Criminal IP ASM

위협 인텔리전스 기반
공격표면관리 자동화 솔루션

Agenda

1 ASM(공격표면관리)

- 공격표면관리(AMS)란?
- 해커의 공격 프로세스
- 기존 보안 방식과의 차이점
- 자산 노출로 인한 해킹 피해사례
- 점점 더 중요시 되는 공격표면관리

2 Criminal IP ASM

- Criminal IP ASM 특장점
- 전체 기능 및 제품 UI 설명
- Criminal IP 검색엔진과의 연동
- 다른 ASM과 Criminal IP ASM의 차이

3 Product Features

- Criminal IP ASM 도입 방법
- Criminal IP ASM 공격표면관리 사례

4 About AI Spera

- 글로벌 CTI 선도 기업 AI Spera의 미션
- 경영진
- Trusted by the best
- Products
- 언론 속 AI Spera
- 기술력과 경영으로 인정받은 기업

1

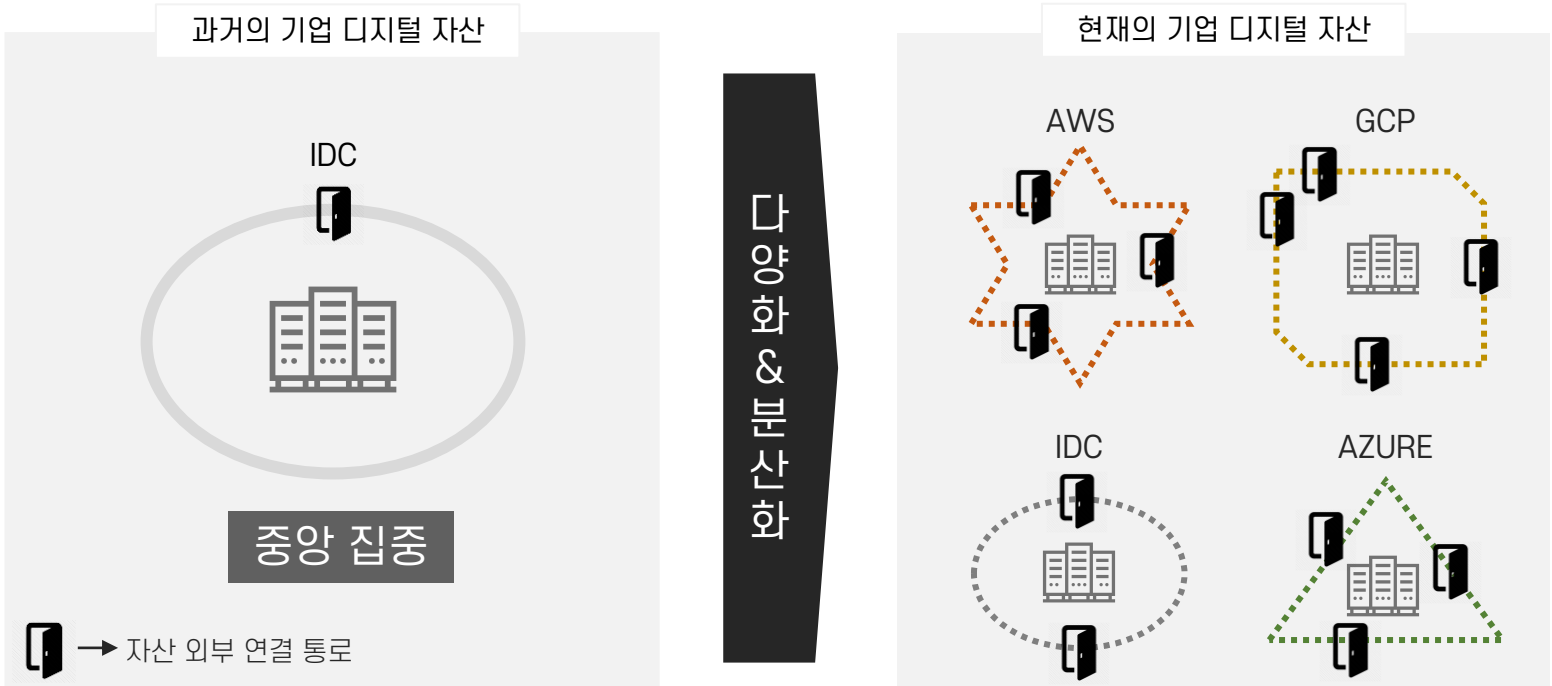
ASM(공격표면관리)

- 공격표면관리(AMS)란?
- 해커의 공격 프로세스
- 기존 보안 방식과의 차이점
- 자산 노출로 인한 해킹 피해사례
- 점점 더 중요시 되는 공격표면관리

공격표면관리(ASM)란?

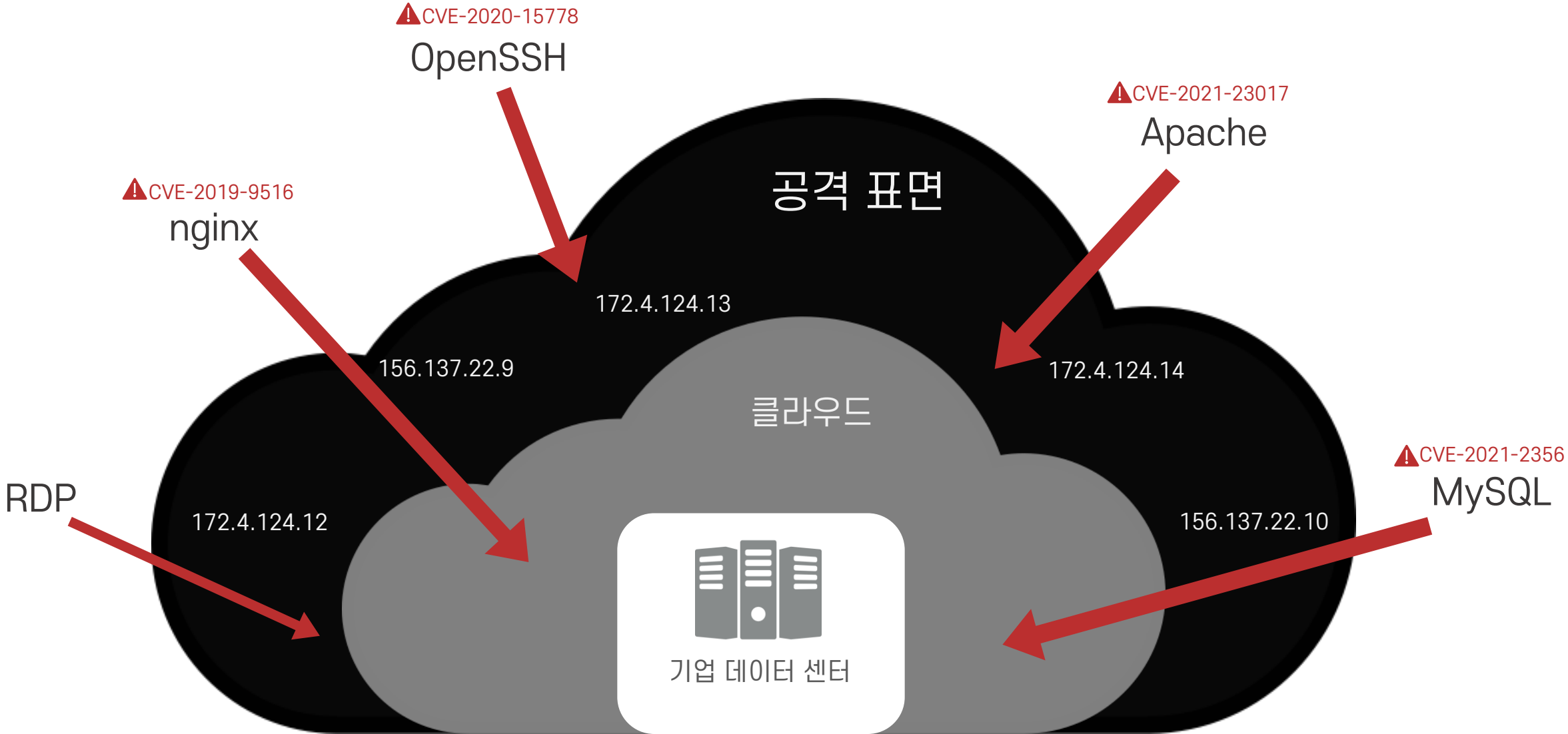
기업과 기관에는 수많은 네트워크 장비와 DB, 서버, 어플리케이션, 도메인이 존재하며, 이러한 모든 IT 자산은 IP 주소와 Port로 운영됩니다.
해커가 침투할 수 있는 열린 Port와 각종 서버 취약점, 유사 도메인과 피싱, 악성코드 유포 도메인 등의 공격 표면을 미리 탐지하고 관리하는 것이 '공격표면관리 (Attack Surface Management)'입니다.

기업의 IT 환경이 급격하게 변화하면서
공격표면은 파악하기 어려울 만큼 다양해지고 넓어지고 있습니다.



Attack Surface

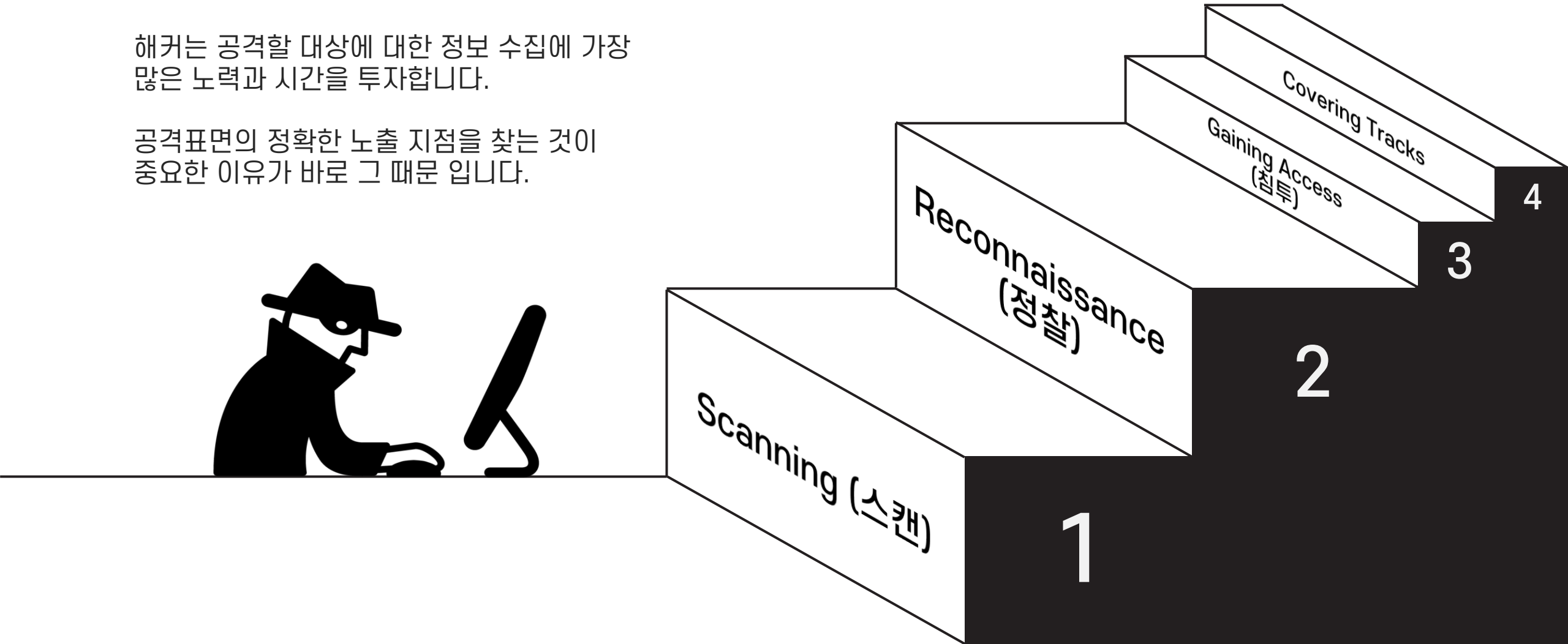
외부망의 모든 자원은 해커의 공격 타겟이 될 수 있습니다.



해커의 공격 프로세스

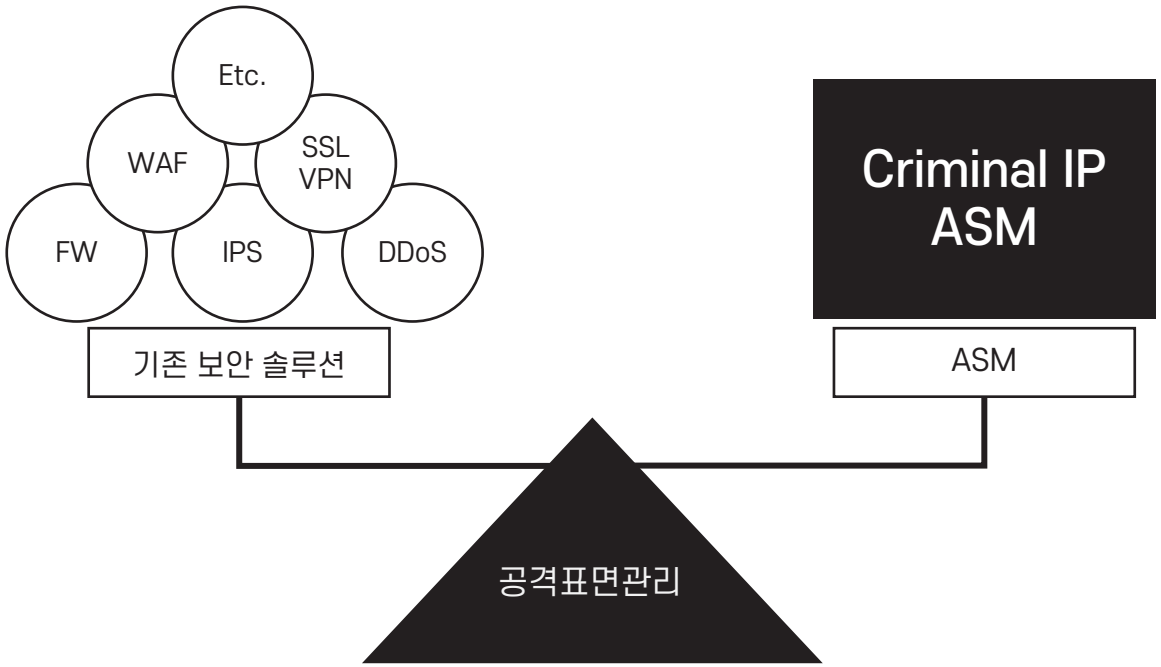
해커는 공격할 대상에 대한 정보 수집에 가장 많은 노력과 시간을 투자합니다.

공격표면의 정확한 노출 지점을 찾는 것이 중요한 이유가 바로 그 때문 입니다.



기존의 보안 방식과 공격표면관리의 차이점

기존 보안 장치와 솔루션은 공격이 발생하고 난 이후 대응에 주력합니다.
공격표면관리를 통한 보안 방식은 공격 가능한 자산 노출을 미리 파악하고 관리해 일어날 수 있는 공격을 사전에 차단합니다.



복잡한 작업
장애 위협 다수!

기존 보안 솔루션

- 별도의 장비 혹은 Software 설치 필요
- 연동 및 커스터마이징
- 수동적 정책 설정
- 지속적 업데이트 및 관리
- 장애 Point 다수
- 장애 발생 시 업무 중단

간소화 작업
장애 위협 없음

ASM
(Attack Surface Management)

SaaS 기반 Service로 번거로운 작업 없이
자동화 운영 가능

기존 보안 솔루션 취약점 탐지 Process

Hwang, Seong Oun. (2012). A Methodology for Security Vulnerability Assessment Process on Binary Code. The Journal of The Institute of Internet, Broadcasting and Communication, 12(5), 237–242. https://doi.org/10.7236/JIWIT.2012.12.5.237

ASM System 취약점 탐지 Process

ASM 도입 효과

공격표면 침투 확률 감소

비용&리소스 절감

업무효율 증가

공격표면 보안성 향상

1. ASM 자산 노출로 인한 해킹 피해사례

2020.04

국내 패션, 뷰티 커머스

기업 약 640만 건의 개인 정보 유출 피해

2020.05

국내 온라인 인테리어

플랫폼 약 200만 건의 개인정보 다크웹에서 판매

2020.06

2국내 여행 플랫폼

외부 공격자 서버 접속키 탈취
DB 정보 탈취

2021.03

현대 자동차 그룹

내부망 구조도, 보안 점검 보고서 등 3,500 여개 내부자료 다크웹에 유출

디지털 자산의 공격 표면 노출로 인한 피해 지속 증가

2021.06

한국원자력연구원

VPN 취약점으로 인해 13개 외부 IP에서 비인가 접속, 메일 시스템 및 KMS 인증서버 피해

2021.07

국내 자동차 관련 기업

매출 1조원 규모의 국내 자동차 관련 기업의 내부망 접근 권한 다크웹에 판매

2021.09

서울 성모 병원

해킹을 통한 개인정보 유출 사고
(ID, PW, 이름, 주민등록번호, 우편번호, 휴대전화번호 등 10개 항목)

2021.11

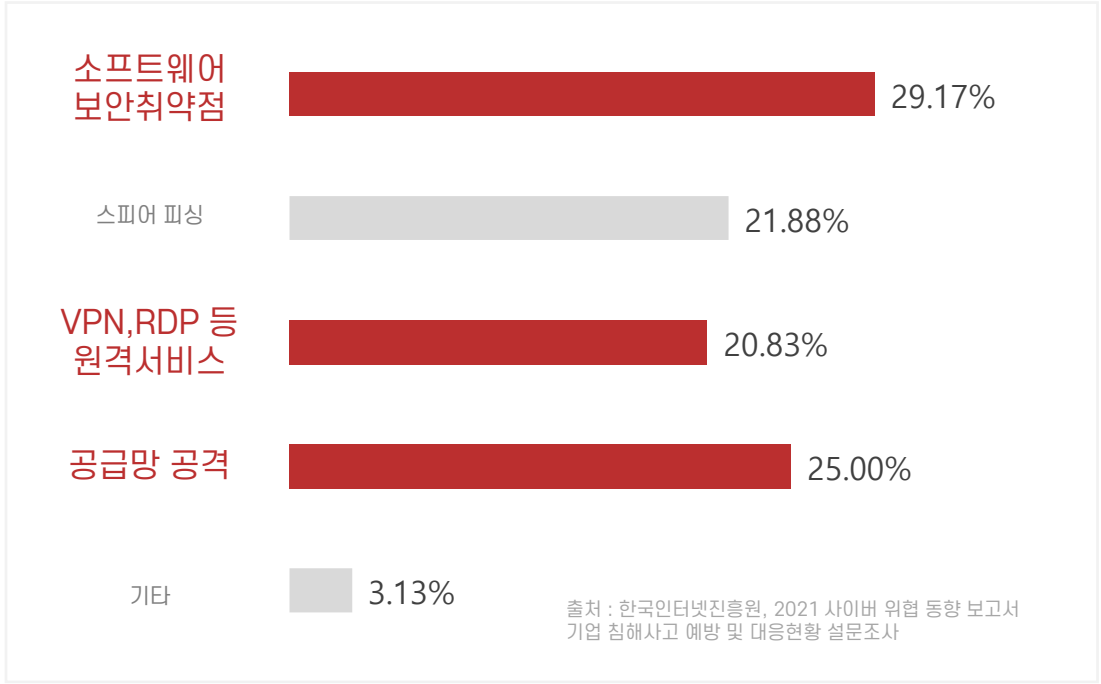
국내보안관리업체

A,B,C사의 월패드 해킹 사고
국내 아파트 내부 촬영 영상 다크웹에서 거래

한국인터넷진흥원 2021 하반기 사이버 위협 동향 보고서
한국재정정보원 사이버위협 정보 및 통계

기업에 가장 위협적인 공격 경로는

“자산 취약점과 원격 서비스 "



출처 : 한국인터넷진흥원, 2021 사이버 위협 동향 보고서
기업 침해사고 예방 및 대응현황 설문조사

코로나로 인한 재택 근무 확대
클라우드 작업환경으로의 전환
4차 산업 혁명 시대의 도래

사용자의 편의 증대
=
공격자의 위협 증가

보안 취약점을 미리 파악하여 공격표면을 줄이는 **공격표면관리의 필요성 증가**

2022년에도 해커의 타겟이 될 수 있는 공격표면은 증가할 것으로 예상됩니다.

- 다크웹의 대중화 추세, 사이버 범죄의 확산
- IoT 보안 패러다임 변화
- 클라우드 확산에 따른 보안 위협
- 전략의 혁신으로 중흥기 맞은 랜섬웨어
- 분산 네트워크와 제로트러스트의 대두
- 대선/올림픽/월드컵 등 대형 이벤트 노린 사이버 공격
- 메타버스/NFT 등 가상세계 플랫폼 확산과 보안 위협
- 수술실/지하철/요양원까지.. CCTV 의무 설치 확대
- 중대재해처벌법 시행에 따른 안전과 보안장비의 융합
- 비대면 트렌드에 따른 인증수단 다양화와 보안 강화

출처 : 2021.01.02 보안뉴스 “2022 보안 핫키워드 -10”

현재 정보보안시장에서 가장 주목받고 있는 공격표면관리(Attack Surface Management)의 필요성

Gartner®

"ASM은 조직이 인식하지 못할 수 있는 인터넷 연결 자산 및 시스템에서 오는 위험을 식별하는데 도움을 주는 새로운 솔루션이다. 최근 기업에 대한 성공적인 공격의 1/3 이상이 외부와 연결된 자산으로부터 시작되며 ASM은 CIO, CISO에게 필수의 과제가 될 것이다."

「2021 Emerging Technologies:
Critical Insights for External Attack Surface Management」

FORRESTER®

"조직은 ASM을 통해 평균적으로 30% 이상의 알려지지 않은 외부 자산을 발견한다. 일부는 알려진 자산의 몇 배나 더 많은 자산을 발견하기도 한다. "

「2022 ASM Report:
Find and Cover Your Assets with Attack Surface Management」

공격표면과 취약점 관리는 더이상 선택이 아닌 필수입니다

조직이 새로운 자산과 워크플로우를 더 넓고 깊게 수용할 수록,
ASM 도입은 선택이 아닌 필수가 될 것 입니다.

- ✓ 가트너 “디지털 워크플레이스, 직원들의 디지털 역량을 강화해 몰입적이고 직관적으로 업무할 수 있는 환경을 만드는 것“
- ✓ 디지털 전환 트렌드에 따라 AI, 클라우드, IoT 융합기술에 대한 기업의 투자와 관심 역시 집중
- ✓ 하지만 디지털워크플레이스는 ICT 기술이 활용돼 해커들의 새로운 공격대상으로 등극
- ✓ 이용자의 편익이 높아진 만큼, 해킹 위협도 증가
- ✓ COVID-19 대유행과 그에 따른 재택 근무 경제로 인해 기업의 공격 표면이 확대
- ✓ 기업은 클라우드 기반 애플리케이션, 장치 및 인적 보안 요소에 더 강점을 두고 있는 상황
- ✓ 분산된 디지털 작업 환경의 위험을 해결하는 확장된 취약성 관리 기능에 대한 수요는 그 어느때보다 강력
- ✓ 조직이 새로운 비즈니스 모델 운영에 익숙해짐에 따라, 새로운 플랫폼 및 애플리케이션을 위한 취약점 관리 기능이 선호될 것.

재택 근무의 일반화

- Covid-19 대유행과 그에 따른 재택 근무 확대로 기업의 공격표면이 확대
- VPN 등 원격 SW 대상으로 한 제로데이 취약점 증가
- 82%의 기업은 Covid-19 이후에도 재택근무 계속 지원

디지털 워크플레이스로의 전환

- 디지털 전환 트렌드에 따라 클라우드 작업환경에 대한 기업의 투자와 관심 집중
- ICT 기술이 적용된 디지털 워크플레이스는 해커들의 새로운 공격대상으로 등극
- 이용자의 편익이 높아진 만큼, 해킹 위협도 증가

4차 산업 혁명 시대, IoT 기기의 증가

- IoT 기기를 활용한 새로운 비즈니스 혁신
- 지난 5년 간 약 205억 개에 달하는 Device 연결

출처 : Frost & Sullivan, Global Vulnerability Management Market, Forecast to 2025

2

Criminal IP ASM

- Criminal IP ASM의 특장점
- 전체 기능 및 제품 UI 설명
- Criminal IP 검색엔진과의 연동
- 다른 ASM과 Criminal IP ASM의 차이

고객 자산 자동 탐지

고객이 알고 있는 자산과 알지 못하는 자산까지 전체 인터넷 대상으로 스캔하여

사용중인 IP주소와 열려 있는 모든 Port에서 운용 중인 네트워크 자산 전체를 탐지합니다.

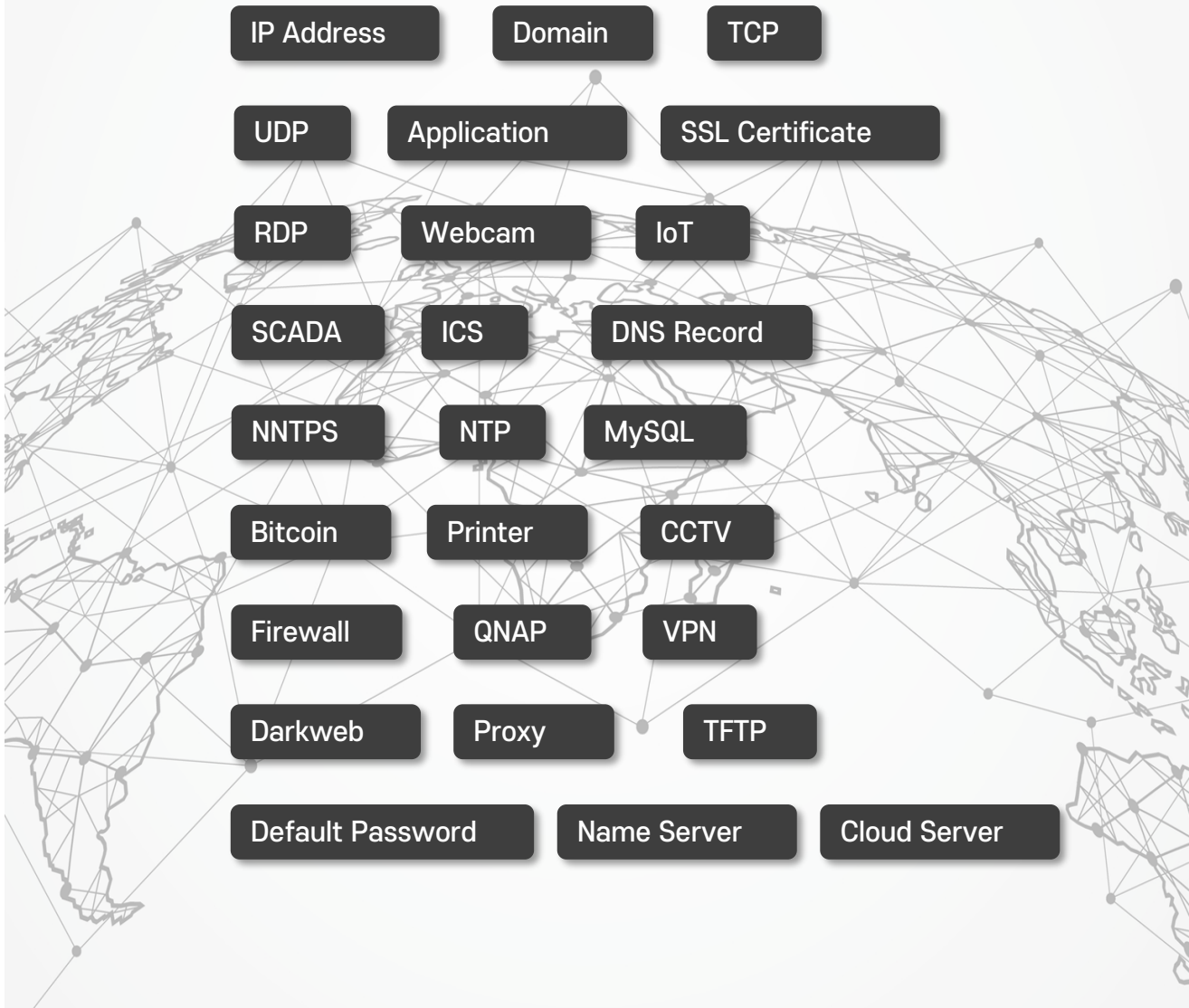
IP 42억 개 IP주소 정보

+

Port 전 세계 Port 스캔 데이터

+

Domain 3억 개 이상의 Domain 주소 데이터



클라우드 기반 웹 인터페이스

Criminal IP ASM은 SaaS 형태의 ASM 제품으로
도입 시 고객사 서버 내에 하드웨어 또는 소프트웨어를
설치하거나 구축할 필요가 없습니다.

고객사 계정 등록 이후 고객사의 네트워크가 연결된
PC, 태블릿, 모바일 기기의 브라우저를 통해
웹 인터페이스로 빠르고 쉽게 공격표면관리 솔루션을
사용할 수 있습니다.

설치형 On-Premises

유지 비용

- 초기 제품 설치 및 내부 서버 구축
- 시스템 업데이트 패치, 업그레이드
- 내부 서버 및 네트워크 장애 이슈 관리
- 하드웨어 유지보수 및 업그레이드
- 네트워크 유지보수 및 업그레이드
- 보안 유지보수 및 업그레이드
- 데이터베이스 유지보수 및 업그레이드

클라우드 SaaS

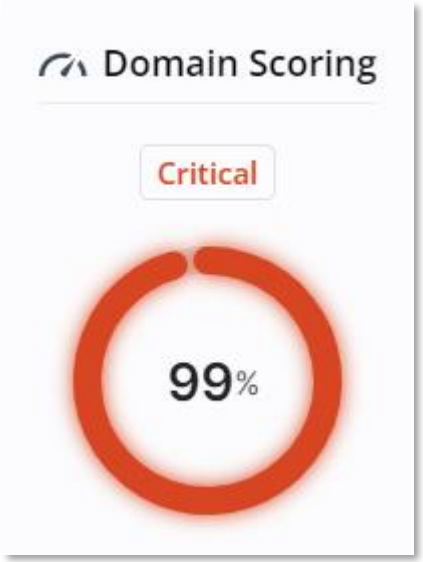
유지 비용

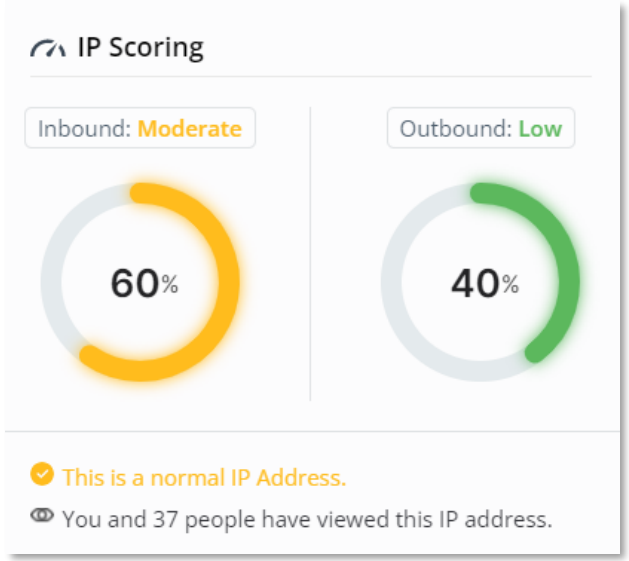
- [x] 연간 구매
- [x] 사용법 가이드 및 교육
- [x] 맞춤형 커스터마이징

자산 및 취약점 위험도 스코어링

AI 머신러닝을 통한 자체 알고리즘을 통해 실시간 탐지된
모든 자산을 5 단계의 위협 스코어링으로 시각화 합니다.

보안 담당자는 시각화된 스코어링을 통해 사이버 위협 우선순위를
지정하여 빠르고 정확하게 보안 위협에 대응할 수 있습니다.





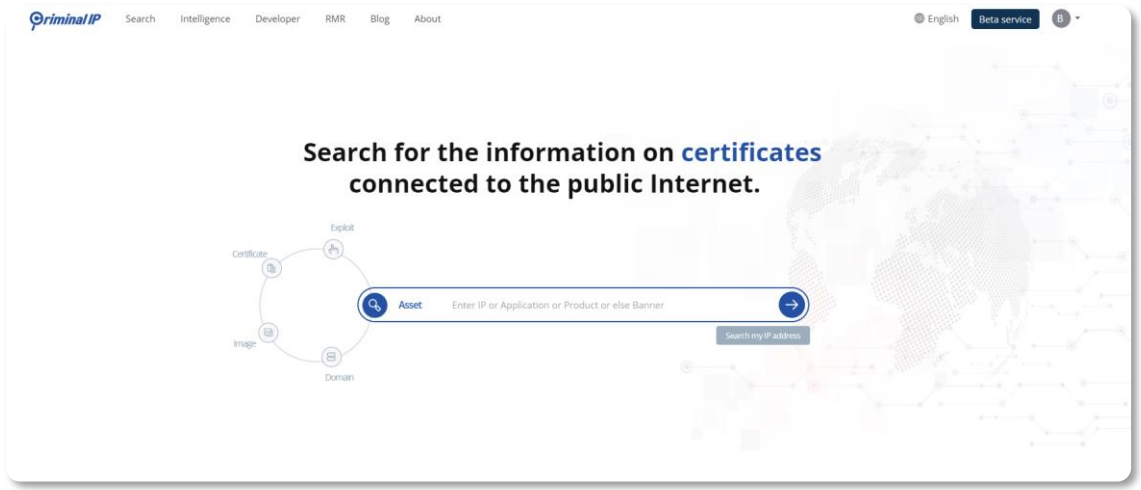
	IP/Asset	Domain/Certificate
Critical	네트워크 및 자산에 공격의 흔적이 있거나 공격 당하고 있는 상태	도메인과 인증서가 위조되었거나 악성 링크가 포함되어 위험한 상태
Dangerous	네트워크 및 자산이 공격표면에 노출되어 공격 될 수 있는 상태	도메인이 위조되었거나 인증서가 유출 또는 만료되어 관리가 필요한 상태
Moderate	네트워크 및 자산이 일반적인 보안 정도를 유지하고 있는 상태	도메인과 인증서가 일반적인 보안 정도를 유지하고 있는 상태
Low	네트워크 및 자산이 외부에 노출되어 있지 않고 안전한 상태	도메인이 위조되었거나 인증서가 유출, 만료되지 않은 안전한 상태
Safe		

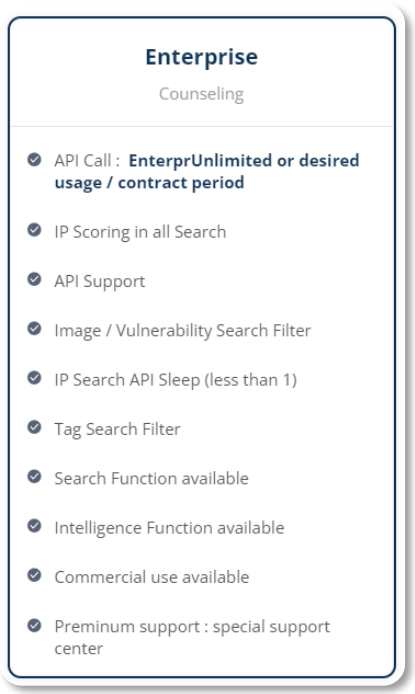
CTI 검색엔진 무료 연동

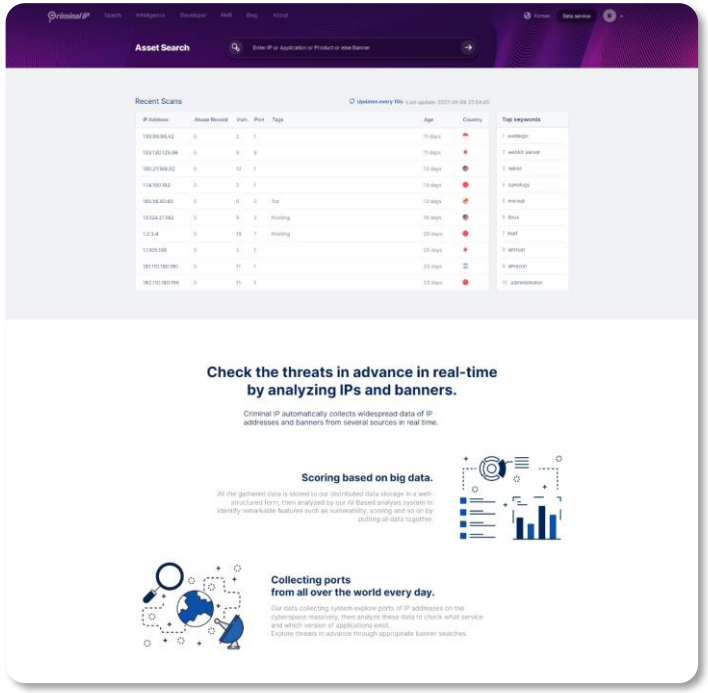
인터넷에 연결된 모든 IP주소와 배너정보를 검색할 수 있는
Cyber Threat Intelligence 검색엔진 Criminal IP에서 ASM에
탐지된 기업 자산 정보를 상세하게 검색할 수 있도록 제공합니다.

Criminal IP 검색엔진 주요 기능

Search	Intelligence
Asset Search	Banner Explorer
Domain Search	Vulnerability
Image Search	Statistics
Certificate Search	Element Analysis
Exploit Search	Map

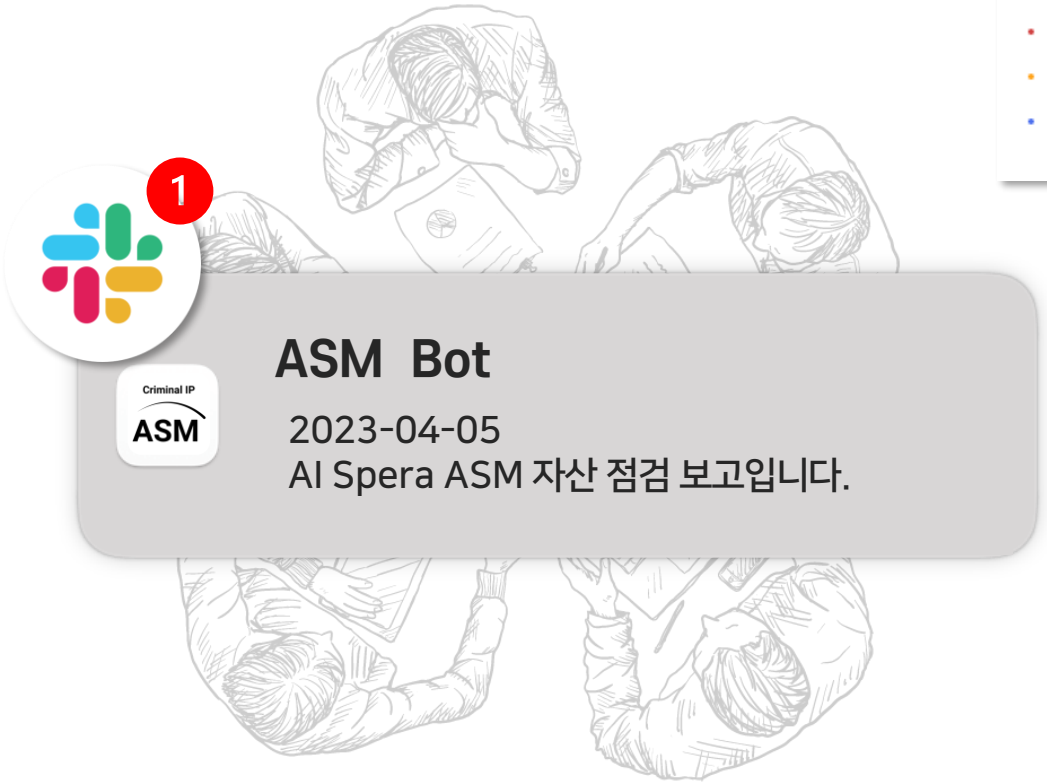






데일리 분석 리포트 발송 & 메신저 연동

신규 자산 및 취약점에 대한 데일리 리포트 메일이 자동으로 발송되며, Slack 등 업무 메신저를 연동해 빠른 대응이 가능한 알람 서비스를 제공합니다.



Criminal IP ASM 전체 기능

전 세계 IP 정보 기반의 사용정보, 위험등급을 제공합니다.
간단한 검색만으로도 악성 URL 및 도메인 검증, 노출된 취약점 정보를 파악할 수 있습니다.

New Assets
추가되거나 변경된 자산을 자동으로 탐지합니다.

IP Assets
탐지된 IP주소의 열린 포트를 스캔하여 제공합니다.

Domain
탐지된 IP주소의 연결된 도메인, 서브도메인을 제공합니다.

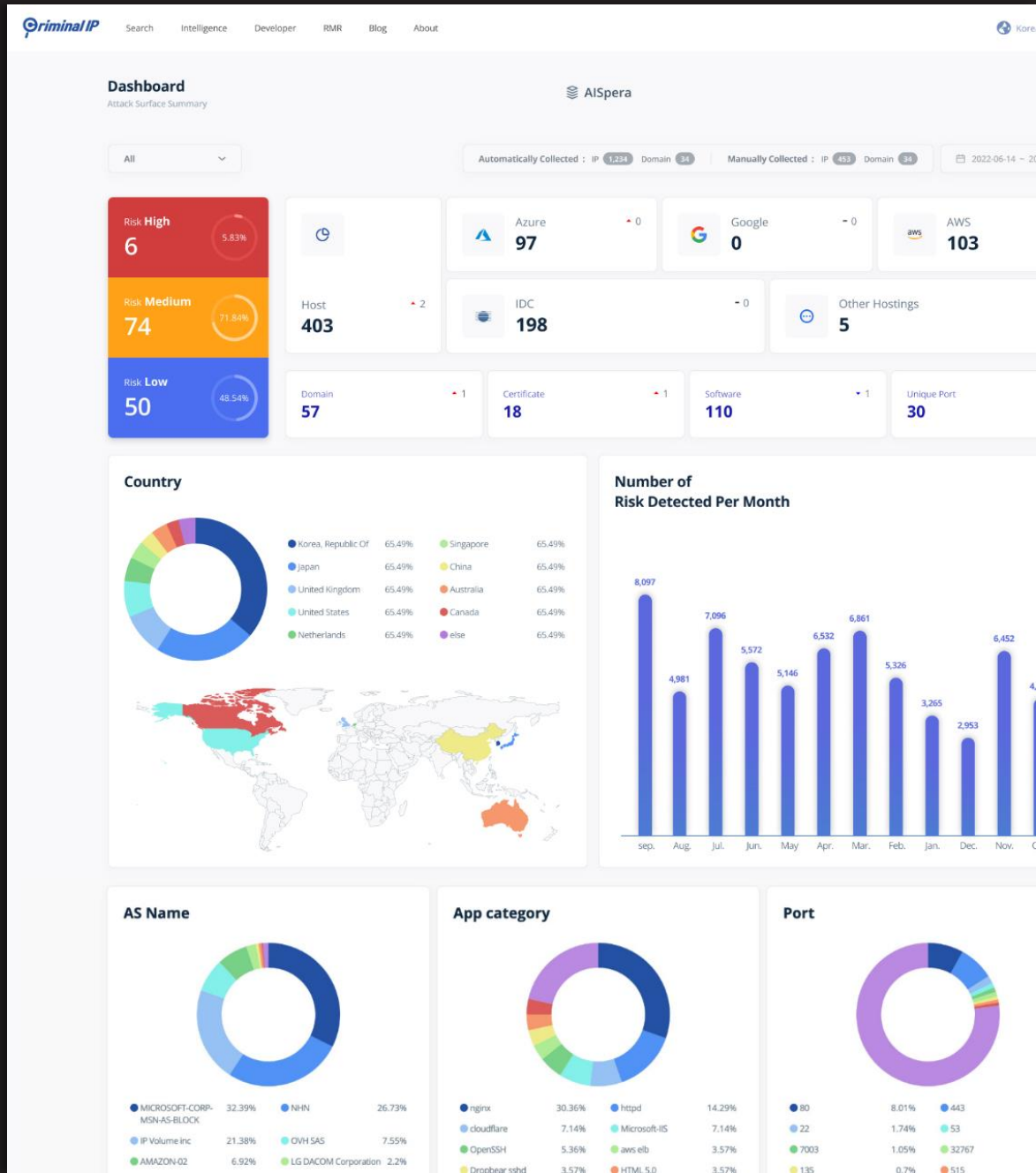
Certificate
도메인에 적용된 인증서 종류와 정보를 제공합니다.

Risk
IP, 도메인, 인증서, 어플리케이션 등 모든 자산의 공격 가능한 취약점을 제공합니다.

Intelligence Search Result
자산의 공격표면 노출 정보와 취약점에 대한 상세 정보를 확인할 수 있습니다.

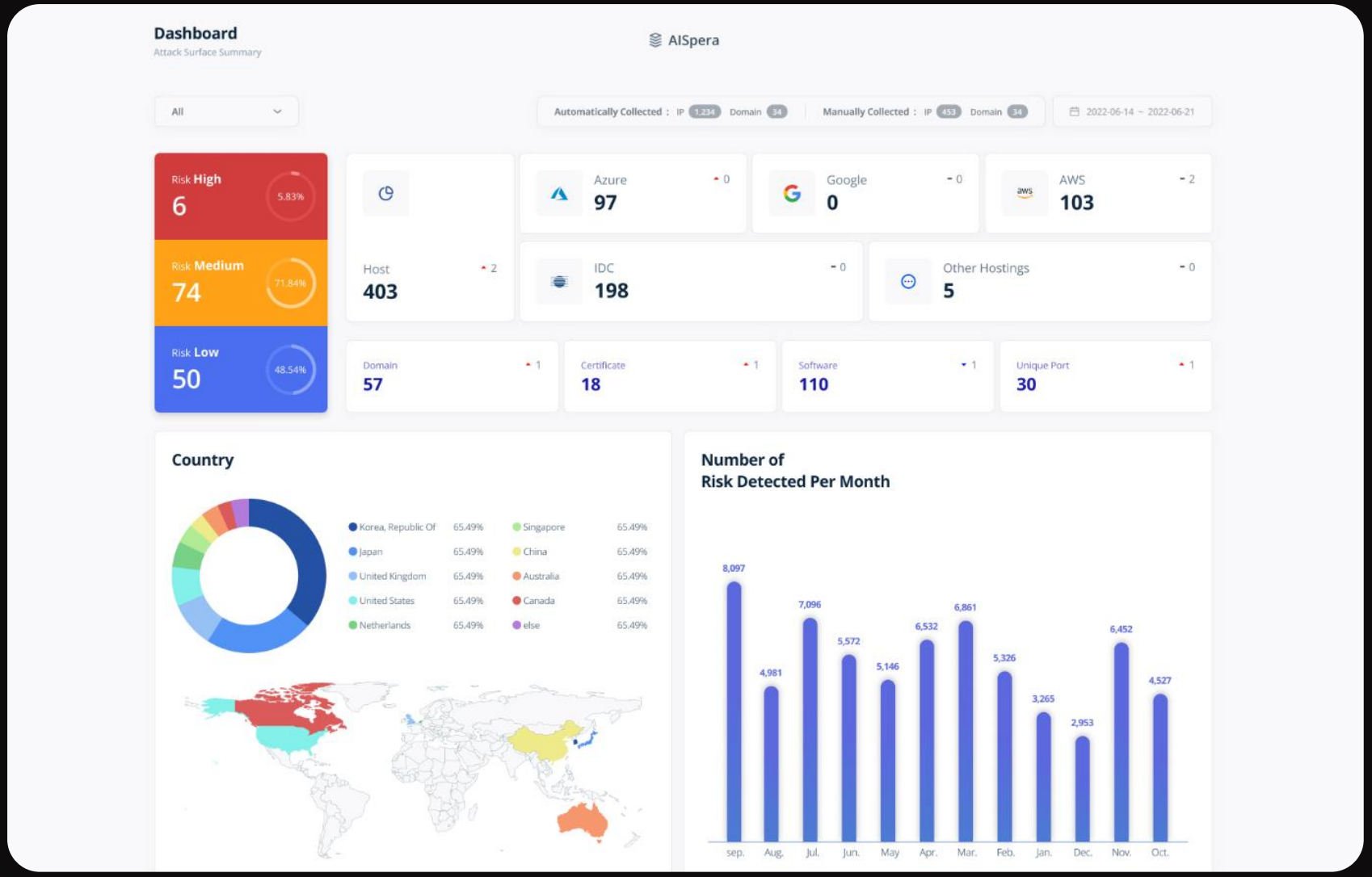
Dashboard
전체 자산 통계와 자산 위치 정보, 취약점 현황과 그래프를 대시보드로 제공합니다.

OSINT (Google Hacking)
구글에 노출된 자산 정보를 모니터링할 수 있도록 제공합니다. 자산 검색 쿼리를 제공합니다.



Dashboard

Criminal IP ASM에서 자동 탐지된 기업이 가지고 있는 전체 IT 자산의 전체 통계와 지리 정보, 취약점 현황을 한눈에 볼 수 있습니다.



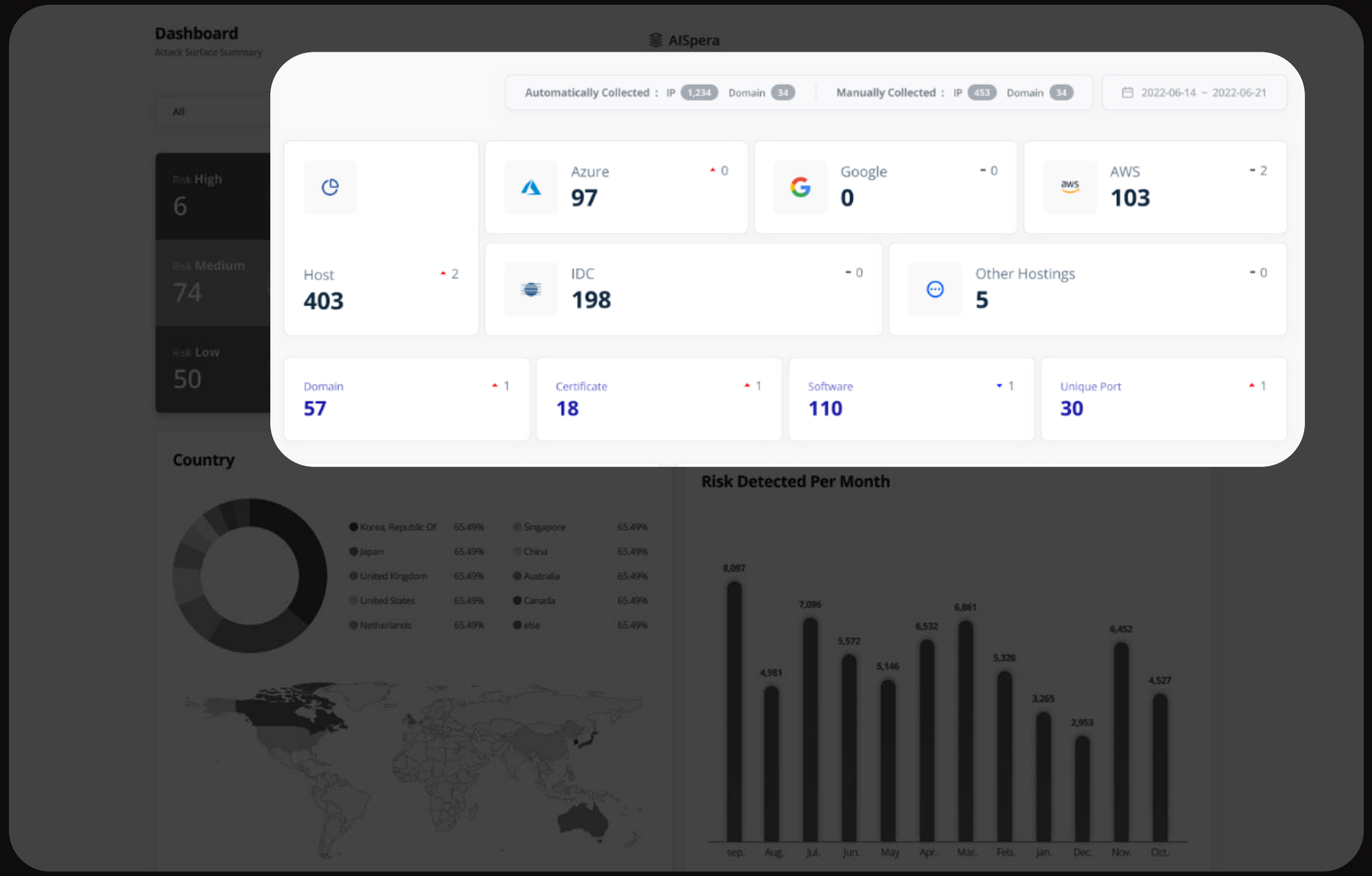
Risk 분류

자동 탐지된 자산을 위험도에 따라
High, Medium, Low 3단계로 구분하여
보안 조치가 시급한 자산을 빠르게
파악할 수 있습니다.

Host, 클라우드 통계

자동 탐지된 기업의 전체 Host 수와
클라우드 자산 현황을 보여줍니다.

각 클라우드로 분류된 자산과 IDC 자산의
총 합계는 전체 Host 수와 일치합니다.

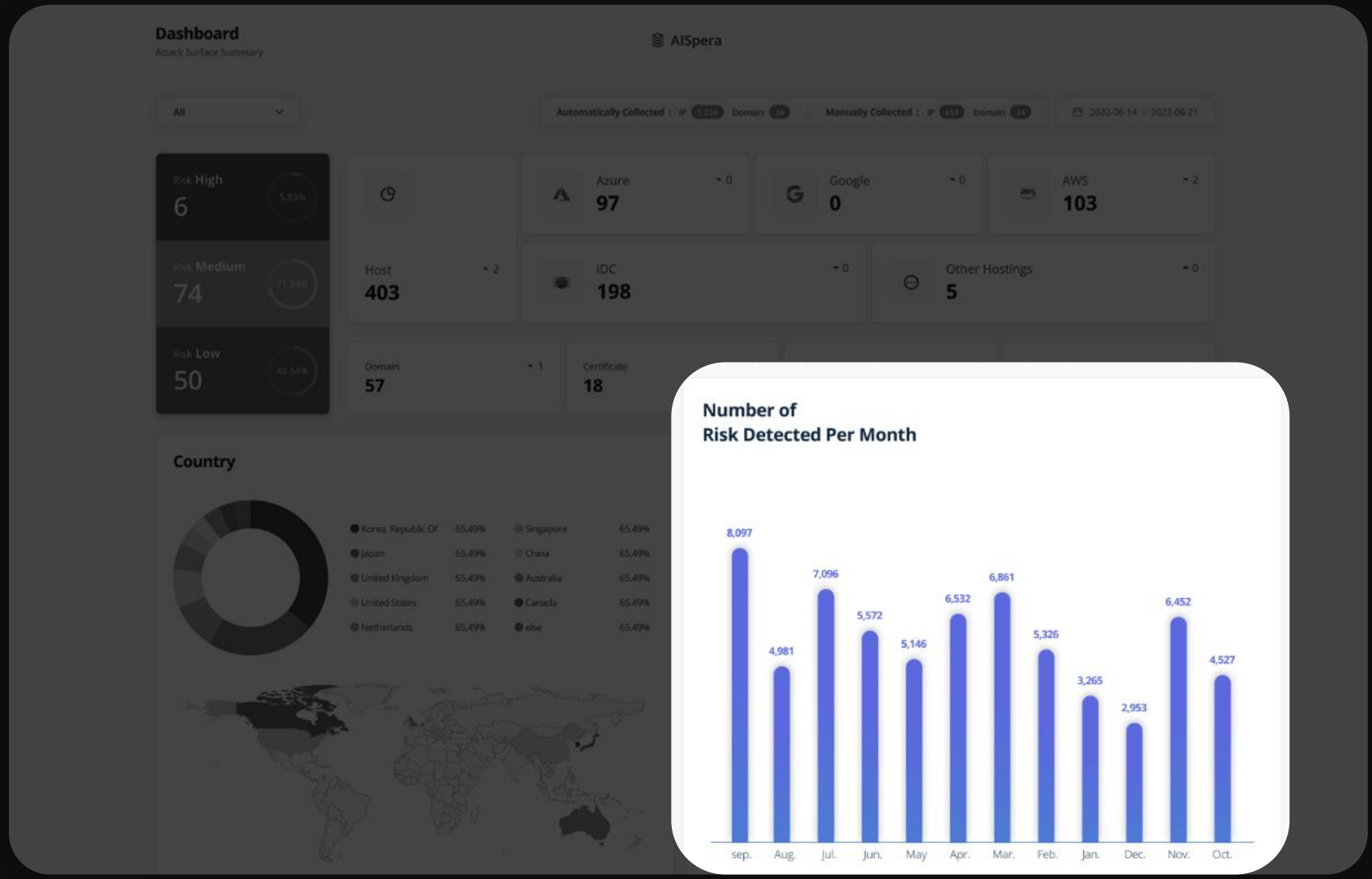


자산 지리적 통계

전 세계의 IP 주소 데이터를 바탕으로
기업의 IT 자산의 지리적 분포를
확인할 수 있습니다.

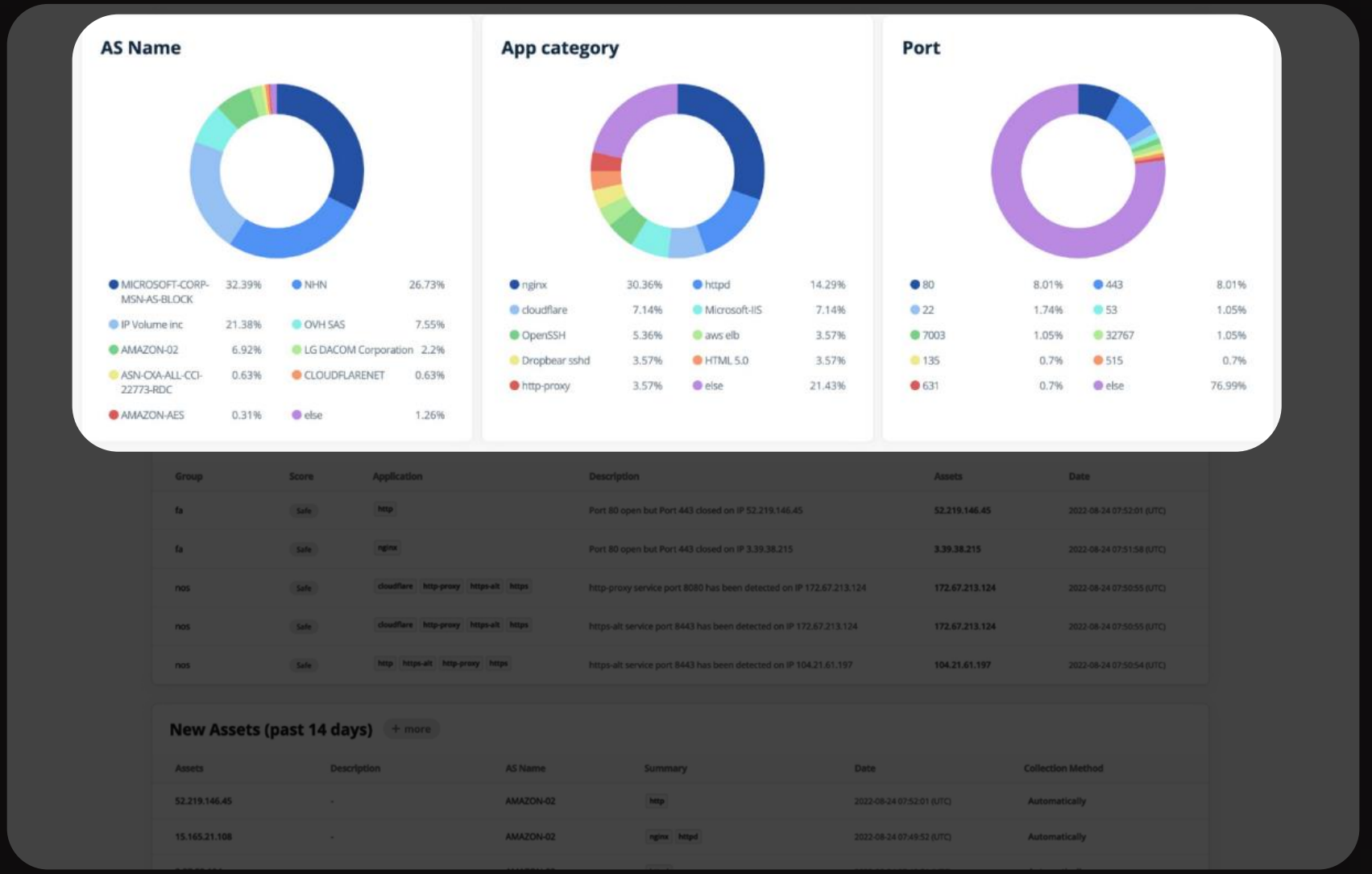
취약 자산 그래프

탐지된 자산 중 취약한 자산의 개수를 월 별 그래프로 보여줍니다.



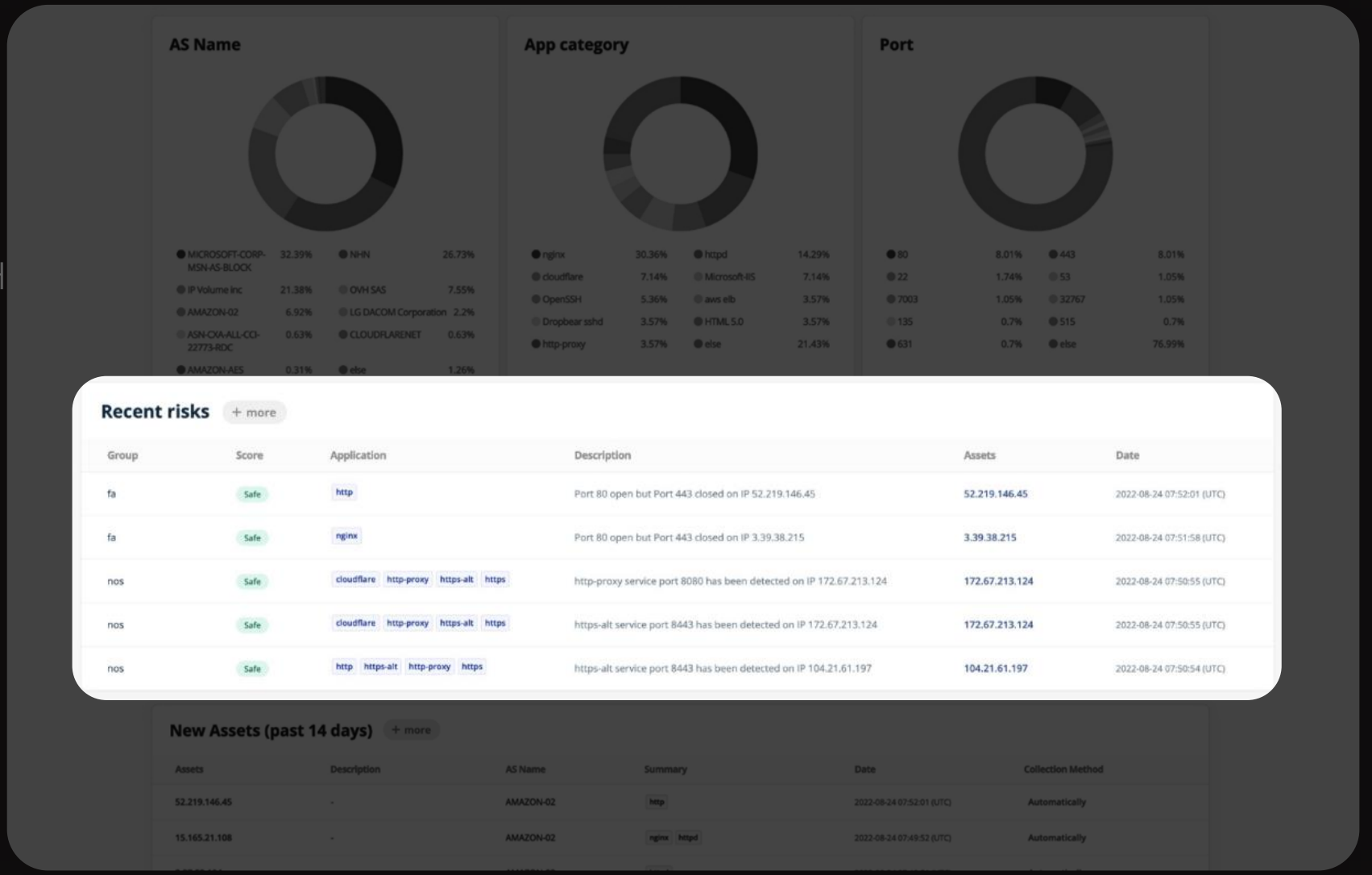
AS Name, Software, Port 통계

탐지된 자산의 ASN, 어플리케이션,
열려 있는 포트의 비율을 차트로
시각화 하여 쉽게 확인할 수 있습니다.



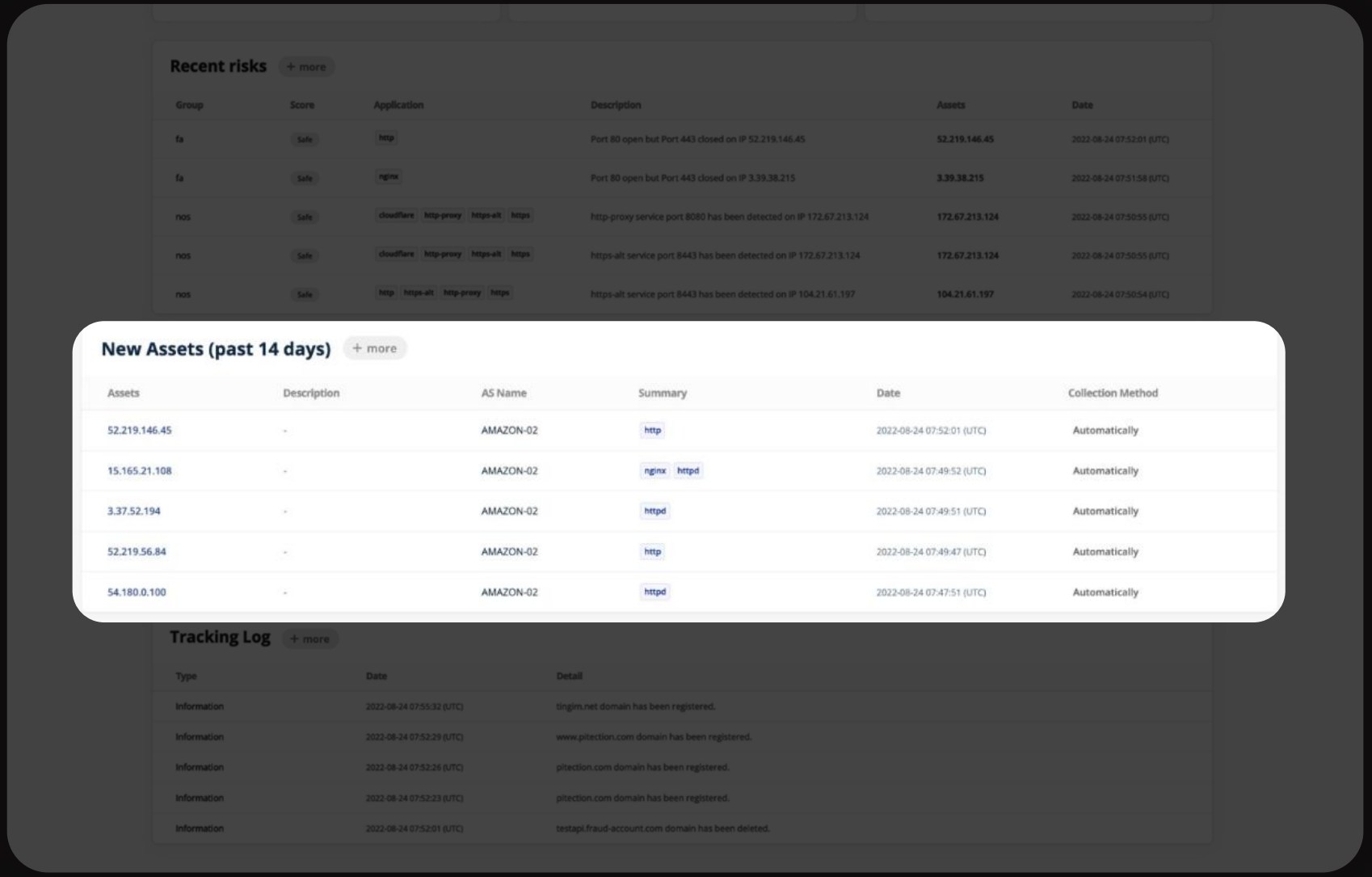
Recent Risks

가장 최근 발견된 자산 취약점을 보여줍니다.
데이터(Assets)를 클릭하면 해당 취약점에 대
상세 정보를 확인할 수 있습니다.



New Assets

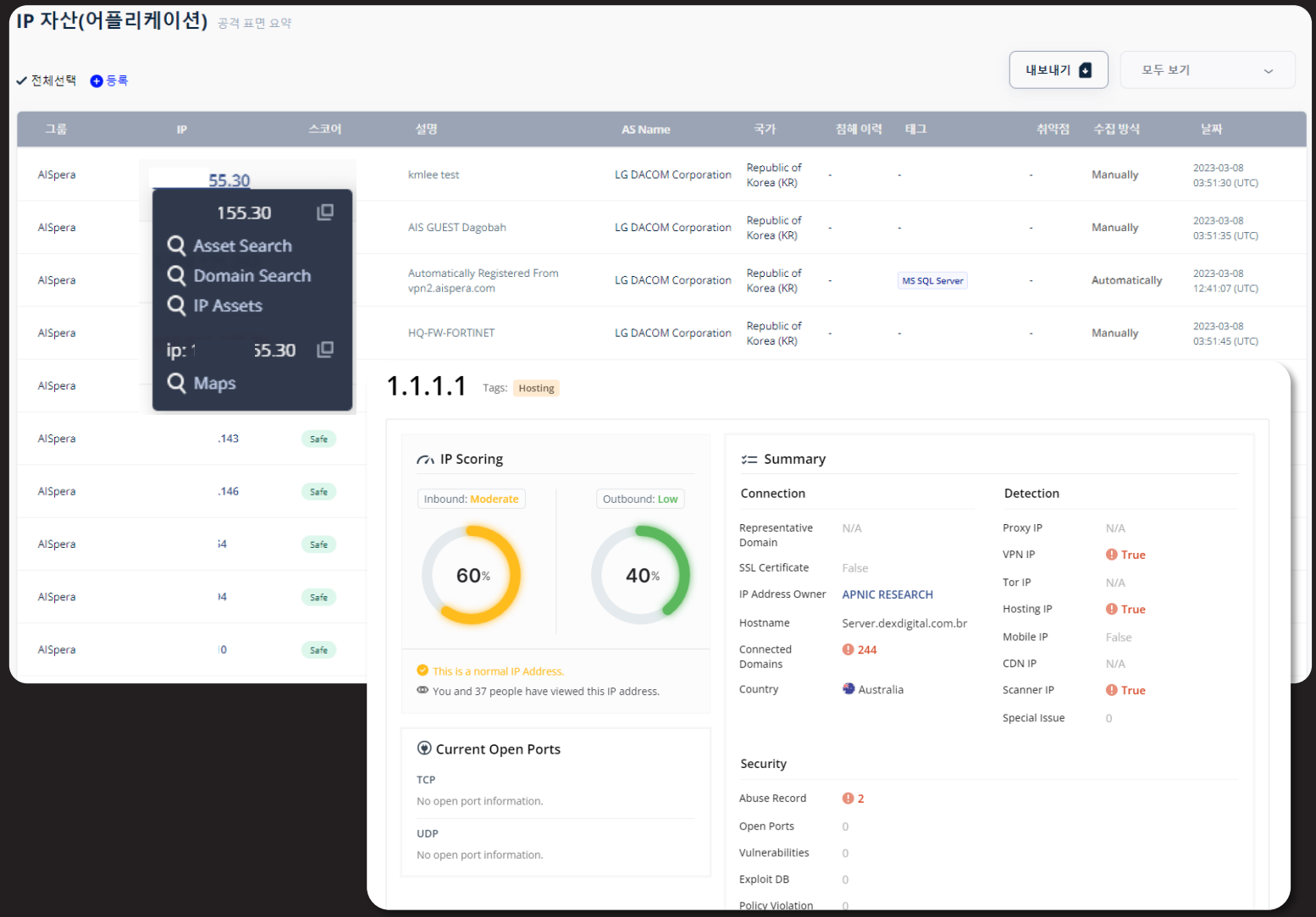
가장 최근 추가된 자산 데이터를 보여줍니다.
각 Assets을 클릭하면 자세한 자산 정보를 확인할 수 있습니다.



IP Assets (Application)

탐지된 IP 자산의 요약된 정보 (위험도 Score, AS Name, 위치 정보, 취약점)를 확인할 수 있습니다.

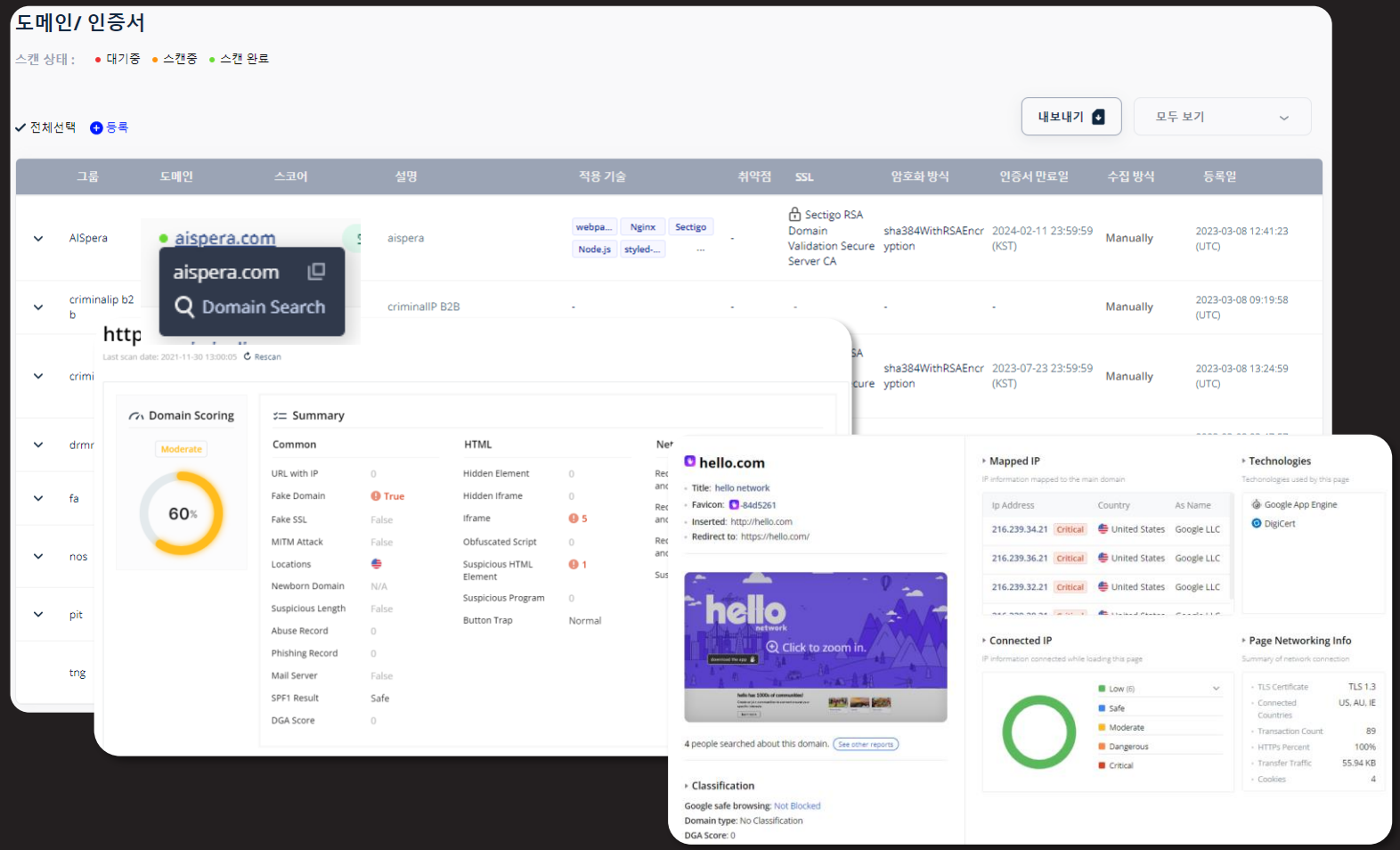
IP 주소를 클릭하면 인텔리전스 검색엔진으로 연동되어 IP 주소에 대한 위협 인텔리전스를 조회할 수 있습니다.



Domain / Certificate

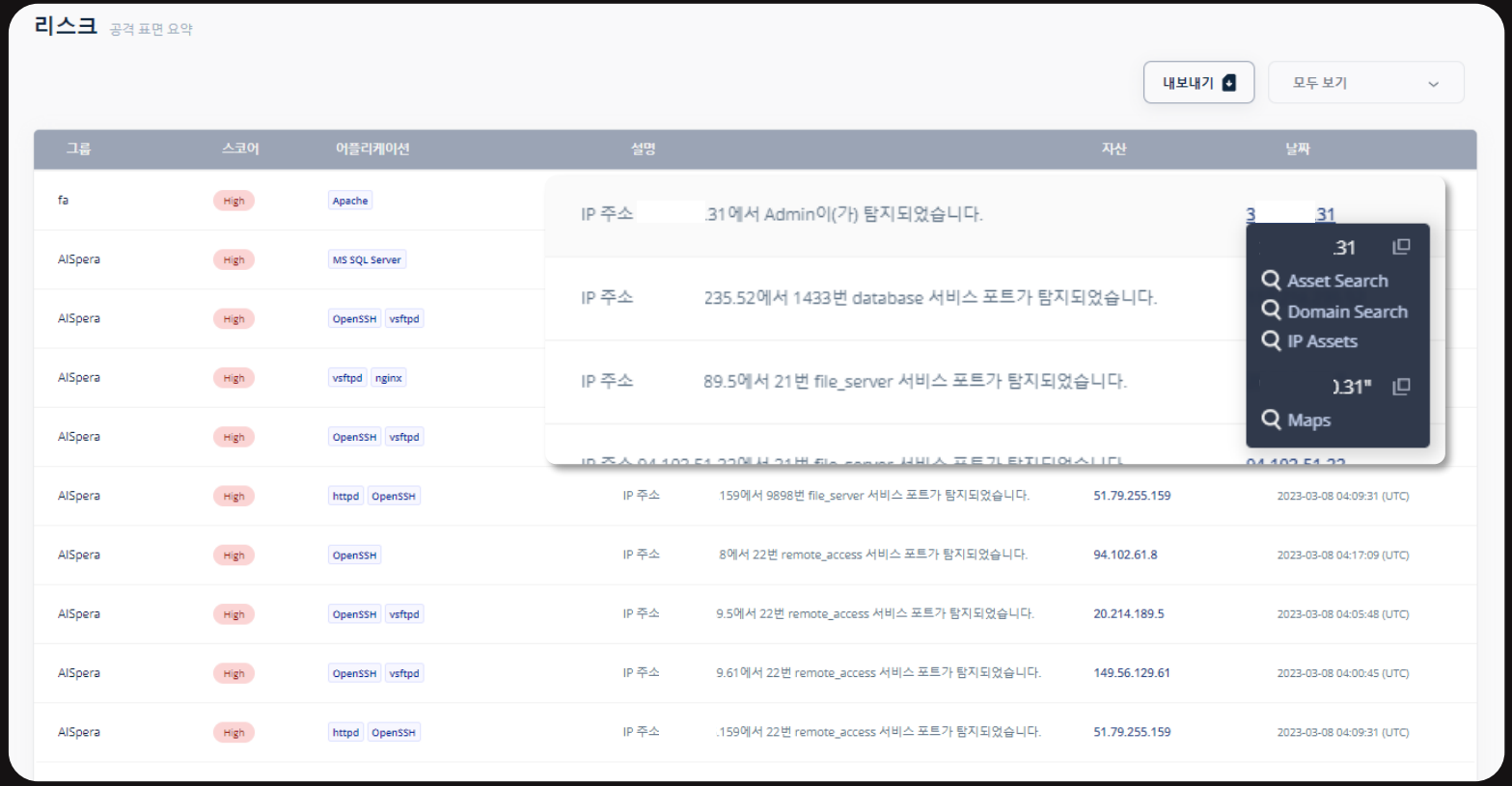
사용자가 등록한 도메인에 대한 요약된 정보(Score, Technology, jQery, PHP 등)와 도메인에 대한 취약점 개수(Vuln.), 인증서 정보(SSL, Encryption, SSL Expire Date), 서브 도메인에 대한 요약 정보를 보여줍니다.

도메인 클릭 시 인텔리전스 검색엔진으로 연동되어 도메인과 인증서에 대한 위협 인텔리전스를 조회할 수 있습니다.



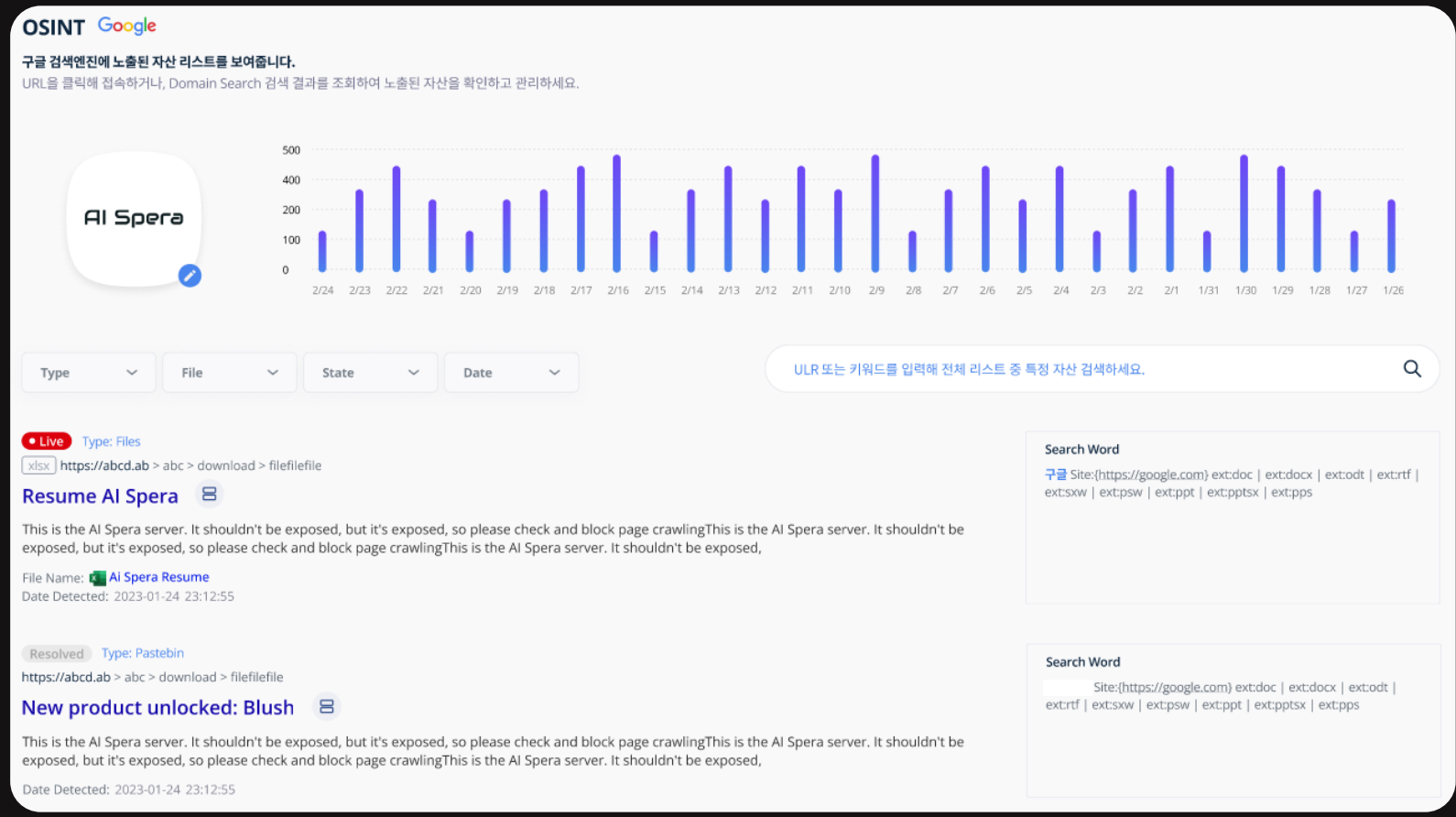
Risks

사용자가 등록한 자산(IP, Domain)에서 위협점이 발견되면 자동으로 Risk 페이지에 추가되어 위협에 노출된 자산 정보를 빠르게 확인할 수 있습니다.



OSINT(Google Hacking)

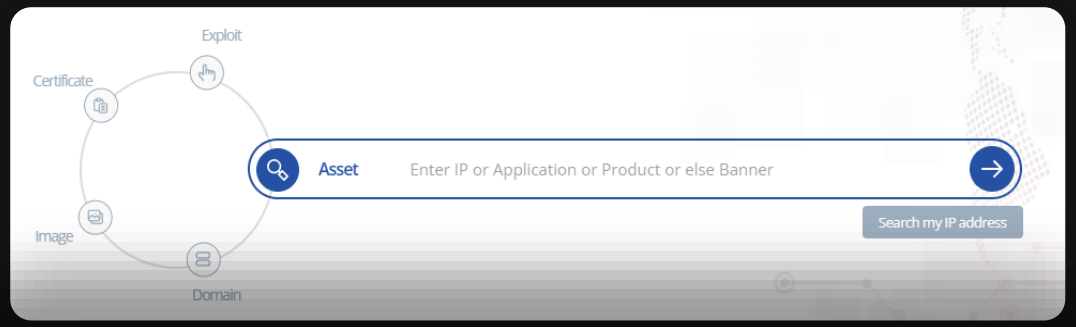
구글 검색엔진에 노출된 자산의 리스트를 보여줍니다.
노출된 자산의 Type, File 유무, 접속 가능 상태 등을 확인할 수 있습니다.

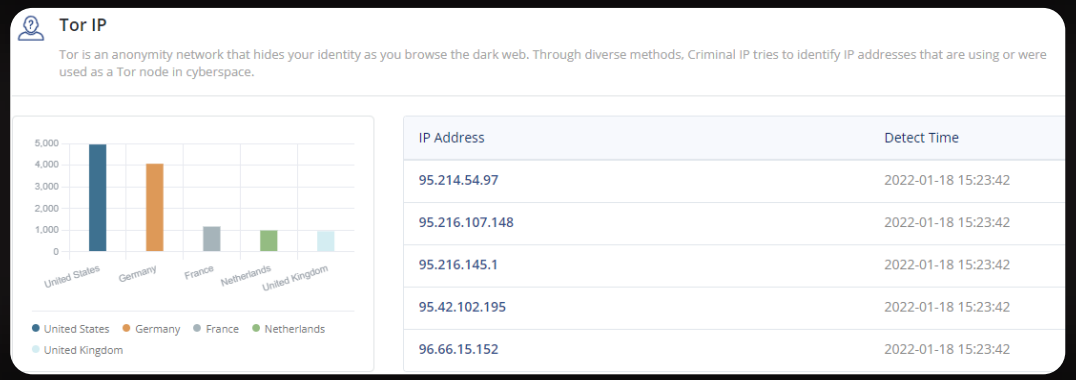


Criminal IP
위협인텔리전스 검색엔진

Criminal IP ASM 도입 시 Criminal IP CTI 검색엔진의 Search, Intelligence, API 통합 기능을 추가적으로 사용할 수 있습니다.

최신 글로벌 보안 위협에 대한 분석 리포트와 통계를 통해 빠르게 보안 동향을 파악 할 수 있습니다.





다른 ASM 제품과 Criminal IP ASM의 차이

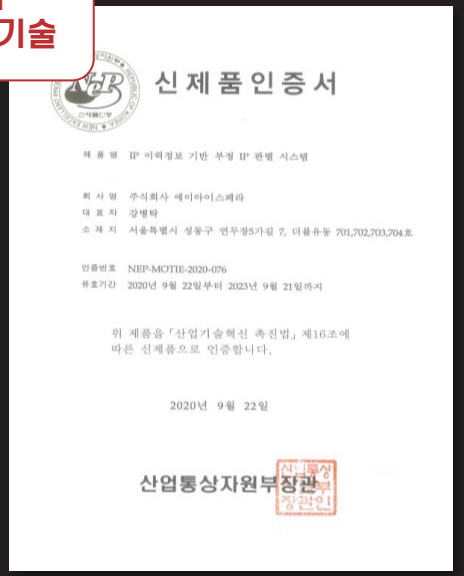
	Criminal IP ASM	G사	F사
Company Location	국내 유일	외산	외산
인증	NEP인증, GS인증	X	X
Automation	O	O	△
Data Update	24시간 이내	??	??
자산 상세 검색기능	O	X	X
IP 인공지능 분류/분석	O	X	X
Domain 인공지능 분류/분석	O	X	X
HoneyPot	공격 대비 맞춤형 HoneyPot 운영	O	O
Alert 기능	Issue 발생 시 Report 발송	일간 Report	△
서비스 중인 어플리케이션 탐지/분류	O	△	X

국내 유일 ASM System 제조업체

- 국내 특수한 보안 시장에 대해 분석가능한 인력(능력)보유
- 급속히 변화하는 국내 보안 동향에 맞춰 가장 빠르게 대응 준비
- 국내 보안시장 동향 분석 전문가 다수 -> 빠르게 변화하는 보안 취약점에 대한 대응 준비 가능
- 국내 보안에 대한 광범위한 지식 및 노하우를 바탕으로 AI 기술력을 더하여 신속한 제품 개발
- 모든 규모의 기업에서 합리적인 가격으로 ASM 서비스를 제공 할 수 있도록 최적화된 제품을 개발

국내 유일 제조사

국가가 인정한 신기술



신 제 품 인 증 서

제 품 명 IP 이력정보 기반 부정 IP 판별 시스템

회 사 명 주식회사 에이아이스페라
대 표 자 강병탁
소 재 지 서울특별시 성동구 연무장5가길 7, 더블유동 701,702,703,704호

인증번호 NEP-MOTIE-2020-076
유효기간 2020년 9월 22일부터 2023년 9월 21일까지

위 제품을 「산업기술혁신 촉진법」 제16조에 따른 신제품으로 인증합니다.

2020년 9월 22일

산업통상자원부장관

국내 최초 개발 제품

NEP 인증 획득

NEP인증 대상제품 :
국내에서 최초로 개발된 기술 또는 이에 준하는 대체기술로서 기존의 기술을 혁신적으로 개선 개량한 신기술이 적용된 제품으로 사용자에게 판매되기 시작한 후 3년을 경과하지 않은 신 개발제품

인증된 신제품 지원 항목

- 공공기관 20% 의무구매(산업기술혁신촉진법, 산업통상자원부)
- 공공기관 우선구매 대상(중소기업청)
- 산업기술혁신촉진법에 따라 산업기반자금 융자사업자 선정 시 우대
- 기술우대보증제도 지원대상(기술심사 면제)
- 혁신형 중소기업 기술금융지원(국민은행, 기업은행, 산업은행, 우리은행)
- 중소기업기술혁신개발사업에 가점(중소기업청)
- 자본재공제조합의 입찰보증, 계약보증, 차액보증, 지급보증, 하자보증 우대 지원
- 신기술실용화 정부포상 대상

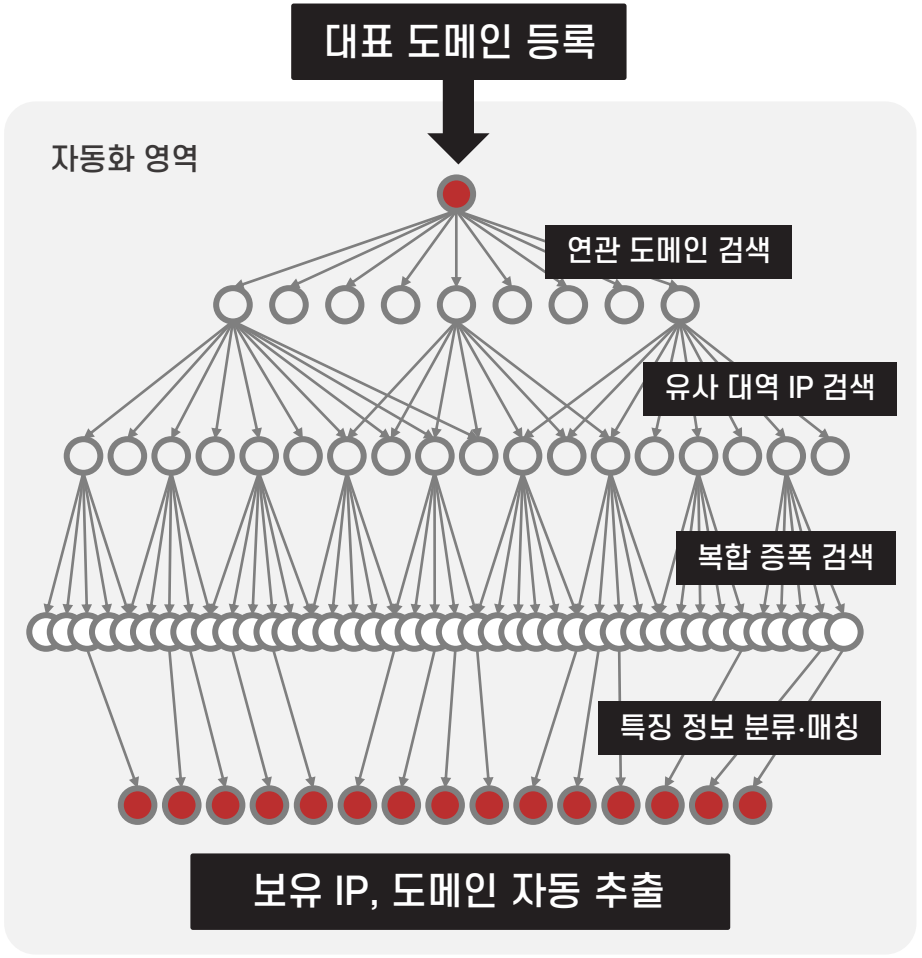
3

Product Features

- Criminal IP ASM 도입 방법
- Criminal IP ASM 공격표면관리 사례
- 자산의 공격표면 노출 Real Data

Criminla IP ASM 도입에는 오직 한 가지만 필요합니다.

Criminal IP ASM 도입을 원하는 기업 및 기관에 여러가지 정보를 요청하지 않습니다.
운용하고 있는 자산 중 단 한 개의 도메인 주소만 있으면 전 세계 네트워크에 분포되어 있는 모든 자산을 자동으로 식별하여 공격표면 관리를 시작할 수 있습니다.



자동 등록

Attack Surface Management

Criminal IP ASM로 발견한 공격표면 Real Data

지금 이 순간에도 수 많은 기업 및 기관의 주요 자산들이 공격표면에 무방비로 노출되고 있습니다.

SW 패치 서버

Dev/Test 시스템

마케팅 이벤트 페이지

협력업체 공유시스템

새로운 취약점이 발견되는 경우

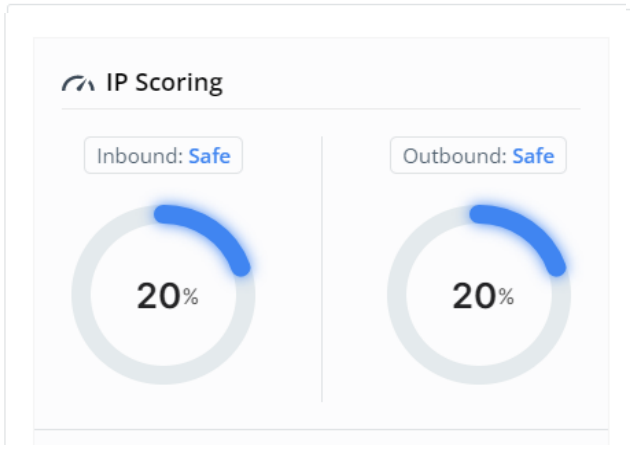
기업이 운용 중인 자산에 대한 위협 인텔리전스 분석을 통해 공격 가능한 취약점이 있는 자산의 경우
위협 스코어링으로 시각화 하여 리포트를 제공합니다. Criminal IP의 Vulnerability 기능을 통해 취약점에 대한 대응방안을 확인할 수 있습니다.

Safe

2021.01.30
(Before)

Server A

1.2.3.4 Tags: Hosting



New
CVE-2021-44228

Critical

2021.02.01
(After)

Server A

1.2.3.4 Tags: Hosting

3. Product Features Criminal IP ASM을 통한 공격표면관리 사례

새로운 취약점이 발견되는 경우

공공기관 B

국정원 지침에 따라 **6개월 마다 취약점을 점검**하는 공공기관 'B'

취약점 점검

1월

대규모 취약점 점검 진행

시스템 패치

2월

한달 간 전체 시스템 순차적으로 패치 진행

취약점 방치

3월~6월

하반기 점검 일정까지 신규 취약점 유무 확인 불가

Criminal IP ASM

공공기관 B에 공격표면관리 자동화 솔루션 Criminal IP ASM 도입

Criminal IP ASM

CIP ASM 도입

Criminal IP ASM을 통한 상시 취약점 점검 실행

LOG4J

취약점 발생

대규모 보안 취약점(Log4shell) 이슈 발생

자동 점검

Criminal IP ASM으로 취약점 (Log4shell) 보유한 자산 전체 점검

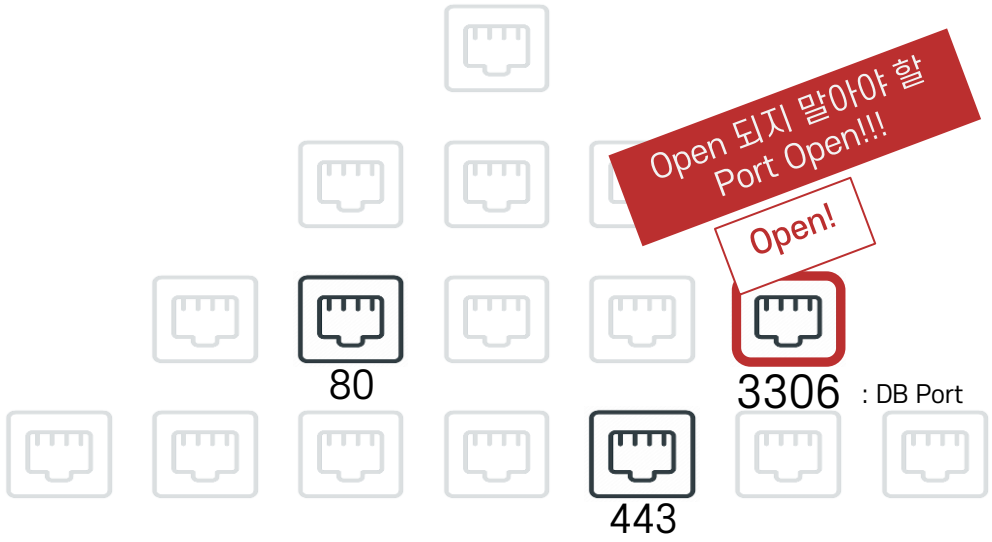
즉각 대응

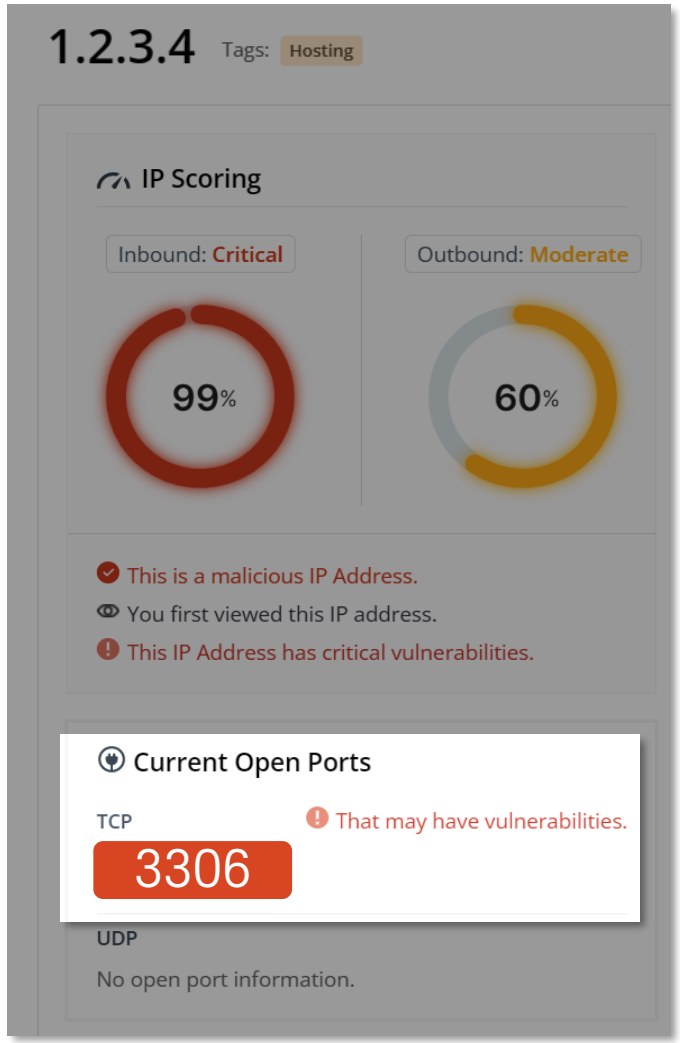
AI Spera 고객 전담 보안분석팀 대응프로세스에 따라
취약점 리포트 확인 및 즉각 대응 조치

상,하반기 대규모 취약점 점검 해제
Criminal IP ASM으로 자동 리포트 보고

위험한 포트가 오픈되는 경우

열려 있으면 안되는 포트가 실수로 오픈 되었거나, 오픈된 채로 방치된 경우
Criminal IP ASM이 실시간으로 모든 IP의 포트를 스캔하여 위협 리포트를 제공합니다.





3. Product Features Criminal IP ASM을 통한 공격표면관리 사례

위험한 포트가 열리는 경우

제조 업체 P

ERP 시스템을 사용하는 제조업체 'P'

ERP 장애 발생

ERP에 장애 발생

DB 문제 확인

내부 개발자가 확인 후 DB 문제 발견

외부 담당자 요청

휴가중인 DBA(데이터베이스 관리자,DataBase Administrator) 에 작업 요청

3306포트 개방

외부에서 DB 접속하기 위해 급하게 DB 포트 '3306' 외부 오픈

방화벽 시스템 에러

방화벽 관리 솔루션으로 DB포트 사용기한 설정 해 뒀으나, 시스템 에러로 3306포트 지속 개방

3306 포트 노출

3306포트 개방된 채로 방치

Criminal IP ASM

6개월 후 제조업체 P에 riminal IP ASM 도입

Criminal IP ASM

CIP ASM 도입

Criminal IP ASM을 통한 실시간 포트 및 운용자산 스캔

포트 감지

외부 접근 제한된 오픈 포트 및 자산 다수 발견

즉각 대응

ASM 자동 리포트로 확인 후 포트 폐쇄 및 즉각 대응 조치

Criminal IP ASM으로 실시간 운용 포트 및 자산 관제

새로운 자산이 추가되는 경우

외부에 노출된 채로 방치되어 있거나 파악하지 못하고 있는 자산을 Criminal IP ASM의 실시간 자산 스캐닝을 통해 파악할 수 있습니다.

New Assets (past 14 days)

Assets	Description	AS Name	Summary	Date
22.1.20.16	c	d	tt	2022-01-21 3:22:45
22.1.20.122	c	google	ttest	2022-01-21 3:22:02
22.1.20.13	c	TEST	ttest	2022-01-21 3:05:11
22.1.20.14	c	c	ttest	2022-01-21 3:05:07
22.1.20.12	c	b	ttest	2022-01-21 3:05:04

3. Product Features Criminal IP ASM을 통한 공격표면관리 사례

새로운 자산이 추가되는 경우

IT 서비스 기업 A

멀티 클라우드를 운용하는
IT 서비스 기업 'A'

멀티 클라우드 운용

주 클라우드 서비스로 Google Cloud, AWS, Azure 사용 중

랜딩페이지 생성

마케팅팀에서 신규 서비스 출시 기념 이벤트 랜딩페이지 생성

NEW
Alibaba Cloud
알리바바 클라우드 사용

마케팅 대행사 측 제안으로 알리바바 클라우드 사용

이벤트 운영

마케팅팀 개별 프로젝트로 보안팀 확인 없이 운영

개인정보 활용

개인정보 관련 API 호출하여 EDM 등 발송에 사용(단발성 이벤트 페이지로 사용됨)

이벤트 종료 후 도메인 방치

이벤트 종료 후 고객 정보 및 서버 방치

Criminal IP ASM
2년 후 IT 서비스 기업 A에 Criminal IP ASM 도입

Criminal IP ASM
CIP ASM 도입

Criminal IP ASM을 통한 사이버 자산 실시간 자동 탐지

NEW
미확인 자산 발견

알리바바 클라우드에 미확인 자산 발견

즉각 대응

ASM 자동 리포트로 확인 후 서버 삭제 및 즉각 대응 조치

미사용 중인 이벤트 페이지 폐쇄 및 Criminal IP ASM으로 클라우드 자산 관리 자동화

4

About AI Spera

- 글로벌 CTI 선도 기업 AI Spera의 미션
- 경영진
- Trusted by the best
- Products
- 언론 속 AI Spera
- 기술력과 경영으로 인정받은 기업

Cyber Threat Intelligence 전문기업

AI Spera

우리는 공격표면에 흩어져 있는 자산에 대한 가시성을 확보하고 관리하여
공격자의 위협에서 최대한 빠르게 안전해질 수 있는 방법을 계속해서 연구합니다.
그들(해커)이 더 많은 수단과 방법으로 공격할 수록 우리는 네트워크 전체에서
공격 가능한 틈을 찾아내기 위해 더 노력합니다.

4. About AI Spera 경영진

에이아이스페라 CEO 강병탁

온라인 게임보안,악성코드 분석전문가1세대

AI Spera는 주력 사업분야인 사이버 위협 인텔리전스 (Cyber Threat Intelligence CTI)를 이용하여 사이버상에서 수집 가능한 모든 위협 데이터셋으로 가치 높은 정보를 도출합니다.
IT 자산정보를 포함한 각종 보안위협과 공격자 및 공격수단, 악성코드 및 취약점 등 데이터를 인공지능 기반으로 가공하여 침해사고, 사이버범죄 대응 및 예방에 활용하고 있습니다.

| 주요경력

2021. – 2021. : 고려대학교 정보보호대학원 겸임교수
2018. – 2020. : 고려대학교 정보보호대학원 산학협력중점교수
2016. – 2017. : 네오플 인프라기술실 총괄실장
2012. – 2016. : 넥슨 아메리카 Infosec Team 팀장
2007. – 2012. : 넥슨 코리아 게임보안팀 팀장
2009. – 2010. : Microsoft MVP Developer Security
2004. – 2007. : 잉카인터넷 엔진개발팀 Lead Programmer

| 주요저서

- 2010-2012 월간 마이크로소프트 : 3년간 해킹/보안 연재
- 리버스 엔지니어링 바이블 저자
- 인프라 보안 저자
- 대학교와 기관 등에서 해킹/보안을 주제로 한 초청강연 수행

주요경력 |

2021. – 정보보호의 날 표창 수여
2018. – 현재 : 고려대학교 사이버보안대학원(구, 정보보호대학원) 교수
2017. – 현재 : 카카오 프라이버시정책 자문위원회
2015. – 2018. : 삼성전자 소프트웨어/보안 부문 자문단
2015. – 현재 : KISA ISMS 인증위원회 위원
2012. – 현재 : 한국정보보호학회 이사
2004. – 2010. : 엔씨소프트 정보보안실장
1999. – 2004. : A3 Security 창업자, 대표

주요실적 |

- FDS, 온라인게임 봇 및 작업장 탐지, CTI개발, 악성코드, 관련 프로젝트 수행 경험 다수
- NDSS, WWW, IEEE TIFS 등 국제 최고수준 컨퍼런스 및 논문지 게재 실적 다수
- 정보보호 R&D 데이터챌린지 주관 (안드로이드악성앱, 자동차용 침입탐지 등)

에이아이스페라 Co-Founder 김휘강

해커 출신 1호 교수

AI Spera 의 미션은 끊임없이 진화하는 사이버 위협 및 사기 범죄로부터 고객을 보호하는 것 입니다.
AI Spera 는 data-driven security 의 최신 기술을 이용하여 이러한 사이버 위협들로부터 고객을 보호할 수 있도록 최선을 다하겠습니다.

국내외 최고의 기업 및 기관이 신뢰합니다.

간편결제솔루션, 보안 책임자

"AI Spera의 솔루션은 다른 CTI 검색엔진이 가지지 못한 넓은 범위와 깊이의 데이터를 갖고 있습니다."

글로벌 게임사, 고객 프로파일 개발자

"데일리 자동탐지, 리포트 및 모니터링은 서비스 유저와 비즈니스의 손실을 최소화합니다. 간단하고 단순한 인텔리전스 자산 탐지 툴입니다."

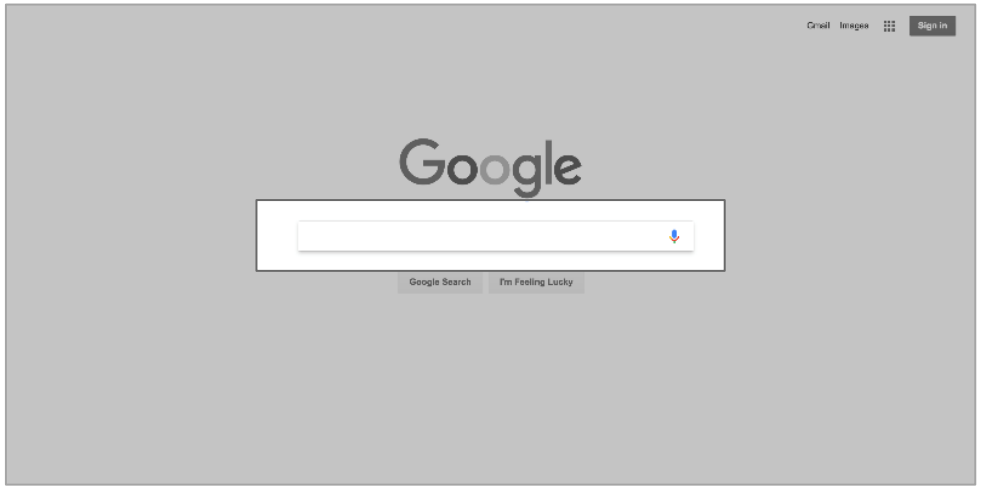
교육 및 연구, 연구원

"정보보안 교육 연구 분야에서 간단히 이용할 수 있고, 정상적이지 않은 자산 탐지에 도움이 되는 데이터를 제공해 줍니다. API는 전부터 사용하던 시스템에 연동하기 쉽습니다. 어떤 서비스보다도 속도가 빠릅니다."

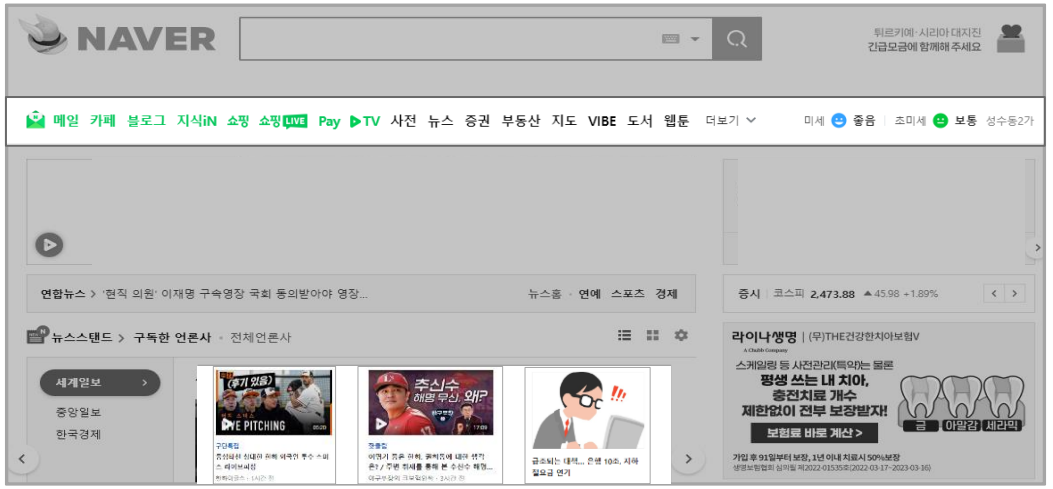
Products

위협 인텔리전스 검색엔진, Criminal IP

Criminal IP는 사이버보안 분야의 검색엔진 필요성으로부터 시작되었습니다.



이 세상의 모든 정보를 찾을 수 있는 '구글'



뉴스, 포스트 등 사용자가 필요한 정보를 제공하는 '네이버'

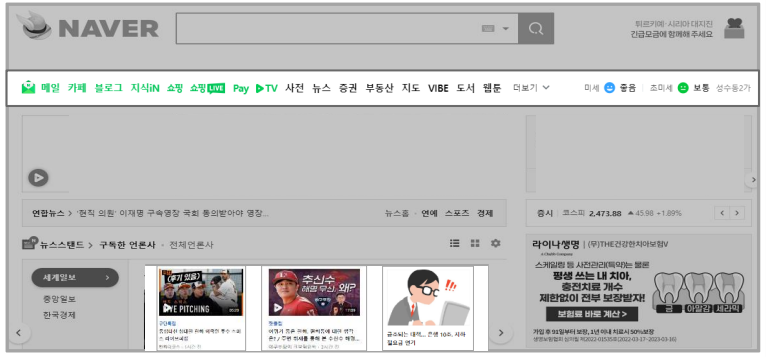
사이버보안 분야에서,

모든 정보를 찾을 수 있고, 사용자가 원하는 정보를 제공하는 검색엔진은 왜 없을까?

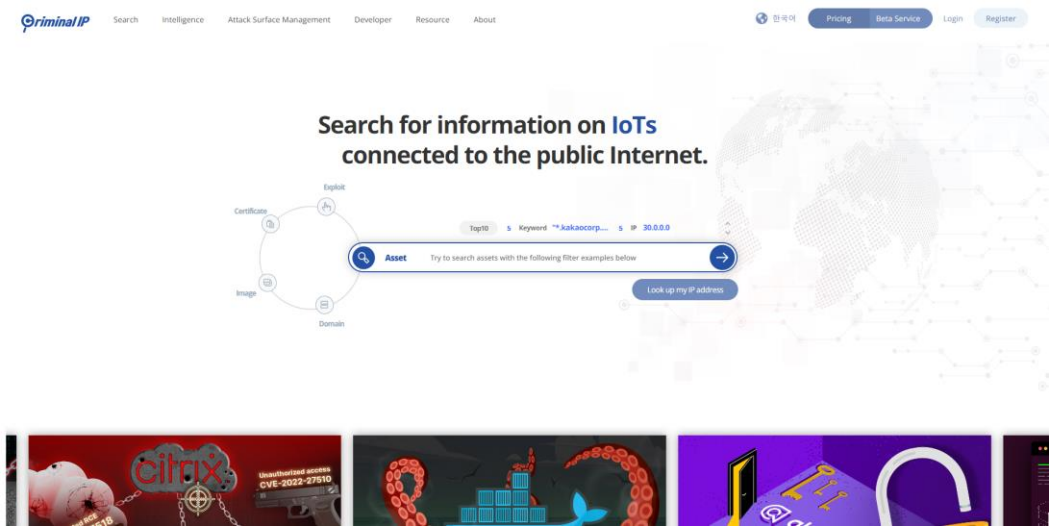
Products

위협 인텔리전스 검색엔진, Criminal IP

Criminal IP는 IP주소 기반 모든 정보와 사용자가 원하는 정보를 제공하는 사이버보안 분야의 검색엔진입니다.



IP주소 기반 모든 정보와 사용자가 원하는 정보를 제공하는
대한민국 최초 위협 인텔리전스 검색엔진 'Criminal IP' 탄생



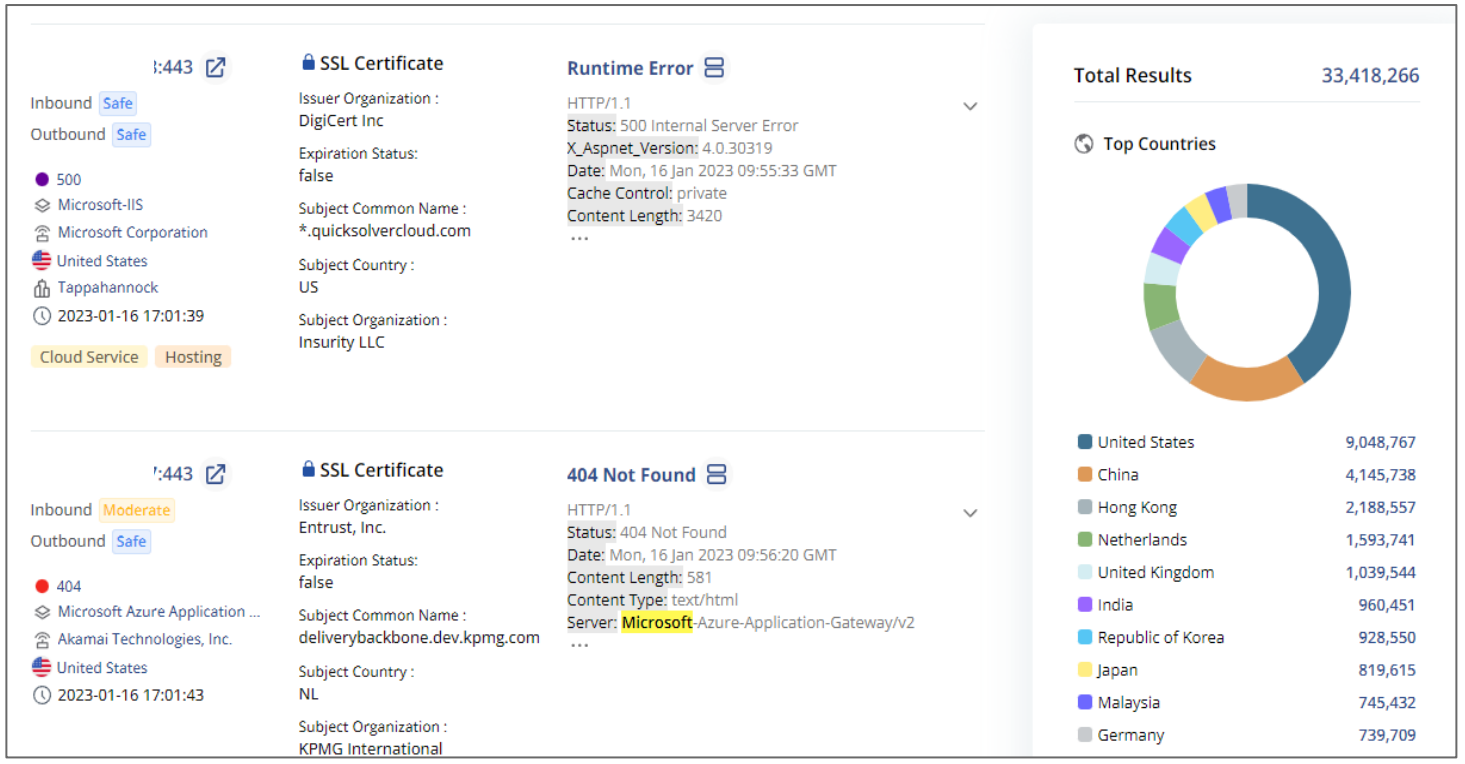
Products

위협 인텔리전스 검색엔진, Criminal IP

Criminal IP는 IP주소 기반 모든 정보와 사용자가 원하는 정보를 제공하는 사이버보안 분야의 검색엔진입니다.

'Microsoft' 검색 결과(Google)

'Microsoft' 검색 결과(Criminal IP)

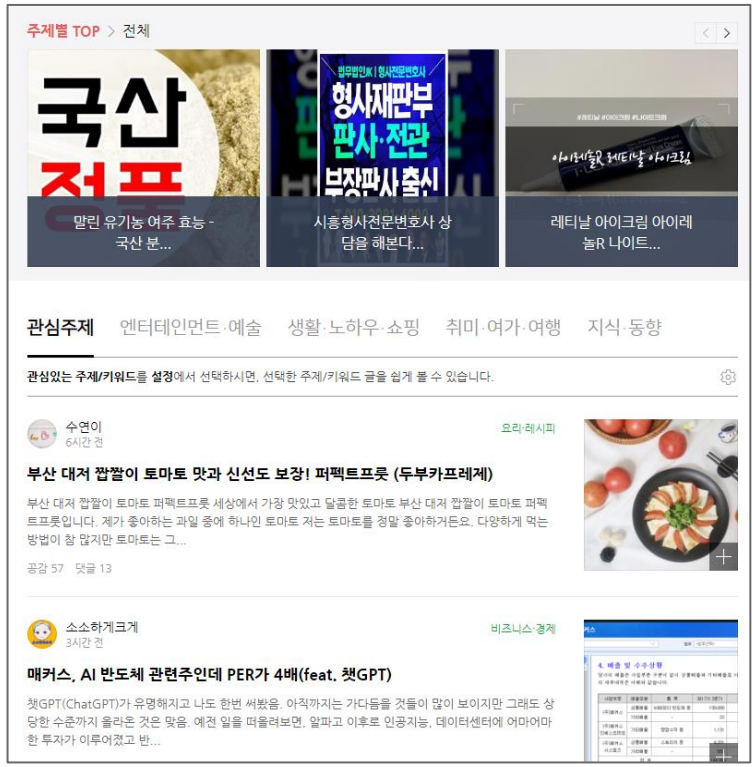


Products

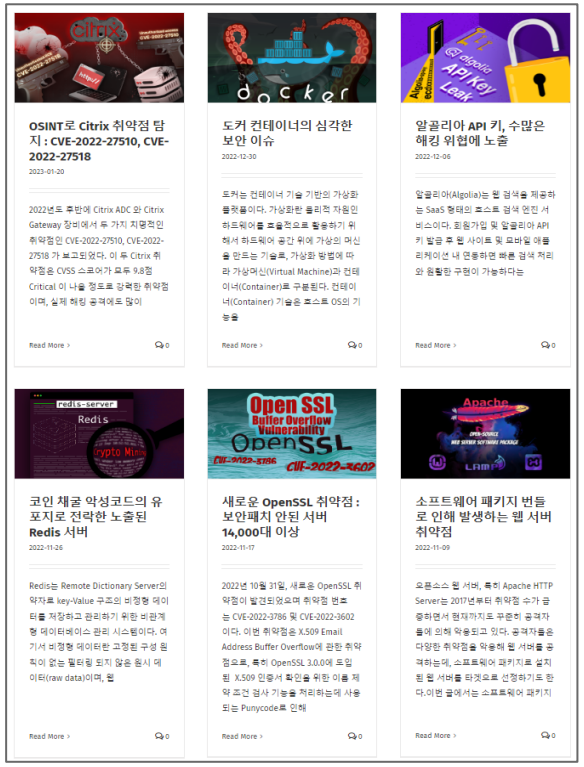
위협 인텔리전스 검색엔진, Criminal IP

Criminal IP는 IP주소 기반 모든 정보와 사용자가 원하는 정보를 제공하는 사이버보안 분야의 검색엔진입니다.

'블로그' 메뉴 선택 후 화면 (Naver)



'블로그' 메뉴 선택 후 화면(Criminal IP)



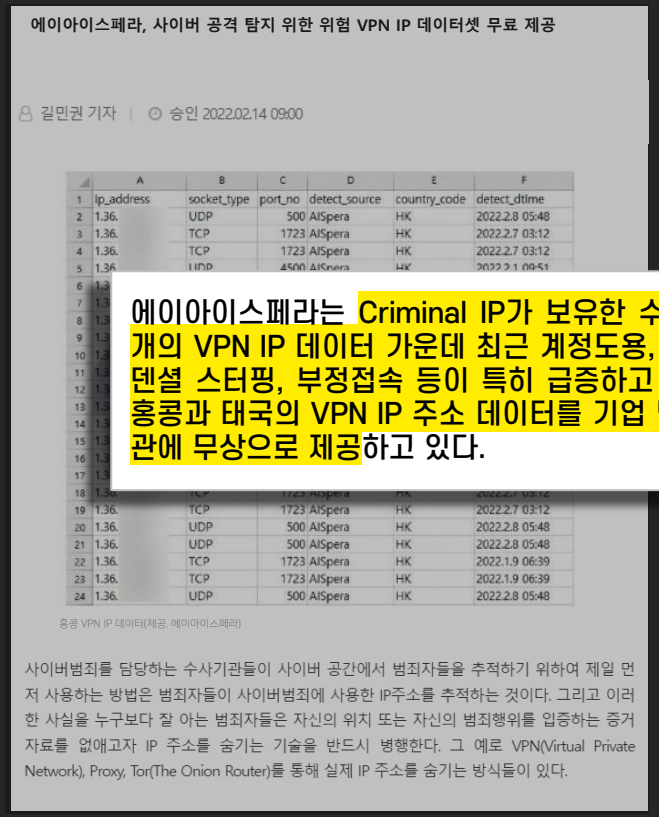
Products

사이버 위협 인텔리전스와 AI/머신러닝을 적용한 솔루션을 제공합니다.
AI Spera의 솔루션은 개인부터 기업, 국가의 다양한 분야에서 활용되고 있습니다.

Criminal IP

ASM	FDS	Privacy	Brand
공격 표면 관리 인텔리전스	인텔리전스 기반 이상유저감지	고객 개인정보 유출 방지	브랜드 침해 사이트 자동 탐지
• 노출 IT 자산 탐지 • 자동 취약점 탐지 • 구글 OSINT 탐지 • 모니터링 대시보드 • 자산 위협 인텔리전스 분석	• 이상 유저 IP 인텔리전스 확인 • 이상 유저 실시간 모니터링 • 이상 유저 서비스 제한 및 차단 활용	• 악성 URL 탐지 • 개방형 WiFi 해킹 탐지 • IoT 기기 정보 유출 탐지	• 불법 게임 서버 탐지 • 불법 스트리밍 사이트 탐지 • 위조상품 판매 사이트 탐지 • 브랜드 사칭 피싱 사이트 탐지
타겟 고객			
인프라 보안 관계자 보안 점검 관련 부서 IT 자산 부서 보안관제 관련 부서	Fintech 부서 관계자 부정 행위 탐지 부서 FDS 인증 개발, 플랫폼 팀 Fraud 부서 관계자	B2C 모바일 앱 서비스 부서 Fintech 부서 관계자 금융권 기업 관계자	위험 관리 부서 감사 부서 보안 부서 대회 협력 부서

언론에 소개된 AI Spera



에이아이스페라, 사이버 공격 탐지 위한 위험 VPN IP 데이터셋 무료 제공

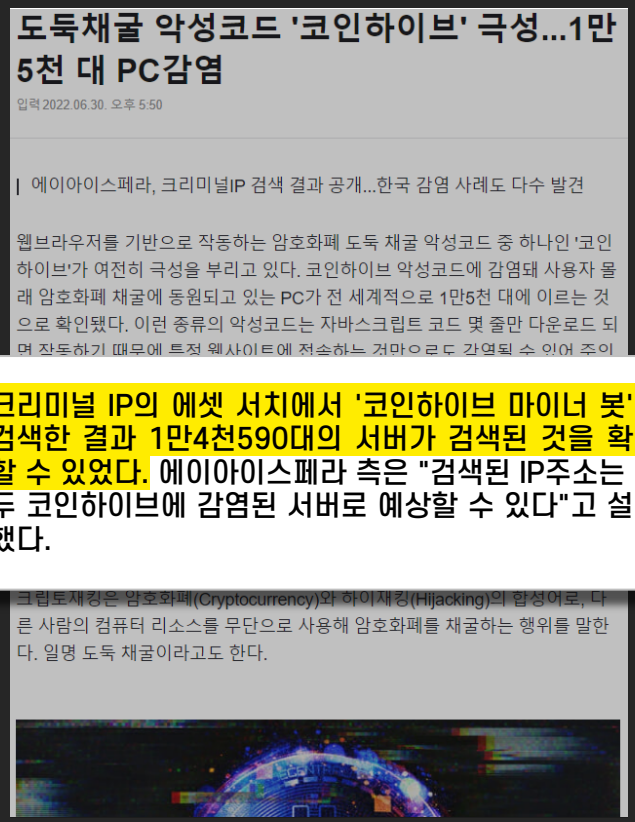
길민권 기자 | 승인 2022.02.14 09:00

	A	B	C	D	E	F
1	ip_address	socket_type	port_no	detect_source	country_code	detect_dtime
2	1.36.	UDP	500	AISpera	HK	2022.2.8 05:48
3	1.36.	TCP	1723	AISpera	HK	2022.2.7 03:12
4	1.36.	TCP	1723	AISpera	HK	2022.2.7 03:12
5	1.36.	UDP	4500	AISpera	HK	2022.2.1 09:51
19	1.36.	TCP	1723	AISpera	HK	2022.2.7 03:12
20	1.36.	UDP	500	AISpera	HK	2022.2.8 05:48
21	1.36.	UDP	500	AISpera	HK	2022.2.8 05:48
22	1.36.	TCP	1723	AISpera	HK	2022.1.9 06:39
23	1.36.	TCP	1723	AISpera	HK	2022.1.9 06:39
24	1.36.	UDP	500	AISpera	HK	2022.2.8 05:48

중공 VPN IP 데이터(제공: 에이아이스페라)

사이버범죄를 담당하는 수사기관들이 사이버 공간에서 범죄자들을 추적하기 위하여 제일 먼저 사용하는 방법은 범죄자들이 사이버범죄에 사용한 IP주소를 추적하는 것이다. 그리고 이러한 사실을 누구보다 잘 아는 범죄자들은 자신의 위치 또는 자신의 범죄행위를 입증하는 증거자료를 없애고자 IP 주소를 숨기는 기술을 반드시 병행한다. 그 예로 VPN(Virtual Private Network), Proxy, Tor(The Onion Router)를 통해 실제 IP 주소를 숨기는 방식들이 있다.

에이아이스페라는 Criminal IP가 보유한 수십억 개의 VPN IP 데이터 가운데 최근 계정도용, 크리덴셜 스터핑, 부정접속 등이 특히 급증하고 있는 홍콩과 태국의 VPN IP 주소 데이터를 기업 및 기관에 무상으로 제공하고 있다.



도둑채굴 악성코드 '코인하이브' 극성...1만5천 대 PC감염

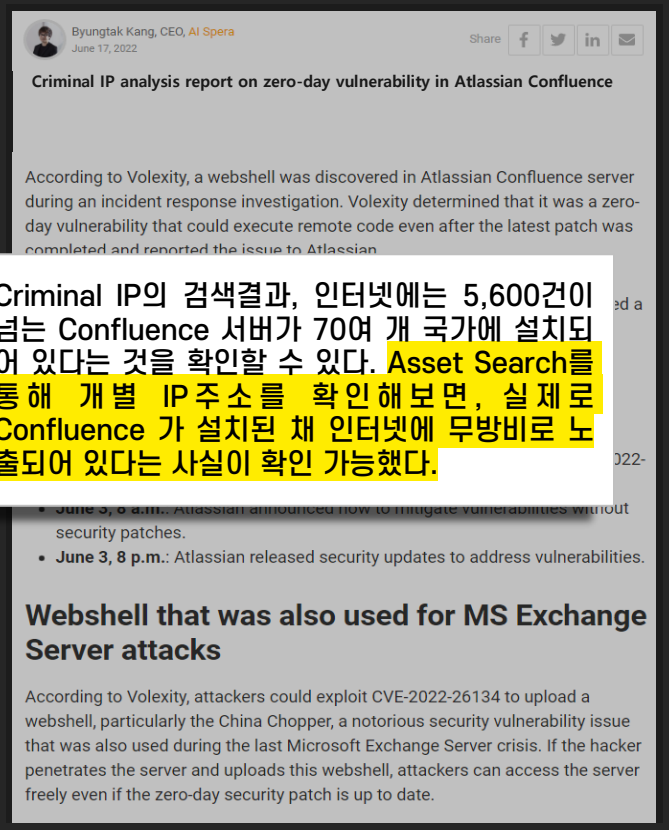
입력 2022.06.30. 오후 5:50

| 에이아이스페라, 크리미널IP 검색 결과 공개...한국 감염 사례도 다수 발견

웹브라우저를 기반으로 작동하는 암호화폐 도둑 채굴 악성코드 중 하나인 '코인하이브'가 여전히 극성을 부리고 있다. 코인하이브 악성코드에 감염돼 사용자 몰래 암호화폐 채굴에 동원되고 있는 PC가 전 세계적으로 1만5천 대에 이르는 것으로 확인됐다. 이런 종류의 악성코드는 자바스크립트 코드 몇 줄만 다운로드 되면 작동하기 때문에 특정 웹사이트에 전송하는 경망으로도 감염될 수 있어 주의

크립토재킹은 암호화폐(Cryptocurrency)와 하이재킹(Hijacking)의 합성어로, 다른 사람의 컴퓨터 리소스를 무단으로 사용해 암호화폐를 채굴하는 행위를 말한다. 일명 도둑 채굴이라고도 한다.

크리미널 IP의 에셋 서치에서 '코인하이브 마이너 봇'을 검색한 결과 1만4천590대의 서버가 검색된 것을 확인할 수 있었다. 에이아이스페라 측은 "검색된 IP주소는 모두 코인하이브에 감염된 서버로 예상할 수 있다"고 설명했다.



Byungtak Kang, CEO, AI Spera
June 17, 2022

Share

Criminal IP analysis report on zero-day vulnerability in Atlassian Confluence

According to Volexity, a webshell was discovered in Atlassian Confluence server during an incident response investigation. Volexity determined that it was a zero-day vulnerability that could execute remote code even after the latest patch was completed and reported the issue to Atlassian.

- June 3, 8 a.m.: Atlassian announced how to mitigate vulnerabilities without security patches.
- June 3, 8 p.m.: Atlassian released security updates to address vulnerabilities.

Webshell that was also used for MS Exchange Server attacks

According to Volexity, attackers could exploit CVE-2022-26134 to upload a webshell, particularly the China Chopper, a notorious security vulnerability issue that was also used during the last Microsoft Exchange Server crisis. If the hacker penetrates the server and uploads this webshell, attackers can access the server freely even if the zero-day security patch is up to date.

Criminal IP의 검색결과, 인터넷에는 5,600건이 넘는 Confluence 서버가 70여 개 국가에 설치되어 있다는 것을 확인할 수 있다. Asset Search를 통해 개별 IP주소를 확인해보면, 실제로 Confluence 가 설치된 채 인터넷에 무방비로 노출되어 있다는 사실이 확인 가능했다.

에이아이스페라, 사이버 공격 탐지 위한 위험 VPN IP 데이터셋 무료 제공, <데일리시큐>, 2022.02.14

도둑채굴 악성코드 '코인하이브' 극성...1만5천 대 PC감염, <ZDNet Korea>, 2022.06.30

Criminal IP analysis report on zero-day vulnerability in Atlassian Confluence, <HELPNET SECURITY> ,2022.06.17

기술력과 회사 경영에 관련된 다수의 인증을 획득하였습니다.

- 한국산업기술진흥협회 –기업부설연구소 인증
- 여성가족부 - 가족친화 인증
- 국제표준인증원 - ISO 9001 인증
- 한국정보통신기술협회 - GS인증 1등급(Criminal IP)
- 한국정보통신기술협회 – GS인증 1등급(민심)
- 산업통상자원부장관 – NEP 인증(Criminal IP)
- 조달청-해외조달시장 진출 유망기업(G-PASS기업) 지정
- 과학기술정보통신부 – 우수 기업부설연구소 지정
- 특허청 - 직무발명보상 재인증
- 특허청 - 특허 등록 “인공지능 기반 악성 도메인 분류 방법 및 프로그램”
- 특허청 - 특허 등록 “P2P 네트워크에서의 불법콘텐츠의 배포와 관련된 정보를 제공하는 장치, 방법 및 프로그램”
- 특허청 – 특허 등록 “선불폰 검증 장치, 방법 및 프로그램”
- 특허청 - 특허 등록 "사기피해 정보 제공 방법 및 프로그램“
- 특허청 - 특허 등록 "악성 DNS 서버 탐지 장치 및 그 제어방법“
- 특허청 - 특허 등록 "보안 관제 장치 및 그 제어방법“
- 특허청 - 특허 등록 "IP 기반 보안 관제 방법 및 그 시스템“
- 특허청 – 특허 등록 "사설 서버 탐지 장치 및 그 제어방법"

Thank you

Address

서울시 성동구 연무장5가길 7, 7층

Tel

02-6419-1090

E-mail

support@aispera.com

Website

https://www.criminalip.io/ko