Playbook

침해 이후 골든 타임 확보가 관건

Dwell Time 줄이는 AhnLab EDR 대응 플레이북

AhnLab

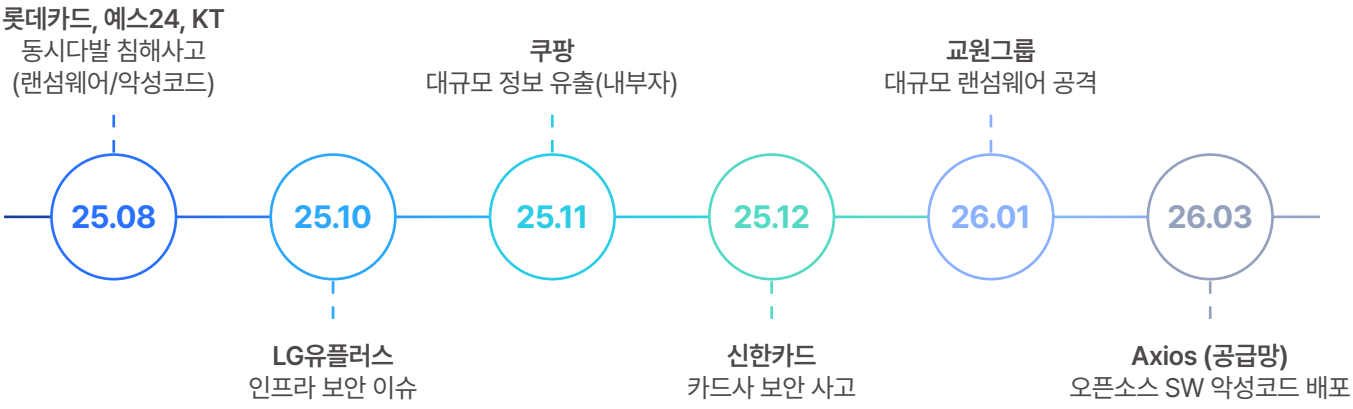
목차

2025~2026 주요 침해사고 인사이트

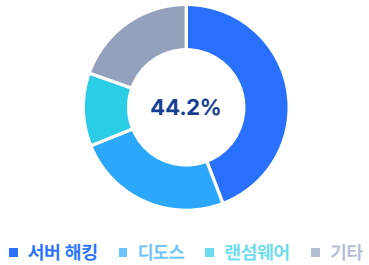
국내 침해사고는 2025년 들어 뚜렷한 증가세를 보였으며, 공격 양상 역시 복합화되고 있다. 2025년 침해사고는 총 2,383건으로 전년 대비 26.3% 증가했고, 이 중 서버 해킹이 44.2%로 가장 높은 비중을 차지했다. 디도스(DDoS)와 랜섬웨어도 주요 위협으로 확인됐다.

이는 기업 인프라 전반에 대한 다층적 공격이 이어지고 있음을 보여준다. 주요 사고 흐름을 보면, 2025년 8월 롯데카드·예스24·KT에서 랜섬웨어 및 악성코드 기반 침해사고가 동시다발적으로 발생했고, 이후 LG유플러스 인프라 보안 이슈, 쿠팡 대규모 정보 유출, 교원그룹 랜섬웨어 공격, Axios 공급망 공격 등이 이어졌다. 이들 사례는 공격자가 서버, 계정, 정상 소프트웨어, 오픈소스 패키지 등 다양한 경로를 악용하고 있음을 보여준다.

주요 사건으로 보는 공격 트렌드와 대응 시사점

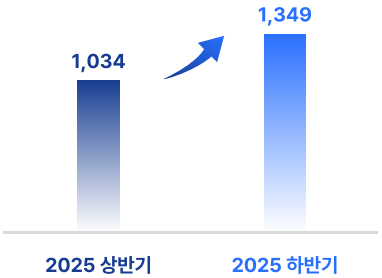


서버 해킹 비중 1위



2025년 침해사고 유형 중
가장 높은 비중 차지

침해사고 발생 속도 가속화



2025년 하반기 **1,349건**
상반기 대비 **36.5%** 증가

대기업 타깃 공격 확대

5.8%

랜섬웨어·공급망 공격 중심
표적형 위협 고도화

Threat Highlights

- 침해사고는 양적으로 증가했을 뿐만 아니라 공격 대상과 방식도 함께 고도화되고 있다.
- 공격자는 서버 해킹, 랜섬웨어, 공격망 공격 등 다양한 경로를 활용해 기업의 핵심 자산과 운영 환경을 정밀하게 노린다.
- 대기업과 주요 서비스 인프라를 겨냥한 표적형 공격이 확대되면서, 침해사고는 장기 잠복, 정보 유출, 서비스 중단으로 이어질 가능성이 커지고 있다.
- 기업은 사고 발생 이후의 대응 속도를 높이고, 공격 흐름을 조기에 식별·차단할 수 있는 EDR 중심 대응 체계를 강화할 필요가 있다.

결국 침해 대응은 공격 유입을 막는 데 그치지 않고, 침투 이후 공격자가 내부에서 머무는 시간을 줄이고 데이터 유출이나 대량 암호화로 이어지기 전에 공격 흐름을 끊는 것이 무엇보다 중요하다. 이때 핵심 지표가 바로 공격자의 체류 시간, 즉 Dwell Time이다.

본 가이드는 2025~2026년 주요 침해사고를 바탕으로, EDR 관점에서 침해 이후 탐지와 대응 방안을 정리한다. 랜섬웨어/서버 해킹, 정상 도구 악용 공격, 패키지 공급망 공격, 신뢰 기반 위장 공격 등 주요 공격 사례를 4가지 Playbook으로 재구성해 각 공격 흐름과 EDR 탐지 포인트, 차단·격리 중심의 대응 방안을 살펴본다. 이를 통해 Dwell Time을 줄이기 위해 어느 지점에서 탐지하고 차단해야 하는지를 제시한다.

가이드 활용법

- **최근 침해사고 흐름과 주요 위협 유형 파악**
  2025년 침해사고 증가세와 서버 해킹, 디도스, 랜섬웨어 등 주요 공격 유형을 살펴보고, 국내 주요 사고가 어떤 흐름으로 전개됐는지 확인한다.
- **Dwell Time 단축의 중요성 이해**
  침투 이후 공격자가 내부에 머무는 시간이 길어질수록 데이터 유출, 내부 확산, 대량 암호화로 이어질 가능성이 커진다. Dwell Time을 침해 대응의 핵심 지표로 보고, AhnLab EDR로 이를 단축하는 방법을 제시한다.
- **대표 침해 시나리오별 EDR 탐지 포인트 확인**
  랜섬웨어/서버 해킹, 정상 도구 악용 공격, 패키지 공급망 공격, 신뢰 기반 위장 공격 등 4가지 Playbook을 통해 공격 흐름과 탐지 포인트를 확인한다.
- **침해 이후 즉시 대응해야 할 액션 점검**
  의심 프로세스 종료, 감염 호스트 격리, C2 통신 차단, 악성 파일 제거, 인증서 폐기·재서명 등 사고 유형별 대응 방향을 살펴본다.
- **AhnLab EDR 도입 이후 운영 과제 구체화**
  30/60/90일 로드맵을 바탕으로 보호 자산 식별, 탐지 정책 설정, 룰 튜닝, 자동화 대응, 침해 대응 훈련 등 운영 단계별 과제를 정리한다.

왜 기존 보안만으로는 부족한가

최근 침해사고는 전통적인 악성코드 탐지만으로 식별하기 어려운 방식으로 전개되고 있다. 공격은 단일 파일 실행으로 끝나지 않고, 침투 이후 권한 확보·측면 이동·C2 통신·데이터 수집·대량 암호화 등 여러 행위가 연결된 흐름으로 나타난다. 이에 따라 침해 대응은 프로세스 실행, 파일 생성, 레지스트리 변경, 외부 통신과 같은 엔드포인트 행위를 종합적으로 분석하고, 공격 흐름을 조기에 차단하는 방식으로 확장돼야 한다.

시그니처·평판 기반 탐지의 한계

기존 백신/엔드포인트 보호 플랫폼(EPP)은 알려진 악성코드 차단과 시그니처·평판 기반 탐지에 강점이 있지만, 신·변종 위협이나 랜섬웨어 우회에는 한계가 있다.

정상 도구·정상 서명·정상 패키지 신뢰 악용

공격자는 조직이 신뢰하는 요소를 우회 경로로 활용한다. AnyDesk와 같은 정상 원격 도구는 원격 제어 유지에 악용될 수 있고, 탈취된 코드서명 인증서는 악성코드를 정상 프로그램처럼 위장하게 만든다. 오염된 오픈소스 패키지는 개발 환경과 CI/CD 파이프라인까지 공격 경로를 넓힐 수 있다.

단일 이벤트가 아닌 공격 흐름으로 전개

공격은 취약점 악용이나 웹셸 침투에서 시작해 권한 확보 → 내부 정찰 → 측면 이동 → C2 통신 → 데이터 수집 → 대량 암호화로 이어질 수 있다. 개별 이벤트는 정상처럼 보일 수 있지만, 타임라인으로 연결하면 침해 흐름이 드러난다.

최근 공격 양상은 다음과 같은 탐지 기준의 전환을 요구한다.

기존 탐지 방식의 한계	최근 공격 방식	필요한 대응 관점
알려진 악성코드 중심 탐지	신종·변종·파일리스 공격	행위 기반 탐지
정상 프로그램 신뢰	AnyDesk 등 정상 도구 악용	실행 맥락 분석
서명 파일 신뢰	코드서명 인증서 유출	서명 여부·행위 검증
패키지 신뢰	Axios 등 오픈소스 공급망 공격	설치 이후 프로세스·통신 추적
단일 이벤트 중심 분석	장기 잠복, 정찰, C2 통신	공격 타임라인 가시화

> 기존 탐지 방식의 한계는 단순히 악성 파일을 놓치는 데 있지 않다. 문제는 정상처럼 보이는 실행, 설정 변경, 외부 통신이 서로 연결될 때 만들어지는 침해 흐름을 얼마나 빠르게 식별하느냐에 있다. AhnLab EDR은 이런 행위의 연관성을 공격 타임라인으로 재구성해 데이터 유출이나 대량 암호화에 도달하기 전 대응할 수 있도록 돕는다.

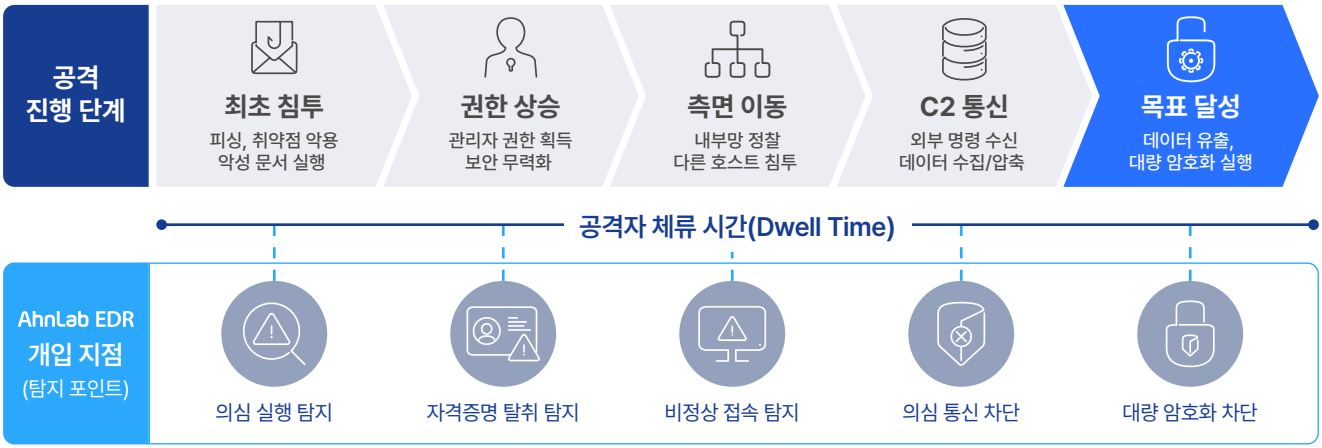
Dwell Time 단축이 중요한 이유: AhnLab EDR의 역할

Dwell Time은 공격자가 최초 침투한 이후 탐지·제거되기까지 내부에 머무는 시간을 의미한다. 이 시간이 길어질수록 공격자는 내부 정찰, 권한 상승, 데이터 수집, C2 통신, 측면 이동을 반복하며 공격 범위를 넓힌다. 랜섬웨어 공격은 대량 암호화와 이중 협박으로, 정보 유출 사고는 장기간의 고객 데이터 수집과 외부 전송으로 피해가 확대될 수 있다.

침해 대응의 핵심은 공격자가 목표를 달성하기 전 MTTD와 MTTR을 줄이는 것이다. MTTD는 위협 발생 후 탐지까지 걸리는 시간, MTTR은 탐지 후 격리·삭제·복구까지 걸리는 시간을 의미한다. 두 지표가 줄어들수록 Dwell Time이 짧아진다.

AhnLab EDR은 공격 사이클의 각 단계에서 의심 행위를 실시간으로 탐지하고, 악성 프로세스 종료, 감염 호스트 격리, C2 통신 차단 등 대응 조치를 수행한다. 이를 통해 공격자가 데이터 유출이나 대량 암호화에 도달하기 전 공격 흐름을 미리 차단한다.

공격 단계별 AhnLab EDR 개입 지점과 Dwell Time 단축 흐름



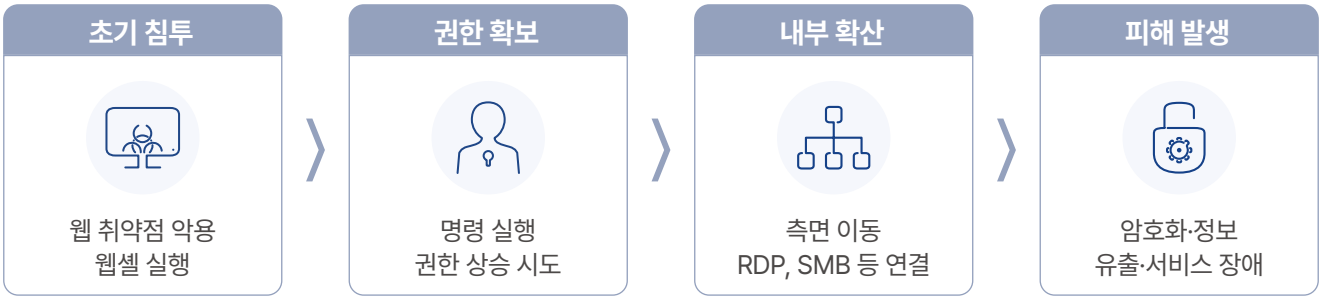
정상처럼 보이는 실행, 설정 변경, 외부 통신도 서로 연결되면 일련의 침해 흐름이 된다. AhnLab EDR은 이런 공격 흐름을 조기에 식별해 탐지 지연을 줄이고, 공격자가 목표를 달성하기 전 조기에 대응할 수 있도록 돕는다.
이때 핵심은 위협을 인지까지 걸리는 MTTD와 탐지 이후 조치까지 소요되는 MTTR을 함께 줄여, 공격자의 Dwell Time과 피해 확산 가능성을 낮추는 것이다.

Playbook 1. 랜섬웨어/서버 해킹

대량 암호화·서비스 중단·정보 유출 대응

랜섬웨어/서버 해킹은 취약 서버나 웹셸을 통해 내부망에 침투한 뒤, 내부 정찰과 측면 이동, C2 통신을 거쳐 대량 암호화나 정보 유출, 서비스 장애로 이어질 수 있다. 백업 삭제 시도나 데이터 유출이 결합되면 비즈니스 중단·개인정보 유출·이중 협박으로 피해가 확대되고, 기업 평판에도 직접적인 영향을 미친다.
대응의 핵심은 피해가 가시화된 후 복구하는 것이 아니라, 침투 이후의 의심 프로세스 실행, 장기 잠복, 내부 확산, 대량 파일 변경 징후를 조기에 식별해 차단하는 것이다.

랜섬웨어/서버 해킹 공격 흐름



AhnLab EDR 기반 탐지 포인트

랜섬웨어/서버 해킹 대응에서는 악성 파일 자체보다 침투 이후의 행위 흐름을 먼저 봐야 한다. 웹셸이나 취약 서버를 통해 실행된 의심 명령, 내부 정찰과 측면 이동, C2 통신, 대량 파일 변경은 암호화나 정보 유출로 이어지기 전 포착해야 할 핵심 징후다.

탐지 영역	EDR 탐지 포인트
침투 이후 실행 행위	웹셸 이후 웹 서버 프로세스 하위의 비정상 명령·스크립트 실행 탐지
내부 확산·통신 행위	내부 정찰, 측면 이동, 원격 접속, C2 통신, 데이터 수집·전송 연관 분석
피해 발생 전조 행위	대량 파일 변경, 암호화 패턴, 볼륨 섀도우 복사본 삭제, 백업 파일 손상 시도 탐지

탐지 이후 대응 절차

이런 징후가 확인되면 공격 흐름을 즉시 차단하는 것이 대응의 첫 번째 단계다. 감염 의심 서버를 격리해 내부 확산을 막고, 실행 중인 악성 프로세스와 외부 통신을 차단한 뒤, 암호화·유출·백업 손상 범위를 확인해 복구와 재발 방지 조치로 이어가야 한다.

No.	대응 단계	수행 내용	EDR 활용 포인트
1	감염 서버 격리	감염 의심 서버·호스트를 네트워크에서 분리	호스트 격리 정책 적용
2	실행 차단	의심 프로세스 종료, 웹셸·악성 스크립트 제거	프로세스 트리 기반 종료
3	통신 차단	C2 통신 및 추가 원격 접속 차단	의심 네트워크 연결 차단
4	피해 범위 확인	대량 파일 변경, 백업 삭제, 데이터 접근·유출 여부 확인	파일·네트워크 이벤트 타임라인 분석
5	복구·재발 방지	백업 무결성 확인, 동일 IOC·행위 전사 검색	IOC·행위 패턴 기반 헌팅

> **골든 타임: 웹셸 침투와 내부 확산 징후가 나타나는 초기 단계**
> AhnLab EDR은 의심 실행, 내부 확산, C2 통신, 대량 파일 변경 흐름을 공격 타임라인으로 연결해 암호화 및 정보 유출 이전의 차단 시점을 앞당긴다. 이를 통해 Dwell Time을 수 시간 또는 수 분 단위로 줄이고, 대규모 감염과 서비스 중단, 데이터 유출 피해를 최소화한다.

Playbook 2. 정상 도구 악용 공격

AnyDesk 등 정상 도구를 통한 지속 제어 대응

AnyDesk와 같은 정상 원격 제어 도구는 IT 지원 및 원격 근무에 활용되지만, 공격 흐름 안에서는 내부 제어권을 유지하고 탐지를 우회하는 수단으로 악용될 수 있다. 공격자는 취약한 서버나 계정을 통해 초기 침투한 뒤 백도어를 실행하고, PowerShell 스크립트 등을 활용해 원격 제어 도구를 백그라운드로 설치하거나 무인 액세스 설정을 강제할 수 있다.

이 유형의 공격에서는 원격 제어 도구의 실행 자체보다 설치 맥락과 실행 주체, 설정 변경, 외부 통신을 함께 보는 것이 중요하다. 정상 프로그램처럼 보이는 도구도 비정상 흐름 안에서 실행된다면, 공격자의 지속 제어 수단으로 전환될 수 있기 때문이다.

정상 도구 악용 공격 흐름

AhnLab EDR 기반 탐지 포인트

정상 도구 악용 공격은 개별 행위만 보면 정상 운영 활동처럼 보일 수 있다. AhnLab EDR은 프로세스 실행, 파일 생성, 설정 변경, 외부 접속의 연관성을 분석해 정상적인 원격 지원과 공격자의 지속 제어 행위를 구분한다.

탐지 영역	EDR 탐지 포인트
비정상 실행 흐름	서버·업무 프로세스 하위에서 원격 제어 도구 설치 또는 명령·스크립트 실행이 발생하고, 백도어 실행으로 이어지는 흐름 탐지
정상 도구 악용 행위	비인가 경로 파일 생성, Silent 설치, 무인 액세스 설정, 서비스·레지스토리 등록 등 비정상 설치·설정 변경 탐지
지속 제어·외부 통신	원격 제어 세션, C2 통신, 우회 포트 연결, 데이터 유출 트래픽 등 외부 제어 흐름의 지속 여부 확인

탐지 이후 대응 절차

정상 도구 악용 공격에 대응하려면 원격 제어 세션이 장기화되기 전 공격자의 제어 흐름을 차단하는 것이 우선이다. 감염 의심 호스트를 격리하고 실행 중인 원격 제어 도구, 스크립트, 백도어 프로세스를 종료한 뒤, 무단 설정과 지속성 확보 흔적을 제거해 공격자의 재접속 가능성을 차단한다.

No.	대응 단계	수행 내용	EDR 활용 포인트
1	실행 차단	원격 제어 도구, PowerShell 스크립트, 백도어 및 부모 프로세스 트리 강제 종료	고위험 패턴 탐지 시 프로세스 트리 기반 종료
2	호스트 격리	감염 징후가 확인된 서버·단말을 네트워크에서 분리	네트워크 격리 정책 적용으로 내부 측면 이동 차단
3	통신 차단	C2 통신, 비인가 외부 접속, 원격 제어 연결 시도 차단	의심 네트워크 연결 및 우회 포트 차단
4	설정 복구	무인 액세스 설정, 서비스 등록, 레지스트리 변경 등 무단 설정 제거	파일·레지스트리 변경 이벤트 분석 및 정상 상태 복구
5	재접속 방지 점검	비인가 원격 제어 파일 삭제, 계정·접속 정책 점검, 동일 행위 재발 여부 확인	동일 IOC·행위 패턴 기반 전사 헌팅

> **골든 타임: 정상 도구 설치 및 무인 액세스 설정 직후**
> AhnLab EDR은 원격 제어 도구의 실행 맥락, 설정 변경, 외부 통신 흐름을 연관 분석해 비정상 사용 여부를 식별한다. 이를 통해 공격자가 원격 제어 세션을 장기간 유지하기 전 제어 흐름을 끊고, Dwell Time을 줄인다.

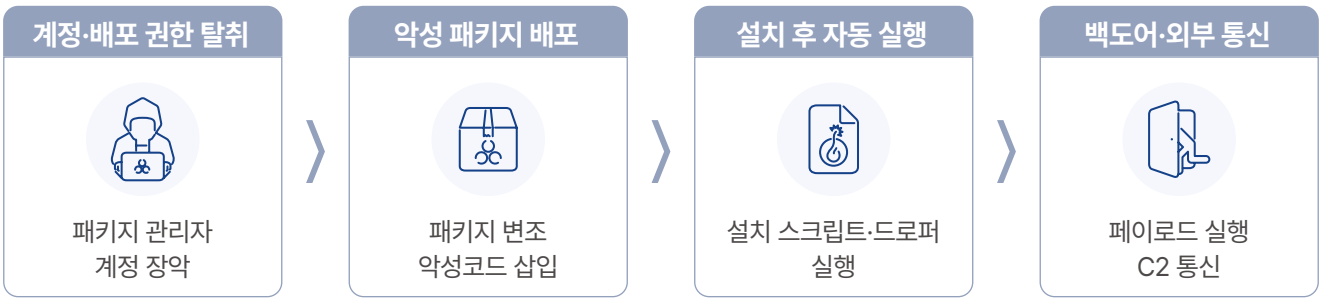
Playbook 3. 패키지 공급망 공격

오픈소스 패키지 설치 이후 악성 실행 흐름 대응

패키지 공급망 공격은 개발자가 신뢰하는 오픈소스 패키지와 설치 과정을 악성코드 유포 경로로 악용한다. Axios 공급망 공격 사례에서는 메인테이너 계정이 탈취된 뒤 악성 버전이 npm에 등록됐고, 설치 과정의 자동 실행 스크립트를 통해 드로퍼와 백도어가 실행되는 흐름이 확인됐다.

패키지 공급망 공격의 핵심 관찰 지점은 설치 이후의 실행 흐름이다. 정상 설치 과정처럼 보이더라도 설치 직후 의심 프로세스와 외부 통신이 이어진다면, 신뢰된 패키지가 개발 환경을 오염시키는 공격 경로가 될 수 있다.

패키지 공급망 공격 흐름



AhnLab EDR 기반 탐지 포인트

패키지 공급망 공격은 정상적인 설치 과정 안에서 시작되기 때문에, 패키지명이나 다운로드 여부만으로는 위협을 판단하기 어렵다. AhnLab EDR은 설치 직후 발생하는 프로세스 실행, 파일 생성, 지속성 확보, 외부 통신을 연관 분석해 정상 설치와 악성 실행 흐름을 구분해야 한다.

탐지 영역	EDR 탐지 포인트
설치 후 실행 흐름	패키지 설치 직후 Node.js 프로세스 하위에서 의심 자식 프로세스가 생성되거나, 스크립트·명령 실행으로 이어지는 흐름 탐지
페이로드·지속성 행위	OS별 페이로드 다운로드, 은닉 경로 파일 생성, 레지스트리 Run 키 등록 등 지속성 확보 행위 탐지
C2 통신·정보 수집	주기적 비커닝(Beaconing), 외부 C2 통신, 시스템 정찰·파일 열거·명령 실행 등 백도어 행위 연관 분석

탐지 이후 대응 절차

패키지 공급망 공격은 감염 단말 조치만으로 끝나지 않는다. 악성 패키지 버전과 설치 이력을 확인하고, 개발자 PC와 CI/CD 환경을 격리한 뒤, 캐시·토큰·API 키 등 개발 환경 전반의 노출 가능성을 함께 점검해야 한다.

No.	대응 단계	수행 내용	EDR 활용 포인트
1	영향 범위 확인	악성 패키지 버전, 설치 이력, 의존성 포함 여부 확인	패키지 설치 시점과 프로세스 실행 이벤트 연계 분석
2	환경 격리	감염 의심 개발자 PC 및 CI/CD 환경 격리	의심 행위가 확인된 개발자 워크스테이션 격리 및 추가 실행 차단
3	실행 차단	Node.js 하위 의심 프로세스, 드로퍼, 백도어 프로세스 종료	프로세스 트리 기반 악성 스크립트·백도어 실행 차단
4	통신 차단	C2 도메인·IP·포트로의 외부 통신 차단	의심 네트워크 연결 및 악성 도메인 아웃바운드 트래픽 차단
5	재발 방지	패키지 캐시 정리, 패키지 버전 고정, 토큰·API 키 교체, SBOM 기반 구성 요소 점검	Node.js 하위 프로세스와 외부 통신 행위 지속 모니터링

골든 타임: 패키지 설치 직후 악성 스크립트가 실행되는 단계

AhnLab EDR은 패키지 설치 이후의 프로세스 실행, 페이로드 다운로드, 외부 통신 흐름을 조기에 식별해 개발 환경과 CI/CD 파이프라인으로 확산되기 전 대응 지점을 확보한다. 이를 통해 악성 패키지 설치 이후의 Dwell Time을 줄이고, 연쇄 감염 가능성을 낮춘다.

Playbook 4. 신뢰 기반 위장 공격

코드서명 인증서·정상 SW 위장 악용한 탐지 우회 대응

신뢰 기반 위장 공격은 코드서명 인증서, 정상 소프트웨어(SW), 인증기관·보안기업의 신뢰 체계를 악용해 악성 행위를 정상 활동처럼 보이게 만드는 공격이다. 코드서명 인증서 유출 및 정상 SW 위장 사례에서처럼, 서명된 파일이나 정상 모듈은 악성 행위를 숨기는 수단으로 악용될 수 있다.

인증서 유출이나 정상 모듈 변조가 발생하면 키로깅·C2 통신·정보 탈취로 이어질 수 있다. 따라서 '서명된 파일' 또는 '정상 프로그램'이라는 전제만으로 안전성을 판단하지 않고, 실행 이후의 행위를 기준으로 위협 여부를 식별해야 한다.

신뢰 기반 위장 공격 흐름(코드서명 인증서 유출 및 정상 SW 위장 사례)

AhnLab EDR 기반 탐지 포인트

EDR 관점에서는 파일의 서명 상태보다 실행 후 발생하는 행위 이벤트를 먼저 확인해야 한다. 웹셸 생성, 정상 모듈 위장, 키 입력 탈취, 외부 C2 통신처럼 정상 서명이라는 신뢰 뒤에 숨어 있는 행위를 연관 분석하는 것이 탐지의 출발점이다.

탐지 영역	EDR 탐지 포인트
서명 파일 위장 실행	정상 프로그램처럼 서명된 악성 파일 실행, 정상 플러그인 또는 실행 파일로 위장한 악성 모듈 교체 탐지
웹셸·파일 변조 행위	웹 루트 경로의 웹셸 삽입, 웹 서버 프로세스 하위의 비정상 명령 실행, 파일 무결성 훼손 탐지
정보 탈취·외부 통신	메모리 인젝션, 키로깅 API 후킹, 비정상 아웃바운드 연결, C2 통신 및 데이터 전송 시도 탐지

탐지 이후 대응 절차

코드서명 인증서 유출 사고는 악성 파일 삭제만으로는 종료되지 않는다. 서명된 악성 행위와 외부 통신을 차단하는 동시에 유출 인증서 폐기, 신규 인증서 발급, 패키지 재서명 등 신뢰 체계 복구 조치가 함께 이루어져야 한다.

No.	대응 단계	수행 내용	EDR 활용 포인트
1	악성 행위 차단	서명된 악성 파일 및 관련 프로세스 종료	악성 프로세스 탐지·종료
2	통신 차단	C2 통신 및 비정상 외부 연결 차단	의심 네트워크 연결 차단
3	변조 복구	변조된 파일·레지스트리 설정 제거 및 복구	파일·레지스트리 변경 이벤트 분석
4	인증서 조치	유출 인증서 폐기, 신규 인증서 발급, 패키지 재서명	서명된 프로그램의 행위 기반 모니터링
5	추가 유포 차단	추가 악성코드 유포 가능성 차단, 의심 파일·통신 추적	IOC·행위 패턴 기반 헌팅

> **골든 타임: 서명된 악성 파일의 최초 실행과 C2 통신 시작 단계**
> AhnLab EDR은 서명 여부를 넘어 실행 이후의 메모리 접근·키로깅·지속성 확보·외부 통신 행위를 분석해 위협을 식별한다. 이를 통해 정상 SW로 위장한 악성 행위의 은닉 시간을 줄이고, Dwell Time이 장기화되기 전 공급망 확산을 억제한다.

AhnLab EDR 도입부터 운영까지 로드맵

EDR 도입 효과를 높이기 위해서는 솔루션 구축만으로는 충분하지 않다. 보호 자산 식별, 정책 설정, 룰 튜닝, 자동 대응, 위협 헌팅, 운영 KPI 관리까지 단계적으로 정착시켜야 한다. AhnLab EDR 운영 로드맵은 도입 초기 90일 동안 조직이 수행해야 할 과제를 30일, 60일, 90일 단위로 구체화한다.

AhnLab EDR 30/60/90일 로드맵

기반 구축	최적화 및 연동	고도화 및 내재화
30일	**60일**	**90일**
• 보호 자산 식별 및 분류 • 에이전트 파일럿 배포 • 기본 탐지 정책 설정 • 격리 플레이북 초안 마련	• 고위험 행위 룰 튜닝 • 오탐 최소화 작업 • 선제적 위협 헌팅 시작 • SOAR 및 기존 인프라 연동	• 전사 에이전트 확대 배포 • 운영 KPI 대시보드 구축 • 자동화 대응 프로세스 적용 • Tabletop 침해대응 훈련 정례화

AhnLab EDR 운영 성과 점검 항목

핵심 성과 지표	거버넌스 및 운영 성숙도 관리
• **MTTD:** 위협 발생부터 인지까지의 시간 단축 • **MTTR:** 탐지 후 억제·격리·복구까지의 시간 단축 • **평균 Dwell Time:** 침해 조직 내 체류 시간 축소(목표: 수 시간 이내) • **자동 격리 비율 / 오탐률:** 자동 대응 품질 관리	• 사고 조사(IR) 리포팅 시간 단축 • 위협 헌팅 활성화 • 규제 준수 및 감사 증적 확보 • 침해대응 훈련 정례화

> EDR 운영의 핵심은 도입이 아니라 내재화다. 30/60/90일 로드맵에 따라 프로세스 정립, 탐지 룰 튜닝, 관제 역량 강화를 단계적으로 추진하면 MTTD·MTTR·Dwell Time을 지속적으로 줄이고, 사고 대응 비용과 업무 중단 리스크를 낮출 수 있다.