Kaspersky Threat Intelligence

資安情資運用例分享

卡巴斯基 台灣技術總監
謝長軒 Chandler Hsieh
chandler.hsieh@kaspersky.com

kaspersky

威脅的趨勢及挑戰

供應鏈攻擊趨勢增加

241 npm and PyPI packages caught dropping Linux cryptominers

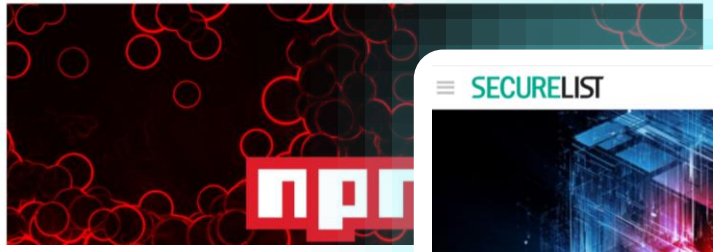
By Ax Sharma

August 19, 2022 04:11 PM 0

NPM supply-chain attack impacts hundreds of websites and apps

By Sergiu Gatlan

July 5, 2022 01:55 PM 2



Python library 'ctx' uploads secrets to

Heavily downloaded PyPI package 'ctx' has been compron
published versions exfiltrating your environment variable

'ctx' is a minimal Python module that lets developers man
variety of ways. The package, although popular, had not b
seen by BleepingComputer. However, newer versions eme
contained malicious code:

SECURELIST

INCIDENTS

LofyLife: malicious npm packages steal Discord tokens and bank card data

28 JUL 2022 1 minute read

Not just an infostealer: Gopuram backdoor deployed through 3CX supply chain attack

APT REPORTS 03 APR 2023 4 minute read

GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Bala
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM
GReAT Ideas. Gree
JOHN HULTQUIST, BRIAN BARTHO
SUGURU ISHIMARU, VITALY KAML
YUSUKE NIWA, MOTOHIKO SATO

XZ backdoor story – Initial analysis

INCIDENTS 12 APR 2024 12 minute read

// AUTHORS

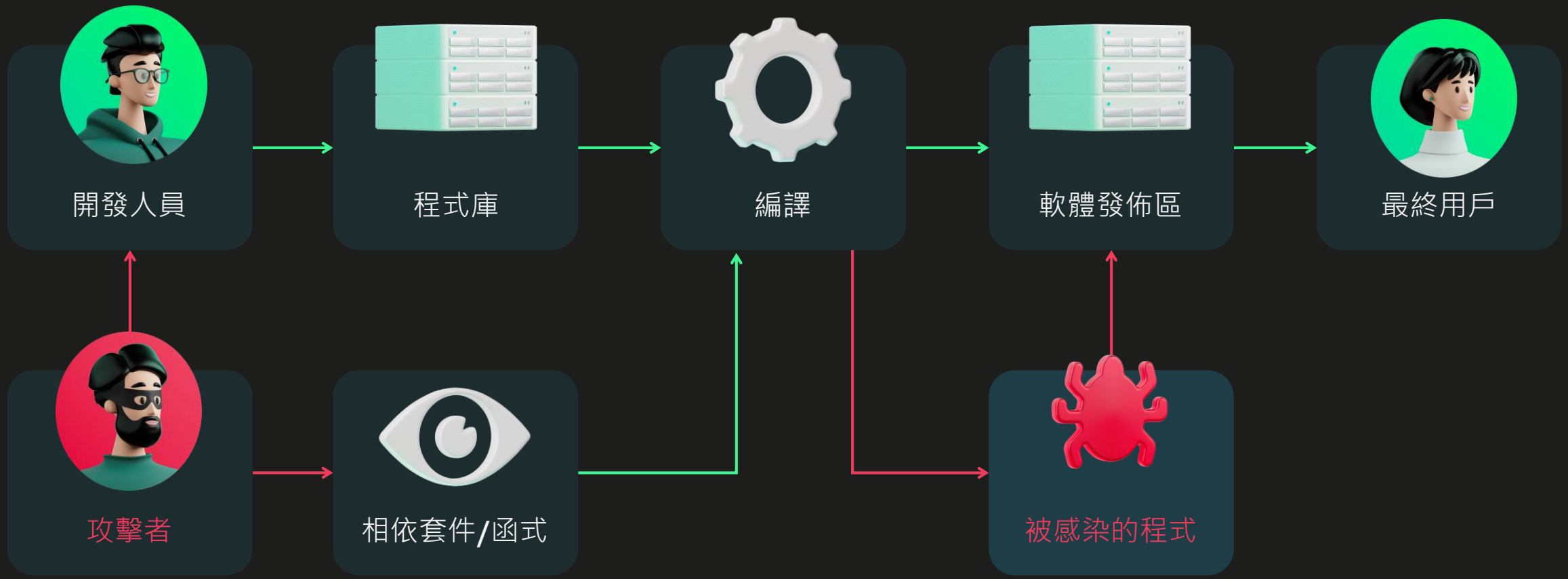
GREAT

On March 29, 2024, a single message on the Openwall OSS-security mailing list marked an important discovery for the information security, open source and Linux communities: the discovery of a malicious backdoor in XZ. XZ is a compression utility integrated into many popular distributions of Linux.

Two more malicious Python packages in the PyPI

INCIDENTS 16 AUG 2022 4 minute read

標準軟體供應鏈攻擊流程

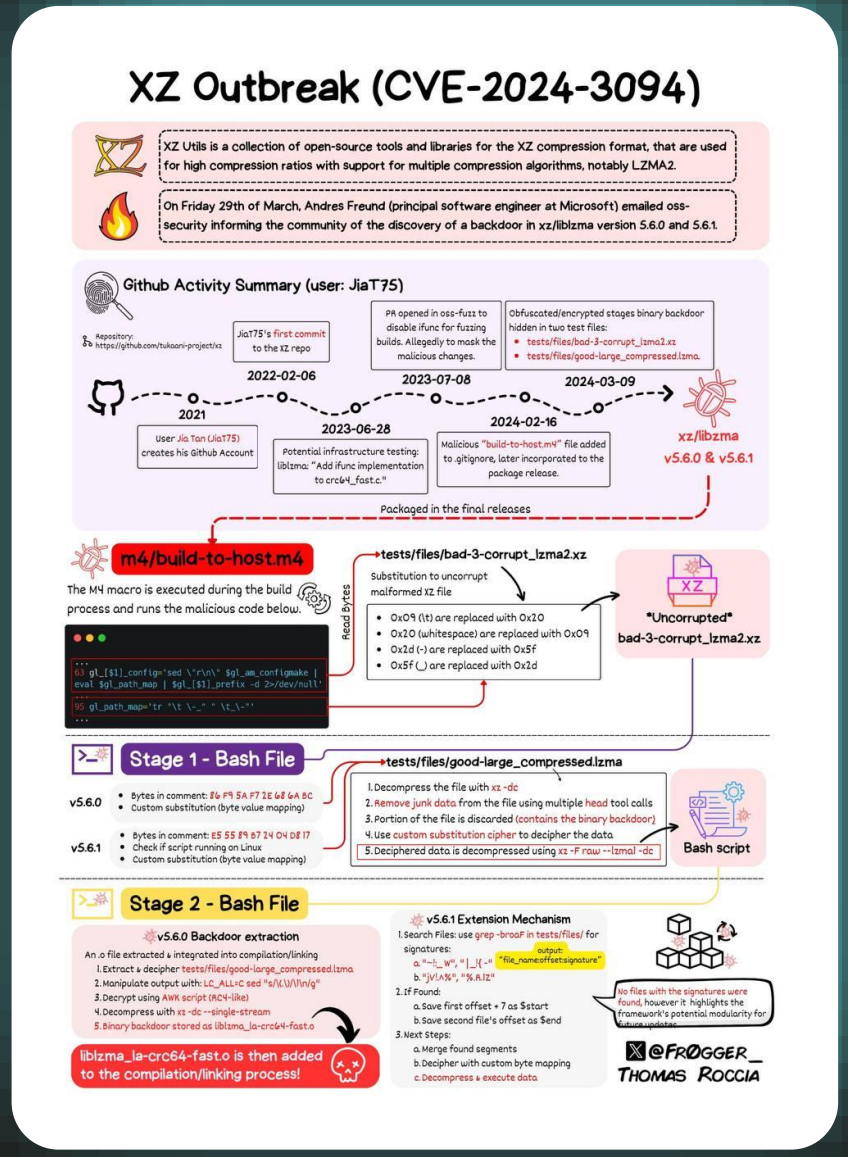


XZ案例

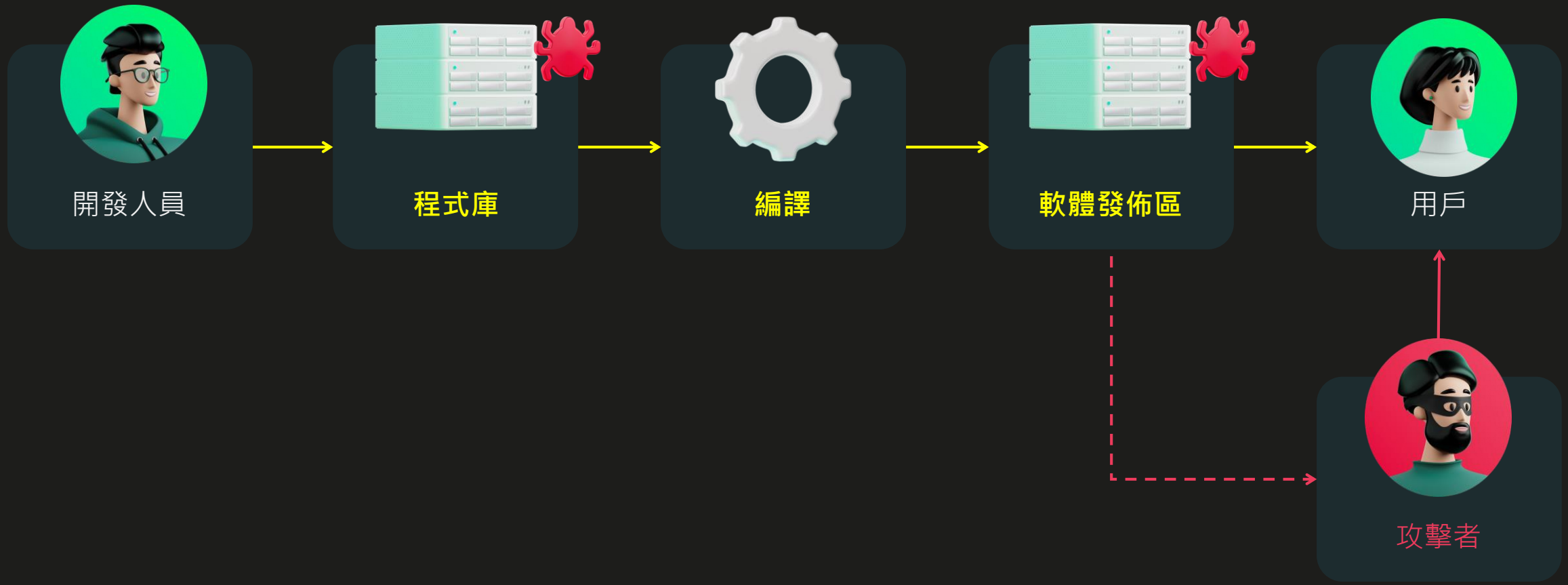
一個常被使用的Linux函式庫發起的供應鏈攻擊

通過幾年的社交工程...等手段

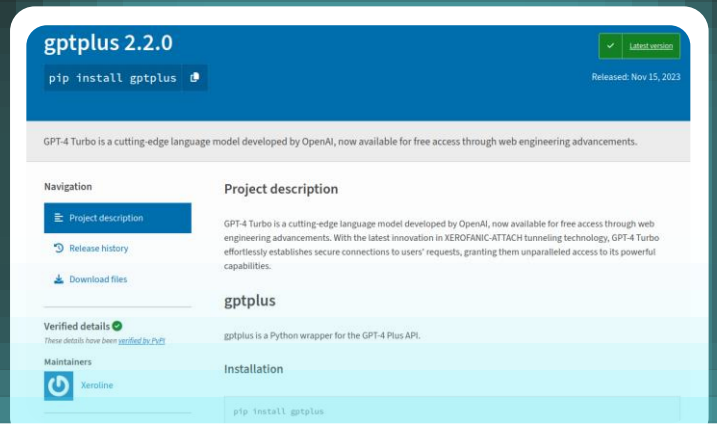
攻擊者具有非常專業的惡意軟體開發和社交工程技能



常見的**供應鏈攻擊**



用於 ChatGPT/DeepSeek 的假站台及惡意軟體



Kaspersky uncovers year-long PyPI supply chain attack using AI chatbot tools as lure

November 20, 2024

一年来，JarkaStealer 以 AI 工具的名義在 PyPI 庫上分發

至少 30 個國家/地區的用戶下載了超過 1700 次的軟體

該惡意軟體會竊取瀏器記錄、截取屏幕截圖及收集 Telegram 對話記錄

卡巴斯基對軟體供應鏈的應用

開源軟體威脅資料

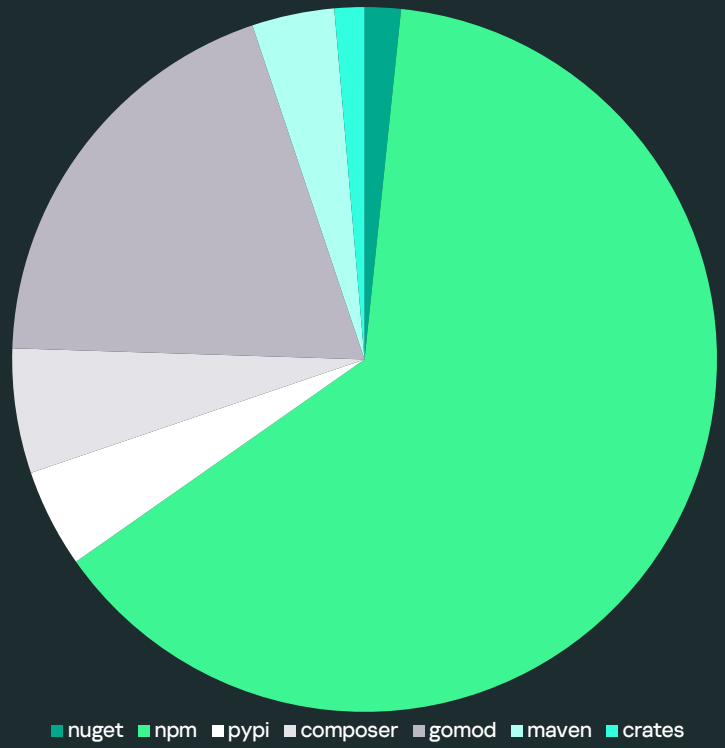
漏洞及 CVE 信息

被篡改的程式庫

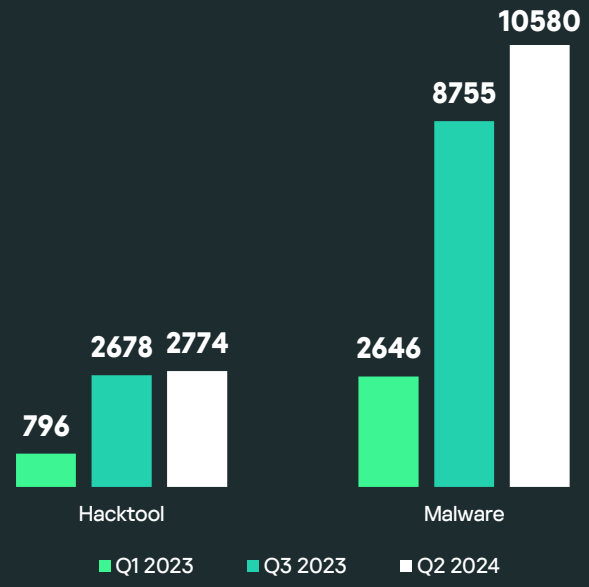
含有惡意軟體的程式庫

風險軟體及駭客工具

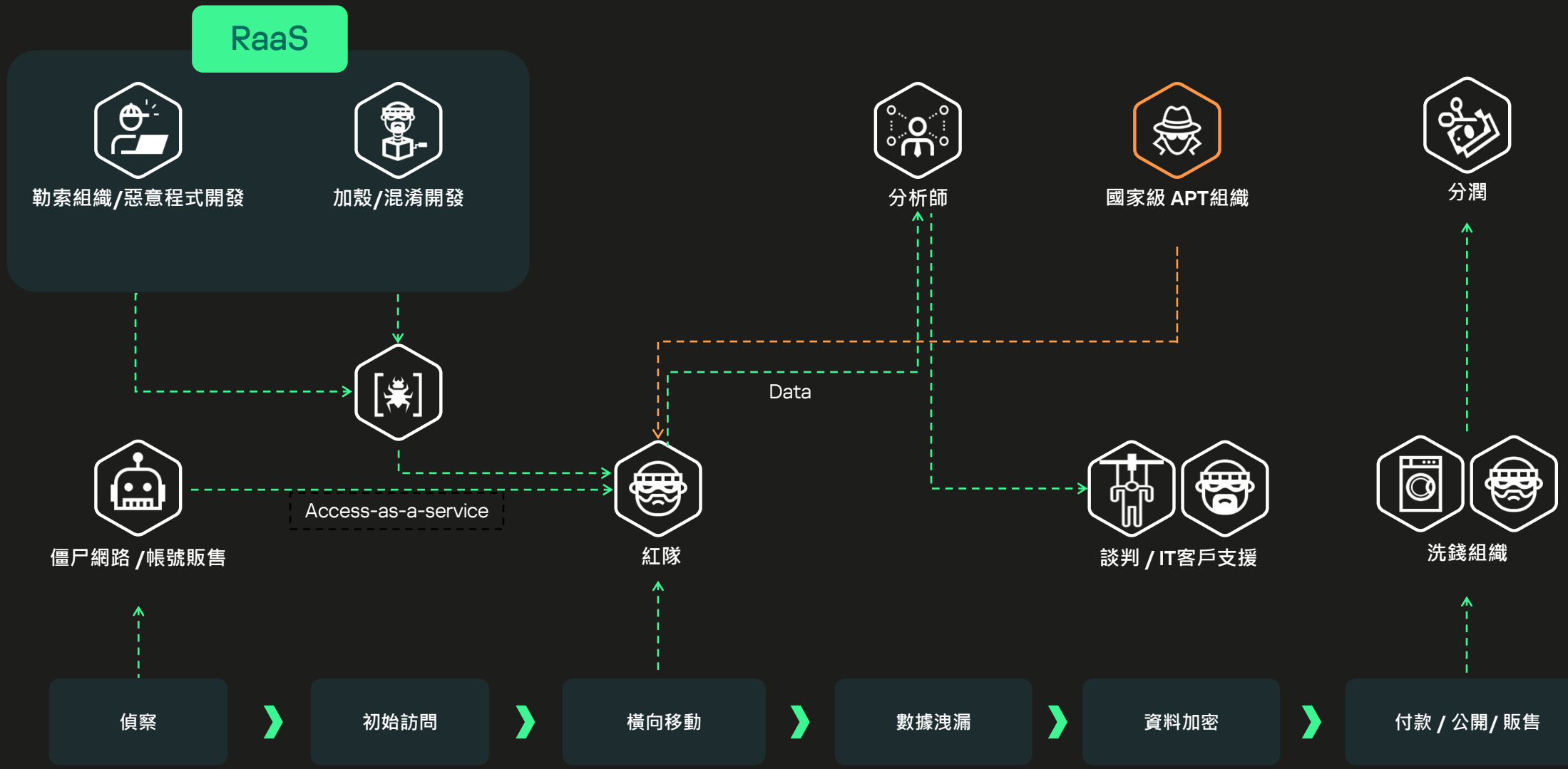
開源程式庫



開源程式威脅趨勢



勒索軟體"生態圈"


RaaS
勒索組織/惡意程式開發
加殼/混淆開發
分析師
國家級 APT組織
分潤
Data
Access-as-a-service
僵尸網路 /帳號販售
紅隊
談判 / IT客戶支援
洗錢組織
偵察
初始訪問
橫向移動
數據洩漏
資料加密
付款 / 公開/ 販售

針對式攻擊

適應性

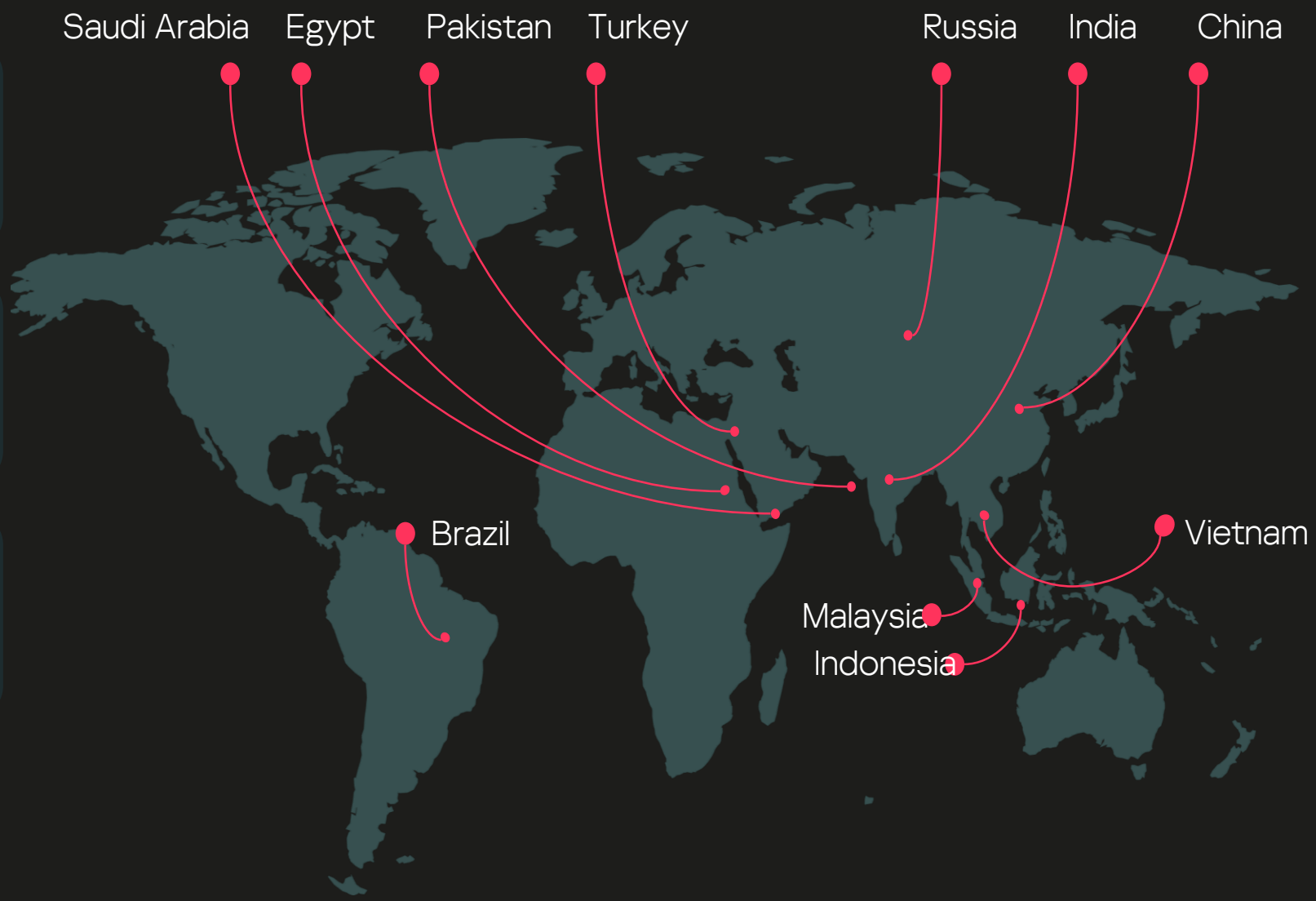
攻擊方繞過防護機制而調整方法和工具的能力

隱匿性

攻擊者設計攻擊手法以儘可能不被受害者發現的能力

複雜性

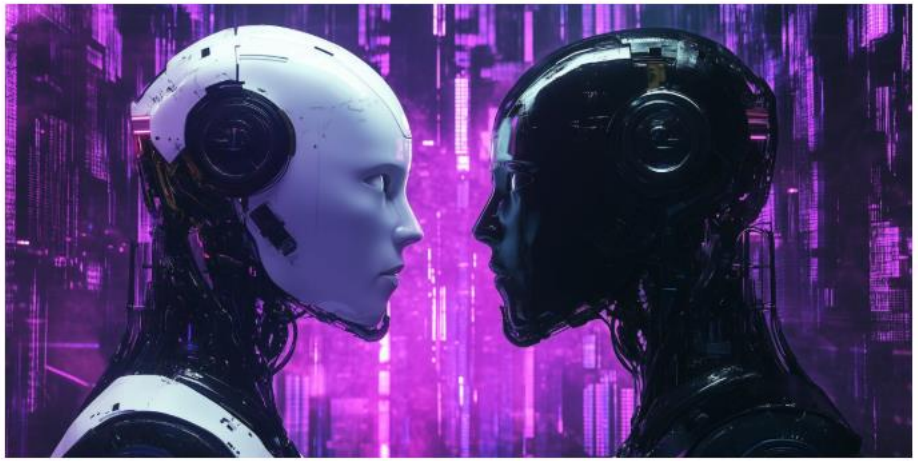
攻擊者使用進階技術和工具來規避并進行攻擊



更多利用合法軟體掩護的攻擊手法 - 針對這類手法持續的追蹤及揭露

How ToddyCat tried to hide behind AV software

INCIDENTS 07 APR 2025 6 minute read



// AUTHORS

ANDREY GUNKIN

To hide their activity in infected systems, APT groups resort to various techniques to bypass defenses. Most of these techniques are well known and detectable by both EPP solutions and EDR threat-monitoring and response tools. For example, to hide their activity in Windows systems, cybercriminals can use kernel-level rootkits, in particular malicious drivers. However, in the latest

Date	Group	Report ID	Report	Tags
28 Mar 2025	APT	231cbe27-e370-4...	Organizations in CIS are attacked with ShadowPad	Financi

We detected a set of attacks that took place in April 2024 - January 2025, targeting governmental entities and private companies in Russia and Kyrgyzstan. During our investigation, we found a new ShadowPad loader distributed with a set of malicious plugins. It uses DLL sideloading, imitating popular software to deploy a sophisticated RAT with a huge range of capabilities. ShadowPad is a famous RAT software popular among APT threat actors. Having originally emerged in 2017 during Netsarang attack, it has overgrown a lot of modifications and has been widely used by many APTs and crimeware groups such as PryingKomodo, APT41 and others.

Executive summary (En): base. Organizations in CIS are attacked with ShadowPad Report Id: APT-20250309 Version: 1.0 (28.March

IOC: <description>Organizations in CIS are attacked with ShadowPad</description> <authored_by>APT Reports</authored_by>

YARA Rule: meta: descrition = "Loader to detect shadowpad modules orchestrator" author = "Kaspersky"

Report (En): meta: descrition = "Loader to detect shadowpad modules orchestrator" author = "Kaspersky"

Download: YARA Rule IOC Executive summary (En) Report (En)

Overview

Hits	≈ 1,000	Size	103.50 KB (105984 B)	Signed by	—
Format	dll x64	Packed by	—	Signature trust	—

First seen Jun 4 2023 05:25
Last seen Apr 15 2025 05:54

MD5 E0D17318B6BEED1DDCEB23DC980EF58B
SHA1 E4082EFB01BD906AB1DC012B15458D33F6C8E22B
SHA256 D807F8E2A885E823A7585E9EFBCFBCEBF56FE9222EA1AC025AFF8DF99BDBE3F6

Categories APT
Reports Flash Report – ScatterBrain variant of ShadowPad used in attacks on organizations in APAC and Latin America
Data Feeds APT Hash Data Feed | Go to Data Feeds
Industries —

AC and Latin

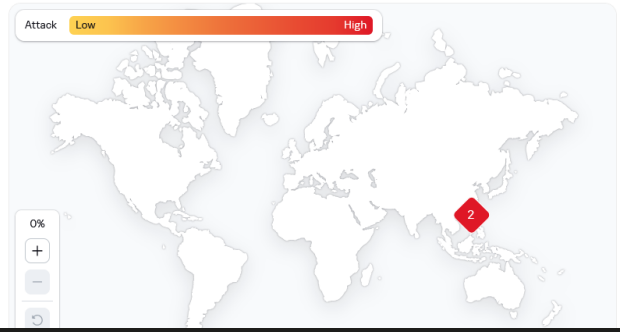
rs using the
y PwC. However,
fuscator, an
amples have been
erica regions. This
ttacks.
adowPad has

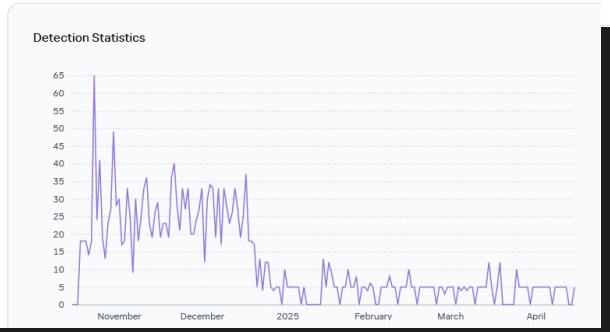
tions in APAC and

ersky"
s utilized the

Argenti
India
Mongol
Taiwan

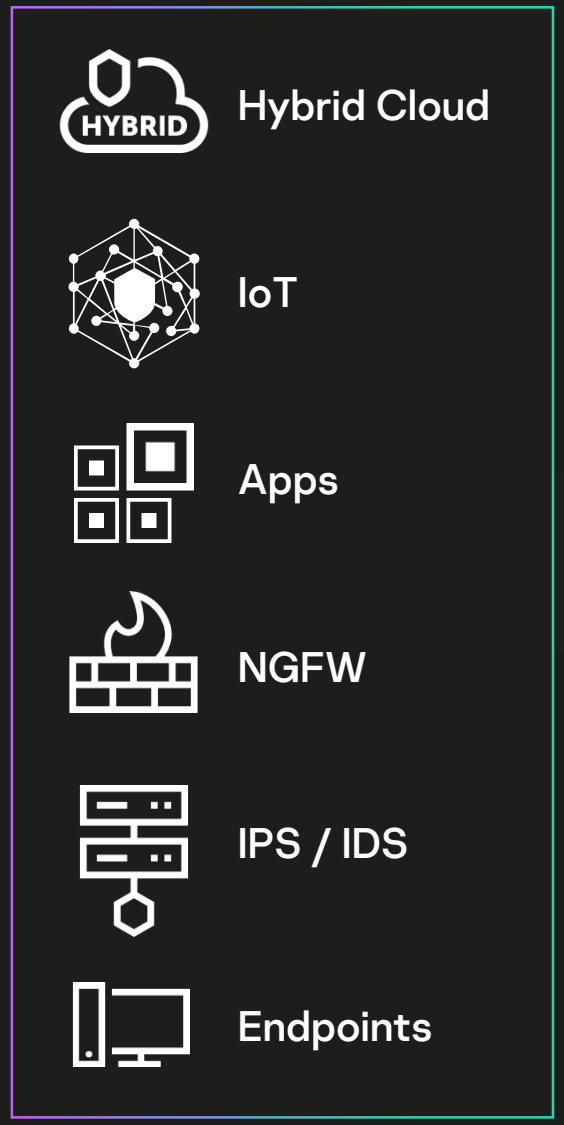
Statistics





為何需要安全威脅情報

不斷變化的網路安全挑戰

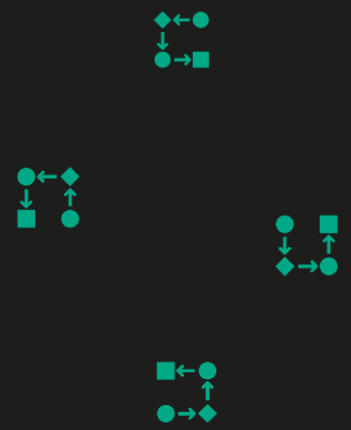


- 來自不同的安全技術造成安全警報的優先順序不明確
- 缺乏專業分析師與員工流動率上升
- 事件響應效率低下，導致恢復成本高
- 基礎設施內部潛伏著未被發現的威脅
- 缺乏全面的威脅概述，阻礙了有效的安全計畫規劃

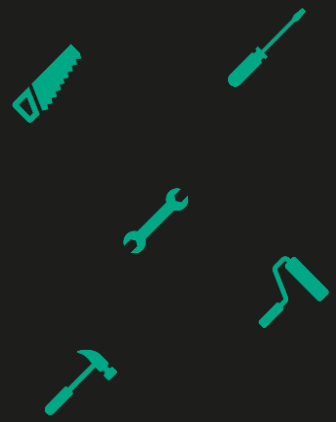
提昇 SOC/MDR 團隊響應及調查速度

人員

流程



技術/工具



提昇 SOC/MDR 團隊響應及調查速度

威脅情報常用場景 - Anywhere

Plan

戰略情報，有助於識別易受攻擊的薄弱環節，並為整體資訊安全策略的制定提供依據

Detect

機器可讀的威脅情報可透過與現有安全控制系統的整合，加快威脅偵測的速度

Respond

下架惡意與網路釣魚網域、假冒的社群帳號以及行動應用程式商店中的假應用，有助於降低針對企業及其品牌的威脅。

Investigate

線上可搜尋的威脅情報、合法物件及其各種關聯性的資料庫，有助於加快事件調查與應對的速度。

威脅情報分類

Tactical

低層級且時效性高的資訊，用於支援安全營運與事件應變。戰術性情報的例子包括與新發現攻擊行為相關的指標（IOCs）

Roles:

- SOC Analyst

Systems:

- SIEM
- NGFW
- IPS
- IDS
- SOAR

Processes:

- Threat Hunting
- Monitoring

Operational

這一層級通常包含有關攻擊行動（campaigns）及較高層次的戰術、技術與程序（TTPs）的資料，也可能包含特定攻擊者的歸屬資訊，以及其能力與意圖

Roles:

- SOC L3 Analyst
- DFIR Analyst
- IR Analyst

Systems:

- SIEM
- NTA
- EDR/XDR
- TIP

Processes:

- Incident Response
- Threat Hunting

Strategic

這一層級的情報用於支援高階主管（C-level）和董事會在風險評估、資源分配及組織策略等重大決策上的判斷。此類資訊包含趨勢、攻擊者動機及其分類

Roles:

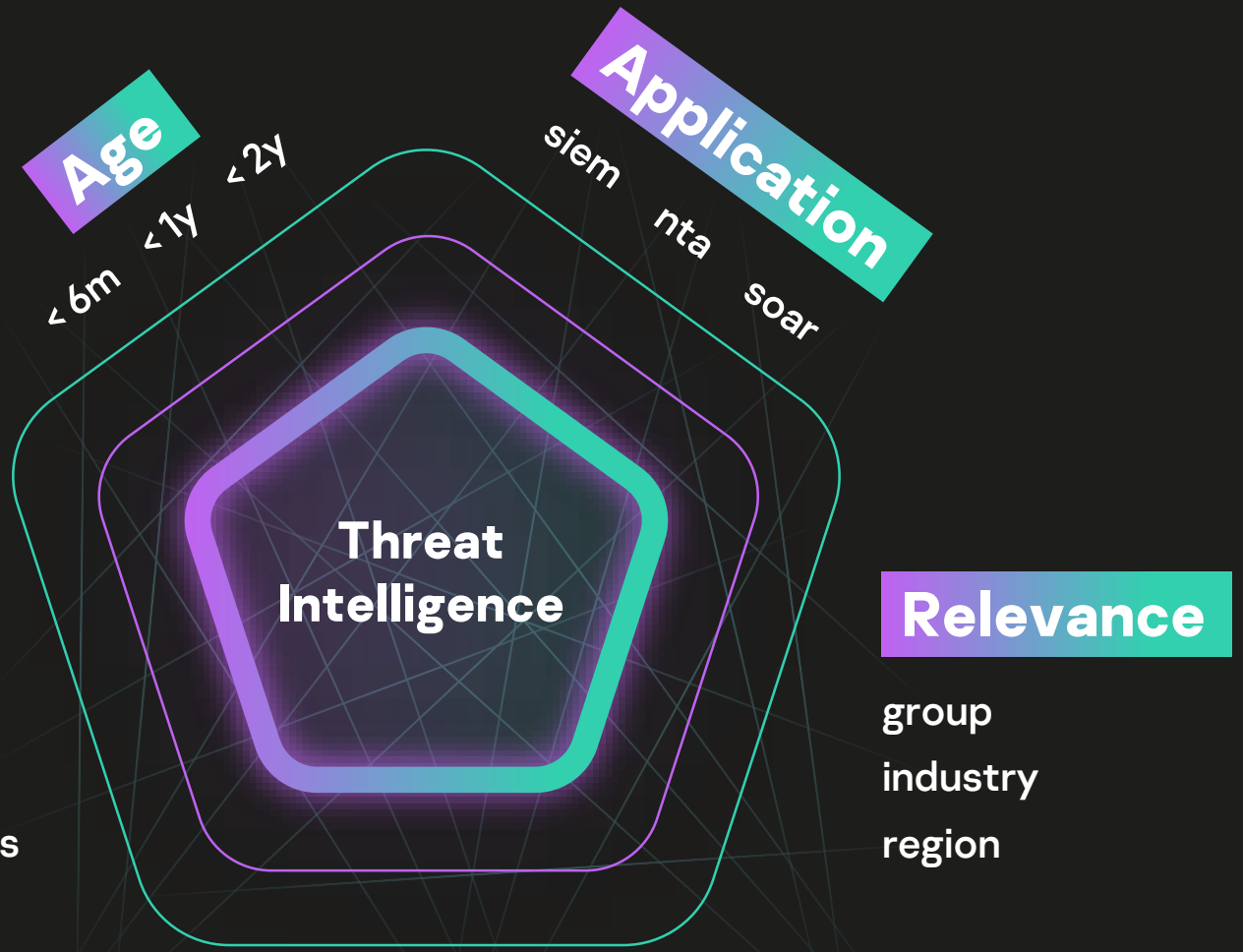
- CISO
- CTO
- CIO
- CEO

Processes:

- Building an IS strategy
- Awareness raising

如何挑選適合的安全情報

如何挑選合適的情報



IOC / IOA

domains ttps
IPs tools
hashes artifacts

Relevance

group
industry
region

Kill chain

execution persistance
initial access impact

卡巴斯基威脅情報相關服務

Machine-readable Threat Intelligence

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Threat Intelligence expert support

- Kaspersky Takedown Service
- Kaspersky Ask the Analyst

Kaspersky Threat Intelligence

- Tactical
- Operational
- Strategic

○ Available via

Kaspersky Threat Intelligence Portal

Human-readable Threat Intelligence

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - Sandbox
  - Attribution
  - Similarity
- Kaspersky Threat Intelligence Reporting
  - APT
  - Crimeware
  - ICS
- Kaspersky Threat Infrastructure Tracking

卡巴質斯基威脅情報覆蓋範圍

預防阻擋

- Threat Data Feeds
- Threat Intelligence Reports
- Digital Footprint Intelligence

偵測威脅

- Threat Data Feeds
- CyberTrace
- Threat Lookup
- Threat Intelligence Reports

威脅調查

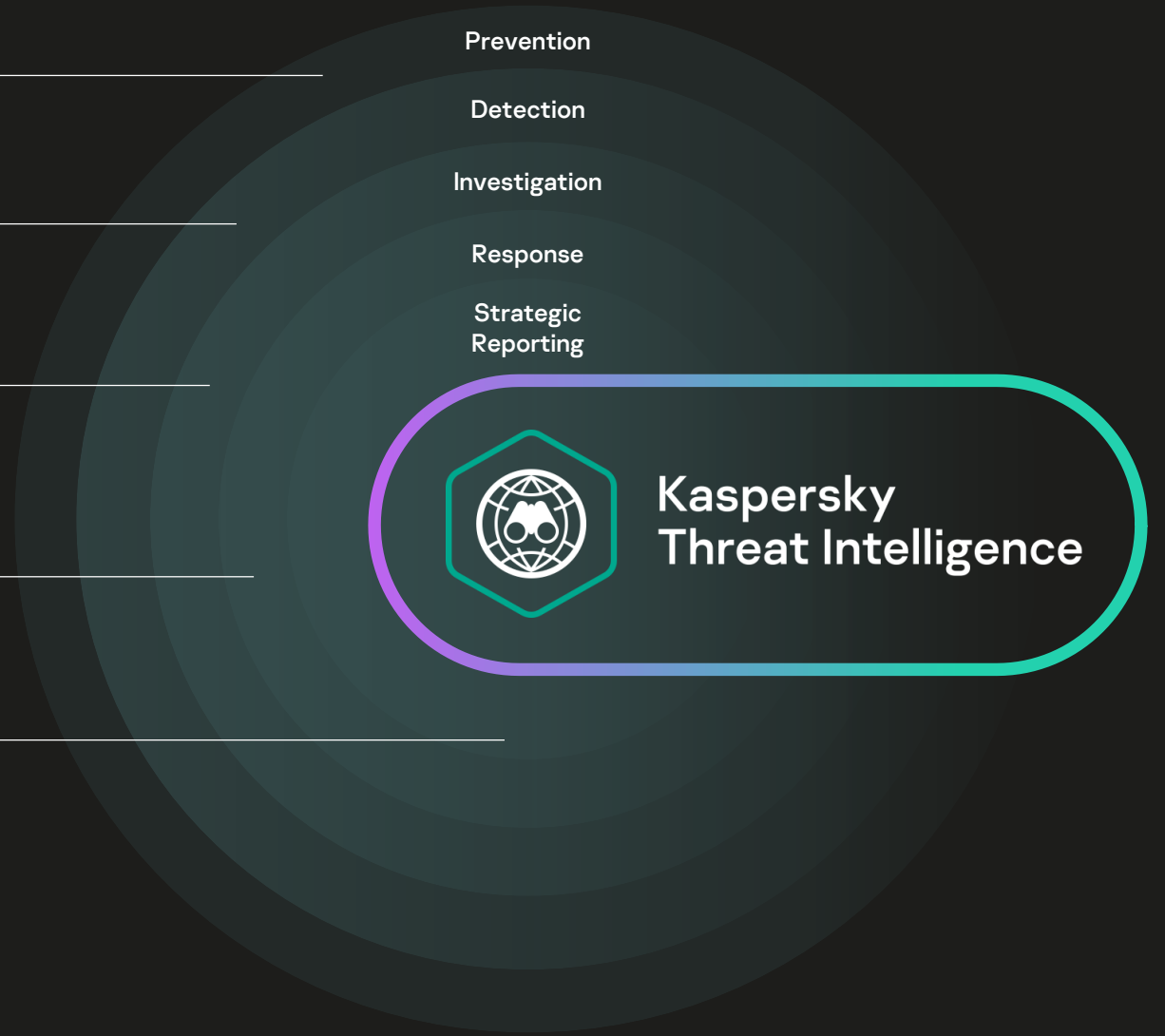
- CyberTrace
- Ask the Analyst
- Threat Lookup
- Threat Analysis
- Digital Footprint Intelligence
- Threat Intelligence Reports

威脅響應

- Ask the Analyst
- Takedown Service
- Digital Footprint Intelligence

戰略情報

- Digital Footprint Intelligence
- Threat Intelligence Reports



卡巴斯基威脅情報服務如何以及在何處增強 IT 安全能力

與 SOC 成熟度的對應

Emerged IT security capability or SOC

TIER 1
監控 及 分類

- 監控
- 事件辨識
- 基本調查及基本修正

TIER 2
控制 及 修復

- 深入調查
- 完整修正
- 調整相關政策機制

TIER 3
鑑識、獵捕 及 智能情報

- Malware analysis
- Digital forensics
- Threat intelligence
- Threat hunting

Threat Intelligence Services

- Threat Data Feeds
- CyberTrace
- Threat Lookup
- Cloud Sandbox
- APT Intelligence Reporting – IOCs and Yara rules → APT Intelligence Reporting - TTPs
- Financial TI Reporting – IOCs and Yara rules → Financial TI Reporting - TTPs
- ICS Reporting – IOCs and Yara rules → ICS Reporting- TTPs
- Digital Footprint Intelligence

Kaspersky Threat Intelligence

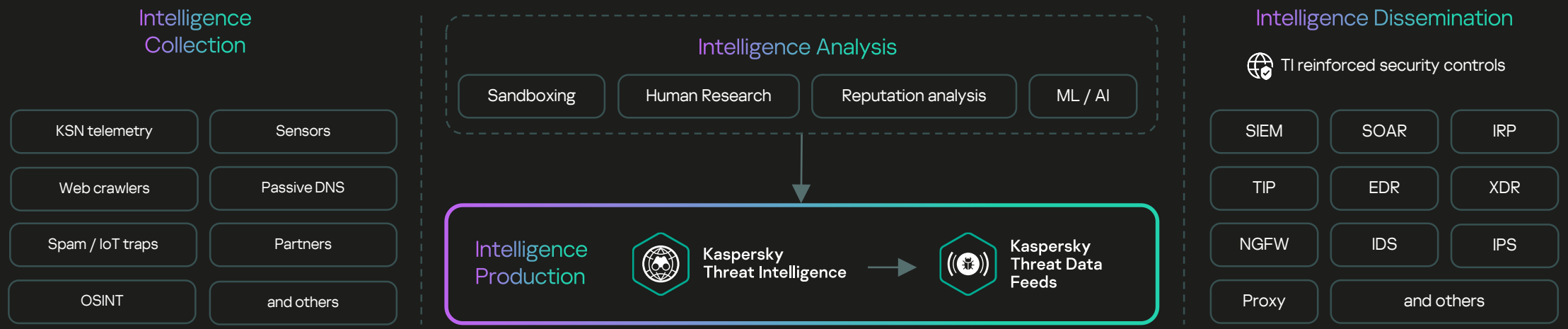
Kaspersky Threat Intelligence Portal

提供單一存取介面支援存取各種威脅情報及整合豐富相關情報的應用。

將卡巴斯基所有的安全威脅專業知識與技術整合於一處，該平台能夠利用專有的數據處理與標準化技術，監控與特定組織相關的威脅，並分析惡意軟體樣本及進行後續歸屬判定。

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds



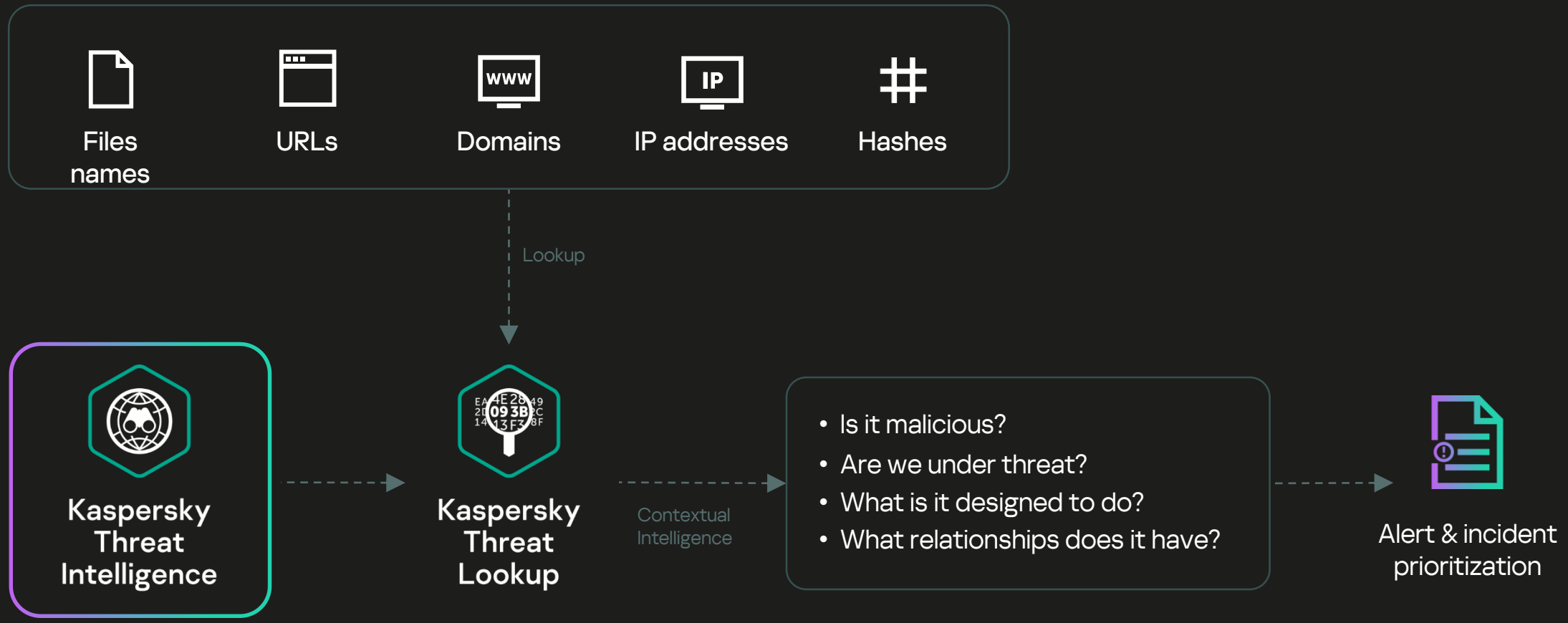
Kaspersky Threat Data Feeds

- Malicious URL Data Feed
- Ransomware URL Data Feed
- Phishing URL Data Feed
- Botnet C&C URL Data Feed
- Mobile Botnet C&C URL Data Feed
- Malicious Hash Data Feed
- Mobile Malicious Hash Data Feed
- IP Reputation Data Feed
- IoT URL Data Feed
- Vulnerability Data Feed
- ICS Vulnerability Data Feed
- **ICS Vulnerability Data Feed in OVAL format**
- ICS Hash Data Feed
- pDNS Data Feed
- Suricata Rules Data Feed
- Cloud Access Security Broker Data Feed
- **APT** Hash Data Feed
- **APT** IP Data Feed
- APT URL Data Feed
- **APT Yara Data Feed**
- **Open Source Software Threats Data Feed**
- Crimeware Hash Data Feed
- Crimeware URL Data Feed
- Crimeware Yara Data Feed

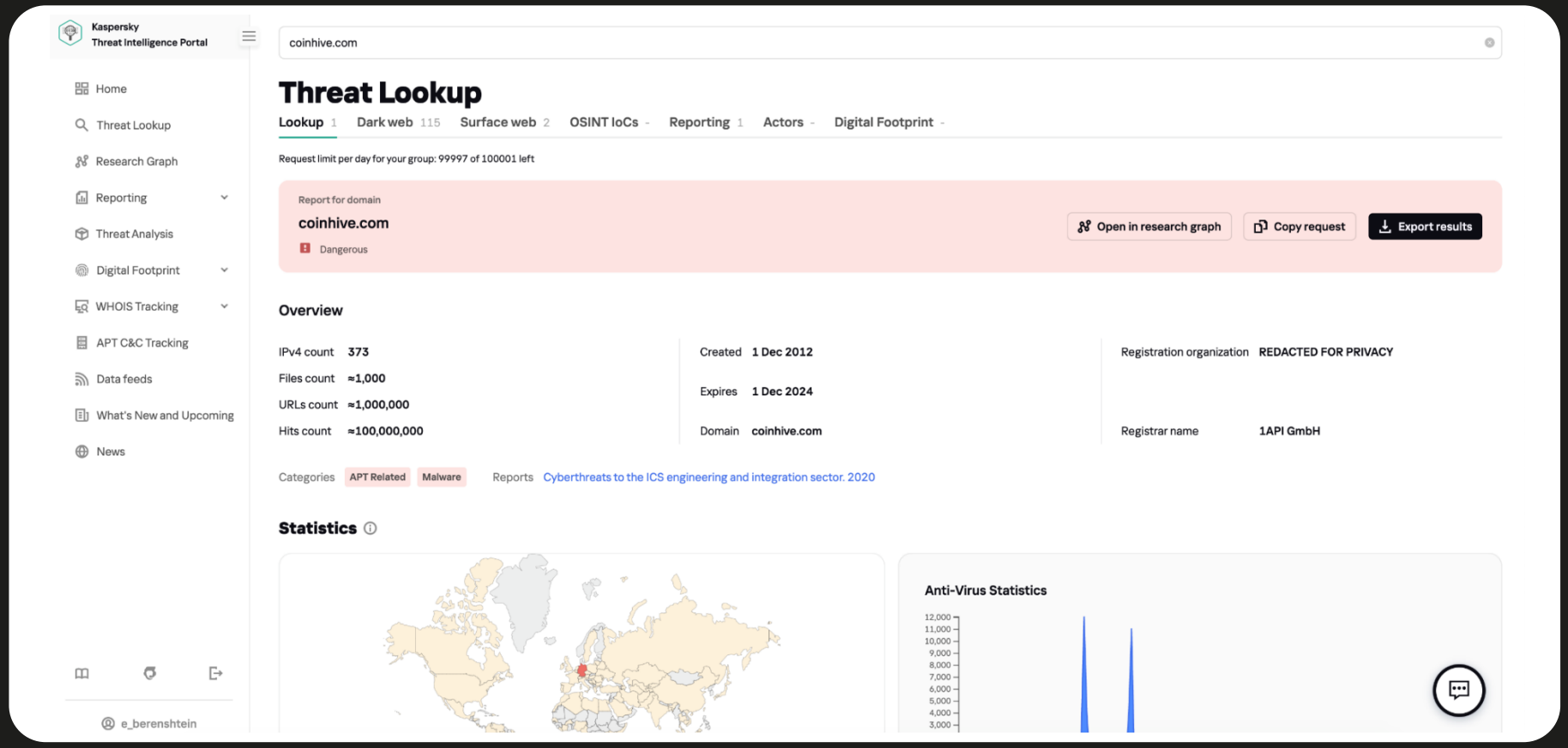
The list of data feeds is constantly expanding

Kaspersky Threat Lookup

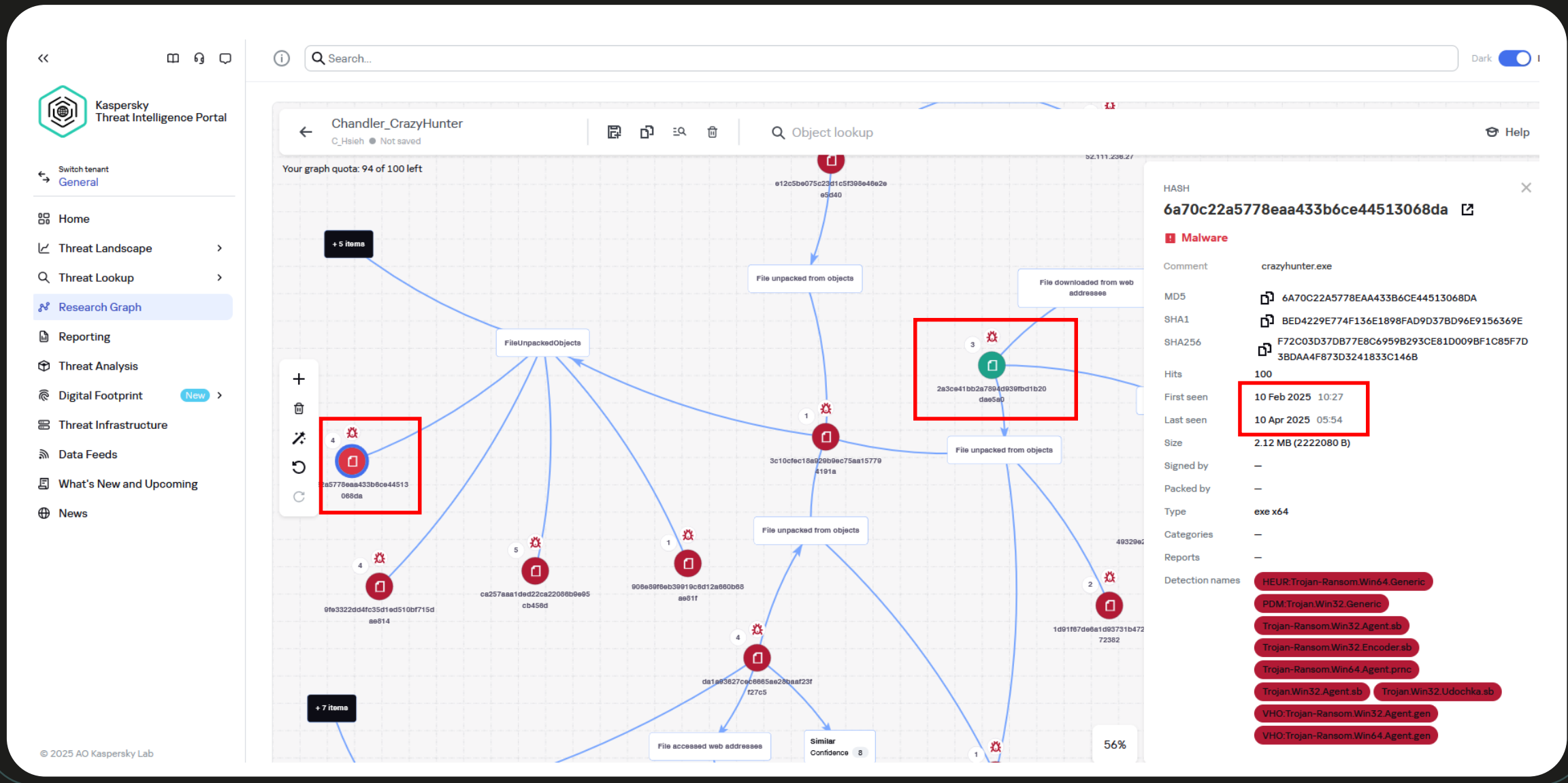
Objects to analyze



Rich contextual information



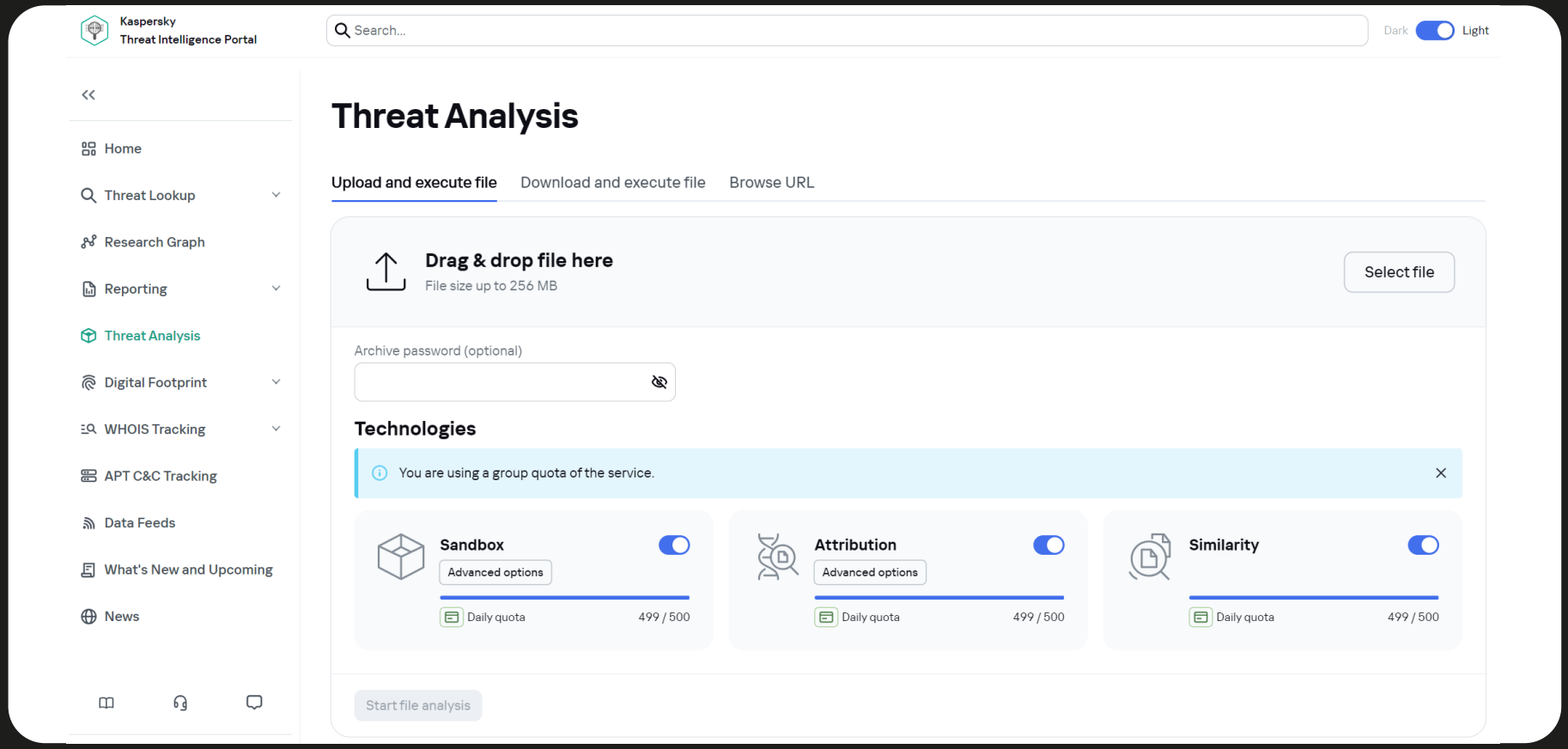
Research graph – CrazyHunter 為例



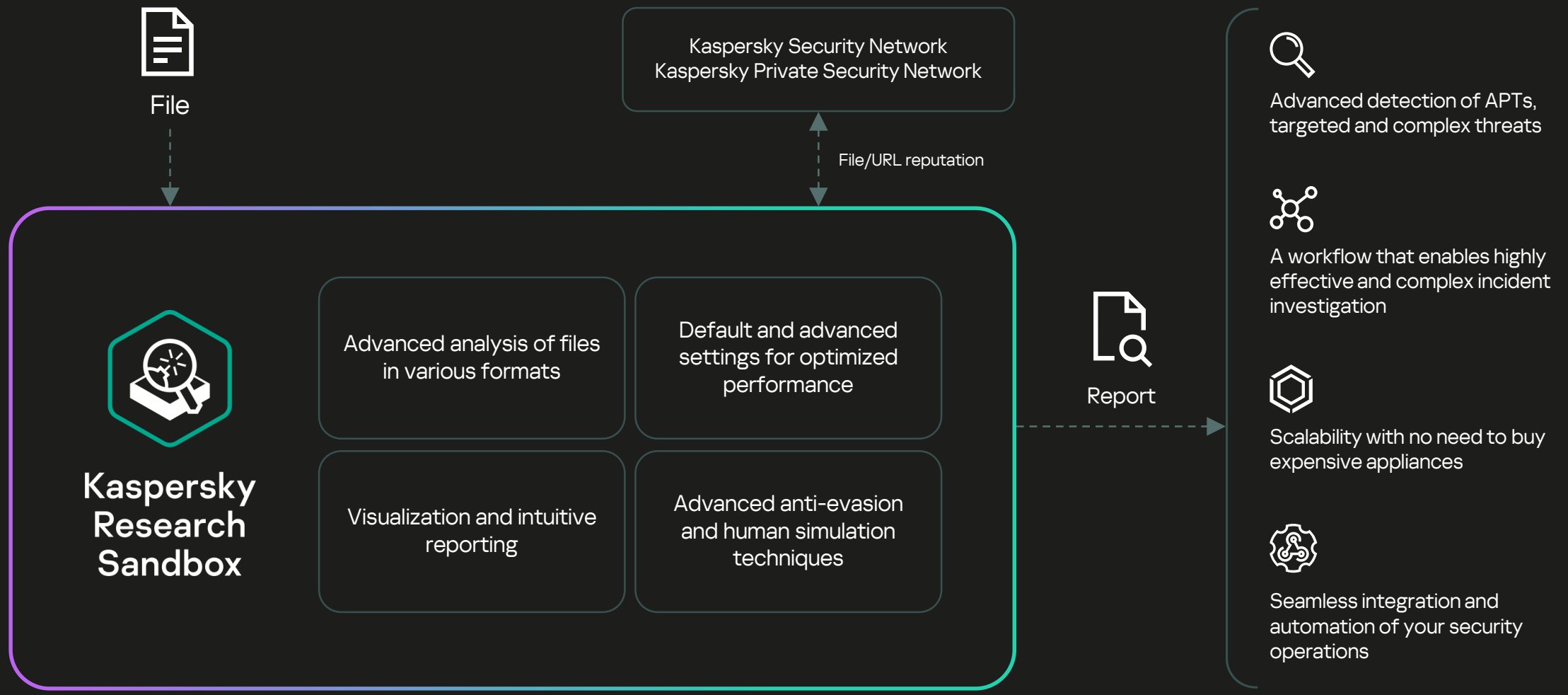
Kaspersky Threat Analysis

Single interface for complex file analysis 自動化動態分析工具

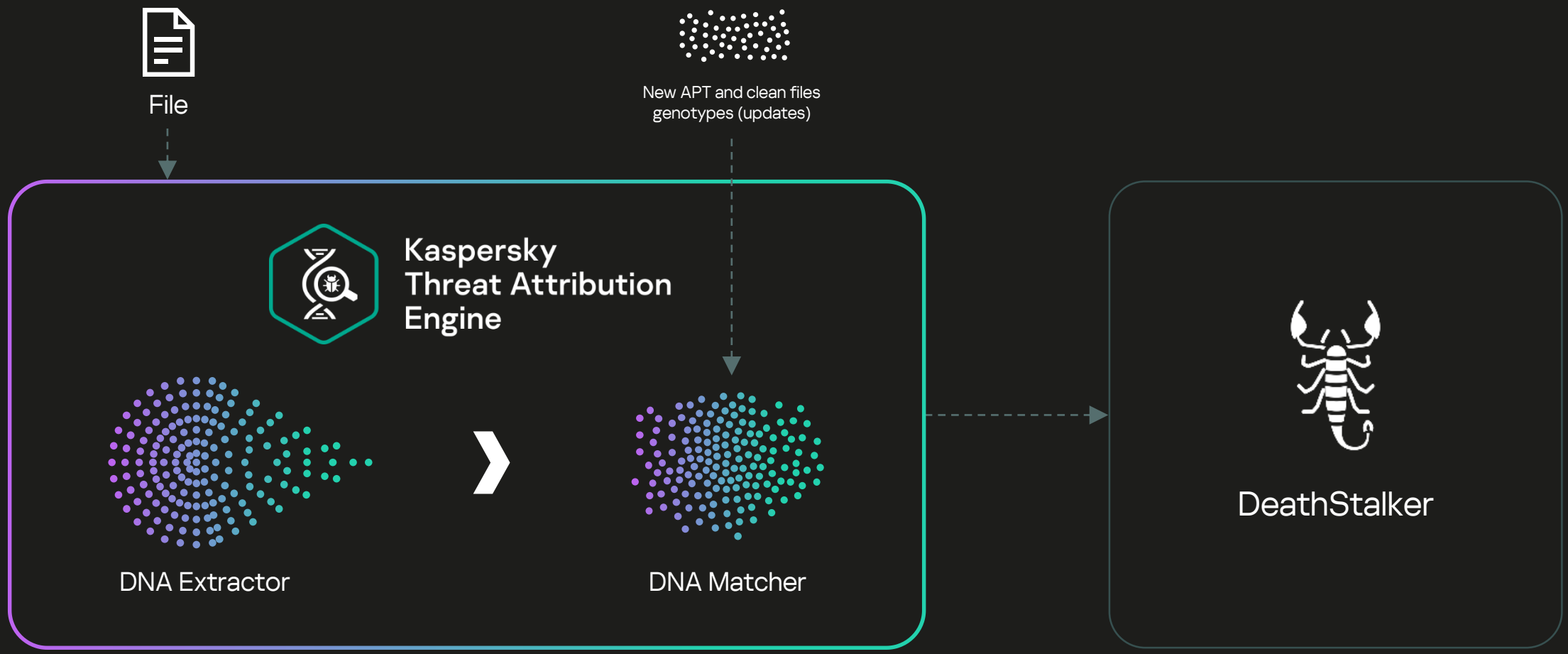
Single interface for complex file analysis



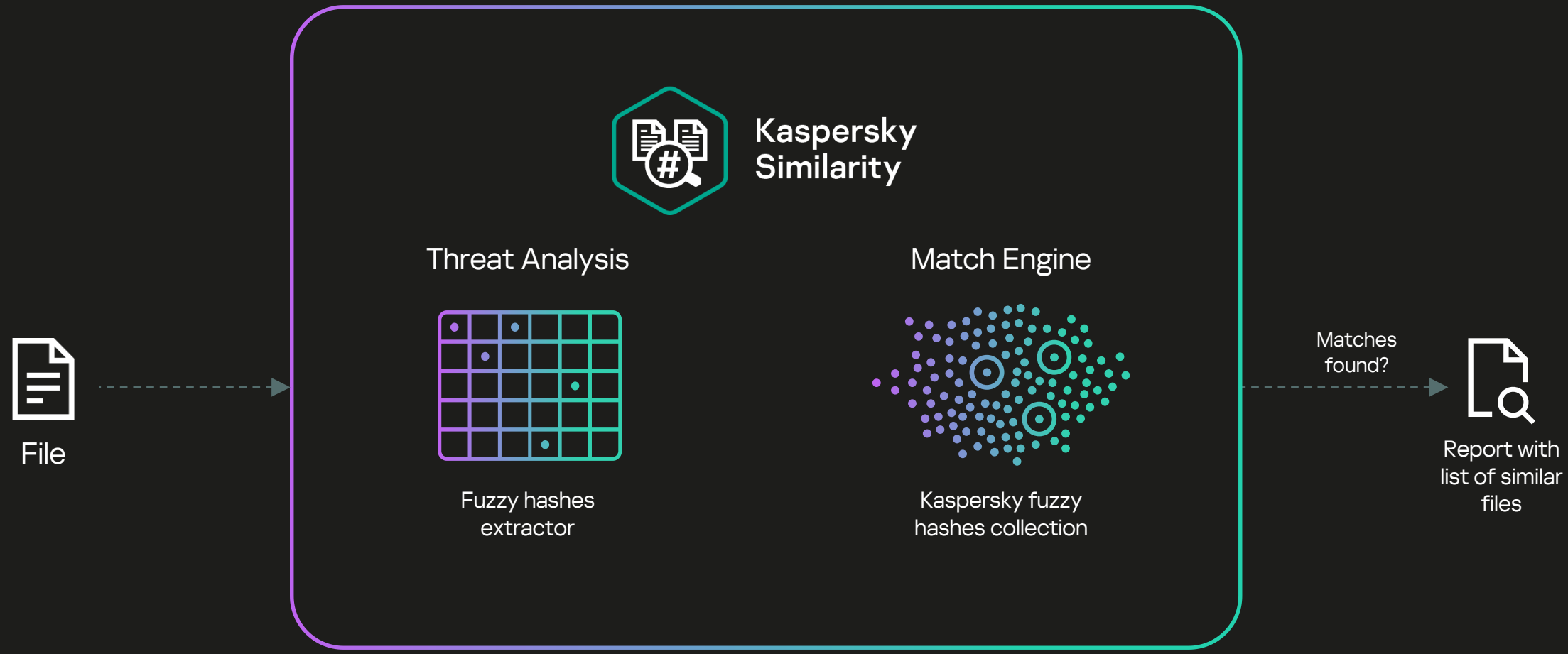
Kaspersky Research Sandbox



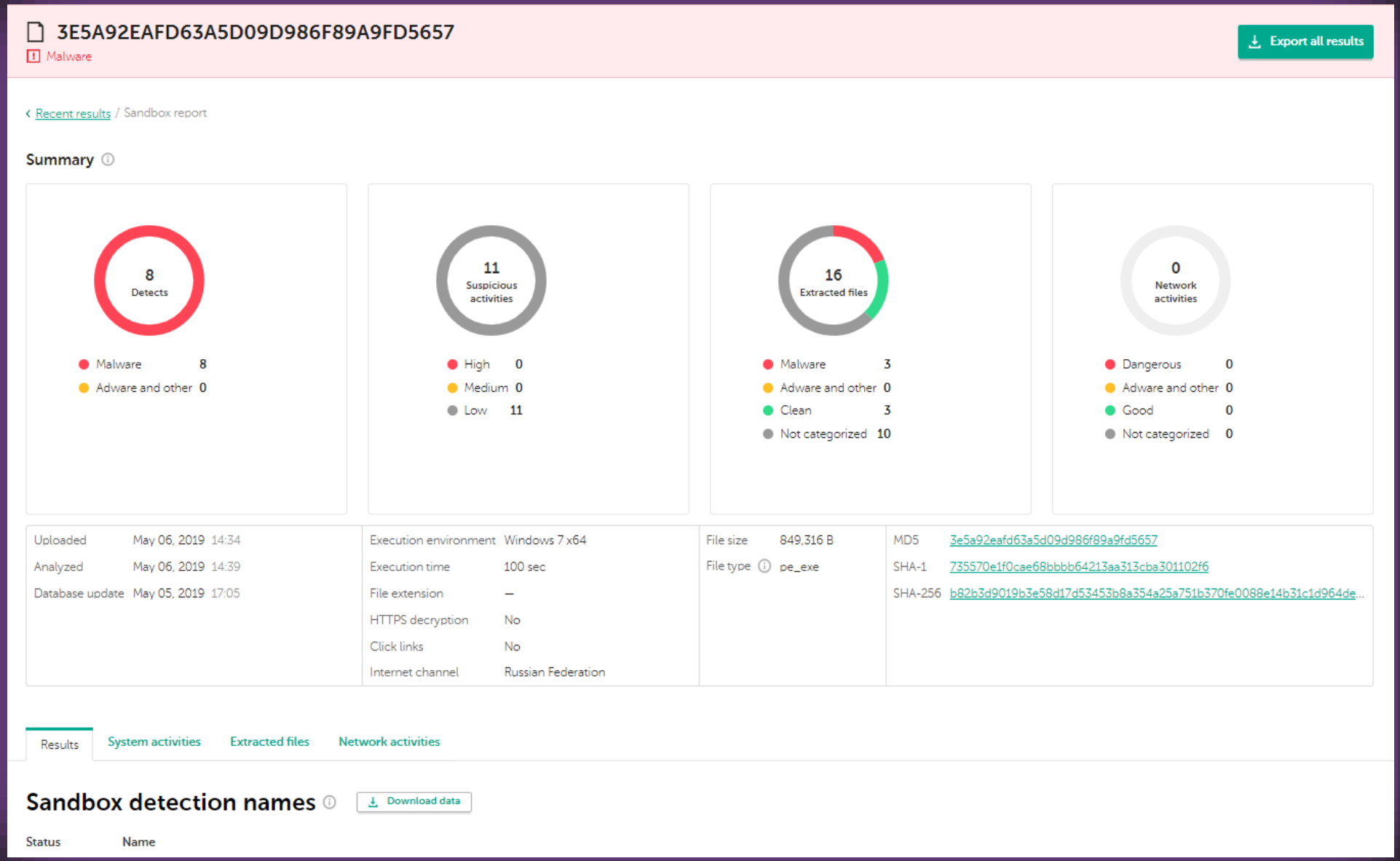
Kaspersky Threat Attribution Engine



Kaspersky Similarity

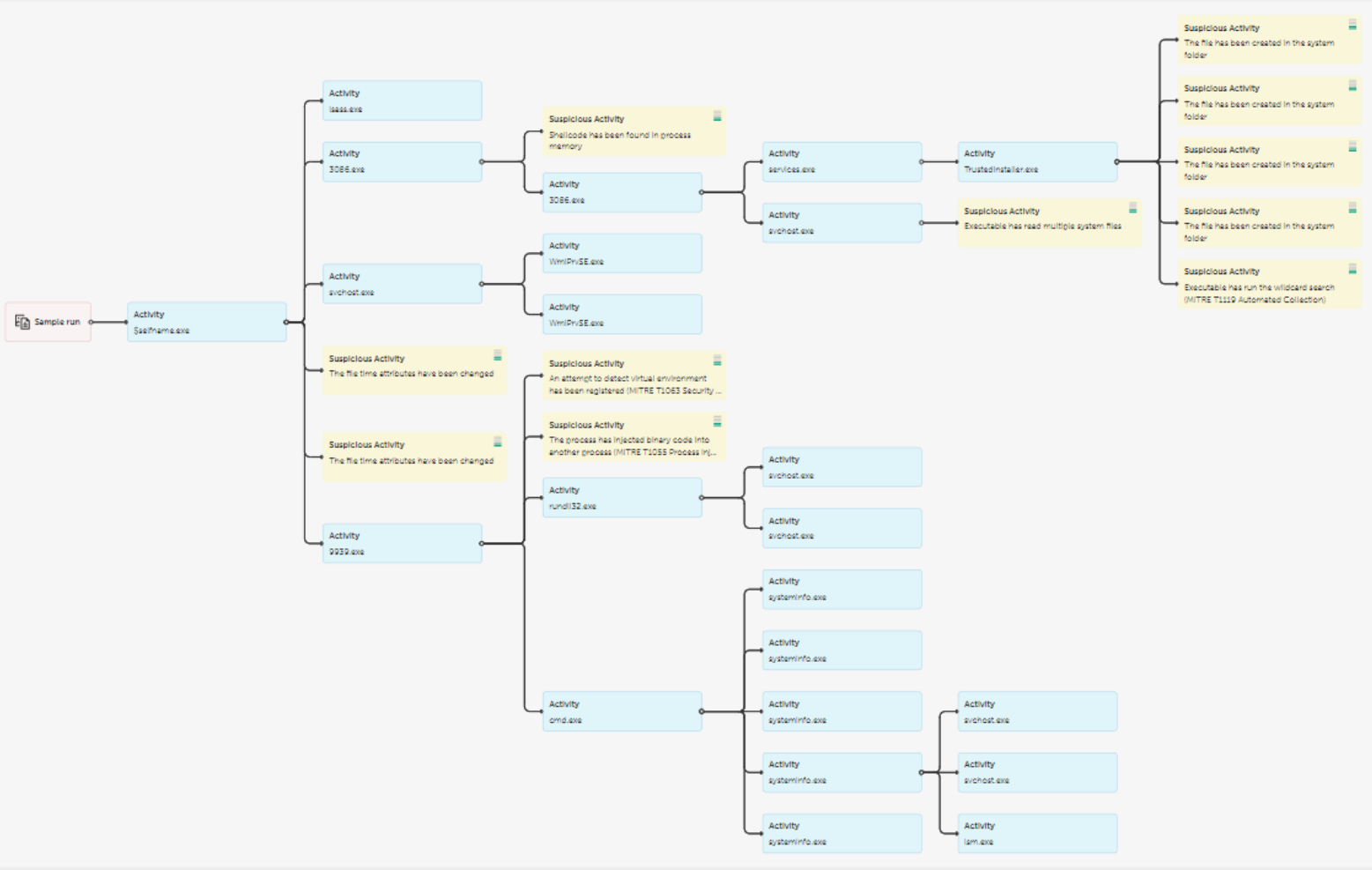


Kaspersky Cloud Sandbox – 儀表版



Kaspersky Cloud Sandbox – 執行關聯圖

Execution map



Kaspersky Cloud Sandbox – 可疑行為分析及執行截圖

Suspicious activities

Download data

Status	Severity	Description
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf.
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms.
Low	290	Shellcode has been found in the memory of the process $user\$temp\RarSFX0\3086.exe.
Low	290	The process $user\$temp\RarSFX0\9939.exe has attempted to detect a virtual environment (MITRE: T1063 Security Software Discovery).
Low	290	The process $user\$temp\RarSFX0\9939.exe has injected the binary code into the process $windir\$system32\rundll32.exe (MITRE: T1055 Process Injection).
Low	290	The process $windir\$system32\svchost.exe has read multiple system files.
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms.
Low	290	The process $windir\servicing\TrustedInstaller.exe has created the file in the system folder: $windir\$system32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms.
Low	200	The process $windir\servicing\TrustedInstaller.exe has run the wildcard search: $windir\servicing\sqm*.sqm (MITRE: T1119 Automated Collection).
Low	100	The process $selfpath\$selfname.exe has modified the time attributes of the file $user\$temp\RarSFX0\3086.exe.

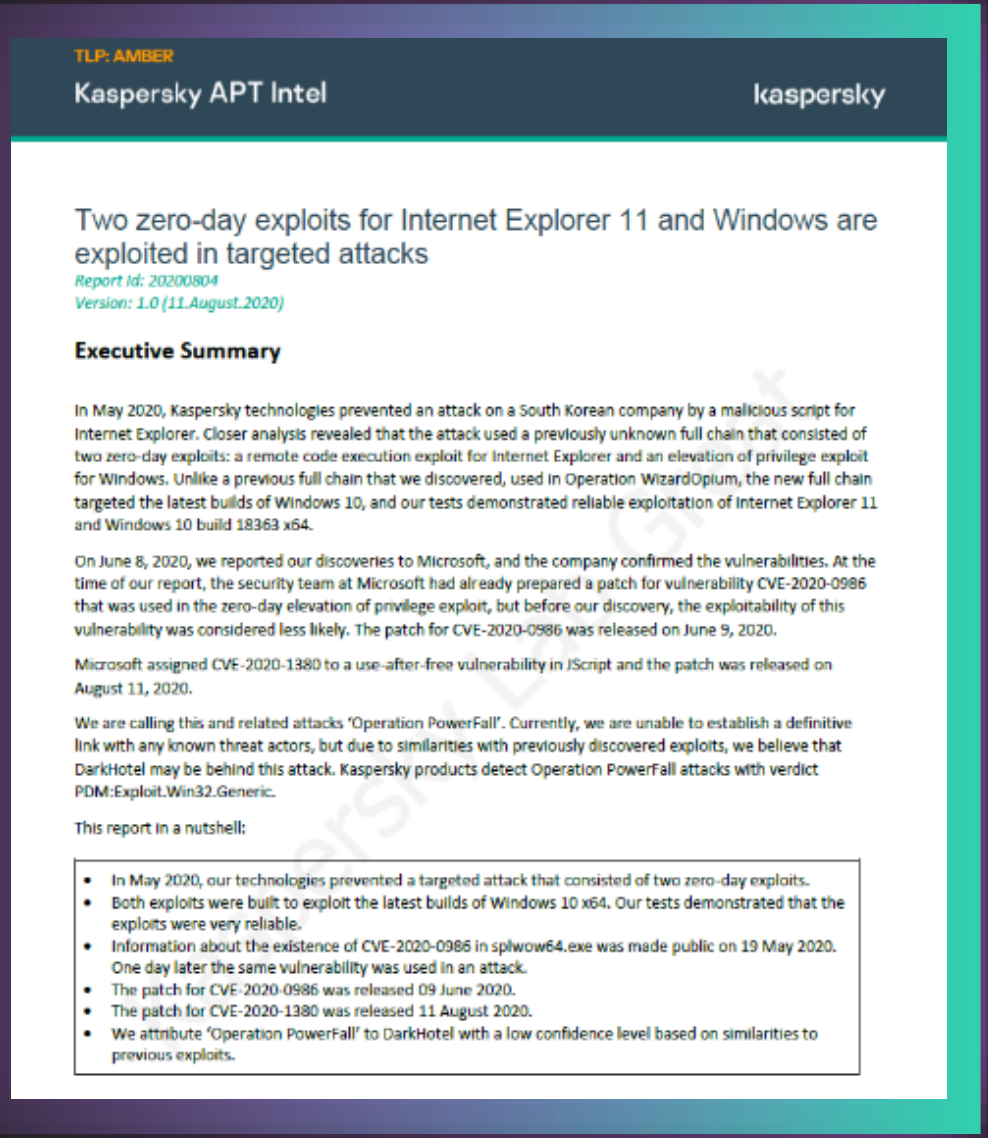
Show more (100)

Screenshots (19)

Download data

Kaspersky APT Intelligence Reporting

Kaspersky APT/ Crimeware/ICS 報告



TLP: AMBER

Kaspersky APT Intel

kaspersky

Two zero-day exploits for Internet Explorer 11 and Windows are exploited in targeted attacks

Report Id: 20200804
Version: 1.0 (11.August.2020)

Executive Summary

In May 2020, Kaspersky technologies prevented an attack on a South Korean company by a malicious script for Internet Explorer. Closer analysis revealed that the attack used a previously unknown full chain that consisted of two zero-day exploits: a remote code execution exploit for Internet Explorer and an elevation of privilege exploit for Windows. Unlike a previous full chain that we discovered, used in Operation WizardOpium, the new full chain targeted the latest builds of Windows 10, and our tests demonstrated reliable exploitation of Internet Explorer 11 and Windows 10 build 18363 x64.

On June 8, 2020, we reported our discoveries to Microsoft, and the company confirmed the vulnerabilities. At the time of our report, the security team at Microsoft had already prepared a patch for vulnerability CVE-2020-0986 that was used in the zero-day elevation of privilege exploit, but before our discovery, the exploitability of this vulnerability was considered less likely. The patch for CVE-2020-0986 was released on June 9, 2020.

Microsoft assigned CVE-2020-1380 to a use-after-free vulnerability in JScript and the patch was released on August 11, 2020.

We are calling this and related attacks 'Operation PowerFall'. Currently, we are unable to establish a definitive link with any known threat actors, but due to similarities with previously discovered exploits, we believe that DarkHotel may be behind this attack. Kaspersky products detect Operation PowerFall attacks with verdict PDM:Exploit.Win32.Generic.

This report in a nutshell:

- In May 2020, our technologies prevented a targeted attack that consisted of two zero-day exploits.
- Both exploits were built to exploit the latest builds of Windows 10 x64. Our tests demonstrated that the exploits were very reliable.
- Information about the existence of CVE-2020-0986 in splwow64.exe was made public on 19 May 2020. One day later the same vulnerability was used in an attack.
- The patch for CVE-2020-0986 was released 09 June 2020.
- The patch for CVE-2020-1380 was released 11 August 2020.
- We attribute 'Operation PowerFall' to DarkHotel with a low confidence level based on similarities to previous exploits.

Threat actor profiles

Mapping to MITRE ATT&CK

Executive summary

- C-level oriented information

Deep technical analysis

- Attack methods
- Exploits used
- Malware description
- C&C infrastructure and protocols description
- Victim analysis
- Data exfiltration analysis
- Attribution

Conclusions and recommendations

Indicators of Compromise (IOCs) and YARA rules

卡巴斯基 APT 報告特色

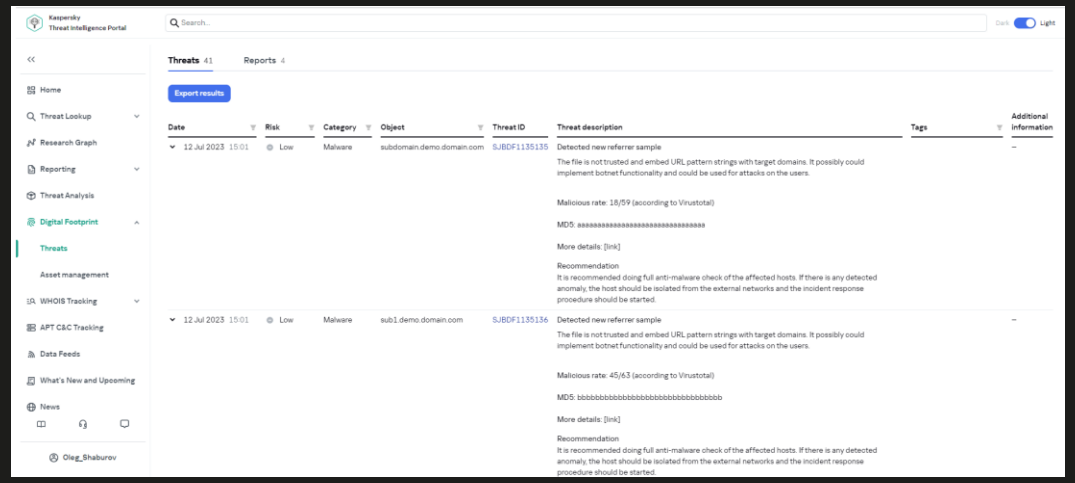
追蹤超過 300+ 威脅來源 超過 500+ 不同組織

每年超過 200+ 公開/未公開報告

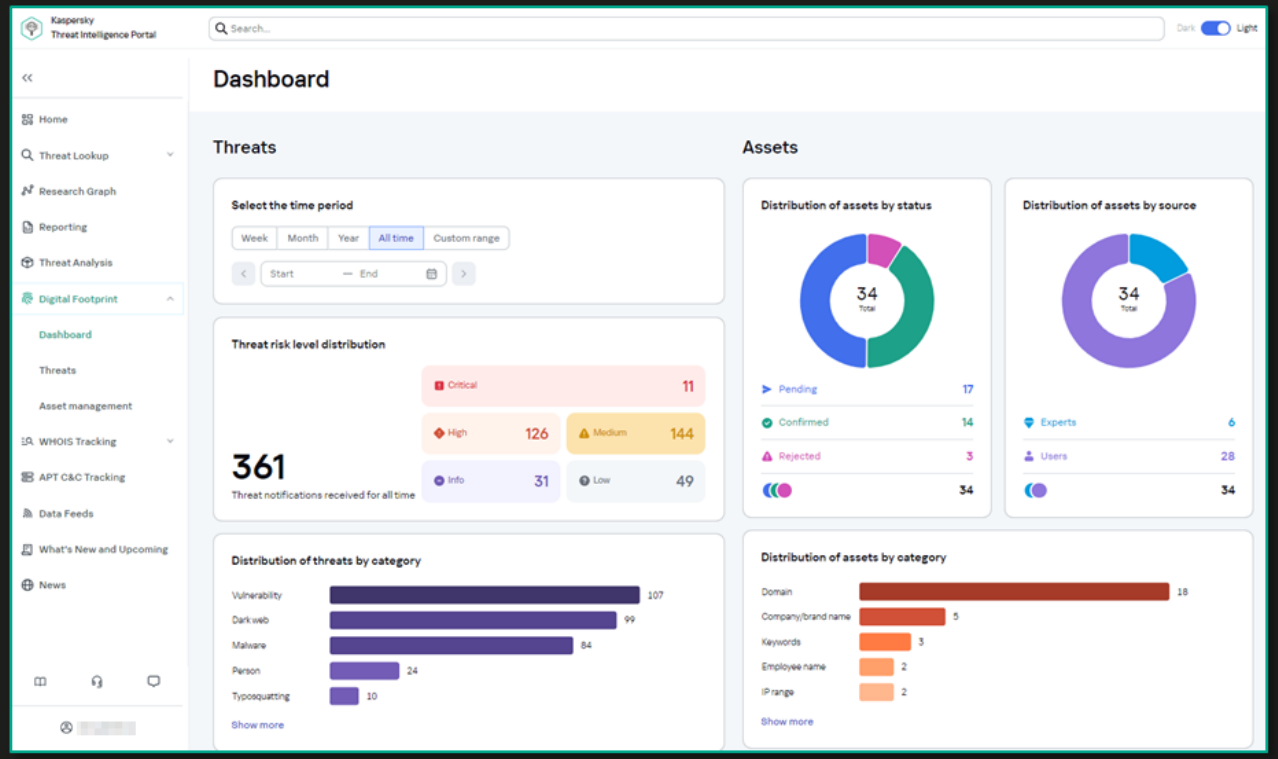
超過 17000+ IoCs 及 2500+ Yara rules

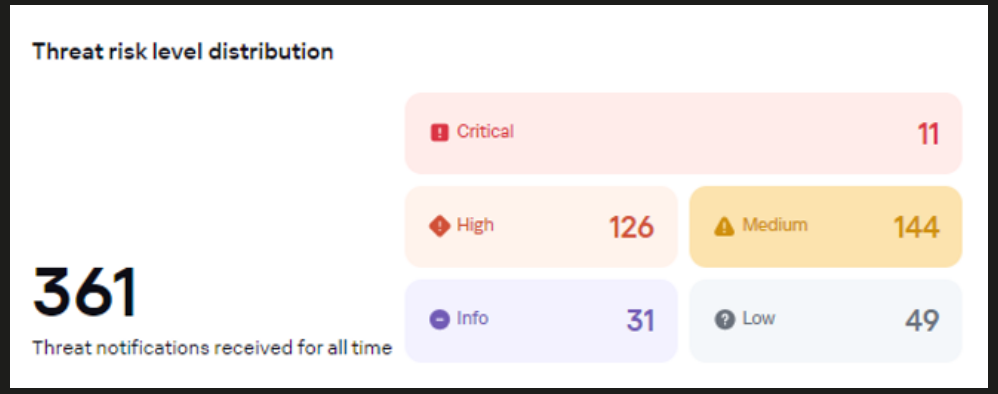
Kaspersky Digital Footprint Intelligence
攻擊面風險管理

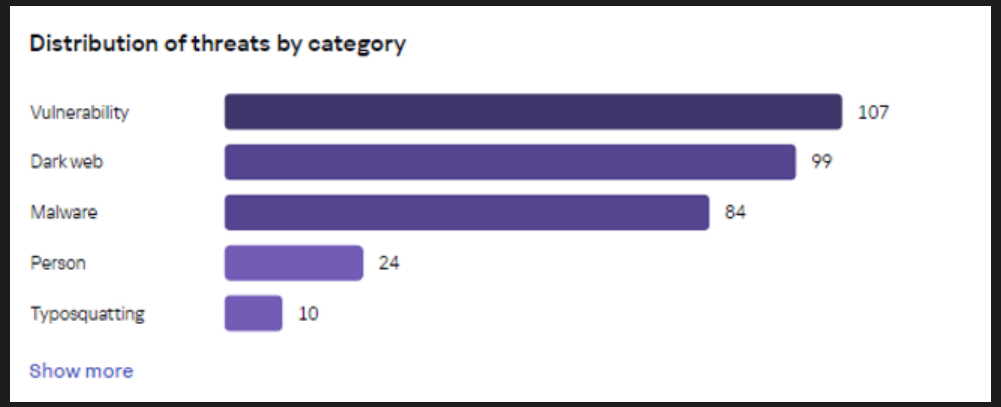
- 邊界網路資訊清單
- 暗網監控
- 品牌保護
- 資料外洩發掘



DFI 常見威脅內容：外部攻擊面分析、暗網洩露訊息收集







可先了解自己有哪些弱點是被別人掌握的

Digital Footprint Intelligence – 攻擊面管理

暗網監控 Dark Web Monitoring

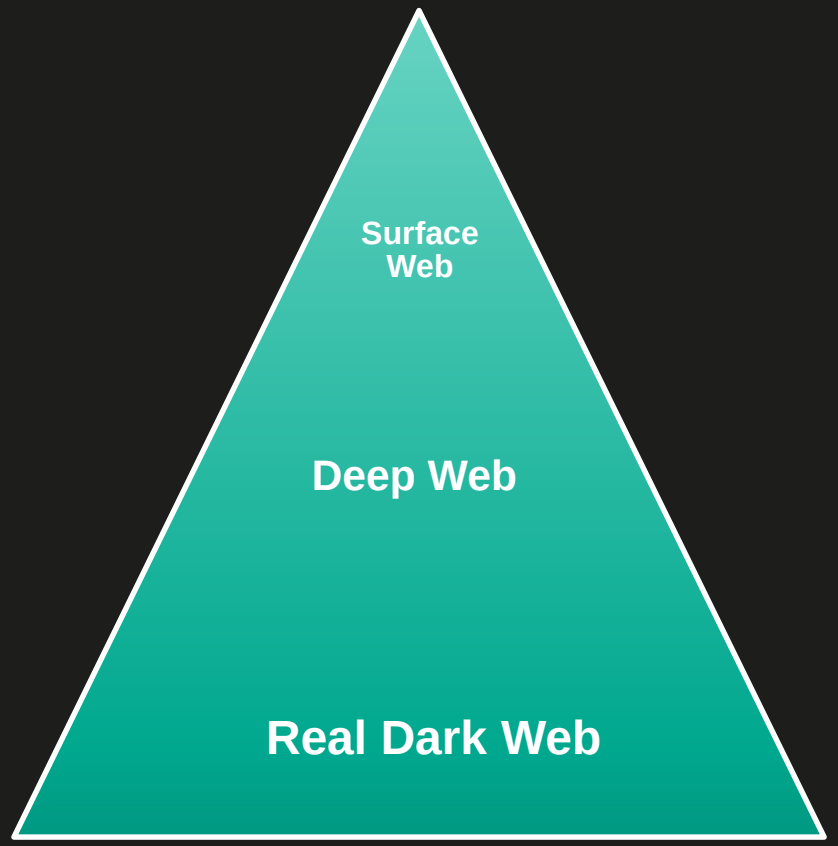
80%
論壇

10%
通訊平台

5%
洋蔥

5%
私人訪問論壇

語言限定?!



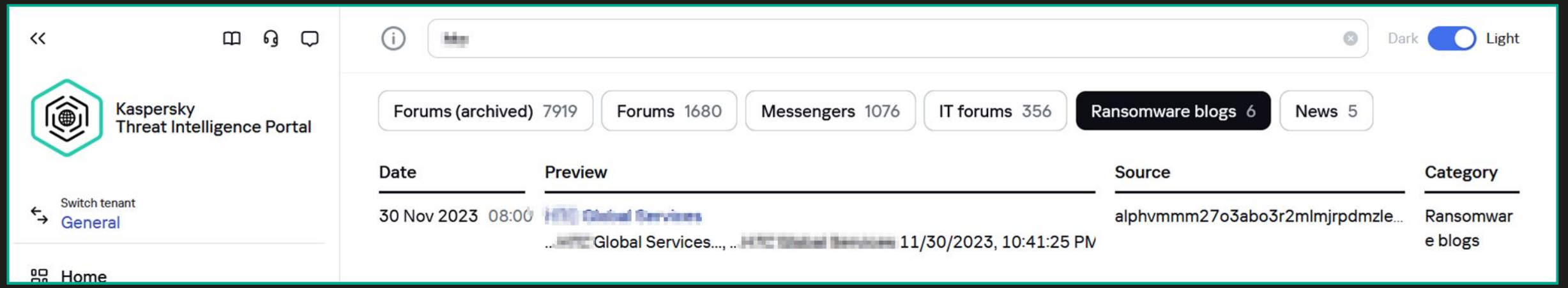
500 000+
每日分析資訊數量

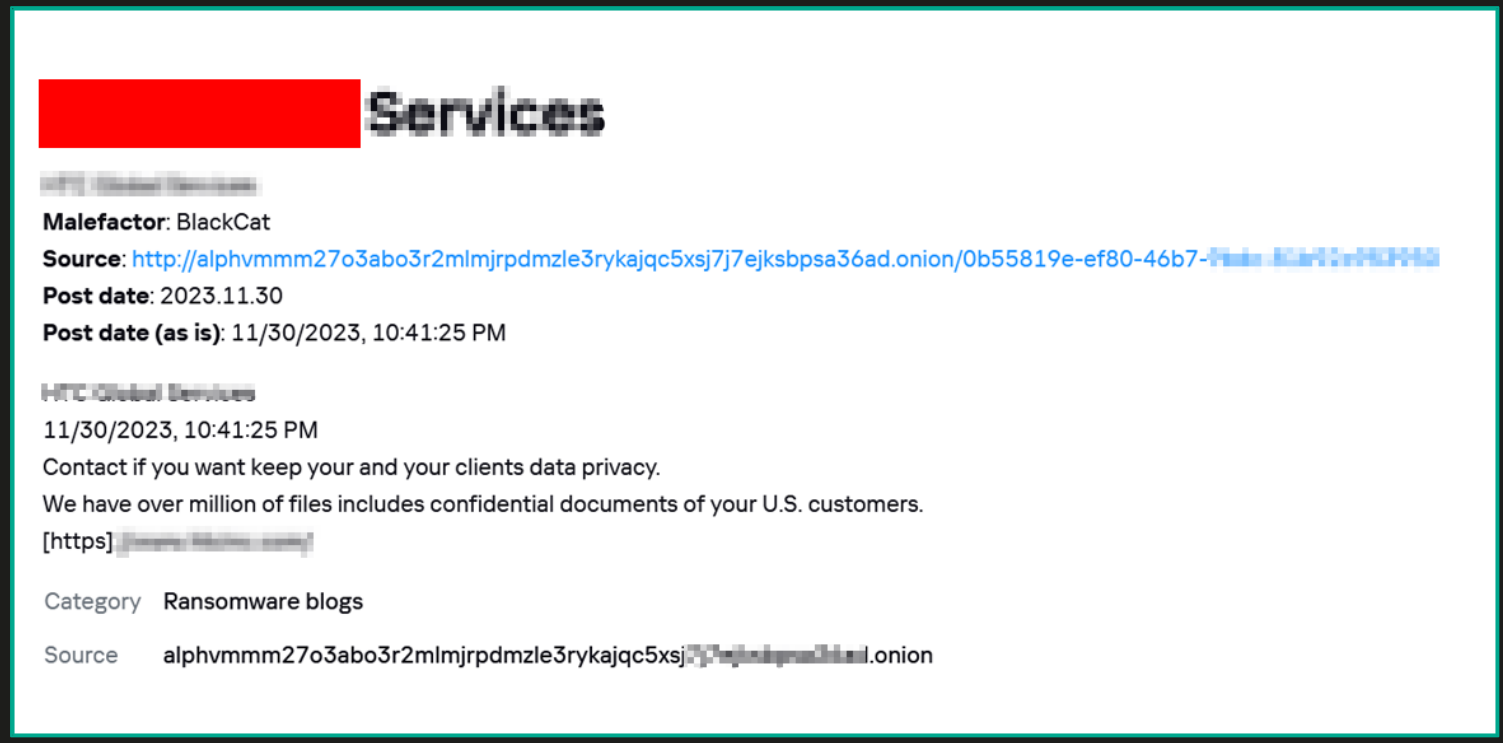
全球趨勢
已知攻擊事件的結果/內容
使用簡單腳本即可進行攻擊
舊的外泄資料

與駭客組織相關廣告
與客戶相關的零日漏洞
資料外泄

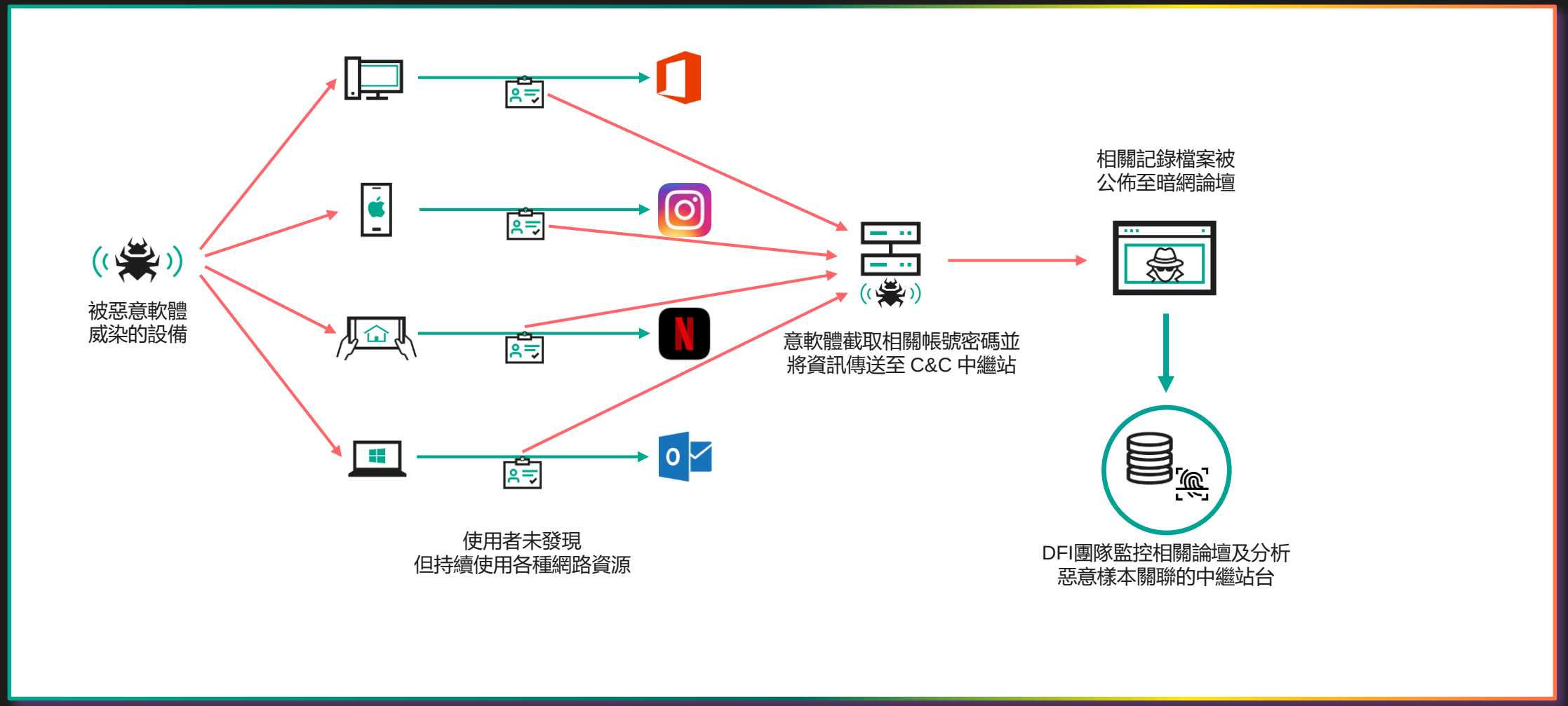
攻擊者計劃 (出售感染網路的存取帳號)
被盜的員工帳號
內賊的招募活動

暗網搜尋資訊

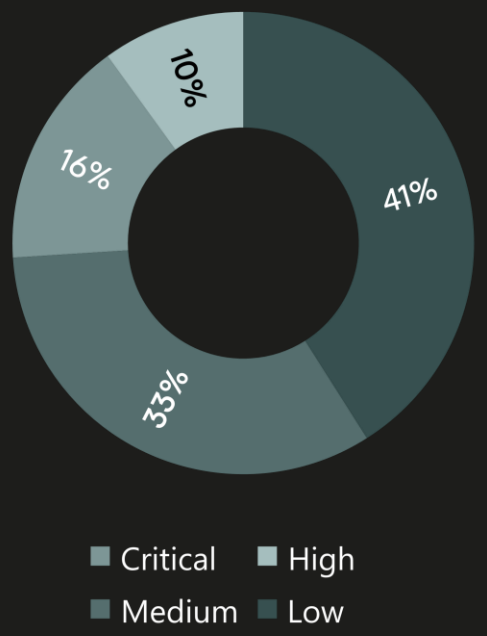

Kaspersky
Threat Intelligence Portal
Switch tenant
General
Home
Dark
Light
Forums (archived) 7919
Forums 1680
Messengers 1076
IT forums 356
Ransomware blogs 6
News 5
Date
Preview
Source
Category
30 Nov 2023 08:00
...Global Services..., .. 11/30/2023, 10:41:25 PM
alphvmmm27o3abo3r2mlmjrpdmzle...
Ransomware blogs


Services
Malefactor: BlackCat
Source: http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/0b55819e-ef80-46b7-
Post date: 2023.11.30
Post date (as is): 11/30/2023, 10:41:25 PM
11/30/2023, 10:41:25 PM
Contact if you want keep your and your clients data privacy.
We have over million of files includes confidential documents of your U.S. customers.
[https]
Category Ransomware blogs
Source alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj .onion

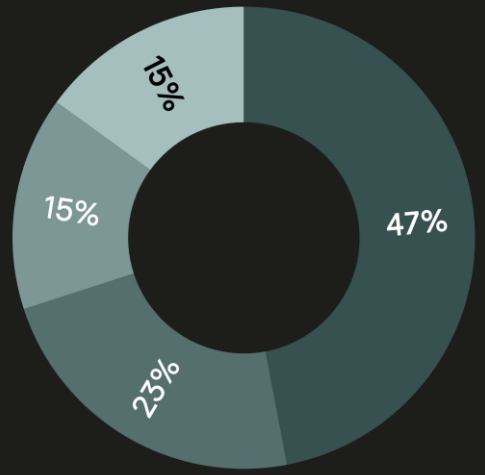
資料泄露分析 (malware log files)



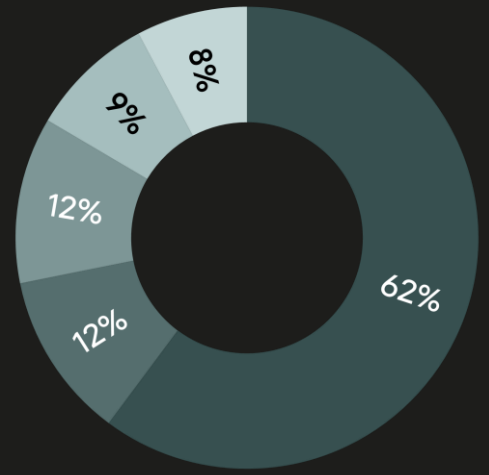
XXX vulnerabilities



Types of vulnerabilities



Exposed services



攻擊面管理 – 快速了解已知的風險

網路邊界資訊-常見威脅類型

- 未正確設定的網路服務
- 可辨識的已知漏洞
- 被洩漏或已被入侵的相關資源

暗網資訊-常見威脅類型

- 欺詐計劃和網路犯罪的計劃
- 信用卡被盜和外洩的帳號資訊
- 內賊活動

惡意程式-常見威脅類型

- 釣魚郵件攻擊
- 僵屍網路活動
- 針對式攻擊
- APT 活動

資料外洩

- 公司文件被公開存取
- 員工在社群網路外洩的資訊
- 遭到外洩的帳號

品牌冒充

- 假冒網站
- 假冒社群帳號
- 假冒手機 apps

先了解自己有那些弱點是被別人掌握的

威脅情報服務選擇的要點

情報來源能否覆蓋全球區域的範圍

情報的品質有時比情報的數量還重要

非安裝式產品，沒有地緣政治的疑慮

現有安全服務的使用是否滿足企業SOC短、中、長期的需求

知識的分享 + 提昇現有安全等級
(是否有別人沒有的情報，或別人都有為什麼我沒有?!)

Why Kaspersky

為什麼選擇 **Kaspersky?**

國際認証威脅獵捕

我們的專家團隊皆有通過各種專家認証並專注在 數位鑑識、逆向工程、惡意程式分析及網路安全...等相關領域。

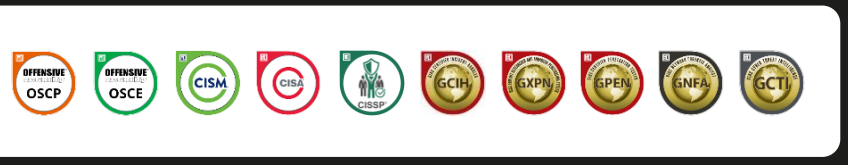
自適性研發 工具及遙測數據收集

威脅偵測 透過 **IoC**、**TTP**、 **YARA**及威脅智能情報.

透過簡易過程就可修正我們的偵測規則、工具及數據收據方式，找出新類型的威脅。

可執行的威脅智能情報內容

身為全球威脅智能情報提供者，並非只是提供黑名單資料。而是包含白名單及各種關聯性數據庫。可方便快速找出威脅訊息。



FORRESTER®

Kaspersky is Positioned as a Leader in Forrester New Wave: External Threat Intelligence Services, 2021

Kaspersky Threat Intelligence Recognitions

安全行業別威脅情報的最佳提供廠商之一

INTERPOL

Interpol accelerates fight against cybercrime through Kaspersky partnership

GREAT GLOBAL RESEARCH & ANALYSIS TEAM

Kaspersky TI powered by our globally recognized expert team – Kaspersky GREAT that maintain a successful track record of spotting new threats early

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION
*kaspersky.com/top3

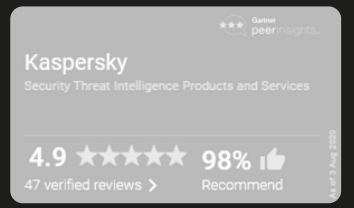
The quality of our intelligence is backed by our most tested and most awarded threat protection technologies

MITRE | ATT&CK®

Kaspersky has contributed info about CozyDuke, Carbanak prior the MITRE Evaluation Round2 and Round 3 preparation stage to support improvements to MITRE ATT&CK

FORRESTER®

Kaspersky is Positioned as a Leader in Forrester New Wave: External Threat Intelligence Services, 2021



Kaspersky has the highest overall rating and the most recommended among all vendors in the Security Threat Intelligence Products and Services Market

FROST & SULLIVAN

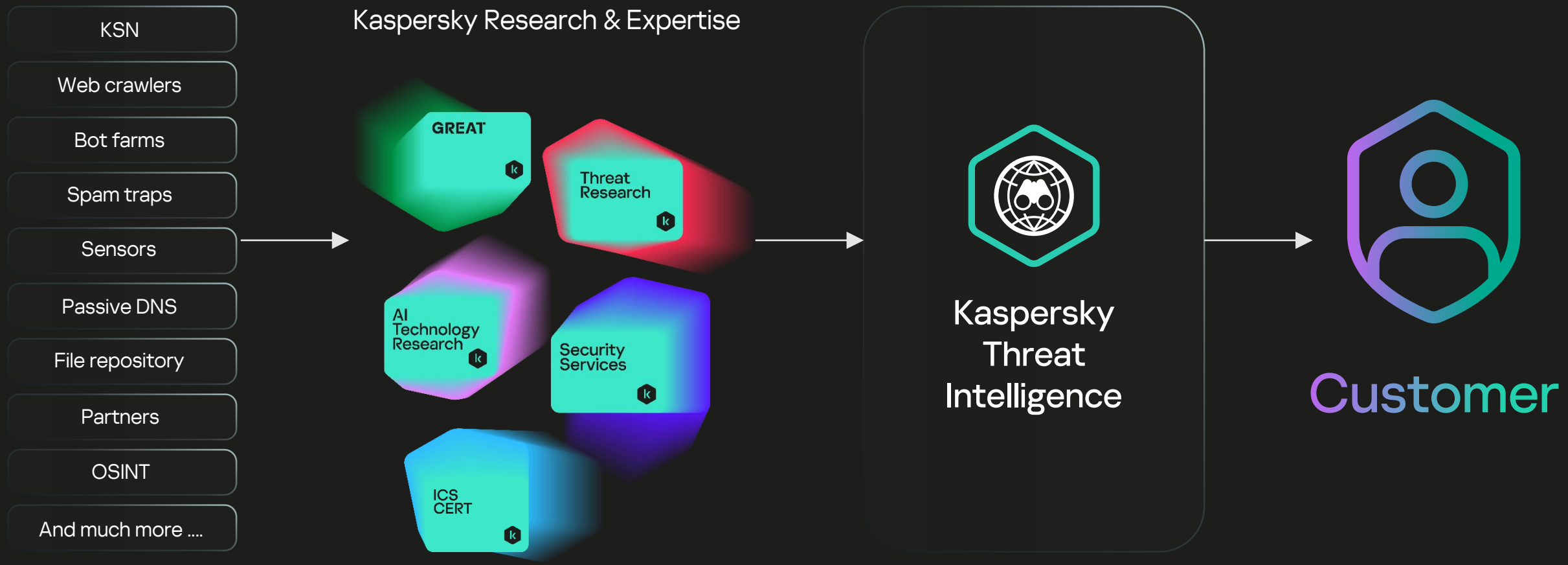
Kaspersky has been named as an Innovation Leader in the Cyber Threat Intelligence research 2024

GIGAOM

"Kaspersky's suite of threat intelligence solutions, its services and intelligence network positions it as a leader"

Kaspersky has been recognized as a Leader in the 2024 SPARK Matrix™: Digital Threat Intelligence Management by Quadrant Knowledge Solutions

卡巴斯基威脅情報來源



Kaspersky Threat Intelligence provides access to a wide range of information gathered by our world-class analysts and researchers to help your organization counter today's cyberthreats effectively.

卡巴斯基威脅情報來源

Every center contributes to Kaspersky's solutions and services

- Threat Research
- Incident Investigation

Kaspersky Global Research and Analysis Team

- Researches the most complex threats; APT, cyber espionage campaigns, global cyber epidemics, etc.
- Security of future-focused technologies
- Investigates sophisticated financial cybercrime

Kaspersky Threat Research

- Anti-Malware Research
- Content Filtering Research
- SSDLC & Secure-by-Design Methodologies

Kaspersky AI Technology Research

- AI Cybersecurity
- GenAI Research
- AI-Powered Threat Detection / Solutions

Kaspersky Security Services

- MDR
- Incident Response
- Security Assessment
- SOC Consulting
- Digital Footprint Intelligence

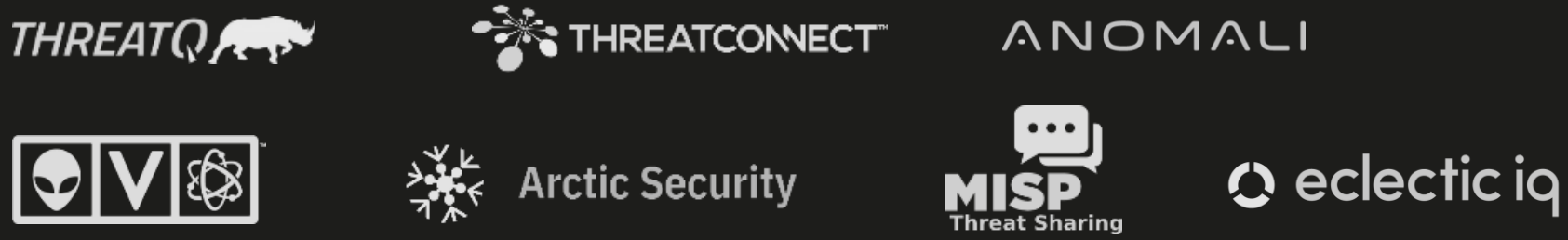
Kaspersky ICS CERT

- Critical Infrastructure Threat Analysis
- ICS Vulnerability Research and Assessment
- Technology associations, analytics and standards

支援整合多種不同平台及應用

SIEM / SOAR / IRP

Threat Intelligence Platforms



Network Security Controls

SOC 顧問服務 – 成熟度評估、架構開發、流程設計

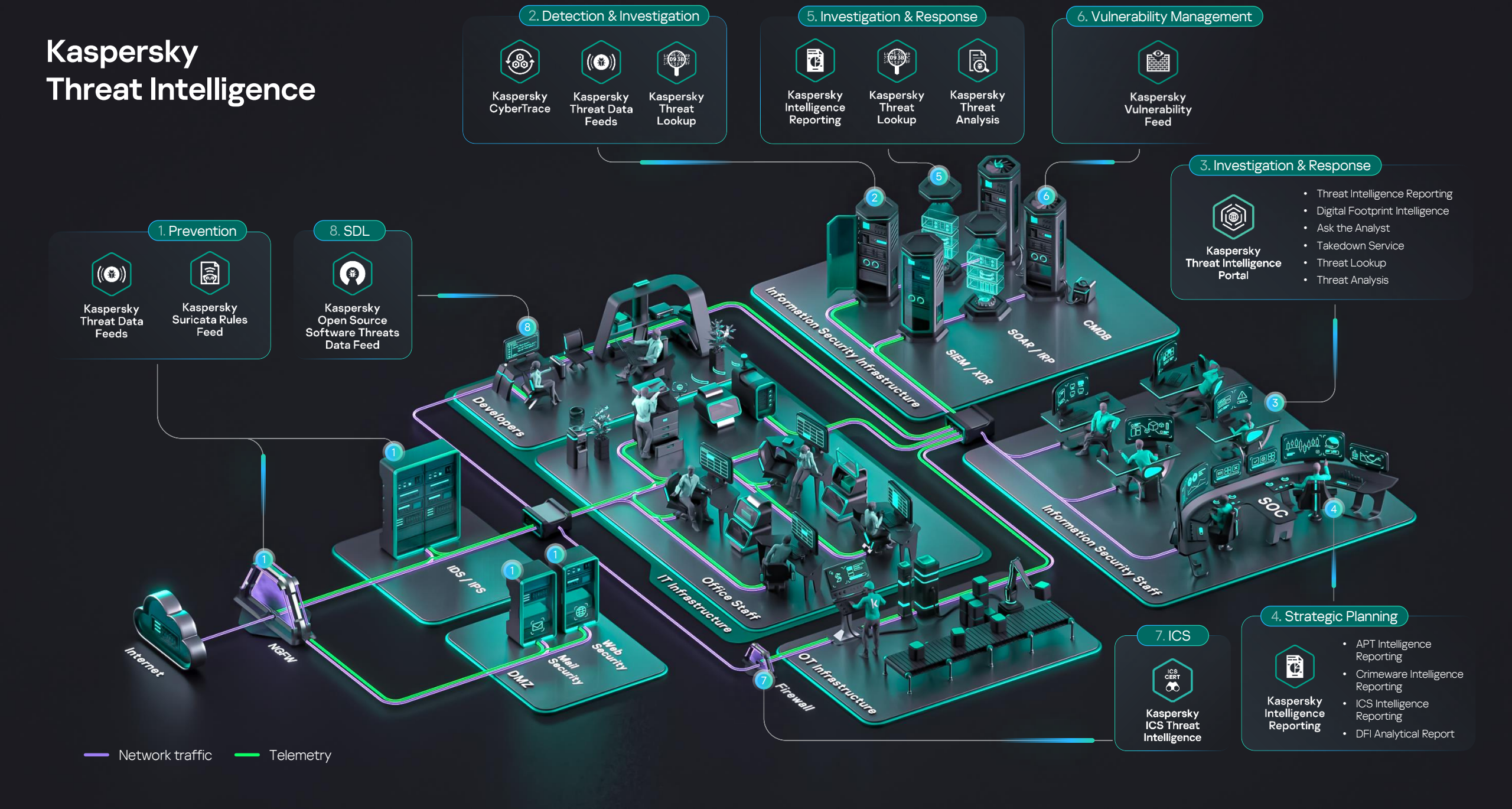
Weak domains Strong domains

Current

Target

卡巴斯基SOC/MDR 團隊獲得 SOC CMM 金級夥伴
https://www.soc-cmm.com/services/support/

Kaspersky Threat Intelligence



Thank you!

kaspersky