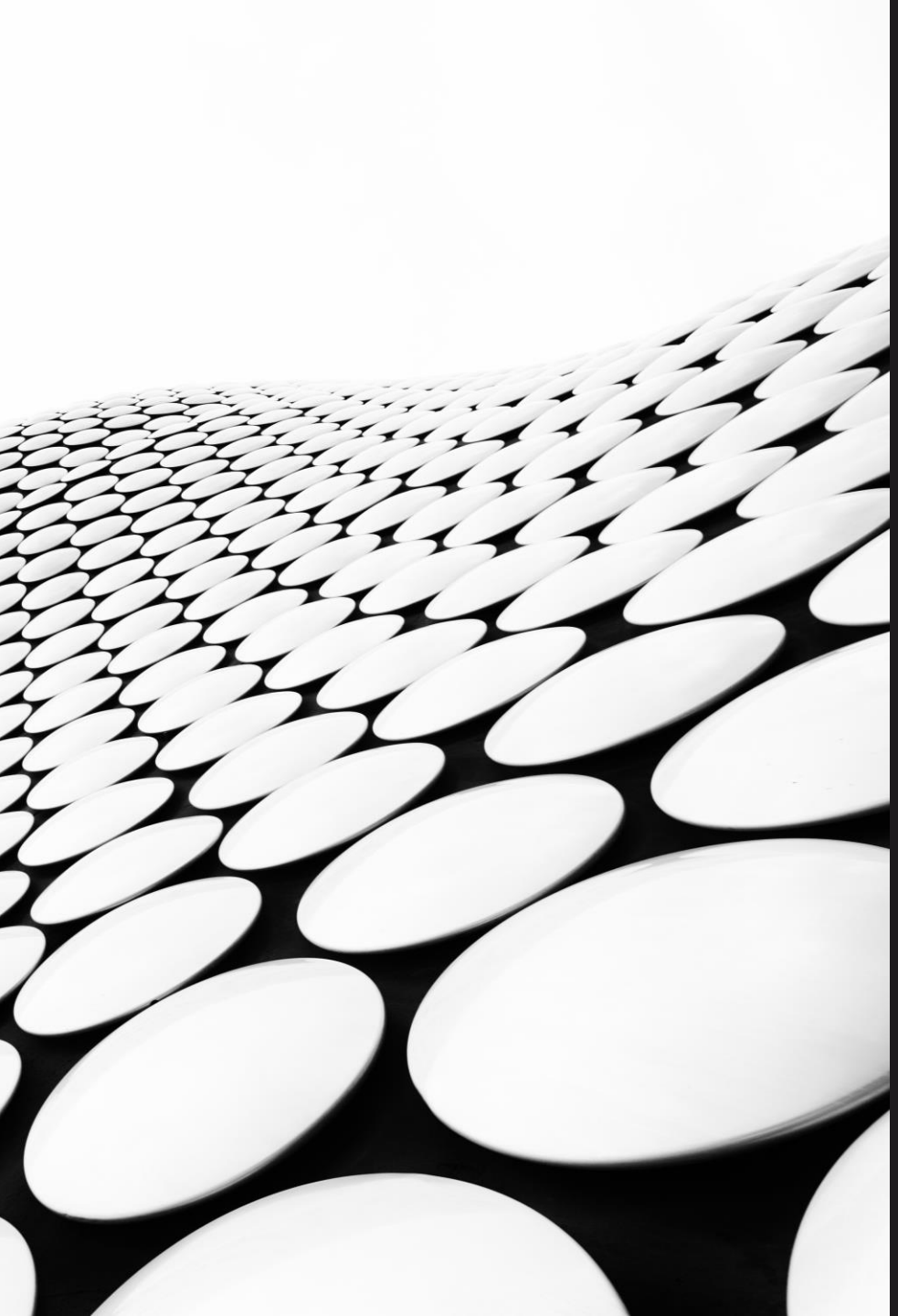


AION SENTINAL 매뉴얼

SecureNet AI

홈 API 관리 다운로드 내 대시보드 로그아웃

API 관리

SecureNet AI API 키를 생성하고 관리하여 웹사이트에 보안 모니터링을 통합하세요.

+ 새 API 키 생성

이름, 용도 작성 후 생성

py_test_key

생성일: 2025. 11. 4. 오전 3:00:44 • 마지막 사용: 2025. 11. 10. 오후 11:07:34

API 키 보기 | Auth 키 보기

해당 버튼을 누르면
API키와 Auth키를 볼 수 있습니다.

••••••••••••••••••

••••••••••••••••••

코드 테스트

AION Sentinel

AION Sentinel

- 실시간 분석
- 상태 대시보드
- 위험 IP 목록
- 설정 및 인증 관리

설정 및 인증 관리

--- AI 분석 서버 인증 ---

API Key (Hash):

인증 Key (AUTH):

--- 네트워크 Flow 분석 설정 ---

네트워크 인터페이스: Wi-Fi

윈도우 집계 시간 (초): 5.0

Flow 비활성 제한 시간 (초): 10.0

RAM 사용량 경고 기준 (%): 90.0

--- 위험 IP 임계값 설정 ---

IP 접속 횟수 임계값 (Window): 1000.0
(0 입력 시 비활성화)

모든 설정 저장 및 반영

변경사항을 저장하면
config.json 파일이 생성됩니다.

py_test_key
생성일: 2025. 11. 4. 오전 3:00:44 • 마지막 사용: 2025. 11. 10. 오후 11:07:34

API 키 보기 | Auth 키 보기

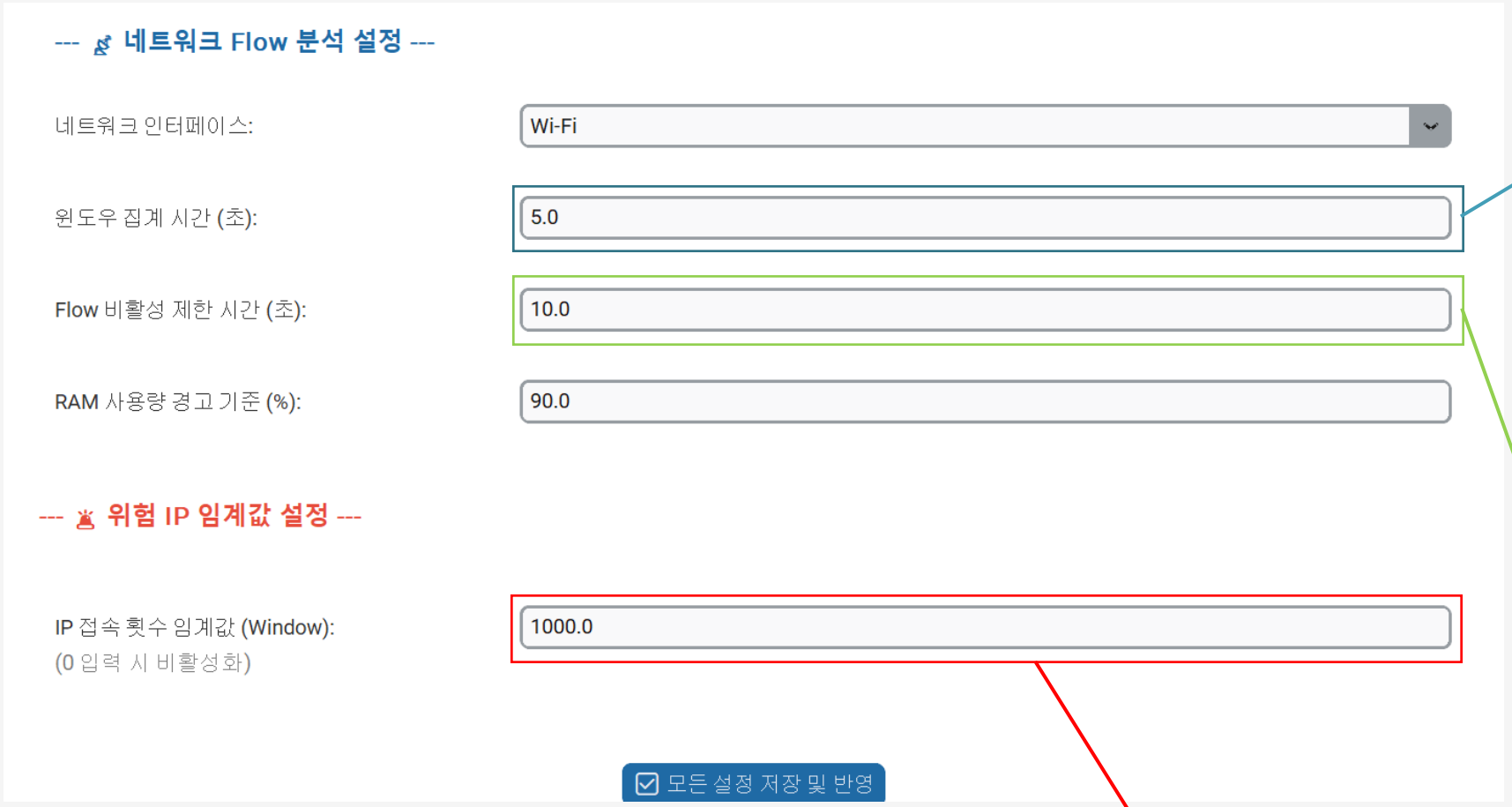
•••••••••••••••••• API 키

•••••••••••••••••• Auth 키

코드 테스트

사용자 환경에 맞게 설정
config.json 파일 안에서
수정 가능합니다.

분석기 관련 설정 팁/도움말

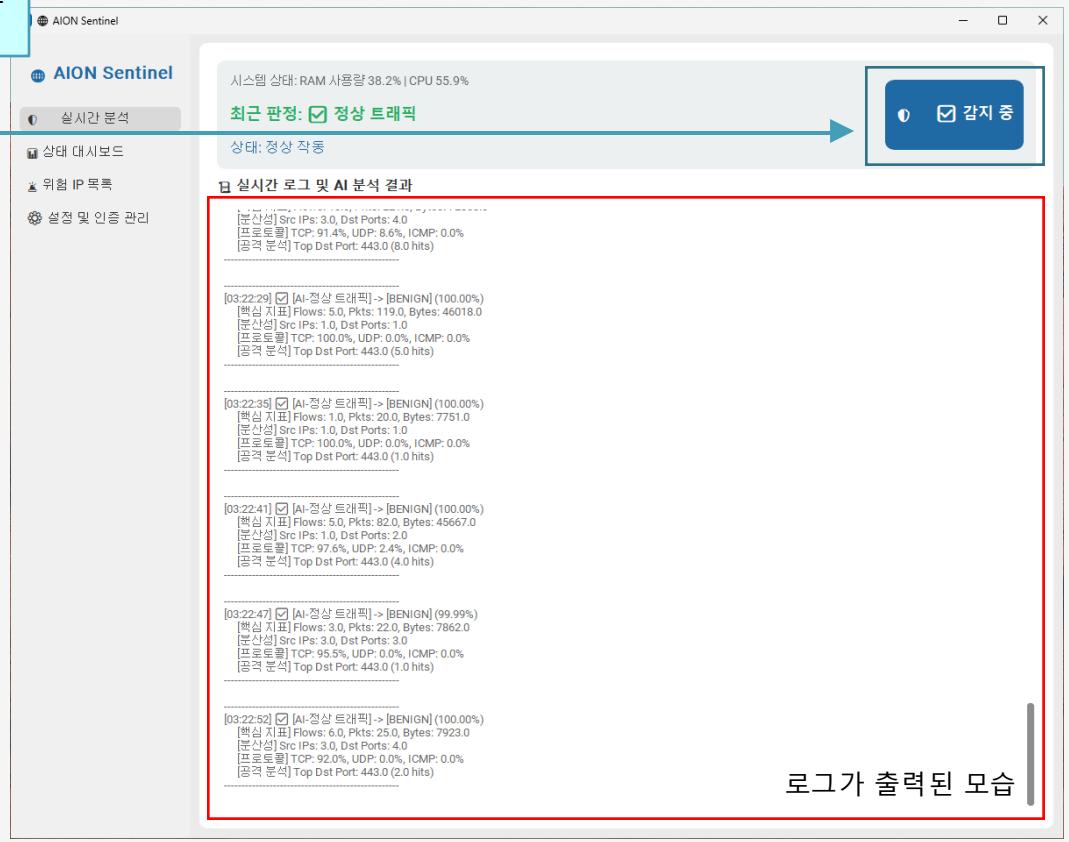


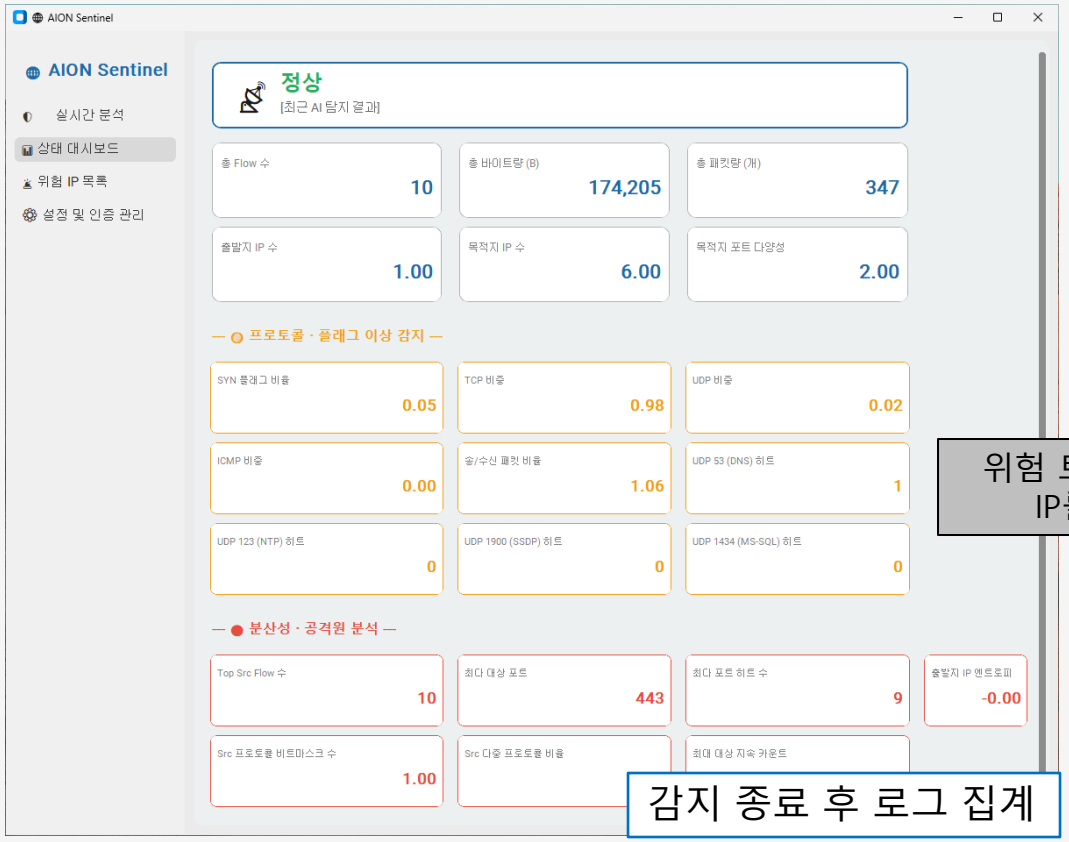
윈도우 집계시간 설정 팁
낮은 값: 실시간 탐지에 유리 (리소스 사용량 증가)
높은 값: 시스템 부하 감소 (탐지 속도 둔화)

플로우 비활성화 시간
데이터가 없는 연결(플로우)를 비활성으로 처리할 때까지의 대기시간입니다.
낮은 값: 정상적인 느린 연결을 오탐할 가능성이 있습니다
높은 값: 리소스 낭비 및 공격 탐지 지연 가능성이 있습니다.

위험 IP 임계치
IP의 '위험점수'가 이 값을 초과하면 '위험IP"로 분류하고 조치합니다.
낮은 값: 탐지 민감도 증가 (오탐 가능성이 높아질 수 있음)
높은 값: 오탐 감소 (초기/경미한 위협 누락 가능성)

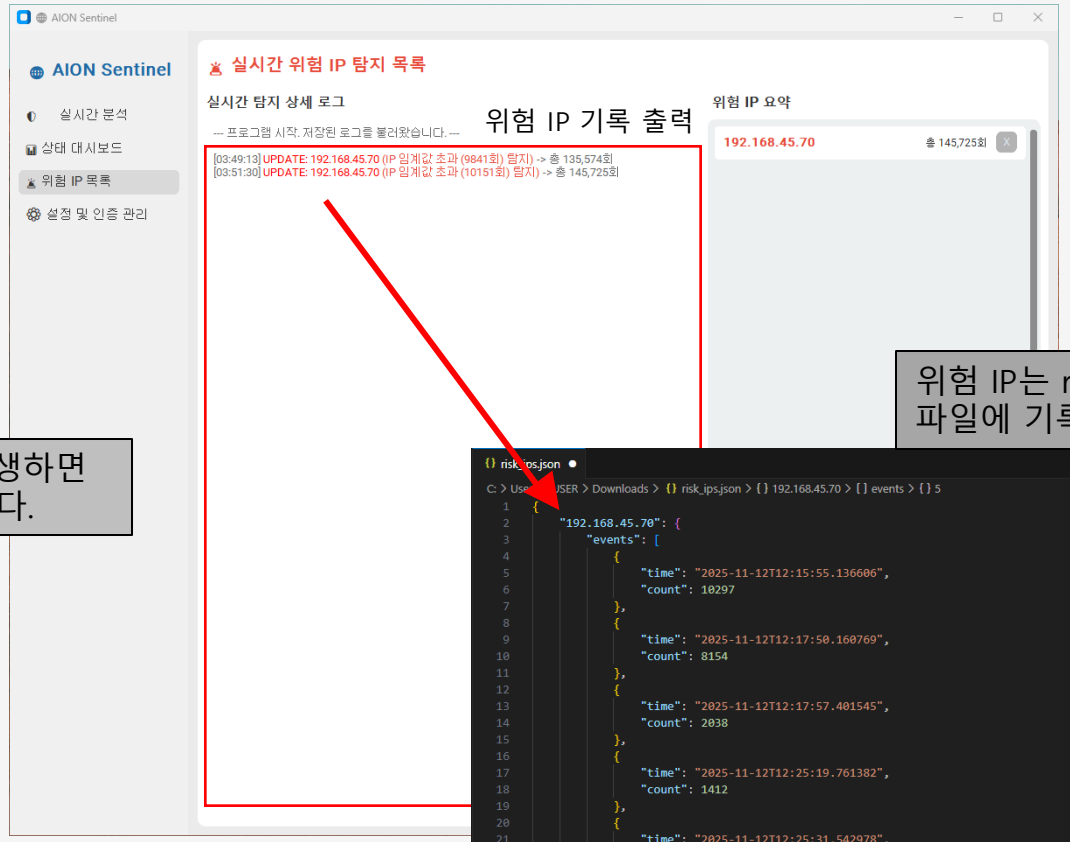
감지시작 버튼을 누르면
감지가 시작됩니다.



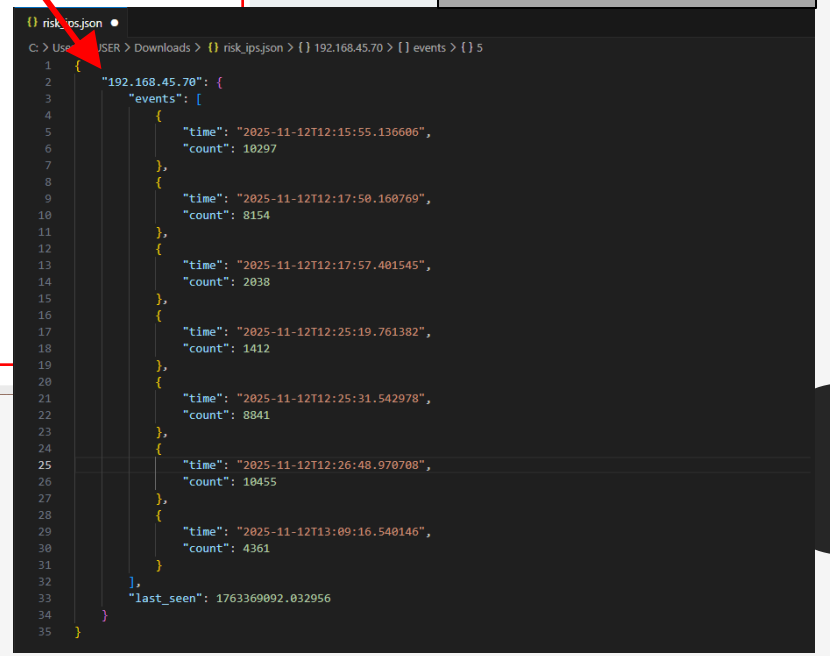


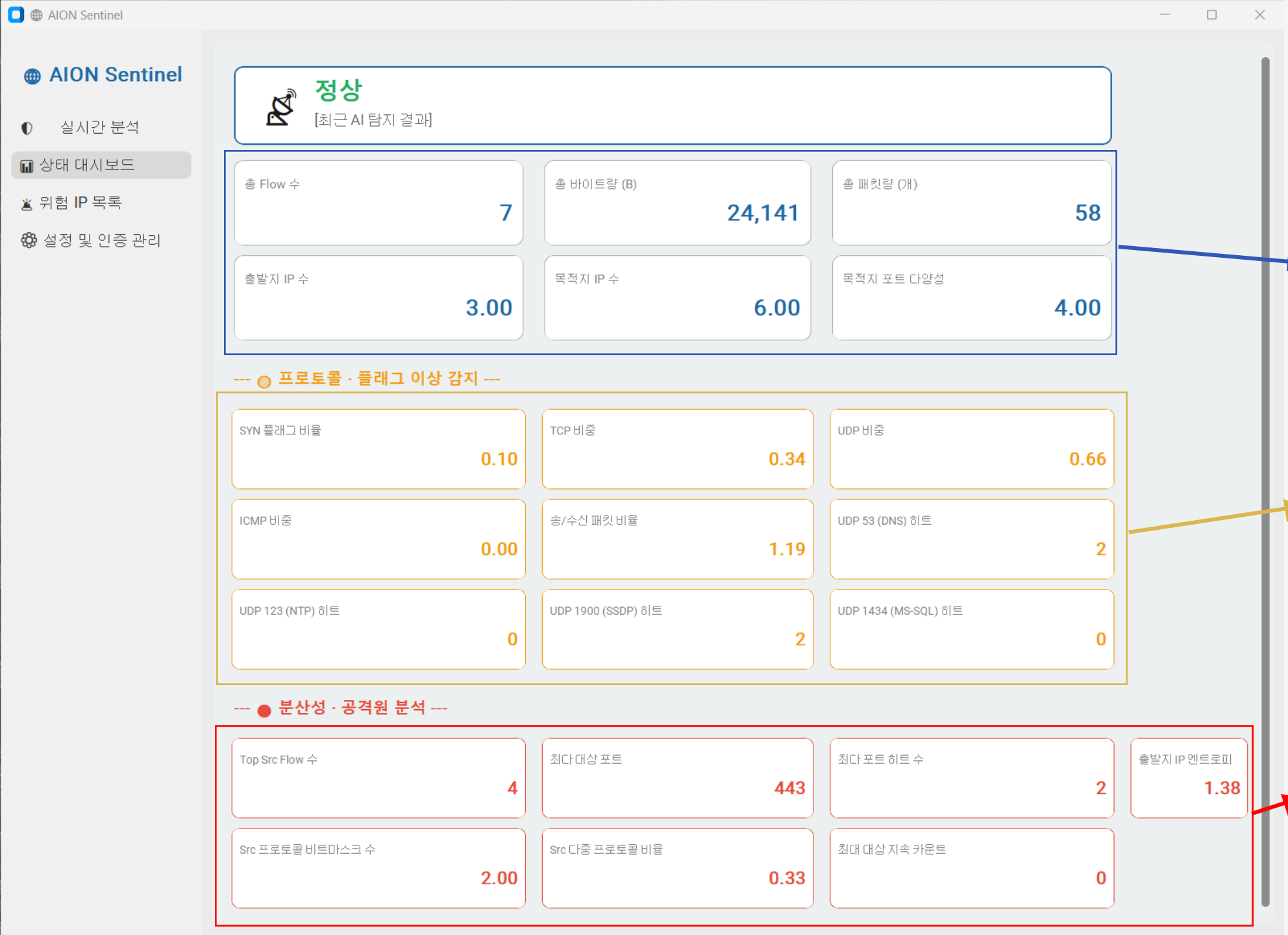
위험 트래픽이 발생하면
IP를 기록합니다.

감지 종료 후 로그 집계



위험 IP는 risk_ips.json
파일에 기록됩니다.





핵심 지표:
설명: 가게에 들어온 손님 수(Flow), 짐의 무게(Byte), 발자국 수(Packet)를 셉니다.

핵심: 평소에는 조용하던 수치가 갑자기 폭발적으로 늘어나면 **"아, 누군가 물량 공세(Flood)를 하고 있구나"**라고 판단합니다.

프로토콜·플래그 이상 감지(행동 유형):
설명: 손님들이 정상적으로 물건을 사는지, 아니면 이상한 행동(예약만 하고 끊기, 쓰레기 던지기)만 골라서 하는지 **비율(Ratio)**을 봅니다.

핵심: 정상적인 가게라면 여러 행동이 섞여 있어야 하는데, 특정 행동(예: TCP, UDP)만 높은 확률로 공격입니다.

분산성·공격원 분석 (위협 강도):
설명: 들어온 사람들이 무작위로 왔는지, 아니면 특정 지령을 받고 조직적으로(Entropy) 움직이는지, 문고리를 하나씩 다 따보고 있는지(Scan) 분석합니다.

핵심: 공격자가 숨기려고 해도 드러나는 **'공격의 패턴'**을 찾아내는 가장 정밀한 영역입니다.

DDoS (분산 서비스 거부 공격)
상황: 지휘관(해커)의 명령을 받은 수만 대의 좀비 PC(감염된 컴퓨터)가 우리 가게를 마비시키려고 동시에 쳐들어오는 상황입니다.

- **출발지 IP 수가 폭증할 때:**"평소엔 손님이 3~5명인데, 갑자기 수천 명, 수만 명으로 늘어났나요?" → 어떤 공격 방식이든 간에, 일단 이 숫자가 폭발하면 DDoS 공격이 시작된 것입니다.
- **출발지 IP 엔트로피가 높을 때:**"손님들의 출신지가 자연스러운가요?" → 공격자가 자신의 정체를 숨기려고 신분증(IP)을 위조해서 무작위로 들어오고 있다는 수학적 증거입니다.

유형 A. Flood 공격 (무식한 물량 공세)

① SYN Flood (예약 전화 테러)

상황: "예약할게요"라고 전화만 걸고, 직원이 받으면 침묵하는 '가짜 예약' 공격입니다.

탐지 비결:

- **SYN 플래그 비율:**"전화한 사람들의 99%가 용건 없이 **'여보세요(예약 요청)'**만 외치고 있나요?" → 이 비율이 **1.0(100%)**에 가까우면서, 동시에 **총 패킷량 (개)**이 폭발적으로 늘어난다면 업무를 마비시키는 테러입니다.
- **송/수신 패킷 비율:**"말을 걸었으면 대답을 듣나요?" → 나는 말만 하고(송신), 상대방의 대답은 듣지 않는(수신 없음) 비정상적인 비율이 나타나면 공격입니다.

② TCP Flood (회전문 마비 작전)

상황: 수많은 인파가 회전문(서버 입구)을 꽉 막아버리는 '무식한 물량' 공격입니다.

탐지 비결:

- **TCP 비중:**"지금 몰려온 수만 명의 사람이 전부 'TCP'라는 똑같은 옷을 입고 있나요?" → 다른 손님은 없고 오직 TCP 옷을 입은 사람들만 가득 차 있다면 의심해야 합니다.
- **총 패킷량 (개):**"잠시동안 지나간 사람 수가 경기장 관중 수만큼 많은가요?" → 단순히 TCP 비중만 높은 게 아니라, 이 숫자가 평소와 달리 감당 불가능할 정도로(수십만 단위) 폭증할 때 공격으로 판단합니다.

③ UDP Flood (우편함 쓰레기 투척)

상황: 확인 절차 없이 거대한 쓰레기 더미(데이터)를 우편함에 쑤셔 넣는 공격입니다.

탐지 비결

- **UDP 비중:**"배달된 물건들이 전부 '내용 확인 불요(UDP)' 우편물인가요?" → 중요한 서류는 없고 그냥 던져 넣는 우편물만 압도적으로 많다면 공격입니다.
- **총 바이트량 (B):**"우편물 무게가 얼마나 되나요?" → 이 숫자가 기가바이트(GB) 단위로 미친 듯이 커진다면, 쓰레기로 우편함을 꽉 채워 터뜨리려는 의도입니다.

④ ICMP Flood (초인종 누르기 장난)

상황: 아이들이 남의 집 초인종을 쉬지 않고 누르며 **"거기 있어요? 거기 있어요?"라고 계속 괴롭혀서, 주인이 아무것도 못 하게 만드는 상황입니다.**

탐지 비결:

- **ICMP 비중:**"가게에 온 손님들이 물건은 안 보고 **초인종(ICMP)**만 계속 누르고 있나요?" → 웹서핑이나 게임을 할 때는 이 수치가 낮아야 정상입니다. 하지만 공격 시에는 이 비중이 1.00(100%) 가까이 치솟습니다.
- **총 패킷량 (개):**"초인종을 1분에 한 번 누르나요, 1초에 1,000번 누르나요?" → ICMP 비중이 높은 상태에서, 패킷 숫자까지 감당 못 할 정도로 폭증한다면 100% 초인종 테러(공격)입니다.

유형 B. Amplification (배달지 위조 / 반사 / 증폭)

상황: 공격자가 직접 오지 않고, **제3자(DNS, NTP 서버 등)를 속여서 우리 가게로 **엄청난 양의 응답(반사체)**을 쏟아붓게 만듭니다.**

탐지 비결:

- **UDP 53 (DNS) 히트 / UDP 123 (NTP) 히트 등**:"평소엔 '0'이거나 잠잠하던 특정 창구 숫자가 갑자기 수천 건으로 올라가나요?" → 범인이 이 서비스들을 악용해서 공격을 증폭시키고 있다는 확실한 증거입니다.

Port Scan (빈집털이범의 문고리 확인 / 정찰)
상황: 도둑이 침입하기 전, 아파트 복도를 돌며 모든 집의 문고리를 하나씩 다 돌려보며 열린 문(약점)을 찾는 정찰 행위입니다.

탐지 비결:
- **목적지 포트 다양성:** "방문한 집의 호수가 몇 개나 되나요?" → 평소엔 낮은 숫자지만, 이 수치가 혼자서 수백, 수천으로 치솟는다면 한 명이 온 동네 문을 다 두드리는 것이므로 정찰입니다.
- **출발지 IP 수:** "문은 수천 개를 두드리는데, 방문자는 단 1명인가요?" → 방문자 수는 적은데 방문한 곳(목적지 포트 다양성)만 많다면 확실한 빈집털이범입니다.

Slowloris (카페 자리 독점족 / 슬로우 공격)
상황: 커피 한 잔만 시켜놓고 하루 종일 자리를 차지해서, 막상 점심시간에 온 진짜 손님들이 앉을 자리가 없어 돌아가는 상황입니다.

탐지 비결:
- **최대 대상 지속 카운트**: "저 손님, 커피 다 마신 지가 언젠데 아직도 안 나가고 버티나요?" → 용무가 끝났는데도 연결을 끊지 않고 질질 끄는 시간이 길어지면 공격입니다.
- **총 Flow 수 vs 총 패킷량 (개):** "매장에 빈자리는 하나도 없는데(Flow 꽉 참), 주방에 들어오는 주문은 거의 없나요(Packet 적음)?" → 북적북적해 보이지만 실속 없이 자리만 차지하는 허수아비 손님들입니다.