

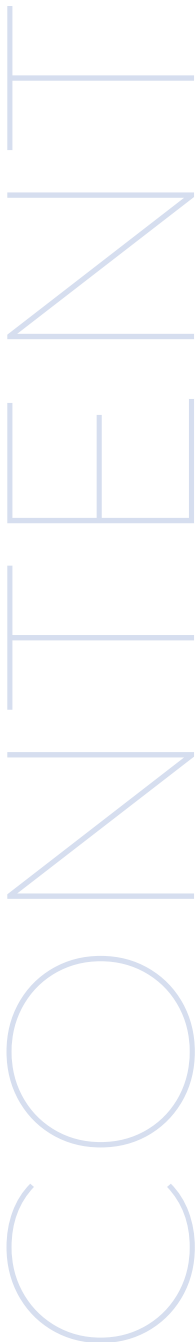
DEFINING THE FRONTLINE

파고네트웍스 · 웨어드IT 장두환 공동 집필

PAGO Security Summit Insight Report

2025

목차



I. 침해보다 앞선 보안: 대응이 아닌 출발점으로서의 MDR 재정의

1. MDR이 대체 뭐길래?
2. 기존 보안 체계의 한계
3. 파고의 MDR이 차별화된 특징은?
4. 파고 MDR로 기업은 어떤 효과를 얻을 수 있을까?
5. 보안의 기준은 기술이 아니라 책임이다

II. 현장에서 증명된 방어력: 실제 위협을 막는 것은 무엇인가

1. AI는 보안팀을 대체할 수 있을까? SentinelOne 세션 요약
2. SIEM은 왜 실패했는가? Stellar Cyber 세션 요약
3. 위협은 내부가 아닌, 외부에서 먼저 감지된다 StealthMole 세션 요약
4. 탐지에서 억제까지 - 파고 기술팀이 말하는 실전 운영 전략

III. 변화하는 전선: 파고가 제시하는 새로운 보안 프론트라인

1. 보안 사고는 구조의 실패에서 시작된다
2. 위협은 알려지기 전에 막아야 - 파고의 프론트라인 전략
3. 기술보다 중요한 것은 사람의 판단과 책임감
4. 하나의 사고를 모두의 보안으로 바꾸는 조직 - 파고네트웍스

결론



INTRODUCTION

”

**이 정도면 막았다고
생각했는데, 왜 뚫렸
을까요?**

사이버 공격이 발생하면 기업 내부에서 가장 먼저 나오는 말입니다. EDR도 설치했고, 외부 모의 해킹도 받았고, 침입 탐지 시스템도 나름 괜찮은 걸 도입했는데, 막상 사고가 터지고 나면 대부분의 기업은 '왜 이런 일이 벌어졌는지'조차 설명하지 못합니다.

현장에선 이런 현실을 자주 마주합니다.

“우린 탐지를 했지만, 대응하지 못했다.”
“우린 로그는 모았지만, 이상 징후는 못 봤다.”
“사고인지 몰랐다. 보고를 받기 전까진...”

I. 침해보다 앞선 보안: 대응이 아닌 출발점으로서의 MDR 재정의

지금의 보안 환경은 이미 '탐지' 중심에서 '대응' 중심으로 무게추가 옮겨지고 있습니다. 예방이 완벽할 수 없다면, 침입 이후라도 얼마나 빨리 대응하느냐가 피해를 결정짓습니다. 그리고 바로 이 지점에서 등장한 개념이 MDR(Managed Detection and Response)입니다. MDR은 단순한, 특정 보안 솔루션 이름이 아닙니다. 하루 24시간, 주 7일 내내 기업 대신 위협을 감지하고, 판단하고, 막는 행위 그 자체라고 할 수 있죠. 그리고 그 역할을 가장 강하게 주장하는 회사가 있습니다. 바로 파고네트웍스(PAGO Networks)입니다.

이제, 보안은 장비가 아니라 사람이 지키는 시대입니다. 그렇다면, 파고가 말하는 MDR은 기존과 무엇이 다를까요? 왜 기업들은 지금 MDR을 고민해야 할까요? 저는 지난 4월 23일(수) 오전 7시부터 오후 5시 30분까지, 10시간 넘게 인터컨티넨탈 서울 파르나스에 머무르며 파고가 주최한 조찬 세미나, 기자 간담회, 그리고 PAGO Security Summit 2025에 참석했습니다. 이날 제가 듣고 체험하고 습득한 정보들을 토대로, MDR이란 무엇이며 왜 필요한지, 사이버 보안 환경을 위해 파고가 어떻게 기여할 수 있는지 총 3개의 글을 통해 자세히 알아보겠습니다.

웨어드IT 장두환

1. MDR이 대체 뭐길래?

“우리는 MSS, 보안 관제 서비스 사용하고 있는데, MDR이 꼭 필요할까요?”

이 질문은 보안 담당자들이 MDR(Managed Detection and Response)을 접할 때 가장 먼저 떠올리는 의문입니다. 겉으로 보기엔 비슷해 보이지만, MDR은 기존 관제 서비스(MSS)와 근본적으로 다른데요. 한마디로 말하면, MSS가 '경고를 알려주는 체계'라면 MDR은 '직접 싸우는 체계'입니다. 먼저, MSS와 MDR의 차이를 간단히 표로 살펴봅시다.

항목	MSS (Managed Security Service)	MDR (Managed Detection & Response)
중점 영역	이벤트 모니터링 및 알림	위협 탐지 + 능동적 대응
대응 방식	이상 징후 발생 시 고객에게 알림 → 고객이 대응	위협 감지 시 즉시 분석 및 선조치 가능
탐지 방식	룰 기반 / 시그니처 매칭	AI 분석 + 위협 헌팅 중심
분석 깊이	이벤트 중심 단편적 분석	행위 기반 분석 + 정황 종합 판단
운영 시간	주간 8×5 운영이 일반적	연중무휴 24×7×365 운영
인력 구성	모니터링 위주	실전 대응 가능한 분석 전문가 팀

지금부터 이야기 할 MSS와 MDR의 차이가 뭔지 감이 오시나요? 아직 잘 모르겠다는 분들을 위해 사례를 하나 들어볼게요. 금요일 밤 11시, 한 제조 기업의 시스템에서 이상 징후가 발생합니다. 이때 MSS에서는 어떤 일이 벌어질까요? 먼저 경고 알림이 담당자에게 전송됩니다. 하지만 이 경고에 대한 조치는 담당자가 출근할 때까지 미뤄질 가능성이 크죠. 그 사이 공격자는 내부 시스템을 정찰하고, 데이터를 암호화하며 치명적인 피해를 남깁니다. 만약 MDR 서비스를 받고 있다면? MDR 팀은 실시간으로 이상 징후를 분석합니다.

이미 승인된 권한 범위 내에서 해당 계정을 격리하고, 의심 IP를 차단하죠. 그리고 아침에 고객에게 보고가 올라갑니다. 피해는 '0'에 가깝고, 위험은 사전에 봉쇄됐습니다. 이 차이의 본질은 '책임의 범위'입니다. MSS는 고객에게 정보를 '전달'하는 데 그칩니다. 하지만 MDR은 정보를 '이해'하고, 즉시 대응하며, 결과를 책임지는 보안 파트너입니다. 특히 파고는 MDR의 운영 방침을 "사고가 나면 대응하는 게 아니라, 사고가 안 나게 미리 개입하는 것"이라고 정의합니다. 그렇다면 MSS와 같은 기존 보안 체계는 왜 이 역할을 해내지 못하는 것일까요?

2. 기존 보안 체계의 한계

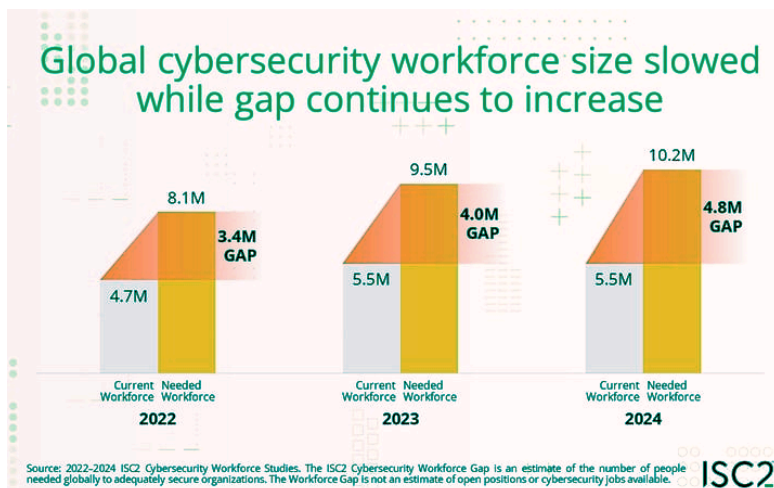
“ EDR도 있고, SIEM도 도입했는데 왜 또 사고가 나죠? ”

많은 기업들이 이 질문 앞에서 멈춰섭니다. 수억 원을 들여 보안 솔루션을 갖췄는데, 정작 사고는 금요일 밤이나 주말 새벽처럼 가장 대비가 취약한 순간에 터진단 말이죠. 그래서 보안 담당자는 "대체 그 많은 보안 예산을 들었는데 왜 사고가 나는 거냐"며 경영진에게 질책을 당하기 일쑤입니다. 그런데 보안 담당자도 답답합니다. 사실 보안 담당자도 할 말이 많거든요. 문제는 기술이 아니라, '운영'의 한계입니다. 그럼, 어떤 한계점들이 있는 걸까요?

① 보안 인력 부족

ISC2 (International Information System Security Certification Consortium)의 보고서, 2024 Cybersecurity Workforce Study에 따르면, 2024년 기준 전 세계 사이버 보안 인력 부족 규모는 약 480만 명이라고 합니다.

전 세계적으로 약 480만 명의 사이버 보안 인력이 부족하다는 것인데, 특히 한국에서는 몇몇 대기업 혹은 빅테크 기업이 아니라면 숙련된 분석가(레드팀, 블루팀급)를 확보하는 것은 매우 어렵습니다. 게다가 중소기업은 물론이고, 대기업조차 24시간 대응팀 구성은 인건비와 교대근무 문제로 운영하기 어려운 것이 현실이죠.



<이미지 출처 : ISC2, Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen>

② 보안 기술의 복잡성과 정보 단절 문제

EDR, NDR, SIEM, XDR. 이런 최신 보안 솔루션들은 각각은 훌륭한 역할을 수행하고 있습니다. 하지만 서로 다른 UI, 룰셋, 경고 체계로 인해 통합이 어렵고 이로 인해 '보안 사일로'가 생깁니다.

예를 들어, 네트워크에서 수상한 접속이 있었는데, 그 계정이 어떤 엔드포인트에서 어떤 행위를 했는지 파악하려면 별도의 콘솔을 열고, 로그를 추적하고, 연결을 수작업으로 해야 합니다.

이 과정에서 제 때에 대처해야만 하는 골든타임을 놓치게 되고, 공격자는 더 깊이 침투하게 되는거죠.

차단한 위협 중 47%가 업무시간 외에 발생했습니다.

③ AI도 완벽하지 않다

많은 기업들이 “AI로 탐지하면 되지 않나?”라고 묻습니다. 맞는 말입니다. 하지만 AI도 패턴에 근거한 확률적 판단을 내릴 뿐, 의심스러운 정상행위(예: 탈취된 계정의 이상 사용)까지 구분하긴 어렵습니다.

게다가 AI가 감지해도, 그 위협이 진짜인지 판단하고 조치하는 건 여전히 ‘사람의 역할’입니다. AI가 완벽하다 한들, 사람은 그렇지 못하기 때문에 최후의 보루는 여전히 사람의 영역이라는 거죠.

④ SOC 24/7 운영의 현실적인 어려움

사이버 공격은 사람처럼 낮에만 활동하지 않습니다. 랜섬웨어 공격은 금요일 밤, 휴일 새벽 같은 보안 인프라가 가장 느슨해진 시간을 노립니다. 일부러요. 실제로 파고의 데이터에 따르면, 차단한 위협 중 47%가 업무시간 외에 발생했습니다.

하지만 현실적으로 대부분의 기업은 SoC (Security Operations Center)의 24시간 운영 체계를 구축하지 못합니다. 이 때문에 대부분의 이상행위는 새벽에 감지되더라도, 월요일 오전까지 방치된 채로 확산되곤 하죠.

결국, 기업들이 겪는 보안 사고의 상당수는 기술이 부족해서가 아니라, 그 기술을 제대로 다룰 사람과 구조가 없기 때문입니다. 이제 필요한 것은 ‘도구’가 아니라 그 도구를 실제로 사용해 줄 파트너, 그리고 침입 시 대응까지 책임지는 체계가 돼야 합니다. 그렇다면 파고는 이 공백을 어떻게 채우고 있을까요? 이어서, 좀 더 구체적으로 살펴보겠습니다.



3. 파고 MDR 서비스의 특징

많은 보안 서비스 기업들이 MDR을 표방합니다. 하지만 “탐지하고 알려주는 것”과 “직접 막아주는 것” 사이엔 큰 간극이 있죠. 파고는 이 간극을 메우는 것을 목표로 합니다. 좀 더 구체적으로 살펴볼까요?

① 선제적 대응 원칙: 귀사의 보안 프론트라인

파고는 단순한 보안 관제 서비스를 제공하지 않습니다. 그들은 사고가 발생하면 보고하는 게 아니라, 발생하지 않도록 개입하는 것을 철칙으로 삼았는데요. 그래서 이들이 내건 슬로건은 단순하지만 강력합니다.

“Your Frontline Against Cyber Threats” (당신을 대신해 사이버 위협의 최전선에 선다) 이는 마케팅 문구가 아니라 실제 파고 MDR 서비스 모델을 한 문장으로 요약한 것으로 볼 수 있습니다. 요약입니다.

② 글로벌 확장과 실제 고객 대응 사례

2017년 설립 이후, 파고는 국내를 넘어 동남아시아 지역(싱가포르, 베트남, 필리핀, 말레이시아, 인도네시아, 태국, 라오스)까지 서비스 지역을 확장했습니다.

일부 국가는 OEM 기반의 MDR 센터를 구축해 현지 고객을 직접 대응하고 있으며, 2025년 하반기에는 미국 미주 지역에도 센터 오픈을 준비 중이라고 합니다.

현재 파고는 약 350여 고객사, 하루 평균 약 20만 건의 보안 이벤트를 실시간 분석하고 있습니다.

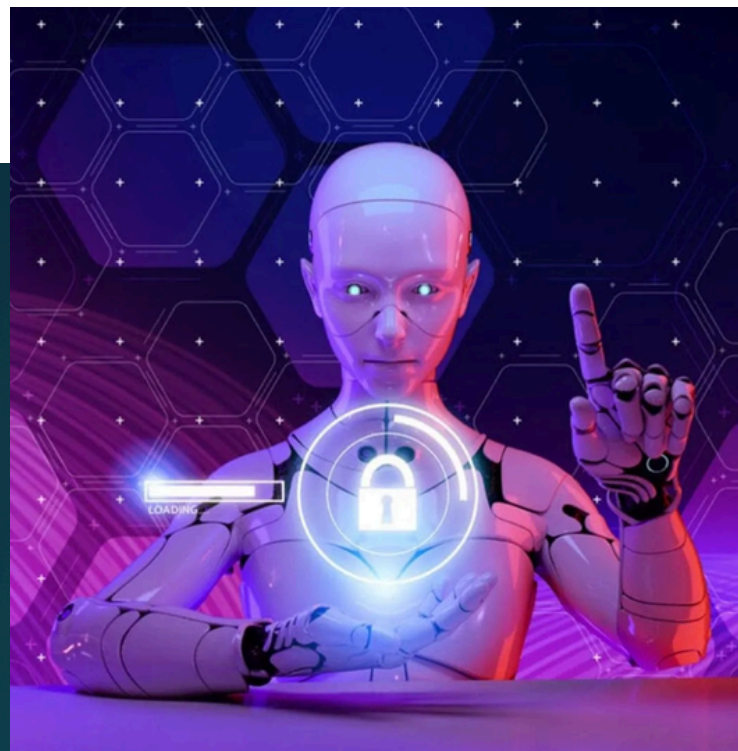
③ 파고 MDR의 운영 방식

파고는 고객사를 위한 ‘가상 SOC(Security Operations Center)’를 구성합니다. 주요 특징을 간단히 요약하면,

- 멀티테넌시 기반 대응 체계: 고객별 정책과 환경을 분리 관리
- 자동화된 탐지 룰 + 수작업 헌팅 결합: 기술과 사람의 조화
- 실시간 위협 판단 및 선조치 권한 운영: 승인 기다리지 않고 빠르게 격리 및 차단
- 사고 이후 재발 방지를 위한 룰 리디자인 및 지속 포렌식

위와 같은 특징을 기반으로 파고 MDR의 가장 큰 차별점을 한 문장으로 표현하면 “사고가 터져야 대응하는 보안팀”이 아닌, 사고가 안 났더라도 움직이는 보안팀”이라고 요약할 수 있겠습니다. 이런 철저한 실전 중심 운영 방식은, MDR을 단순한 ‘외주 서비스’가 아니라 특정 기업을 위한 보안 파트너로 진화시킨 사례라고 볼 수 있지 않을까요?

이제 MDR이 어떤 서비스인지 조금은 감을 잡으셨을 것 같은데요. 그런데 사실 MDR 서비스를 제공하는 기업은 많습니다. 파고만 MDR을 하는 게 아니거든요. 그럼, 이 MDR이라는 개념을 파고는 어떻게 제공하고 있을까요? 그리고 파고의 방식이 실제 위협 상황에서 다른 기업의 MDR과 어떤 차이를 만들어내는지 좀 더 자세히 알아보시다.

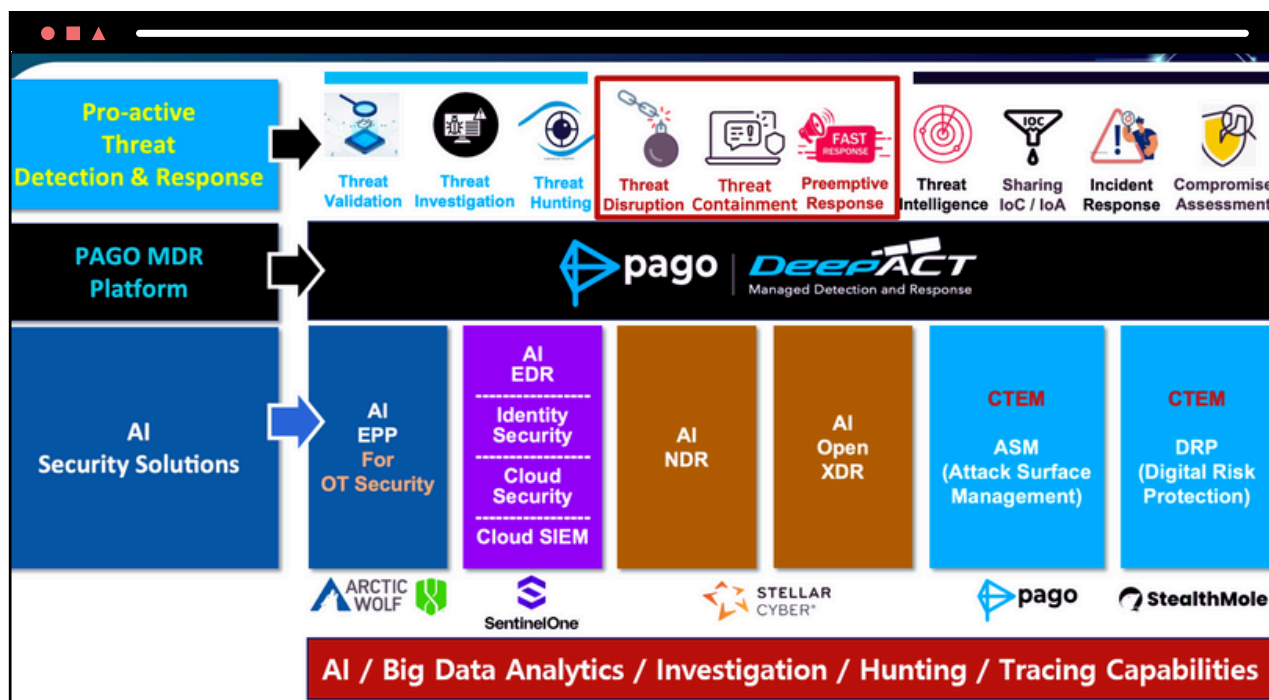


4. 파고의 MDR이 차별화된 특징은?

많은 보안 업체들이 MDR을 이야기합니다. 하지만 위협을 감지한 순간, 누가 움직이고 어디까지 개입하느냐에 따라 그 서비스의 본질은 완전히 달라집니다. 파고는 이 질문에 대한 답을 “우리가 직접 막는다”라는 한 문장으로 명쾌하게 정리합니다. 좀 더 구체적으로 알아보기 위해 새벽 3시에 이상 행위가 발생했다고 해봅시다.

단계	일반적인 MDR	파고 MDR
탐지	알림 감지됨	알림 감지됨
대응	이메일/전화로 고객 통보 후 대기	파고 분석팀 즉시 분석 착수
분석	고객사 출근 후 대응 시작 (6~8시간 지연)	선조치: 계정 격리, 의심 IP 차단
결과	랜섬웨어 확산, 업무 중단	확산 전 차단, 사고 없음

이 차이를 만들어내는 건 속도이자 결단이고, 그 중심에는 ‘위임된 권한’과 ‘현장 판단’이 있습니다. 단순히 위협을 감지하는 것을 넘어, 그 위험이 더 퍼지지 않도록 격리, 억제시키고, 고객의 자산을 보호하기 위해 고객으로부터 안전하게 위임받은 권한을 직접 행사에 필요한 조치까지 취하는 것이 파고 MDR의 차별점입니다. 그런데, 잘 안와닿죠? 좀 더 자세히 살펴봅시다.



① 위협 탐지를 넘어 차단까지

파고는 위협 탐지 → 봉쇄(Containment, 확산 차단) → 중단(Disruption, 공격 차단) → 포렌식 및 롤 재설계까지

모든 단계의 대응 체계를 내부화하고 있습니다. 즉, 단순한 알림형 서비스가 아니라, 공격자의 침투 방식과 확산 경로를 파악해 다른 고객에게도 발생할 수 있는 위협을 미리 막는 구조를 갖추고 있다는 건데요. 이를 위해 파고는 '사고가 안 났더라도 헌팅은 계속된다'는 원칙 아래 정상 로그 안에서도 이상 징후를 찾는 Live Threat Hunting 체계를 운영합니다

③ 멀티 테넌시 기반, 동시에 350개 고객의 '내부 보안팀'처럼

파고가 350여 고객사의 시스템을 동시에 보호하면서도 각 고객사의 정책, 자산, 위협 히스토리에 맞춘 '맞춤형 보안 운영'을 가능하게 하는 핵심은 바로 멀티 테넌시 기반 MDR 아키텍처입니다. 이에 대한 내용은 두 번째 글에서 좀 더 자세히 다룰거고요. 아무튼, 고객별 룰셋 분리, 위협 전파는 실시간 공유, 사고 패턴은 전사적으로 학습 및 반영으로 이어지는 이 구조는 파고가 규모의 효율성과 개별 대응의 정밀성을 동시에 가져갈 수 있는 이유입니다.



② IOC는 사고가 없어도 만들어져야

보통 IOC(Indicator of Compromise)는 사고 발생 이후 만들어집니다. 하지만 파고는 "사고가 없더라도 IOC는 사전에 정의돼 있어야 한다"는 원칙을 갖고 있는데요. 이 말은 곧, "우리는 위협을 인지한 뒤 대응하는 것이 아니라, 위협이 있을 수 있다고 가정하고 먼저 막는다"는 의미입니다. 이 선제적(Proactive) 사고방식은 파고가 프론트라인으로 기능할 수 있는 핵심 역량입니다.

그리고 이러한 구조가 반영되어 다수의 고객들에게서 수집되는 정보는 모두 파고에서 자체 개발한 MDR 플랫폼, DeepACT로 모입니다. 이 중앙화된 플랫폼에서 파고 직원들이 각각의 개별적인 고객의 위험 상황을 분석하고 대처할 수 있게 되는 것으로 보시면 되겠습니다.



“글로벌 해킹 대회인 SentinelOne Poseidon CTF 에서 파고 팀은 세계 40개국 참가자 중 TOP 10에 랭크, 일부 참가자는 단 2점 차이로 우승을 놓쳤을 정도의 실력을 보였습니다.”



S1 ThreatOps (POSEIDON-PAGO)

+ Create - Game Management - Tools & Upgrades - Backup/Restore - Configuration - Scoreboard - admin

Team	Flags	Score
1 God's Warriors 56 Since Score	4	20
2 iteawon freedom 4 Since Score	3	15
3 What Can We Do 2 Since Score	2	10
4 Gobby	0	0
5 Hades	0	0

THREAT OPS
SENTINELONE THREATOPS CHALLENGE

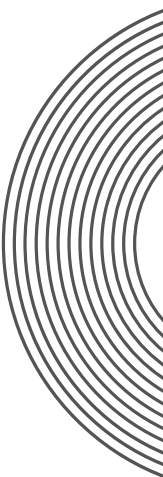
④ 실전 기반의 대응 조직

파고의 MDR 서비스는 '실전에서 사고를 다뤄본 전문가'들이 대응하는 구조입니다. 전체 인력 중 60% 이상이 위협 분석 전문가이며, 이들은 단순 로그 분석을 넘어서 공격자의 시나리오와 의도를 꿰뚫는 위협 헌팅 능력을 갖췄습니다.

이러한 능력을 입증하기 위해, 파고는 [PAGO Security Summit 2025](#)에서 인상적인 내용을 발표했는데요. 글로벌 해킹 대회인 SentinelOne Poseidon CTF 에서 파고 팀은 세계 40개국 참가자 중 TOP 10에 랭크, 일부 참가자는 단 2점 차이로 우승을 놓쳤을 정도의 실력을 보였습니다.

따라서, 파고는 단순한 'MDR 서비스 제공 기업'이 아닙니다. 위협 앞에 먼저 움직이는 사람들, 사고가 나기 전에 판단을 내리는 책임자들, 그리고 고객 대신 침투를 막는 진짜 프론트라인이라고 할 수 있죠.

그렇다면 이런 파고의 방식이 실제로 기업에게 어떤 가치를 가져다줄까요? 이어서 그 내용을 살펴보겠습니다.



5. 보안의 기준은 기술이 아니라 책임이다

많은 기업들이 보안 강화를 위해 새로운 솔루션을 도입합니다. 하지만 진짜 중요한 건 기술 그 자체가 아니라, 그 기술을 어떻게 운영하고, 누가 책임지는가라는 것을 이제 잘 아셨으리라 생각되는데요. 사이버 보안은 이제 “얼마나 잘 탐지하느냐”보다 “얼마나 빠르게, 그리고 확실하게 대응하느냐”가 관건입니다. 그리고 이 대응의 무게를 대신 짊어지는 이들이 바로 파고입니다.

MDR

in the Era of Generative AI



기술이 아니라 '사람'이
만드는 보안

파고는 사고가 발생하면 움직이는 조직이 아니라, 사고가 나기 전에 먼저 움직이는 조직입니다. 위협 탐지 시스템이 알려주기도 전에, 로그가 이상하다고 판단되기 전에 → 파고는 고객의 입장에서, 현장에서, 먼저 움직입니다.

이것이 그들이 말하는 '프론트라인'입니다. 그리고 그 프론트라인에는 책임을 지는 사람이 있습니다. 결국, 보안에 있어 가장 중요한 것은 여전히 '사람'이니까요.



고객이 자는 사이, 대신
깨어 있는 사람들

위협은 낮과 밤을 가리지 않지만, 기업의 보안 체계는 그렇지 못합니다. 파고는 고객이 보지 못하는 시간에도 위협을 찾고, 판단하고, 조치하는 사람들로 구성된 조직, 단순히 '알려주는 사람'이 아니라 '직접 막는 사람'입니다.

앞서 자세히 설명했듯이, MDR은 단지 서비스의 이름이 아닙니다. 보안의 책임을 함께 지는 구조, 사고의 앞단에서 고객을 대신해 움직이는 철학입니다. 그리고 이 철학을 단순한 말이 아니라, 실제로 구현하고 있는 국내 대표 기업이 바로 파고네트웍스입니다.



II. 현장에서 증명된 방어력: 실제 위협을 막는 것은 무엇인가

“말로만 ‘보안’이 아니라,
진짜 막아본 사람이 말하는
보안이 궁금하다면?”

그럼, 파고는 어떻게 이런 서비스를 제공할 수 있는 것일까요? 위협을 빠르게 탐지할 수 있는 솔루션을 직접 개발한 것일까요? 아니면 이미 상용화 된 솔루션을 가져다가 파고만의 노하우를 얹은 것일까요? 그래서 아래와 같은 궁금증이 생길 수 있습니다. “파고는 실제로 어떻게 사고를 막고 있는 거지?”

지난 4월 23일, 파고는 국내 주요 보안 담당자와 CISO들을 초청해 ‘PAGO Security Summit 2025’를 개최했습니다. 이 자리에서 파고는 실제 SoC 운영 현장에서 증명된 보안 전략을 소개했고, 함께 협력 중인 SentinelOne, Stellar Cyber, StealthMole 등 글로벌 파트너사들의 역할과 기술을 공유했는데요. 이번 글에서는 이 행사에서 공유된 세션들의 주요 내용을 정리하며 파고가 실전에서 어떻게 위협을 막고 있는지, 그리고 그 전략의 기반이 되는 파트너 생태계는 어떻게 구성되는지를 함께 살펴보겠습니다.

웨어드IT 장두환

1. AI는 보안팀을 대체할 수 있을까?

SentinelOne 세션 요약

”

AI가 SOC를 완전히 자동화할 수 있다면, 이제 보안팀은 필요 없는 시대가 오는 걸까요?

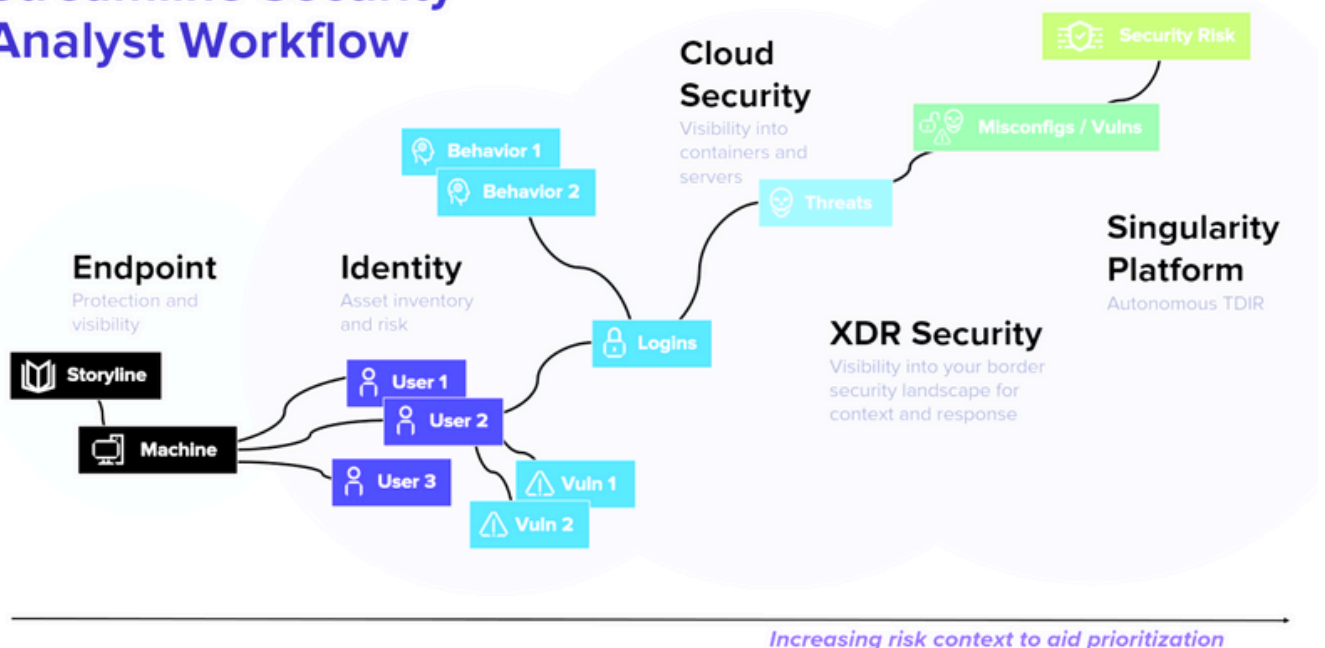
SentinelOne은 이 질문에 이렇게 답합니다. AI는 보안팀의 '팔'이자 '눈'은 될 수 있어도, '머리'가 되기엔 아직 멀었습니다.

■보안의 패러다임이 바뀌고 있다

예전에는 '알려진 위협'을 얼마나 잘 막는지가 중요했습니다. 하지만 이제는 알려지지 않은 위협을 얼마나 빨리 탐지하고 대응할 수 있는지가 보안의 경쟁력이 되었버렸죠. 글로벌 EDR 솔루션 시장을 Crowdstrike와 함께 양분하고 있는 SentinelOne은 이러한 변화의 한복판에서, AI 기반 행위 탐지 기술로 주목받기 시작한 기업이고요.

2010년부터 머신러닝을 기반으로 한 차세대 엔드포인트 보안 솔루션을 표방하며 시장에 진입했고, 현재는 엔드포인트, 아이덴티티, 클라우드까지 포괄하는 통합 보안 플랫폼으로 진화했습니다.

Streamline Security Analyst Workflow



■Purple AI: 보안 분석 방식을 바꾸는 대화형 AI

이번 서밋에서 소개된 SentinelOne Purple AI는 마치 LLM 처럼 자연어로 질의할 수 있는 보안 특화 AI로, 기존의 보안 분석 과정을 완전히 재정의합니다. Purple AI 덕분에

- 분석가는 더 이상 복잡한 쿼리를 입력할 필요 없습니다.
- 예를 들어, “지난 24시간 동안 가장 많이 공격받은 사용자 계정은?” 이라고 물어보면 → Purple AI는 그 결과를 즉시 제공합니다.

여기서 인상적인 것은 AI가 “다음에 뭘 물어볼 수 있을지”까지 제안한다는 점입니다. 만약 보안 담당자가 Purple AI에게

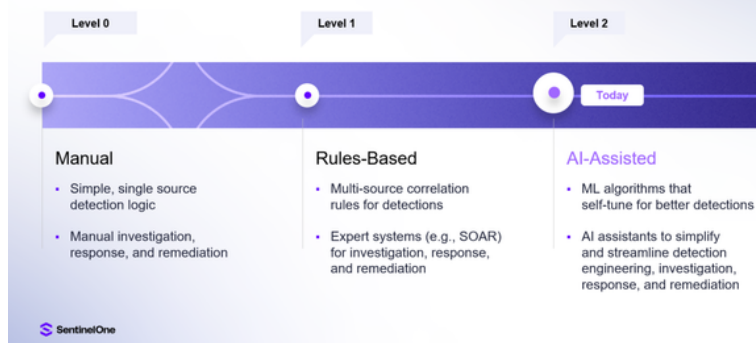
- “이 공격과 관련된 사용자 로그는?”
- “의심스러운 파일은 어떤 경로로 실행됐어?”

라고 물어볼 수 있다는 겁니다. 결국 Purple AI의 목표는 담당자가 더 깊이 있게 원인을 분석하고 빠르게 침투 경로를 찾아나갈 수 있도록 지원하는 것에 있다고 할 수 있습니다.

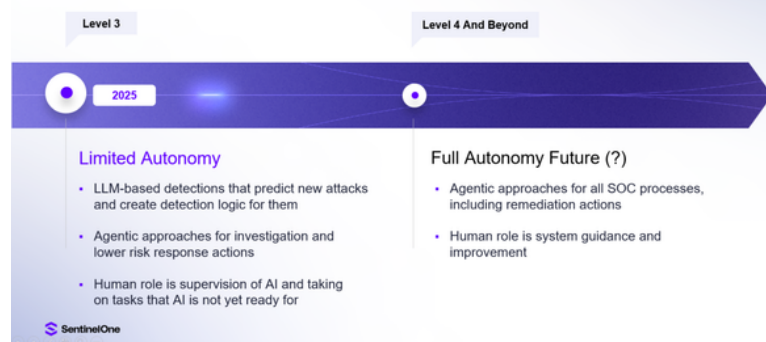
■AI는 파트너이지, 최종 판단자가 아님을 명심해야

SentinelOne은 “AI가 사람을 대체한다”는 관점을 경계합니다. Purple AI는 판단을 대신하지 않고, 판단을 돕는 보조 뇌 역할에 집중해야 한다는 거죠. 즉,

Automation Levels: SOC Maturity Model



Automation Levels: SecOps Maturity Model



- 위협 탐지 → AI가 제안
- 조치 여부 판단 → 여전히 분석가, 담당자의 몫으로 남겨둬

이 구조는 파고의 MDR 운영 철학과도 정확히 맞아떨어집니다. 사고가 나기 전에 먼저 움직이는 사람들, 그들의 결정을 더 빠르고 정확하게 만들어주는 AI, 그 조합이 바로 오늘날 MDR의 이상적인 구조인 셈이죠. 물론 AI가 어떻게 조치하라고 사람에게 알려주기도 하지만, 어쨌든 그 조치를 실제로 취해야 하는 것은 사람이니까요.

■파고 × SentinelOne: 기술과 실전의 결합

이날 기자 간담회에서 SentinelOne 김성래 지사장은 “SentinelOne의 기술과 파고 분석가의 실전 감각은 수년간 축적된 최고의 파트너십”이라고 말합니다. 즉, SentinelOne이 AI 기반 보안의 기술력을 제공하고, 파고는 이를 실전에 즉시 적용할 수 있는 사람 중심의 분석 역량을 더해서 MDR 서비스를 완성하는 거죠.

SentinelOne의 콘솔에서 탐지된 위협을, 글로벌 CTF 대회에서 실력을 입증한 파고의 전문가들이 실시간으로 해석하고 조치하는 구조. 이것이 바로 파고와 SentinelOne이 긴밀하게 협업하는 가장 근본적인 이유입니다. 아무리 기술이 뛰어나도, 그 가치를 실전에서 끌어내는 건 결국 사람의 역량입니다. 하지만 모든 기업이 그런 실전 전문가를 직접 고용하기란 쉽지 않죠. 그래서 이 파트너십이 중요합니다. 기업은 파고 MDR을 통해 마치 고급 위협 분석 전문가를 자체 보유한 것과 같은 수준의 대응력을 그대로 누릴 수 있기 때문입니다.

■데이터 프라이버시를 지키는 AI

AI가 강력해질수록, 그 윤리성과 프라이버시 기준도 중요해집니다. SentinelOne은 “우리는 고객 데이터를 공유하거나 학습용으로 전환하지 않는다.” 고 밝혔습니다. 즉,

- 데이터는 고객별로 분리
- AI는 고객 내에서만 작동

이 메시지는 AI 시대 보안 기술이 가져야 할 윤리 기준을 선제적으로 제시하는 사례라고 할 수 있고요. 앞으로 점점 더 중요하게 여겨질 부분이지 않을까 싶습니다. 기업들은 AI의 뛰어난 능력을 십분 활용하기만을 원할 뿐, 우리 데이터를 AI 제공 회사가 활용해서 이 노하우가 밖으로 새어 나가는 것은 극도로 경계할 테니까요.

Hyper Automation: The Engine driving the Automated Security Operations Centre with Pago



Automated Tasks

Hyperautomation enables automation. It also enhances SOC tasks. This reduces human error. It also optimizes efficiency.



AI-Driven Insights

AI provides better insights. It also allows faster threat detection. Automation improves incident response. This speeds up resolution.



Integrated Systems

Integration creates a cohesive defense. It enhances threat visibility. Orchestration improves coordination. All systems work together.

2. SIEM은 왜 실패했는가? Stellar Cyber 세션 요약

”

보안 로그는 많은데, 정작 위협은 못 막는 이유가 뭘까요?

Stellar Cyber는 이 질문으로 세션을 시작했습니다. 수많은 기업이 SIEM(Security Information and Event Management)을 도입했지만, 보안 담당자는 여전히 과로에 시달리고, 사고는 계속 터집니다. 무엇이 문제일까요?

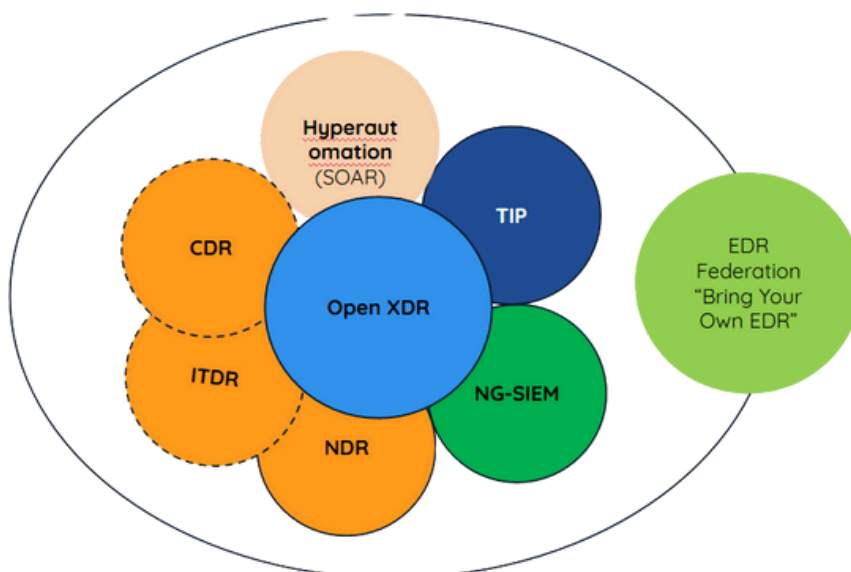
■XDR vs Open XDR

XDR(eXtended Detection and Response)은 여러 보안 도구(EDR, NDR 등)를 하나의 흐름으로 엮어 탐지와 대응의 정확도를 높이려는 전략입니다. 하지만 대부분의 XDR은 한 벤더 생태계 안에서만 작동하죠. Stellar Cyber는 여기에 문제의식을 가졌습니다.

우리는 처음부터 이걸 ‘보안 분석 플랫폼’이라 불렀습니다. 진짜 XDR은 모든 벤더의 데이터를 받아들이고, 상관 분석해서 실시간으로 위험을 판단할 수 있어야 하죠.

그래서 탄생한 개념이 Open XDR입니다.

Open XDR – An Open, End-to-End Unified SOC Platform

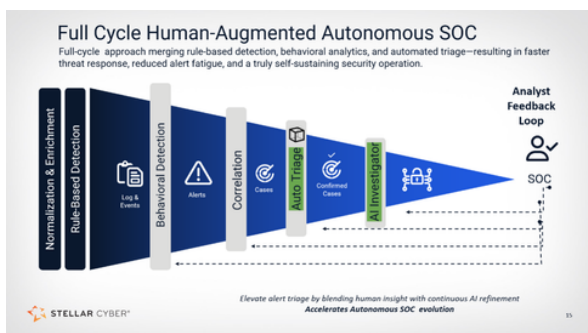


■ SIEM, EDR, XDR, Open XDR은 어떻게 다를까?

구분	SIEM	EDR	XDR	Open XDR
범위	로그 기반	단말 탐지	다중 보안 영역 연계	다양한 벤더 통합 지원
분석	이벤트 중심	단말 내부	연계 흐름 기반	데이터 간 상관관계 중심 분석
대응	수동 조사	단말 차단	자동 조치 일부	API 연동 통한 전사적 자동화
유연성	낮음	중간	중간	높음

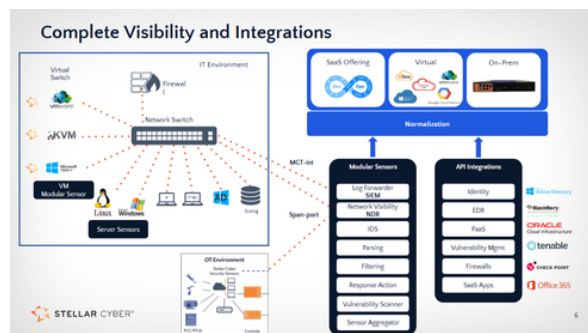
간단히 표로 요약해 봤는데요. Stellar Cyber가 지향하는 Open XDR은 극도로 고도화된 위협을 빠르게 탐지할 수 있도록 가능한 많은 데이터를 활용한다는 것에 방점을 찍고 있습니다. 그리고 이 과정에 AI가 개입하는데요. AI가 사람을 대체하는 것이 아닌, AI를 활용하고 AI에게 배워서 사람의 업무를 효율적으로 만들어 주는 것이 핵심입니다.

■ 보다 명확한 인과관계를 따지기 위한 Case 기반 위협 분석



Stellar Cyber의 핵심 기능 중 하나는 '케이스 (Case)' 기반 위협 분석입니다. 단편적인 이벤트가 아닌, 킬체인 단계별 타임라인으로 익스플로잇 → 확산 → 내부 정찰 → 통신 시도까지 → 공격의 전체 흐름을 시각화해서 원인을 명확하게 규명해낼 수 있다는 것인데요. 덕분에 보안 위협 분석가는 '이게 대체 뭐지?'를 반복하지 않고, '이게 왜 이런 흐름을 탔는지'를 직관적으로 이해할 수 있게 됩니다.

■ 네트워크 기반 탐지의 가치 - 보호되지 않는 자산에 대한 가시성



많은 기업은 전체 IT 자산의 30~40%가 Shadow IT 상태로 존재합니다. Shadow IT는 보안 에이전트가 설치되지 않은 장비들이라고 볼 수 있는데요. 입니다. 산업 기기나 IoT 기기, 의료기기, 프린터, BYOD 기기 등 이런 기기들을 탐지할 수 있는 방법은 네트워크 뿐입니다. 이 기기들의 네트워크 트래픽을 들여다볼 수 있어야 보안 홀이 생기지 않는다는 거죠. 애초에 Stellar Cyber는 NDR(Network Detection and Response)에서 출발했습니다. 그래서 이 영역에서의 높은 전문성을 바탕으로 Shadow IT에서 발현된 위협도 탐지해낼 수 있는 것입니다.

■통합 보안 플랫폼이 만들어내는 시너지

그래서 Stellar Cyber 플랫폼을 사용하면 뭐가 좋을까요? 간단히 특징을 네 가지로 정리해 봤습니다.

요소	설명
가시성 확대	다양한 보안 영역(클라우드, 엔드포인트, 네트워크) 통합 뷰 제공
컨텍스트 강화	이벤트 단편이 아닌, 위협 스토리 단위로 정보 구성
자동 대응	API 연동 통한 AD, 방화벽 등과의 자동화 연계
분석 효율화	분석가는 콘솔을 오가며 분석하지 않아도 됨

■파고 MDR과의 통합 운영 - 기술과 경험의 결합

파고의 MDR 분석가들은 Stellar Cyber의 Open XDR 플랫폼을 이렇게 활용합니다.

- SentinelOne의 단말 위협 정보
- Stellar Cyber의 네트워크 위협 흐름
 - 하나의 분석 시나리오로 통합
 - 위협 헌팅 속도 단축, 조치 결정 신속화

또한 Stellar Cyber는 멀티 테넌트 구조라서 테넌트 별로 사용자 계정을 관리하고, 접근 권한을 세분화 하여 운영자, 분석가, 감사자 등으로 분리해서 관리할 수 있고요. 특히 자동화된 워크플로우와 AI 기반 탐지 기능이 테넌트 간 독립적으로 작동하면서도 중앙에서는 상관분석과 통합 위협 인텔리전스를 구현할 수 있다는 것이 차별점입니다.

파고가 관리하는 350여개의 고객들은 서로 다른 인프라 환경에서 각기 다른 보안 정책을 운영하고 있죠. 그래서 Stellar Cyber의 멀티 테넌시 기능을 바탕으로 고객 별 맞춤형 탐지 룰을 세팅할 수 있음은 물론 운영 효율성을 위해 공통의 위협 탐지 룰도 적용할 수 있습니다. 그리고 이 모든 고객 테넌트들은 파고의 자체 플랫폼에서 실시간으로 모니터링됩니다.

요점	내용
위협 탐지 실패 이유	SIEM은 개별 이벤트는 수집하지만, 공격 흐름 간의 상관관계 분석이 어렵고 실시간 대응 불가
대안은?	Open XDR - 다양한 데이터 소스 연계, 상관 분석, 자동화
Stellar Cyber 가치	타임라인 기반 분석, 보호되지 않는 자산에 대한 탐지
파고와의 시너지	기술(플랫폼) + 사람(위협 헌팅)의 결합으로 MDR 성과 극대화

3. 위협은 내부가 아닌, 외부에서 먼저 감지된다 StealthMole 세션 요약

“당신의 기업 정보는 이미 다크 웹 어딘가에 떠돌고 있을지도 모릅니다.

스텔스몰(StealthMole)의 발표는 이 강렬한 메시지로 시작됩니다. 많은 보안 시스템이 조직 내부의 위협 감지에 집중하고 있지만, 공격자들은 이미 조직 바깥, 다크웹이라는 익명 공간에서 다음 침입을 준비하고 있다는 것인데요. 그래서 이런 위협을 ‘미리’, ‘밖에서’ 찾아내는 것이 바로 스텔스몰의 역할입니다. 어디서 찾을까요? 바로 딥웹과 다크웹입니다.

■딥웹과 다크웹의 차이, 그리고 보안 침해의 흐름

보안 위협은 종종 “어디서 유출됐는가?”를 이해하는 데서 출발합니다. 그런 의미에서 웹의 3가지 층위를 정확히 구분할 필요가 있겠는데요. 일반적으로 Google과 같은 검색 엔진에 검색되는 웹을 표면웹(Surface Web)이라고 부릅니다. 그럼 딥웹과 다크웹은 무엇일까요? 아래의 표를 보시죠.

구분	설명	접근 방법	보안 맥락
표면웹 (Surface Web)	검색엔진에 노출된 일반 웹사이트 (예: 뉴스, 쇼핑몰)	구글 등으로 접근 가능	대부분 공개 정보, 민감도 낮음
딥웹 (Deep Web)	인증 없이는 접근 불가능한 내부 정보 (인트라넷, DB, ERP 등)	로그인 필요, 검색 불가	대부분 보호받는 합법적 시스템 정보 해커의 주요 침입 대상
다크웹 (Dark Web)	Tor 등 특수 브라우저로 접근하는 익명화된 웹 공간	일반적인 브라우저로 접근 불가	딥웹에서 탈취한 정보가 유통되거나, 공격 계획이 논의되는 공간

이제 우리가 일반적으로 사용하는, 지금 이 글이 보여지는 웨어드IT와 같은 표면웹과 딥웹, 그리고 다크웹이 어떻게 다른지 아시겠죠? 해커는 딥웹에 접근해서 기업의 민감 데이터를 훔쳐내고, 이 정보를 다크웹에 올려 거래하거나 공격을 사전 공유합니다. 따라서, 다크웹은 해킹의 결과가 노출되는 공간이며, StealthMole은 이 다크웹에 노출된, 추가 해킹이 발생할 수 있는 조짐을 추적하는 서비스라고 할 수 있습니다.

■StealthMole: 다크웹 인텔리전스 플랫폼

StealthMole은 수많은 다크웹, 딥웹, 폐쇄형 채널을 모니터링하면서 아래와 같은 정보를 수집하고 태깅해서 분석합니다.

- Tor, I2P, Telegram, Discord 기반 폐쇄 커뮤니티
- 해커 포럼, 크리덴셜 마켓, RaaS(서비스형 랜섬웨어) 판매처
- 기업명, 이메일 도메인, 시스템 구성 정보 등 노출 여부

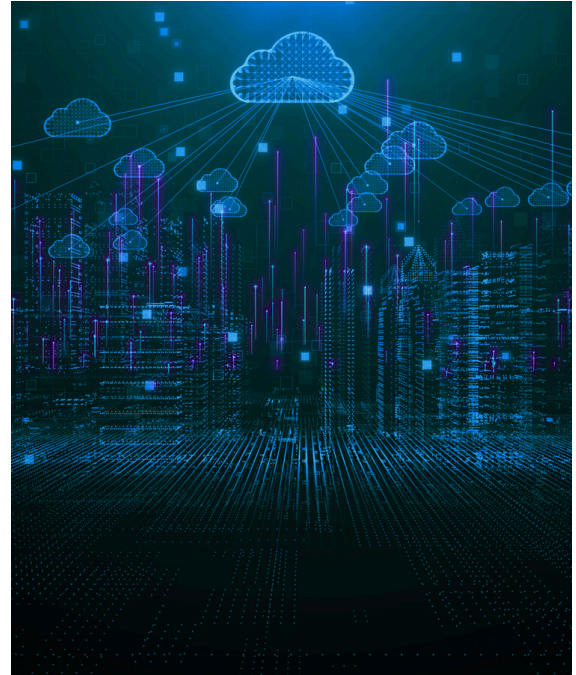
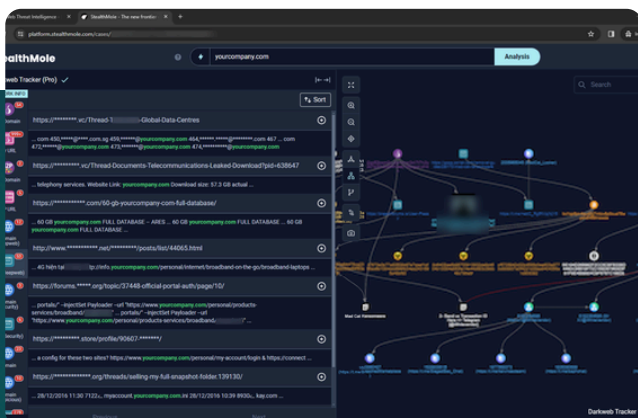
즉, 공격자가 특정 기업을 목표로 삼기 전에, 그 조짐을 미리 발견할 수 있도록, 그리고 침해 후에는 유출 여부를 추적하고 대응 전략을 수립할 수 있도록 돕습니다.

■실시간 시연 사례: 누구나 검색 가능한 다크웹 모니터링

우리는 ChatGPT처럼, 누구나 다크웹을 검색할 수 있게 합니다.

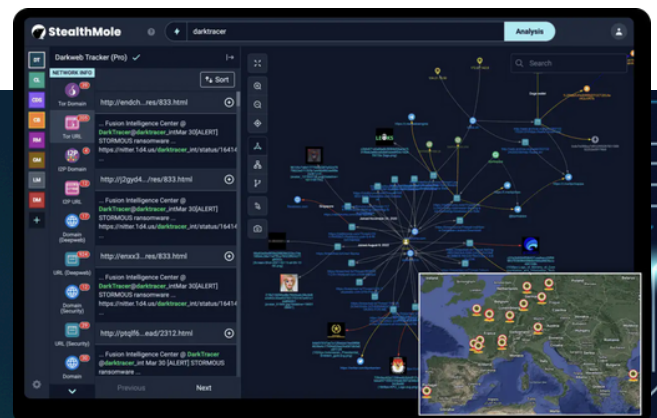
StealthMole 세션에서 실제 데모를 볼 수 있었는데요. 이번 데모에서 StealthMole 허영일 대표는

- 북한 함흥 지역을 기준으로 반경 설정
- 해당 지역의 텔레그램 사용자 81명 탐색
- 이 중 다수가 북한 연계 암호화폐 사기 활동에 연루
- 일부는 ChatGPT API 호출 기록까지 탐지됨을 확인



이 데모에서는 북한과 같은 폐쇄적인 국가 내부에서도, 텔레그램 사용자 활동이나 암호화폐 사기와 연관된 행위자들이 존재함을 확인할 수 있었는데요. 허영일 대표는 위도, 경도와 반경을 지정해 특정 지역 중심의 텔레그램 사용자 목록을 추출했는데, 이 중 일부는 북한에서 활동하는 해커 그룹과 연계된 패턴을 보였습니다.

따라서, 북한과 같이 설령 국가 차원에서 인터넷이 폐쇄된 환경이라 하더라도, 우회된 채널(해외 IP, 오픈 메신저, 클라우드 API 등)을 통해 실질적인 위협 활동을 탐지하고 지역 기반 위협 분석을 수행할 수 있다라고 보시면 되겠습니다.



■기업이 활용할 수 있는 다크웹 인텔리전스 전략

그럼 이렇게 StealthMole 플랫폼을 통해 다크웹에서 수집한 정보를 어떻게 활용하면 좋을까요? 간단히 정리해 봤습니다.

활용 전략	설명
데이터 유출 조기 탐지	자사 도메인/계정 정보가 다크웹에 등장했는지 실시간 모니터링
공격자 그룹 추적	라자루스 등 APT 그룹의 활동 경로, 행위자 ID 추적
임직원 크리덴셜 감시	이메일, 비밀번호, MFA 우회 정보 유출 여부 확인
공급망 리스크 관리	파트너사/협력사 관련 유출 여부 모니터링
브랜드 보호	자사 명의의 피싱 사이트, 가짜 SNS 식별 및 대응

실제로 StealthMole은 이렇게 활용할 수 있는 다양한 정보들을 수사기관에 제공하고 있다고 합니다. 사이버 범죄 조직을 쫓는 데에 반드시 필요한 정보들이라고 할 수 있겠죠? 그리고 파고에서도 이 정보들을 활용합니다. 파고의 MDR 플랫폼, DeepACT에 앞서 보셨던 SentinelOne, Stellar Cyber와 더불어 StealthMole도 통합되어 있거든요. StealthMole에서 수집한 정보를 토대로 파고 분석가들은 아래와 같은 일을 합니다.

- 악성 도메인/IP/해시 값을 기반으로 탐지 룰 강화
- 조직명, 계정명, 이메일 등의 검색을 통해 실시간으로 유출 여부 확인 및 고객사별 경고
- 다크웹 공격자 정보를 기반으로 룰셋 재정비 및 선제적 헌팅

즉, SentinelOne과 Stellar Cyber가 내부를 보는 눈이라면, StealthMole은 외부를 감지하는 귀이자 망을 보는 눈입니다. 파고의 권영목 대표도 아래와 같이 StealthMole을 언급했습니다.

“다크웹 인텔리전스는 단순한 모니터링이 아니라, MDR 서비스의 위협 헌팅을 가속화하고, 디지털 리스크를 입체적으로 관리하는 전략적 무기입니다.”

이제, 세션의 핵심 내용만 간단히 요약해 봅시다.

항목	내용
탐지 대상	다크웹, 딥웹, 폐쇄형 커뮤니티, 텔레그램 채널
분석 방식	자연어 검색 + 지리 기반 위협 인식 가능
적용 전략	유출 조기 감지, 공격자 추적, IoC 강화, 공급망 리스크 대응
파고 연계	헌팅 룰셋 보강, 사전 대응 정비, 다크웹 기반 선제 인텔리전스 통합

4. 탐지에서 억제까지 – 파고 기술팀이 말하는 실전 운영 전략

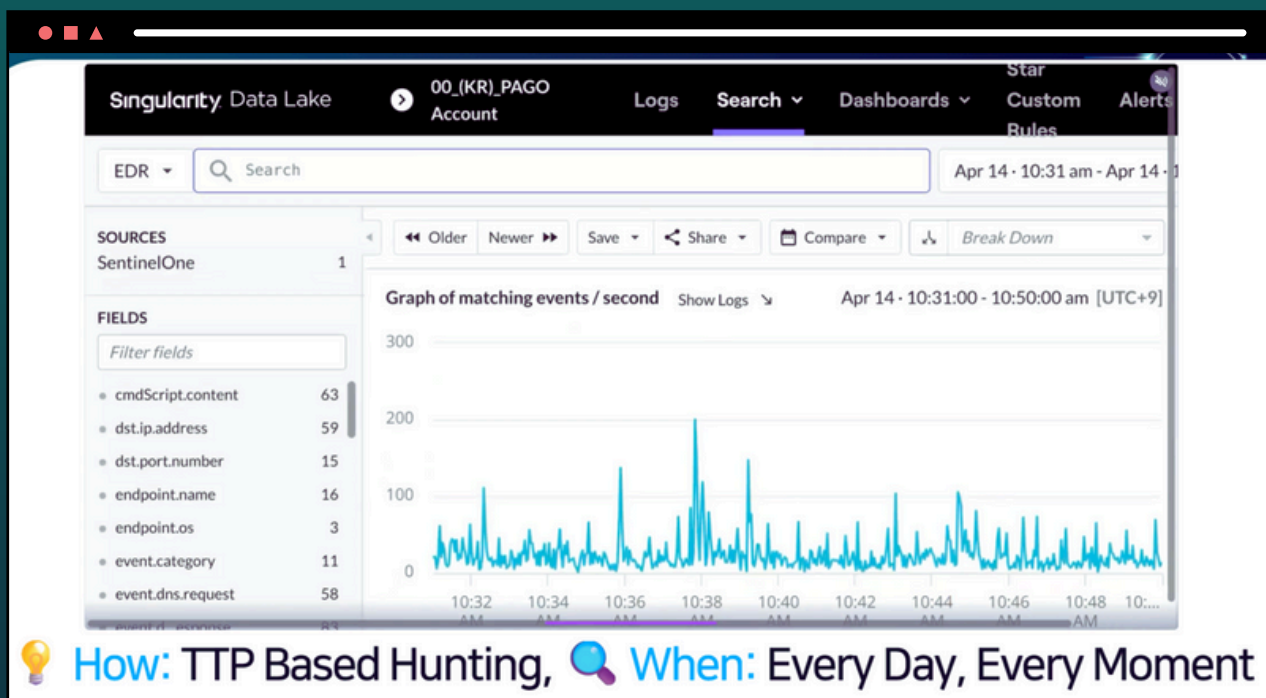
보안은 사고가 난 뒤에 대응하는 것이 아니라, 사고가 ‘안 났더라도’ 발생할 수 있었던 위협을 찾아 대응하는 것입니다.

파고 임직원들의 기술 세션에서 가장 인상 깊었던 건 단순한 알람 기반 대응이 아니라, 능동적으로 위협을 헌팅하고 조기에 차단하는 실전 전략이었습니다. 이 발표는 두 명의 파고 기술팀 구성원이 각각 위협 헌팅 전략과 CSIRT 운영 모델을 소개하며 파고가 어떻게 MDR의 전략적 본질을 기술로 구현하고 있는지 보여준 시간이었는데요. 그럼, 구체적으로 어떤 내용이 소개되었는지 살펴볼까요?

■알림을 기다리지 않는다 – 위협 헌팅과 선제적 대응 전략

파고의 분석가들은 솔루션에서 알람이 오면 분석하는 것이 아닌, 그 전부터 자신들만의 노하우로 위협 헌팅을 합니다. 이게 기존의 탐지 방법과 어떻게 다른지 간단히 정리하면 아래와 같습니다.

Threat Hunting Starting Point



구분	전통적인 탐지	파고의 위협 헌팅
탐지 방식	SIEM/EDR 알람 수신 → 수동 확인	알람 여부와 무관하게 능동 조사
대상	알려진 패턴	정상 행위 속 비정상 시도, Living off the Land 기법
대응 시점	이벤트 발생 후	공격 체인 초기에 선제 차단

예를 들어, 랜섬웨어는 마지막에 암호화가 일어나죠? 하지만 이 데이터 암호화는 결과이지 원인이 아닙니다. 즉, 해커에게 다시 랜섬웨어 공격을 당하지 않으려면, 암호화가 발생되기 전에 벌어지는 계정 유출, UAC 우회, RDP 접근이 핵심 탐지 포인트라는 것입니다.

이를 위해 파고는 비정상 시간대 로그인, 해외 IP에서 관리자 권한 접근 시도, PowerShell의 의심스러운 사용, 사용자 행동 기준선과의 편차를 감지는 등, 이런 요소들을 기반으로 알림 없이도 위협을 선제적으로 포착하는 위협 헌팅을 수행합니다.

파고의 이러한 헌팅 전략은 단발성 탐지에 그치지 않고, 디텍션 엔지니어링 프로세스로 발전시켜 운영하고 있습니다. 즉, 공격자의 전술(TTPs)을 기반으로 Sigma 탐지 룰을 설계하고, 테스트 → 룰 강화 → 검증을 반복하며 실제 고객 환경에 최적화된 탐지 체계를 구축하는 방식으로 운영 중이라는 겁니다.

■ 탐지 이후 단계별 대응 프로세스 - 핵심은 Live Forensic

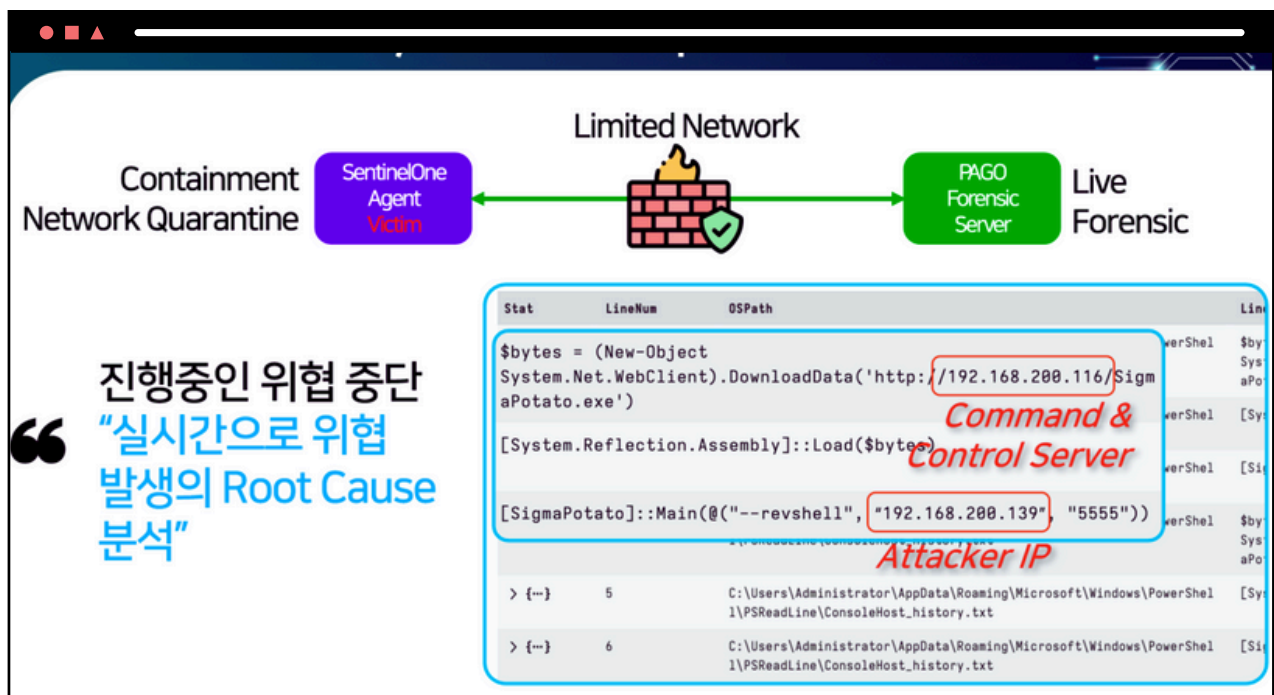
파고 기술팀은 탐지 이후 위협을 다음과 같은 4 단계로 나눠서 설명했습니다.

여기서 말하는 Live Forensic은 공격자가 활동 중인 상태에서 에이전트 로그, 실행 중 프로세스, 메모리 및 네트워크 흐름 등을 실시간 수집하며 실시간 포렌식 분석을 수행하는 것을 의미합니다. 사고 이후 복구를 위한 분석이 아닌, 진행 중인 위협에 즉시 대응하고 공격 흐름까지 추적하는 실전 개입 방식이라고 할 수 있죠.

그리고, 이어서 한 제조기업에서 발생한 위협을 조기에 탐지하고 조치까지 한 경험을 공유했는데요. 솔루션에서 별다른 알림은 발생하지 않았지만 분석가가 일상적인 헌팅 중 비정상 PowerShell 실행을 탐지했고, 조사 결과 공격자가 해외의 C2 서버와 통신을 한 흔적을 발견했다고 합니다. 그래서 파고 네트워크는 다음과 같은 조치를 취했습니다.

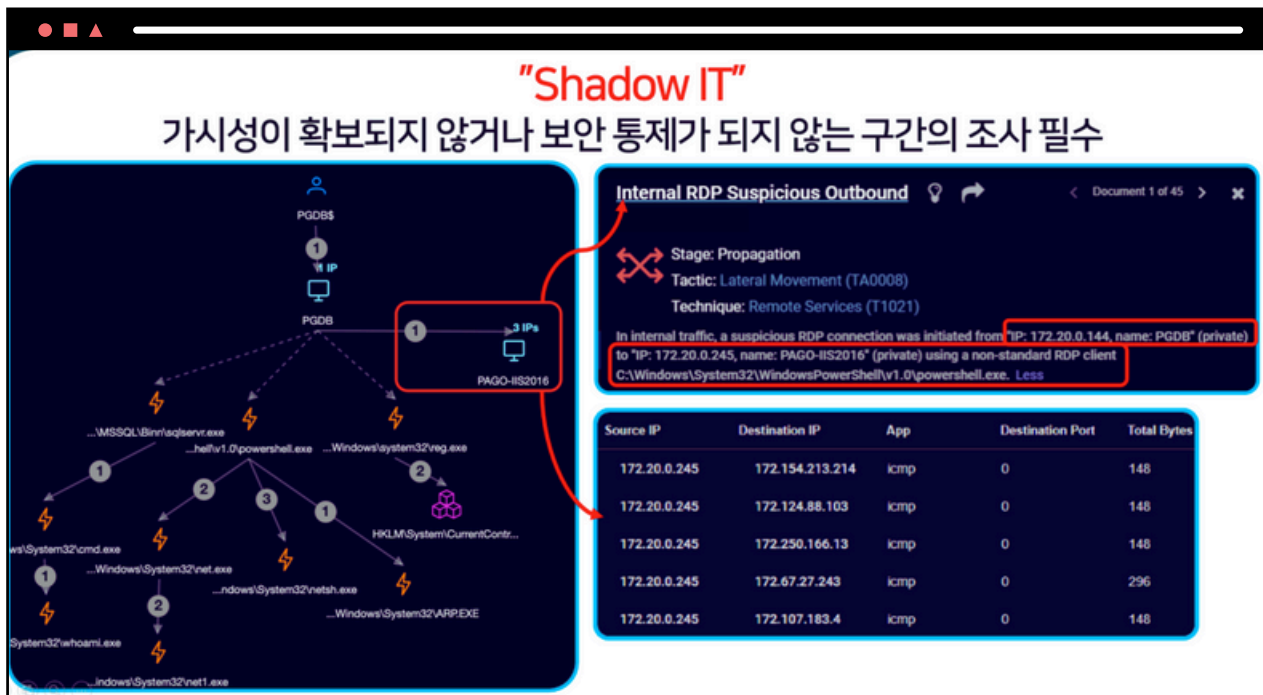
- 해당 워크스테이션 격리
- 공격 계정 정지
- C2 서버 IP 차단 및 블랙리스트 등록
- 유사 명령 탐지 룰 배포

만약 알림이 없었다는 이유로 아무런 조치를 취하지 않았다면? 약 48시간 뒤 랜섬웨어 배포로 이어질 수 있었을 겁니다. 실제로 사고가 발생해서 해커가 피해를 입히지 않았지만, 마치 사고가 발생한 것처럼 대응하는 방식인거죠. 이렇게 위협 헌팅을 통해 해커의 공격 초기 단계에서 차단하는 것을 일깨워준 사례가 아닌가 싶네요.



■ 보호되지 않는 자산도 놓치지 않는다

Lateral Movement Toward Unsecured Assets



파고 기술팀은 위협 탐지 이전 단계에서부터 공격자가 사용했을 법한 경로를 가설로 설정하고 헌팅을 수행하며, 필요 시 고객 승인 하에 자산 격리, 계정 정지, C2 통신 차단 등 즉각적인 조치까지 전개한다고 앞서 언급했었죠? 파고는 여기서 한발 더 나아가, EDR로 보호할 수 없는 사각지대까지 실시간으로 커버하고 있는데요. 보안 에이전트를 설치할 수 없는 환경에서도 위협을 놓치지 않는 구조를 만든 것입니다. 그렇다면, 이렇게 보안 에이전트를 설치할 수 없는, EDR로 보호되지 못하는 자산은 어떻게 보호해야 할까요? 먼저 자산 유형 별로 파고가 어떻게 대응하고 있는지 간단히 정리해 봅시다.

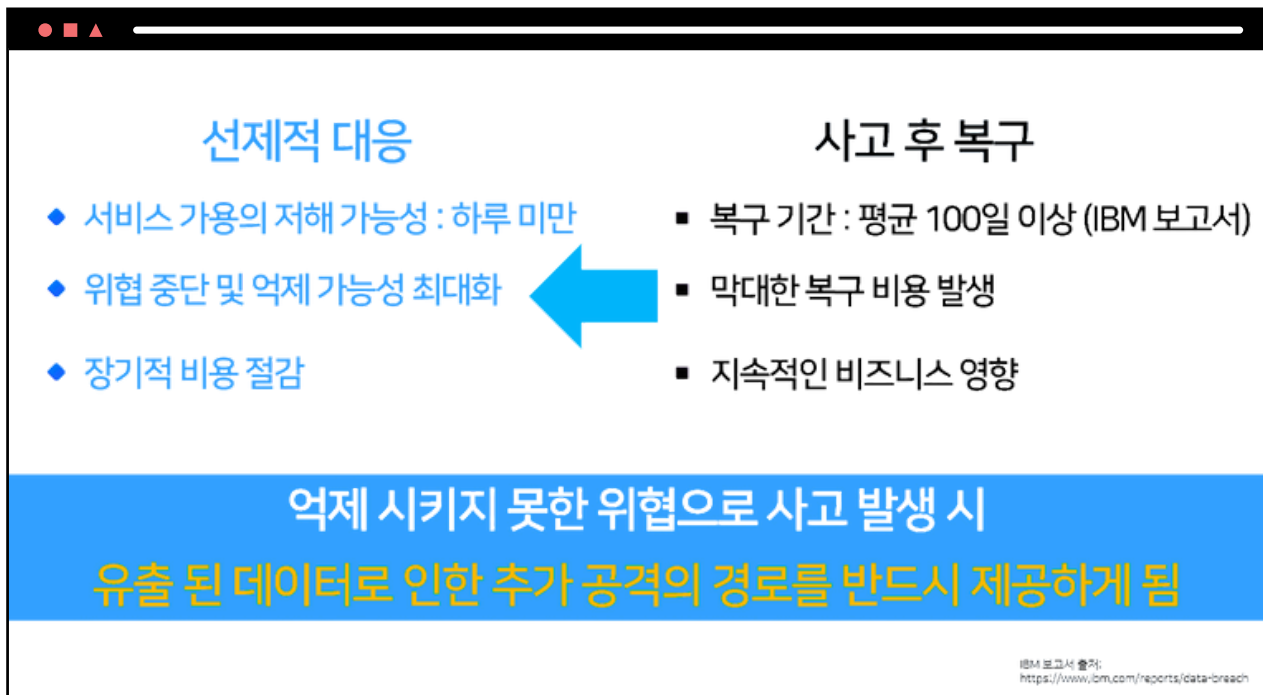
자산 유형	의미	대응 방식
Shadow IT	보안팀이 존재를 인지하지 못한 장비	NDR 기반 트래픽 흐름 분석
Legacy 시스템	Windows XP 등 미지원 운영체제	네트워크 위협 감시
IoT/의료기기	에이전트 설치가 불가능한 기기	포트, 프로토콜 기반 탐지
임베디드 장비	사내 개발 또는 인증 이슈 장비	내부 통신 흐름의 상시 모니터링

이처럼 다양한 자산 유형이 혼재된 환경에서는 단일 보안 솔루션으로는 탐지 사각지대가 생길 수밖에 없습니다. 그래서 파고는 다음과 같은 하이브리드 보안 모델을 활용합니다.

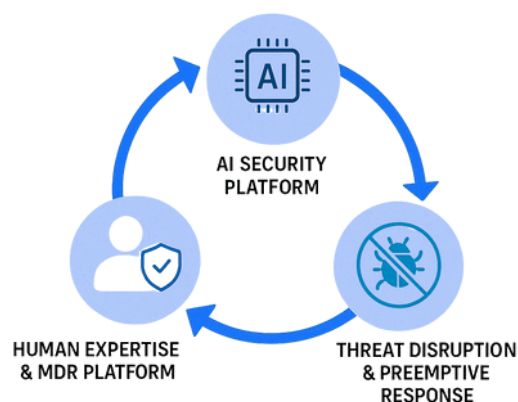
- 보호 가능한 자산은 EDR(SentinelOne)으로 커버
- 보호할 수 없는 자산은 XDR(Stellar Cyber)로 실시간 모니터링

■사고 후 복구가 아닌 선제적 대응이 필요한 이유

Why Preemptive Response Matters



IBM 2024 보고서에 따르면 랜섬웨어 사고 이후 평균 복구 기간은 100일 이상 걸리는 경우도 있다고 합니다. 그래서 파고는 '사고가 나기 전에 멈춰야 한다'는 원칙 하에, 실제로는 사고가 발생하지 않았더라도 이를 사고처럼 간주하고, IOC 생성과 룰 반영까지 수행하는 Preemptive Response 모델을 운영하고 있다고 밝혔는데요. 이렇게 복구에 의존하기 전에 먼저 사고를 차단하는 방식이야말로, 파고가 강조하는 선제적 대응 전략의 핵심입니다.

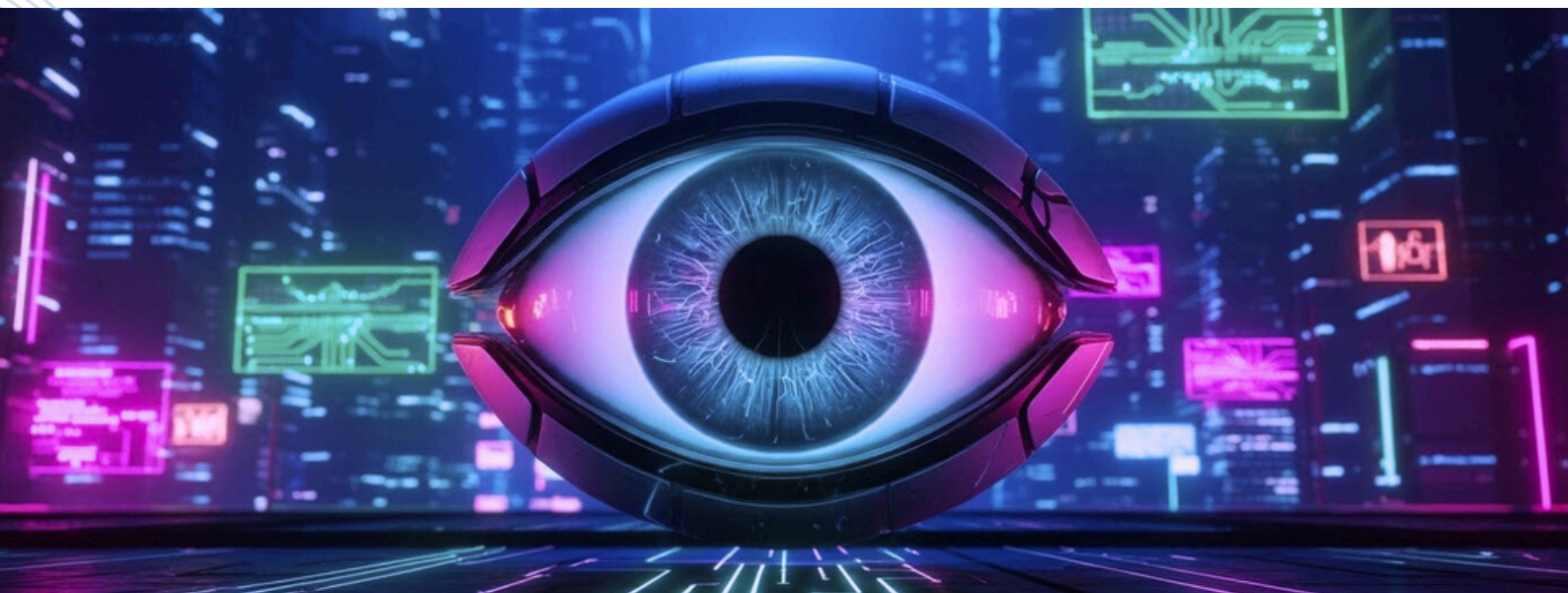


항목	설명
핵심 전략	알림이 없어도 탐지하는 위협 헌팅 기반 보안
실행 방식	IOC 없이 탐지, Live Forensic, Disruption, Playbook 운영
프로세스	헌팅 → 검증 → 차단 → 룰 강화 → 반복 개선
운영 범위	보호 가능한 자산 + 보호할 수 없는 자산 모두 커버
기술 연계	SentinelOne + Stellar Cyber + StealthMole 통합 대응

이번 [PAGO Security Summit 2025](#)에서는 기술이 아닌 '실전'이 만든 보안 전략이 어떻게 구현되는지를 확인할 수 있었던 자리였습니다. 단순히 MDR이 무엇인지 설명하는 수준을 넘어서, 어떻게 탐지하고, 언제 개입하며, 어디까지 대응할 수 있는지를 각각의 스폰서 세션과 파고 기술 세션을 통해 구체적으로 확인할 수 있었는데요.

마무리로는, 행사에서 발표된 각 세션의 내용을 한 문장으로 간결하게 요약한 표를 통해 정리하고자 한다. 다소 축약된 느낌이 있을 수 있으나, 표 형태로 정리된 정보가 더 직관적으로 전달되는 측면이 있다.

세션	핵심 메시지
SentinelOne	AI는 SOC의 '두뇌 보조 장치'로, Purple AI를 통해 분석가의 판단을 가속화
Stellar Cyber	SIEM의 한계를 넘는 Open XDR 기반 통합 분석과 자동화된 대응
StealthMole	다크웹 인텔리전스를 기반으로, 내부 보안체계가 감지하지 못하는 외부 위협 조기 인지
파고 기술팀	알림을 기다리지 않는 위협 헌팅, Live Forensics, 피해가 없어도 실제 사고 상황처럼 대응



■다음글 예고: 선제적 보안 시대, 파고가 제시한 프론트라인의 진정한 의미

여기까지 PAGO Security Summit 2025의 주요 내용을 정리했고요. 그렇다면, 다음 질문은 이겁니다.

"이 모든 기술과 전략의 중심에 내제된, 파고만의 철학이 뭐지?"

"그래서, 프론트라인이 무슨 뜻이라는 거야? 아직 잘 감이 안오는데..."

단순히 기술을 조합하고 활용하는 것이 아니라, 위협을 어떻게 인식하고, 누가 책임지고, 어디서부터 대응을 시작할 것인가에 대한 보다 근본적인 질문이 필요하지 않을까요? 그래서, 다음 글에서는 '선제적 보안 시대, 파고가 제시한 프론트라인의 진정한 의미'라는 주제에 대해 다뤄보려고 합니다.

기술 뒤에 숨은 철학, 전략을 만든 결단, 그리고 진정한 프론트라인 보안의 의미를 다시 짚어볼 수 있는, 파고의 담대한 메시지는 무엇일까요?

III. 변화하는 전선: 파고가 제시하는 새로운 보안 프론트라인

“사고가 나면 막는 게 보안
이 아니라, 사고가 날 수 있
다는 전제하에 구조를 만
드는 게 보안입니다.”

파고네트웍스 권영목 대표의 이 말은 이번 파고 서밋 전체를 관통하는 메시지였습니다. 첫 번째 글에서는 MDR이 무엇이며 파고 MDR은 어떤 차별점이 있는지, 두 번째 글에서 파고 MDR이 실제로 어떻게 작동하는지를 확인했다면, 이제 MDR이 왜 존재해야 하는지, 그리고 파고가 이 시장에서 어떤 철학을 갖고 움직이고 있는지를 짚어볼 차례입니다.

이제 기술은 충분히 진화했습니다. 남은 건, 그것을 어떻게 쓰느냐입니다.

파고는 이제 자신들을 “사이버 위협의 최전선에서 싸우는 조직”이라 부릅니다. 이는 단순 기술 공급자가 아닌, 위협이 발생하기 직전에 개입해 고객을 보호하는 ‘프론트라인’ 역할을 수행하겠다는 선언이죠. 그래서 이번 마지막 글에서는 왜 지금 ‘선제적 보안’이 필요한지, MDR이 단순 위협 탐지를 넘어 어떤 구조적 역할을 해야 하는지, 그리고 파고네트웍스가 실전 경험 속에서 깨달은 ‘진짜 보안’의 철학은 무엇인지 함께 정리해보겠습니다.

1. 보안 사고는 구조의 실패에서 시작된다

사이버 보안 사고는 흔히 '누군가의 실수'로 인한 단편적인 문제처럼 여겨지곤 합니다. 어떤 직원이 피싱 메일을 열었거나, 취약한 패스워드를 사용했거나, 로그를 실시간으로 확인하지 못해 이상 징후를 놓쳤다가거나 하는 식이죠. 하지만 파고 네트워크는 그렇게 생각하지 않습니다.

보안 사고는 시스템의 한계 이전에, 조직의 구조가 실패했을 때 발생하며, 그 구조의 실패는 대부분 '공유되지 않은 정보', '책임지지 않는 체계', '움직이지 않는 판단'에서 비롯된다고 보는 것인데요. 그래서 파고는 보안 사고가 발생했을 때, '이걸 왜 못 막았을까?'라는 질문 대신 아래와 같이 질문합니다.

- 그 징후는 이미 내부에 존재하고 있던 것 아닌가?
- 누군가는 감지했지만, 공유되지 않았던 건 아닐까?
- 알림은 울렸지만, 조직 구조상 누가 먼저 움직여야 할지 불명확했던 건 아닐까?

실제로 많은 기업의 사고 사례를 들여다보면, 위협은 이미 여러 시스템 안에서 조용히 신호를 보내고 있었고, 그 신호가 분산되고, 누락되고, 사일로에 갇혀 조치를 받지 못한 채 누적된 끝에, 사고라는 결과로 폭발한 경우가 많죠.

사례를 하나 들어볼까요? 파고가 경험한 어떤 고객사의 경우, 관리되지 않은 외부 협력사 계정이 주말 새벽 시간에 내부 VPN을 통해 접속했지만, 로그는 각 보안 시스템에서 잘 기록되고 있었지만, 이들 간의 연동은 구조적으로 분리되어 있었고, 그 조각들이 서로 연결되지 않으면서 전체 흐름을 인식하지 못한 채 지나갔습니다.

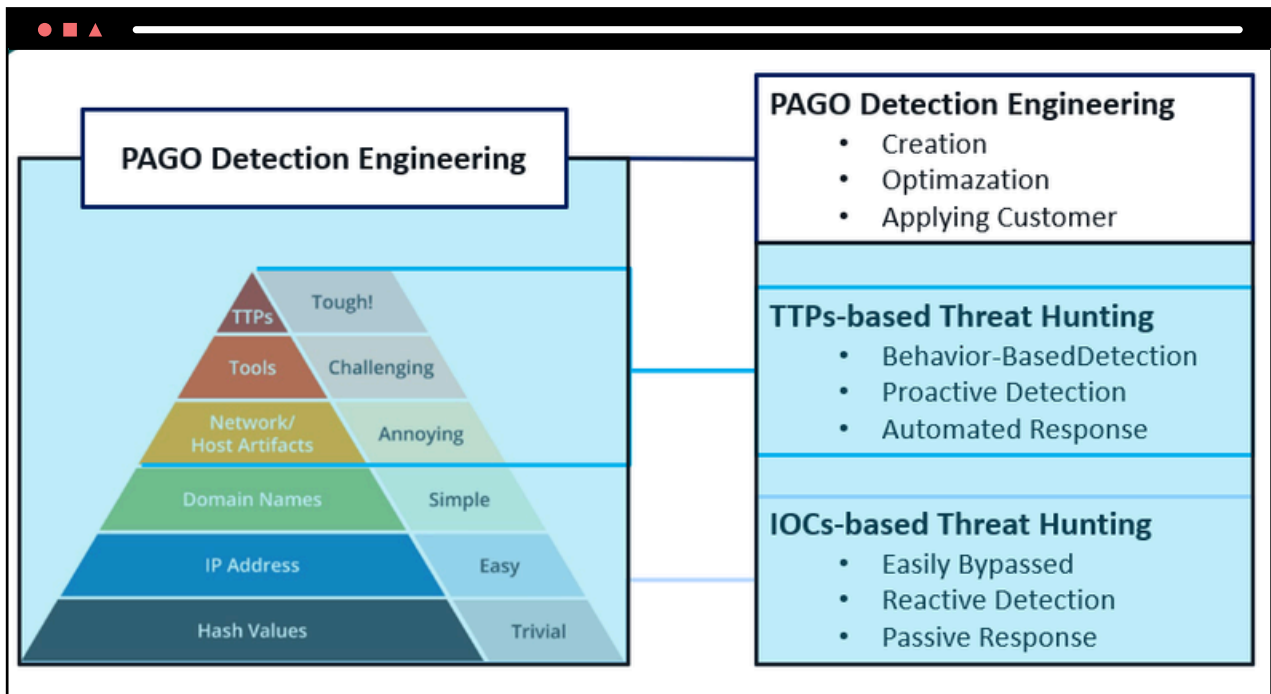


이는 솔루션의 문제가 아니라, 보안 이벤트를 종합적으로 판단할 수 있는 구조가 사전에 마련되지 않았던 것입니다.

심지어, 이 시간대는 담당자의 근무 시간이 아니었기에 아무런 조치도 취해지지 않았습니다. 이때 사용된 계정은 이전에도 비정상적인 사용 패턴을 보였던 계정이었고, 이 정보를 이미 알고 있던 팀도 있었음에도 불구하고 말입니다. 하지만 그 정보는 위험 수준으로 분류되지 않았고, 다른 팀에게 전달되지 않았으며, 누구도 이 연결고리를 파악하지 못했습니다.

- 경고는 누가 먼저 받고, 어떻게 공유되는가
- 기준선은 명확한가, 사람에 따라 해석이 갈리지 않는가
- 공격이 시작됐을 때 첫 번째 반응권한은 누구에게 있는가

보안은 단일 장비가 아니라, 탐지→판단→공유→억제로 이어지는 구조가 하나의 시스템으로 연결되어야 작동합니다. 이 구조가 작동하지 않는다면, 아무리 뛰어난 솔루션도 결국 “봤지만 못 막은 사고”를 만들 수밖에 없다는 거죠.



파고는 이러한 실패를 ‘기술의 문제’가 아니라 ‘설계되지 않은 책임의 문제’라고 진단합니다. 즉, 누군가가 실수했기 때문이 아니라, 누가 먼저 움직여야 할지 정해져 있지 않았기 때문에 사고가 벌어진 것입니다. 조사할 단서는 많았지만 정보가 각각 분산되어 있어 통합적인 가시성을 제공하지 못하고, 어떤 조치를 먼저 취해야 할 지 갈피를 잡지 못하기 때문이죠. 그래서 파고는 기술보다 먼저, 고객의 보안 구조를 진단합니다.



파고가 말하는 ‘탐지 이전의 보안’은 이런 구조의 허점을 전제로 움직입니다.

"사고가 일어날 수 있는 가능성 자체를 줄이자"
"누가 먼저 움직여야 할지를 구조로 정해두자"

그것이 파고가 첫 번째로 만드는 ‘보안 체계’입니다.

2. 위협은 알려지기 전에 막아야 - 파고의 프론트라인 전략

보안은 경보가 울린 다음에 움직이는 것이 아닙니다. 이미 위협이 시스템 안에 들어왔을지도 모른다는 전제 하에, 경보보다 먼저 움직이고, 실시간으로 억제하고, 재앙이 일어나기 전에 차단하는 것이 진짜 보안입니다.

파고 네트워크가 이야기하는 '프론트라인'은 이러한 '탐지 이전의 대응', '알람이 없더라도 움직이는 보안'을 의미합니다. 우리가 흔히 접하는 대부분의 보안 시스템은 EDR, SIEM, XDR 등 다양한 탐지 솔루션에 의존하죠. 이들은 알려진 패턴이나 룰셋에 기반해 이상행위를 탐지하고, 그 결과를 분석가에게 전달하는 것이 일반적인데요. 문제는 여기에 있습니다. 이 탐지 시스템이 작동하기 위해선 '알람을 울릴 만큼의 이상'이 발생해야 한다는 전제가 있죠.

하지만 실제 공격자들은 이 탐지 임계값보다 아래에서 움직입니다. 정상 사용자 계정을

탈취하고, 정상 툴(PowerShell, WMI 등)을 사용하며, 마치 시스템 관리자인 것처럼 내부를 돌아다니거든요.

파고는 이 지점을 정확히 노립니다. 알람이 없더라도, 이상한 로그인 시간, 의심스러운 명령어 패턴, 낯선 IP에서의 접근, 그 자체만으로도 위협의 조각을 포착하는 것. 이게 바로 파고의 '위협 헌팅 전략'입니다.

파고의 분석가들은 단순히 탐지된 이벤트를 분석하는 것이 아니라, 공격자가 선호하는 침투 경로, 회피 전략, 초기 정찰 방식 등을 가설로 세우고 실제로 그 흔적이 고객사 내부에서 발생하고 있는지 '사냥하듯이' 추적합니다. 예를 들어 한 제조기업에서는 알람이 전혀 발생하지 않은 상태에서 분석가가 반복적으로 실행되는 PowerShell 명령을 포착했고, 해당 장비가 해외 C2 서버와 통신을 시작하고 있던 사실을 확인했습니다.



이때 파고는 단순히 보고서를 작성하거나, 다음 날 조치를 요청하지 않았습니다. 이미 고객사로 부터 승인받아 둔 사전 대응 프로토콜에 따라 즉시 해당 워크스테이션을 네트워크에서 격리했고, 공격 계정을 일시 정지하며, C2 IP 주소를 전체 고객사에 블랙리스트로 등록했죠. 고객사 담당자에게 경고와 취해야 할 조치 사항을 전달하고 끝내는 것이 아니라, 직접 적절한 조치까지 고객사 담당자를 대신해 수행한 겁니다.

덕분에 해커의 공격은 '막 시작된 참사'의 상태에서 바로 끊겼고, 그 대응 경험은 다시 파고의 IOC(Indicators of Compromise, 침해 지표)로 정제되어 다른 고객사 환경에 바로 적용됐습니다. 파고는 이러한 전체 과정을 아래와 같이 구조화했는데요.

- Threat Hunting - 알림 없이도 능동적으로 위협을 탐지하고, Pre-incident 대응을 수행
- Containment & Live Forensics - 탐지된 위협을 격리하고 동시에 실시간 포렌식 분석을 통해 공격 흐름을 추적
- Threat Investigation - Lateral movement, C2 통신 등 공격 확산 경로를 파악하고 차단 조치를 설계
- Preemptive Response - 고객 승인 범위 내에서 즉시 계정 정지, 통신 차단, 롤백 등 선제적 대응 실행

그리고 이 구조가 이제 이렇게 진화했습니다.



여기서 중요한 것은, 먼저 선 조치하고 사고가 날 뻔한 원인을 규명해 나간다는 것입니다. 사고가 나야 움직이는 구조가 아니라, 사고가 '날 수도 있는 흐름'을 먼저 끊는 보안 구조라고 할 수 있죠. 여기서 핵심은 '선조치'입니다. 일단 먼저 조치해서 위협이 퍼져 사고가 되는 것을 막는다는 것이 이 구조의 핵심입니다.

그래서 파고는 자신을 프론트라인이라 부릅니다. 이는 단지 '제일 앞에 서겠다'는 선언이 아닌, 위협이 오기 전에 막아야 하는 책임을 자처하겠다는 약속인 것인데요. 실제 [PAGO Security Summit 2025](#) 조찬 세션에서 파고 네트워크 권영목 대표는 아래와 같이 언급했습니다.

”

응급실은 병을 고치지는 않습니다. 하지만 생명을 잃는 걸 막을 수는 있습니다.

일반적으로, 우리 몸의 상처를 완전히 치유하는 데는 어느정도 시간이 필요합니다. 그리고 이 완치의 영역은 병원의 각 전문 과목이 담당하죠. 반면, 응급실의 역할은 상태가 악화되기 전에 빠르게 개입해 위기를 막는 것입니다. 응급실에서 응급 처치를 받은 다음에야 비로소 입원 치료든 외래 진료든 시간을 들여 본격적인 치료가 시작되잖아요? 파고의 역할은 바로 그 '응급실'에 해당합니다. 위협이 더 커지기 전에 즉시 개입해 확산을 억제하고, 상황을 통제하는 것. 이것이 바로 파고가 말하는 프론트라인 보안의 핵심입니다.

3. 기술보다 중요한 것은 사람의 판단과 책임감

AI 탐지, 시그니처 기반 룰셋, 자동화된 대응 정책 등, 많은 보안 솔루션은 자동화를 강조합니다. 하지만 자동화는 기존에 정의된 위협에 대해서만 반응하곤 하죠. 그런데 문제는, 현실의 위협은 언제나 정의 밖에서 움직인다는 데 있다는 것입니다.

- 공격자들은 탐지 룰을 회피
- 정상적인 사용자 권한을 활용
- 정상적인 명령어를 교묘하게 조합해 움직임
- 심지어 기존 룰셋이 회피할 수 있도록 공격 방식을 맞춤형으로 설계

이런 위협 앞에서는 '정의된 탐지 기준'보다 '판단할 수 있는 사람'이 훨씬 중요해집니다. 그래서 파고는

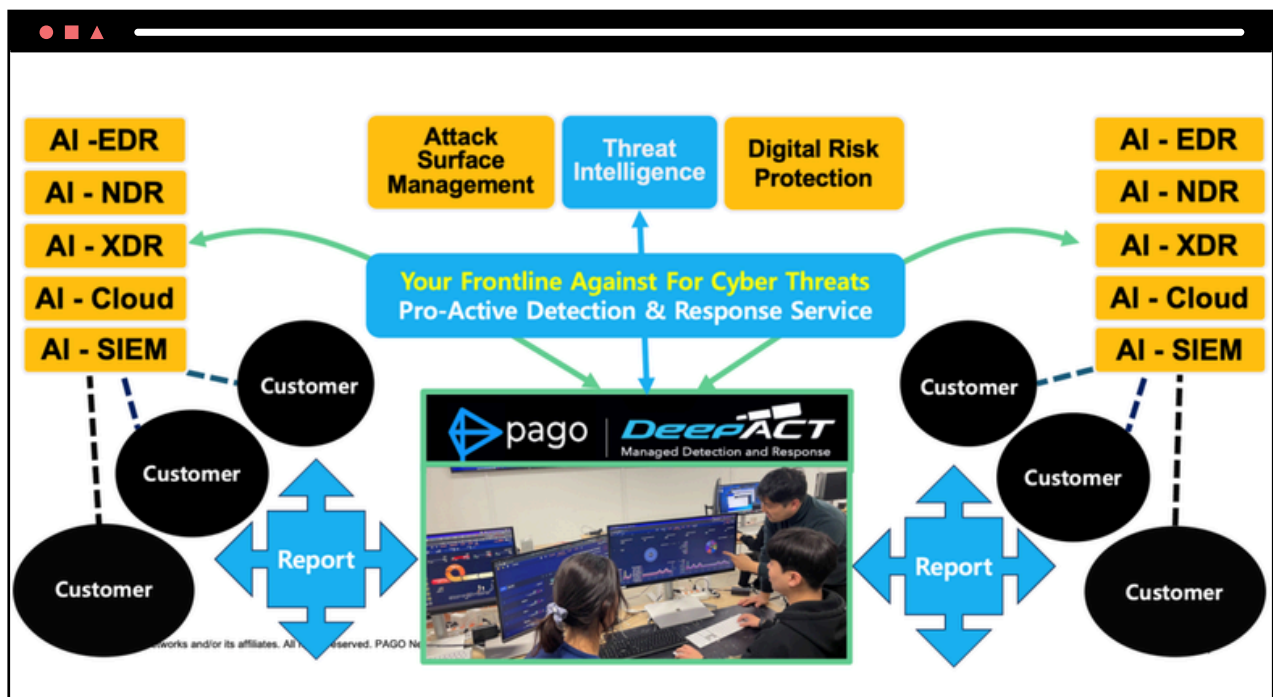
“위협을 찾는 것은 AI가 할 수 있습니다. 하지만 그 위협이 진짜인지, 어떻게 대응해야 하는지는 결국 사람이 판단해야 합니다.”

라고 말합니다. 실제로 파고의 분석가들은 알림이 발생하지 않아도 움직이고 있는데요. IOC가 없어도 로그를 파고들고, 공격자의 흔적을 추적하는데요.

예를 들어, 어떤 분석가는 특정 자산에서 비정상적인 Powershell 명령이 반복 실행되는 로그를 포착합니다. 해당 명령어는 명확한 악성 행위는 아니었지만, IP 주소만 다르게 하며 반복적으로 특정 외부 호스트와 연결을 시도하고 있었다는 점에서 의심이 생겼다고 해봅시다.

이 분석가는 즉시 해당 워크스테이션을 포렌식 분석하고, C2 통신 가능성을 판단한 뒤, 즉시 네트워크 격리 조치를 실행합니다. 이 시점까지도 EDR이나 SIEM은 침묵하고 있었지만, 분석가의 판단이 한 발 먼저 움직인 겁니다.

파고는 이렇게 '사람이 하는 판단'과 '즉시 조치할 수 있는 구조'를 보안의 핵심 사항으로 가져가고 있습니다. 기술은 판단의 도구가 될 수 있지만, 판단을 대신할 수는 없다고 굳게 믿고 있기 때문이죠.



실제로 파고의 분석가들은 글로벌 해킹 대회인 SentinelOne CTF에서도 실력을 증명했습니다. 24시간 내 위협을 찾아 대응하는 시뮬레이션 상황에서 전 세계 수십 개 팀 중 상위권을 차지하며, '자동화된 탐지'를 넘는 '실전 위협 대응' 역량을 입증한 겁니다. 기술이 발전하더라도 최종 책임은 그 기술을 활용한 사람에게 있기에, 사람의 역량이 무엇보다 중요하다고 믿고 있기 때문에 파고는 이렇게 사람, 휴먼 리소스 역량 확보에 가장 많은 투자를 하고 있습니다.

또한 파고 내부에서는 단 한 건의 분석도 '어느 한 사람의 분석'으로 끝나지 않는데요. 모든 위협은 리뷰되고, 공유되며, 더 나은 룰셋과 대응 전략으로 바뀌어 나갑니다. 이건 '사람이 판단한다'는 의미를 단순히 개인 역량에 맡기는 것이 아니라, 조직이 구조적으로 그 판단을 존중하고, 이 과정을 시스템화, 자동화한다는 뜻이기도 하죠.

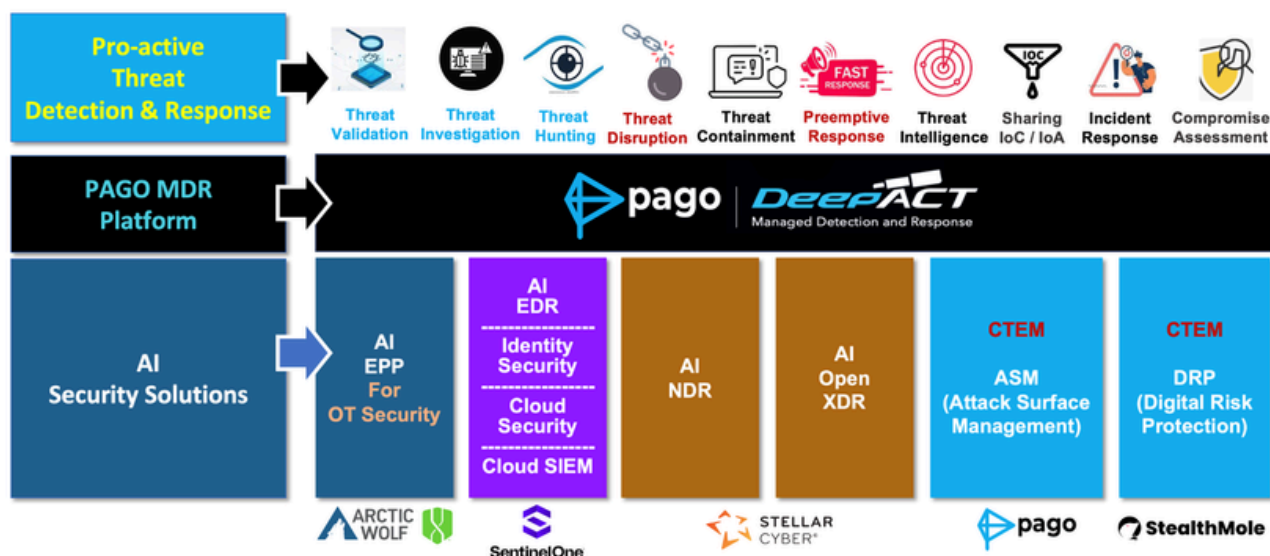
이 시스템이 바로 파고의 MDR 플랫폼 DeepACT입니다. 350개의 많은 기업들에게 동등한 고품질 MDR 서비스를 제공할 수 있는 원동력도 DeepACT를 기반으로 앞서 언급한 다양한 업무가 자동화되어있기 때문이라고 할 수 있습니다.

결국 중요한 것은, 기술의 판단을 기다리기 전에 사람이 먼저 인지하고 판단해야 된다는 것, 이것 꼭 기억해주세요.



4. 결론: 하나의 사고를 모두의 보안으로 바꾸는 조직 - 파고네트웍스

“모든 거짓말에는 대가가 있습니다. 그리고 그 대가는 단지 거짓말을 한 사람에게만 부과되지 않고 우리 모두에게 부과됩니다.”



이 말은 HBO 드라마 체르노빌의 마지막 장면에서 주인공이 남긴 말입니다. 사고의 원인을 외면하거나, 진실을 감추거나, 문제를 축소하면 그 결과는 결국 시스템 전체에 치명적인 비용을 남긴다는 의미심장한 발언이죠.

사이버 보안에서도 똑같은 교훈이 반복됩니다. 사고는 한 조직에서 발생하지만, 그 침투 경로는 다시 쓰이고, 그 공격 기법은 다음 기업의 취약점을 향하고, 그 실패에서 배우지 않으면 다른 고객, 다른 산업, 전체 생태계가 똑같은 위험에 노출됩니다. 그래서 파고는 보안 사고를 단지 “복구해야 할 문제”로 보지 않습니다. 한 번의 사고가 전체 보안 구조를 개선할 수 있는 기회가 되어야 한다는 철학을 갖고 있습니다. 예를 들어, 한 고객사에서 발생한 침해 사고가 있다고 가정해 봅시다. 이때 파고는 단지 그 고객의 시스템만 복구하는 데 그치지 않습니다.

그 침해의 원인은 무엇이었는지, 공격자는 어떤 경로를 통해 내부로 들어왔는지, 비슷한 환경을 가진 다른 고객사에서도 동일한 공격이 반복될 수 있는 가능성은 없는지에 대한 데이터를 다양한 보안 솔루션에서 수집해 DeepACT 플랫폼으로 한데 모아 함께 분석합니다.

이 분석을 기반으로

- IOC를 정제하고,
- 탐지 물을 강화하며,
- 기존의 대응 프로세스에 선제적 차단 절차를 추가하고,
- 이 모든 결과를 다른 고객의 환경에도 곧바로 반영합니다.

즉, 한 명의 고객이 겪은 사고는 전체 고객이 얻는 교훈으로 전환되는 것이고요. 파고 내부에서는 이 과정을 이렇게 표현합니다.

한 명의 사고는 모든 고객의 수업료가 되어야 한다.

이러한 구조는 파고가 단순한 MDR 서비스를 제공하는 보안 벤더가 아니라, 고객의 보안 구조를 함께 설계하고 성장시키는 파트너라는 점을 분명히 보여줍니다. 보통의 보안 대응이 “침해가 발생하면 복구하고, 분석하고, 보고서를 정리하는 것”이라면, 파고의 접근법은 그보다 한 단계 더 나아가는 것이 핵심이죠. 그래서 파고는, 고객사에 사고가 발생하면 담당자에게 이렇게 묻습니다.

그래서 파고는

1. 문제를 축소하지 않습니다.
2. 책임을 미루지 않습니다.
3. 구조를 바꾸는 것을 두려워하지 않습니다.

- 이 공격이 다시 일어나지 않으려면 무엇을 바꿔야 할까요?
- 기존 룰셋으로는 왜 탐지되지 않았을까요?
- 공격자가 다시 온다면, 다음엔 어디를 노릴까요?
- 현재 구조에서 여전히 남아 있는 허점은 무엇인가요?



이 질문들에 답하는 과정은 단순한 사고 복구가 아니라, 보안 구조의 리팩토링(refactoring)입니다. 고객 시스템을 다시 정비하는 것이 아니라, “왜 그 시스템이 위험에 노출됐는가”를 중심으로 전체 구조를 다시 설계하는 작업이라는 거죠. 이렇게 개선된 룰, 프로세스, 인사이트는 사고가 없었던 고객에게도 바로 적용됩니다.

그럼, 왜 이런 질문이 필요할까요? 한 번 공격을 당하면, 반드시 다음 공격이 이어지기 마련입니다. 게다가 더 큰 문제는, 다음 공격은 탐지 시점이 더 앞당겨질 수 있다는 거죠. 해커 입장에서 한 번 찾은 맛집을 한 번만 방문하기란 아쉬울테니까요.

기술은 계속 발전하고, 위협은 더 정교해지겠지만, 파고는 항상 사고 이전에 먼저 움직이고, 한 번의 실패도 전체 보안 전략을 바꿀 수 있는 자산으로 만드는 조직으로 남고자 합니다. 그래서 파고는 자신들을 이렇게 정의합니다.



우리는 마지막 방어선이 아니라, 가장 앞선 방어선입니다. 우리는 사고가 없더라도 움직이는 사람들입니다.

최근 발생한 굵직굵직한 보안 사고로 인해 기업은 막대한 피해를 입었고, 많은 사람들이 불안에 떨고 있습니다. 사고가 발생한 다음 취하는 조치는 이미 늦은 겁니다. 사고가 발생하기 전에 막아야 하죠. 그리고 사고를 일으킬 위험을 조기에 차단할 수 있어야 합니다. 이건 기술이, **AI가 할 수 없습니다.** 사람이 해야 합니다. 그런데 모든 기업이 보안 전문가를 보유할 수 없고, 보유했다 하더라도 그들이 24시간 해커의 공격을 탐지하며 모니터 앞을 떠나지 않기란 불가능에 가깝습니다.

그래서 파고가, MDR 서비스가 필요합니다. 여러 보안 솔루션을 활용해 데이터를 수집해서 위험을 조기에 감지하고, 선제적으로 조치해 위험을 차단해야 대형 보안 사고를 막을 수 있지 않을까요?

'Your Frontline Against Cyber Threats'

이제, 이 슬로건이 어떤 의미인지 잘 아시리라 생각합니다.

그럼 이쯤에서 이런 의문이 들 수 있습니다.

"우리 회사도 보안 솔루션 많은데 왜 조용한거지? 이거 괜찮은건가?"

"파고의 MDR 서비스 한번 받아보고 싶은데, 저 많은 솔루션들 다 도입해야 하나?"

만약 이런 궁금증이 생긴 분들이라면, 파고의 **Freemium Threat Cleaning**, Incident Response 서비스를 받아보시기 바랍니다. 말 그래도 무료 서비스이며, 최대 3개월까지 파고가 제공하는 MDR 플랫폼, DeepACT는 물론, SentinelOne, Stellar Cyber, StealthMole까지 모두 체험해 보실 수 있습니다.

파고 권영목 대표의 말에 따르면, 실제로 이 무료 서비스를 체험해 보시고 유료 고객으로 전환되는 확률이 80%에 달한다고 합니다. 우리 회사의 보안 상태가 걱정되신다면, 지금 바로 파고네트웍스의 전문가에게 연락하셔서 Freemium 서비스를 신청해 보시기 바랍니다.

파고네트웍스 MDR 서비스 문의하기

080-077-5171

sales@pagonetworks.com

www.pagonetworks.com

이번 세 편에 걸쳐 파고 네트워크스가 개최한 PAGO Security Summit 2025의 주요 내용과 함께 파고만의 독특한 보안 운영 철학을 깊이 있게 살펴보았습니다. 이 글들이 끊임없이 변화하는 사이버 위협 속에서 고군분투하는 보안팀에 도움이 되길 바랍니다.

