

600+ deep integrations

Normalized, not just connected

Every source lands in one schema — not an API call returning a foreign format.

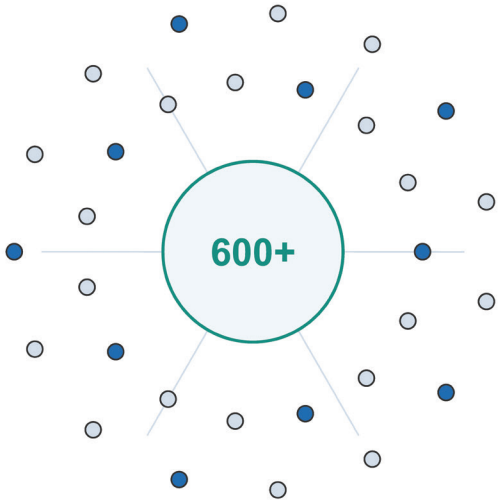
Maintained against vendor drift

Field types and formats change upstream. Someone has to own that, forever.

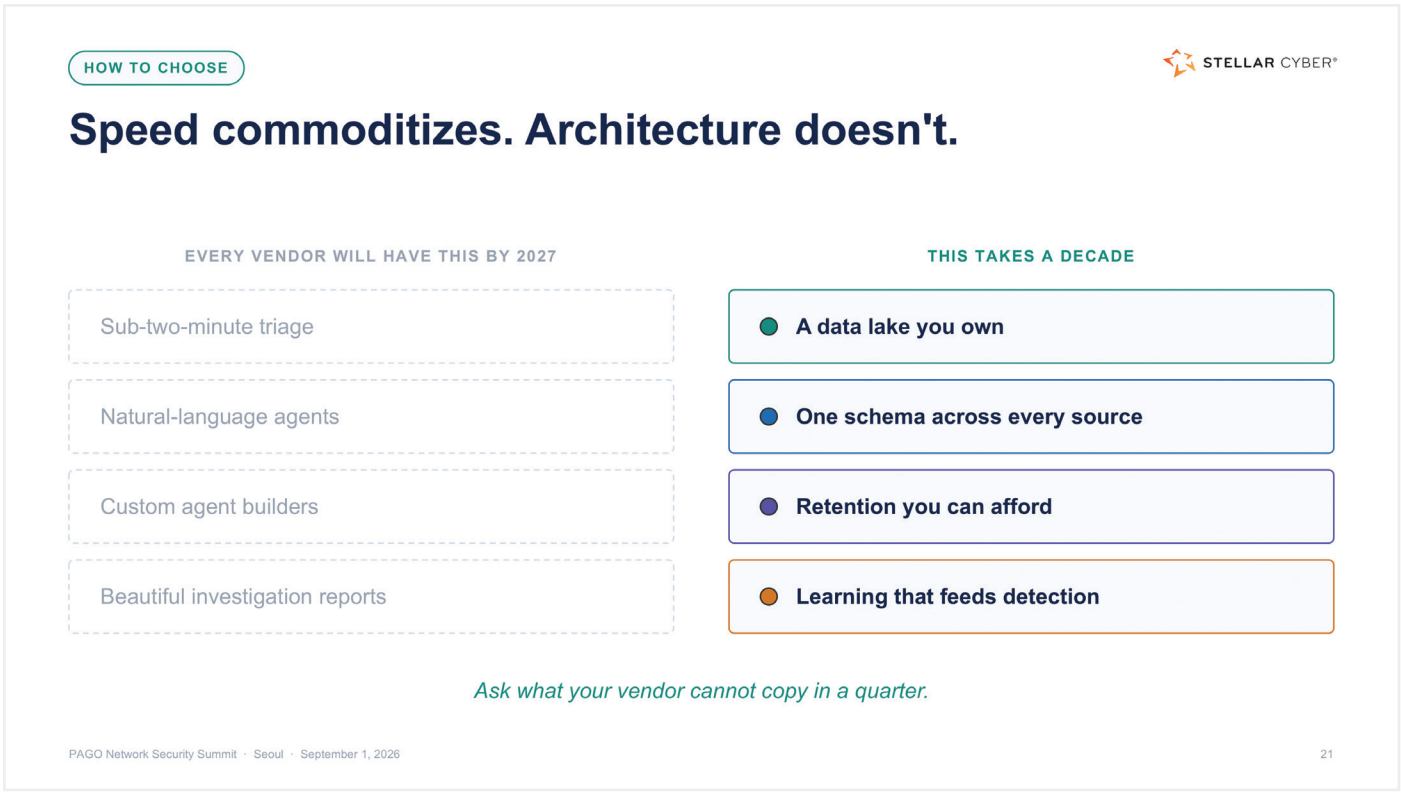
Ten years of accumulation

Integration depth is the context graph. It cannot be bought in a quarter.

A Gartner analyst has argued the advantage goes to vendors with the best context graph — either broad first-party coverage, or hundreds of connectors.



PAGO Network Security Summit · Seoul · September 1, 2026 20



그리고 이러한 작업이 한 번 해두고 끝나는 게 아니라는 점도 강조했는데요. 벤더들이 제품을 업데이트할 때마다 로그 형식이 계속 바뀌기 때문에(이걸 vendor drift라고 표현하더군요.), Stellar Cyber 600여 개 제품 각각의 변화를 10년 동안 놓치지 않고 따라가며 스키마를 유지보수해왔고, 이 누적된 작업량 자체가 신생 벤더는 몇 달 안에 흉내 낼 수 없는 영역이라는 겁니다.

발표 말미에 Wei CTO는 두 종류의 역량을 구분했습니다. 하나는 "2분 이내 경보 분류, 자연어 AI 에이전트, 커스텀 에이전트, 보기 좋은 조사 리포트"처럼 지금은 벤더마다 차이가 있지만 2027년이면 거의 모든 벤더가 기본으로 갖추게 될 기능들입니다. 다른 하나는 앞서 설명한 것과 같은 "직접 구축한 데이터 레이크, 모든 데이터 소스에 걸친 하나의 표준 형식, 감당 가능한 비용의 데이터 보존, 실제 탐지 결과로 이어지는 학습 구조"로, 몇 년에서 10년 단위로 쌓아야 하는 역량들입니다. 그는 이걸 "속도는 상향평준화되지만, 아키텍처는 그렇지 않다"며, 이게 Stellar Cyber만의 강력한 경쟁력이라고 강조했습니다.

“ 속도는 상향평준화되지만, 아키텍처는 그렇지 않다

생각해 봅시다. 특정 솔루션을 검토하는 자리에서, 벤더사 직원들이 데모에서 흔히 보여주는 "경보를 2분 안에 분류합니다"는 것만으로는 벤더 간의 역량 차이가 두드러지게 드러나지 않을 수 있습니다. 이건 Wei CTO가 언급했듯 2027년이면 다 비슷해질, 상향평준화 될 지표이기 때문입니다. 대신 "이 판단을 내릴 때 참고한 데이터 소스가 몇 개였는가", "그 소스들의 로그 형식이 바뀔 때마다 누가, 얼마나 자주 스키마를 다시 손보는가"를 물어보면 벤더 간 역량 차이를 가늠해 볼 수 있지 않을까요? 최근 1~2년 새 AI 기능을 부랴부랴 얹은 벤더라면 이러한 질문에 구체적인 숫자나 사례로 답하기 어려울 가능성이 클 테니까요.

SentinelOne
Autonomous AI Meets Human Expertise: The Future of Modern Security Operations



발표자로 나선 Roshan Pradeep Kumar CTO는 초기 침투부터 횡적 이동(Lateral Movement)이 시작되기까지 걸리는 시간이 평균 29분이라는 수치를 제시했습니다. 그러면서 제조와 반도체, 헬스케어 환경에서는 이 29분이 사실상 사람이 개입해 대응할 수 있는 시간의 전부라고 설명했습니다.

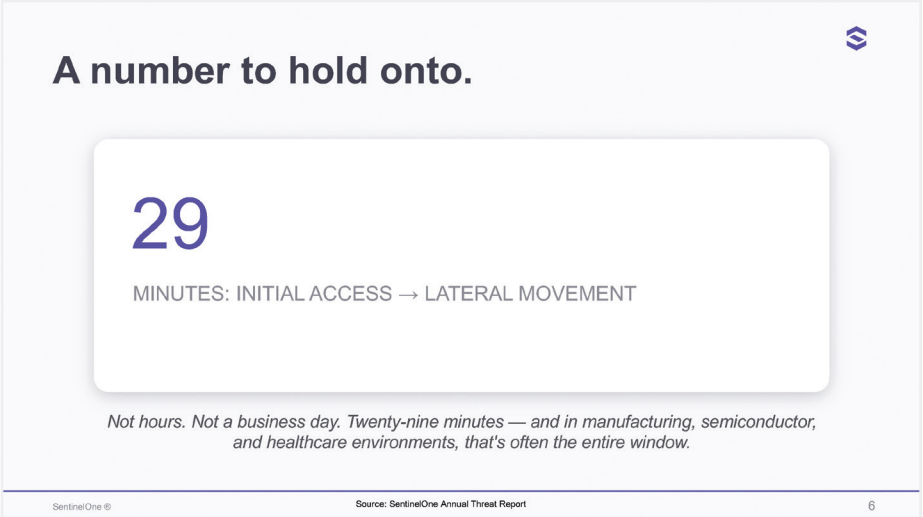
이어 AI와 사람의 역할을 나눈 그림을 보여줬는데, AI는 하루 수백만 건의 이벤트를 실시간으로 상관분석하고 기계 속도로 위협을 차단하는 노이즈 제거 역할을 맡고, 사람은 애매하고 판단이 필요한 결정과 AI가 한 번도 본 적 없는 새로운 상황에 대한 대응을 맡는다는 구도였습니다.

이어 실제 방어 사례가 공개됐습니다. 3주 사이에 1티어급 공급망 공격이 세 건 발생했다는데요. AI 코딩 에이전트가 승인 절차 없이 악성 패키지를 자동 설치한 LiteLLM 공격, 북한 배후로 추정되는 조직이 방치된 npm 토큰을 탈취한 Axios 공격, 정상 서명된 바이너리에 악성코드가 심겨 유포된 CPU-Z 공격이었습니다.

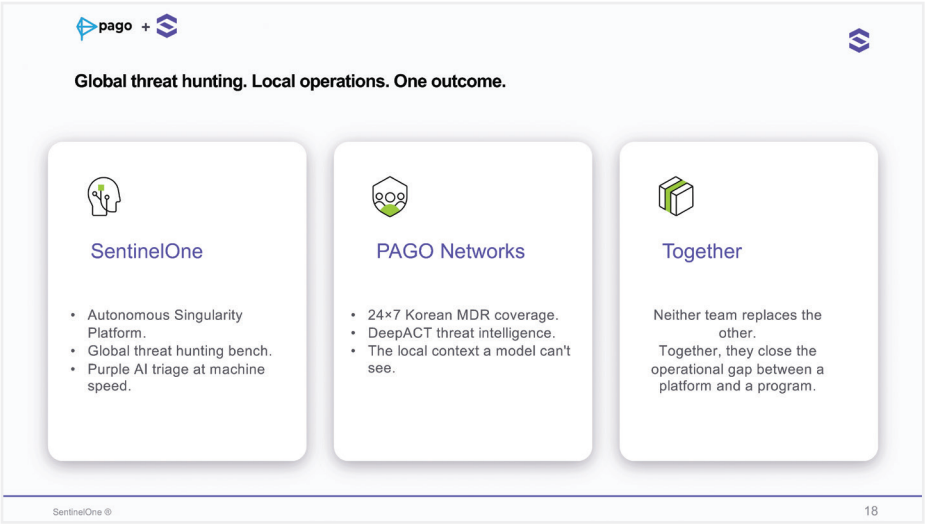
SentinelOne은 이 세 건 모두를 알려진 시그니처나 클라우드 판정 없이 행위 패턴만으로 자율 차단했다며, LiteLLM의 경우 인터프리터 실행, Base64 디코딩, 하위 프로세스 생성이라는 행위 조합만 보고 44초 만에 관련 이벤트 424건을 전부 종료시켰다고 밝혔습니다.

발표 말미에 Kumar CTO는 파고네트웍스와의 관계도 언급했습니다. SentinelOne이 자율 탐지 및 차단 플랫폼과 글로벌 위협 헌팅을 맡고, 파고네트웍스가 24×7 한국 현지 대응과 AI 모델이 알 수 없는 맥락(국내 규제, 조직 문화, 언어)을 맡는다는 구도라는 것인데요. 어느 한쪽이 다른 쪽의 업무를 줄여주는 게 아니라, 플랫폼 혼자서는 메울 수 없는 운영의 간극을 파트너가 채운다는 설명이 이어졌습니다. 이건 7월 발표된 SentinelOne x 파고네트웍스 Hybrid MDR에 대한 내용인데, 곧 다시 다루겠습니다.

정리하면, SentinelOne 발표는 29분과 44초라는 상징적인 두 숫자로 요약됩니다. 보안 솔루션 벤더를 검토할 때 "탐지율이 몇 퍼센트냐"보다 "본 적 없는 공급망 공격 패턴에서 시그니처 없이도 차단할 수 있느냐"가 실제 방어력을 가늠할 수 있다는 겁니다. 다만 이 사례가 SentinelOne 단독의 성과가 아니라 24×7 MDR 서비스를 제공하는 파트너와의 분업 하에 나온 결과라는 점에 주목해야 합니다. 아무리 빠른 자율 차단 엔진이라도, 그 결과를 해석하고 조직 상황에 맞게 후속 조치할 사람이 상시 붙어 있지 않으면 이 44초는 그저 벤더가 자체적으로 테스트한 숫자로 치부될지도 모를 일입니다.







AI

하루 수백만 건 이벤트를 실시간 상관분석, 기계 속도로 차단, 노이즈 제거

사람

애매한 판단과 AI가 본 적 없는 새로운 상황

SENTINELONE + PAGO

자율 플랫폼과 글로벌 헌팅. 파고: 24×7 현지 대응과 AI가 모르는 맥락(규제, 조직 문화, 언어).

파고네트웍스 세션

HYBRID SECOPS IN ACTION:
TWO TEAMS, ONE SECURITY OPERATION
권영목 대표



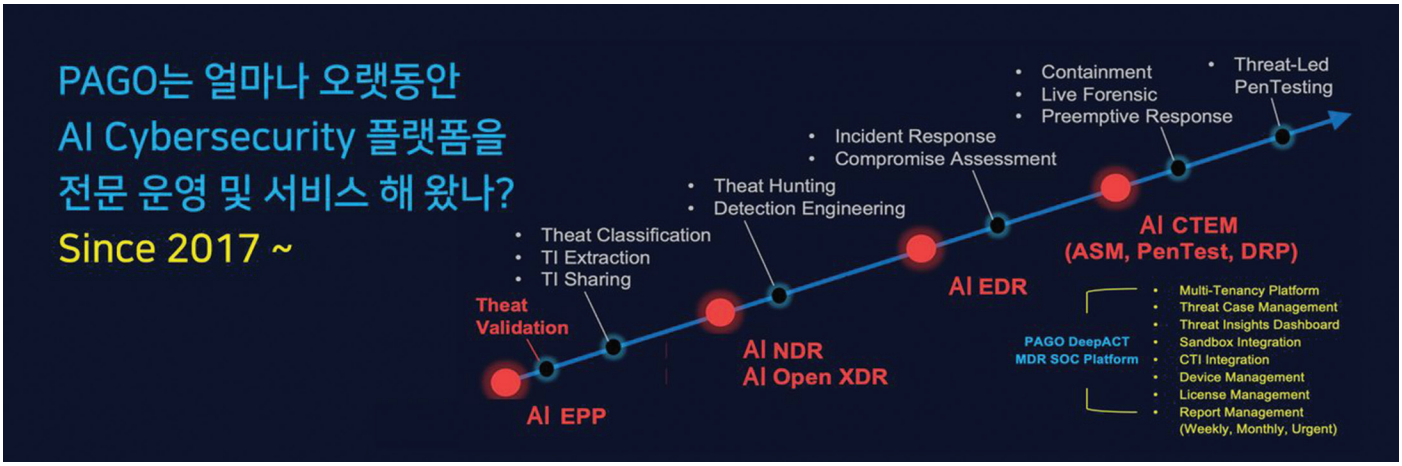
권 대표는 파고의 초기 AI 보안을 백조에 비유했습니다. 수면 위에서는 우아하게 떠 있지만, 물밑에서는 쉴 새 없이 발길질하고 있었다는 것인데요. 탐지 성능 자체는 좋았지만, 전문가가 직접 룰을 만들고 그 결과를 슬랙이나 메일로 일일이 공유하는 노동집약적인 구조였다는 설명이 이어졌습니다.

그는 AI 에이전트와 에이전틱 AI가 등장하면서 파고도 이 흐름을 받아들이기 시작했고, 지금도 플랫폼을 하나하나 만들어가는 중이라고 밝혔습니다. AI로 인한 기술의 변화 속도 자체가 서비스 제공자인 파고 입장에서도 체감될 만큼 빠르다고 느꼈기 때문에, 이 격차를 따라잡기 위한 파고의 노력은 여전히 진행 중입니다.

이어서 권 대표는 SentinelOne과의 2 Team 1 Security Operation, Hybrid MDR 모델이 나온 배경을 설명했습니다. 원래 SentinelOne 자체도 자사 EDR을 기반으로 한 MDR 서비스를 제공하고 있어서, 고객사에 파고 MDR을 제안할 때마다 "본사가 직접 MDR을 하면 더 낫지 않냐"는 의문에 부딪혔다고 하는데요. 같은 제품을 두고 벤더의 MDR과 파고의 MDR이 경쟁하는 상황이 반복되자, 경쟁 대신 두 팀을 합치는 쪽으로 미국 본사와 합의했습니다.

그 결과가 하이브리드 MDR 모델로, 고객사는 추가 비용 없이 벤더사의 MDR 팀까지 함께 얻고, 두 팀은 같은 경보를 나눠 보는 게 아니라 서로 헌팅 트리거를 주고받는 형태가 되었습니다. 미국 팀이 트리거를 만들면 파고가 대응하고, 파고가 자체 룰로 트리거를 만들면 그 내용이 미국 본사의 탐지 체계에 업데이트로 반영되는 식입니다. 이 모델은 SentinelOne 본사에서 혁신성을 인정받아 다른 벤더로도 전이되고 있다고 밝혔습니다.

여기에 Stellar Cyber로부터는 공식 MDR 서비스 프로바이더 인증을 받았습니다. 권 대표는 이런 벤더 협업을 9년 반 동안 이어오면서, 이제는 파고가 주도하는 PAGO Trusted AI Alliance를 통해 반대로 벤더들의 제품이 자사 서비스 안에서 제대로





작동하는지 인증하는 역할까지 하고 있다고 설명했고요. 현재 11개 벤더와 협업 중이며, 이 중 7개는 이미 하이브리드 또는 공식 MDR 프로바이더 지위를 확보했고 나머지 4개는 협의가 진행 중이라고 밝혔습니다.

PAGO DeepACT 플랫폼은 방어자 관점(DEFENSE)과 공격자 관점(ATTACK)을 나눠 운영하는데, 권 대표는 이 두 관점 모두에서 위험 이벤트가 뜨지 않는 경우에도 Detection-Engineering이 헌팅 룰을 100% 자동화해 매일 업데이트한다고 설명했습니다. 경보가 없다는 게 공격이 없다는 뜻인지, 아니면 솔루션이 못 찾고 있는 것인지 구분하기 위해 만든 헌팅 룰셋을 예전엔 사람이 만드는 데 매달렸지만, 지금은 AI가 위협 인텔리전스와 프론티어 모델까지 연계해 자동으로 생성하고 코드처럼 버전 관리한다고 설명했습니다.

MDR 서비스를 검토하는 조직이라면 이번 파고네트웍스와 SentinelOne과의 협업 결과물인 하이브리드 MDR 서비스에 주목합시다. 보통 EDR 벤더가 직접 제공하는 MDR을 쓸지, 아니면 별도의 전문 MDR 업체를 쓸지를 놓고 하나를 고르게 되는데, 이 둘이 같은 경보를 두고 경쟁하거나 한쪽만 선택해야 한다는 전제 자체가 당연하게 여겨지기 때문이죠. 하지만 벤더와 파트너사가 서로 트리거를 주고받으며 협업하는 구조라면, 이 양자택일이 불필요할 수 있습니다. 더군다나 한 회사의 MDR 서비스에서 부족한 부분을 다른 회사의 MDR 서비스에서 메워줄 수 있다면 말이죠.

지금 검토 중인 EDR 벤더의 MDR 서비스와 실제 운영 주체인 파트너사가 어떤 형태로 협업하는지, 여전히 한 쪽만 선택해 서비스를 받아야 하는지 점검해 볼 필요가 있겠습니다.

PAGO DeepACT Platform 특징

3대 브랜드 유기적 통합	공격 이전 / 이후, 전체 사이클 대응	AI + 보안전문가 협업 시너지
DeepACT ATTACK	→ 공격 이전 단계 (선제적 위험 검증)	**AI : 대규모 데이터 분석 / 자동화**
DeepACT DEFENSE	→ 공격 이후 단계 (고도화된 탐지 대응)	**보안전문가 : 위협 맥락 / 대응 순위**
DeepACT Detection-Engineering	→ 통합 시너지 단계 (인텔리전스 연계)	**지향점 : 더 많은 탐지를 넘어,** **:** 더 나은 의사결정 구현

PROACTIVE SECOPS:
REDUCING RISK BEFORE THE ATTACK WITH CTEM & EXPOSURE VALIDATION
이시우 주임



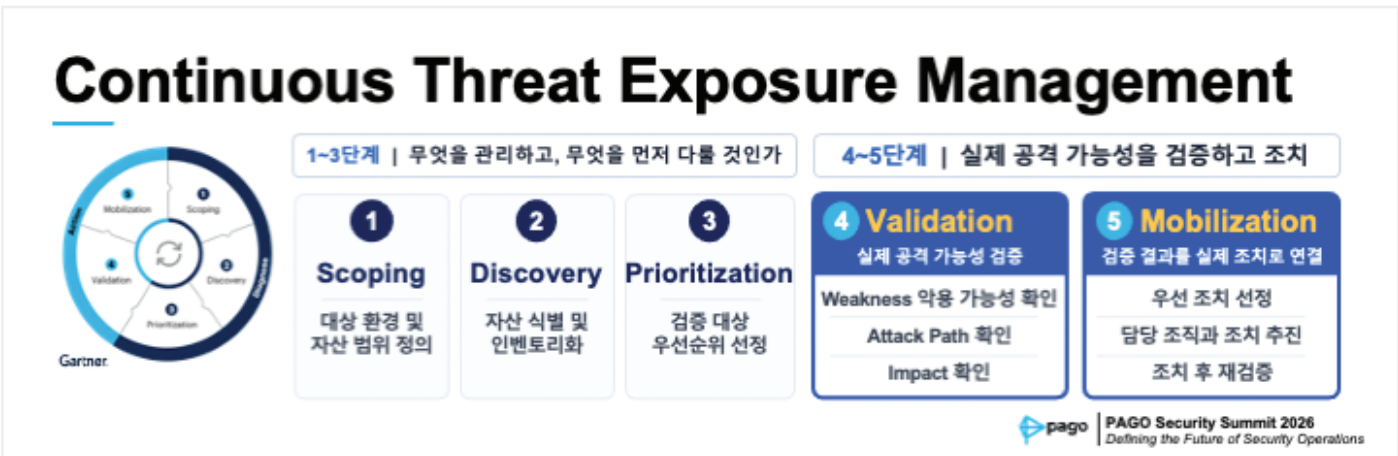
이시우 주임은 기존 EDR, NDR, XDR이 다루는 영역이 경보가 뜬 이후에 국한돼 있다고 짚었습니다. 공격자는 경보가 뜨기 훨씬 전부터 외부 노출을 탐색하고 초기 침투를 거쳐 공격을 확장하는데, 이 구간을 Detection Gap이라고 설명했고요. 이 차이를 선제적으로 관리하지 않으면, 분류(Triage)와 대응(Response)이 아무리 빨라져도 결국 사후 대응에 머무른다는 게 그가 제기한 문제의식입니다.

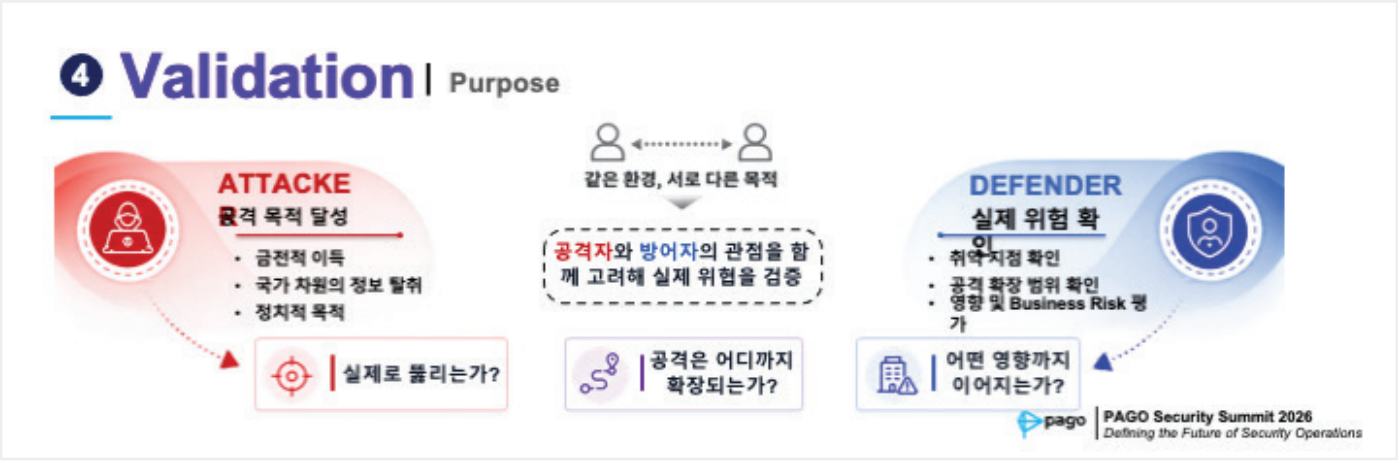
이걸 관리하는 프레임워크로 Gartner의 CTEM(Continuous Threat Exposure Management) 프레임워크를 가져와 스코핑 → 디스커버리 → 우선순위 결정 → 검증 → 조치 5단계로 소개했습니다.

그는 검증(Validation) 단계에서는 취약점 악용, 자격증명 확보, 내부 이동, 도메인 권한 확보까지 각 단계마다 실제 증거를 자동으로 확보하는 자율형 침투 테스트를 수행한다고 설명했습니다. 단순 스캐너가 "여기 구멍이 있다"고만 알려주는 것과 달리, 그 구멍을 통해 실제로 어디까지 침투할 수 있는지를 증거로 보여준다는 것인데요.

이 대목을 "우리 회사가 A 그룹의 공격을 받았다" 또는 "A 그룹이 우리를 노리고 있다"처럼 실제로 특정 공격자가 확인됐다는 뜻으로 잘못 받아들이면 안됩니다. 실제로는 "이 취약점의 특성이 A 그룹이 과거에 썼던 수법과 닮았다"는 유사성 참고 자료일 뿐, 우리 회사를 실제로 그 그룹이 공격했다거나 공격할 거라는 걸 입증하는 증거가 아니라는 겁니다.

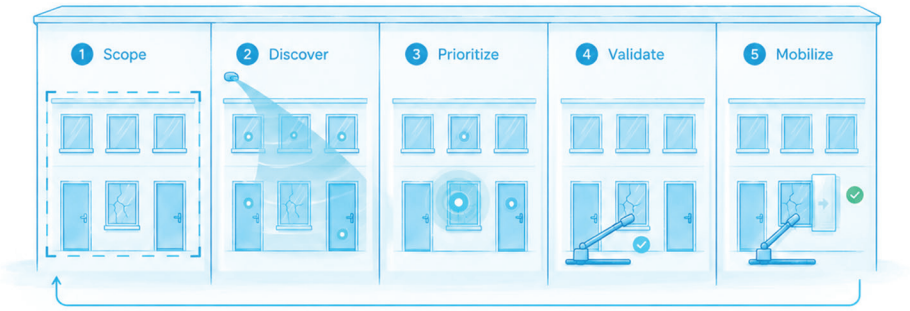
이 구분이 중요한 이유는 실무에서 흔히 이 정보를 근거로 "





우리는 국가 배후 조직의 표적이다"라며 과도하게 대응하거나, 반대로 특정 그룹만 방어하면 된다고 오판하는 경우가 생기기 때문입니다. 그는 이 정보를 그러한 결론의 근거로 쓰지 말고, 그저 "이 취약점이 왜 위험한지"를 이해하는 데 참고하는 부가 정보 정도로만 받아들이라고 강조했습니다.

이어지는 설명에서, 그는 파고네트웍스는 내부적으로 검증된 위험을 실제 조치로 옮기는 단계에서 근본 원인을 제거하는 리미디에이션(Remediation)과 당장 위험도만 낮추는 미티게이션(Mitigation)을 상황에 따라 병행한다고 설명했습니다. 이 조치를 실제로 이끌어내는 역할이 SES(Security Engagement Specialist)인데, 단순히 위험 목록을 전달하는 게 아니라 고객과 우선순위를 협의하고 조치 과정에 직접 참여해 결과까지 확인하는 역할입니다.



여기서 SES는 파고네트웍스가 새롭게 만든 직군이 아니라, Gartner가 정의한 Mobilization Coordinator라는 역할을 파고식으로 재정의한 것이라는 것을 참고해 주시고요. 발표 말미에는 실제 재검증 사례도 공개했는데, 조치를 마친 뒤에도 인프라가 계속 바뀌면서 신규 자산과 신규 취약점이 계속 발견됐다는 내용이 이어졌습니다.

이번 세션을 듣고 나서 문득 그런 이런 생각이 들었습니다. 지금 우리 회사에서 사용하는 보안 서비스가 "취약점을 찾아서 알려주는 것"까지인지, 아니면 "그 취약점이 실제 조치로 이어졌는지 확인하는 것"까지인지 확인해 볼 필요가 있지 않을까 하는 생각입니다. 만약 전자에서 끝나는 서비스라면, 발견된 위험이 부서 간 조율 실패로 방치되는 일이 반복될 가능성이 크지 않을까요? 위협이 발견은 되는데, 해결은 안되는 그런 상황에 놓일 수 있다는 겁니다.





AI-POWERED SECOPS: ACCELERATING ALERT TRIAGE WITH AI INVESTIGATOR

김재근 주임

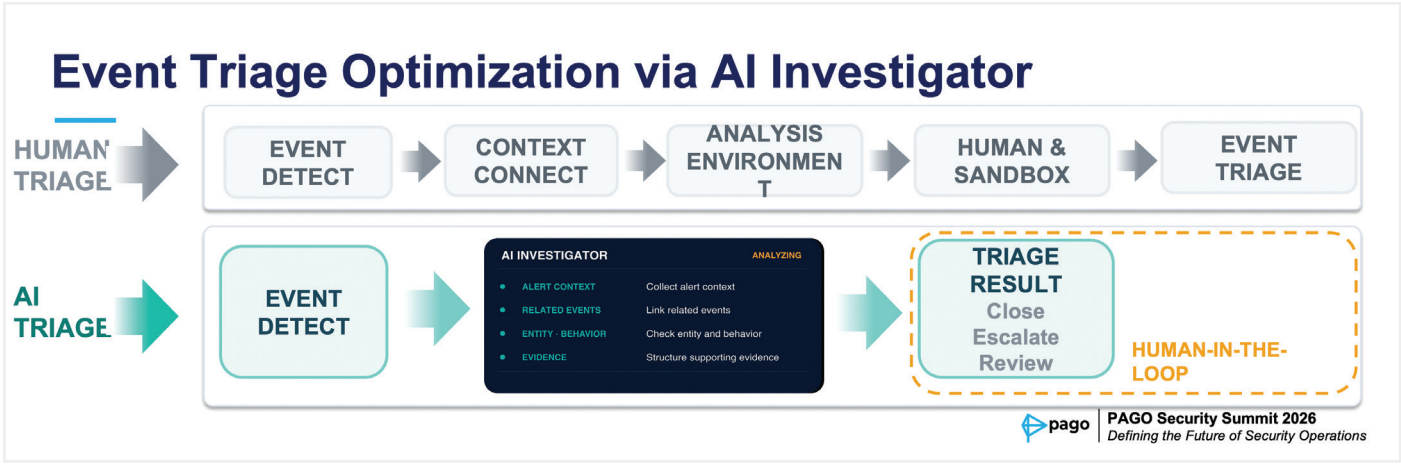
이번 발표에서 김재근 주임은 AI Investigator 도입을 하나의 전문 인력을 채용하는 과정에 비유했는데요. 조직 내에서 반복되는 보안 운영 업무를 분류하고 AI가 맡을 조사 범위를 구체적으로 정의하는 Define, 흩어진 데이터를 맥락에 맞게 연결하는 Context, 조사 근거와 함께 최종 판정을 구조화해 제시하는 Verdict, 이 세 요소로 작동한다고 설명했습니다.

좀 더 구체적으로 들여다 봅시다. 기존의 분류작업, Triage는 이벤트가 탐지되면 분석가가 직접 맥락을 연결하고, 안정적인 분석 환경(샌드박스 등)에서 정적, 동적 분석을 거쳐 검증까지 마쳐야 했습니다. 이 과정에서 분석가가 여러 툴과 로그 화면을 오가며 많은 시간을 썼다는 게 발표자의 설명이었고요.

반면 AI 협업 트리아지는 이벤트가 탐지되면 AI 인베스티게이터가 관련 Alert, Entity, Behavior 데이터를 곧바로 수집하고 분석해서 결과를 사람에게 전달합니다. 그리고 사람은 AI가 전달해 준 데이터를 기반으로 판단을 하는 구조입니다.

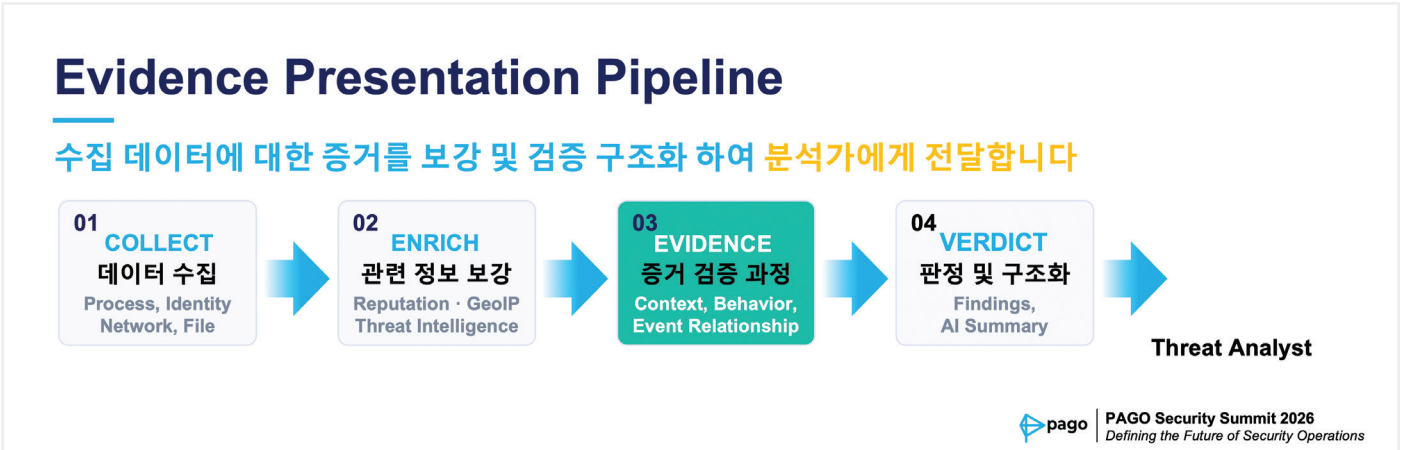
그는 AI의 판정을 신뢰할 수 있게 만드는 장치로 관측 데이터 수집 → 정보 보강(TI, GeoIP) → 증거 검증 → 판정 및 요약으로 이어지는 증거 파이프라인을 공개했습니다. 실제 사례로는 미식별 해외 IP의 비정상 RDP 로그인, 그 세션 안에서의 파워셸 실행, 외부 URL에서의 악성 페이로드 다운로드까지 이어지는 흐름을 AI가 하나의 시나리오로 엮어 제시한 걸 보여줬는데요.





여기서 최종 조치 승인과 AI 튜닝을 위한 피드백은 사람이 맡는다는 원칙을 강조했는데, Gartner Security Summit 2026의 조사에서 실무자의 60%가 "반드시 인간의 결정으로 운영되는 SOC가 필요하다"고 답했고 64%는 "AI 결과물에 인간의 검증과 책임이 수반돼야 한다"고 답한 것을 근거로 들었습니다. 그는 이 변화를 제본스의 역설에 빗대어, AI가 반복 업무를 줄여주는 만큼 그 여유 자원이 위협 헌팅과 탐지 엔지니어링 같은 더 고도화된 업무로 재배치된다고 정리했습니다.

이번 세션에서 소개된 Triage 비교 장표는 보안 담당자나 CISO가 보안 벤더 평가 시 활용하면 아주 좋습니다. "우리 조직에서 Triage 하나에 지금 몇 명이 몇 단계를 거쳐 처리하고 있는가"를 먼저 파악해두면, 이후 AI 도구를 붙였을 때 그 단계 중 실제로 무엇이 줄었는지를 구체적으로 비교할 수 있겠죠. 보안 솔루션을 검토할 때 단순히 "엄청 빨라집니다"는 벤더의 말만 믿고 판단지 말고 우리 조직의 Triage 과정을 먼저 단계별로 파악해 봅시다. 그러면 AI 기반 보안 솔루션 혹은 서비스 도입 효과를 더 명확하게 예측할 수 있을겁니다.

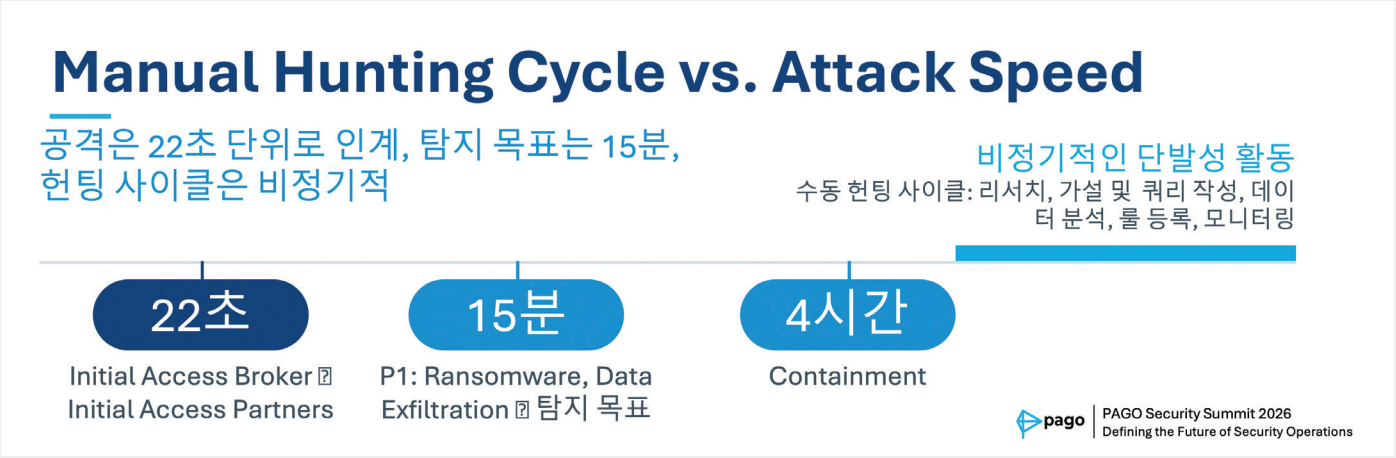




ADVANCED SECOPS:
HUMAN-LED THREAT HUNTING & DETECTION ENGINEERING IN THE AI ERA
권표 이사

발표자 권표 이사는 과거 Initial Access Broker가 침투 경로를 확보해 다른 공격 그룹에 넘기는 데 약 8시간이 걸렸다면, 이제 Initial Access Partner는 계정 탈취부터 백도어 설치까지 단 22초 만에 끝낸다고 소개했습니다. 이에 맞서는 파고네트웍스의 목표치는 15분 내 탐지, 4시간 내 격리라고 밝혔는데요. 공격자의 시간 단위가 초로, 방어자의 목표는 분, 시간으로 여전히 그 차이가 크다는 것을 보여준겁니다.

그리고 이 격차를 메울 유일한 방법이 분석가 개인의 직관에 의존하는 비정기적 헌팅이 아니라, 탐지 로직 자체를 소프트웨어처럼 자산화하는 디텍션 엔지니어링이라고 강조습니다.



그는 이번에 Gartner의 "탐지 콘텐츠 없는 SIEM은 중립 기어에 놓인 슈퍼카와 같다. 비싸지만 아무 데도 가지 않는다"는 표현을 인용하면서, 이를 위해 AI가 글로벌 위협을 리서치하고, 가설을 세워 쿼리를 만들고, 벤더에 종속되지 않는 시그마 룰을 생성하는 3단계 파이프라인을 운영한다고 설명했습니다.

실제 사례로는 지난 8월 4일 발견된 ChainDrop NPM Worm(868개 패키지, 1,381개 버전 감염)의 IOC를 시그마 룰로 만들어 17억 건이 넘는 이벤트에 검증한 결과, 캠페인 마커가 전혀 없다는 걸 확인했다고 소개했고요. Tomcat 관련 룰도 초기 7만여 건의 매칭을 튜닝을 거쳐 0건으로 좁혔다고 합니다.

이 과정에서 AI는 매주 자동으로 리서치 → 조사 → 튜닝 → 문서화까지 마치고, 사람에게 남는 건 Pull Request를 검토하고 실제 배포로 승인하는 Merge 권한 하나뿐이라고 소개하며, 이걸 Detection-as-Code로 정리했습니다.

그러면서 "왜 이 룰을 만들었는가", "어떤 오탐 때문에 수정했는가" 같은 맥락이 Git 같은 코드 저장소에 커밋 기록으로 전부 남게 된다고 했는데요. 이렇게 하면 그 지식은 특정 분석가 한 사람의 머릿속이 아니라, 누구나 열어볼 수 있는 조직의 기록이 됩니다. 그럼 특정 분석가가 퇴사하거나 부서를 옮겨도 탐지 룰의 히스토리와 판단 근거는 그대로 남아 있어 자산이 되는거죠. 이 룰이 배포되는 EDR을 비롯한 보안 솔루션 전체가 점점 더 강력해 질겁니다.

하지만 이와 반대로 사람에만 의존하게 되면, 특정 베테랑 분석가가 "이 룰은 예전에 이런 문제 때문에 이렇게 만들었다"를 기억으로만 알고 있고, 그 사람이 없으면 왜 그 룰이 그렇게 설정돼 있는지 아무도 설명할 수 없는 상태가 될 수 있습니다. 이 경우 그 분석가가 퇴사하면 탐지 체계의 판단 근거 자체가 남지 않게 될겁니다. 그래서 Detection-as-Code 기반 탐지 룰 자산화가 필요한 것이라고 이해하시면 되겠습니다.

From Ad-hoc Rules to Detection-as-Code

BEFORE - AD-HOC

Analyst discretion | Ad-hoc rule creation | Manual Rule Entry

분석가 개인의 시간에 종속되는 구조

AFTER - DETECTION-AS-CODE

Git Commit | Pull Request Review | Automated CI/CD

버전 관리되고 추적되는 팀의 자산

코드로 다루는 탐지 콘텐츠는 변경 주체, 시점, 이유가 이력으로 남음

pago | PAGO Security Summit 2026
Defining the Future of Security Operations

이번 세션의 핵심은 탐지 및 조치 프로세스의 자산화입니다. 조직에서 운영하는 탐지 룰이 특정 분석가의 기억에만 있는지, 아니면 코드 저장소에 기록으로 남아 누구나 확인할 수 있는지가 중요하다는 건데요. 지금 우리 조직의 탐지 룰을 두고 "이걸 왜 이렇게 설정했는지" 물었을 때, 특정 인물에게 물어봐야만 답이 나오는지, 아니면 기록만 열어봐도 되는 상태인지 점검해 봅시다. 이 자산화의 시작이 우리 회사 보안을 한층 더 강화할 수 있는 첫 걸음이 될겁니다.

PR-Based Validation and Human Approval

AI는 변경안 제출까지, 배포 승인은 보안 전문가만 수행

STEP 04 / 04

Weekly threat hunt 2026-08-10/16: Lazarus reverse_ssh #3

Merged | merged 1 commit into main from weekly-hunt/2026-08-10_202

Conversation 0 | Commits 1 | Checks 0 | Files changed 5

Pull Request: 룰 변경 기안, Merge: 승인 및 배포

Test plan

- python3 scripts/validate_s1_pq.py - 135/135 rules scanned, converted, no duplicate IDs
- Live PowerQuery hunt for each of the 3 new rules + 2 prior-week rules against 2026-08-10T00:00:00Z-2026-08-17T00:00:00Z
- Base-rate sanity queries to confirm zero-hit results reflect real telemetry absence, not a broken query or empty data source

AI의 검증 근거를 바탕으로 결과가 사실인지 사람이 판단

pago | PAGO Security Summit 2026
Defining the Future of Security Operations



> 탐지 콘텐츠 없는 SIEM은 중립 기어에 놓인 슈퍼카와 같다. 비싸지만 아무 데도 가지 않는다





여기까지 PAGO Security Summit 2026 오후 세미나 내용 중 조찬 및 기자 간담회에서 소개되지 않은 세션 위주로 정리했습니다. 1부와 이번 2부 칼럼을 통해 PAGO Security Summit 2026이 어떤 내용이 발표된 행사였는지 가늠하실 수 있을텐데요. 하지만, 아직 좀 부족하다는 느낌을 지울 수 없습니다. 1년 만에 돌아온 행사의 내용을 정리하는 것으로 파고네트웍스가 나아가고자 하는 Augmented SOC with Agentic AI라는 목표와 가치를 충분히 이해하기에 다소 부족하지 않나 라는 생각이 듭니다.

그래서 3부를 준비했습니다. 이어지는 3부 칼럼에서는 파고네트웍스 권영목 대표와의 단독 인터뷰 내용을 토대로 저만의 생각을 겻들여 풀어보겠습니다. 인터뷰 전체 영상도 공개할 예정이니 기대해 주세요. 끝!

PART

03

권영목 대표 단독 인터뷰

소수 의견을 지우지 않는다는 것

칼럼 3부

2054년 워싱턴 D.C., 살인 사건은 일어나기 전에 예측되고, 범인은 죄를 저지르기도 전에 체포됩니다. 스티븐 스필버그의 2002년 영화 <마이너리티 리포트>에 나오는 프리크라임(Precrime) 시스템 이야기입니다. 6년간 워싱턴 D.C.에서 살인 사건이 단 한 건도 발생하지 않았다는 설정으로 영화는 시작하죠.

당시 영화는 허공위에 뜬 대시보드를 손으로 조작하는 주인공의 모습으로 화제가 됐었는데, 상당히 철학적인, 생각할 거리를 많이 던져주었던 영화로 기억합니다. 이 영화에 등장하는 프리크라임 시스템의 핵심은 범죄가 일어난 뒤 수사하는 게 아니라 일어나기 전에 막는다는 이 발상인데, 지난 두 편의 칼럼에서 다룬 파고네트웍스의 문제의식과 유사한 것이 있습니다. 알람이 울리고 나서 대응하는 게 아니라, 알람이 울리기 전에 개입해야 한다는 것 말이죠.

영화에서 프리크라임을 움직이는 건 세 명의 예지자입니다. 이들이 각자 범죄를 예측하고, 이 세 예측이 일치하는 장면을 근거로 아직 죄를 저지르지 않은 사람이 체포되죠. 그런데 세 예지자의 예측이 서로 어긋나는 일도 생깁니다. 다수의 예측과 다른 예측 하나, 이게 영화 제목이기도 한 마이너리티 리포트, 소수 의견입니다. 하지만 프리크라임은 무결성 유지를 위해 무조건 다수 의견인 메이저리티 리포트만 시스템에 전달하고, 소수의견인 마이너리티 리포트는 폐기해 버립니다.

이번 칼럼 3부에서는 파고네트웍스 권영목 대표와의 단독 인터뷰를 계기로, 소수 의견이라는 이 개념을 빌려 필자 나름의 해석을 풀어보려 합니다. 인터뷰에서 나온 이야기도 가져오겠지만, 이번 글의 뼈대는 필자가 사전에 준비한 질문지를 토대로 진행한 인터뷰 내용이라는 점을 미리 밝힙니다. 목차는 아래와 같습니다.

소수 의견을 지우지 않는다는 것의 의미

■ 하나의 사건에 두 개의 결론이 있다면?

영화 속 프리크라임 시스템은 소수 의견을 숨겼지만, 인터뷰에서 권 대표가 들려준 이야기는 사뭇 달랐습니다. 그는 EDR, NDR, XDR에 적용된 AI가 하고 있는 일을 Triage, 분류 작업이라고 하면서, 이벤트를 상관분석하고 위협 인텔리전스를 스스로 조회해서 이게 실제 위협(True Positive)인지 오탐(False Positive)인지 증거와 함께 제출하는 단계까지는 와 있다고 했습니다.

그런데, True Positive라는 판정이 나왔는데도, 맥락을 보면 이게 오탐일 수도 있다는 반대 근거를 AI가 스스로 내놓는 경우가 있다고 합니다. 하나의 사건을 두고 AI가 서로 다른 두 개의 결론을 동시에 제시하는 경우인건데, 프리크라임의 세 예지자 중 한 명이 다른 예측을 내놓는 장면과 마찬가지죠. 영화의 프리크라임 시스템은 이 불일치를 폐기했지만, 권 대표가 설명하는 파고만의 방식은 반대입니다. 반대 근거가 나왔다는 것 자체를 "사람 여러분, 같이 고민해 주세요"는 신호로 받아들인다는 겁니다.

AI 자동화 레벨: 현재 우리의 위치

권(Kwon)은 AI 자동화를 레벨 1부터 4까지로 구분합니다.
현재 보안 AI는 가장 낮은 단계에 있습니다.

레벨 4

레벨 3

레벨 2 — AI가 근거와 함께 분류(triage)하고, 사람이 검증

레벨 1 — AI가 이벤트를 상관분석하고 위협 인텔리전스를 조회

현재: 레벨 1, 또는 레벨 1과 2 사이

1차 분류(FIRST-PASS TRIAGE)가 AI로 넘어가면, 이 업무를 맡던 사람은 두 갈래 중 하나로 이동합니다.

위로 (Up)
더 높은 수준의 판단 업무

옆으로 (Across)
AI의 결과물을 검증하는 감독자



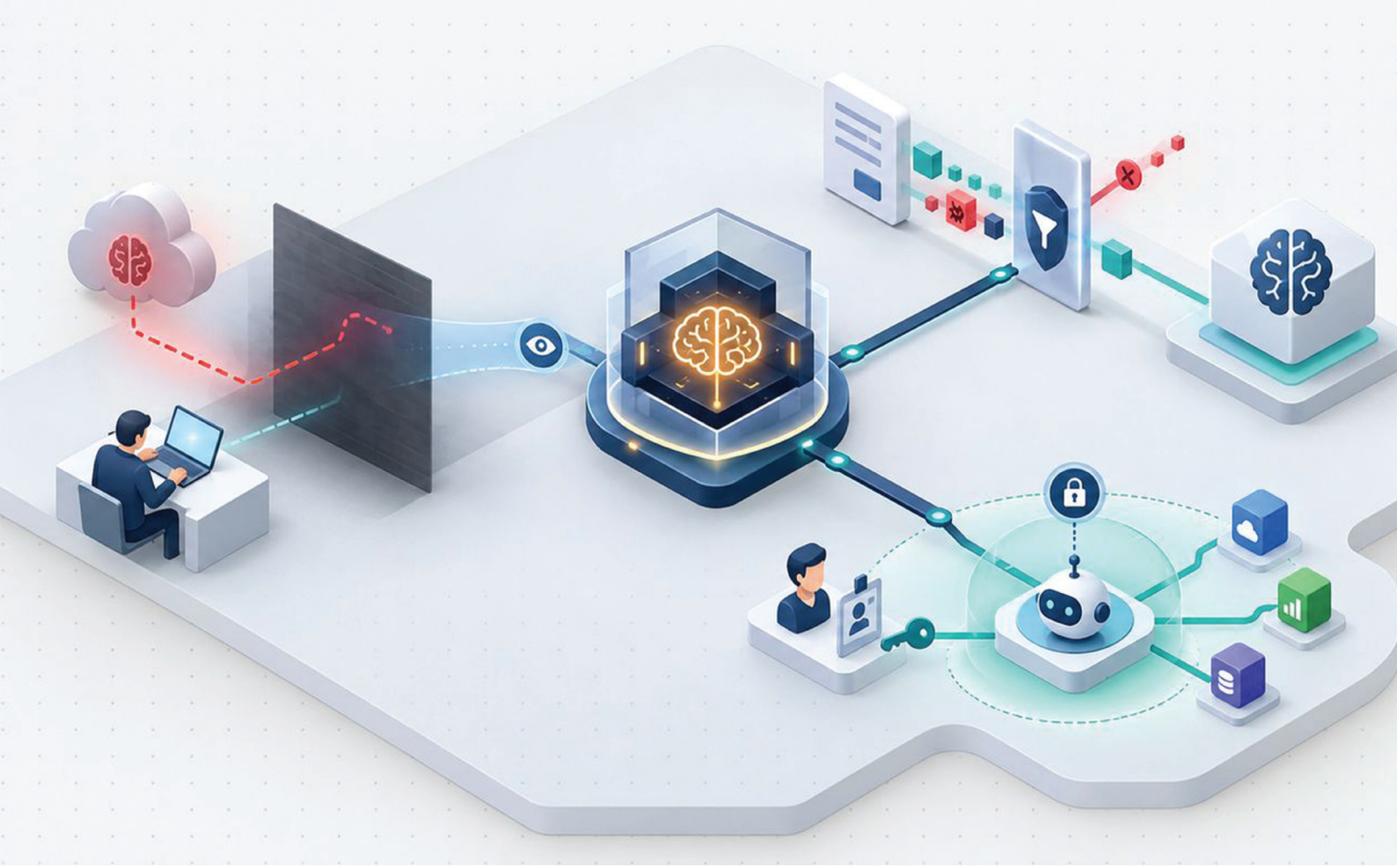


■ 현재의 AI 자동화 수준은 1단계, 혹은 1에서 2로 가는 중간 어디쯤

권 대표는 이어 AI의 자동화 수준을 1단계부터 4단계까지 나눴을 때, 지금 보안 솔루션에 적용된 AI는 1단계, 혹은 1단계에서 2단계로 넘어가는 중간 정도라고 밝혔습니다. 그리고 이 구간에서 사람의 역할이 어떻게 바뀌는지도 구체적으로 설명했는데요. 기존에 분석가가 직접 하던 1차 분류 업무가 AI로 넘어가면, 그 업무를 하던 사람은 두 갈래 중 하나로 이동합니다. 더 상위 단계의 판단 업무로 올라가거나, AI가 내놓은 결과값이 맞는지를 검증하는 감독 역할을 맡게 되는거죠. "AI가 다 알아서 해드립니다"가 아닌, 여전히 사람의 역할이 존재하는 상황이라는 겁니다. AI 시대의 역설이라고 해야 할까요?

영화의 프리크라임 시스템은 자신의 예측이 틀리지 않는다고 전제했기 때문에, 그 예측을 사람이 다시 검토하는 절차 자체가 없었습니다. 그 결과 주인공 앤더튼이 프리크라임 시스템에서 살인을 저지를 것으로 예측되자, 실제로는 죄를 저지르지 않았는데도 범죄예방수사국의 누구도 이 예측을 의심하지 않고 그를 범죄자로 체포하죠. 시스템이 완벽하다고 전제하는 순간, 그 시스템이 틀렸을 때 이를 잡아내고 책임질 사람이나 절차 자체가 설계에서 제외되는 것이 얼마나 위험한지를 여실히 보여주는 장면입니다.

권 대표가 앞서 AI 자동화 수준이 완성형이 아니라 1~2단계라고 못박아 둔 건 이와 결이 다른 맥락입니다. AI의 한계를 인정하면 그 판정을 사람이 다시 확인해야 한다는 절차가 자연스럽게 따라붙고, 그 확인을 맡은 사람이 곧 결과에 책임지는 사람이 된다는 것입니다. 즉, 우리와 함께 해야 할 AI 보안 시스템은 오탐 없이 완벽하게 맞히는 게 아니라, 스스로 확신하지 못하는 부분을 감추지 않고 드러내어 사람의 도움을 요청하는 것이어야 하지 않을까요?



AI 보안에서 봐야 할 것과 보지 말아야 할 것

■ AI SECURITY가 해결하려는 세가지 유형의 문제

권 대표는 인터뷰에서 AI Security가 해결하려는 영역을 세 갈래로 나눠 설명했습니다. 첫 번째는 섀도우 AI, 직원들이 회사가 파악하지 못한 개인 계정으로 외부 AI 모델에 접속하는 문제로, 여기엔 가시성 확보가 우선이라고 했습니다. 두 번째는 프롬프트 입력값과 그 응답값, 즉 인풋과 아웃풋 데이터 보안으로, 과거 DLP가 해결하려던 문제와 일맥상통합니다. 사용자가 AI에게 물어보기 위해 프롬프트에 무분별하게 데이터를 복사 & 붙여넣기 하는 과정에서 데이터가 유출될 수 있고, Ai만 읽을 수 있는 교묘한 악성코드가 문서에 심어져있어 프롬프트 인젝션 공격이 발생할 수 있죠.

세 번째는 권한과 인증입니다. 원래 특정 직원 A가 회사 시스템에서 가진 권한은 자시 부서 자료만 조회가 가능한 것과 같이 제한적입니다. 그런데 이 직원이 AI 에이전트에게 업무를 맡기면서 MCP 같은 방식으로 여러 SaaS 애플리케이션과 연동시키면, 그 AI 에이전트는 A의 권한을 대신 사용해서 여러 시스템에 접근하게 됩니다. 문제는 이 과정에서 AI 에이전트가 여러 앱을 넘나들며 작업하다 보니, 원래 A 한 사람에게 묶여 있던 제한적 권한이 AI를 매개로 실제로 접근 가능한 범위가 눈덩이처럼 커진다는 겁니다. 생산성 향상이라는 명분으로 권한이 확장되는 건데, 이러한 권한 상승 문제가 시스템 해킹 또는 데이터 유출로 이어질 위험이 있습니다.



■ 봐야할 것과 보지 말아야 할 것을 구분해야

이 세 갈래 중 꽤 애매한 것이 뒤의 두 가지, 인풋과 아웃풋 데이터와 권한 및 인증입니다. 둘 다 "AI가 무엇을 하고 있는지"를 보안 벤더가 어디까지 들여다봐도 되는가라는 의문이 생기기 때문입니다. 프롬프트 안에 어떤 내용이 오갔는지, 그 AI 에이전트가 정확히 어떤 데이터에 접근했는지, 이걸 외부에서 서비스를 제공하는 파고와 같은 보안 벤더가 직접 확인해도 되는 걸까요?

권 대표는 여기에 명확히 선을 그었습니다. 프롬프트 안의 입력값과 응답값 그 자체는 고객의 자산이라 파고가 함부로 들여다보지 않는다는 겁니다. 대신 권한이 어떻게 움직였는지, 즉 AI 에이전트가 원래 부여된 범위를 넘어서 접근하거나 스스로 권한을 확장한 흔적 같은 이벤트는 EDR과 XDR이 감시하는 이벤트와 마찬가지로 매니지드 서비스 영역에서 다룬다고 밝혔습니다. 내용물 자체는 손대지 않고, 그 내용물이 만들어낸 움직임만 지켜본다는 겁니다.

사실 "저희는 고객 데이터에 접근하지 않습니다"는 보안 업계에서 흔하게 쓰이는 문구이지만, 실제로 그들이 뭘 보고 뭘 안 보는지는 회사마다 다르고 대부분은 이걸 구체적으로 밝히지 않습니다. 권 대표의 답이 다른 점은, 이 경계를 AI가 알아서 판단하게 두지 않고 사람이 미리 정해뒀다는 겁니다. 어디까지는 봐도 되고 어디부터는 안 되는지, 그 선을 긋는 일 자체를 AI에게 맡기지 않는다는 겁니다.

■ 선을 그을 줄 안다는 것의 원동력은?

그런데 이 선은 처음부터 저절로 그어지지 않습니다. 프롬프트는 안 보고 권한 이동은 봐도 된다는 판단은, 어느 쪽이 실제로 위협 신호가 되고 어느 쪽이 그냥 고객의 사적 영역인지를 수없이 구분해본 경험에서 나옵니다. 즉 이 경계를 그을 줄 안다는 것 자체가 하나의 역량이고, 이 역량이 어디서 만들어지는지가 파고의 경쟁력이 된다는 것인데요. 이게 무엇인지 이어서 살펴봅시다.





똑똑해 보이는 건 AI지만, 판단하는 몫은 결국 사람에게 주어진다

■ 워터탱크 속의 재능

프리크라임에서 진짜 예측 능력을 가진 건 시스템이 아니라 애거사를 비롯한 세 예지자입니다. 이들은 워터탱크 안에 몸을 담근 채 하루 종일 누워 있죠. 프리크라임이라는 이름의 첨단 인터페이스, 그러니까 앤더튼이 손을 휘저으며 이미지를 조작하는 그 장면은 사실 껍데기에 지나지 않습니다. 예측이라는 원천 능력은 탱크 속 세 예지자에게서 나오고, 나머지는 그 능력을 눈에 보이는 형태로 가공하는 장치일 뿐입니다.

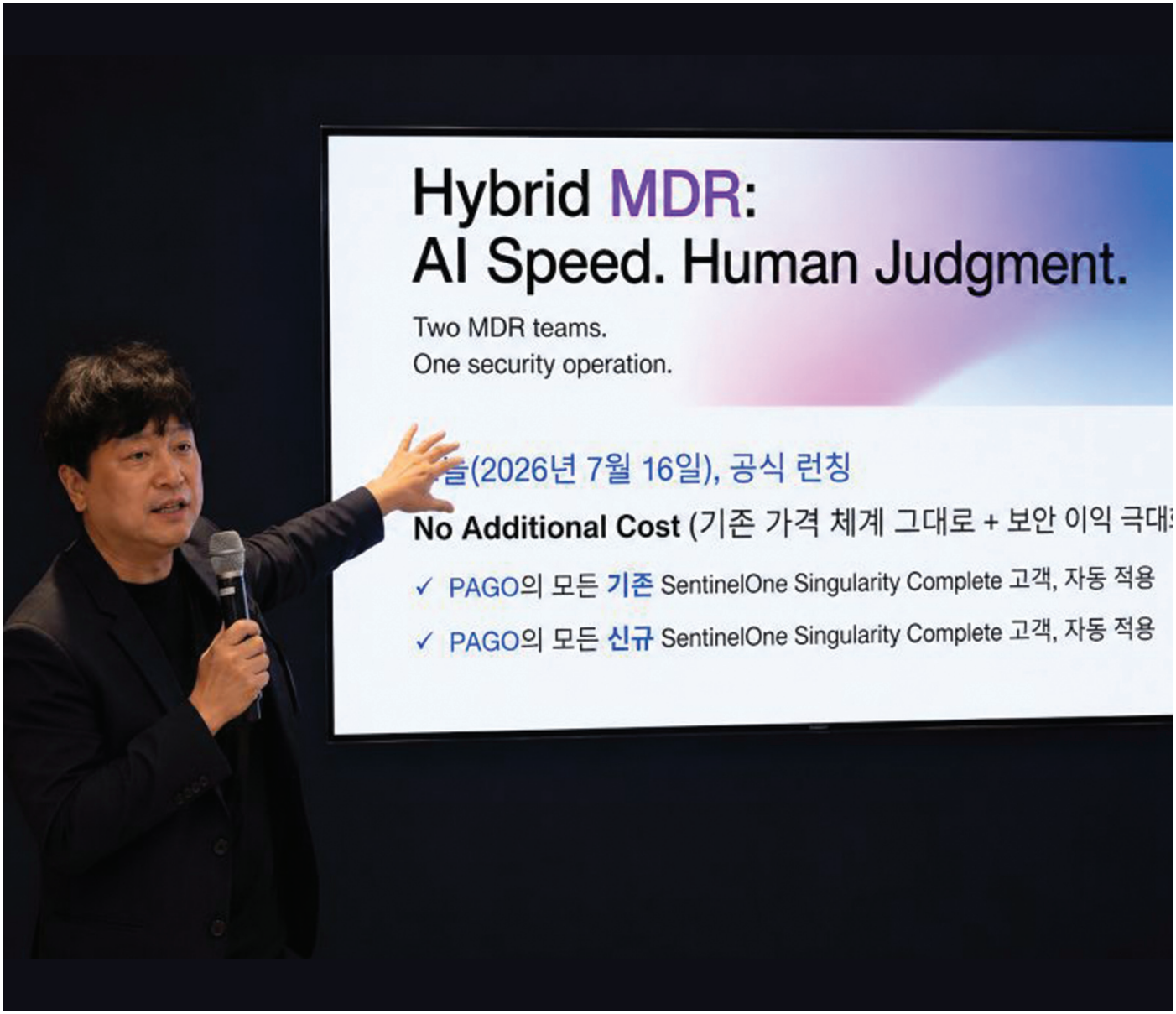
DeepACT 같은 플랫폼과 그 안의 AI 기능들은 프리크라임의 인터페이스에 해당합니다. 이 인터페이스 뒤에서 실제로 판단 능력을 만들어내는 애거사 역할은 파고네트웍스에서 누가 담당하고 있을까요?



■ 처음 겪는 사람이 있어야 한다

AI는 과거 데이터를 학습해서 패턴을 찾아냅니다. 이 패턴이라는 건 누군가 이미 한 번은 겪었던 일이라는 뜻이기도 합니다. 매뉴얼에 없는 신종 공격, 지금까지 본 적 없는 침투 방식은 정의상 학습할 데이터가 존재하지 않습니다. 이걸 처음 마주치는 순간, AI가 내놓은 답을 곧이 곧대로 믿어서는 안됩니다. 바로 이 때 할루시네이션이 발생할 가능성이 높더근요. 그래서 사람이 필요합니다. 사람의 경험이 기록되고 축적된 뒤에야, 다음번엔 AI가 그 패턴을 학습해서 더 빠르게 처리할 수 있게 됩니다.

앞서 짚은 선을 긋는 역량도 마찬가지입니다. 프롬프트는 안 보고 권한 이동은 본다는 지금의 기준은 완성된 정답이 아니라, 수많은 애매한 사례를 실제로 겪으면서 다듬어온 결과라는 이름의, 파고만의 고유한 역량입니다. AI가 잘하는 일의 재료는 결국 사람이 먼저 겪어낸 최초의 경험입니다. 이 경험을 얼마나 많이, 얼마나 먼저 쌓아왔는가가 그 조직의 판단 능력, 애거사의 재능에 해당하는 부분이지 않을까요?



이미지 출처: GTT Korea, AI 공격 시대, 센티넬원·파고네트웍스 '하이브리드 MDR' 출시...글로벌 위협 헌팅과 24시간 대응 결합

■ 역량을 글로벌하게 인정받다

인터뷰에서 권 대표는 SentinelOne 같은 글로벌 벤더와 파고가 동등한 지위에서 하이브리드 MDR을 운영하게 된 과정을 자세히 설명했습니다. 처음엔 파고가 벤더의 기술을 잘 다루는 서비스 기업 정도로 여겨졌지만, 지금은 벤더 본사가 파고를 자신들과 같은 레벨의 MDR 팀으로 인정하고 공식 파트너십을 맺었다고 언급했는데요.

여기서 말하는 하이브리드는 자동차의 하이브리드 엔진과 같은 맥락입니다. 엔진과 전기 모터가 결합돼 저속으로 달릴 때에는 연비 절약을 위해 모터를, 전기가 떨어지면 충전 + 자동차를 굴러가게 하기 위해 엔진이 작동하죠. 그리고 순간적으로 폭발적인 힘이 필요할 때에는 전기 모터와 엔진이 함께 작동합니다. 이게 하이브리드 엔진의 핵심이고, SentinelOne + 파고네트웍스의 하이브이드 MDR도 마찬가지입니다. 마치 두개의 심장을 가진 차를 운전하듯, 고객은 24/7로 두 회사의 MDR 역량을 오롯이 누릴 수 있게 되니까요.

이 지위는 결국 파고가 오랜 시간 실제 위협을 가장 먼저 맞닥뜨려온 조직이었다는 것을 검증받았다는 것으로 이해할 수 있습니다. SentinelOne같은 벤더가 가진 건 잘 만들어진 EDR 과 같은 탐지 및 대응 도구입니다. 파고가 가진 역량은 그 도구를 실전에서 수년간 써오면서, 도구가 놓친 부분과 새로 나타난 위협을 가장 먼저 겪어본 경험이죠. 벤더가 파고를 동등하게 대우하기 시작했다는 건, 이 경험치를 도구 자체만큼 가치 있게 보기 시작했다는 뜻입니다. 인터페이스는 벤더가 만들었지만, 그 인터페이스를 실제로 채워온 애거사는 파고 쪽에 있었다는 것을 벤더에서 인정한 것이라고 할 수 있습니다.

결론: AI 시대, 여전히 시스템이 아니라 사람이 중요한 이유

■ 프리크라임은 사라지고 애거사는 남았다

영화의 결말에서 프리크라임은 폐지됩니다. 완벽하다고 믿었던 예측 시스템이 사실은 조작될 수 있었고, 소수 의견을 지운 대가로 무고한 사람을 가둘 뻔했다는 게 드러났기 때문입니다. 시스템이 사라진 자리에 남은 건 애거사를 비롯한 예지자들, 판단력을 실제로 갖고 있던 사람들입니다. 화려한 인터페이스는 사라졌지만, 그 인터페이스가 의존했던 진짜 재능은 남았습니다. 바로, 사람의 능력입니다.

총 3부에 걸쳐 계속 언급했던 것도 이 사람의 능력이 여전히 중요하다는 것입니다. 앞서 조찬 세션과 세미나에서 우리는 AI가 True Positive 판정과 함께 반대 근거를 동시에 내놓는다는 걸 봤고, 이번 CEO 인터뷰에서는 프롬프트는 안 보고 권한 이동은 본다는 선을 사람이 직접 그어뒀다는 걸 확인했습니다.

하나의 사건을 두고 AI 스스로 서로 다른 결론을 내놓는 것, 그리고 어디까지 봐도 되고 어디부터는 안 되는지가 딱 떨어지지 않는 것, 둘 다 AI가 아직 미숙해서 생기는 현상이 아닙니다. 프리크라임의 세 예지자가 어긋난 것도 시스템의 결함이 아니라, 판단이라는 행위 자체에 원래 여러 갈래가 있다는 증거였습니다. AI가 아무리 정교해져도 이 갈래를 하나로 확정하는 마지막 선은 매번 사람이 그어야 합니다.



“AI가 아무리 정교해져도 이 갈래를 하나로 확정하는 마지막 선은 매번 사람이 그어야 합니다.

Top 250 MSSP 2025
By MSSP Alert

GPTW for Woman
By Great Place to Work

MSSP Partner of the Year 2025 & 2026
SentinelOne

MSSP Partner of the Year 2025
Stellar Cyber

Top MSSP in APAC 2024
By Enterprise Security

■ 그 선을 가장 많이 그어본 기업, 파고네트웍스

이 선을 긋는 역량은 하루아침에 생기지 않습니다. 처음 보는 위협을 가장 먼저 맞닥뜨리고, 그 판단이 맞았는지 틀렸는지를 실전에서 몇 번이고 검증해본 조직만이 이 역량을 쌓습니다. 파고네트웍스가 SentinelOne, Stellar Cyber 같은 글로벌 벤더와 동등한 지위를 인정받게 된 것도 이 축적된 판단 경험 때문입니다.

이 인터뷰를 준비하며 던지고 싶었던 질문, “AI가 파고의 노하우까지 흡수하면 그때 파고의 경쟁력은 무엇이냐”는 질문에 대한 답도 여기 있습니다. AI가 흡수할 수 있는 건 이미 벌어진 사건에 대한 기록뿐입니다. 아직 벌어지지 않은 사건을 가장 먼저 마주치고 판단해낸 경험은 매번 새로 쌓입니다. 그러니 AI가 발달할수록 그 경험을 가장 오래 쌓아온 조직과 나머지 조직 사이의 격차가 오히려 벌어지게 되지 않을까요? 이게 글로벌 보안 리더들이 파고네트웍스를 동등하게 바라보고, LG U+가 파고네트웍스를 인수한 진짜 이유이지 않을까 감히 예상해 봅니다.

이번 칼럼에서 미처 다루지 못한, 보다 자세한 인터뷰 내용은 아래의 영상에서 확인해 보시기 바랍니다.

AI는 사람의 판단을 도와주는 존재일 뿐, 사람 대신 판단해 주지 않습니다. 물론 기술이 점점 발전해서 그 순간이 정말 다가올 지도



Available on: https://youtu.be/TY43w4RB6ZY

모르겠습니다. 다만 인류가 존속하기 위해서는 그 선을 넘지 않기를 바랄 뿐입니다. 다행히 업계는 그런 방향으로 흘러가고 있는 것 같네요.

SOC의 미래에는 여전히 사람이 있습니다. 그리고 그 사람의 역량을 강화시켜 나가야 한다는 것이 Augmented SOC with Agentic AI, AI와 함께 증강된 SOC이고, AI는 SOC를 대체하는 것이 아닌, 사람의 역량을 증강시키는 존재로 활용돼야 한다는 것을 기억합시다.

PAGO Security Summit 2027을 기약하며, 칼럼 3부를 마무리합니다. 이번 칼럼을 통해 미래의 SOC 발전 방향과 AI 시대에서 우리의 역할은 무엇인지 잠시나마 생각해볼 수 있는 시간이 되었다면 더할 나위 없이 기쁘겠습니다. 끝!

일반 문의 사항은 영업팀에 문의하세요.
- 데모 / POC / 계약 / 파트너
- 프리미엄 위협 청소 서비스
- 사고 대응 서비스

서울특별시 용산구 회나무로 65 (04344)
080-077-5171
sales@pagonetworks.com
www.pagonetworks.com

pago

무료 보안 위협 탐지 및 대응 서비스

네트워크에서 이상 징후를 감지하셨나요?

PAGO 분석가가 조사하고, 차단하고, 정리합니다. 무료로.

랜섬웨어 피해, 침입 징후, 점검 후에도 남은 악성코드.
PAGO의 24/7 MDR 팀이 최대 3개월간 탐지, 대응, 복구를 맡습니다. 기존 보안 환경은 그대로 유지합니다.

탐지 — 대응 — 복구

DeepACT
PAGO의 MDR 플랫폼, 분석가가 직접 운영

SentinelOne
엔드포인트 탐지 및 대응

Stellar Cyber
네트워크 탐지 및 Open XDR

StealthMole
다크웹 및 유출 계정 인텔리전스

신청 대상

랜섬웨어 피해 기업
랜섬웨어 공격을 받은 기업

보안 사고 의심 기업
공격으로 의심되는 징후가 보이는 기업

악성코드 제거 필요 기업
점검 후에도 제거해야 할 악성코드가 남아 있는 기업

진행 방법

1. **온라인 신청.** 회사 이메일로 현재 겪고 있는 문제를 작성해 주세요.
2. **PAGO 전문가 연락.** 담당 전문가가 연락드려 사례 대응을 시작합니다.
3. **기존 환경 그대로.** 기존 보안 인프라는 변경하지 않습니다.

지금 무료 서비스를 신청하세요

문의: 영업팀
080-077-5171
sales@pagonetworks.com



www.pagonetworks.com

© 2026 PAGO Networks. All rights reserved.