



AION SENTINAL 매뉴얼



API 관리

SecureNet AI API 키를 생성하고 관리하여 웹사이트에 보안 모니터링을 통합하세요.

[+ 새 API 키 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

새 API 키 생성

새로운 API 키를 생성하세요.

키 이름

예: Production API Key

설명

이 API 키의 용도를 설명해주세요

이름, 용도 작성 후 생성

취소

생성

설정 및 인증 관리

AI 분석 서버 인증

API Key (Hash):

인증 Key (AUTH):

네트워크 Flow 분석 설정

네트워크 인터페이스:

윈도우 집계 시간 (초):

Flow 비활성 제한 시간 (초):

RAM 사용량 경고 기준 (%):

위험 IP 임계값 설정

IP 접속 횟수 임계값 (Window):
(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](#) [삭제](#)

..... API 키

..... Auth 키

코드 테스트

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

분석기 관련 설정 팁/도움말

--- 🌐 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):

(0 입력 시 비활성화)

1000.0

☒ 모든 설정 저장 및 반영

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.

AION Sentinel

실시간 분석

상대 대시보드

위협 IP 목록

설정 및 인증 관리

시스템 상태: RAM 사용량 30.0% | CPU 79.6%

최근 판정: 대기 중

상태: 대기 중

실시간 로그 및 AI 분석 결과

[03:16:21] ☒ 1개의 위협 IP를 파일에서 불러왔습니다.

[03:16:21] ☐ 설정 파일에서 정보를 불러왔습니다.

[03:16:21] GUI: 1개의 저장된 위협 IP를 목록에 표시합니다.

감지 시작

로그가 출력되는 부분

AION Sentinel

실시간 분석

상대 대시보드

위협 IP 목록

설정 및 인증 관리

시스템 상태: RAM 사용량 38.2% | CPU 55.9%

최근 판정: ☒ 정상 트래픽

상태: 정상 작동

실시간 로그 및 AI 분석 결과

[분산성] Src IPs: 3.0, Dst Ports: 4.0
[프로토콜] TCP: 91.4%, UDP: 8.6%, ICMP: 0.0%
[공격 분석] Top Dst Port: 443.0 (8.0 hits)

[03:22:29] ☒ [AI-정상 트래픽] -> [BENIGN] (100.00%)
[핵심 지표] Flows: 5.0, Pkts: 119.0, Bytes: 46018.0
[분산성] Src IPs: 1.0, Dst Ports: 1.0
[프로토콜] TCP: 100.0%, UDP: 0.0%, ICMP: 0.0%
[공격 분석] Top Dst Port: 443.0 (5.0 hits)

[03:22:36] ☒ [AI-정상 트래픽] -> [BENIGN] (100.00%)
[핵심 지표] Flows: 1.0, Pkts: 20.0, Bytes: 7751.0
[분산성] Src IPs: 1.0, Dst Ports: 1.0
[프로토콜] TCP: 100.0%, UDP: 0.0%, ICMP: 0.0%
[공격 분석] Top Dst Port: 443.0 (1.0 hits)

[03:22:41] ☒ [AI-정상 트래픽] -> [BENIGN] (100.00%)
[핵심 지표] Flows: 5.0, Pkts: 82.0, Bytes: 45667.0
[분산성] Src IPs: 1.0, Dst Ports: 2.0
[프로토콜] TCP: 97.6%, UDP: 2.4%, ICMP: 0.0%
[공격 분석] Top Dst Port: 443.0 (4.0 hits)

[03:22:47] ☒ [AI-정상 트래픽] -> [BENIGN] (99.99%)
[핵심 지표] Flows: 3.0, Pkts: 22.0, Bytes: 7862.0
[분산성] Src IPs: 3.0, Dst Ports: 3.0
[프로토콜] TCP: 95.5%, UDP: 0.0%, ICMP: 0.0%
[공격 분석] Top Dst Port: 443.0 (1.0 hits)

[03:22:52] ☒ [AI-정상 트래픽] -> [BENIGN] (100.00%)
[핵심 지표] Flows: 6.0, Pkts: 25.0, Bytes: 7923.0
[분산성] Src IPs: 3.0, Dst Ports: 4.0
[프로토콜] TCP: 92.0%, UDP: 0.0%, ICMP: 0.0%
[공격 분석] Top Dst Port: 443.0 (2.0 hits)

감지 중

로그가 출력된 모습

AION Sentinel

실시간 분석

상태 대시보드

위험 IP 목록

설정 및 인증 관리

정상

[최근 4시간 결과]

총 Flow 수

10

총 바이트량 (B)

174,205

총 패킷량 (개)

347

출발지 IP 수

1.00

목적지 IP 수

6.00

목적지 포트 다양성

2.00

— 프로토콜 · 플래그 이상 감지 —

SYN 플래그 비율

0.05

TCP 비율

0.98

UDP 비율

0.02

ICMP 비율

0.00

술/수신 플릿 비율

1.06

UDP 53 (DNS) 히트

1

UDP 123 (NTP) 히트

0

UDP 1900 (SSDP) 히트

0

UDP 1434 (MS-SQL) 히트

0

— 분산성 · 공격원 분석 —

Top Src Flow 수

10

최다 대상 포트

443

최다 포트 히트 수

9

출발지 IP 엔트로피

-0.00

Src 프로토콜 비트마스크 수

1.00

Src 다중 프로토콜 비율

최대 대상 지속 카운트

감지 종료 후 로그 집계

위험 트래픽이 발생하면
IP를 기록합니다.

AION Sentinel

실시간 분석

상태 대시보드

위험 IP 목록

설정 및 인증 관리

실시간 위험 IP 탐지 목록

실시간 탐지 상세 로그

위험 IP 기록 출력

위험 IP 요약

--- 프로그램 시작 저장된 로그를 불러왔습니다. ---

[03:49:13] UPDATE: 192.168.45.70 (IP 임계값 초과 (9841회) 탐지) -> 총 135,574회

[03:51:30] UPDATE: 192.168.45.70 (IP 임계값 초과 (10151회) 탐지) -> 총 145,725회

총 145,725회

위험 IP는 risk_ips.json
파일에 기록됩니다.

```
1 {
2   "192.168.45.70": {
3     "events": [
4       {
5         "time": "2025-11-12T12:15:55.136606",
6         "count": 10297
7       },
8       {
9         "time": "2025-11-12T12:17:50.160769",
10        "count": 8154
11      },
12      {
13        "time": "2025-11-12T12:17:57.401545",
14        "count": 2038
15      },
16      {
17        "time": "2025-11-12T12:25:19.761382",
18        "count": 1412
19      },
20      {
21        "time": "2025-11-12T12:25:31.542978",
22        "count": 8841
23      },
24      {
25        "time": "2025-11-12T12:26:48.970708",
26        "count": 10455
27      },
28      {
29        "time": "2025-11-12T13:09:16.540146",
30        "count": 4361
31      }
32    ],
33    "last_seen": 1763369092.032956
34  }
35 }
```