

Criminal IP ASN

Threat Intelligence-based Automated Attack Surface Management Solution



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





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 distributing malicious code.

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



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.



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



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

Gartner

⁷2021 Emerging Technologies: Critical Insights for External Attack Surface Management

"ASM is a new solution that helps organizations identify risks associated with internet-connected ass ets 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 be come an essential task for CIOs and CISOs."

FORRESTER[®]

⁷2022 ASM Report: Find and Cover Your Assets with Attack Surface Management_J

"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





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.



4.2 billion IP address info

+



Scan Port data from all over the world

+



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-touse 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





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	The domain is not falsified or a certificate is free from
Safe	and are kept safe	leakage or expiration, and is kept 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.





Domain Search	Vulnerability
Image Search	Statistics
Certificate Search	Element Analysis
Exploit Search	Мар

Daily Analysis Report & Messenger Integration



Al Spera					
ewly discove lease refer to the scovered IP, Do	ered risks e following r main, and Ri	: 4 eport for newly isk information	y 1.	Total Assets Domain IP :	328 • 12 12 317 • 17 55 11 • 55
AS Name	\mathbf{O}	App category	\bigcirc	Port	0
waactobicg serv contracts contracts contracts contracts contracts contracts contracts	40.2% • MEXAOPT COM- MENAS BLOCK 10.2% • PMArraine 4.5% • 0.056ABNET 6.1% • 0.650004 0.2% • Inte	22.2% Orgin Din. Bouches 16A. Cowilla 16A. Cowilla 16A. Ortho.50	16.54% Anzan Coulinet (5.23% Energi 3.27% Energi 4.42% Anate 4.64% Ede	15,8% 0.0 15,23% 0.22 6,42% 0.225 6,42% 0.255 5,3% 0.25 5,3%	02794 445 25576 5488 9205 2.845 2849 921 1346 1349 6000 1346 5570 9458 13251
Risk					

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



Risk

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



IP Assets

Scans open ports of

detected IP addresses

Intelligence Search Result

Gets details about the exposure status and vulnerabilities on the statistics, geographic information, attack surface



subdomains of

the detected IP address

X

Dashboard

Presents asset information on

and vulnerability status



(Google Hacking)

Monitors information about assets exposed to Google



Certificate

Displays information about the certificate applied to the domain

P





OSINT





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.

Recent risks	+ more				
Group	Score	Application	Description	Assets	Date
fa	Sale	http	Port 80 open but Port 443 closed on IP 52.219.146.45	52.219.146.45	2022-08-24 07:52:01 (UTC)
fa	Sale	nginx	Port 80 open but Port 443 closed on IP 3.39.38.215	3.39.38.215	2022-08-24 07:51:58 (UTC)
nos	Sele	cloudflare http-proxy https-alt https	http-proxy service port 8080 has been detected on IP 172.67.213.124	172.67.213.124	2022-08-24 07:50:55 (UTC)
nos	Sele	cloudflare http-proxy https-alt https	https-alt service port 8443 has been detected on IP 172.67.213.124	172.67.213.124	2022-08-24 07:50:55 (UTC)
nos	Safe	http: https-alt http-proxy https	https-alt service port 8443 has been detected on IP 104.21.61.197	104.21.61.197	2022-08-24 07:50:54 (UTC)

New Assets (past 14 days) + more

Assets		Description		AS Name		Summary		Date	Collection Method	
	45	ж.		AMAZON-02		http		2022-08-24 07:52:01 (UTC)	Automatically	
	108			AMAZON-02		nginx httpd		2022-08-24 07:49:52 (UTC)	Automatically	
194	4	×		AMAZON-02		httpd		2022-08-24 07:49:51 (UTC)	Automatically	
	84			AMAZON-02		http		2022-08-24 07:49:47 (UTC)	Automatically	
10	00	×		AMAZON-02		httpd		2022-08-24 07:47:51 (UTC)	Automatically	
	Tracking Log	+ more								ĺ
	Туре		Date		Detail					
	Information		2022-08-24 07:55:32 (UTC)		tingim.net domain	has been registered.				
	Information		2022-08-24 07:52:29 (UTC)		www.pitection.com domain has been registered.					
	Information		2022-08-24 07:52:26 (UTC)	pitection.com domain has been registered.						
	Information		2022-08-24 07:52:23 (UTC)							
	Information		2022-08-24 07:52:01 (UTC)		testapi.fraud-acco	unt.com domain has been deleted.				

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.

IP Assets (Applications) Attack Surface Summary

Select

Register					Export	Тад	~			Q
	IP	Score	Description	AS Name	Country F	Abuse Record	Тад	Vuin.	Collection Method	Date
	3	Safe	-	CLOUDFLARENET	Australia (AU) 2		cloudflare		Manually	2023-03-24 03:05:21 (UTC)
	52	Safe	Automatically Registered From vpn2.aispera.com	LG DACOM Corporation	Republic of . Korea (KR)		MS SQL Server	-	Automatically	2023-03-22 13:53:55 (UTC)
	10	Safe	T-CIP-ALB-00-KR	NHN	Japan (JP) -		nginx	-	Manually	2023-03-24 03:06:16 (UTC)
	235	Safe	AWS-HOME-WEB-01	AMAZON-02	Republic of . Korea (KR)		nginx	-	Manually	2023-03-24 03:07:27 (UTC)
	138	Safe	.1.1.1 Tags: Hosting							
	89	Safe	Co IP Scoring		;≓ Summary					
	166	Safe	Inbound: Moderate	Outbound: Low	Connection			Detection		
	186	Safe			Representative Domain	N/A False		Proxy IP VPN IP	N/A True	
	209	Safe	60%	40%	IP Address Owner	APNIC	RESEARCH	Tor IP Hosting IP	N/A ① True	
	211	Safe	This is a normal IP Address.		Connected Domains	Server.	dexdigital.com.br	Mobile IP CDN IP	False N/A	
			You and 37 people have viewed this You and 37 people You and 37 people	s IP address.	Country	🅙 Aus	tralia	Scanner IP	Itrue	
			() Current Open Ports		Security			Special Issue	e 0	
			TCP		Abuse Record	9 2				
			UDP No open port information.		Open Ports Vulnerabilities Exploit DB	0				
	Register	■ Register IP 3 52 10 235 138 89 166 186 209 211	IP Score 3 Safe 52 Safe 10 Safe 235 Safe 138 Safe 166 Safe 186 Safe 209 Safe 211 Safe	Register IP Score Description 3 Safe . 52 Safe Automatically Registered From yop2 alignera com 10 Safe F-CIP-ALB-00-KR 10 Safe AVS-HOME-WEB-01 138 Safe AVS-HOME-WEB-01 166 Safe Information 209 Safe Safe 209 Safe Safe 211 Safe No gen port information. UP No gen port information. UP	Pergister IP Score Description At Name 3 3% - CLOUDPLARENET 52 3% - CLOUDPLARENET 10 3% T-CIP-ALB-00-AR NHN 235 3% AVIS-HOME-WEB-01 AMAZON-02 118 3% From Person (Construct) (Constru	Pregner Sore Description AS Name Country P 3 see - CLOUDPLARENET Australia (AU) 2 52 see Automatically Registered From ynp2 atspera.com LG DACOM Corporation Republic of Korea (RP) - 10 see T-CIP-ALP-00-KR NHN Japan (P) - 10 see T-CIP-ALP-00-KR NHN Japan (P) - 10 see T-CIP-ALP-00-KR NHN Japan (P) - 138 see T-CIP-ALP-00-KR AMAZON-02 Republic of Korea (RP) - 138 see T-CIP-ALP-00-KR AMAZON-02 Republic of Korea (RP) - 138 see fill T-CIP-ALP-00-KR AMAZON-02 Republic of Korea (RP) - 138 see see fill fill Mazon-02 Republic of Korea (RP) - 138 see see fill fill fill Sill - 139 see see fill fill fill - - - -<	Pregner Export Trg 1 Sore Description Ad Name County Abute Record 3 SM - CLOUDFLARENET Australia (AU) 2 52 SM Automatically Registered From uppe 2 supper a con Lis DACOM Corporation Republic of Korea (RR) - 10 SM T-CIP-ALB-00-RR NHN Japan (P) - 25 SM AUS+HOME-WEB-01 AMAZON-02 Republic of Korea (RR) - 18 SM I.1.1.1.1 Tags: Hosting Sint - 186 SM FIP Scoring Outbound: Low Sint MA 186 SM FIP Scoring Connection Representative MA 186 SM Fib is a normal IP Address. Outbound: Low Sinter Hist Reame Sinter WA 209 SM Fib is a normal IP Address. Outpot address. Outpot address. Outpot address. Outpot address. Outpot address. 0 Current Open Ports Top Natare on a strateging address. Outpot address. Outpot address. Outpot addres. Ou	Prepare Export Tog 1 Sore Description A Share Caurdy Abace Tag 3 Sofe - CLOUGHABENET Ausraia (AU) 2 countere 2 Sofe - CLOUGHABENET Ausraia (AU) 2 countere 10 Sofe T-CIPALBOOHR NHN Japa (DF) - resolution 10 Sofe T-CIPALBOOHR NHN Japa (DF) - resolution 13 Sofe NUSHOME-WEB-01 AMAZONO2 Republic of Korea (DR) - resolution 138 Sofe NUSHOME-WEB-01 AMAZONO2 Republic of Korea (DR) - resolution 138 Sofe NUSHOME-WEB-01 AMAZONO2 Republic of Korea (DR) - resolution 138 Sofe - - - - resolution 138 Sofe - - - - - - - 139 Sofe - - - - - - - - <t< th=""><th>Preperer Teg Teg Teg 10 Sore Conception Advanatically Registered From up2.2.appera.Conception Australia (AU) 2 Somethie - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Strage, Sore - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Strage, Sore - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Ist Sore, Sore - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Ist Sore - 138 Sore TCIP-ALB-00-R NHN Japen (P) . Ist Sore - 138 Sore TCIP-ALB-00-R MAZOHO2 Republic off . Ist Sore - 138 Sore TCIP-ALB-00-R MAZOHO2 Republic off . Ist Sore - - 138 Sore TCIP-ALB-00-R MAZOHO2 Republic off . Ist Sore - - - - - - - - - <t< th=""><th>Preper Tg Tg P Xore Description Al Name Cauruy Maced Tg Vale Admendia 3 Mar CLOUCH-ARENET Australia (Adu) 2 Marced - Marced 2 Marced Automatically Registrand from Age20 algone Acom LG DACOM Corportion Repail of P - Marced - Marced Automatically Registrand from Age20 algone Acom - Marced - Ma</th></t<></th></t<>	Preperer Teg Teg Teg 10 Sore Conception Advanatically Registered From up2.2.appera.Conception Australia (AU) 2 Somethie - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Strage, Sore - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Strage, Sore - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Ist Sore, Sore - 10 Sore TCIP-ALB-00-R NHN Japen (P) . Ist Sore - 138 Sore TCIP-ALB-00-R NHN Japen (P) . Ist Sore - 138 Sore TCIP-ALB-00-R MAZOHO2 Republic off . Ist Sore - 138 Sore TCIP-ALB-00-R MAZOHO2 Republic off . Ist Sore - - 138 Sore TCIP-ALB-00-R MAZOHO2 Republic off . Ist Sore - - - - - - - - - <t< th=""><th>Preper Tg Tg P Xore Description Al Name Cauruy Maced Tg Vale Admendia 3 Mar CLOUCH-ARENET Australia (Adu) 2 Marced - Marced 2 Marced Automatically Registrand from Age20 algone Acom LG DACOM Corportion Repail of P - Marced - Marced Automatically Registrand from Age20 algone Acom - Marced - Ma</th></t<>	Preper Tg Tg P Xore Description Al Name Cauruy Maced Tg Vale Admendia 3 Mar CLOUCH-ARENET Australia (Adu) 2 Marced - Marced 2 Marced Automatically Registrand from Age20 algone Acom LG DACOM Corportion Repail of P - Marced - Marced Automatically Registrand from Age20 algone Acom - Marced - Ma

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.

Domain/ Certificates Scan Status : Not Started In Process Complete Export All Select All Register 🗄 Sectigo RSA aispera.com webpa... Nginx Sectigo Domain sha384WithRSAEncr 2024-02-11 23:59:59 2023-03-22 13:53:56 AlSnera Manually aispera Validation Secure votion (KST) aispera.com 🛛 📮 Server CA Q Domain Search 2023-03-22 10:27:40 criminalip b \sim ninalIP R2P Manually http Last scan date: 2021-11-30 13:00:05 C Rescan sha384WithRSAEncr 2023-07-23 23:59:59 2023-03-23 18:26:24 \sim cr Manually (KST) re votion (UTC) Co Domain Scoring HTML Common dr hello.com Mapped IF ▹ Technologies URL with IP Hidden Element and Title: hello network True Fake Domain Hidden Iframe \sim fa Favicon: 1 -84d5261 Google App Engine In Address As Name 60% **0** 5 Fake SSL Iframe Inserted: http://hello.com O DigiCert 216.239.34.21 Critical 👙 United States Google LLC MITM Attack Redirect to: https://hello.com Obfuscated Script Der and 216.239.36.21 Critical 👙 United States Google LLC Locations 4 Suspicious HTML **0** 1 Sus Element Newborn Domain 216.239.32.21 Critical United States Google LL Suspicious Program hello Suspicious Length Button Trap Normal Abuse Record Connected IP ▶ Page Networking Info Click to zoom in Phishing Record Mail Server TLS 1.3 Low (6) SPF1 Result Safe Marriel and British US, AU, IE Safe DGA Score Moderate 89 4 people searched about this domain. See other reports Bangerous 100% 55.94 KB Critical 14 Classification Google safe browsing: Not Blocked Domain type: No Classification DGA Score: 0

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.

isks Attack Surf	face Summary				
				Export	All ~
Group	Score	Application	Description	Assets	Date
AlSpera	High	MS SQL Server	database service port(s) 1/22 has been on ID 11	52	44: 50
AlSpera	High	OpenSSH vsftpd	database service port(s) 1455 has been account of the fit	52	3.37 11 🗉
AlSpera	High	HTML 5.0 OpenSSH vsftpd	file_server service port(s) 21 has been detected on IP 2	5	Q Asset Search Q Donnain Search
AlSpera	High	nginx vsftpd			Q IP Assets
AlSpera	High	OpenSSH httpd	file_server service port(s) 21 has been detected on IP {	12	"3.37. 1" 🛛
AlSpera	High	OpenSSH	remote_access service port(s) 22 has been detected on IP 17	17	2023-03-24 03:24:05 (UTC)
AlSpera	High	OpenSSH	remote_access service port(s) 22 has been detected on IP 57	57	2023-03-24 03:26:14 (UTC)
AlSpera	High	OpenSSH	remote_access service port(s) 22 has been detected on IP 8	8	2023-03-24 03:31:47 (UTC)
AlSpera	High	OpenSSH vsftpd	remote_access service port(s) 22 has been detected on IP 5	5	2023-03-24 03:20:16 (UTC)
AlSpera	High	HTML 5.0 OpenSSH vsftpd	remote_access service port(s) 22 has been detected on IP 232	232	2023-03-24 03:24:10 (UTC)

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.

OSINT Google

Displays a list of assets exposed to Google search engines.

Click the URL to access the site, or view the Domain Search results to view and manage exposed assets.



xisx https://abcd.ab > abc > download > filefilefile

Resume Al Spera 🗧

This is the resume of the applicant for the position of Al Spera's senior marketer.

File Name: 🙀 Ai Spera Resume Date Detected: 2023-01-24 23:12:55

Resolved Type: Files https://abcd.ab > abc > download > filefilefile

Customer info.sql 🗧 This is the customer database of Criminal IP.

File Name: Customer_info.sql Date Detected: 2023-01-24 23:12:55

Al Spera Resume Site:(https://google.com) ext:doc | ext:docx | extodt | extrtf | extsxw | extpsw | extppt | extpptsx | extpps

Search Word

Criminal IP DB extitut | extisql | exticnf | exticonfig | extlog & intext:"admin" | intext:"root" | intext:"administrator" & intext:"password" | intext:"root" | intext:"admin" | intext:"administrator" +site: company.com

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 Tor IP

Tor is an anonymity network that hides your identity as you browse the dark web. Through diverse methods, Criminal IP tries to identify IP addresses that are using or wer used as a Tor node in cyberspace.

5,000	IP Address	Detect Time
4,000	95.214.54.97	2022-01-18 15:23:42
2,000	95.216.107.148	2022-01-18 15:23:42
0 United States Germany France Neitherlands United Kingdom	95.216.145.1	2022-01-18 15:23:42
United States Commany Campany Campany Natherlande	95.42.102.195	2022-01-18 15:23:42
United Kingdom	96.66.15.152	2022-01-18 15:23:42

API Integration

Provides APIs that detach risk socred IPs or block malicious domain links. All other functions of the Criminal IP and sample codes that allows access to the database are seamlessly integrated into the enterprises' infra.

Get Started Sample Codes

• Determine VPN on accessed IP / Hosting / To

Determine malicious domain links

 Vulnerabilities in the attack surface of organizational infrastructure

- → ~/octocat-classifier npm install eslint
- + eslint@7.8.1

added 109 packages from 64 contributors and audited 109 packages in 3.491s

9 packages are looking for funding run `npm fund` for details

found 0 vulnerabilities

→ ~/octocat-classifie

2. Criminal IP ASM Competitors

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





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.



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.



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.



Case 1 : When new vulnerabilities are discovered



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



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



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



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)

\neg	

4				
Assets	Description	AS Name	Summary	Date
22.1.20.16	¢	d	tt.	2022-01-21 3:22:45
22.1.20.122	¢	google	ttest	2022-01-21 3:22:02
22.1.20.13	e.	TEST	ttest	2022-01-21 3:05:11
22.1.20.14	¢	c	ttest	2022-01-21 3:05:07
22.1.20.12	¢	ь	ttest	2022-01-21 3:05:04

Case 3 : When new assets are added





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/

