Criminal IP

criminalip.io

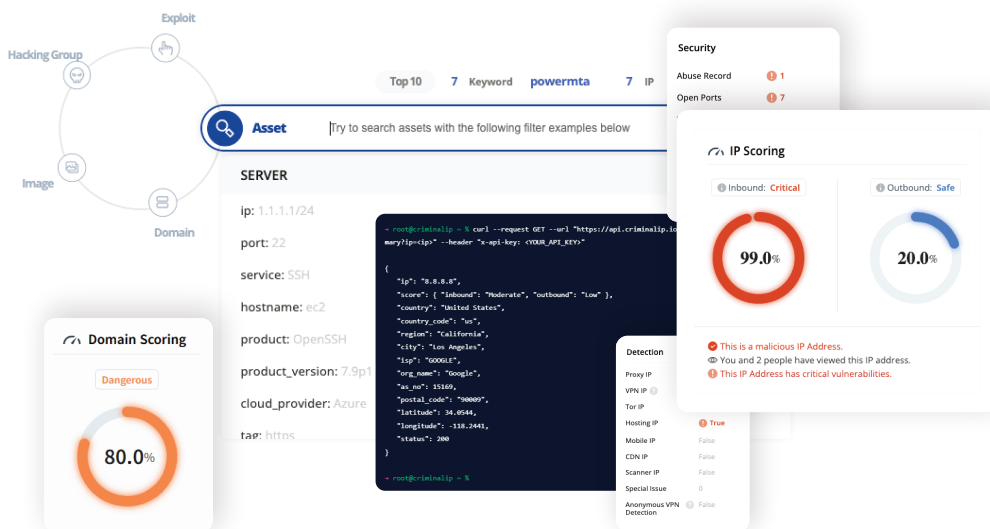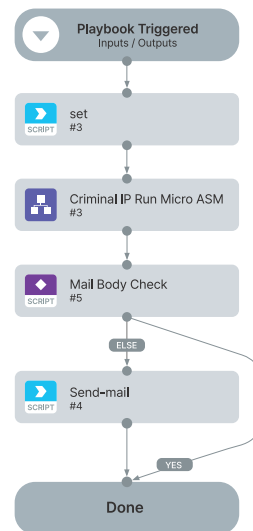Criminal IP TI

Criminal IP ASM

Advanced Cyber Threat Intelligence

Criminal IP Threat Intelligence combines comprehensive IP and domain intelligence to help security teams identify, analyze, and respond to emerging threats.

Example of Palo Alto Integration

Criminal IP Main Features

Unmatched IP Threat Intelligence Coverage

Access the industry's most extensive IP intelligence database, providing deep insights into malicious activities, infrastructure, and emerging threats across the globe.

Real-Time Domain Intelligence

Stay ahead of threats with instant domain scanning capabilities that detect and analyze suspicious activities as they emerge.

Advanced Filters & Tags

Pinpoint exactly what you're looking for with our comprehensive system of threat tags and customizable filters, transforming vast data into actionable intelligence.

Enterprise API for Seamless Security Workflow Integration

Streamline your security operations with our enterprise-grade API that seamlessly integrates threat intelligence into your existing security workflows and automation processes.

Integrated with Leading Security Tools and Platforms

Enhance your security stack with our pre-built integrations across leading security platforms, enabling immediate threat intelligence enrichment without additional development.

Threat Intelligence-Powered Attack Surface Discovery & Protection

Criminal IP ASM

Criminal IP ASM delivers comprehensive visibility and monitoring of your external assets, combining continuous discovery, threat detection, and security assessment with Criminal IP's integrated threat intelligence capabilities.
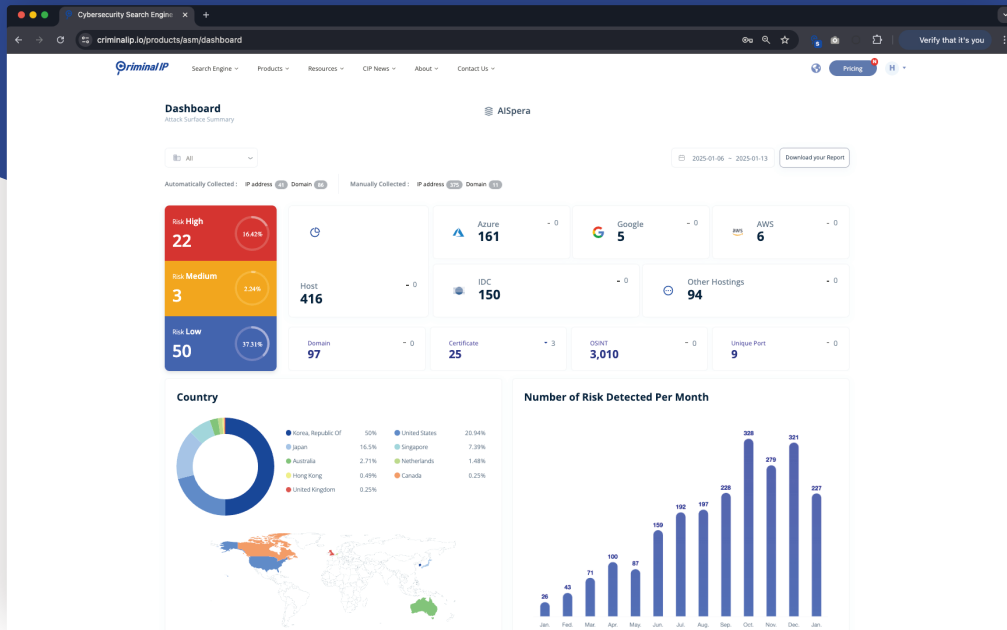
- Detect mismatch in cloud assets
- Identify discrepancies in server locations
- Detect discrepancies in ISP information
- Assess application status
- Track additions and changes to IT assets
- Identify assets exposed to new CVEs

Criminal IP ASM Main Features

Criminal IP ASM automatically detects IT assets scattered across various domains from a single domain and visualizes them on the dashboard.

Dashboard
Provides a comprehensive overview of corporate IT assets

IP Assets (Application)
Provides overview information of detected IP assets

Domain/Certificates
Offers threat information related to domains/subdomains/certificates

Risks
Automatically provides threat information for registered assets (IP, Domain)

OSINT (Google Hacking)
Provides a list and keywords of sensitive information, including files and servers exposed on Google

Dark Web
Automatically monitor all leaked credentials on the dark web

Trusted By

eon

CCN centro criptológico nacional

SecurityHQ

SAMSUNG 삼성서울병원 SAMSUNG MEDICAL CENTER

HYBE

LG U+

SUPSI Scuola universitaria professionale della Svizzera italiana

AT&T

GOVERNMENT OF BERMUDA

S-RM

Service NSW

FUTURE MEDIA

CNI CENTRO NACIONAL DE INTELIGENCIA

PBGC Pension Benefit Guaranty Corporation

MBC

INDUSFACE™

NHN

toss securities

Mphasis The Next Applied

Hanwha Life

AhnLab

kt cloud

NHN PAYCO

WOOWABROS.

IGLOO

Ministry of Science and ICT

KOREA UNIVERSITY

yanolja

Ministry of National Defense Republic of Korea

Agency for Defense Development

KB

Smilegate®

Ministry of Trade, Industry and Energy

Technology Alliances and Integrations

paloalto NETWORKS

tines

MALTEGO

IBM

CISCO

wazuh.

F:RTINET

HYBRID ANALYSIS

quad9

tenable

CYWARE™

POLYSWARM

sumo logic

snowflake®

ANOMALI

Microsoft

VIRUSTOTAL

splunk>

POLARITY

BeyGoo

OnTheHub® by Kivuto

SWIMLANE

Simbian

AI Spera

AI Spera America Inc.
19700 S. Vermont Ave. Suite #200 Global Business Center,
Torrance, CA, 90502, U.S.A.

✉ support@aispera.com

Criminal IP

www.criminalip.io