

Kaspersky Digital Footprint Intelligence

23



Questions for experts

What's the best way to launch an attack against your organization?

What is the most cost-efficient way to attack you?

What information is available to an attacker targeting your business?

Has your infrastructure already been compromised without your knowledge?

Kaspersky Digital Footprint Intelligence answers these and other questions as our experts piece together a comprehensive picture of your attack status, identifying weak spots ripe for exploitation and revealing evidence of past, present and even planned attacks.

Intro

As your business grows, the complexity and distribution of your IT environments grow too, presenting a challenge: protecting your widely distributed digital presence without direct control or ownership. Dynamic and interconnected environments enable companies to derive significant benefits. However, ever-increasing interconnectivity is also expanding the attack surface. As attackers become more skilled, it's vital not only to have an accurate picture of your organization's online presence, but also to be able to track its changes and react to external threats aimed at exposed digital assets.

Organizations use a wide range of security tools in their security operations but there are still digital threats that loom which require very specific capabilities — to detect and mitigate data leakages, monitor plans and attack schemes of cybercriminals located on dark web forums, etc. To help security analysts explore the adversary's view of their company resources, promptly discover the potential attack vectors available to them and adjust their defenses accordingly, Kaspersky has created Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence provides

Kaspersky Digital Footprint Intelligence is a comprehensive digital risk protection service that helps customers monitor their digital assets and detect threats from the surface, deep, and dark webs.



Network Reconnaissance

Identification of the customer's network resources and exposed services which are a potential entry point for an attack. Tailored analysis of existing vulnerabilities, with further scoring and comprehensive risk evaluation based on the CVSS base score, availability of public exploits, penetration testing experience and location of the network resource (hosting/infrastructure).



Dark Web Monitoring

Continuous monitoring of dozens of dark web resources (forums, ransomware blogs, messengers, tor sites, etc.), detecting any references and threats relating to your company, clients and partners. Analysis of active targeted attacks or attacks that are being planned, APT campaigns aimed at your company, industry and regions of operation.



Discovery of Data Leaks

Detection of compromised employees, partner and client credentials, bank cards, phone numbers and other sensitive information that can be used to carry out an attack or pose reputational risks for your company.



Threats Detection

Monitoring of fraudulent activities that can damage a company's reputation and/or deceive customers.



Multitenancy support

Enhanced capabilities for managed security service providers (MSSPs) and large organizations with a multi-branch structure.

How it works

Configure	Collect	React	Filter
Information discovery about the company's digital assets	Automated data collection from surface, deep and dark webs, and the Kaspersky knowledgebase	Providing operational threat notifications on Kaspersky Threat Intelligence Portal or via API	Threat detection, analysis and prioritization managed by analysts

Key service deliverables



Useful dashboards with detailed statistics



Search quota in the social media database



Analytical reports compiled by our experts*

2)

Search quota in the dark web database



Presentations and Q&A sessions with experts



Takedown requests*



Threat alerts in Threat Intelligence Portal



Machine-readable data

Kaspersky Threat Intelligence Portal		(Q Search					Dark 🦲 Light	
Seitch account General	Dashboard								
Q Tenant center	Threats				Asset				
82 Home	Setting up the period threat Week Month Year All period	Customize period (1Apr	2024 - 31 Apr 2024		Distribution of assets by status		Distribution of assets by source		
Reporting Threat Analysis Digital Footprint	Distribution of the threat risk level	Critical		8	137 Total			05	
Dashboard Threats Asset managment	29	 ніgh 6 міло 5 	▲ Medium	5	Confirmed	95			
Tenant Center 와. WHOIS Tracking ~ 용 Threat Infrastructure Track	Threat notifications received for all time Distribution of threat categories				Pending Rejected	22 10 137	Lusers	95 10 105	
 Data feeds 型 What's New and Upcoming ● News 	Vulnersbilly Malware Person Leakage Davinet Show more		8 8	12	Distribution of assets by categor keyword IP(rdyne) UP Range	pry		a A A	
	Threat schedule by notification recei	pt date		30 28 Jan 2024	Domain Show more		8		
ED 9 ⊂ ⊗ User_name					Top 10 objects assets				
		300123			Lorem ipsum is placeholder Lorem ipsum is placeholder		6 Lorem ipsum is placeholo Corem ipsum is placeholo		
					3 Lorem ipsum is placeholder tex Lorem ipsum is placeholder tex Lorem ipsum is placeholder tex				
		28 29	30 31	10					

Threat types

Kaspersky Digital Footprint Intelligence empowers organizations to rapidly and efficiently respond to potential threats with real-time alerts. It reduces the likelihood of harm to brand reputation, customer trust, and overall business operations. Companies can customize the service's monitoring capabilities to meet their specific needs, and comprehensive reporting and analytics offer valuable insights into the scope and impact of brand infringement and other potential risks.

Network perimeter-related threats

- Misconfigured network services
- Identification of vulnerabilities
- Defaced or compromised resources

Data leakages

- Compromised corporate resources
- Compromised credit cards
- Compromised credentials

Dark web-related threats

- Fraud schemes and cybercriminals' plans
- Data breach sale
- Insider activities

Malware-related threats

- Phishing attacks
- Targeted attacks
- APT campaigns

Intelligence sources

It's essential that our customers have a comprehensive understanding of their external security posture. To provide this information, Kaspersky security analysts collect and aggregate information from the following intelligence sources:



- IP addresses
- Company domains
- Brand names
- Keywords
- Network ranges
- BIN/IIN card numbers
- Employee information

Network perimeter inventory

Surface, deep and dark web search

Kaspersky Knowledge Base search Threat alerts

Real-time search across Kaspersky's, surface and dark web sources

Takedown requests*

Analytical reports*

Service delivery capabilities

Digital Footprint Intelligence provides advanced capabilities for managed security service providers (MSSPs) and large multi-branch organizations.

Kaspersky Threat Intelligence Portal interface, through which DFI service is provided, allows MSSPs to differentiate access to information related either to subsidiaries of large organizations or to individual organizations to which MSSP provides security management services.

Creation of separate tenants and access control configuration through administration panel

Management is accomplished by creating tenants - logical entities created for each new structure, which must be managed separately from the others.



Access control by API token and TOTP

Capability to change tenant licenses

Switch account	Access control	
3 Home	Account	
🖞 Threat Landscape 🛛 🗸	Tenant quota 5 _{/10} Expired API token 1 Expires soon API token 1 Current API token 1 None API token	2
C Threat Lookup 🗸	+ Add tenant 🕆 Delete tenant 🗠 Request token 🕹 Download API token Search by name	٩
) Reporting	Date	ctions
Digital Footprint ~	12 July 2023 11:48 Tenant1 1 API Token Lorem ipsum is placeholder text commonly used in th_ Expiration date Current (29 Feb 2024	0 🖻
WHOIS Tracking V	7 Jun 2023 09:27 Tenant 2 Lorem ipsum is placeholder text commonly used in th Expiration date Expired 02 Feb 2024	0 🖻
Threat Infrastructure Track Data feeds	6 July 2023 11:48 Tenant 3 Lorem ipsum is placeholder text commonly used in th Expiration date Expires soon 16 Feb 2024	0 0
What's New and Upcoming	6 July 2023 13:54 Tenant 4 1 API Token – Lorem ipsum is placeholder text commonly used in th Expiration date None API token	0 🖻
) News	4 Jun 2023 09:27 Tenant 5 Lorem ipsum is placeholder text commonly used in th Expiration date None API token	0 🖻
	Total 5 < 1 > 10/page	• ~
ш <u>9</u> Ф		
) User_name		

Centralized statistics on each tenant's threats and assets

Providing the service to a large number of organizations, it is necessary to have tools for monitoring the current state of tenants. Tenant Center displays summary for each tenant, including number of detected threats with their criticality level, as well as information on the assets that tenant would like to monitor and their statuses.

Kaspersky Threat Intelligence Portal	Q Search					Dark 🚺 Ligi
Switch account	Tenant center					
Home	Day Week Month Year	All period Custom	Range < 05 Feb 2024	×	>	
 Threat Landscape	В зависимости от выбора даты количество а	ассетов не изменяется				
↓ Threat Lookup V	Threats Critical 1 High O	Medium 1	Low 1 Info	Assets 3 Confirmed	5 Pending 5	Rejected 5
Reporting	Q Search by name					
Threat Analysis	- Genericy ridille					
	Name	Threats ≑	Details of Threats	\$ Assets	Details of Assets	÷
	Tenant1	2		17	2 10 5	
Dashboard	Tenant 2	2	0 0 0 1 1	13	1 7 5	
Threats	Tenant 3	0	0 0 0 0 0	8	1 3 4	
Asset managment	Tenant 4	2	0 0 1 0 1	4	0 2 2	
Tenant Center	Tenant 5	0	0 0 0 0 0	4	121	
A WHOIS Tracking ∽	Total 5				< 1 >	10 / page 🗸
B Threat Infrastructure Track						
Data feeds						
] What's New and Upcoming						
) News						
ш <u> </u>						
User_name						

Detailed monitoring

MSSP or head office can view a detailed summary for each tenant:

- The total number of threats identified over a given period and their criticality to the organization
- Categorization of detected threats
- The most vulnerable tenant's assetsThreat landscape changing over time

Kaspersky Threat Intelligence Portal	Q Search								Dark 🚺
~	Dashboard								
Home									
Q, Threat Lookup V	Threats					Assets			
🕫 Research Graph									
Reporting	Select the time period					Distribution of assets by st	atus	Distribution of assets by so	ource
Threat Analysis	Week Month Year All time C	Custom range	Start	— End					
Digital Footprint						12 Total		12 Total	
Dashboard	Threat risk level distribution					Total		Total	
Threats		Critical			9				
Asset management		🔶 High	11	A Medium	9	Pending	8		
WHOIS Tracking ~	39					Confirmed	3	Experts	0
B APT C&C Tracking	Threat notifications received for all time	Info	3	Low Low	7	A Rejected	1	🛓 Users	12
Data Feeds						(()	12	()	12
] What's New and Upcoming	Distribution of threats by category								
	Vulnerability				18	Distribution of assets by ca	tegory		
News	Compromised account	8				Domain			9
	Malware	6				Company/brand name	2		
	Leakage 2					IP range	1		
ш 9 Ф	Dark web 2								
پ وہ ت	Show more								
						Top risks			

Asset management

Tenant is able to add new assets for monitoring both separately via Kaspersky Threat Intelligence Portal interface and by uploading files with a large amount of assets. This approach essentially simplifies the process of keeping assets up-to-date.

Kaspersky Threat Intelligence Portal	Q Search					Dark 🚺 Li	
Switch account General	Asset managemen		natically our overste wil	I touto add accate from			
88 Home	this field to the search. For more informatio			ruy to add assets from			
∠ Threat Landscape ∨							
Q Threat Lookup 🗸	Submitted files with assets					∧ Hide all	
Reporting	+ Add file						
Threat Analysis	+ Add file						
Digital Footprint	Submitted 💠 File			\$ Status		\$	
	4 Mar 2024 12:20 Name file.json	,	Pending vi	Pending validation			
Dashboard			-	-			
Threats	4 Mar 2024 12:20 Name file3			\rm A Rejected			
Asset managment	15 Jan 2024 14:50 Name_2.json			Confirmed	I		
Tenant Center	Total 3				< 1 ÷	10 / page 🗸 🗸	
E9. WHOIS Tracking ~							
Threat Infrastructure Track	All assets						
Data feeds							
S What's New and Upcoming	+ Add 🗇 Delete						
⊕ News	Asset	Category St	atus	Role in monitoring	Status details	Source	
	test_asset	Keywords	Confirmed	Include	_	Name file.json	
	test_asset	Keywords 🔒	Rejected	Include	Processed by test_user	Submitted by user	
ш <u>9</u> Ф	test_asset	Keywords >	Pending validation	Include	-	Submitted by user	
Ø User_name	test_asset	Keywords	Pending validation	Include	-	Submitted by user	

Business values

Kaspersky Digital Footprint Intelligence delivers powerful benefits and significant value to your organization:



Protects your brand

Detect potential threats in real-time to protect your brand reputation, preserve customer trust, reduce the risk of financial loss and damage to business operations.



Reduce cyber risks

Equip your key stake holders (CxO and Board) with information on where to focus cybersecurity spending by revealing gaps in the current setup and the risks they bring.



React faster

Additional context for security alerts improves incident response and reduces your Mean Time To Respond (MTTR).



Reduce the attack surface

Manage your company's digital presence and control external network resources to minimize attack vectors and vulnerabilities that can be used for an attack.



Understand your adversaries

Forewarned is forearmed – know what cybercriminals are planning and discussing about your company on the dark web so that you're prepared for it.



Know the unknown

Improve your ability to withstand cyberattacks and identify threats outside the jurisdiction of your internal security teams.



Service delivery efficiency

Rapid start and easy scaling in multitenancy mode saves time both for managed security service providers (MSSP) and their customers, as well as large multi-affiliate organizations.

To find out more about the various subscription plans, please get in touch with our team

Get in touch



Kaspersky Digital Footprint Intelligence

Learn more

www.kaspersky.com

© 2024 AO Kaspersky Lab. Registered trademarks and service marks are the property of their respective owners. #kaspersky #bringonthefuture