pago

PAGO THREAT INTELLIGENCE REPORT 2026

The Leader in Business Technology Media
NETWORK TIMES | DATANET IT·정·보·마·당

PAGO
THREAT
INTELLIGENCE
REPORT
2026

Table of Contents

EXECUTIVE SUMMARY

2025년 잇달아 발생한 대규모 사이버 위협은 조직의 전체 운영 모델을 재검토해야 한다는 사실을 보여준다. 공격자는 합법적인 자격증명, 공개된 취약점과 PoC를 이용하며, AI·자동화를 활용해 빠른 속도로 침투한다. 특히 아시아 태평양(APAC) 지역에서는 공급망 공격, 노출 자산 탐색, 허위 정보(Disinformation)를 이용한 평판 공격이 등장하면서 기존 방어 프레임으로 해결할 수 없는 새로운 위협 축이 형성되고 있다. 이에 따라 조직의 운영 모델 전체를 재검토해야 하는 시점에 도달했다.

24/7 운영과 선제적 대응

기업의 IT 환경이 복잡해지면서 보안 대응은 한층 더 어려워졌다. IT, OT, IoT, SaaS, 클라우드, AI가 동시에 확장·연결되면서 기업 내부와 외부의 경계가 사라지고 공격표면이 광범위하게 확장됐다. 이러한 변화에 민첩하게 대응해야 할 보안 운영센터(SOC)는 이벤트 모니터링의 한계를 벗어나지 못하는 상황에 놓여있다.

AI 시대의 보안 운영은 기본적인 설계부터 다시 시작해야 한다. AI가 초기 이벤트를 탐지하고, 리스크 우선순위를 평가하면, 전문가가 맥락과 의도, 비즈니스 영향도를 분석해 최종 판단을 내리며, 그 결과는 플레이북에 따라 자동으로 실행되는 프로세스다. AI의 분석을 사람이 검증하고, 정책·플레이북으로 환류시켜 탐지 품질과 대응 속도를 끌어올릴 수 있다. 특히 24/7 중단없는 운영으로 보안 공백 없이 실시간으로 탐지하고, 지속적인 위협 노출 관리(CTEM)로 선제대응을 강화해야 한다.

2026년 이후 보안 전략은 ①공격 전에 리스크를 줄이고 ②공격 시 신속히 복구하는 구조를 어떻게 설계할 것인가에 초점을 맞춰야 한다.

2026년 이후 보안 운영 모델

이 보고서는 경영, 운영, 기술 관점에서 보안이 어떻게 작동해야 하는지 근본적인 질문과 해답을 담고 있다. 2023년부터 2025년까지 파고 MDR 센터가 실제 현장에서 탐지·대응한 사례와 글로벌 보고서를 상호 검증해 종합 분석한 데이터를 기반으로, 기업이 2026년 이후 보안 운영 모델을 어떻게 설계해야 하는지 제안한다.

이 보고서를 통해 기업은 다음의 세 가지 질문에 대한 답을 구할 수 있다.

Q1. 실제 공격 과정에서의 '결정적 순간(Critical Moment)'은 무엇인가?

Q2. 경영 관점에서 보안 운영은 어떤 점에 집중해야 하는가?

Q3. 2026년 이후 보안 운영 모델은 무엇인가?

이 보고서를 통해 2026년 이후 보안전략 수립을 위한 중요한 기준점을 찾고, AI로 인해 전례 없는 속도와 범위로 전개되는 위협을 효과적으로 관리할 수 있는 최적의 운영모델을 설계하기를 바란다.

파고네트웍스 대표이사 **권영목**

2025 글로벌 위협 환경

2025년의 글로벌 위협 환경은 단순히 '공격이 증가했다', '위협이 정교해졌다'는 수준으로 표현할 수 없는 변화의 연속이었다. 새로운 관점의 공격 패턴이 등장하고, 예상하지 못한 영역까지 공격표면이 확대되었다.

무엇보다 중요한 변화는 '속도와 비용'이다. 사이버 범죄 조직은 AI와 자동화 기술을 사용해 광범위한 영역에서도 빠르고 정확하게 타깃 맞춤형 공격을 진행한다.

특히 2025년은 공격의 대규모 자동화가 본격적으로 시작된 해로, 공격자는 다음과 같은 자동화 도구와 기술을 이용해 공격 효과를 높인다.

- 자동화된 대규모 인증 시도 도구
- 정교한 스캐닝·PoC 적용 자동화 도구
- 공격 대상 기업의 자산 구성 자동 수집
- 깃허브·SaaS·CI/CD 환경의 비정상 키 탐색
- 디스인포메이션·봇넷 기반 협박 메시지 자동 생성

공격 도구 및 전술·전략 변화

2025년 파고 MDR이 대응한 침해사고 분석 결과, 공격자가 유효한 VPN 계정을 통해 내부에 침투한 시점부터 전사적인 랜섬웨어 배포까지 단 48시간밖에 걸리지 않았다.

글로벌 조사 보고서에서도 빠르게 전개되는 공격을 경고한다. '크라우드스트라이크 글로벌 위협 리포트(GTR) 2025'에서는 공격자가 초기 접근 권한을 획득한 후 침입하고 확장하는데 걸린 시간이 평균 48분, 가장 빠른 시간은 51초라고 분석했다.

보안 탐지를 쉽게 우회하면서 신속하게 목표 시스템에 도달하기 위해 공격자들은 다음의 방법을 사용한다.

▪ 알려지지 않은 위협(Unkown Threat)

2025년 위협 패턴에는 정상행위처럼 위장하는 새로운 공격 방식이 등장했다. 정상 사용자 계정으로 수행되는 비정상적인 행위, 정상적인 사용자 행위 범위에서 발생하지만 매우 빠르게 전개되는 내부 이동, 노출된 자산을 악용하는 비인가 자동화 스크립트 등 기존 보안 기술로는 탐지하지 못하는 위협 행위가 나타났다. 이러한 행위를 모두 공격이라고 단정하고 차단할 수는 없기 때문에 상황과 맥락에 따라 위험도를 평가하고 그에 맞게 조치하는 새로운 보안 방식이 필요하다.

▪ 합법적인 자격증명 탈취

합법적인 자격증명을 탈취하는 것이 침해의 기본 경로가 되고 있다. 명확한 물리적인 보안 경계가 사라진 클라우드 시대에는 아이덴티티가 '새로운 보안 경계'가 되고 있기 때문이다. '버라이즌 데이터 침해 조사 보고서(DBIR) 2025'에서는 침해사고의 75~86%가 '도난된 계정'에서 시작되며, MFA를 사용하지 않는 계정에 대한 공격 성공률은 2023년 대비 2.3배 증가했다고 분석한다.

자격증명을 이용하면 정교한 침투 기술이 필요 없으며, 정상

적인 권한으로 접근하기 때문에 비정상 로그가 남지 않고, 공격 초기 단계에서 매우 빠르게 내부 확산이 가능하다. 특히 클라우드 접근 키 하나만 탈취되어도 전체 SaaS·IaaS·CI/CD 환경이 연쇄적으로 침해될 수 있다.

실제로 2025년 한 해 동안 발간된 '파고 딥액트 주간 위협 인텔리전스 리포트'에서도 공격자들은 초기 단계에서 자격증명 수집에 집중하는 것으로 나타난다. 파고 고객 환경에서 탐지·차단된 위협의 70% 이상이 정보탈취를 위한 인포스틸러, 원격 액세스 트로이 목마(RAT)였다.

특히 서비스형 멀웨어(MaaS: Malware-as-a-Service) 방식으로 광범위하게 유포되는 AgentTesla, FormBook, Remcos RAT 등이 주를 이뤘다. 이 악성코드는 특정 표적을 정밀 타격하는 것이 아니라 대규모 스팸·피싱 등으로 무차별적으로 퍼지며, 감염된 시스템의 웹 브라우저, 이메일 클라이언트, VPN 소프트웨어에 저장된 자격증명을 탈취해 C2 서버로 전송한다.

▪ 합법적인 도구 악용

공격자는 EDR과 같은 고급 탐지 기술을 회피하기 위해 LotL(Living off the Land) 전술을 사용한다. 이는 시스템에 기본 내장된 도구나 기능, 상용 원격관리 기술 등 합법적인 도구를 악용하는 것이다. 공격자는 별도의 비용 없이 보안 탐지를 피하면서 침투한다. 그러나 기업은 합법적인 도구에서 발생하는 비정상 행위를 더 정교하게 찾아내야 하기 때문에 정교한 고급 보안 기술에 더 많이 투자해 탐지와 분석을 고도화해야 한다.

파고 MDR이 2025년 대응한 가장 피해가 큰 침해 사고를 보면, 공격자는 VPN, RDP, net.exe, PsExec 등 윈도우 환경에서 광범위하게 사용되는 합법적인 관리 도구나 정상적인 행위처럼 간주되는 도구를 사용했다. 이외에도 공격자가 침해된 시스템에 애니데스크, 크롬 리모트 데스크톱, 팀뷰어 등 상용 원격관리 도구를 설치한 후 C2 채널 및 영구적인 백도어로 활용하는 사례도 다수 확인되었다.

파고 MDR이 탐지한 사건 중 마이크로소프트 서명이 있는 합법적인 드라이버 PROCEXP152.sys의 취약점을 악용한 사례도 있다. 합법적인 서명이 있는 드라이버의 활동이기 때문에 기존 보안 솔루션은 그 이상행위를 탐지하지 못한다.

공격자의 목표는 커널 메모리에 직접 접근해 커널 레벨에서

파고 딥액트 2025년 Top 10 위협 TTPs

2025년 파고 MDR이 실제 침해 사고 및 위협 헌팅을 통해 탐지한 가장 빈번하고 위험도가 높은 행위 기반 TTPs는 다음 표와 같다.

순위	TTP	설명
1	T1505.003: Web Shell	IIS(w3wp.exe) 또는 Exchange OWA 프로세스를 통해 원격 명령 실행
2	T1059.001: PowerShell	Invoke-WebRequest 등 악성 스크립트 실행, 방어 정책 우회
3	T1078: Valid Accounts	탈취된 VPN, RDP, AD 계정을 사용해 시스템에 정상 로그인
4	T1003.001: LSASS Memory	Mimikatz, NLBrute 등을 이용한 LSASS 메모리 덤핑 및 자격증명 추출
5	T1490: Inhibit System Recovery	vssadmin 등을 이용한 볼륨 섀도우 복사본 삭제(랜섬웨어 전조)
6	T1548.002: UAC Bypass	ConsentPromptBehaviorAdmin 레지스트리 수정을 통한 UAC 무력화
7	T1053.005: Scheduled Task	작업 스케줄러를 통한 악성 스크립트/프로그램 지속성 확보
8	T1021.001: Remote Desktop Protocol	RDP를 이용한 내부 측면 이동(Lateral Movement)
9	T1059.003 / T1087: Command Shell	sqlservr.exe가 cmd.exe를 실행, net group 등 정찰 명령어 수행
10	T1218: System Binary Proxy Execution	certutil 등 합법적 시스템 바이너리(LOLBin)를 이용한 C2 페이로드 다운로드

제조 기업의 RDP 노출 자산 선제 차단

2023년부터 2025년까지 파고 MDR이 탐지한 제조·에너지·식음료 기업의 IT·OT 환경에서 매우 위험한 노출 요소중 하나는 외부로 열려 있는 RDP 포트였다. 파고 MDR의 선제적인 위협 대응 프로세스는 기업 환경을 스캔해 무단으로 열려있는 RDP를 찾아 조치해 피해 발생 전에 예방했다. 제조 기업 A사는 외부에 노출된 RDP 자산이 자동화 스캐너에 의해 반복적으로 탐색되고 있었는데, 해당 이벤트를 단순 스캐닝으로 분류해 위험성을 낮게 판단하고 있었다. 파고 MDR은 이 이벤트가 단순 스캐닝이 아니라고 판단하고 RDP 포트를 차단하고 피해를 예방했다.

파고 DeepACT MDR 대응 프로세스

1. EASM으로 노출 자산 식별
   - 평소와 다른 시간대에 외부에서 RDP 포트를 통해 접근
   - 동일 IP 대역에서 수십 건의 로그인 시도 발생

2. 위협 헌팅으로 공격 의도 분석
   - 사용자 에이전트 분석 → 자동화 도구(Bot) 패턴 확인
   - 동일 해커 그룹이 다른 산업에서도 활동 중임을 확인

3. 검증 단계에서 위험도 재분류
   - 단순 스캔이 아닌 '자격증명 기반 초기 침투 노력'으로 판단
   - 우선순위 상향

4. 자동 차단, 규칙 기반 격리
   - RDP 포트 임시 차단
   - 화이트리스트 기반 접근 재정의
   - 방화벽 정책 수정

파고 MDR의 선제적 대응을 통해 공격자는 인증 단계까지 도달하지 못했으며, 기업의 생산 설비·제조 시스템에 영향 없이 위험을 차단했다.

EDR 솔루션이 작동하는 데 필수적인 사용자 모드 API 후킹을 제거하고, EDR의 보호된 프로세스를 강제로 종료시키는 것이었다. 파고 전문가의 위협 헌팅을 통해 비정상적인 드라이버 로드 및 커널 레벨의 행위를 탐지하고 고도의 회피 기술을 사전에 차단할 수 있었다.

▪ 섀도우 AI·섀도우 IT

AI 사용이 급증하면서 승인되지 않은 AI 도구, 자동화 스크립트, 개인용 AI 앱 등 섀도우 AI로 인한 위협이 크게 증가하고 있다. 외부 SaaS와 연동되는 AI 봇 역시 관리 사각지대에 놓이기 쉽다.

섀도우 AI로 인해 발생할 수 있는 위협은 ▲외부 API 키 유출 ▲학습 데이터에 포함된 민감 정보 노출 ▲LLM 기반 자동화 스크립트의 오남용 ▲SaaS 간 무단 연결에 의한 계정 권한 상승 등을 들 수 있다.

특히 AI 스크립트가 SaaS를 자동으로 연결해 정상 업무 흐름으로 위장하면서 민감 데이터를 전송하면 로그에서는 합법적인 활동으로 보이기 때문에 탐지하기 어렵다.

섀도우 AI 뿐만 아니라 다양한 디지털 자산이 관리조직의 승인 없이 무단으로 사용되면서 섀도우 IT를 크게 확장시키고 있다. 섀도우 IT의 취약점이나 잘못된 설정, 섀도우 IT에 방치된 데이터와 자격증명 등은 쉽게 침투할 수 있는 유용한 도구가 된다.

▪ 확장되는 공격표면

섀도우 IT, 잘못된 설정이나 패치되지 않은 취약점, 방치된 계정 정보와 자격증명 등은 공격자가 침입할 수 있는 공격표면(Attack Surface)이 된다. 비즈니스 확장으로 다양한 유형의 IT 자원이 사용되고, 원격·하이브리드 업무 환경이 도입되면 관리 사각지대가 늘어나고 공격표면이 확장된다. 공격자는 아주 간단

한 스캐닝만으로도 목표 시스템에 침입할 수 있다.

파고 MDR의 대응 사례에서도 충분히 관리할 수 있었던 공격 표면에서 위협이 시작된 경우를 다수 볼 수 있다. 파고 사고 대응 데이터에서 나타나는 핵심적인 노출 지점은 다음과 같다.

- 인터넷에 직접 노출된 RDP 포트는 브루트포스 공격 표적이 됨
- 패치되지 않은 MS 익스체인지 서버 또는 보안이 취약한 웹 애플리케이션은 웹셸 업로드 및 내부 정찰의 발판으로 악용됨
- 추측하기 쉬운 취약한 데이터베이스 패스워드는 공격자에게 즉각적인 RCE 권한을 부여함

▪ 취약한 공급망

2025년에는 공급망 리스크가 전 세계, 모든 산업군으로 확장됐다. 공격자는 특정 시스템의 취약한 지점을 정조준하기보다, 공급망의 취약한 지점으로 침투한 후 공급망 생태계 전체를 감염시켜 더 광범위한 피해를 발생시키고 있다.

'IBM 2025년 데이터 유출 비용(CODB) 보고서'에 따르면 공급망을 통한 2차 피해 비용이 1차 피해보다 평균 30% 더 높은 것으로 나타난다. 실제로 2024~2025년 사이 APAC 지역에서는 노출된 SaaS 계정, 토큰 탈취, 클라우드 IAM 권한 오남용을 활용한 2차 확산형 공격이 폭발적으로 증가했다.

특히 APAC 지역은 다음 두 가지 특징으로 인해 더욱 심각한 공급망 위협에 직면해 있다.

- 중소 규모 MSP·MSI 및 SaaS 리셀러에 대한 의존도
- IT·OT, 본사·지사, 내부·외부 시스템의 혼재된 구조

높아지는 공격자 수익률

사이버 범죄 조직은 시간과 비용을 효율적으로 투자해 높은 수익을 얻으려고 하기 때문에 더 쉽게 침투해 목표를 달성할 수 있는 조직을 찾는다. APAC 지역의 제조산업은 공격자가 가장 좋아하는 타깃으로, IT·OT 수준에 비해 보안 대책은 충분하지 않아 비교적 쉽게 침투할 수 있으며, 높은 수익을 얻을 수 있다.

▪ 수익성 높은 제조업 대상 공격

제조산업은 첨단기술을 적극적으로 도입하면서 AI·클라우드 혁신을 이루고 있지만, 수십년 된 레거시 설비도 여전히 운영하고 있다. 오래된 설비는 보안 패치, 펌웨어 업데이트가 제대로 되지 않아 보안에 매우 취약한 상태인데, 별도의 보안 조치 없이 AI·클라우드를 적용하면서 외부 연결 접점이 늘어나 공격표면이 크게 확장되고 있다.

우리나라를 포함한 APAC 지역에는 첨단 반도체·자동차 제조사가 집중되어 있는데, 충분한 보안 고려 없이 AI·클라우드 혁신을 진행하고 있어 공격당하기 매우 쉬운 환경이 되고 있다. 또한 APAC 지역은 클라우드 도입 속도가 매우 빠르기 때문에 보안 설정 오류, 구성 실패, 제대로 관리되지 않은 자산 등 클라우드의 취약성을 이용한 공격 빈도가 높아지고 있다. 파고 MDR 데이터에 따르면, APAC 지역 기업의 클라우드 구성 오류에서 비롯한 복합적인 침해 비용이 미국보다 훨씬 높은 것으로 나타난다.

▪ 공급망 피해 높은 APAC 지역

APAC 지역은 글로벌 공급망 생태계의 중심에 있기 때문에 이 지역 제조사를 공격하면 글로벌 공급망 전체를 위험에 빠뜨릴 수 있다. 코로나19 동안 중국의 제조공장이 운영을 중단하자 전 세계 모든 산업의 공급망이 정지되었던 사례가 있다.

이러한 현실을 파악하게 된 공격자들은 공격 타깃을 미국에서 APAC 지역으로 돌리고 있다. APAC 제조산업은 IT-OT 융합 환경이 빠르게 성장하고 있지만, 보안 성숙도는 높지 않으며, 쉬운 공격 기술로도 광범위한 공급망 피해를 일으킬 수 있기 때문이다. 특히 중소규모 공급망 사업자들은 보안 수준이 충분하지 않으며, 국가별로도 보안 품질 차이가 크기 때문에 공격이 훨씬 쉽다.

실제로 파고 MDR 센터에서 탐지한 표적 공격 중 이 분야를 노린 공격 시도가 60%를 차지해 APAC 지역 제조사에 대한 보안 대책이 시급한 상황이다.

▪ 복잡한 규제·허위정보 악용

사이버 침해가 산업과 국가 안보를 위협하게 되자 우리나라를 포함한 세계 여러 국가들은 사이버 보안 규제를 강화하면서 대응

책 마련에 나서고 있다.

특히 심각한 사고 시 막대한 벌금과 과징금을 부과하는데, 유럽연합(EU)의 일반 데이터 보호 규정(GDPR)의 경우 연간 전 세계 매출의 4%, NIS2 지침은 2%의 벌금을 부과한다. 우리나라 개인정보보호법은 최대 3%의 과징금을 부과한다. 미국의 경우 상장사가 침해 사실을 인지한 후 증권거래위원회(SEC)에 신고하지 않으면 최대 상장폐지까지 당할 수 있다.

그러자 공격자는 '규제갈취(Regulation Extortion)'라는 새로운 방식으로 더 높은 수익을 얻고 있다. 침투에 성공한 후 피해 기업에게 "침해 사실을 관계기관에 제대로 신고하지 않으면 막대한 벌금을 부과받을 것"이라는 내용으로 공격자에게 돈을 주고 무마하라고 협박하는 방식의 공격이다.

규제에 대한 이해가 낮은 기업뿐만 아니라 규제 대응이 비교적 잘 되어 있는 기업조차 이러한 협박에 끌려다니게 된다. 특히 해외 사업을 하는 기업 중 일부는 해당 국가의 규제를 정확하게 파악하지 못해 공격자의 요구를 들어주게 된다.

허위 정보를 이용해 평판을 악화시키는 공격도 빈번해지고 있다. SNS, 인터넷 등을 이용해 기밀정보·고객정보를 대규모 탈취했다고 거짓으로 폭로하거나 기타 허위정보를 유포해 기업의 신뢰를 훼손시키는 방식이다. AI로 인해 언어와 문화의 장벽이 사라지자, 고유의 언어·글자를 사용하는 아시아 국가들도 허위 정보로 인한 피해를 입고 있다.

수익 극대화 위한 공격 생태계 진화

공격자들은 수익을 극대화하기 위해 공격 전술·전략·도구와 생태계를 끊임없이 개선하고 있다. 초보적인 기술을 사용하면서도 교묘한 방법으로 보안 탐지를 우회하며, 피해자의 심리를 악용해 수익을 극대화한다.

데이터를 암호화 하기 전에 먼저 유출하고, 이를 공개하겠다고 협박하는 동시에 클라우드 백업을 삭제하면서 피해 조직이 대응할 시간을 주지 않고 협상에 임할 수밖에 없도록 만들고, 피해 기업의 매출과 사이버 보험 여부, 규제와 소송 시 발생하는 피해액 등을 알리면서 그보다는 낮은 비용으로 피해 사실을 무마해주겠다고 회유하기도 한다.

그러나 공격자의 요구를 들어준다고 해서 피해를 온전히 복원할 수 있는 것은 아니며, 다시 공격당하는 비율도 매우 높다. 사이버리즌 조사에 따르면 랜섬머니를 지불한 조직의 78%가 두번째 랜섬웨어 공격을 받았으며, 이 중 63%는 두번째에서 더 높은 금액을 요구받았다. 두번째 공격의 36%는 동일한 공격자였다. 돈을 지불한 조직 중 47%만이 손상없이 복구할 수 있었던 것으로 분석됐다.

이러한 공격 방식은 '랜섬웨어 대응을 위해 백업 시스템을 잘 갖춰야 한다'는 전통적인 대응 전략을 무용지물로 만든다. 피해 기업은 랜섬웨어로 인한 직접적인 피해뿐만 아니라 고객 이탈, 평판 하락, 규제 리스크까지 부담해야 하며, 고객으로부터 집단 소송을 당할 수도 있다.

공격 기술 아닌 공격 패턴 변화

2025년은 사이버 위협 패턴의 전면적인 변화가 시작된 해로, 공격 속도가 매우 빨라지면서도, 다수 대중을 대상으로 한 광범위한 공격, 정교한 타깃 맞춤형 공격까지 전방위적으로 발생하고 있다.

2025년 파고 MDR이 탐지한 위협 사례와 글로벌 보고서에서 주목한 위협 트렌드를 종합한 핵심 메시지는 다음과 같다.

- 공격은 더 지능화되었을 뿐만 아니라 더 빨라졌다.
- 공격표면은 우리가 인지하지 못했던 곳에서 폭발적으로 증가하고 있다.
- 자격증명 탈취가 모든 공격의 기본 경로가 되고 있다.
- 공급망은 더 작은 조직을 먼저 노린 뒤, 더 큰 조직으로 확산한다.
- 섀도우 AI는 새로운 공격표면이다.
- 랜섬웨어는 암호화보다 평판 공격 중심으로 이동하고 있다.
- 자동화된 공격과 수동 대응 간의 격차는 점점 더 커지고 있다.

3년간의 인사이트(2023~2025년)

2020년 1월부터 2023년 5월까지 3년 4개월 동안 이어진 글로벌 팬데믹은 사이버 위협 환경을 완전히 바꾸어놓았다. 보안의 경계가 클라우드로 확장되면서 '보호해야 할 내부 네트워크'의 개념이 희미해졌다. 기업의 자산이 클라우드, MSP 및 기타 서드파티와 연결되면서 공격표면이 확장됐고, 점점 더 복잡해지는 하이브리드 환경에서의 권한 및 구성 오류로 인한 침해 가능성이 높아졌다.

팬데믹 이후 이어진 AI 혁신은 위협 환경의 변화를 한층 더 가속화했다. 에이전틱 AI와 AI를 탑재한 애플리케이션 증가로 조직의 관리 범위를 벗어나는 AI 영역이 빠르게 늘어나고 있다.

반면 보안은 기존 보안 시스템을 유지하면서 새로운 위협 환경에 대응해야 한다는 이중의 고통을 안고 있다. IT, OT, 클라우드가 서로 연결되어 있음에도 불구하고 보안은 각각 별도로 구축된 체계와 프로세스를 따르기 때문에 정보가 제대로 공유되지 않는다. 그래서 초기 침투부터 확장까지 전체 공격 주기를 가시화하고 제대로 대응하기 어렵다.

전통적인 탐지 기술 한계

파고 MDR을 통해 탐지한 최근 3년간의 위협 동향과 글로벌 전문기업의 조사보고서를 분석해보면 '기술이 아니라 방법'에 방점을 두어야 한다는 결론에 이르게 된다.

그러나 현재 SOC는 단순한 이벤트 분석과 알림 처리에 머무르고 있기 때문에 보안을 우회하며 속도감 있게 전개되는 공격을 막는데 제약이 있다.

현재 SOC가 갖고 있는 한계는 다음과 같다.

▪ EDR 탐지 우회하는 신원 기반 공격

신원 기반 공격(Identity Attack)은 단순한 계정 탈취를 넘어 무단 권한 상승, 세션 하이재킹, 토큰 재사용, SaaS 로그인 악용 등 ID를 악용하는 모든 공격 행위를 포함한다. 새로운 보안 경계가 된 ID에 공격이 집중되고 있다.

2023년부터 2025년까지 신원과 관련된 공격의 변화 추이는 다음과 같다.

- 신원 기반 공격 관련 이벤트 약 2.8배 증가
- 클라우드·SaaS 접근 권한 악용 시도 2.5배 증가
- 정상 계정으로 위장한 내부 이동 시도 70% 증가

정상 신원 악용 공격은 EDR을 우회하는 대표적인 수법이다. EDR은 엔드포인트 위협 탐지에는 탁월하지만, 정상계정을 이용한 접근을 막지 못한다. 그래서 2026년에는 ITDR (Identity Threat Detection and Response), 권한 기반 리스크 스코어링, SaaS 접근 패턴 분석이 필수 운영 요소로 재편될 것이다.

▪ 시그니처·패턴 기반 탐지의 한계

시그니처와 패턴 기반 탐지는 알려지지 않은 위협(Unknown

정상 사용자 계정 악용한 알려지지 않은 위협

파고 MDR은 2025년 상반기, 한 금융 서비스 기업에서 정상 사용자 계정의 이상 동작을 탐지했다. 이 행위는 그동안 사용자가 수행해 온 업무 패턴과 다른 정황으로 진행되었지만, 시그니처 기반 보안 솔루션으로는 탐지되지 않는 범위에 있었다.

파고 DeepACT MDR 대응 프로세스

1. 맥락 기반 탐지(Context-Driven Detection)
   - 로그인은 정상 위치에서 이뤄졌으나, 기존 업무 패턴에서 나타나지 않았던 특정 파일 접근 시도 탐지
   - 해당 계정의 '정상 근무 시간 외 활동' 감지

2. 정상 사용자의 과거 행태와 비교 검증
   - 30일간 행위 패턴 분석
   - 비정상 파일 다운로드 경로 발견

3. 위협 헌팅 시작
   - 샘플 파일 해시 분석
   - 다른 사용자 계정과 연관성 조사
   - 원격 명령 실행 흔적 탐색

4. 초기 자동 격리 → 보안팀 협업 → 최종 정리
   - 의심 파일 접근 차단
   - 계정 일시 잠금
   - SecOps와 IR 팀의 공동 대응

분석 결과, 공격자는 정상 사용자 계정을 탈취해 내부 중요 데이터에 접근하려 한 것으로 확인되었다. 파고 DeepACT MDR이 초기 단계에서 이상행위를 차단해 공격자가 데이터에 접근하지 못했다.
이처럼 알려지지 않은 위협은 탐지 기술만으로 식별할 수 없다. 맥락(Context) + 헌팅(Hunting) + 즉각 대응이 결합된 MDR을 통해 성공적으로 조치할 수 있다.

Threat)을 이용하는 공격을 막지 못한다. 가장 자주 탐지되는 알려지지 않은 위협의 예시는 다음과 같다.

- 정상 행위처럼 보이지만 맥락(Context)이 다른 이벤트
- 정식 사용자 계정으로 수행된 비정상적 로그인 시도
- 내부 이동이 정교하지 않으나 속도가 빠른 공격
- 노출 자산을 악용한 비인가 자동화 스크립트

파고가 자체 수집한 데이터와 크라우드스트라이크 조사 결과를 종합하면, 알려지지 않은 위협이 증가하게 된 원인을 다음과 같이 정리할 수 있다.

- **자동화된 공격 확산:** PoC(Proof of Concept) 기반 공격 스크립트가 대량 유통되면서 개별 공격 패턴이 일정하지 않고 '비정형적 행동'을 보임
- **섀도우 AI·비관리 자동화 확산:** AI 기반 스크립트·SaaS 간 자동 연결 도구는 정상 행위로 위장되기 때문에 파일 해시, 패턴 매칭 기반 탐지가 어려움
- **신원 기반 위협 증가:** 합법적 계정을 사용하는 공격은 시그니처·패턴 기반 탐지를 무력화함

▪ 단축되는 TTE(Time-to-Exploit)

모든 시스템과 애플리케이션에는 취약점이 있다. 그래서 보안 연구자와 화이트해커들은 알려지지 않은 취약점을 찾아 악용 가능성을 테스트하며, 그 과정과 결과에 대한 PoC를 커뮤니티에 공개한다. 이는 다른 연구자나 개발사에서 검증하고 빠르게 보안 패치나 보안 권고를 배포하도록 돕는 필수적인 활동이다.

문제는 PoC가 공격자의 익스플로잇 개발 비용과 시간을 크게 단축시킨다는 점이다. 공격자는 PoC가 게시되면 이를 악용하기 위한 시도를 '즉시' 시작한다.

최근 국내외 보안업계와 주요 보안업체의 침해 사례 분석에 따르면, PoC 공개 후 익스플로잇 시도까지 소요되는 시간은 몇 주에서 며칠, 혹은 몇 시간대로 단축되는 추세가 뚜렷하게 나타나고 있다. 클라우드플레어는 PoC 공개 후 공격을 개시하기까지

단 22분밖에 걸리지 않았던 사고도 공개한 바 있다.

TTE가 단축되면서 보안팀이 패치 공지를 이해하기도 전에 공격자가 악용할 수 있게 됐으며, 이로 인해 제로데이 취약점 공격 빈도와 성공률이 높아지고 있다.

취약점에 빠르게 대응하기 위해 보안 조직은 AI 기반 실시간 취약점 스캐너를 이용하고 있지만, 방대한 IT 시스템에서 취약점의 영향을 받는 요소를 찾기 쉽지 않다. 또한 취약점 영향을 받는 요소가 시스템 내에 압축되어 있거나 파편화되어 있어 탐지되지 않는 경우도 많다.

패치로 인한 추가적인 문제가 발생할 수도 있어, 패치 전에 반드시 충분히 검토하고 테스트해야 한다. 예를 들어 WAN-facing 서비스는 사실상 실시간에 준하는 패치 적용 속도를 요구하지만, 서비스 연속성을 우려하는 관리자는 실시간 패치에 소극적일 수밖에 없다.

이처럼 비즈니스 연속성을 고려해야 하는 보안은 취약점 대응 속도를 높이는데 분명한 제약을 받고 있다. 그러나 범죄자들은 자동화된 취약점 탐지 도구를 이용해 거의 실시간으로 취약한 시스템을 찾아 공격할 수 있다. '메타스플로잇(Metasploit)'과 같은 상용화된 침투테스트 도구를 사용하면 별도의 취약점 스캐닝 도구를 개발하지 않고도 효과적으로 공격을 진행할 수 있다.

이러한 문제를 해결하기 위해서는 패치 관리 작업을 '운영 작업(Operation Task)'이 아니라 '위험 감소 전략(Risk-Reduction Strategy)'으로 격상시켜야 한다. 새로 공개된 취약점의 악용 가능성을 파악하고 우선순위에 따라 조치하는 한편, 지속적인 위협 노출 관리(CTEM) 전략을 통해 제거되지 않은 취약점이나 공개된 노출표면을 찾아 제거함으로써 위험을 줄여나가야 한다.

사고 대 침해 비율(IB Ratio)

글로벌 위협 인텔리전스와 파고 MDR의 실제 사고 대응 사례를 종합해보면, 탐지가 이루어졌음에도 대응 지연으로 인해 피해로 이어지는 사례가 계속 보고되고 있다. 이를 '사고 대 침해 비율(IB Ratio: Incident-to-Breach Ratio)'이라고 하는데, ▲탐지했지만 대응이 늦었거나 ▲탐지된 정보의 컨텍스트가 부족해 대응하지 못했기 때문에 발생하는 사고다.

실제로 파고 MDR에서 탐지한 사건 중 초기 경보(Alert)가 발생했음에도 운영 공백·절차 지연·승인 프로세스 문제 등으로 대응이 늦어져 실제 침해로 이어진 사례가 적지 않았다.

이는 다음과 같은 전통적인 SOC의 한계에서 비롯된다.

- **이벤트 중심 구조(Event-Centric Architecture):** 룰·서명에 의존해 알려지지 않은 위협과 신원 기반 공격 탐지 어려움
- **경보 처리 중심(Alert Handling Process):** 경보 → 티켓 생성→ 분석→ 고객 통보→ 후속조치 과정을 거치면서 공격 속도보다 한참 뒤처진 대응
- **부분 운영(Partial Operation):** 24/7 모니터링을 수행하더라도 24/7 판단·격리·조치는 불가능한 경우가 많음
- **분리된 기능 조직:** 모니터링, 침해대응, 위협 인텔리전스가 분리되어 있어 의사결정과 실행 사이에 지연 발생

따라서 위협을 '탐지' 하는 것만으로는 충분하지 않으며, 탐지된 위협을 실시간 검증하고 대응하는 체계가 반드시 갖춰져야 한다.

보안 투자의 효율성

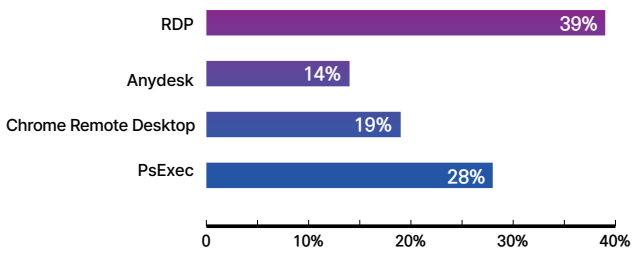
사이버 위협에 대응하기 위한 기업의 투자는 지속적으로 늘어나고 있지만, 침해로 인해 발생하는 비용을 줄이지 못하고 있다. 포레스터는 전 세계 사이버 보안 지출이 2024년 1546억달러에서 2025년 1748억달러로 13.1% 증가할 것으로 예상했으며, 이후에도 매년 두 자릿수 이상 성장해 2029년 3025억달러에 이를 것으로 예측했다.

이러한 투자가 침해 비용을 낮추는 결과로 이어지지는 않고 있다. 'IBM CODB'에서 분석한 평균 침해 비용은 2025년 444만달러로, 2024년 488만달러에 비해 9% 감소했지만, 2023년 445만달러와 비슷한 수준이다.

특히 APAC 지역에서는 공급망 연쇄 피해, 규제위반 리스크, 클라우드 구성 오류 등의 문제가 복합적으로 작용해 침해 비용이 미국보다 22% 높은 것으로 나타난다.

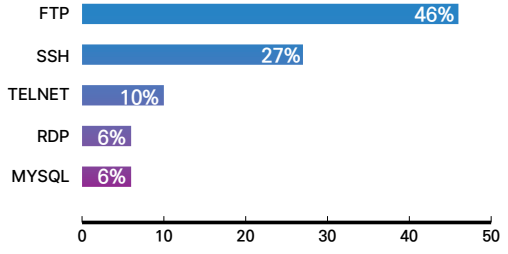
파고는 침해 비용을 낮추지 못하는 이유를 다음과 같이 분석한다.

〈그림 1〉 공격에 사용된 합법적인 원격 접속 도구



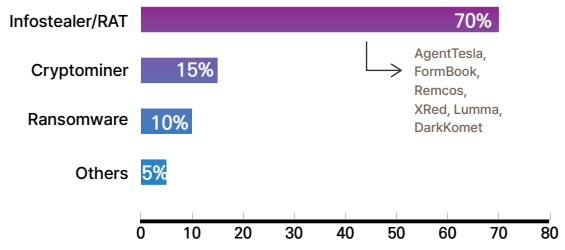
(출처: PAGO DeepACT Threat Intelligence)

〈그림 2〉 표적이 되는 공격 표면



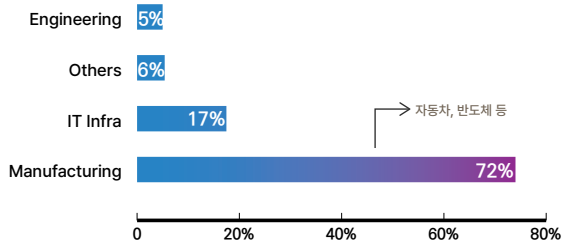
(출처: PAGO DeepACT CTEM Database)

〈그림 3〉 탐지된 악성도구 유형



(출처: PAGO DeepACT Threat Intelligence)

〈그림 4〉 산업별 침해사고 비중



(출처: PAGO DeepACT Compromise Report)

분업을 통한 지하 경제 활성화

지하시장은 점점 더 분업화되어 생태계 전반을 효율화하고 수익성을 높이고 있다. 2025년 파고의 위협 인텔리전스(TI) 데이터를 분석해보면, 하나의 조직이 공격의 모든 단계를 수행하는 것이 아니라는 점을 알 수 있다.
실제로 파고는 2025년 대량의 인포스틸러와 침해사고대응(IR)에서 확인된 '유효한 계정(Valid Accounts)' 사용 간의 강력한 인과 관계를 확인했으며, 이것이 분업화된 지하시장을 보여주는 증거가 된다고 확신한다. 또한 이러한 지하시장의 질서를 통해 공격그룹은 랜섬웨어를 고도로 전문화하고, 확장시키고 있다고 분석한다.
현재 지하시장은 ▲자격증명 탈취(Infostealer)를 전문으로 하는 그룹 ▲초기 침투 및 접근권 판매(Initial Access Broker)를 전문으로 하는 그룹 ▲랜섬웨어 배포(RaaS: Ransomware as a Service)를 전문으로 하는 그룹 등 여러 그룹이 협력해 활동하고 있으며, 이익을 공유하는 고도로 분업화된 생태계를 완성하고 있다.

고도로 분업화되는 공격 생태계

분업화된 공격 생태계는 다음과 같은 4단계를 통해 작동한다.

- **자격증명 수집(Credential Harvesting):** AgentTesla, Lumma Stealer와 같은 인포스틸러가 대량의 피싱 메일을 통해 불특정 다수에게 유포한다.
- **접근권 판매(Access Brokerage):** 탈취된 수많은 RDP, VPN, AD 자격증명은 다크웹 마켓플레이스에서 'Initial Access Broker'를 통해 상품화되어 판매한다.
- **접근권 구매(Access Acquisition):** 락비트(LockBit)와 같은 RaaS 운영 조직은 특정 기업(예: 제조업, IT 인프라)의 유효한 내부 접근 권한을 구매한다.
- **침해 및 수익화(Intrusion & Monetization):** RaaS 그룹은 구매한 유효한 계정을 사용해 타깃 기업 내부에 정상적으로 로그인한다. 이는 전통적인 방화벽이나 침입 탐지 시스템(IDS)을 완벽하게 우회하며, 내부 사용자의 정상 활동처럼 보인다. 이후 이들은 섀도우 복사본 삭제, 랜섬웨어 배포 등 최종 공격을 수행한다.

- 초기 탐지 실패보다 대응 지연이 더 큰 비용을 발생시킨다.
- 클라우드·SaaS 환경에서는 피해 확산 속도가 빠르다.
- 평판·법적 분쟁 비용이 전체 비용에서 차지하는 비중이 증가하고 있다.
- 데이터 유출 후, 고객 이탈률(Attrition Rate)이 반복적으로 늘어난다.

침해 비용을 낮추기 위해 반드시 개선해야 하는 것이 '운영 속도(Operation Speed)'이다. 다음 3가지 요소의 통합 정도에 따라 운영 속도가 달라진다.

1. **탐지 속도(Detection Speed):** AI 기반 상관분석·정규화를 통한 자동화로 탐지 속도 개선
2. **판단 속도(Decision Speed):** 탐지한 위협의 수준을 검증할 수 있는 인텔리전스와 전문 애널리스트의 역량을 결합해 판단 속도 개선
3. **격리 속도(Containment Speed):** 24/7 운영 체계와 자동화된 운영 절차를 통해 확실한 위협을 빠르게 격리

보안 운영 모델의 변화

2026년 기업은 정교한 공격기술 뿐만 아니라 복잡한 운영환경과 빠른 공격속도에 대응하지 못하는 상황으로 인한 도전을 받게 될 것이다. 침투부터 확산까지 진행되는 시간이 점점 짧아지면서 보안의 '골든타임(Golden Time)'이라는 개념이 사라지고 있으며, 공격을 막을 수 있는 '결정적 순간(Critical Moment)'을 포착하는 것도 쉽지 않게 됐다. 그래서 보안 운영은 개별 이벤트를 찾아 제거하는 수준에서 벗어나 '경영 지표(Business Resilience Metrics)'의 한 요소로 격상되고 있다.

보안을 경영 지표로 삼기 위해서는 기업의 지속 가능성 향상과 직접적으로 연결되는 KPI를 수립해야 한다.경영지표가 될 보안의 KPI는 다음과 같다.

- **MTTD(Mean Time to Detect):** 초기 위협 신호를 포착하기까지 걸린 시간으로, 보안 운영체계가 탐지 가능한 상태로 유지되고 있는지 보여주는 지표다. 최근 AI 기반 상관분석·이상행동 탐지 기술로 MTTD는 크게 단축되고 있다.

- **MTTA(Mean Time to Acknowledge):** 경보가 발생했을 때 이를 실제 위협으로 '인지'하기까지 걸린 시간을 말한다. MTTA는 24/7 운영과 경보 우선순위 체계, 검증 프로세스의 성숙도에 의해 결정된다. 운영 체계가 실시간 판단이 가능한 구조를 갖추면 MTTA를 단축시킬 수 있다.

- **MTTR(Mean Time to Respond):** 탐지부터 대응, 격리까지 걸리는 시간으로, 회복력을 나타내는 지표다. 탐지→판단→격리의 각 과정을 분리하지 않고 하나의 구조로 통합한 운영체계를 갖춰야 MTTR을 단축시킬 수 있다. 또한 기술·성능보다 24/7 대응 조직, 자동화 수준, 즉시 판단하고 결정할 수 있는 체계 등의 성숙한 운영방식으로 MTTR을 단축시킬 수 있다.

- **초기 차단 성공 비율(Containment Ratio):** 초기 침투 시도 중 차단에 성공한 비율이다. 이 비율이 높다는 것은 조직이 공격 진행 전 단계에서 자동화된 방어 태세를 갖추었다는 것을 보여준다.

- **노출 감소율(Exposure Reduction Index):** 지속적 위협 노출 관리(CTEM) 기반 운영에 의해 공격표면을 얼마나 줄였는지를 나타내는 지표다. 사후 대응이 아닌 사전 제거 방식으로 위협을 관리하고 있는가를 나타내며, 보안 운영 철학과 프로세스 성숙도를 반영한다.

성숙한 보안 운영 필수 조건

지난 10여 년간 SOC는 '보안의 운영 중심 조직'으로 간주되어 왔으며, 고급 방어 기술을 지속적으로 추가하면서 고도화해왔다. 그러나 SOC는 경보 모니터링, 정형화된 이벤트 분석, 티켓 발행과 후속조치 요청으로 이어지는 선형적인 탐지·대응 모델을 채택하고 있기 때문에, 전장을 넓게 사용하면서 여러 침해 활동을 동시에 진행하는 최근 공격을 차단하는데 한계가 있다.

유출된 자격증명 기반 침해 시도 – 24분 내 격리까지 완료

파고 MDR은 2024년 말 국내 SaaS 기업에 공격자가 유출된 계정을 이용해 클라우드 콘솔 접근을 시도한 것을 탐지했다.
일반적인 보안관제서비스에서 탐지했다면, 로그 기반 탐지 후 티켓 발행→고객 통보→승인→대응의 과정을 거쳐야 하기 때문에 평균 대응 시간이 수 시간에 이른다.
그러나 파고 MDR은 로그인 시도 탐지부터 격리까지 24분 내에 완료했다. 글로벌 평균 대응 시간(MTTR)인 3~6시간보다도 크게 단축한 것으로, 계정 권한 상승 및 내부 이동 시도를 완전히 차단하고 피해를 막았다.

파고 DeepACT MDR 대응 프로세스

1. 로그인 이벤트의 이상 패턴 탐지
   - 정상 사용자 국가와 다른 지역에서 로그인
   - 계정 권한과 무관한 콘솔 기능 탐색
   - 세션 토큰 유효성 검사 반복

2. 검증(Validation) 단계에서 오탐 제거
   - 정상 자동화 스크립트와 패턴 비교
   - 사용자의 업무 패턴과 불일치 검증

3. 분석가의 즉각 판단
   - 크리덴셜 스터핑으로 판단
   - 계정 탈취 위험 판단 후 신속 승인

4. 자동 격리
   - 계정 세션 강제 종료
   - MFA 재등록 강제
   - 위험 IP 자동 차단
   - API Key 무효화

이 사례를 통해 알 수 있는 것은 자격증명 공격은 기술이 아니라 '판단 속도'로 막아야 한다는 점이다. MDR의 검증, 자동화된 대응, 전문가의 판단이 결합되어 공격 확산을 조기에 막을 수 있었다.

빠르게, 그리고 복합적으로 진행되는 공격을 막기 위해서는 전체 공격 주기 관점의 방어 전략이 필요하다. 가트너는 '방어 운영 속도의 결정적 전환기를 맞았다'고 분석하는데, 보안 운영 프로세스, 사람의 개입 속도, 자동화 수준, 위험 의사결정 체계 등 보안 운영의 모든 구조를 다시 설계해야 한다는 것을 뜻한다.

▪ 자동화와 24/7 보안 운영

2025년 이후 보안 전략은 '운영 비용과 손실 비용 사이의 구조적 균형을 어떻게 설계하느냐'에 초점을 맞추고 있다. 특히 보안 투자가 침해 비용 최소화로 이어지도록 하기 위해서는 '자동화 성숙도가 높은 24/7 보안 운영'이 필요하다.

IBM과 가트너의 조사에 따르면 자동화된 24/7 보안 운영 성숙도를 높인 조직은 평균 220만달러를 절감하는 것으로 분석된다. 이는 다음을 합산한 결과다.

- 다운타임 감소
- 생산성 손실 축소
- 규제 벌금 감소
- 클라우드 리소스 폭주 방지
- 고객 이탈 최소화
- 사고 조사 비용 감소
- 법률 대응 비용 절감

▪ '24/7'에 대한 착각

공격자는 자동화를 통해 광범위한 영역에서 빠른 속도로 침해 활동을 벌이고 있지만, 방어자는 공격자의 속도와 범위를 따라가지 못하며, 상당부분 수동으로 대응하고 있다. 이러한 구조로는 보안 투자를 아무리 늘려도 피해를 줄이지 못한다.

보안관제서비스는 탐지한 이벤트를 보안 담당자에게 알리는 수준으로만 대응할 수 있으며, 이벤트 분석과 영향도 평가, 신속한 대응은 보안조직이 직접 수행해야 한다. 24시간 운영되는 SOC라 해도, 보안 담당자가 근무하는 시간 외에는 고위험 이벤트에 즉시 대응하지 못한다.

문제 1: 알림 모니터링을 24/7로 착각

대부분은 '경보 감시'는 24시간이지만 판단·격리·조치는 9시부터 6시까지 근무시간 중 이뤄진다.

문제 2: 티켓 기반 운영 구조

티켓이 생성되고 고객사가 승인하고 내부 보안팀이 다시 결정하는 구조에서 MTTR은 절대로 줄어들지 않는다.

문제 3: 이벤트 중심 SOC 모델의 한계

이벤트 중심 SOC는 '정해진 룰을 어긴 이벤트'만 탐지하기 때문에 알려지지 않은 위협, 신원 기반 공격을 탐지하기 어렵다.

문제 4: 인력 부족을 자동화 부족으로 오해

많은 조직은 자동화를 '탐지 자동화'로 이해하지만, 진정한 자동화는 '격리·차단 자동화'이다.

▪ MTTR 단축의 의미

많은 공격이 침투 1시간 내에 확산, 탈취까지 완료되고 있기 때문에, 보안은 이 시간 내에 탐지, 판단, 격리까지 해야 한다. 크라우드스트라이크가 탐지한 공격 사례처럼 1분이 채 걸리지 않는 침투→확산 공격에 대응하기 위해서는 중요한 결정을 '초' 단위로 내려야 한다.

MTTR을 단축하는 것은 CISO 관점의 기술적 의미만 있는 것이 아니다. CEO·CFO 관점에서는 직접적인 재무 손실을 줄이는 핵심적인 지표로 해석될 수 있다. 실제로 IBM 조사에 따르면 MTTR 30% 단축 시 평균 침해 비용은 49% 감소하는 것으로 나타난다.

침해 비용은 직접적으로 발생한 피해뿐만 아니라 빠르게 대응했을 때 줄일 수 있는 비용까지 포함된다.

✔ 침해로 인한 직접 피해 비용

- 대응 지연으로 인해 발생하는 비용
- 데이터 유출로 인한 피해
- 시스템 격리 시간
- OT/제조 운영 중단 비용
- 법적 대응 비용
- 고객 이탈 증가 및 평판 악화

✔ 빠른 대응에 성공했을 때 줄일 수 있는 비용

- 침해 범위 조기 차단
- 복구 비용 최소화
- 규제 보고 부담 감소
- 영업 손실 최소화

이는 SOC가 MTTR 자체를 줄이는 것뿐만 아니라, 대응 프로세스·역량·운영 체계의 성숙도를 높여야 한다는 것을 보여준다. 실제로 파고 MDR이 수행한 침해 대응 사례에서, MTTR을 지속적으로 줄이는 조직은 다음과 같은 공통점을 갖고 있다는 사실을 알 수 있다.

- 탐지-판단-격리 단계가 분리되지 않고 하나의 흐름으로 통합
- 24/7 대응 체계 가동
- 초기 분석·격리 상당 부분 자동화
- 경보를 검증(Validation)하고 우선순위화하는 프로세스 내재화

▪ 회복력 중심 보안 운영

2023년부터 2025년까지 보안 전문 기업과 기관들이 진행한 사이버 위협 관련 CEO 대상 설문을 분석해보면, '공격을 막지 못한 것 보다 더 중요한 문제는 빠르게 회복하지 못했다'는 공통적인 의견이 등장한다. 실제 파고 MDR의 사례에서도 탐지 및 대응 시간을 단축한 조직은 침해 비용을 크게 줄였다는 사실을 알 수 있다.

이제 보안은 기술 부서만의 과제가 아니라 비즈니스 전반의 회복력(Resilience)을 높이기 위한 핵심 요인이 되었다. 경영진이 바라보는 '회복력'은 침해를 빠르게 식별하고 대응해 사고를 막는 것뿐만 아니라, 사고 시 시스템 중단 시간을 줄이고 빠르게 재개하는 것, 고객 경험 및 브랜드 신뢰도 보호, 복구 비용과 법적 리스크를 최소화하는 것까지 포함한다. 이 모든 요소가 보안 운영에 반영되어야 한다.

보안 운영 재설계

지난 3년간의 위협 데이터와 국내외 위협 동향 분석 보고서는 보안 전략의 중심이 SOC에서 MDR로 이동하고 있다는 것을 분명히 보여준다. 이는 공격 패턴, 운영 환경, 경영 의사결정의 변화를 반영한 흐름으로, 전체 침해 비용과 사이버 리스크, 운영 속도를 고려해 MDR 중심의 보안 전략으로 재설계해야 한다는 것을 의미한다.

MDR은 다음과 같은 점에서 전통 SOC보다 구조적으로 우월하다.

- **탐지–판단–대응–격리까지 '운영 단일화':** 전통적인 SOC는 탐지, 판단, 대응, 격리 기능이 분리되어 있으나 MDR은 이를 통합해 신속하고 정확하게 의사결정하고 조치할 수 있게 한다.
- **24/7 대응:** 전통적인 SOC는 단순 모니터링 중심이지만, MDR은 실제 위협에 대응할 수 있어 중단없는 보안 조치가 가능하다.
- **위협 헌팅을 기본 프로세스로 포함:** 전통적인 SOC는 이벤트 중심의 제한적 대응만 가능하다. 반면 MDR은 위협 헌팅을 통해 이미 진행중인 공격, 알려지지 않은 위협까지 찾아 확실한 증거와 신호를 중심으로 정확하게 조치할 수 있다.
- **CTEM 활용으로 침해 발생 전 대응:** 전통적인 SOC는 침해 후 대응하지만, MDR은 CTEM을 활용해 침해가 발생할 가능성이 있는 모든 지점을 찾아 선제적으로 대응할 수 있다.

가짜 MDR 범람

많은 보안 투자를 단행해 온 글로벌 기업에서도 대규모 보안 사고가 잇달아 발생하면서 기존 보안 운영의 근본적인 개선이 필요하다는 인식이 퍼지기 시작했다. 특히 MDR을 통한 보안 운영 개선 효과가 증명되면서 2025년부터 본격적인 확산이 시작됐다.

그런데 일부 서비스는 단순 모니터링·알림 재전달 수준에 불과함에도 'MDR'이라고 홍보하고 있어 시장에 혼란을 주고 있다. 이러한 서비스는 소수의 포인트 보안 솔루션을 사용해 이벤트를 전달하는 수준으로, 진정한 MDR의 가치를 훼손시키고 있다.

가짜 MDR은 다음의 특징을 갖는다.

- 탐지 이벤트만 전달하고 위험 판단은 고객사에 위임
- 검증되지 않은 티켓 기반 프로세스 사용
- 위협 헌팅 제공하지 않음
- 자동화 기반 대응 및 격리 서비스 제공하지 않음
- 24/7 탐지·대응 인력 없거나 부족함

진정한 MDR은 기업의 비즈니스 전반에서 빠르고 정확하게 위협을 탐지하고, 즉시 조치할 수 있는 기반을 갖추고 있다. 자체 축적한 위협 인텔리전스와 외부 인텔리전스 소스를 기반으로 검증된 전문 인력이 탐지된 위협을 분석하고, 비즈니스 맥락과 영향도에 따라 대응하며, 그 결과에 대해서도 책임을 질 수 있어야 한다.

MDR 필수 요건

성숙도 높은 MDR은 고객의 SOC를 대신 수행할 수 있을 정도의 전문성과 책임성, 신뢰성을 갖추고 있다. 성숙도 높은 MDR을 이용하면, 보안 조직은 비즈니스 관점의 보안 전략을 수립하고 이행하는 '본질적인 보안'에 집중하면서 경영 전반의 리스크를 완화하고 개선해 나갈 수 있다.

성숙도 높은 MDR이 반드시 갖춰야 할 역량은 다음과 같다.

▪ 위협 헌팅과 검증

위협 헌팅(Threat Hunting)은 피해를 예방하기 위한 필수 활동이다. 고객 환경에서 운영되고 있는 보안 솔루션이 탐지하지 못한 침해를 전문 헌터가 직접 찾아 분석하고, 실제 비즈니스에 미치는 영향과 악용 가능성을 진단해 알려지지 않은 위협까지 조기에 대응한다.

파고 MDR이 '실제 위협'으로 판단하고 고객에게 보고한 핵심 TTP를 보면, 대부분의 사고는 파일 기반의 저위험 알림이 아니라, 공격자가 이미 시스템에 침투한 상황에서 발생하는 고위험 침해였다.

이는 위협 헌팅의 필요성을 분명하게 보여주는 사실로, 위협 헌팅은 MDR에서 선택 가능한 '고급 기능'이 아니라 '골든타임 확보'를 위한 필수 전략이다.

위협 헌팅을 통해 찾은 침해 증거가 모두 다 피해로 이어지는 것은 아니기 때문에, 이를 검증(Validation)하는 과정도 필수다. 공격 전반의 맥락과 위협 인텔리전스 데이터를 결합해 실제 악용 가능성과 위협 수준을 정확하게 파악한다. 이를 의사결정(Decision by Signal)을 위한 데이터로 제공해 '적확한' 대응 결정을 내릴 수 있도록 한다.

파고 MDR의 검증 기반 위협헌팅을 통한 개선 효과는 다음과 같다.

- 검증 기반 필터링으로 오탐 31~46% 감소
- 위협 헌팅 기반 탐지로 초기 침투 20~30% 선제 차단
- 검증과 헌팅 통합 시 MTTR 38% 단축
- 수평 이동(Lateral movement) 차단 확률 1.7배 증가

▪ 전문가와 AI의 협업

사이버 공격이 AI를 이용해 빠르고 광범위하게 진행되기 때문에 현재 보안 운영에서 SIEM에 AI를 탑재해 탐지 정확도와 속도를 높이고 있었다. 나아가 진보한 MDR에서는 고도화된 AI-SIEM으로 자동화 수준을 한 차원 높인다.

MDR에서 AI-SIEM의 역할은 다음과 같다.

- 로그 맥락(Context) 자동 분석
- 알려지지 않은 위협 신호 재분류
- SaaS, 클라우드, 아이덴티티 이벤트 통합
- 자동화 기반 대응(Containment Automation) 트리거
- 위협 인텔리전스 기반 위험 점수 부여

AI-SIEM이 이벤트 정규화, 분류, 위험 수준 평가 과정을 자동화해 대응할 수 있지만, 모든 위협을 AI가 대신할 수 있는 것은 아니다. 특히 이전에 탐지되지 않았던 알려지지 않은 위협이나 합법적인 자격증명을 이용하는 신원 기반 공격, 섀도우 AI 및 AI로 인한 새로운 위협은 AI만으로 대응할 수 없다.

그래서 전문가와 AI가 협업하는 증강 AI(Augmented AI)가 MDR의 필수 요건이 된다. 증강 AI는 전사 보안 운영 모델을 지탱하는 구조적 기반(Operational Backbone)이며, MDR의 기본 운영 엔진이 된다.

▪ 지속적 위협 노출 관리

지속적 위협 노출 관리(CTEM)는 조직 전체의 공격표면을 식별하고, 검증하며, 우선순위를 지정하고 수정하는 사전 예방적 보안 전략이다. 공격표면에는 자산, 환경, 애플리케이션, ID 등에서 공격자가 악용할 수 있는 취약점, 구성오류, 미흡한 관리 등이 포함된다.

가트너가 정의한 CTEM 모델은 ▲범위 정의(Scoping) ▲노출 평가(Discovery) ▲노출 우선순위화(Prioritization) ▲검증 기반 위험 평가(Validation) ▲위험 경감(Remediation) 등의 단계를 포함한다. MDR에 CTEM 프로세스를 통합시키면 보안 운영을 '탐지' 중심이 아닌 '공격 전 대응(Preemptive

Defense)' 중심으로 재편할 수 있다.

여기에 ITDR이 포함된다는 것이 중요하다. ITDR은 계정탈취, 크리덴셜 스터핑, 권한 상승 등 신원과 관련된 위협을 탐지·대응하는 기술로, 엔드포인트 중심 탐지에서 신원 중심 탐지 및 대응 전략으로 전환하기 위한 핵심 요소다.

▪ 위협 인텔리전스

위협 인텔리전스는 최신 공격 전략과 패턴, 도구에 대한 실시간 통찰을 제공하는 서비스로, 기존 도구가 놓칠 수 있는 위협을 탐지하고, 잠재적 취약점을 우선순위화하며, 능동적 헌팅을 가능하게 해 피해를 최소화한다. MDR에서 위협 인텔리전스와 전문가의 통찰력을 결합시키면 잠재된 위협을 포착하고 오탐을 줄일 수 있다.

성숙도 높은 MDR은 실제 운영 데이터를 기반으로 정기적인 위협 인텔리전스 리포트를 직접 발행할 수 있는 분석 역량을 갖추고 있다. 최신 위협 동향과 고객·산업이 반드시 알아야 할 위협 정보를 제공해 사회 전반의 보안 수준 향상에 기여한다.

▪ 24/7 운영과 선제적 대응

최근 공격자는 보안 담당자가 즉각 조치하기 어려운 야간, 주말에 공격을 시작한다. 실제 고객 현장에서 발생한 사례를 보면, 토요일 20시 43분 브루트포스 공격이 시작되어 21시 6분에 내부 계정 탈취에 성공했다. 일요일 새벽 3시 45분에 sqlservr.exe를 통한 RCE 공격이 진행되고, 일요일 오전 11시 35분에 UAC Bypass 및 백도어 계정이 생성됐다. 그리고 일요일 22시

위협 헌팅의 핵심, LotL 탐지

파고의 위협 헌팅 전문가는 알려진 악성 파일을 찾는 침해 지표(IoC) 기반 헌팅이 아니라, 시스템 내부에서 발생하는 '의심스러운 행위'를 찾는 데 집중한다. 실제로 파고가 탐지·대응한 침해 시도의 대부분이 시스템에서 활동중인 공격자를 찾아 조치하는 것이었다.
가장 많이 탐지된 인시던트는 파워셸(PowerShell), cmd.exe, w3wp.exe(IIS), sqlservr.exe(MS-SQL) 등 시스템에 기본적으로 내장된 합법적인 도구를 악용하는 LotL 기법으로, 공격자의 표준 공격 모델이 되고 있는 것으로 보인다.
파고는 LotL 공격을 탐지하기 위해 특화된 프로세스 관계 분석 기술을 사용한다. 각각의 개별 프로세스는 정상이지만, 그 실행 관계가 비정상적인 패턴을 식별하는 것이다.

- **사례 1: 웹셸 실행 탐지**
  - 비정상 프로세스 관계: w3wp.exe(IIS 웹 서버 프로세스)가 자식 프로세스로 cmd.exe(명령 프롬프트)를 실행
  - 파고 데이터: 다수의 고객사에서 이 같은 비정상적인 프로세스 관계를 탐지
  - 의사결정을 위한 분석: 웹사이트에 업로드된 악성 웹쉘을 통해 공격자가 원격 명령을 실행하고 있음을 나타내는 강력한 IoC로 분류하고 대응

- **사례 2: SQL 서버를 통한 RCE 탐지**
  - 비정상 프로세스 관계: sqlservr.exe(MS-SQL 서버 프로세스)가 자식 프로세스로 cmd.exe를 실행
  - 파고 데이터: 일부 고객에서 발생한 침해사고에서 비정상 프로세스 탐지
  - 의사결정을 위한 분석: SQL 인젝션 취약점 공격이나 xp_cmdshell 저장 프로시저 악용을 통해 공격자가 데이터베이스 서버의 제어권을 탈취하고 운영체제(OS) 명령을 실행하고 있음

사례 1, 2와 같은 공격은 개별 파일이나 IP를 차단하는 기존 탐지·대응 기술로 해결할 수 없으며, 컨텍스트 기반 행위 분석(Behavioral Analysis)을 통해 이벤트→유의미한 이벤트(Events of Interest)→대응해야 할 인시던트로 전환할 수 있다.

51분에 웹셸을 통한 내부 정찰이 시작되었다.

이처럼 위협 행위가 주말 내내 발생했음에도, 근무일이 아니기 때문에 보안 담당자는 월요일 아침에 출근한 후에야 인지하고 대응할 수 있다.

또 다른 사례에서는 공격자가 주말 동안 모든 위협 활동을 마친 후 시스템을 중단시키거나 협박 메일을 보내왔을 때에야 침해 사실을 알아차렸다.

이 같은 위협을 막기 위해서는 '24시간 365일 중단 없는(Always-On)' MDR 서비스와 위협 대응을 위한 의사결정까지 할 수 있는 선제적 대응(Preemptive Response)이 필수다. 24/7 실시간 탐지로 위협을 식별하고, 보안 조직을 대신해 대응함으로써 위협 확산을 조기에 차단한다.

파고 MDR이 대응한 사고의 침해 데이터를 보면 24/7 운영과 선제적 대응이 왜 필요한지 알 수 있다.

- 자격증명 탈취 공격 탐지 이후 24~40분 내 격리 성공 사례
- 노출된 RDP·SSH 포트 기반 침투 시도 초기 단계에서 차단
- PoC 기반 공격 스캔을 상황 인지 단계에서 선제 차단
- 알려지지 않은 위협 분류 후 맥락 기반 재정의로 오탐 제거
- 자동 격리 + 인간 판단이 결합된 운영 구조로 MTTR 평균 38% 단축

파고 MDR은 '검증-자동화-헌팅(Validation–Automation–Hunting)'을 통해 침해를 빠르게 탐지하고 즉시 대응 방안을 제시한다. 고객이 직접 대응하기 어려운 상황에서는 파고 전문가가 전략적으로 의사결정을 내리고 조치한다.

파고 MDR의 24/7 기반 선제적 대응은 침해가

위협 인텔리전스 기반 국가 배후 그룹 공격 탐지

위협 인텔리전스는 공격자의 전술, 기술, 절차(TTP)를 알 수 있는 중요한 데이터를 제공하는 서비스다. PAGO DeepACT MDR은 실제 사례를 기반으로 인텔리전스를 축적하고 있으며, 외부 공개된 자료인 OSINT 데이터와 결합해 더욱 정확한 위협 탐지가 가능하다.

1. 하프늄(Hafnium) 공격 탐지

파고 MDR은 고객사의 익스체인지 서버에서 비정상 행위를 탐지했다. 핵심 지표는 IIS 애플리케이션 프로세스인 w3wp.exe(구체적으로 MSExchangeOWAAppPool 또는 MSExchangeECPAppPool)가 자식 프로세스로 cmd.exe를 실행시킨 것이다.

· TTP: 위협 행위자는 익스체인지 서버의 /owa/auth/ 또는 /ecp/auth/ 경로에 proxy.aspx, page.aspx와 같은 악성 웹셸을 설치했다. 그리고 cmd.exe를 실행하고, 내부망 정찰 명령을 수행했다.(예: net group Domain computers /domain, ipconfig)

· 위협 인텔리전스 분석: 이러한 행위는 중국 배후 위협그룹 하프늄(HAFNIUM)이 프록시로그온, 프록시셸 취약점을 악용할 때 사용하는 전형적인 공격 체인과 일치한다. 파고 MDR은 파일 시그니처가 없는 파일리스(Fileless) 공격과 비정상적인 프로세스 관계 분석을 통해, 국가 배후 APT 그룹의 초기 정찰 활동을 실시간으로 탐지하고 차단했다.

2. x0wolf 공격 탐지

파고 MDR은 고객사의 침해 사고에서 웹셸(WebShell, modify.aspx)을 통해 유입된 고도의 다단계 공격을 탐지했다.

· TTP: 위협행위자는 합법적인 서명이 있는 마이크로소프트 Sysinternals 드라이버 PROCEXP152.sys 취약점을 악용해 EDR 솔루션을 무력화한 후 코발트스트라이크 페이로드(0302.exe)를 실행했다. 파고 MDR이 확인한 C2 IP는 104[.]21[.]80[.]1였으며, C2 터널링을 통해 lcx5qm.jpg라는 이미지 파일로 위장된 악성 파일이 추가 다운로드됐다.

· 위협 인텔리전스 분석: lcx5qm.jpg 파일은 중국계 위협 그룹 x0wolf가 SOCKS5 프록시 C2 터널링을 위해 사용하는 고유한 커스텀 해킹툴이다. 공격자는 널리 알려진 코발트스트라이크와 x0wolf 그룹의 고유한 툴을 결합해 탐지가 어려운 이중 C2 채널을 구축했다. 파고 MDR은 두가지 툴의 활동을 연계 분석해 공격자를 식별했으며, IoC 차단과 함께 추가 정보를 제공했다.

피해로 이어지기 전에 예방하고, 비즈니스 영향을 최소화할 수 있다. 이는 강력한 보안 전략일 뿐 아니라 전사적 손실을 줄이는 재무적 의사결정이다.

보안 전략의 중심 'MDR'

보안 기술은 상향평준화되고 있으며, SOC는 지속적으로 고급 보안 기술을 도입하면서 보안 침해에 대응하고 있다. 그러나 실제 침해사고는 초보적인 공격 기법으로도 가능한 만큼, 기술이 아니라 운영 방식의 재설계가 시급하다.

그래서 2026년 보안 전략은 더 강력한 솔루션을 도입하는 것이 아니라, 실제로 작동하는 MDR 운영 모델을 갖추는 것이 더 중요하다. 진정한 MDR을 기본 운영 인프라로 채택할 때, '공격 후 대응(Post-Breach IR)'이 아니라 '공격 전 대응(Preemptive MDR)'을 실현할 수 있다.

또한 MDR은 SOC를 위한 추가적인 비용 투자가 아니라 재무적 의사결정(Financial Decision) 전략으로 채택되어야 한다. MDR은 복합적으로 진행되는 빠른 공격도 정확하게 탐지해 대응함으로써 침해를 예방하고 보안 운영을 효율화할 수 있다. 이는 궁극적으로 기업 전반의 비용을 낮추고, 기업이 본연의 업무에 더욱 집중하도록 해 경쟁력을 높일 수 있는 방법이다.

Case Study: 선제적 대응으로 랜섬웨어 예방

랜섬웨어 공격자들이 띄우는 랜섬노트에는, '귀사의 데이터는 암호화되었고, 기밀 데이터는 유출되었다'는 사실을 명시하며, '서비스 중단 및 업무 불가'를 볼모로 금전을 요구한다. 특히 공격자는 피해 기업의 다운타임이 길어질수록 피해가 늘어난다며 자신의 수익을 극대화할 수 있는 압박 전략을 펼친다.

이 같은 피해를 최소화하기 위해서는 선제적인 대응(Preemptive Response)이 가능한 24/7 보안 운영이 필수다.

파고 MDR의 선제적 대응 서비스는 보안 담당자가 근무하지 않는 시간에도 랜섬웨어 피해를 차단한 다수의 성공사례를 갖고 있다.

- 탐지(Detect): 일요일 오전(11:35) 기업의 특정 서버에서 UAC Bypass(T1548.002, ConsentPromptBehaviorAdmin 레지스트리 수정) 시도와 동시에, 'default'라는 신규 관리자 계정 생성(T1136.001) 행위가 발생하는 것을 위협 헌팅을 통해 실시간으로 탐지했다.

- 분석(Analyze): 파고 MDR 센터의 24/7 보안 전문가는 즉시 이 행위가 '백도어 계정 생성을 통한 시스템 장악 및 지속성 확보' 시도로 판단하고, 고위험(Critical) 침해 사고로 상황을 전환했다.

- 대응(Respond): 파고 보안 전문가는 즉시 고객사 비상 연락망을 가동했으나, 일요일 오전이어서 즉시 연락이 닿지 않았다. 그러나 신속하게 확산을 막아야 하는 상황이라고 판단했기 때문에 사전에 정의되고 협의된 대응 정책(Playbook)에 따라 '선제적 네트워크 격리(Preemptive Network Isolation)' 조치를 원격으로 수행했다.

비즈니스 가치 확보 위한 이사회 권고사항

기업의 보안 의사결정권은 전통적인 CISO나 CIO 조직에만 머물러서는 안 된다. 사이버 공격은 IT 사고가 아니라 재무, 운영, 평판, 고객 신뢰의 복합 리스크이기 때문이다. 따라서 2026년 보안 전략은 기술 중심이 아니라 '경영진이 직접 관리해야 하는 비즈니스 리스크(Business Risk)'로 재정의되어야 한다.

보안의 경영적 가치 재정의

기업은 보안 투자를 IT 운영비(OPEX), 규제 준수 비용, 기술 투자 비용으로 분류해왔으나, 이제는 회복 탄력성과 생존 가능성의 문제로 확장시켜야 한다. 이는 보안 예산이 '기술 비용'에서 '리스크-조정 비용(Risk-adjusted Cost)'으로 이동했다는 사실을 의미한다. 보안 투자 규모보다, '보안이 기업을 어떻게 지켜내는가'로 경영의 초점을 바꿔야 한다.

회복과 생존의 관점에서 보안 운영을 위한 의사결정을 할 때, 이사회는 다음의 지표를 확인해야 한다.

- MTTD(평균 탐지 시간)
- MTTA(평균 탐지 인지 시간)
- MTTR(탐지 → 대응 → 격리 시간)
- Containment Ratio(초기 차단 비율)
- Exposure Reduction(노출 감소율)
- IB Ratio(Incident-to-Breach Ratio)

이 지표가 중요한 이유는 가짜 MDR로 인한 혼란을 막기 위해서다. 가짜 MDR은 대응 인력이 부족하거나 존재하지 않으며, 24/7 중단없는 운영이 되지 않고, 검증과 위협 헌팅 기반 탐지 구조가 없다. 실제 공격 상황에서 제대로 대응하지 못하기 때문에 'MDR 무용론'에 빠지기 쉽다. 이는 보안의 실패를 넘어서는 경영의 실패로 이어질 수 있다.

진정한 MDR은 24/7 보안 분석 및 대응 전문가와 조직을 갖추고 있으며, 위협 헌팅과 검증 프로세스, 자동 격리, CTEM 프로세스 내재화, 방대한 위협 인텔리전스, 증강 AI를 통한 고급 대응이 가능하다. 진정성 있는 MDR은 경영을 위한 '운영 기준(Operation Standard)'을 제시하며, 비즈니스 리스크 관리 전략의 일환으로 채택된다.

2026년 이후, 이사회가 물어야 할 질문

보안이 기술 집행 단계에서 이사회 수준의 전략 의사결정으로 올라온 지금, 경영진의 질문도 바뀌어야 한다. 다음 질문은 '성과 보고'가 아니라 '기업의 생존 가능성'을 판단하는 질문이다.

CEO의 질문

- 공격을 얼마나 빨리 발견하고 있는가?
- 탐지 이후 대응은 즉시 이뤄지는가?
- 대응이 사람의 근무시간에 의존하지 않는가?
- 알려지지 않은 위협을 탐지할 수 있는가?
- 공격표면을 줄이는 전략이 실제로 실행되고 있는가?

CFO의 질문

- 사이버 투자 대비 실제 리스크 감소 효과는 얼마인가?
- MTTR 개선이 재무제표에 어떤 영향을 주었는가?
- 보안 조직의 대응 속도는 비용 절감 구조로 이어지고 있는가?

이사회의 질문

- 침해가 발생했을 때 회복 시간은 얼마인가?
- 공격 시나리오별 대응 계획이 문서화·테스트되어 있는가?
- MDR 운영 역량은 내부·외부 모두 검증 가능한가?

부록: 조사 방법과 데이터 출처

본 보고서는 파고네트웍스 의뢰로 IT 전문 매거진 <네트워크타임즈>에서 제작했다.

보고서는 파고 MDR 센터가 2023년부터 2025년까지 축적한 다층적 위협 인텔리전스와 실제 MDR 서비스의 침해대응 사례, 신뢰도 높은 글로벌 보안 기업 및 기관들이 공식 발표한 연례 보고서를 근거로 작성되었다.

각 기관·기업의 보고서는 서로 다른 관점에서 동일한 위협을 바라보기 때문에, 파고 MDR 센터는 파고 MDR 서비스의 실제 사례 및 인텔리전스, 글로벌 보고서의 중복 구간을 식별하고 교차 검증해 신뢰도 높은 영역만 추출해 분석했다.

또한 파고 MDR 센터의 전문적인 보안 인사이트를 통해 기업 보안 조직에서 즉시 활용할 수 있는 인텔리전스를 제공하고자 했으며, 경영진과 이사회에서 경영전략의 일환으로 보안 전략을 수립할 때 반드시 고려해야 할 사항을 제안했다.

본 보고서에서 참고한 글로벌 위협 인텔리전스 기관의 공식 연례 보고서는 다음과 같다.

- 버라이즌 데이터 침해 조사 보고서(DBIR) 2023–2025: 침해 벡터, 공급망 공격, 자격증명 탈취 공격 패턴, 지역별 침해 트렌드
- 크라우드스트라이크 글로벌 위협 리포트(GTR) 2024–2025: Breakout Time, 공격자 전술(TTP), 도메인 이동 속도
- IBM 침해 비용 보고서(CODB) 2023–2025: 침해 비용 구조, 자동화·AI 도입 효과, 인지·대응 지연에 따른 손실 규모
- 맨디언트 M-Trends 2023–2025: 초기 침해 탐지 경로, Dwell Time 변화, 공격자 운영 모델
- 가트너 CTEM & SOC 현대화 프레임워크(2023–2025): 공격표면 관리, 운영 모델 전환(Prevention → Exposure → Resilience) 인사이트

pago

파고네트웍스는 MDR(Managed Detection and Response) 전문 기업으로, 대한민국과 APAC 지역의 에너지, 화학, 반도체, 전력, 제조업, 금융, 의료, 정부 및 연구 등 다양한 산업 고객을 보호하고 있습니다. 파고 MDR 플랫폼 DeepACT는 OT/ICS, IT, 클라우드, 데이터센터를 포함한 다양한 환경과 모든 규모의 고객을 위한 가상 전담 CERT, IR, 또는 SOC 팀 역할을 수행하고 있습니다.
PAGO MDR은 Managed-EPP, Managed-EDR, Managed-NDR, Managed-XDR을 포함한 포괄적인 서비스와 함께 사고 대응, 위협 헌팅, 공격 표면 관리, 침해 평가, TI(Threat Intelligence) 공유 등 확장된 맞춤형 솔루션을 제공합니다.

www.pagonetworks.com/ko
서울특별시 용산구 회나무로 65
대표전화 080-077-5171