From Detection to Decision
Security Fails Without Execution

INCIDENT RESPONSE INSIGHTS

이미 진행되고 있는 공격, 보안은 어떻게 대응해야 하는가
6가지 실제 사고 대응 사례로 본 기업 보안의 현실

2026

pago

The Global MDR Frontline
Owning the Decisions That Matter Most

목차

ABOUT THIS REPORT

이 리포트는 다양한 산업 환경에서 실제로 발생한 Incident Response 사례를 기반으로 구성되었습니다.

PAGO는 수년 간의 현장 경험을 통해, 기업 보안이 어떤 지점에서 취약해지고, 어떤 순간에 사고의 결과가 달라지는지를 지속적으로 관찰해왔습니다. 그 과정에서 확인된 것은 단순한 기술적 문제를 넘어, 보안 운영과 대응 구조 전반에서 반복적으로 나타나는 공통된 패턴이 존재한다는 점입니다.

특히 최근 보안 환경에서는 공격의 속도와 복잡성이 빠르게 증가하고 있으며, 탐지 이후 대응까지 이어지는 시간의 격차가 점점 더 중요한 변수로 작용하고 있습니다. 이와 같은 변화의 배경에는, 자율적으로 판단하고 실행하는 Agentic AI의 등장과 함께 공격과 방어 모두에서 자동화 수준이 빠르게 높아지고 있다는 변화가 나타나고 있습니다. 이에 따라 기존 탐지 중심 보안 모델의 한계가 더욱 빠르게 드러나고 있습니다.

본 리포트는 이러한 변화 속에서, 실제 환경에서 발생하는 보안 사고의 흐름과 그 의미를 다음과 같은 관점에서 정리합니다.

주요 구성 내용

- 실제 침해 사고가 시작되고 확산되는 과정에 대한 구체적인 흐름
- 서로 다른 사례에서 공통적으로 발견되는 공격 및 대응 패턴
- 기존 보안 체계에서 놓치기 쉬운 운영상의 한계
- Incident Response 과정에서 드러나는 현실적인 대응의 어려움

1. EXECUTIVE SUMMARY

오늘날의 보안 환경은 빠르게 변화하고 있으며, 공격의 방식뿐만 아니라 속도와 규모 또한 이전과 비교할 수 없을 정도로 증가하고 있습니다. 이는 단순히 위협이 증가했다기보다, 보안이 작동하는 방식 자체가 변화하고 있음을 의미합니다.
특히 최근에는 자동화된 공격 기법과 함께, 자율적으로 판단하고 실행하는 Agentic AI의 확산 가능성이 논의되면서 기존 대응 모델의 한계가 더욱 빠르게 드러나고 있습니다.

PAGO MDR은 이러한 변화에 대응하기 위해 설계된 보안 운영 모델입니다.

단순한 위협 탐지에 그치지 않고, 탐지 이후의 판단과 실행까지 연결함으로써 공격의 확산을 최소화하고 실제 보안 결과를 개선하는 것을 목표로 합니다. 그러나 많은 조직은 여전히 다음과 같은 구조적 한계를 가지고 있습니다.

- 보안 이벤트는 탐지되지만, 신속한 분석과 대응으로 이어지지 않는 구조
- 야간, 주말 등 운영 공백 시간 동안 발생하는 대응 지연
- 탐지 이후 판단과 승인 과정에서 발생하는 시간 소모

이러한 환경에서는 위협이 인지되었음에도 불구하고 실제로는 차단되지 않는 상황이 반복됩니다. 본 리포트에서 분석한 6가지 Incident Response 사례는 이와 같은 현실을 명확하게 보여줍니다.

공격은 외부에서 침입하는 형태로 시작되기보다, 이미 확보된 계정이나 정상적인 접근 방식을 통해 시작되었으며, 탐지 이후의 대응 지연을 통해 내부 확산으로 이어질 수 있는 구조를 가지고 있었습니다. 이는 기업 보안의 취약성이 단순한 기술의 부재에서만 비롯되지 않음을 보여줍니다.

운영의 공백과 의사결정 구조의 한계가 복합적으로 작용하면서 실제 사고의 규모가 결정되는 경우가 많습니다. 이러한 상황에서 피해를 확대시키는 핵심 요인은 단순한 탐지 능력의 부족이 아니라, **누가, 언제, 어떤 기준으로 대응을 실행할 것인가에 대한 구조의 문제입니다.**

특히 AI 기반 자동화와 Agentic AI의 확산으로 공격의 속도와 반복성이 급격히 증가하고 있는 현재 환경에서는, 탐지 이후의 판단과 실행을 포함한 보안 운영 구조가 더욱 중요해지고 있습니다.

결국 이 리포트가 던지는 질문은 단순합니다.

지금 우리 조직은 위협을 탐지할 수 있는 상태입니까? 아니면, 실제로 대응할 수 있는 상태입니까?

이 질문은 특정 조직에만 해당되는 문제가 아니라, 현재 보안 환경 전반에서 공통적으로 나타나는 구조적인 이슈이기도 합니다. 이러한 변화는 개별 조직의 문제가 아니라, 보안 시장 전반의 흐름과도 맞닿아 있습니다. 현재 보안 시장은 빠르게 재편되고 있으며, 일부 대형 플랫폼 중심으로 운영 모델이 표준화되는 흐름이 나타나고 있습니다.

이러한 환경에서 조직은 단순한 기술 선택을 넘어, 어떤 운영 구조를 기준으로 보안을 정의할 것인지에 대한 선택을 해야 하는 시점에 놓여 있습니다. **결국 차이는 기술이 아니라, 탐지 이후를 누가, 어떻게 책임지고 실행할 수 있는 구조를 가지고 있는가에 있습니다.**

REAL INCIDENT CASES

Part 1

탐지 이후의 공백

- Case 1. 정상 계정 하나로 시작된 전사 랜섬웨어 감염
- Case 2. 보안 솔루션이 있었지만, 이미 수천 개의 위협이 존재했던 환경

Part 2

공격의 속도와 개입 시점

- Case 3. 확산 직전 단계에서 차단된 대규모 공격
- Case 4. 암호화 이전 단계에서 중단된 랜섬웨어 공격

Part 3

보이지 않는 위협과 시간의 문제

- Case 5. 흔적 없이 유지된 시스템 제어
- Case 6. 단 30분 내 차단된 공격 시도

탐지 이후의 공백

본 섹션에서는 실제 Incident Response 과정에서 확인된 사례를 중심으로, 공격이 어떻게 시작되고, 어떤 경로를 통해 확산되며, 결과를 바꾸는 결정적 요인이 무엇이었는지를 순차적으로 살펴본다.
각 사례는 개별 사건이지만, 동시에 현재 기업 보안 환경에서 반복적으로 나타나는 구조적 특징을 보여준다.

특히 최근 보안 환경에서는 자동화된 공격과 함께 자율적으로 판단하고 실행하는 Agentic AI 기반 행위가 증가하면서, 공격은 더욱 빠르고 정교하게 이루어지고 있으며, 탐지 이후 대응의 지연이 더욱 치명적인 결과로 이어질 가능성이 높아지고 있다.

CASE 01

정상 계정 하나로 시작된 전사 랜섬웨어 감염

**공격은 종종 '비정상적인 침입'이 아니라, 지극히 정상적인 로그인에서 시작된다.
이 사례 역시 그 전형적인 흐름을 보여준다.**

WHAT HAPPENED

공격자는 유효한 VPN 계정을 이용해 내부 시스템에 접근했다. 로그인 자체는 실패 기록이나 경고 없이 이루어졌으며, 표면적으로는 정상적인 사용자 활동과 구분되지 않았다.
그러나 로그인 이후, Windows Credential Dump와 같은 행위가 포착되었고, 이를 통해 추가 계정 정보가 확보되면서 공격자는 내부망에서의 이동 권한을 점진적으로 확장해 나갔다.

이후 공용 계정을 활용한 측면 이동이 이어졌고, 결국 여러 시스템에 랜섬웨어가 배포되면서 비즈니스 전반이 중단되는 상황으로 이어졌다.

WHAT WENT WRONG

이 사고는 특정 기술의 부재라기보다, 여러 운영상의 취약 요소가 동시에 작용한 결과였다.

- 야간 시간에 발생하여, 신속한 분석과 대응이 이루어지지 못한 점
- 공용 계정 사용으로 인해 계정 탈취 이후 확산이 용이했던 구조
- 핵심 서버 일부에 보안 솔루션이 적용되지 않아 가시성이 제한된 환경

결과적으로 초기 징후는 존재했지만, 이를 '위협'으로 해석하고 실제 행동으로 이어지는 과정이 지연되었다.

WHAT CHANGED

PAGO는 해당 행위를 단순한 이상 징후가 아닌, 전사적 영향을 초래할 수 있는 고위험 위협으로 판단했다.

이 판단을 기반으로 즉각적인 차단 정책이 적용되었고, 공격자의 이동 경로를 추적하는 포렌식 분석이 병행되었다.

이를 통해 추가 확산은 제한되었고, 사고의 원인과 경로 또한 명확하게 규명될 수 있었다.

탐지 이후 지연 없이 실행된 대응이 확산 범위를 결정적으로 제한한 핵심 요인이었다.

KEY TAKEAWAY

**정상 계정을 활용한 공격에서는 탐지 여부보다 그 이후의 판단과 대응 속도가 결과를 좌우한다.
초기 대응이 지연되는 순간, 공격은 이미 내부 확산 단계로 진입하게 된다.**

CASE 02

보안 솔루션이 있었지만, 이미 수천 개의 위협이 존재했던 환경

"보안 솔루션이 존재한다"는 사실은 "안전하다"는 것을 의미하지 않는다.
이 사례는 그 차이를 명확하게 보여준다.

WHAT HAPPENED

해당 기업은 기존 백신을 운영하고 있었고, 자사 환경이 일정 수준 이상 보호되고 있다고 인식하고 있었다.

그러나 Incident Response 과정에서 확인된 상황은 전혀 달랐다.

- 수천 개에 달하는 해킹툴, 트로이목마, 크립토마이너가 시스템 전반에 잠복해 있었고
- 관리자 계정 탈취 시도와 내부망 스캐닝이 이미 진행 중이었으며
- 일부 서버에서는 단시간 내 대량의 로그인 시도가 반복되고 있었다

즉, 공격자는 이미 내부에서 활동 기반을 확보한 상태였으며,
장기간 탐지되지 않은 상태에서 위협이 누적된 환경이었다.

WHAT WENT WRONG

이 사고의 핵심은 단일 취약점이 아니라, 여러 구조적 문제가 복합적으로 작용했다는 점에 있다.

- 외부에 노출된 웹 서비스와 취약점이 방치되어 있었던 점
- 기존 백신에 대한 신뢰로 인해 추가적인 탐지 체계가 미흡했던 점
- 공격 표면(Attack Surface)에 대한 지속적인 관리가 이루어지지 않았던 환경

이러한 조건 속에서 공격자는 장기간 탐지되지 않은 채 내부에서 활동을 이어갈 수 있었다.

WHAT CHANGED

PAGO는 단순한 위협 탐지에 그치지 않고, 즉각적인 가시성 확보와 대응 체계 재구성을 동시에 수행했다.

- EDR 및 NDR을 통한 전사 가시성 확보
- 외부 공격 표면(EASM) 진단을 통한 노출 자산 식별
- 잠복 위협 제거 및 추가 확산 차단

이를 통해 이미 진행 중이던 위협을 제거하고, 대규모 공격으로 이어질 가능성을 사전에 차단할 수 있었다.

단순 대응을 넘어, 보안 운영 구조 자체를 재정비하는 계기가 되었다.

KEY TAKEAWAY

보이지 않는 위협은 존재하지 않는 것이 아니라, 아직 발견되지 않았을 뿐이다.
탐지되지 않는 환경은 이미 침해된 상태일 가능성을 전제로 바라볼 필요가 있다.

Case Summary

두 사례는 서로 다른 환경에서 발생했지만, 공격의 출발점과 확산 방식은 매우 유사했다.

- 공격은 정상 계정 기반 접근으로 시작되며
- 초기 이상 징후는 존재하지만 신속한 분석과 대응으로 이어지지 않는다
- 이미 내부에서 공격 기반이 형성된 이후에야 상황이 인지된다

결국 문제는 침입 자체가 아니라, 탐지 이후 대응이 지연되는 구조에 있다.

공격의 속도와 개입 시점

앞선 사례들이 보여준 것이 '초기 침투와 대응 지연'이라면, 이 섹션은 한 단계 더 나아가 **공격의 진행 속도와 개입 시점이 결과를 어떻게 바꾸는지**에 집중한다. 실제 현장에서 확인되는 공격은 단순히 발생 여부가 중요한 것이 아니라, **어느 시점에서 대응이 이루어졌는지가 피해 규모를 결정짓는 핵심 변수로** 작용한다.

CASE 03

확산 직전 단계에서 차단된 대규모 공격

공격은 대부분 단일 이벤트로 시작되지 않는다. 오히려 여러 단계의 준비 과정을 거쳐, **최종 실행 단계에서 피해가 발생한다.**

WHAT HAPPENED

공격자는 외부에 노출된 RDP를 통해 관리자 계정을 확보한 뒤, 보안 솔루션을 비활성화하고 내부망 전반에 대한 확산 준비를 진행했다.

이미 수천 대의 자산이 공격 범위에 포함된 상태였으며, 랜섬웨어 배포 직전 단계까지 진행된 상황이었다.

이 시점에서 공격은 사실상 완료 직전 단계에 가까웠다.

WHAT WENT WRONG

이 사례의 핵심은 단일 취약점이 아니라, 공격이 준비되는 **과정에서 이를 차단하지 못한 구조**에 있다.

- 외부에 노출된 RDP 접근이 적절히 통제되지 않았던 점
- 관리자 계정 탈취 이후 추가 행위에 대한 탐지 및 차단이 이루어지지 않았던 점
- 보안 솔루션이 존재했음에도 불구하고 이를 무력화할 수 있는 환경이었던 점

공격은 단계적으로 진행되었지만, 각 단계에서 개입이 이루어지지 못하면서 최종 실행 직전까지 도달하게 되었다.

WHAT CHANGED

일부 행위 패턴을 기반으로 공격 거점 시스템이 식별되었고, 즉각적인 격리가 이루어졌다.

동시에 내부 확산 경로에 대한 분석이 병행되었으며, 공격이 확산되기 직전 단계에서 전체 흐름이 차단되었다.

결정적인 차이는 **얼마나 빨리 대응했는가가 아니라**, 어느 시점에서 개입했는가에 있었다.

KEY TAKEAWAY

공격은 한 번에 발생하지 않는다. **준비 → 장악 → 실행의 단계**를 거쳐 진행되며, 이 중 어느 단계에서 개입하느냐에 따라 결과는 완전히 달라진다.

CASE 04

암호화 이전 단계에서 중단된 랜섬웨어 공격

"많은 랜섬웨어 공격은 실제 암호화 이전에 이미 충분한 준비 과정을 거친다. 이 사례는 그 전형적인 흐름을 보여준다.

WHAT HAPPENED

심야 시간, 정상 계정을 활용한 비정상적인 접근이 발생했고, 공격자는 관리자 권한 확보 및 백도어 계정 생성을 시도했다.

이 과정은 랜섬웨어 공격의 전형적인 사전 장악 단계였으며, 이 시점을 놓칠 경우 실제 암호화로 이어질 가능성이 높은 상황이었다.

WHAT WENT WRONG

이 사례에서 문제는 기술적인 탐지 부족이라기보다, 이러한 행위를 '공격의 시작'으로 인식하지 못하는 구조였다.

- 정상 계정 기반 접근이라는 이유로 초기 위험도가 낮게 평가된 점
- 심야 시간대 발생으로 인해 대응이 지연될 가능성이 높았던 점
- 관리자 권한 확보 시도를 명확한 공격 신호로 연결하지 못한 점

이러한 요소들은 초기 개입 시점을 늦추는 주요 원인으로 작용한다.

WHAT CHANGED

초기 행위를 단순 이상 징후가 아닌 **공격의 전조 단계로 판단하고 즉시 개입함으로써,** 전체 공격 흐름이 실행 이전 단계에서 차단되었다.

관리자 계정과 관련된 활동이 차단되었고, 추가적인 권한 상승 및 확산 시도가 제한되었다.

이로 인해 공격은 실제 비즈니스 영향이 발생하기 이전에 종료될 수 있었다.

KEY TAKEAWAY

랜섬웨어 공격의 핵심은 암호화가 아니라, **그 이전 단계에서 얼마나 빠르게 개입할 수 있는**가에 있다. 실행 단계에서의 대응은 이미 늦은 경우가 많으며, 사전 장악 단계에서의 판단이 결과를 결정한다.

Case Summary

이 두 사례는 공격의 속도와 개입 시점의 중요성을 명확하게 보여준다. 공격은 짧은 시간 안에 대규모 확산 단계로 진입할 수 있으며, 그 이전에는 반드시 준비 및 장악 단계가 존재한다. 초기 징후를 인지하더라도 **개입 시점이 늦어지면 의미를 잃는다.** 사고의 규모는 공격의 강도가 아니라, **언제 개입했는가에 의해 결정된다.**

보이지 않는 위협과 시간의 문제

앞선 사례들이 보여준 것이 공격의 시작과 개입 시점이었다면, 이 섹션은 한 단계 더 나아가 탐지 자체가 어려운 위협과 대응 시간의 중요성에 집중한다. 최근 공격은 단순히 침투하는 것을 넘어, 흔적을 남기지 않거나 정상 행위로 위장하는 방식으로 진화하고 있다.

이러한 환경에서는 무엇을 탐지했는가보다, **무엇이 실제로 일어나고 있는지를 해석하는 능력**이 더욱 중요해진다.

CASE 05

흔적 없이 유지된 시스템 제어

공격은 항상 눈에 보이는 형태로 존재하지 않는다.
이 사례는 그 대표적인 흐름을 보여준다.

WHAT HAPPENED

공격자는 웹쉘(Web Shell)을 통해 시스템에 접근한 뒤, 초기 침투 흔적을 제거하고 메모리 기반으로 동작하는 백도어를 유지했다.

파일 기반의 악성코드는 대부분 삭제되었으며, 시스템에는 명확한 악성 파일이 거의 남아 있지 않은 상태였다.

또한 일부 로그가 의도적으로 삭제되거나 변조되어, 외부에서 확인 가능한 침해 흔적은 최소화된 상황이었다.

표면적으로는 정상 상태처럼 보였지만, 실제로는 외부에서 지속적인 제어가 이루어지고 있는 상태였다.

WHAT WENT WRONG

이 사례의 핵심은 탐지 대상이 명확하게 존재하지 않는 환경에 있었다.

- 파일 기반 탐지 중심의 보안 체계에서는 메모리 기반 공격을 식별하기 어려웠던 점
- 로그에 대한 신뢰가 전제되어 있었으나, 해당 로그 자체가 조작된 상태였던 점
- 행위 간의 연결 관계를 분석하지 못하고 개별 이벤트 단위로만 해석했던 점

이러한 조건에서는 공격이 존재하더라도, 이를 위협으로 인지하기 어려운 구조가 된다.

WHAT CHANGED

PAGO는 개별 이벤트가 아닌, **행위 간의 흐름과 맥락을 기반으로 이상 징후를 재구성했다.**

정상 활동처럼 보이는 행위들 사이의 비정상적인 연결성을 식별했고, 이를 기반으로 공격 흐름을 추적했다.

이 과정에서 숨겨진 백도어와 외부 제어 경로가 확인되었고, 해당 시스템에 대한 격리 및 차단이 이루어졌다.

결과적으로 눈에 보이지 않던 위협이 실제로 제거되었으며, 장기적인 침해 가능성이 차단되었다.

KEY TAKEAWAY

보이지 않는 위협은 존재하지 않는 것이 아니라, **탐지되지 않았을 뿐이다.**
단일 이벤트가 아니라 행위의 흐름을 이해하는 능력이 대응의 핵심이다.

CASE 06

단 30분 내 차단된 공격 시도

모든 공격이 장기간에 걸쳐 진행되는 것은 아니다.
일부 공격은 매우 짧은 시간 안에 확산될 수 있다.

WHAT HAPPENED

공격자는 취약한 웹 업로드 기능을 통해 악성 파일을 업로드하고, 이를 기반으로 리버스 쉘(Reverse Shell)을 생성해 외부와 연결을 시도했다.

이러한 공격 방식은 초기 침투 이후 곧바로 내부 제어권 확보로 이어질 수 있는 구조를 가지고 있다.

특히 외부 연결이 유지될 경우, 추가 명령 실행과 내부 확산이 빠르게 진행될 수 있는 상황이었다.

WHAT WENT WRONG

이 사례에서 문제는 공격의 복잡성이 아니라, 대응까지 허용되는 시간이 매우 제한적이었다는 점이다.

- 웹 애플리케이션 취약점이 사전에 관리되지 않았던 점
- 외부 연결 시도에 대한 즉각적인 탐지 및 차단 체계가 부족했던 점
- 초기 침투 이후 빠르게 진행되는 공격 흐름을 실시간으로 해석하지 못했던 점

이러한 조건에서는 대응이 몇 분만 지연되어도 공격이 내부 확산으로 이어질 수 있다.

WHAT CHANGED

해당 공격은 약 30분 이내에 탐지되었으며, 외부 연결 차단과 함께 관련 세션이 종료되었다.

추가적인 명령 실행이 이루어지기 이전에 공격 흐름이 차단되었고, 내부 확산 없이 종료될 수 있었다.

이 사례에서 중요한 것은 단순한 탐지가 아니라, 짧은 시간 내에 판단과 실행이 동시에 이루어졌다는 점이다.

KEY TAKEAWAY

공격의 난이도보다 중요한 것은 **대응까지 허용되는 소요 시간이다.**
대응이 몇 분만 늦어지더라도, 공격은 이미 다음 단계로 진행될 수 있다.

Case Summary

이 두 사례는 공격이 점점 더 보이지 않는 방식으로 진화하고 있으며, 동시에 대응 시간의 중요성이 더욱 커지고 있음을 보여준다. 위협은 파일이 아닌 행위 기반으로 존재하며, 단일 이벤트만으로는 전체 상황을 판단하기 어렵다. 따라서 대응의 핵심은 탐지가 아니라, 맥락을 해석하는 능력에 있다. 결국 보안은 무엇이 존재하는지를 확인하는 것이 아니라, 무엇이 실제로 일어나고 있는지를 이해하는 문제다.

3. PATTERNS BEHIND THE INCIDENTS

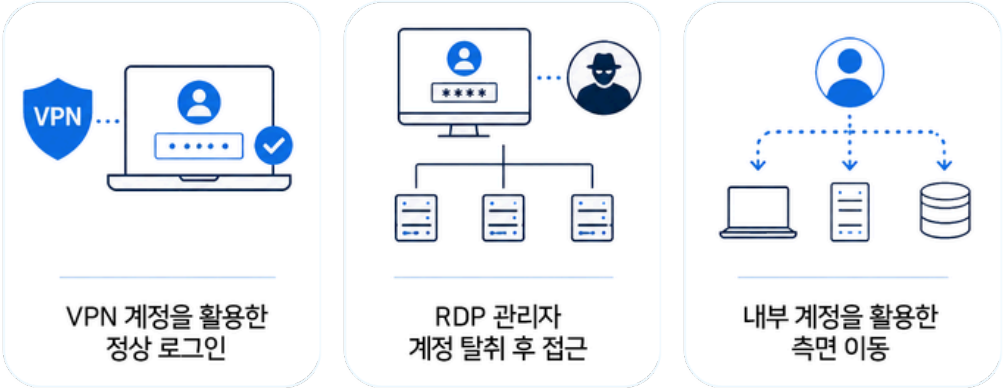
앞서 살펴본 6가지 Incident Response 사례는 서로 다른 산업과 환경에서 발생했지만, 그 전개 방식과 결과는 놀라울 만큼 유사했다. 이 점은 하나의 중요한 사실을 시사한다. **이 사건들은 개별적인 예외가 아니라, 현재 기업 보안 환경에서 반복되고 있는 구조적인 흐름이라는 것이다.**

1 공격은 '침입'이 아니라 '로그인'으로 시작된다

과거에는 외부에서 내부로의 침입 자체가 주요 위협이었다.

그러나 최근 사례에서 반복적으로 확인되는 공격의 출발점은 그와는 다른 양상을 보인다. 공격은 더 이상 경계를 넘는 과정에서 시작되지 않고, 이미 확보된 계정, 혹은 탈취된 인증 정보를 기반으로 정상적인 사용자처럼 시스템에 접근하는 방식이 일반화되고 있다.

반복적으로 확인된 접근 방식

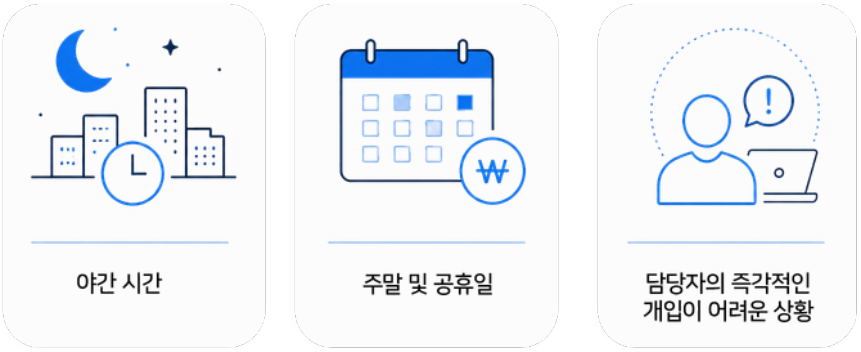


이러한 접근은 시스템 입장에서는 '정상 활동'으로 인식될 가능성이 높다. 이제 공격은 '들어오는 것'이 아니라, 이미 들어와 있는 상태에서 시작된다.

2 공격은 항상 '대응 공백'을 노린다

모든 사례에서 공통적으로 확인된 또 하나의 특징은 공격이 발생하는 시점이다. 대부분의 침해는 조직의 대응 역량이 약해지는 시간대를 선택해 이루어졌다.

주요 발생 시점



이 시간대에는 탐지 이후의 분석과 대응이 지연될 가능성이 높다. 공격자는 단순히 시스템의 취약점만을 노리는 것이 아니라, 조직의 운영 공백까지 함께 활용한다. 공격은 기술을 겨냥하기보다, 대응이 늦어지는 순간을 공략한다.

3 보안은 존재하지만, 완전하지 않다

여러 사례에서 확인된 또 하나의 공통점은 보안 시스템이 존재함에도 불구하고 사고가 발생했다는 점이다. 문제는 '없음'이 아니라 '불완전함'에 있었다.

반복적으로 발견된 환경

이러한 환경에서는 공격자가 보안이 적용되지 않은 지점을 우회 경로로 활용할 수 있다. 보안의 사각지대는 단순한 취약점이 아니라, 공격자가 의도적으로 선택하는 경로다.

4 기존 보안 체계는 공격의 변화를 따라가지 못한다

사례에서 확인된 공격 방식은 기존 보안 체계의 전제를 우회하는 방향으로 진화하고 있다.

주요 특징

이러한 공격은 단순 시그니처 기반 탐지나 단일 이벤트 분석으로는 식별이 어렵다. 특히 최근에는 자율적으로 판단하고 실행하는 자동화된 공격 기법의 증가와 함께, 공격은 더욱 빠르고 은닉된 형태로 진화하고 있다. 탐지 기술은 발전하고 있지만, 공격은 그 전제를 무력화하는 방향으로 진화하고 있다.

5 공격의 속도와 대응의 속도는 다르게 움직인다

현장에서 가장 크게 체감되는 변화는 공격의 속도다.

실제 사례에서 확인된 흐름

이 과정에서 시간은 계속 소모된다. 공격은 실시간으로 진행되지만, 대응은 여전히 단계적으로 지연된다. 이 격차가 실제 피해 규모를 결정짓는 핵심 요인이 된다.

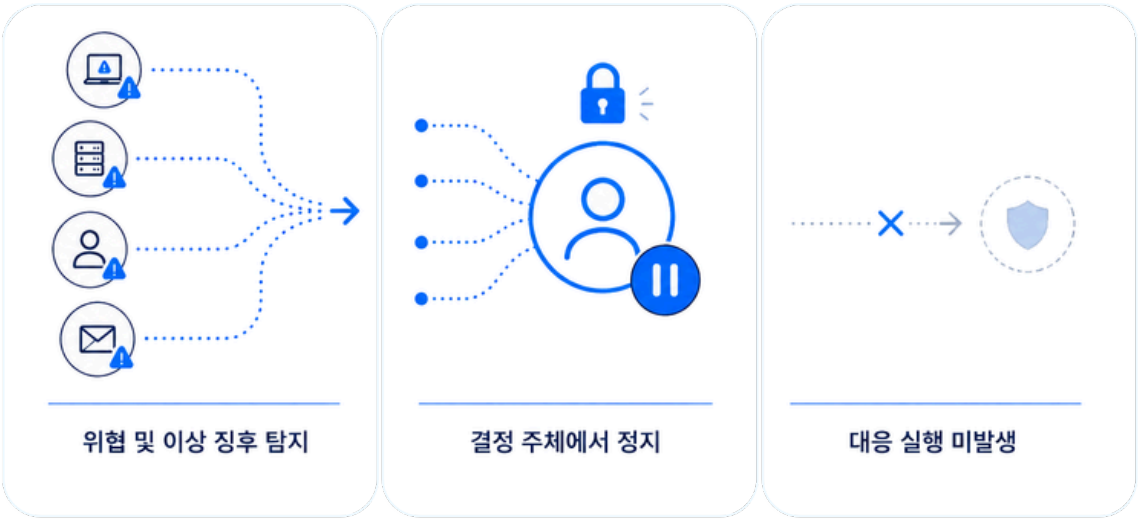
탐지 기술은 발전하고 있지만, 공격은 그 전제를 무력화하는 방향으로 진화하고 있다.

6 그리고 가장 중요한 문제

앞선 모든 패턴을 종합하면 하나의 질문으로 수렴된다. **'누가 결정하는가'**

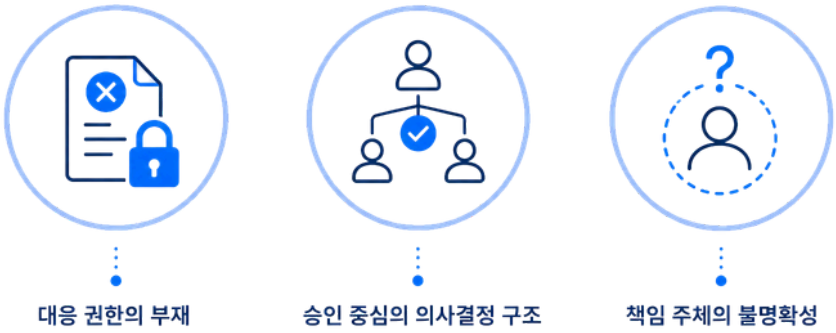
결정 지점에서 멈춘 대응 흐름

위협은 탐지되지만, 결정 구조에서 멈춰 실행으로 이어지지 않는다



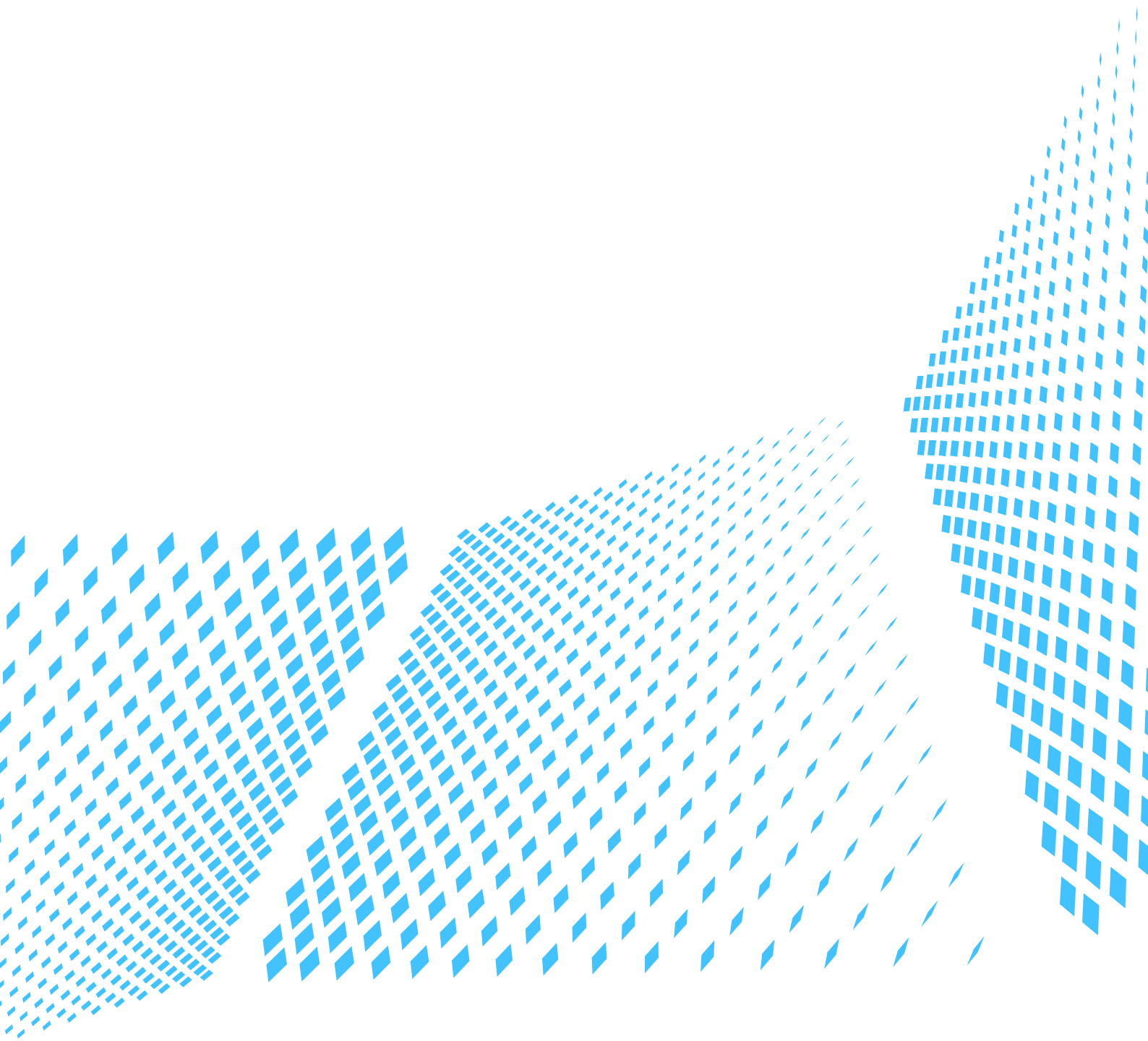
그 이유는 반복적으로 동일하다.

구조적 원인



이러한 환경에서는 탐지된 위협이 실제 대응으로 이어지기 어려워지고, 결국 많은 조직에서 보안은 '알고 있지만 멈추지 못하는 상태'에 머무르게 된다.

6가지 사례가 시사하는 바는 명확하다. **보안은 더 이상 '무엇을 탐지하는가'의 문제가 아니라, '누가, 언제, 어떻게 대응하는가'의 문제로 수렴하고 있다.**



4. INCIDENT RESPONSE를 통해 드러난 현실

많은 조직은 보안 체계를 운영하고 있음에도 불구하고, 실제 위협이 어떻게 발생하고 확산되는지에 대해서는 제한된 가시성만을 가지고 있다. 그 결과, 침해가 발생했음에도 이를 인지하지 못하는 상태가 만들어진다.

보안이 존재한다는 사실과, 실제로 안전한 상태라는 것은 서로 다른 문제다.

1 "우리는 안전하다"는 전제

대부분의 기업은 다음과 같은 이유로 자사의 보안 상태를 일정 수준 이상 안정적이라고 판단한다.

- 백신 및 EDR을 포함한 보안 솔루션 도입
- 방화벽 및 네트워크 보안 장비 운영
- 로그 수집 및 모니터링 체계 구축

이러한 요소들은 분명히 중요한 기반이다. 그러나 Incident Response 현장에서 반복적으로 확인되는 것은, 이러한 기반이 곧바로 '실제 안전'으로 이어지지는 않는다는 점이다.

실제 조사 과정에서는 다음과 같은 상황이 자주 발견된다.

⚠ 이미 내부에 위협이 잠복해 있는 상태
⚠ 공격자가 정상 계정을 활용해 활동 중인 환경
⚠ 일부 자산이 보안 적용 범위에서 제외된 구조

보안이 존재한다는 사실과, 실제로 안전한 상태라는 것은 서로 다른 문제다.

2 왜 많은 조직은 이를 인지하지 못하는가

이러한 간극이 발생하는 이유는 단순하지 않지만, 여러 사례를 통해 반복적으로 확인되는 몇 가지 특징이 존재한다.

탐지되지 않는 위협은 존재하지 않는 것으로 인식된다	탐지 이후의 대응은 별도의 문제로 남는다	가시성의 한계는 구조적으로 발생한다
		
• 파일리스 공격 • 정상 계정 기반 접근 • 로그 조작 및 흔적 제거	• 파일리스 공격 • 정상 계정 기반 접근 • 로그 조작 및 흔적 제거	• 파일리스 공격 • 정상 계정 기반 접근 • 로그 조작 및 흔적 제거
이러한 유형의 공격은 기존 탐지 체계에서 명확한 경고 신호를 남기지 않는 경우가 많다. **결과적으로 위협은 존재하지만, 조직은 이를 인지하지 못한 채 운영을 지속하게 된다.**	이 과정에서 위협은 '알림'으로 남고, 실제 공격은 계속 진행된다.	이러한 구조에서는 조직이 인지하는 보안 상태와 실제 환경 사이에 차이가 발생할 수밖에 없다.

3 Free Incident Response에서 확인 가능한 사항들

PAGO의 Free Incident Response는 단순한 서비스 제공이 아니라, 현재 보안 상태를 실제 환경 기준에서 재해석하는 과정에 가깝다.

Free IR을 통해 확인되는 핵심 요소

- 현재 침해 여부 및 진행 중인 위협
- 기존 보안 체계에서 놓치고 있는 영역
- 공격의 시작 지점과 확산 경로
- 대응 프로세스 및 의사결정 구조의 한계

이 과정에서 많은 조직은 처음으로 다음과 같은 사실을 인식하게 된다. 문제는 탐지 자체가 아니라, 탐지 이후를 어떻게 운영할 것인가에 있다.

4 Free IR 이후의 변화

실제 Incident Response를 경험한 조직은 보안에 대한 관점을 다시 정리하게 된다.

- 보안 상태에 대한 인식의 변화
- 탐지 중심에서 대응 중심으로의 관점 전환
- 운영 구조 및 대응 프로세스 재정비 필요성 인식

이는 단순한 점검 결과를 넘어, 보안 전략 전반에 영향을 미치는 변화로 이어진다. **Free IR은 문제를 해결하는 과정이 아니라, 문제를 정확하게 이해하는 출발점이다.**

5 중요한 질문

이제 다시 처음의 질문으로 돌아간다.
지금 우리 조직은 실제로 안전한가, 아니면 아직 확인되지 않았을 뿐인가.

이 질문에 대한 답은 일반적인 모니터링이나 보고서만으로는 확인하기 어렵다. 실제 환경을 기준으로, 현재 상태를 직접 확인하는 과정이 필요하다.

5. FROM INCIDENT RESPONSE TO MDR

많은 조직은 사고가 발생한 이후에야 문제를 인지하고, 그 시점부터 대응을 시작한다. 이러한 접근은 일정 부분 불가피한 측면도 있다.

앞선 사례와 분석을 통해 확인된 사실은 비교적 분명하다. 많은 조직은 사고가 발생한 이후에야 문제를 인지하고, 그 시점부터 대응을 시작한다. 이러한 접근은 일정 부분 불가피한 측면도 있다. Incident Response(IR)는 침해 여부를 확인하고, 공격의 경로와 원인을 분석하며, 이미 발생한 위협을 제거하는 데 있어 필수적인 과정이기 때문이다.

그러나 실제 현장에서 IR은 종종 "문제를 해결하는 단계"라기보다, 문제가 어디까지 진행되었는지를 확인하는 단계로 기능하는 경우가 많다.

5.1 Incident Response의 역할과 한계

IR은 보안 운영에서 반드시 필요한 기능이지만, 그 특성상 몇 가지 구조적인 한계를 내포하고 있다. 무엇보다 IR은 본질적으로 사고 이후에 작동하는 프로세스로, IR이 시작되는 시점에는 이미 공격자가 내부에 존재하거나, 일정 수준 이상의 활동 기반을 확보한 상태일 가능성이 높다.

또한 IR 과정에서는 다음과 같은 상황이 반복적으로 발생한다.

- 특정 자산을 격리할 것인지
- 서비스를 중단할 것인지
- 계정을 차단할 것인지

이와 같은 결정은 대부분 고객의 승인에 의존하며, 조직 내부의 판단 과정을 거쳐야 한다. 이 과정 자체는 합리적인 절차이지만, 문제는 그만큼 시간이 소모된다는 점이다.

결국 IR은 다음과 같은 구조적 특성을 갖는다.

- 사고 발생 이후에 시작된다
- 대응은 고객의 의사결정에 의존한다
- 실행까지 일정한 지연이 발생한다

그리고 이러한 조건에서는 탐지와 대응 사이에 간극이 생기기 쉽다.

5.2 문제는 '탐지 이후'에서 발생한다

앞선 사례들을 다시 보면, 공통적으로 나타나는 특징이 있다. 위협은 탐지되었지만, 그 순간 즉시 대응으로 이어지지 않았다는 점이다. 이 문제는 기술적인 한계라기보다, 운영 구조에서 비롯된다.

- 대응 권한이 제한되어 있거나
- 승인 절차가 필요하거나
- 책임 주체가 명확하지 않은 경우

위협은 '확인된 상태'에 머무르게 되고, 그 사이에서도 공격은 멈추지 않는다.

오히려 그 시간 동안 내부 확산, 추가 권한 확보, 다음 단계 공격 준비가 이루어진다. 결국 많은 조직에서 보안은 "위협은 알고 있지만, 실제로는 멈추지 못하는 상태"에 놓이게 된다.

5.3 MDR이 해결하는 방식

이 지점에서 등장하는 개념이 **Managed Detection & Response, 즉 MDR이다.**
MDR은 단순히 탐지 기능을 확장하는 것이 아니라, 탐지 이후의 공백을 줄이기 위한 운영 모델에 가깝다.
기존 IR과의 가장 큰 차이는 "판단과 실행이 어디에서 이루어지는가"에 있다.

MDR의 핵심 특징

- 24시간 기반의 지속적인 보안 운영
- 위협에 대한 실시간 분석과 판단
- 사전 정의된 정책에 따른 즉각적인 대응
- 공격 확산 이전 단계에서의 선제적 차단

MDR은 탐지된 위협을 '알림'으로 남기지 않고, 실제 조치로 연결하는 구조를 만든다.

5.4 IR과 MDR의 차이 (구조적 관점)

두 개념은 기능적으로 일부 겹치지만, 운영 방식과 목적에서는 분명한 차이가 존재한다.

구분	Incident Response	MDR
시점	사고 이후	사고 이전 및 실시간
역할	분석 및 원인 파악	판단 및 대응 실행
대응 방식	고객 승인 중심	사전 정의된 ROE 기반
속도	절차에 따라 지연 가능	즉각적
책임 구조	고객 중심	서비스 제공자와 분산

이 차이는 단순한 기능 비교가 아니라, 보안을 바라보는 관점 자체의 차이를 의미한다.

5.5 왜 MDR은 점점 필수 요소가 되는가

공격의 양상은 빠르게 변화하고 있다.

- 정상 계정 기반 접근 증가
- 탐지를 회피하는 방식의 일반화
- 공격 속도의 지속적인 가속

특히 최근에는 자율적으로 판단하고 실행하는 Agentic AI 기반 자동화가 확산되면서, 공격은 더욱 빠르고 반복적인 형태로 진화하고 있다.

이러한 환경에서는 기존의 탐지 중심 구조만으로는 모든 상황에 대응하기 어렵다. 특히 대응이 지연되는 구조에서는 작은 침해가 빠르게 확산될 가능성이 높다. 결국 필요한 것은 더 많은 탐지 기술이 아니라, 탐지 이후를 어떻게 운영할 것인가에 대한 구조다.

5.6 PAGO의 접근 방식

PAGO는 MDR을 단순한 서비스가 아니라 보안 운영 구조 자체로 정의한다.

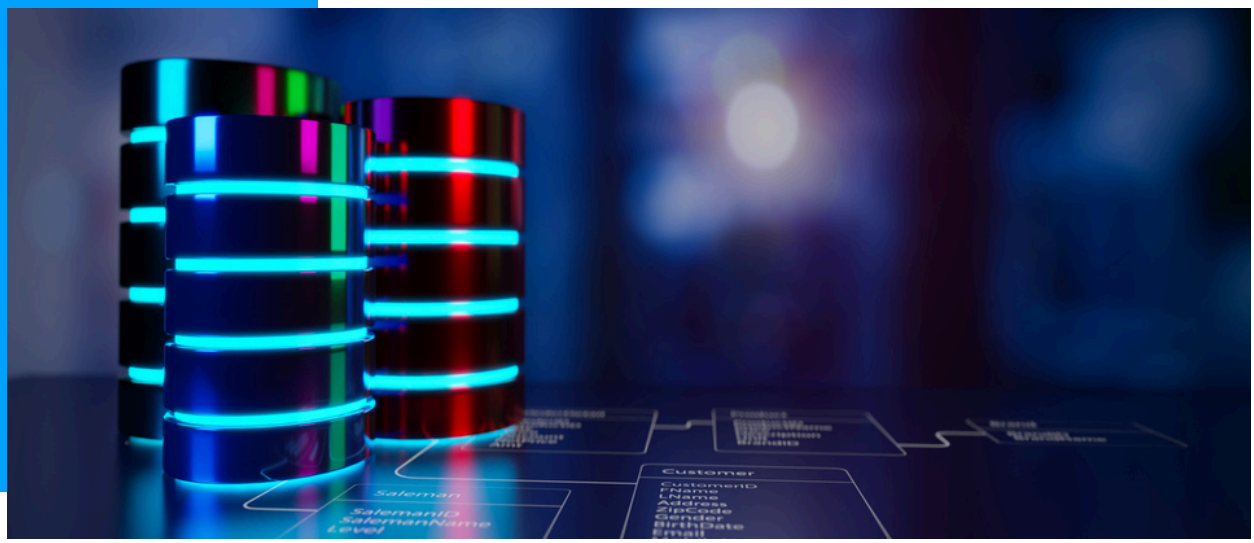
AI 기반 탐지와 전문가 분석의 결합

전사 가시성을 확보하는 통합 플랫폼 구조

Threat Hunting 및 자동화된 대응 체계

필요 시 즉각적인 격리 및 확산 차단

이러한 구조를 통해 탐지된 위협은 단순히 보고되는 것이 아니라, 상황에 따라 즉각적인 조치로 이어진다. PAGO MDR의 핵심은 탐지를 넘어, 결정을 실행하는 것에 있다.



6. CONCLUSION

앞선 사례와 분석을 통해 확인된 사실은 명확하다. 많은 조직은 보안 시스템을 운영하고 있음에도 불구하고, 실제 위협이 어떻게 발생하고 확산되는지에 대해서는 제한된 가시성만을 가지고 있다. 그 결과, 위협은 탐지되거나 인지되더라도 즉각적인 대응으로 이어지지 않는 구조가 반복된다.

이번 리포트에서 살펴본 6가지 사례는 이를 명확하게 보여준다. 공격은 더 이상 외부에서 침입하는 형태로 시작되지 않으며, 정상 계정과 합법적인 접근 방식을 기반으로 내부에서 확산된다. 또한 공격은 짧은 시간 안에 빠르게 진행되며, 대응이 지연되는 순간 이미 다음 단계로 넘어가게 된다.

이러한 환경에서 보안의 핵심은 더 이상 '탐지'가 아니다. 누가, 언제, 어떤 기준으로 대응을 실행할 수 있는가가 실제 결과를 결정짓는 요소가 된다.

특히 현재와 같이 공격의 속도와 복잡성이 지속적으로 증가하는 환경에서는,
탐지 중심의 보안 구조만으로는 모든 상황에 대응하기 어렵다. 결국 필요한 것은
더 많은 경고가 아니라, 더 빠르고 명확한 판단과 실행이 가능한 운영 구조다.
보안은 기술 위에서 시작되지만, 결국 판단과 실행을 통해 완성된다.

7. FREE INCIDENT RESPONSE를 통한 확인

Next Step

현재 보안 환경을 기준으로, 귀사의 실제 상태를 직접 확인해보시기 바랍니다.

PAGO의 Free Incident Response는 단순한 점검이 아니라, 현재 환경에서 실제로 어떤 위협이 존재하고 있으며, 그 위협이 어떻게 진행되고 있는지를 확인하는 과정입니다.

Free IR을 통해 확인 가능한 영역

- 현재 침해 여부 및 진행 중인 위협
- 공격의 시작 지점과 확산 경로
- 보안 사각지대 및 노출 영역
- 대응 프로세스 및 운영 구조

Request Free IR

이 과정은 단순한 상태 점검을 넘어, 실제 대응 가능한 보안 구조를 재정의하는 출발점이 됩니다.

지금, 귀사의 보안 상태를 실제 환경 기준에서 확인해 보시기 바랍니다. **중요한 것은 침해 여부가 아니라, 지금 이를 확인하고 대응할 수 있는 구조를 가지고 있는가에 있습니다.**

www.pagonetworks.com