Criminal IP ASM

Threat Intelligence-based
Automated Attack Surface Management Solution

Agenda

1
ASM
(Attack Surface Management)

- What is ASM?
- Hacker's Attack Process
- Differences
- Why ASM Matters

2
Criminal IP ASM

- Criminal IP ASM Features
- Features and Product UI
- Integration with Criminal IP

3
Application

- Adopting ASM
- ASM Use Cases

1

ASM (Attack Surface Management)

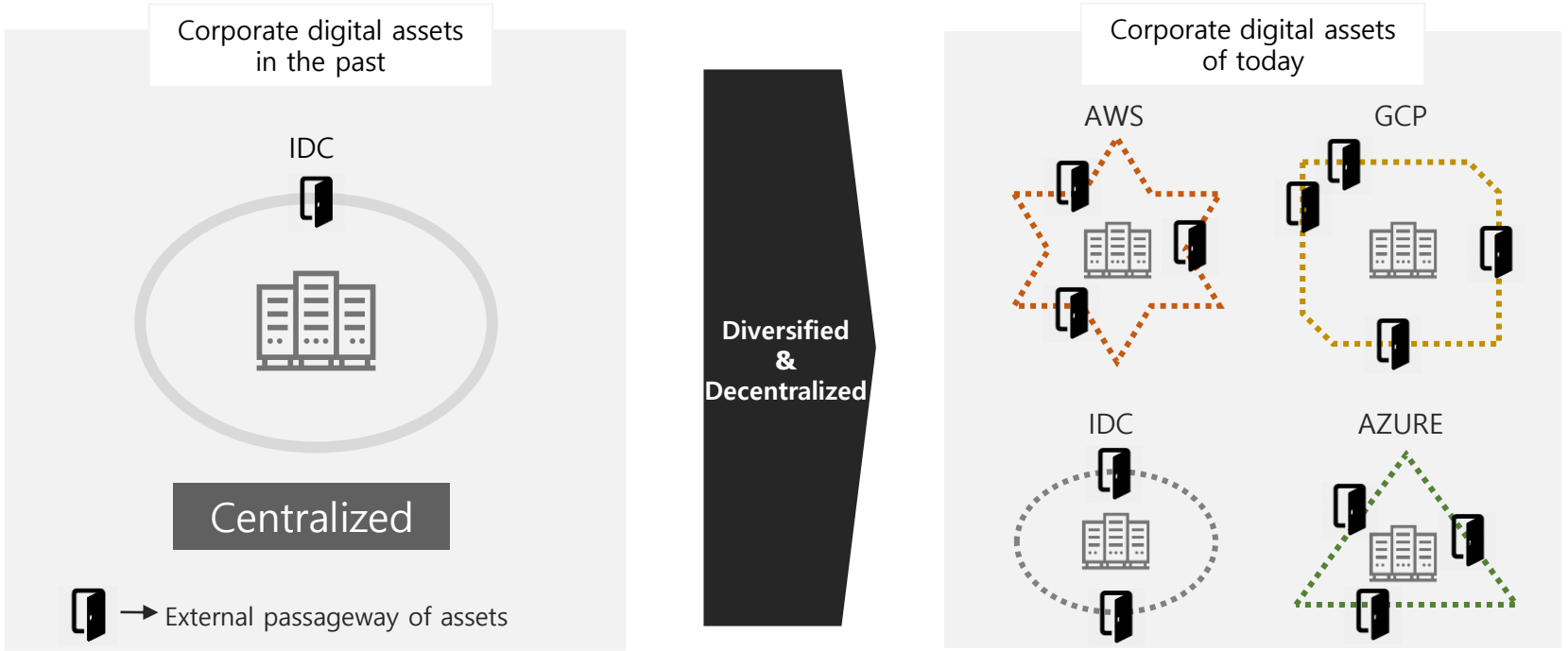
- What is ASM?
- Hacker's Attack Process
- Differences
- Why ASM Matters

What is Attack Surface Management (ASM)?

Businesses and organizations have numerous network devices, databases, servers, applications, and domains, and all of these IT assets are operated by IP addresses and ports.

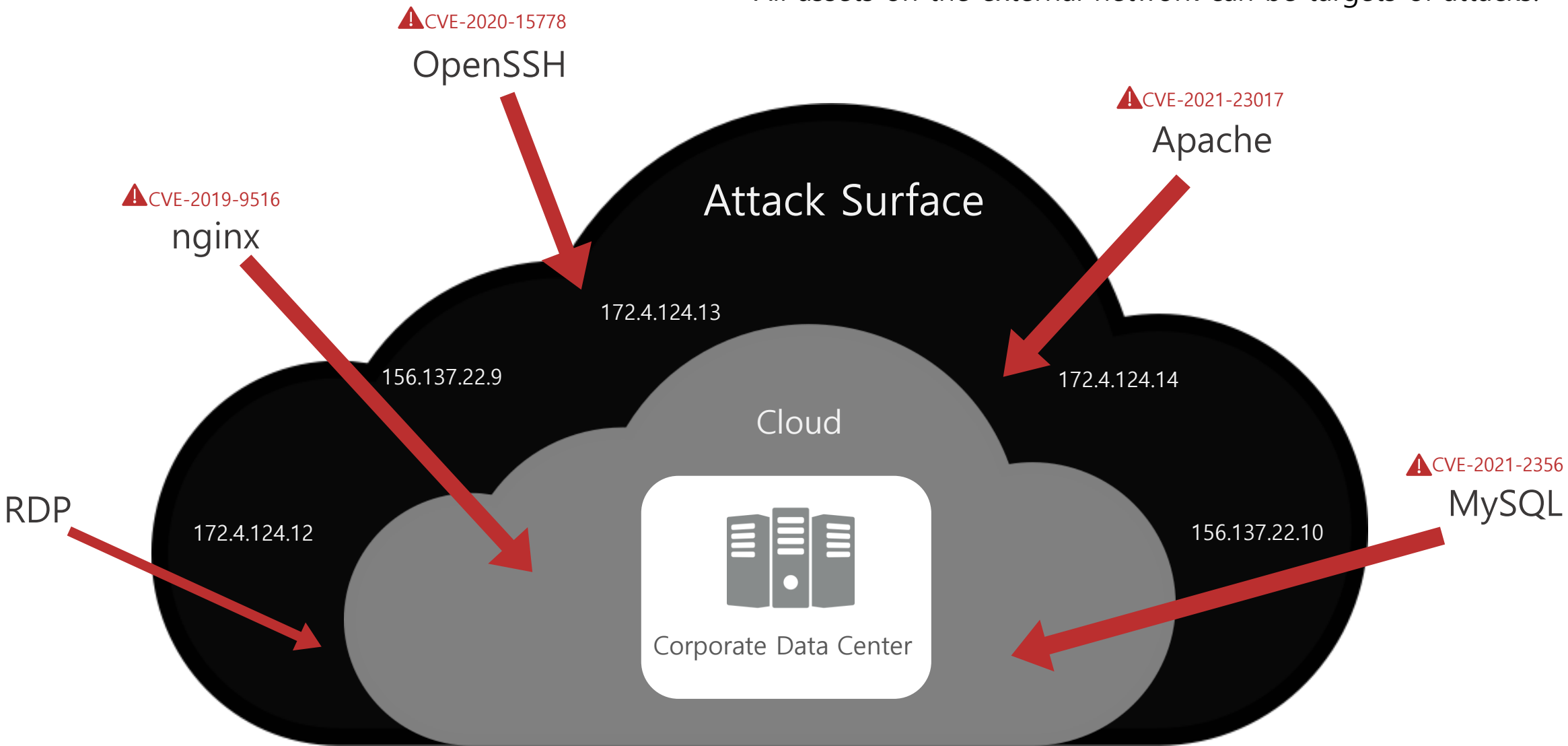
Attack Surface Management refers to the proactive detection and management of attack vectors such as open ports, server vulnerabilities, similar domains, phishing, and domains distribu ting malicious code.

With the rapid change in corporates' IT environment,
attack surfaces are varying and broadening in a bigger scale.



Attack Surface

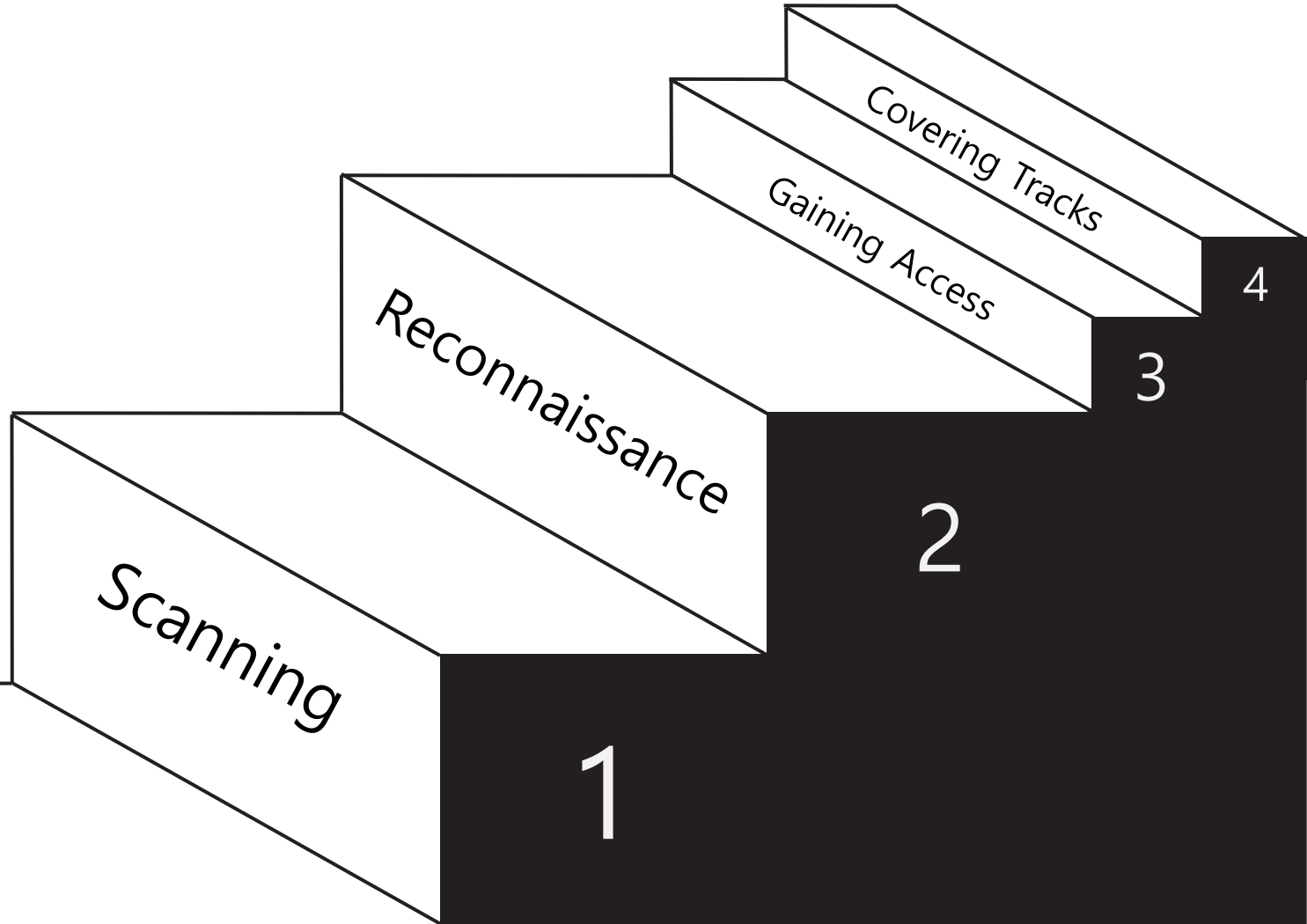
All assets on the external network can be targets of attacks.



Hacker's Attack Process

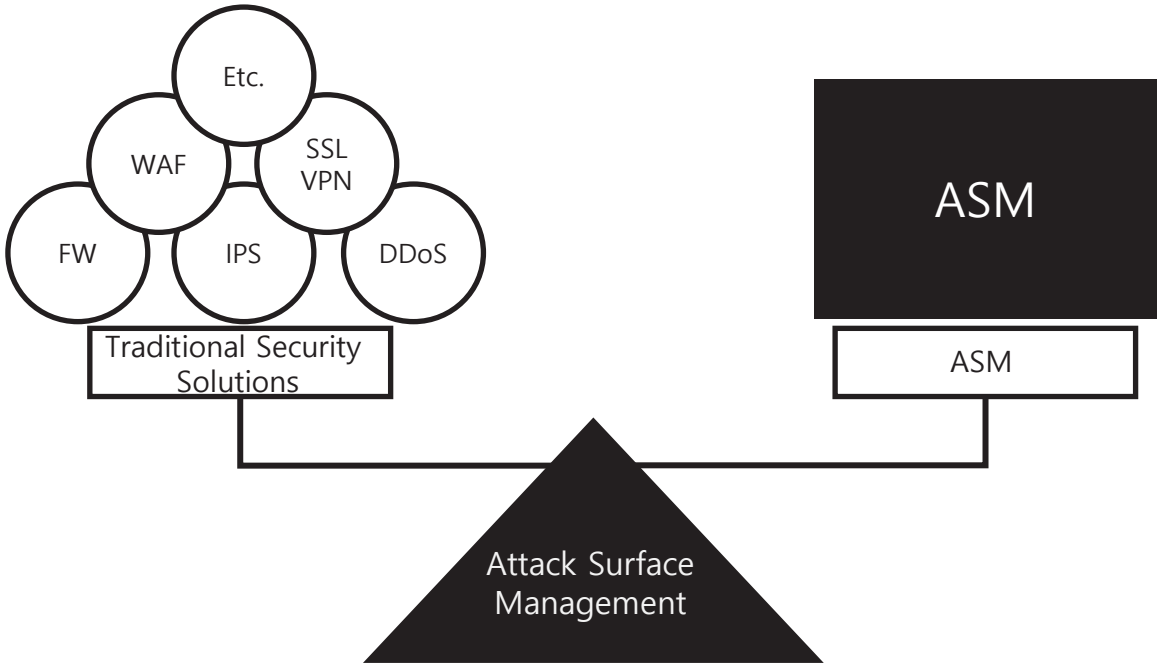
Hackers put a lot of time and effort into collecting information on the target.

Therefore, it is essential to find the exact exposure point of the attack surface.



Differences between Traditional Security Methods and ASM

Traditional security devices and solutions primarily focus on taking action after an attack.
ASM prevents the attack by identifying and managing the exposure of attacks in advance.



Complicated task
Multiple potential failures

Traditional Security Solutions

- Need to install equipment or Software
- Integration and customization
- Passive policies
- Ongoing updates and management
- Multiple failure points
- Work suspended upon failure occurrence

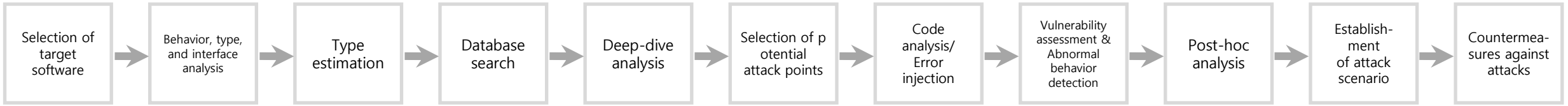
Simple task
No potential failure

ASM
(Attack Surface Management)

SaaS-based service enables automated operation without cumbersome work

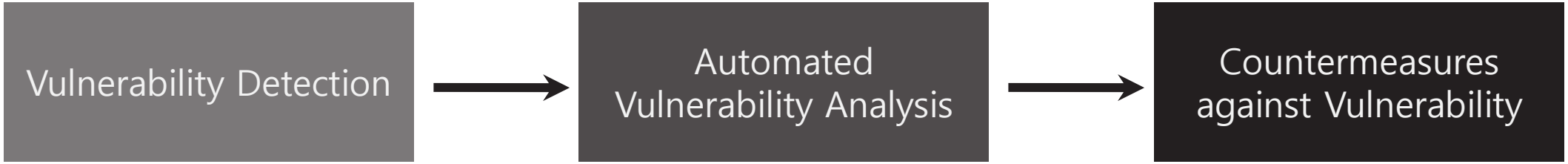
1. ASM Differences

Vulnerability detection process of traditional security solutions



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

Vulnerability detection process of ASM System



Effects of Introducing ASM

Decreased Probability of Penetrating Attack Surface

Reduced Cost&Resources

Increased Work Efficiency

Improved Attack Surface Security

The importance of Attack Surface Management, the major talking point of the information security market

Gartner®

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

"ASM is a new solution that helps organizations identify risks associated with internet-connected assets and systems that they may be unaware of. More than one-third of the recent successful attacks against enterprises originate from externally connected assets. That's why ASM will become an essential task for CIOs and CISOs."

FORRESTER®

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

"Some ASM tools discovered several hundred percent more cloud assets than organizations thought they were using, and on average, attack surface management tools initially discover 30% more cloud assets than security teams know they have."

Managing attack surface and vulnerabilities is now a MUST

As corporates accommodate new assets and workflow more broadly and deeply, adopting ASM will become a MUST.

- ✓ Gartner said, "Strengthening digital abilities of digital workplace employees to create an engaging, intuitive work environment."
- ✓ With the trend of going digital, technology to integrate AI, cloud, and IoT is drawing corporates' investment and attention
- ✓ But with digital workplaces using ICT technology, they have become the new target for hackers' attack
- ✓ Increased user convenience means increased threats of being hacked
- ✓ COVID-19 pandemic and working-from-home trend increased corporate attack surfaces
- ✓ Corporates are putting more emphasis on cloud-based applications, devices, and human security elements
- ✓ Demand for expanded vulnerabilities management to deal with risks in a decentralized digital work environment is more vital than ever
- ✓ As organizations get used to operating the new business model, they will prefer vulnerabilities management for new platforms and applications

Popularization of working from home

- Covid-19 pandemic and increase in working from home expanded corporate attack surfaces
- Increased Zero-day vulnerabilities targeting remote SW, including VPN
- 82% of corporates will support working from home after the end of Covid-19

Transition to the digital workplace

- With the trend of going digital, the cloud working environment draws corporates' investment and attention
- Digital workplace with ICT technology has become a new target for hackers' attack
- Increased user convenience, increased threats of being hacked

Industry 4.0, increase in IoT devices

- Business innovation utilizing IoT devices
- For the past 5 years, approximately 20.5 billion devices were connected

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

2

Criminal IP ASM

- Criminal IP ASM Features
- Features and Product UI
- Integration with Criminal IP
- Differences from Other ASMs

Automatic detection of client assets

Criminal IP ASM conducts an internet-wide scan for known and unknown client assets on IP addresses and open ports.

IP — 4.2 billion IP address info

\+

Port — Scan Port data from all over the world

\+

Domain — Over 300 million domain address data

Cloud-based web interface

Criminal IP ASM is a SaaS-type ASM product that does not require installment or deploying hardware or software on customer servers.

After registering your account, you can use your network's PC, tablet, or mobile device to launch your ASM solution rapidly and readily through an easy-to-use web interface.

Installed On-Premises

Maintenance Cost

- Initial installation of product and building internal server
- System update patch, upgrade
- Internal server and network failure issue management
- Hardware maintenance and upgrade
- Network maintenance and upgrade
- Security maintenance and upgrade
- Database maintenance and upgrade

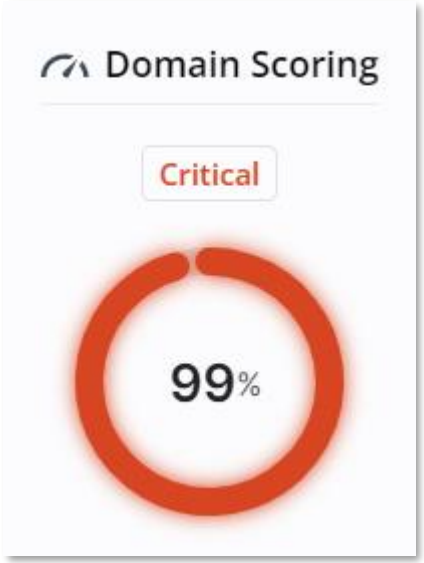
Cloud SaaS

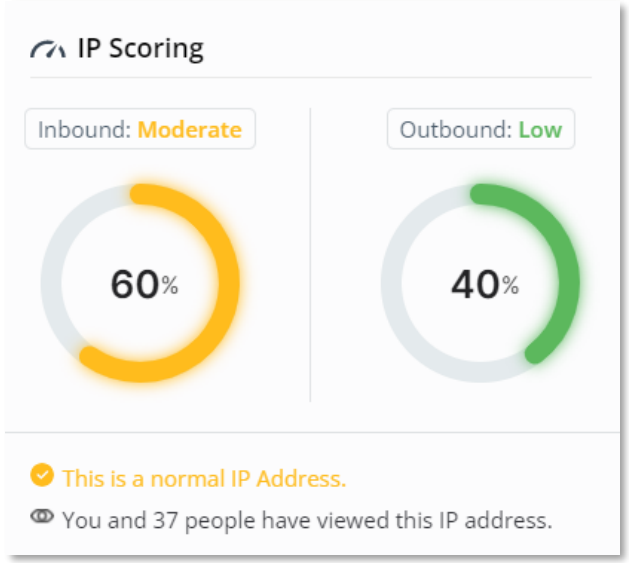
Maintenance Cost

- ☑ Annual purchase
- ☑ User Guide and Training
- ☑ Customization

Asset and vulnerability risk scoring

Our algorithm using AI machine-learning provides real-time detection to visualize the assets with five levels of risk scoring. Cybersecurity managers can prioritize the risks based on the visualized scoring to respond quickly and precisely.

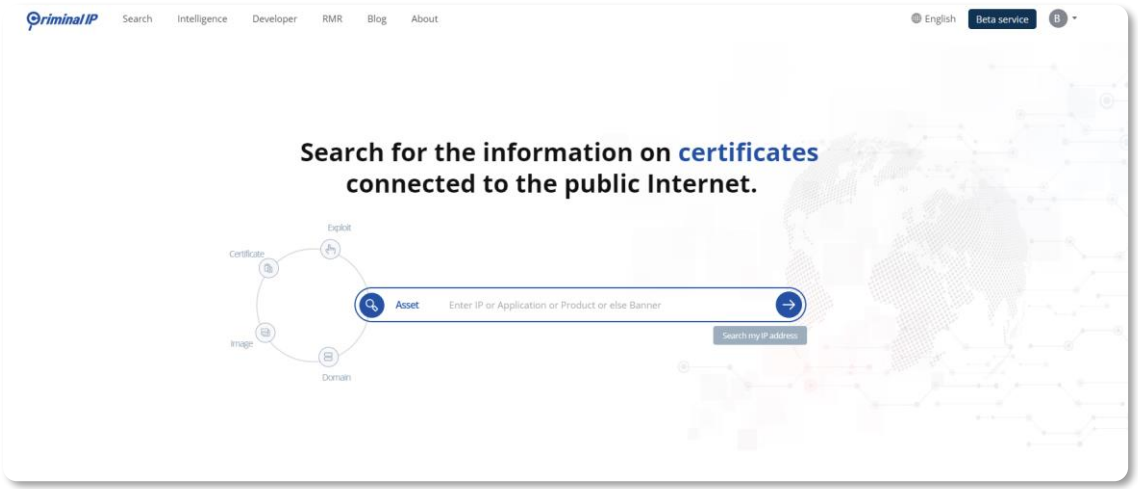




	IP/Asset	Domain/Certificate
Critical	Network/assets have been attacked or are under attack	Domain/certificates are falsified or contain malicious links
Dangerous	Network/assets are exposed to attack surface, vulnerable to attacks	The domain is falsified or a certificate has expired/ leaked, requiring action
Moderate	Network/assets maintain a moderate security level	Domain/certificates maintain a moderate security level
Low	Network/assets are not exposed externally and are kept safe	The domain is not falsified or a certificate is free from leakage or expiration, and is kept safe
Safe		

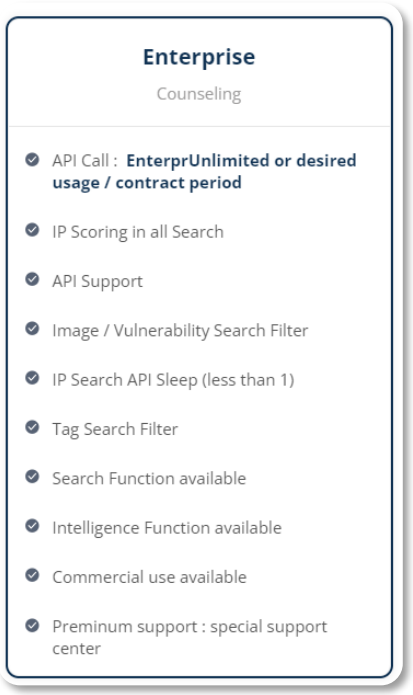
Free integration with CTI search engine

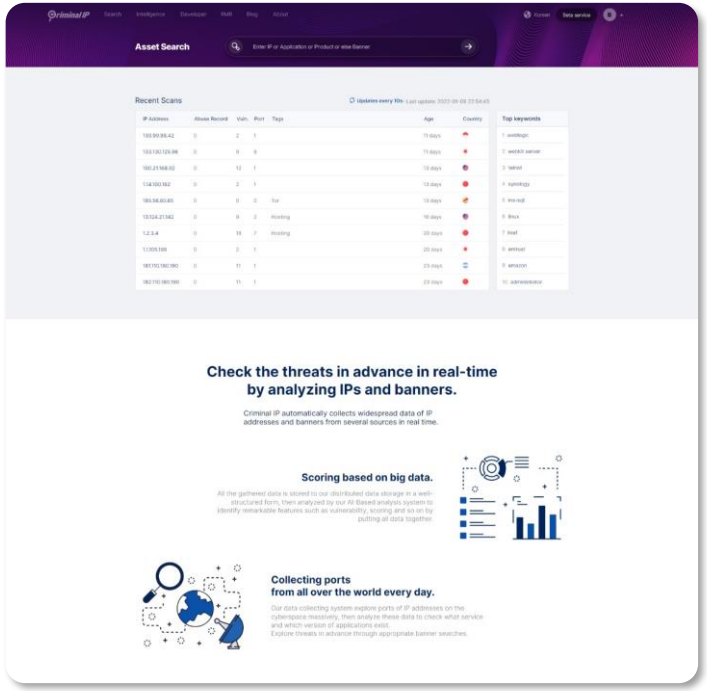
Criminal IP, a Cyber Threat Intelligence search engine, provides a detailed search of corporate's asset data detected by ASM.



Major Features of Criminal IP Search Engine

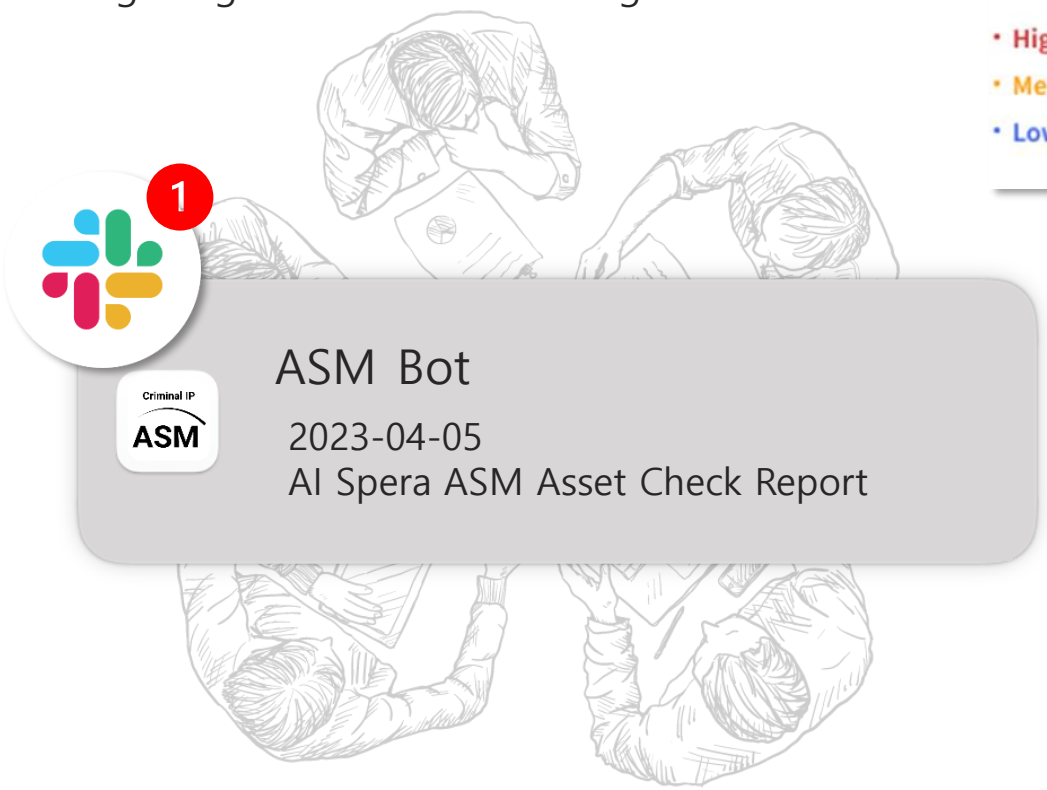
Search	Intelligence
Asset Search	Banner Explorer
Domain Search	Vulnerability
Image Search	Statistics
Certificate Search	Element Analysis
Exploit Search	Map

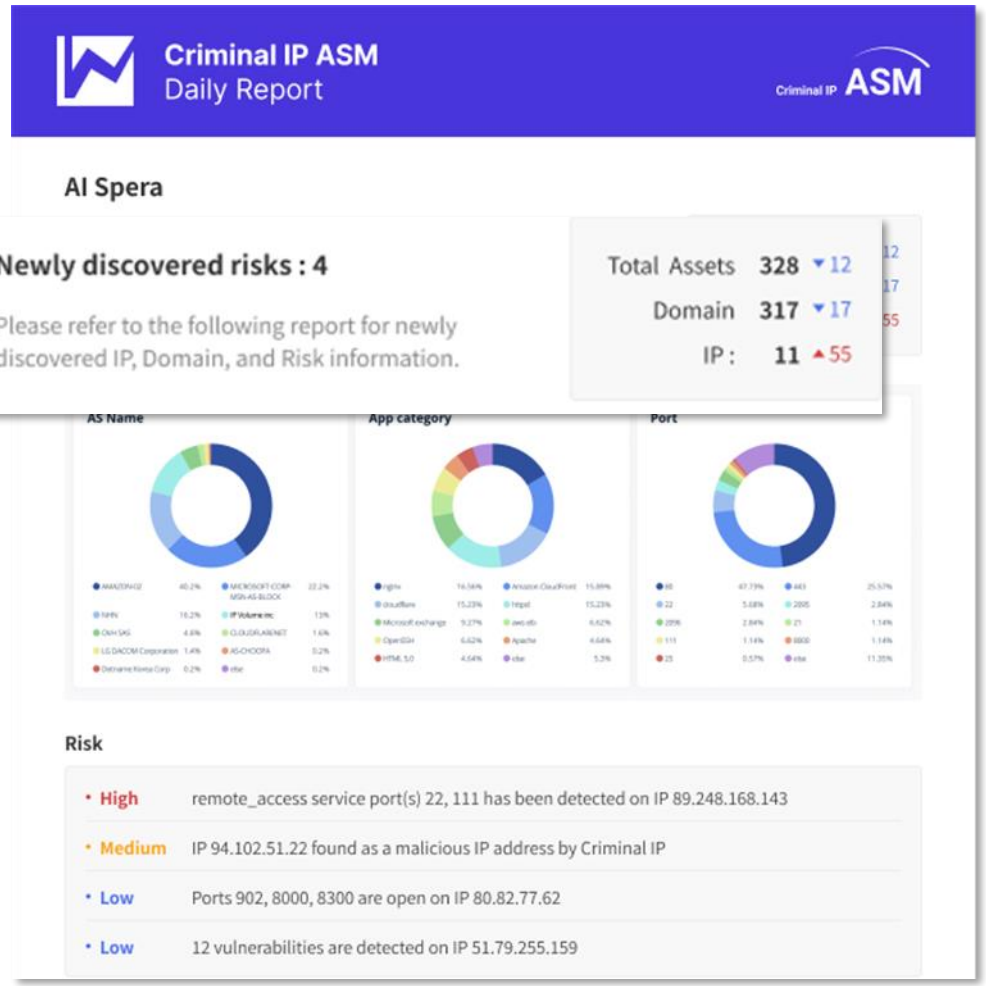




Daily Analysis Report & Messenger Integration

Daily reports on new assets and vulnerabilities are automatically sent via email, and we provide an alarm service that enables quick response by integrating with business messengers such as Slack.





Overview of Criminal IP ASM

Criminal IP ASM automatically monitors and generates a report on assets exposed to the attack surface.
All IT assets are thoroughly detected globally, with a streamlined introduction procedure requiring registration of only one primary domain.

New Assets
Automatically detects assets that have been recently added or changed

IP Assets
Scans open ports of detected IP addresses

Domain
Shows the associated domains and subdomains of the detected IP address

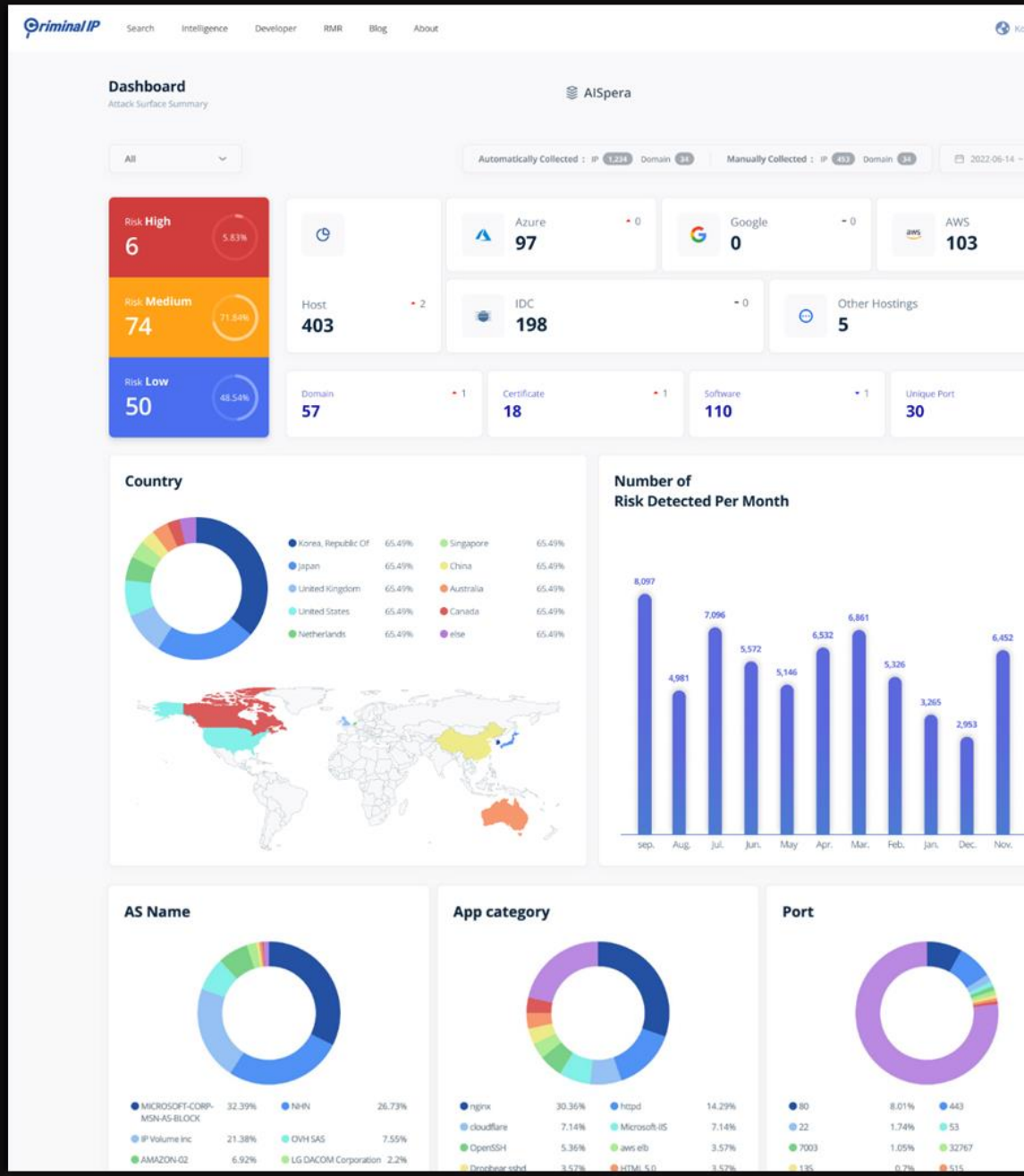
Certificate
Displays information about the certificate applied to the domain

Risk
Alerts users about exploitable vulnerabilities of assets such as IP, domain, certificate, and application

Intelligence Search Result
Gets details about the exposure status and vulnerabilities on the attack surface

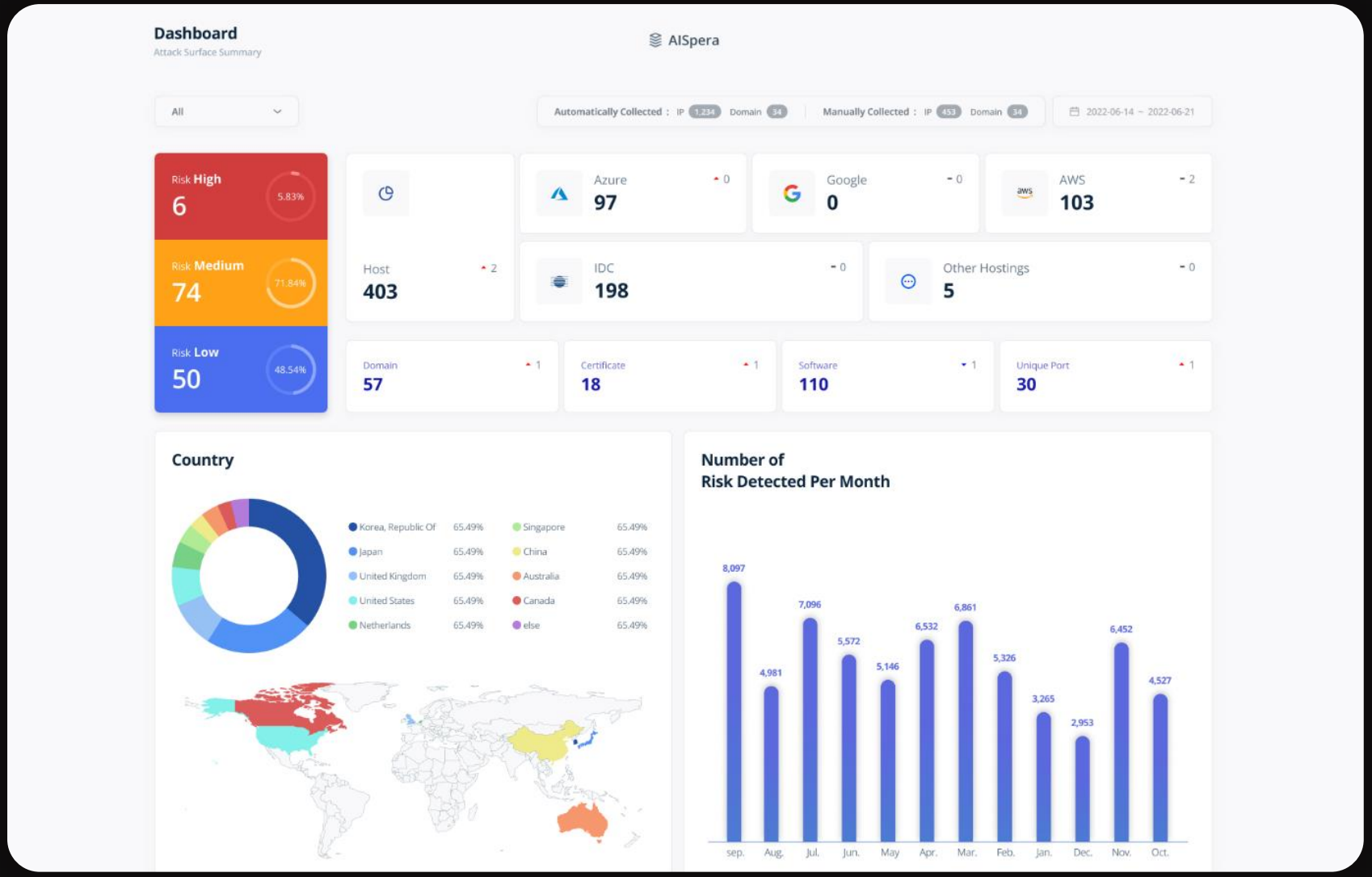
Dashboard
Presents asset information on statistics, geographic information, and vulnerability status

OSINT (Google Hacking)
Monitors information about assets exposed to Google
Provides an asset search query



Dashboard

A real-time view of the entire threat landscape and a solid understanding of your security situation.



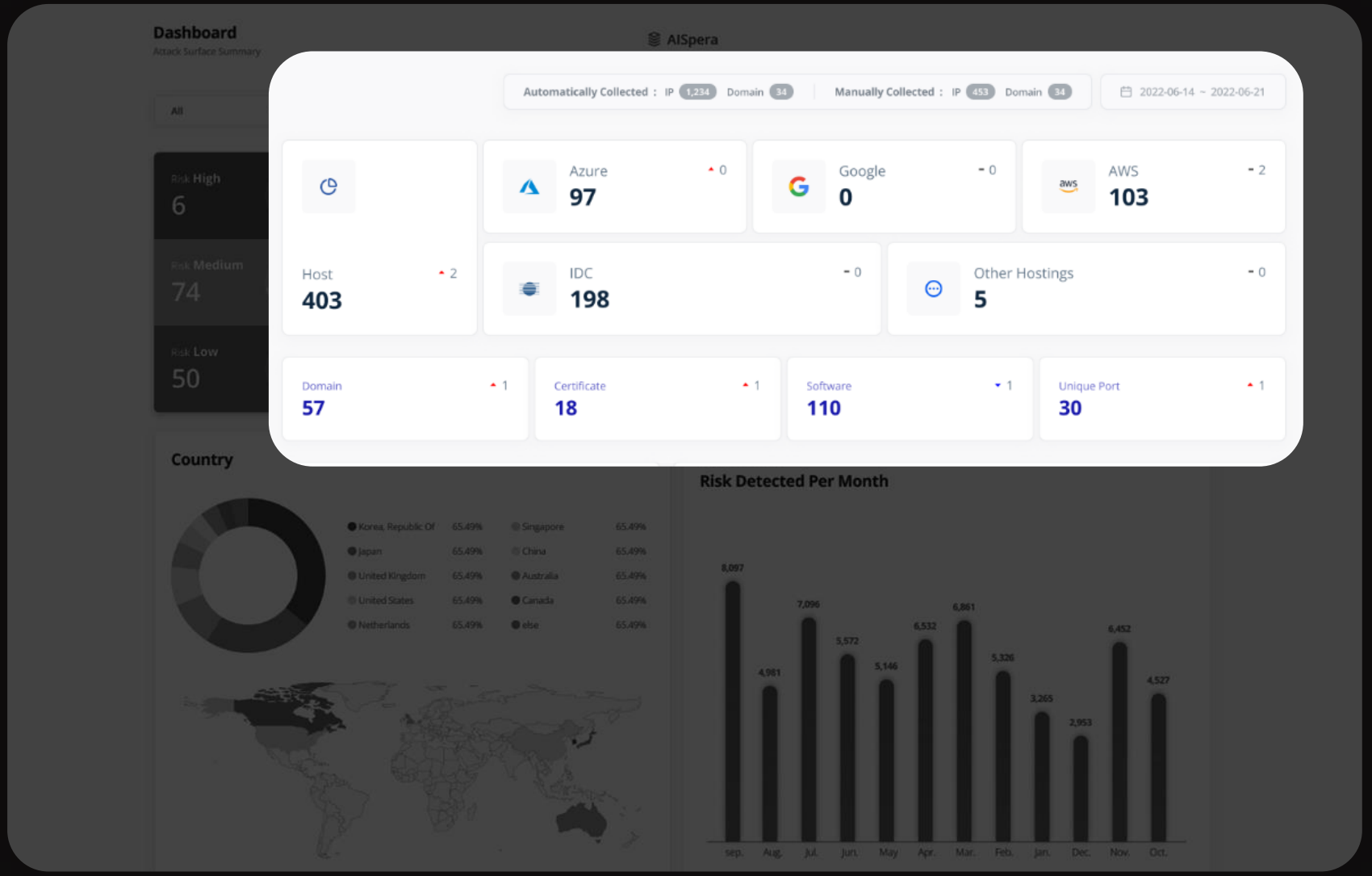
Risk Classification

Assets are automatically detected and classified into three levels depending on risk: High, Medium, and Low, to quickly identify assets that are in urgent need of security measures.

Host & Cloud Statistics

Provides the total number of automatically detected hosts and the status of the enterprise's cloud assets.

The number of Host matches the total sum of assets classified into each cloud and IDC assets.

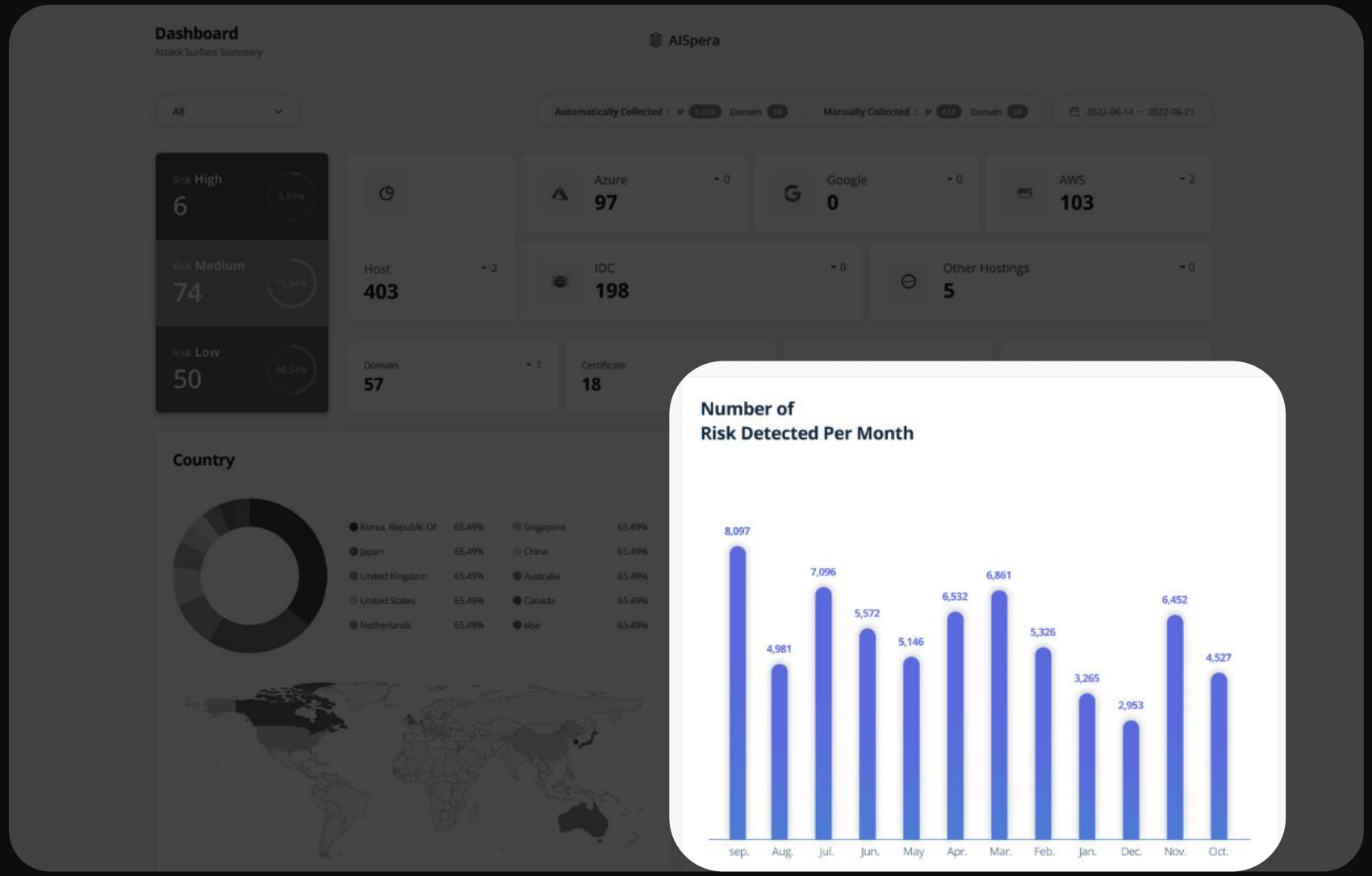


Geographic Statistics of Assets

Provides the geographical distribution of corporate IT assets based on IP address data from over the world.

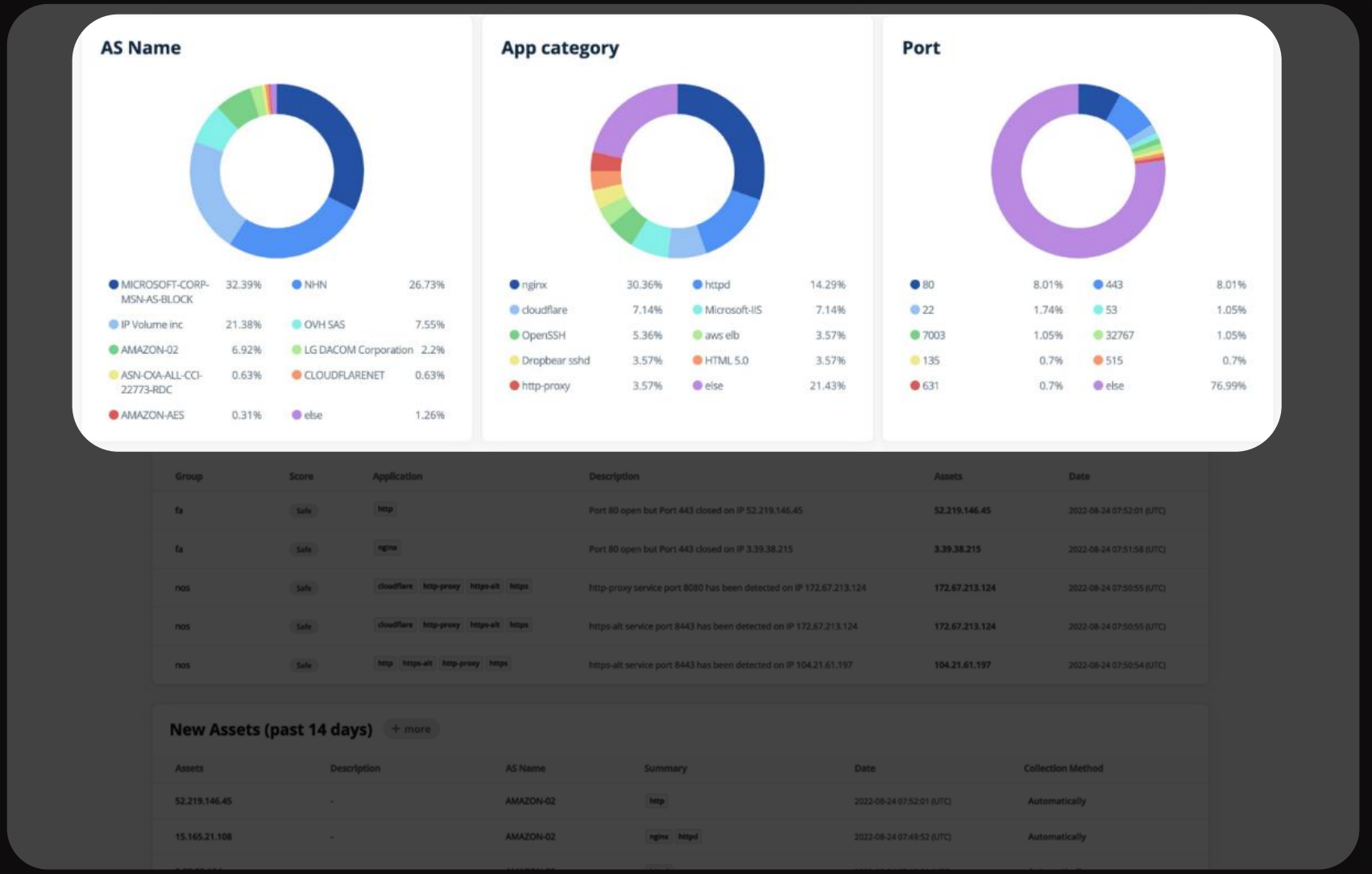
Vulnerable Assets Graph

Shows the number of vulnerable assets detected in a monthly graph.



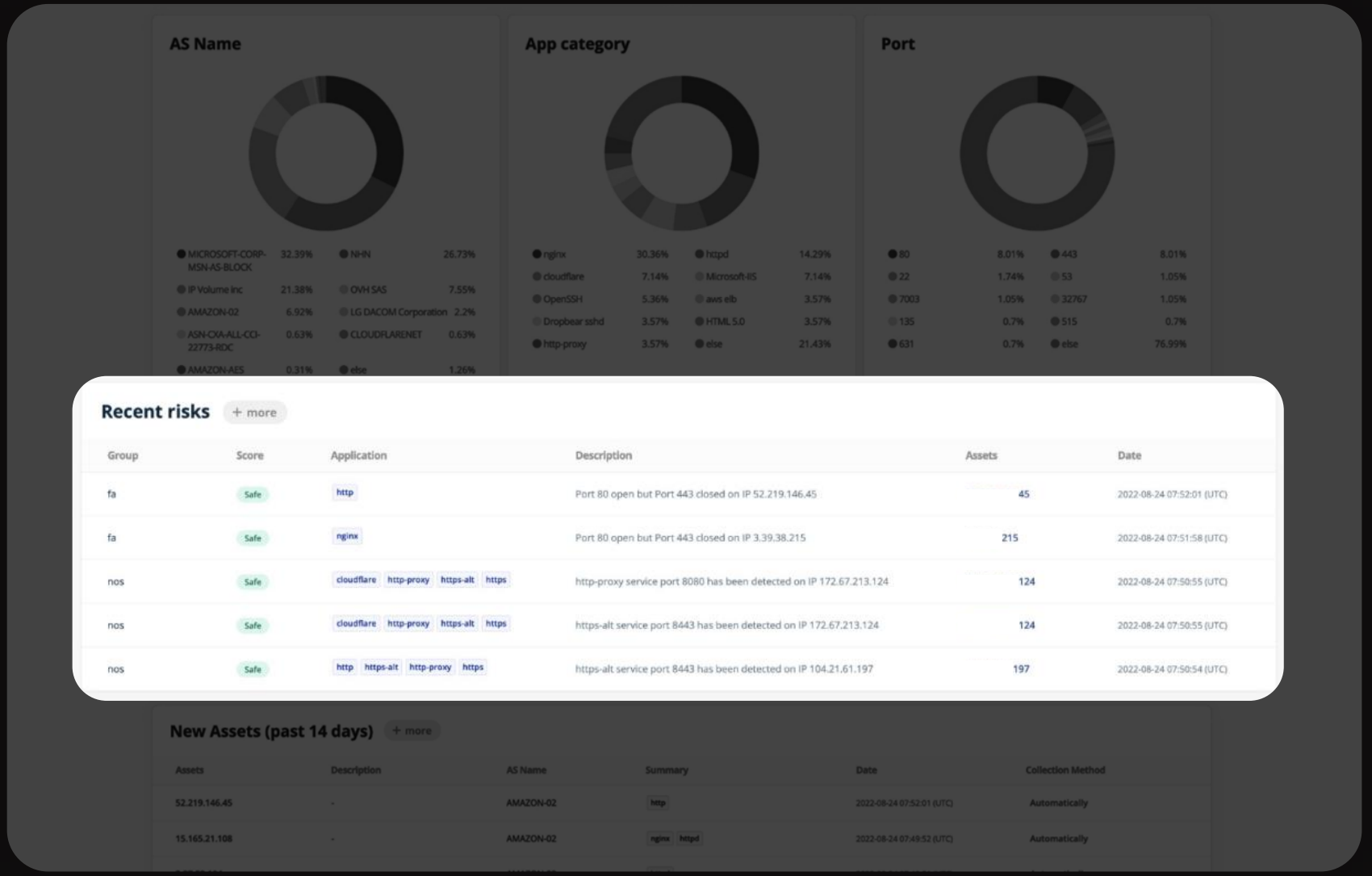
AS Name, Software, Port Statistics

Visualizes the ratio of ASN, application, and open ports in chart formats for better readability.



Recent Risks

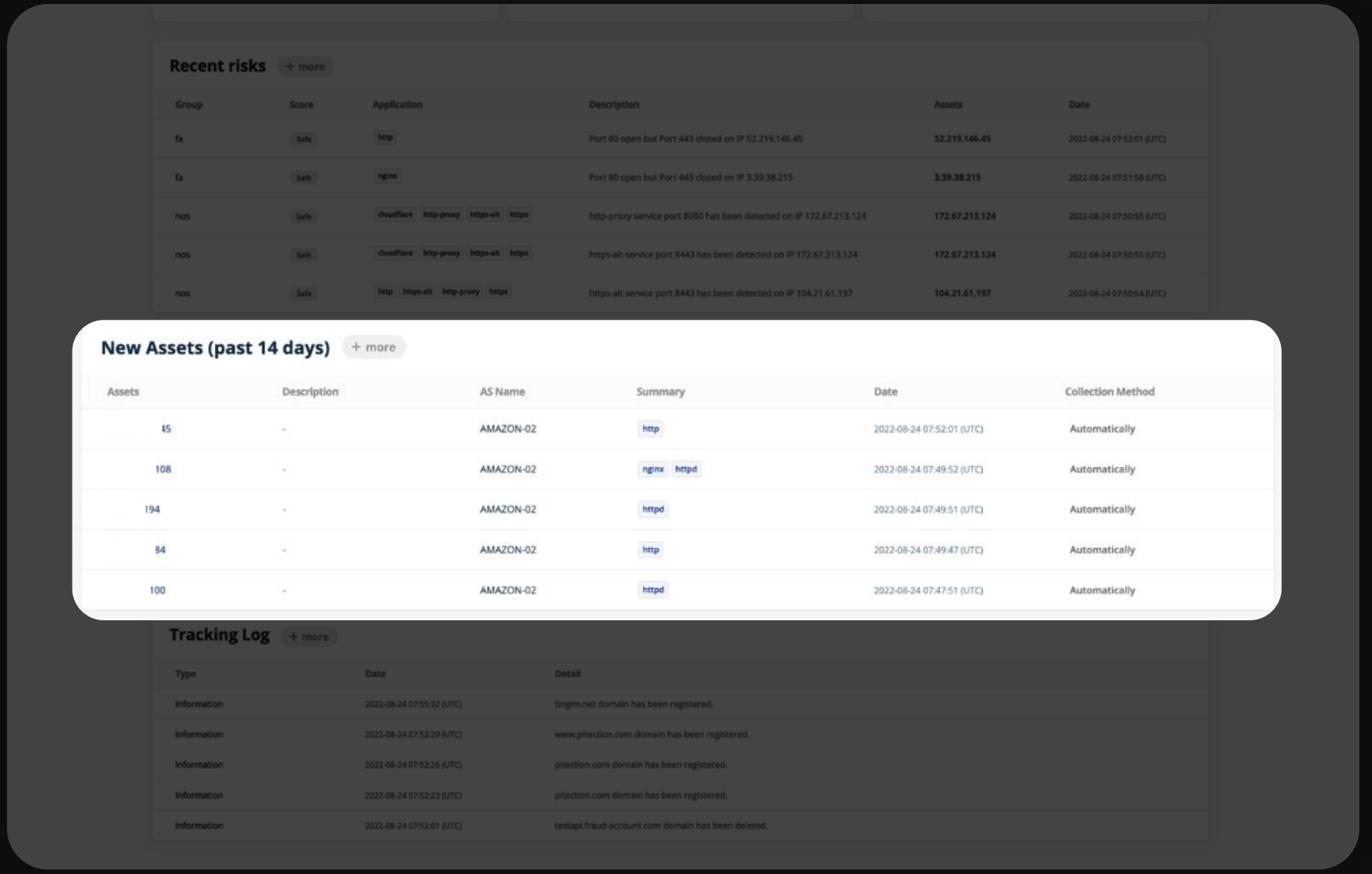
Shows recently detected risks.
Upon clicking data on Assets, you can see details about the vulnerability.



New Assets

Shows recently added new assets.

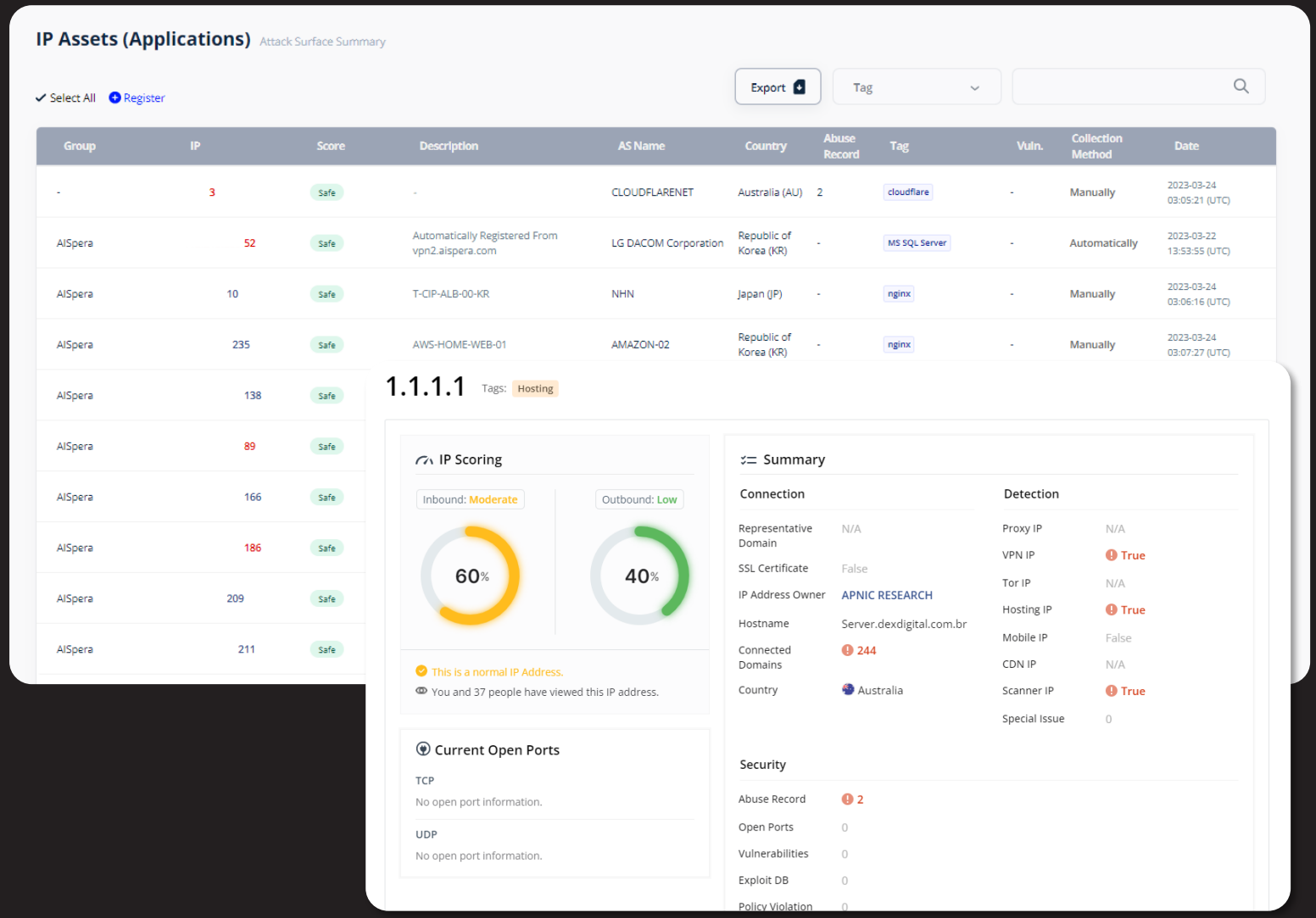
Upon clicking on each asset, you can see detailed information.



IP Assets (Applications)

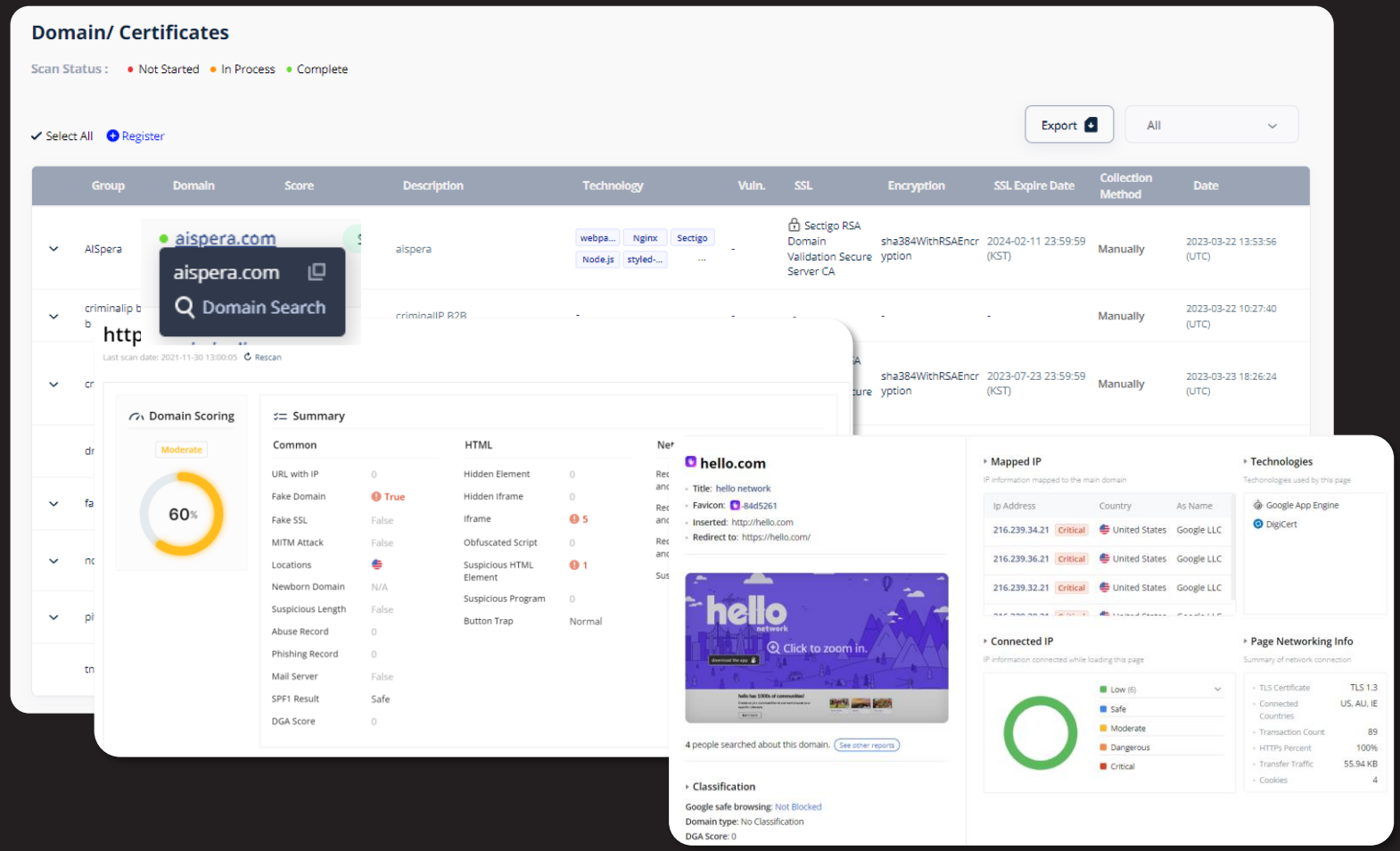
Provides a carefully curated summary (risk score, AS Name, geolocation, vulnerabilities, etc.) of detected IP assets.

Immediately connects to an intelligence search engine upon clicking on an IP address to access enriched threat intelligence.



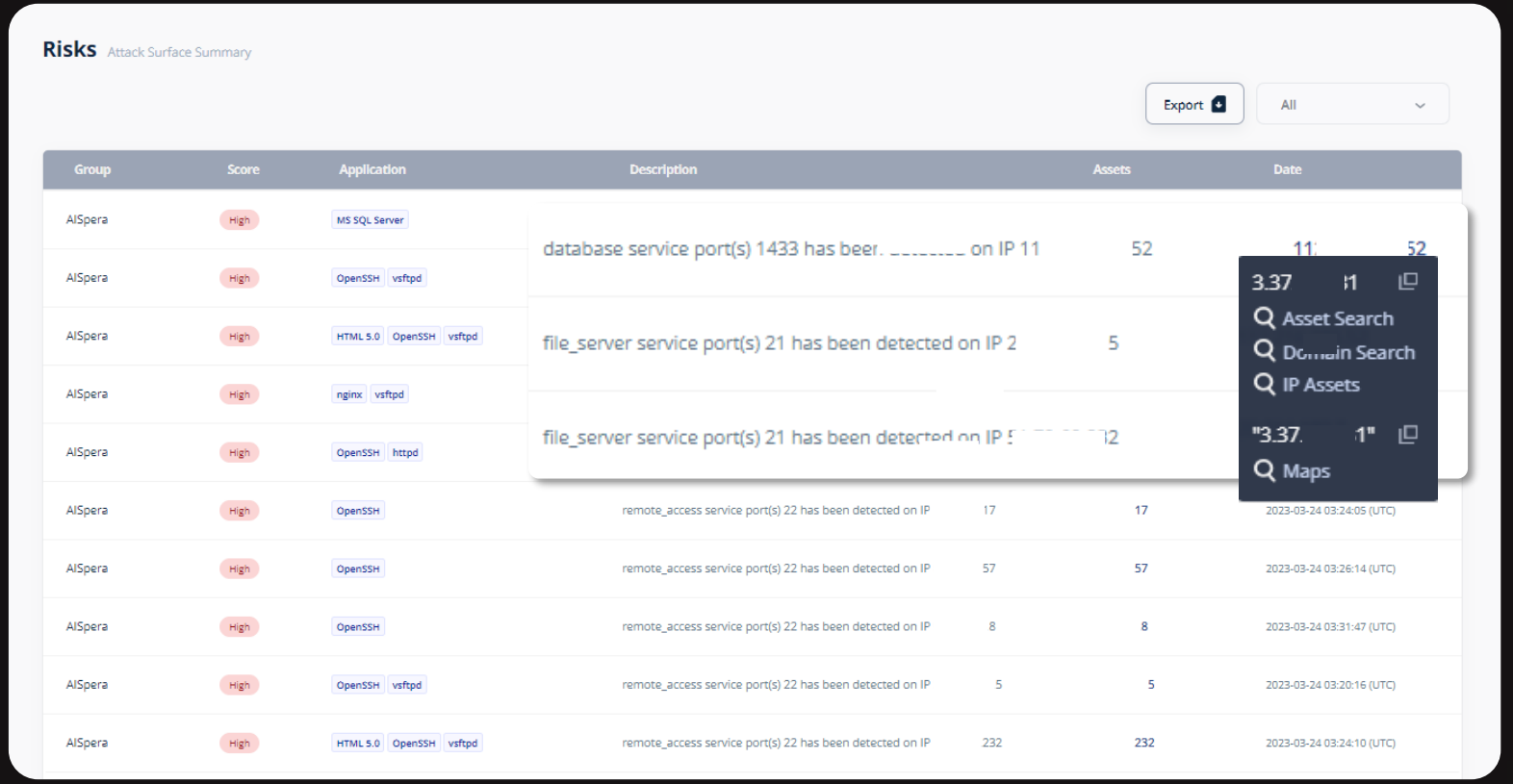
Domain / Certificates

Displays contextualized threat information about a domain (score, technology, jQuery, PHP, etc.), number of vulnerabilities for a domain, certificate information (SSL, encryp-tio n, SSL expiration date), and subdomains.



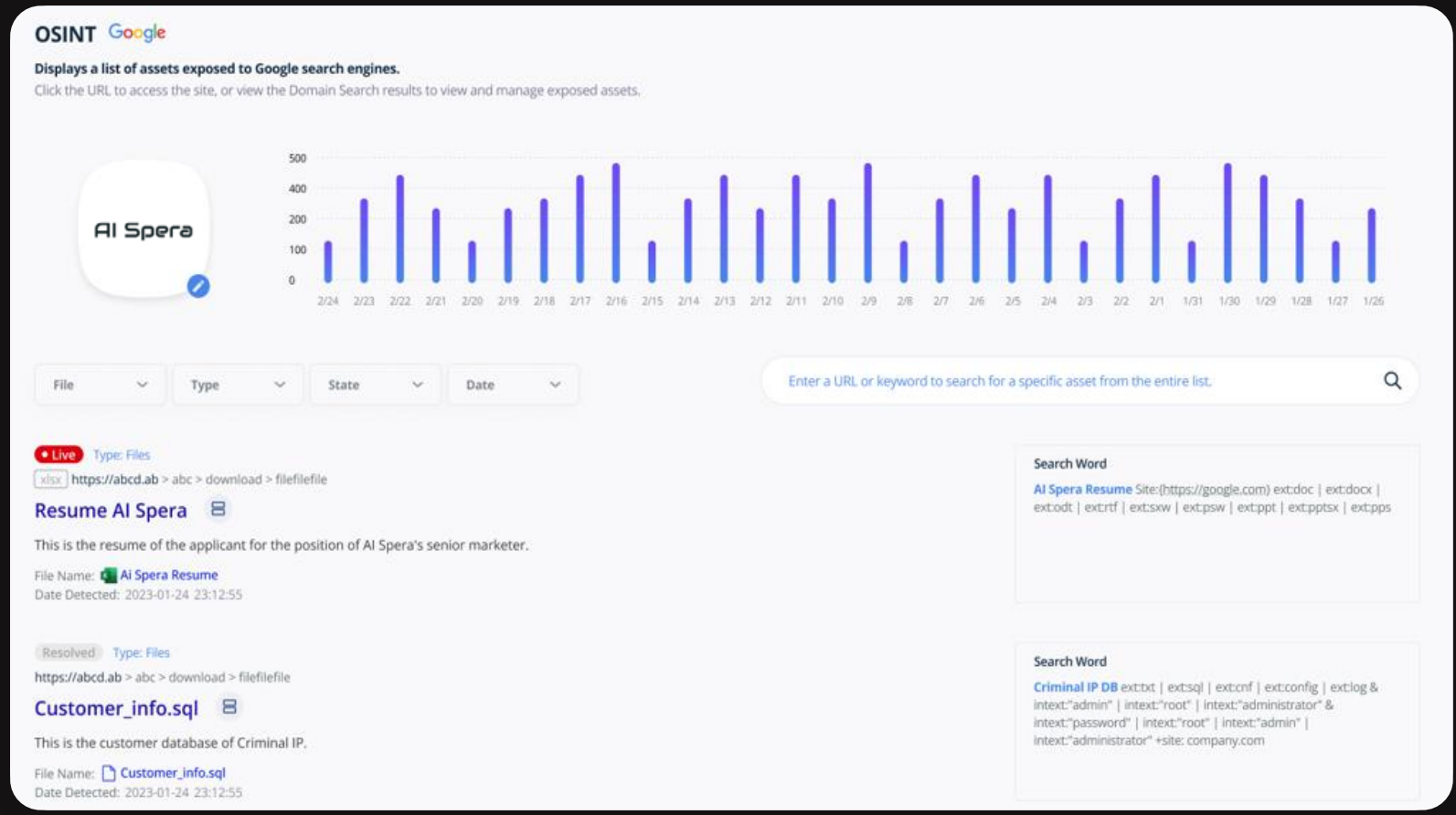
Risks

If threats are detected from registered assets, they are automatically added to the Risks pag e so you can quickly check assets exposed to threats.



OSINT(Google Hacking)

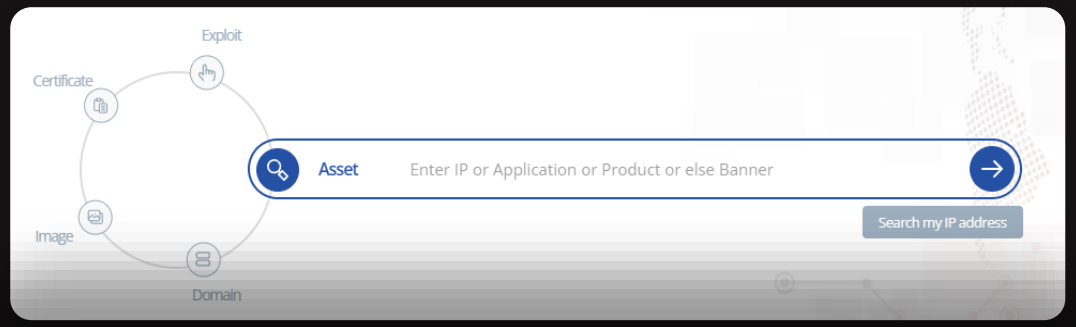
Displays a list of assets exposed to the Google search engine.
You can check the type, file presence, and accessibility status of the exposed assets.

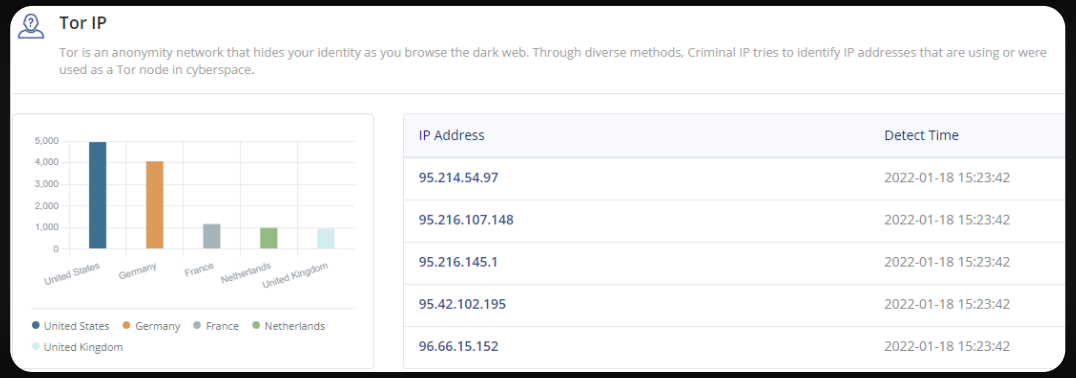


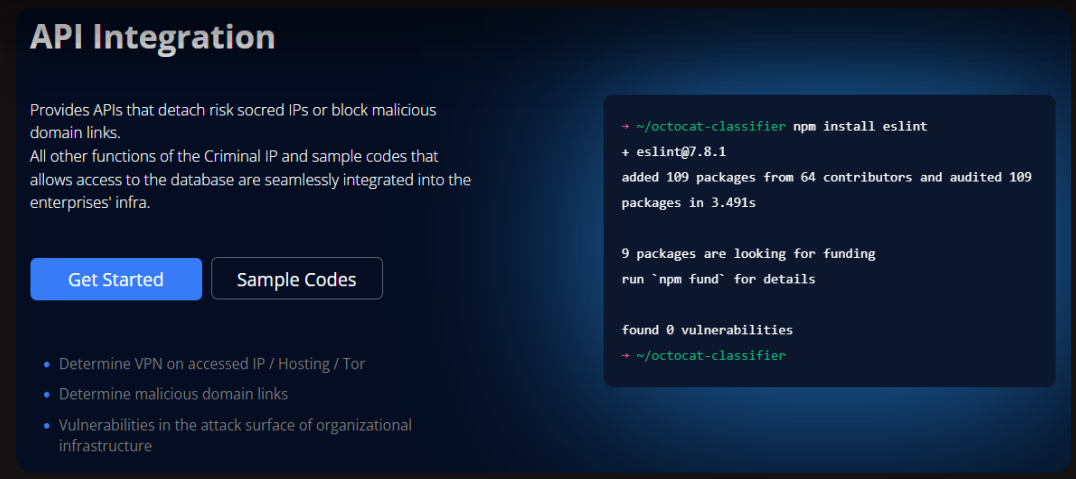
Criminal IP
Threat Intelligence Search Engine

Enjoy additional features of Search, Intelligence, and API integration provided by the Criminal IP CTI search engine paired with ASM.

Stay on top of the latest cybersecurity trends through our compilation of statistics-packed analysis reports on global cyber threats.







2. Criminal IP ASM Competitors

Features	Criminal IP ASM	Censys	Tenable	Mandiant
Ease of use (UI)	★★★★	★★★	★★	★
OSINT (Google Hacking)	★★★★	∅	∅	∅
Access To Threat Intel	★★★★	★★	★★★	★★
Access to Cybersecurity Search Engine/Ability to scan any asset even those not belonging to the company	★★★★	∅	∅	∅
Manual addition of Assets	★★★★	∅	∅	∅
Domain Scanning and Scoring	★★★★	∅	★★	∅
Pricing	$$	$$	$$$	$$$

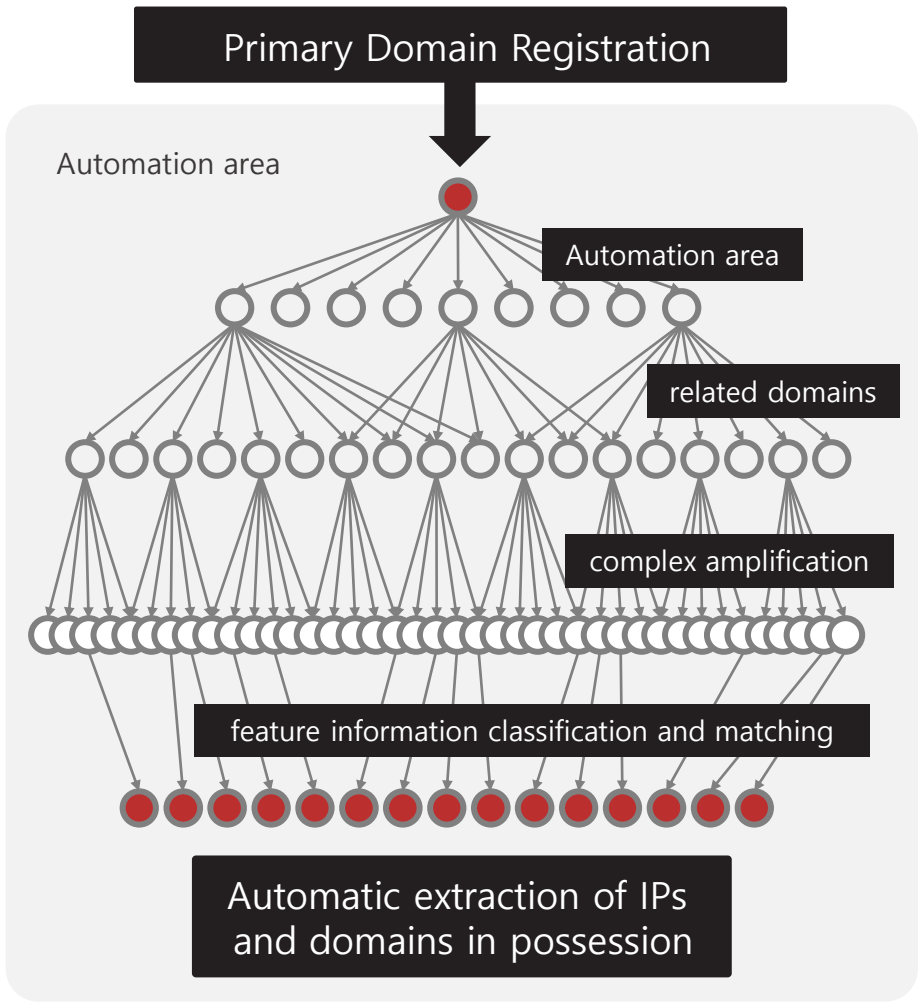
3

Application

- Adopting ASM
- ASM Use Cases

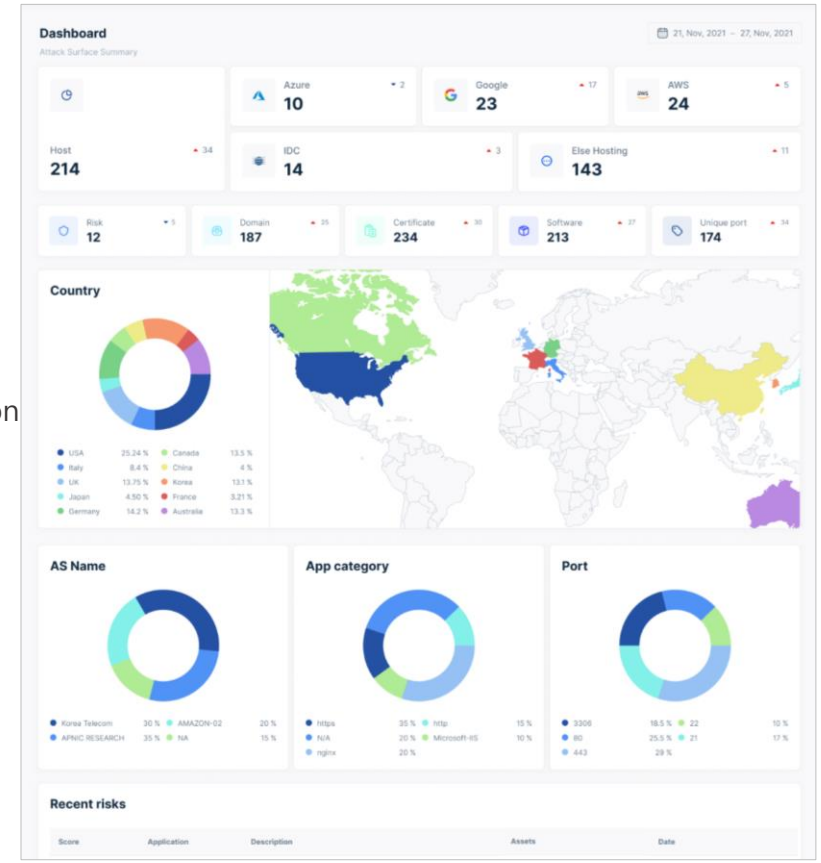
Only one requirement to adopt Criminal IP ASM

We do not request much information from clients when they start using Criminal IP ASM.
Only one domain address of all operating assets is enough to immediately start Attack Surface Management (ASM) as it automatically identifies all network-exposed assets.



Auto-registration

Attack Surface Management



Real Data of attack surfaces detected by ASM

Even at this moment, the major assets of many companies and organizations are exposed and unprotected to attack surfaces.

SW Patch Server

Dev/Test System

Marketing Event Page

Shared System with Cooperators

Case 1 : When new vulnerabilities are discovered

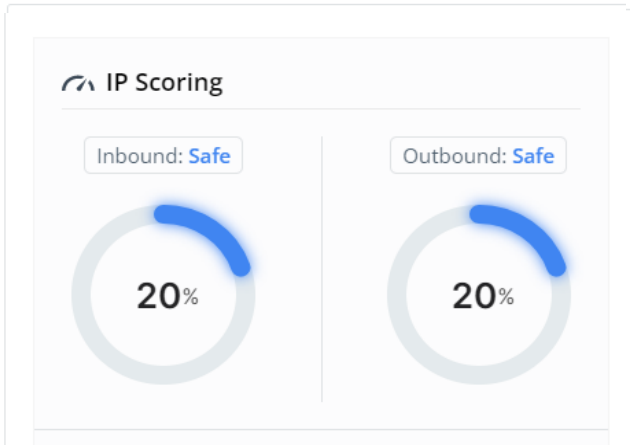
A report with visual risk-scoring is generated if any enterprise assets with exploitable vulnerabilities are discovered through threat intelligence analysis. You can check countermeasures against vulnerabilities through Criminal IP.

Safe

2021.01.30
(Before)

Server A

1.2.3.4 Tags: Hosting



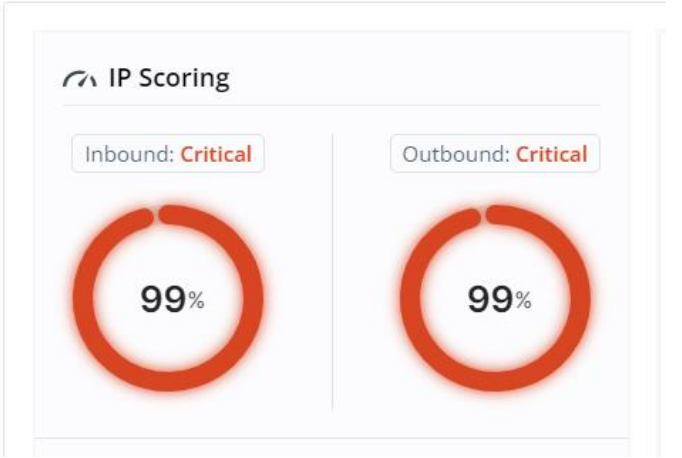
New
CVE-2021-44228

Critical

2021.02.01
(After)

Server A

1.2.3.4 Tags: Hosting



Case 1 : When new vulnerabilities are discovered

Public Institution B

Public institution 'B',
checks vulnerabilities every six months according to NIS policy

Vulnerabilities Check

January

Inspected a large-scale vulnerability

System Patch

February

Patched overall system in order over a month

Vulnerabilities Unattended

March-June

Unable to check new vulnerabilities until the second half of the year

Criminal IP ASM

Introduction of Criminal IP ASM solution to public institution 'B'

Criminal IP ASM Introduction of ASM

Regular vulnerability inspection via ASM

LOG4J Vulnerabilities occurrence

Large-scale vulnerability (Log4shell) issue occurrence

Automatic inspection

Complete inspection of assets with vulnerabilities as soon as the vulnerability is found

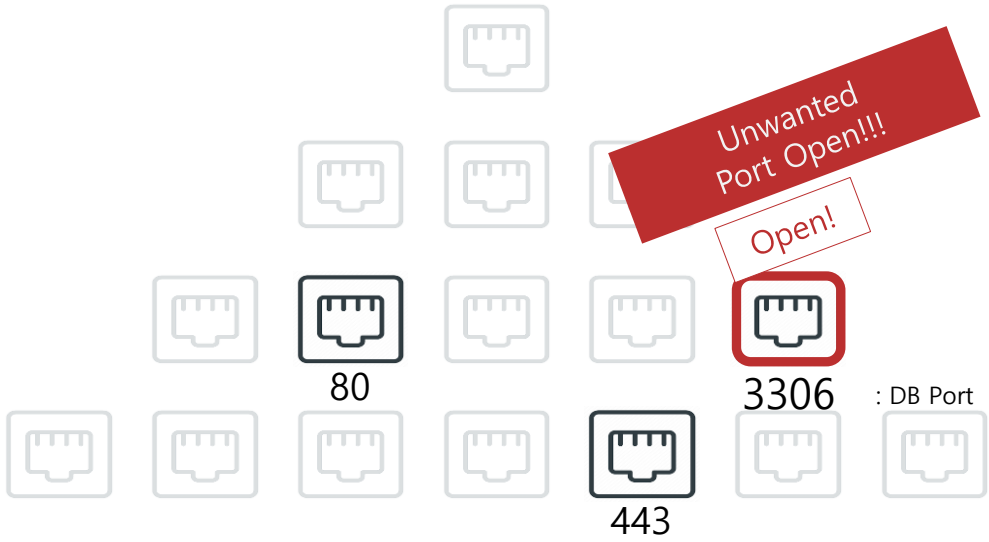
Immediate response

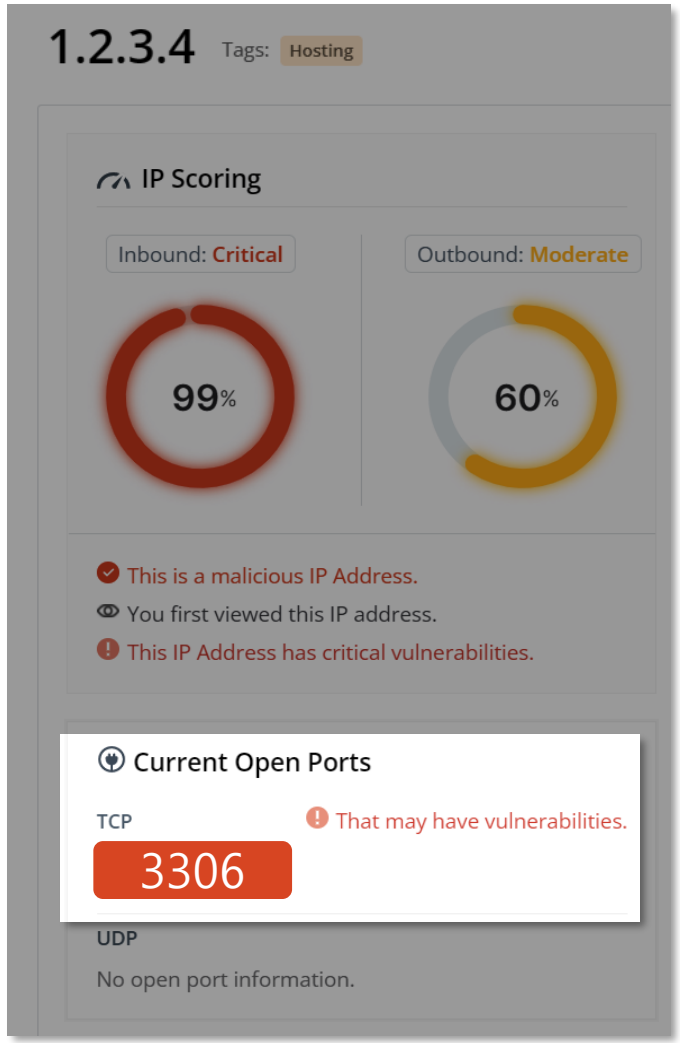
A vulnerability report is generated, and immediate measures are taken by response procedures of the AI Spera security team

No need to check for large-scale vulnerabilities every year
Criminal IP ASM sends automatic reports regularly

Case 2 : When dangerous ports are opened

If a port that should not be open is accidentally opened or left open,
Criminal IP ASM scans all IP ports in real-time and provides a threat report





Case 2 : When dangerous ports are opened

Manufacturer P

Manufacturer 'P'
using ERP system

ERP failure occurred

ERP failure occurred

DB issue detected

Internal developer checked, found DB issue

Request for External Officer

Requested help to DBA (Data Base Administrator), who was on vacation

3306 Port opened

To gain access to DB from outside, DB Port '3306' had to be opened

Firewall system error

Used firewall management solution to set time limit to using DB Port, but due to system error, Port 3306 was left open

Port 3306 exposure

Port 3306 was left open and unattended

Criminal IP ASM

Introduced Criminal IP ASM to Manufacturer P six months later

Criminal IP ASM

Introduction of ASM

Real-time scanning of ports and assets

Port detection

Discovery of multiple open ports and assets with restricted external access

Immediate response

Ports closure and immediate response after verification with ASM automatic report

Real-time management of ports and assets in operation

Case 3 : When new assets are added

Criminal IP ASM's real-time scanning enables the detection of assets that are left exposed or neglected.

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

Case 3 : When new assets are added

IT Service Corporate A

IT Service Corporate 'A' operating multi-cloud

Multi-cloud operation

Using Google Cloud, AWS, Azure as major cloud services

Landing page creation

The marketing team created an event landing page for the new service

Alibaba Cloud adoption

Used Alibaba Cloud as the marketing agency suggested

Event operation

The security team did not provide an inspection, as it was the marketing team's project

Personal information utilization

Called personal-information-related API to send EDM (used as a one-time event page)

Domain unattended after event

After the end of the event, client information and server left unattended

Criminal IP ASM

Introduced Criminal IP ASM to IT Service Corporate A two years later

Introduction of ASM

Real-time automatic detection of cyber assets

Discovery of unknown assets

Discovery of unknown assets scattered on unused clouds

Immediate response

Server removal and immediate response after verification with ASM automatic report

Closing unused event pages and automating cloud asset management with ASM

Thank you

Address

21515 Hawthorne Blvd., Suite 200, Torrance,
California, 90503, The United States of America

E-mail

support@aispera.com

Website

https://www.criminalip.io/