LEVELTHREE

AIENTROPHY Nightwatch

서버 내부 위협 탐지 솔루션

Invisible Protection against Silent Threats

고객 서버에 설치되는 경량 보안 에이전트로, 서버 내부의 파일 시스템을 실시간으로 감시하여 악성코드, 웹셸, 파일 변조를 즉시 탐지하고 자동으로 대응합니다.

버전	1.0	상태	프로덕션 운영 중
작성일	2026-03-20	문서 분류	공개 (Public)

실시간 감시 파일 변경 즉시 탐지	~50MB RAM 경량 리소스 사용	AI 심층 분석 신종 위협 탐지	자동 격리 즉시 위협 차단

Section 1

서버를 노리는 보이지 않는 위협

외부 공격뿐 아니라 서버 내부에서 발생하는 위협은 더욱 치명적입니다. 공격자가 서버에 침투한 후 남기는 악성 파일은 기존 방화벽이나 네트워크 보안으로는 탐지하기 어렵습니다.

1.1 주요 위협 유형

위협 유형	공격 방식	비즈니스 영향
웹셸 업로드	공격자가 서버에 웹셸을 심어 원격 제어	서버 완전 장악, 데이터 유출, 추가 공격의 거점
파일 변조	정상 파일을 악성 코드로 교체	서비스 장애, 악성코드 유포, 고객 피해
확장자 위장	실행파일을 이미지/문서로 위장하여 업로드	보안 검사 우회, 서버 내 악성코드 실행
백도어 설치	지속적 접근을 위한 백도어 파일 생성	장기간 은밀한 침투, 반복적 데이터 탈취

1.2 Nightwatch 솔루션

AIENTROPHY Nightwatch는 이 모든 위협을 실시간으로 탐지합니다. 서버에 설치되는 경량 에이전트가 파일 시스템의 모든 변경을 감시하며, 다단계 분석 파이프라인을 통해 알려진 위협부터 신종 악성코드까지 빠짐없이 탐지하고 자동으로 대응합니다.

기존 방식	Nightwatch
주기적 수동 스캔 (시간 단위/일 단위)	파일 변경 즉시 실시간 탐지 (밀리초 단위)
알려진 악성코드만 탐지	알려진 위협 + AI 기반 신종 위협 탐지
탐지 후 수동 대응 (관리자 확인 필요)	자동 격리 + 즉시 알림 (무중단 대응)
확장자 위장 탐지 불가	파일 내용 기반 위장 탐지
규칙 수동 업데이트 필요	자동 규칙 업데이트 (관리자 개입 불필요)

Section 2

다단계 위협 탐지 파이프라인

Nightwatch는 5단계의 체계적인 탐지 파이프라인을 통해 위협을 분석합니다. 각 단계는 서로 다른 분석 기법을 적용하여 단일 기법의 우회가 불가능한 구조입니다.

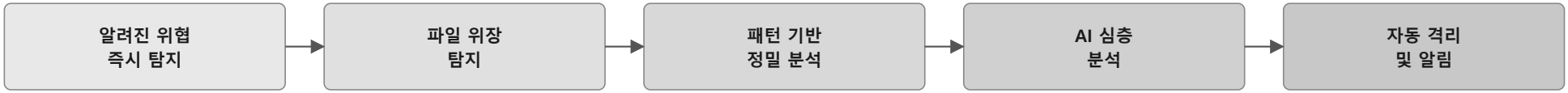

Figure 1. 다단계 위협 탐지 파이프라인 — 5단계 순차 분석

단계	탐지 내용	처리 방식
1단계	**알려진 위협 즉시 탐지**	글로벌 악성코드 데이터베이스와 대조하여 이미 알려진 위협을 즉시 판별합니다.
2단계	**파일 위장 탐지**	파일의 실제 내용을 분석하여 확장자를 변경해 위장한 실행 파일을 감지합니다.
3단계	**패턴 기반 정밀 분석**	악성 패턴 규칙 엔진으로 정밀 분석합니다. 규칙은 자동으로 업데이트됩니다.
4단계	**AI 심층 분석**	기존 규칙으로 판별되지 않는 의심 파일을 AI가 심층 분석하여 신종 위협을 탐지합니다.
5단계	**자동 격리 및 알림**	악성으로 판정된 파일을 자동 격리하고, 관리자에게 즉시 알림을 전송합니다.

* 1~3단계는 서버 내에서 수 밀리초 이내에 처리됩니다. 4단계는 의심 파일만 클라우드 AI가 심층 분석합니다.

Section 3

핵심 기능

Nightwatch는 서버 보안에 필요한 핵심 기능을 하나의 경량 에이전트로 제공합니다.

기능	설명
실시간 파일 감시	서버 내 파일 생성, 수정, 삭제를 실시간으로 감지하여 즉시 보안 검사를 수행합니다. 감시 대상 디렉토리를 유연하게 설정할 수 있습니다.
알려진 악성코드 즉시 탐지	글로벌 악성코드 데이터베이스와 대조하여 이미 알려진 위협을 즉시 판별합니다. 데이터베이스는 자동으로 최신 상태가 유지됩니다.
파일 위장 탐지	실행 파일이 이미지나 문서로 확장자를 변경해 위장한 경우를 감지합니다. 파일의 실제 내용을 분석하여 위장 여부를 판별합니다.
패턴 기반 정밀 분석	업계 표준 규칙 엔진으로 악성 패턴을 정밀하게 탐지합니다. 분석 규칙은 자동으로 업데이트되어 최신 위협에 대응합니다.
AI 기반 신종 위협 분석	기존 규칙으로 판별되지 않는 의심 파일을 AI가 심층 분석합니다. 알려지지 않은 신종 악성코드도 탐지할 수 있습니다.
자동 격리 및 복원	악성으로 판정된 파일을 자동으로 격리하고, 원본 경로와 탐지 사유를 기록합니다. 오탐으로 확인된 경우 원클릭으로 복원이 가능합니다.
자동 규칙 업데이트	탐지 규칙과 악성코드 데이터베이스가 자동으로 업데이트됩니다. 관리자의 수동 개입 없이 항상 최신 보안 상태를 유지합니다.

Section 4

AIENTROPHY 통합 보안 체계

Nightwatch는 AIENTROPHY SDK 및 관리 콘솔과 통합되어 외부 공격과 내부 위협을 동시에 방어하는 포괄적 보안 체계를 구성합니다.

4.1 통합 보안 구성

영역	제품	역할
외부 봇/크롤링 방어	AIENTROPHY SDK	클라이언트 측에서 매크로, 봇, 크롤링 등 자동화 공격을 실시간 탐지 및 차단
서버 내부 파일 보안	AIENTROPHY Nightwatch	서버 측에서 악성코드, 웹셸, 파일 변조, 백도어를 실시간 탐지 및 자동 격리
통합 모니터링 대시보드	AIENTROPHY Console	외부/내부 위협 현황을 단일 대시보드에서 통합 모니터링, 알림 및 정책 관리

4.2 배포 사양

항목	사양
리소스 사용량	약 50MB RAM, CPU 부하 최소 (이벤트 기반 처리)
지원 환경	Linux, Windows 서버
클라우드 지원	AWS, GCP, Azure 등 주요 클라우드 환경 지원
설치 방식	원라인 설치 스크립트로 간편하게 설치
규칙 업데이트	자동 업데이트 (관리자 개입 불필요)
관리	AIENTROPHY Console에서 통합 관리

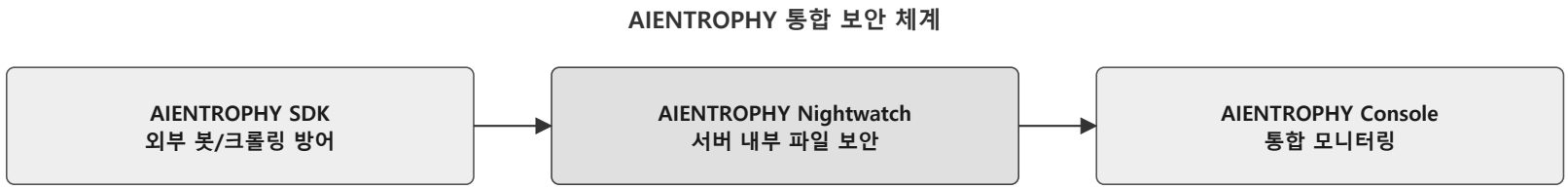

Figure 2. AIENTROPHY 통합 보안 체계 — SDK(외부) + Nightwatch(내부) + Console(관리)

AIENTROPHY Nightwatch

Invisible Protection against Silent Threats

웹사이트	문의	관리 콘솔
aientrophy.com	info@aientrophy.com	console.aientrophy.com

LEVELTHREE