Kaspersky Threat Intelligence

Stay ahead of your adversaries

kaspersky

Kaspersky Threat Intelligence

提升防火牆偵測率應用分享

kaspersky

威脅的趨勢及挑戰

近期威脅趨勢的特性

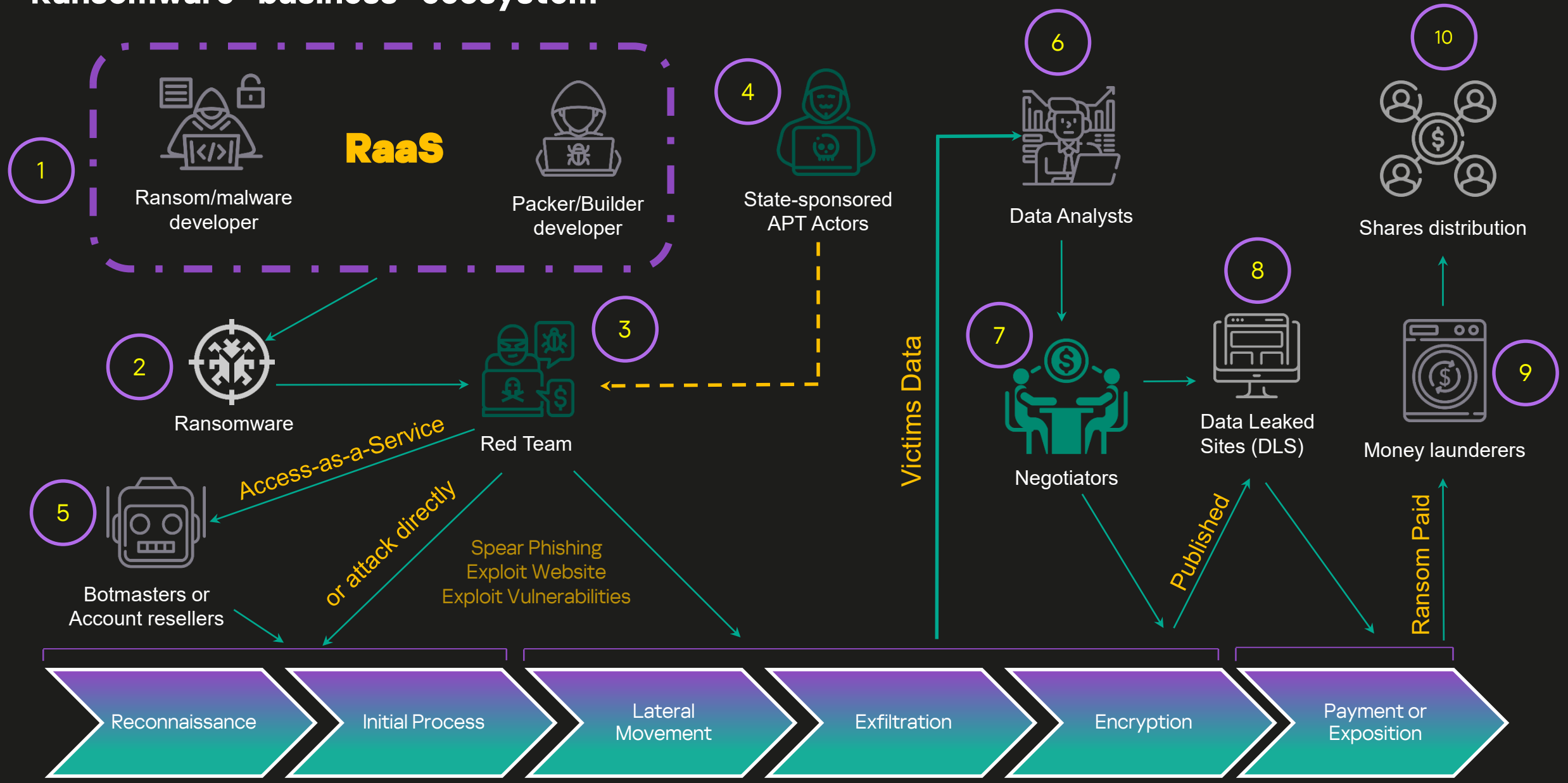
1. **勒索攻擊服務化**
   Ransomware as Service 服務化式的分工

2. **零時差漏洞利用商品化**
   包含防火牆、虛擬化平台、備份系統或行動裝置的漏洞揭露及利用

3. **雲端服務及供應鏈的風險及破口**
   網路邊界安全及零信任的挑戰

4. **AI 武器化應用**
   AI 驅動釣魚與漏洞探查腳本應用

Ransomware "business" ecosystem



LockBit在2024年遭到國際警方的聯手查緝
幾天內 立刻 重起爐灶

LockBit Ransomware 3.0
The most active Affiliate RaaS

新聞

三大勒索軟體集團LockBit、DragonForce與Qilin結盟

美國網路安全暨威脅偵測業者ReliaQuest發布第三季勒索軟體報告，顯示LockBit、DragonForce與Qilin已展開結盟，將分享彼此的戰術及資源

壞人是有技術有組織地在打

而你是被打後，要善後、寫檢討報告，等簽呈要到預算，資安方案都還未啟動，壞人早就走了~~

卡巴斯基提出三個思維層面

A.阻絕不當連線
情資 提升防火牆滲透連線偵測率

B.端點管理與偵測率提升
提升端點行為管理 偵測回應速度

C.安全服務委外
透過專家指導 提昇實務經驗

A. 卡巴斯基威脅情資
提升防火牆偵測不當連線

情資多元化的必要性

Gartner 2024: 情資多元化可提升威脅偵測準確率 45%

- **情資來源多元化**：西方世界 vs 俄羅斯/中東

- **情資種類多元化**：情資不僅限Malicious URL/Hash/IP, 還包括APT 、勒索軟體、ICS 、OpenSource...等

卡巴斯基威脅情報來源豐富性

Kaspersky 威脅情報由我們的世界級分析師與研究人員**蒐集**與**整理**，提供多元化的資訊，協助您的組織有效應對當今的網路威脅。

透過特有的威脅情報補足覆蓋率不足的盲點

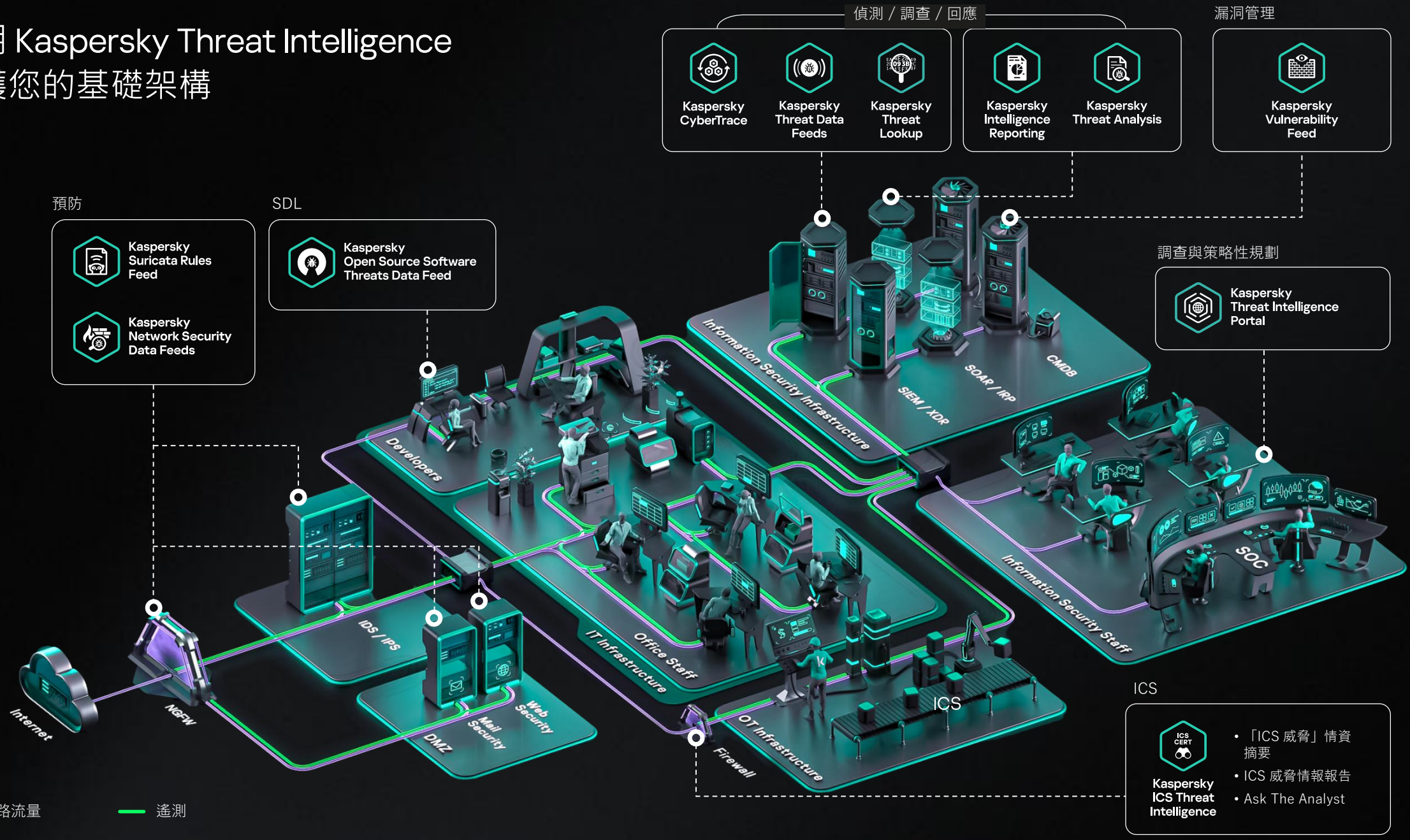
1. 特殊區域的惡意威脅情報收集 - 惡意攻擊發起地較多的區域掌握：俄羅斯、歐洲、中東地區

2. 主動集成，可節省 SOC團隊檢視事件，建自動響應規則等時間
   包含情報汰舊換新的作業時間，避免造成大量誤報事件。

3. 即時套用，立即提昇現有防火牆威脅偵測阻擋覆蓋率

4. 卡巴斯基情報應用可套用多種不同安全機制上實現自動化響應
   包含：Firewall、SIEM、SOAR、TIP(威脅情報平台)、IRP(事件調查響應平台)...等

利用 Kaspersky Threat Intelligence 保護您的基礎架構



Kaspersky威脅情資Threat Data Feeds - 系統自動化應用

30種以上 威脅情報資料庫

滿足不同任務需求，可自由選擇合適的組合

- Tactical TI
- Operational TI

標準常用的威脅資料庫

- Malicious URL
- Ransomware URL
- Phishing URL
- Botnet C&C URL
- Mobile Botnet C&C URL
- Malicious Hashes
- Mobile Malicious Hashes
- IP Reputation
- IoT URL
- ICS Hashes
- APT Hashes
- APT IP
- APT URL
- Crimeware Hashes
- Crimeware URL

Kaspersky Threat Data Feeds

SOC
SIEM, SOAR/IRP, TIP, EDR/XDR

TI Platform

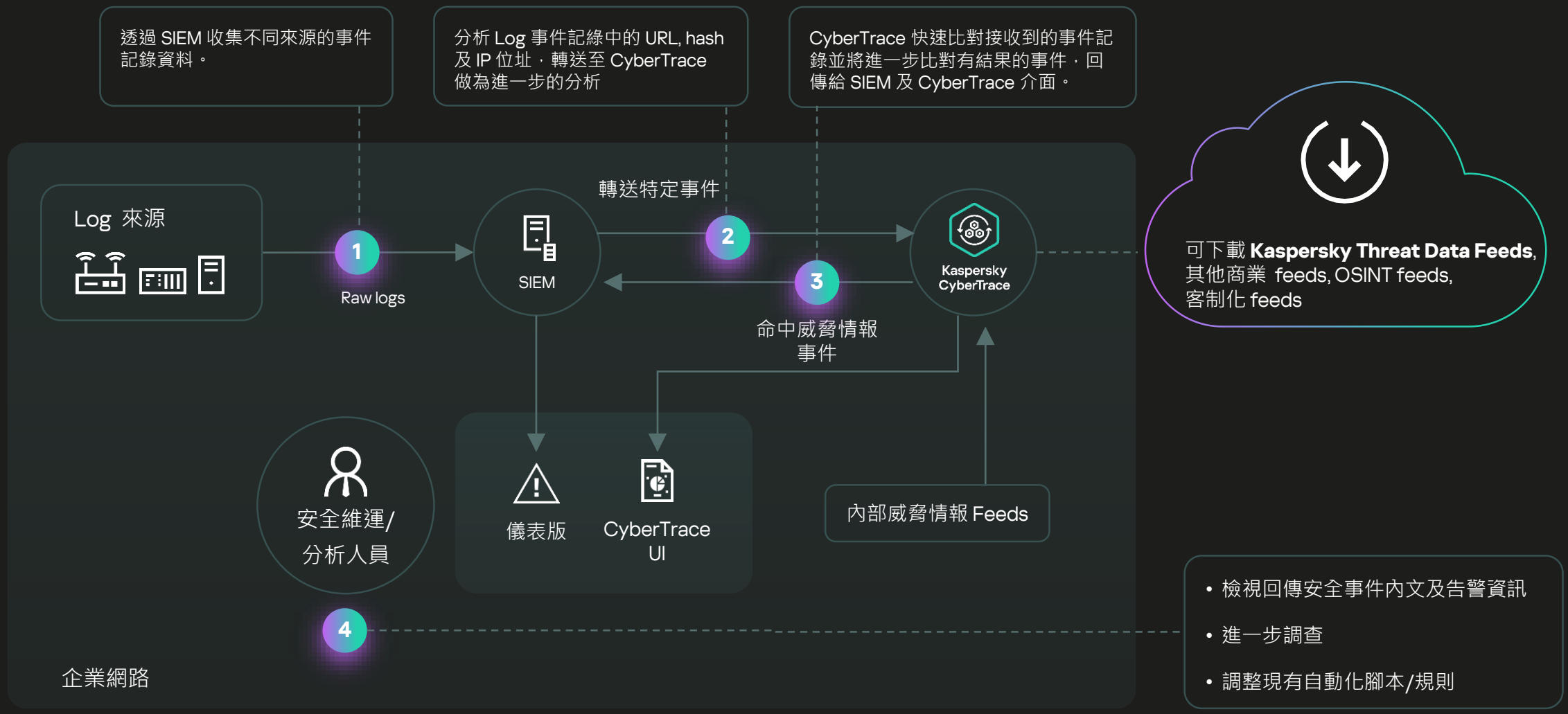
快速將各種威脅情報來源投入運作，並減輕 SIEM 的工作負載

Kaspersky CyberTrace

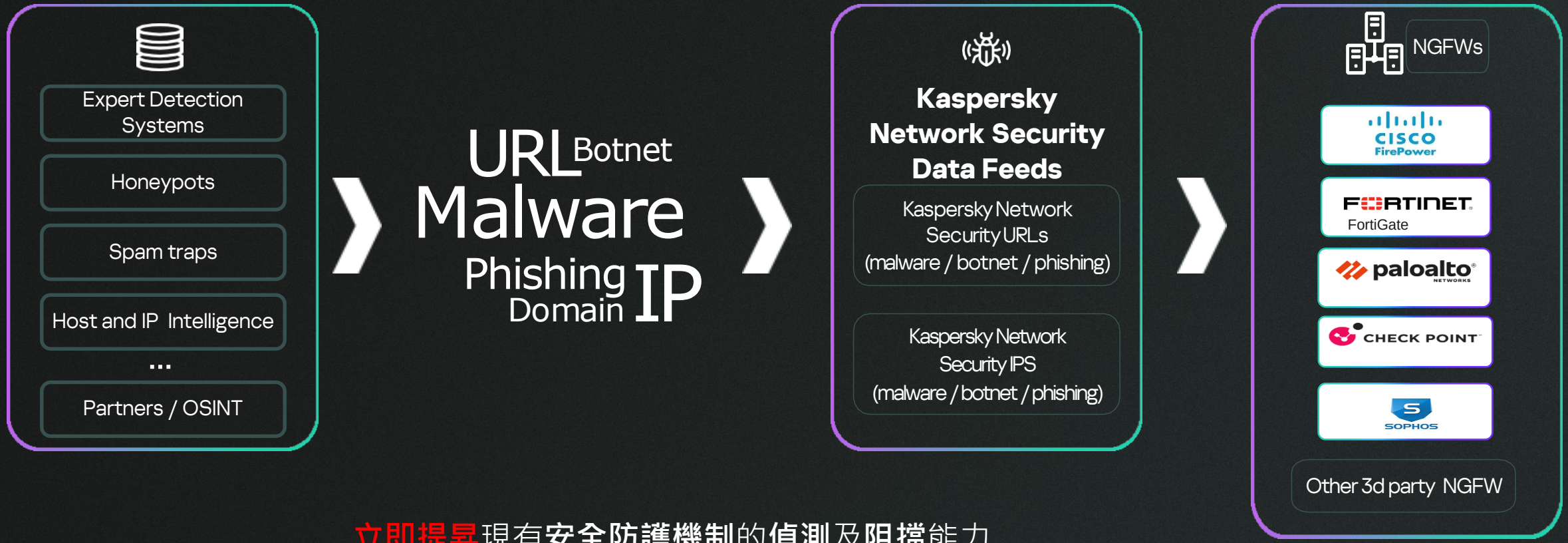
特殊場景設計的威脅資料庫

- Network Security Data Feeds → NGFW
- Suricata Rules Feed → IDS / IPS
- Sigma Rules Data Feed → SIEM / EDR
- Yara Rules Data Feeds → YARA-scanner
- Vulnerability Feed → SBOM /CMDB
- Open Source Software Threats Data Feed → OSA / CSA / ASOC

卡巴斯基威脅情資傳輸 (Threat Data Feeds) – 整合SIEM案例分享



透過威脅情資 Data Feeds 整合應用案例分享



立即提昇現有**安全防護機制**的**偵測**及**阻擋**能力
即時響應及節省維運人力時間

kaspersky

測試結果

FORTINET
FortiGate

Test scenario

The test was conducted using FortiGate's built-in detection rules versus the 1,000 rules from Kaspersky's Network Security Threat Data Feed.

Results

FortiGate Detection Rate **47.7%**

Kaspersky Network Security Threat Data Feed increases the efficacy of threat detection by:

52.3%

paloalto NETWORKS
NGFW

Test scenario

The test was conducted on a Palo Alto PA-220 against 1,000 rules from the Kaspersky Network Security Threat Data Feed, with the following Palo Alto detection lists enabled:

- Known Malicious IP Addresses
- High Risk IP Addresses
- Bulletproof IP Addresses
- Tor Exit IP Addresses

Results

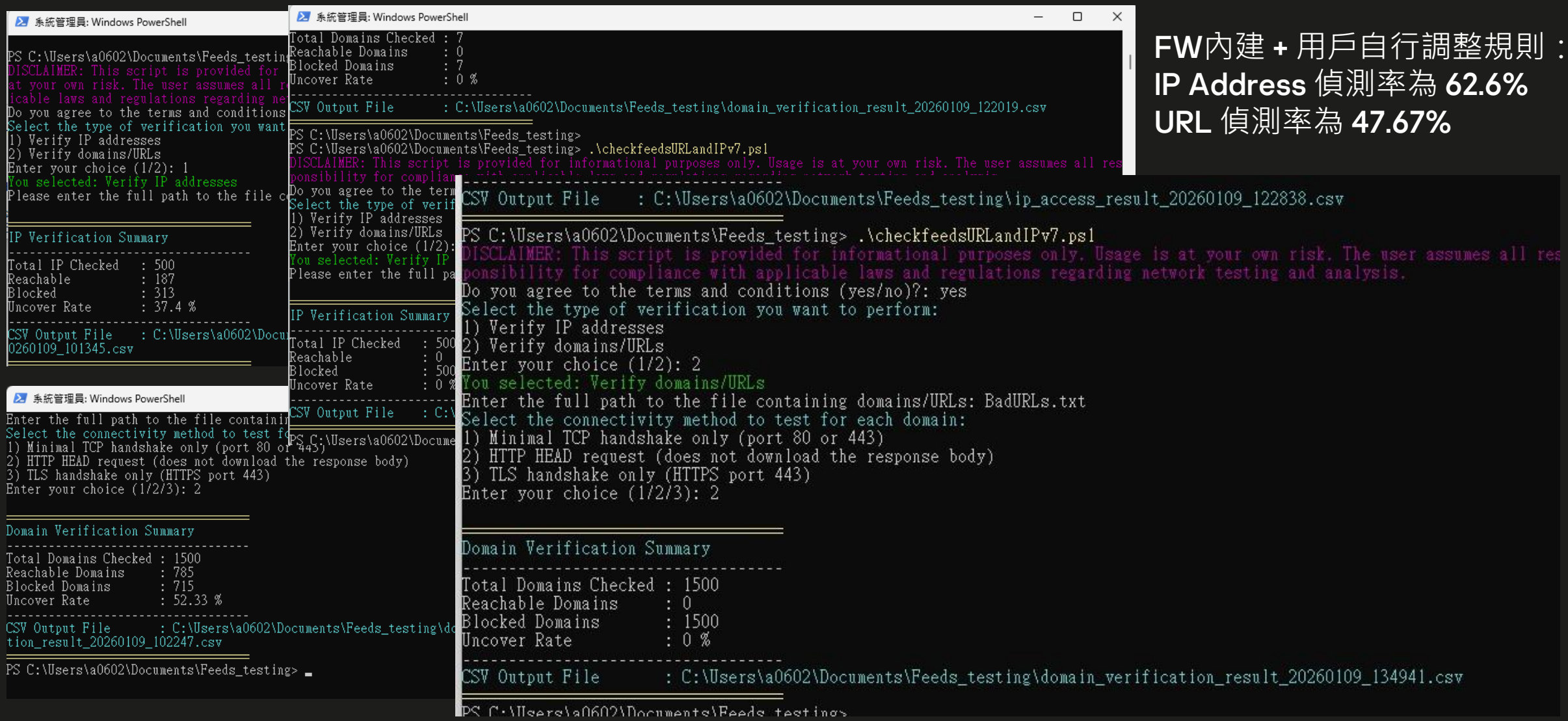
51.3%

Palo Alto Detection Rate

Kaspersky Network Security Threat Data Feed increases the efficacy of threat detection by:

47.9%

實測案例分享



FW內建 + 用戶自行調整規則：
IP Address 偵測率為 62.6%
URL 偵測率為 47.67%

- 立即提昇防火牆阻擋惡意威脅效果。包含外部對內部、**內部對外部**的偵測
- 協助資訊人員，發現內部主機那些會連線至外部惡意**C2**主機。已利後續處理。

kaspersky

一份情資 可支援整合多種平台及多種應用

SIEM / SOAR / IRP

Threat Intelligence Platforms



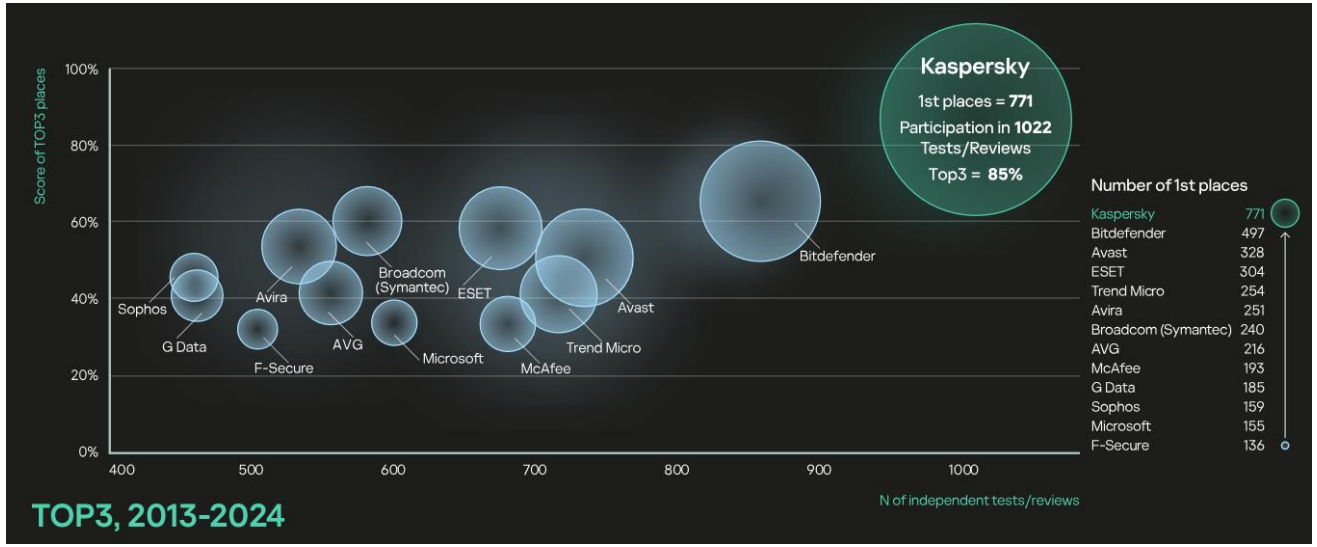
Network Security Controls

More...

Why Kaspersky

We are Kaspersky

1. 2013~2024參加獨立評測最多，偵測率第一，前三名比例最高。



2. 協助台灣客戶將更新主機移往新加坡、荷蘭等非敏感國家。

(三)卡巴斯基更新主機的資訊流向

卡巴斯基的更新伺服器位於許多國家與區域，包括加拿大、荷蘭、德國、法國、中國、香港、墨西哥、新加坡等。卡巴斯基的產品初始值會自行選擇最近且高可用度的伺服器來提供軟體更新，卡巴斯基用戶更可依自選需求設置特定位置的更新主機。**卡巴斯基亦於 2020 年開始將台灣用戶的產品更新初始值從香港轉移至新加坡，目前台灣客戶僅會向新加坡、荷蘭、德國、法國與加拿大的更新主機更新軟體、病毒碼與卡巴斯基安全網路資料庫(Kaspersky Security Network)，以保障客戶的隱私與下載安全。**相對於在台灣仍有營利的全球資安業者，卡巴斯基更主動對台灣客戶承擔資安廠商應負的責任。

3. AVTEST 評測，對抗勒索病毒防禦率最高。

AV-TEST The Independent IT-Security Institute Magdeburg Germany

Advanced Endpoint Protection: **Ransomware Protection test**

Date of report: September 30, 2021

The three assessment scenarios were independently developed and executed by the test lab:

- Real-World ransomware attacks user files on local system
- Real-World ransomware attacks user files on remote shared folder
- Proof of Concept ransomware attacks user files on local system

During the test, the products were expected to detect ransomware activity and its files, block it, roll-back any changes to user files (the other words, to protect all user files) and eliminate the threat from the targeted system. Only these results were considered a true success and the relevant solution was given a credit in each test case.

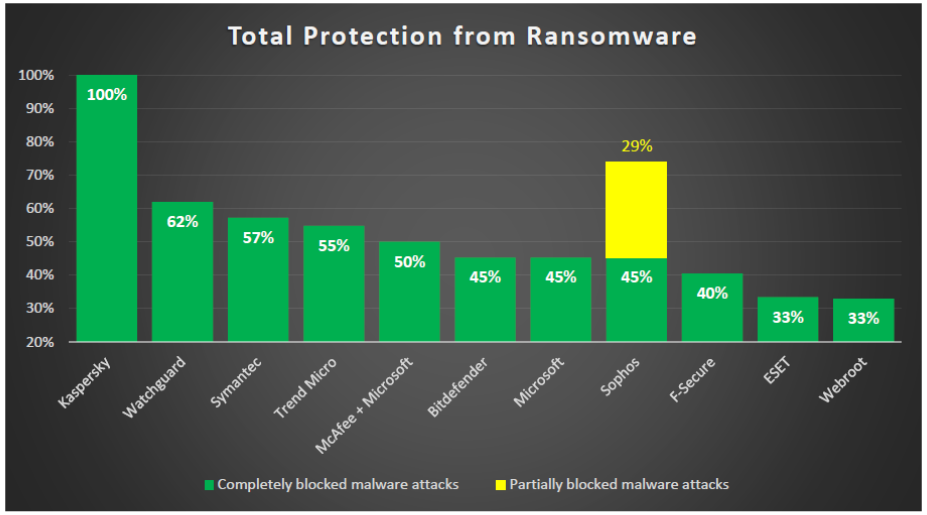


Figure 1. Total ransomware protection by different products basing on all three scenarios.
"Completely blocked" means that ransomware was detected, and all user files were protected.
"Partially blocked" means that ransomware was detected, but some user files were lost (not protected).
Arranged by "completely blocked" values.

GREAT: Cooperation with INTERPOL

- **Interpol Global Complex for Innovation, Singapore**
- **Kaspersky products, cyber alerts and services**
- **Digital forensics, Trainings, Investigation support**

全球機構對卡巴斯基威脅情報的肯定

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

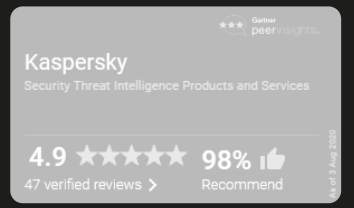
The quality of our intelligence is backed by our most tested and most awarded threat protection technologies

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

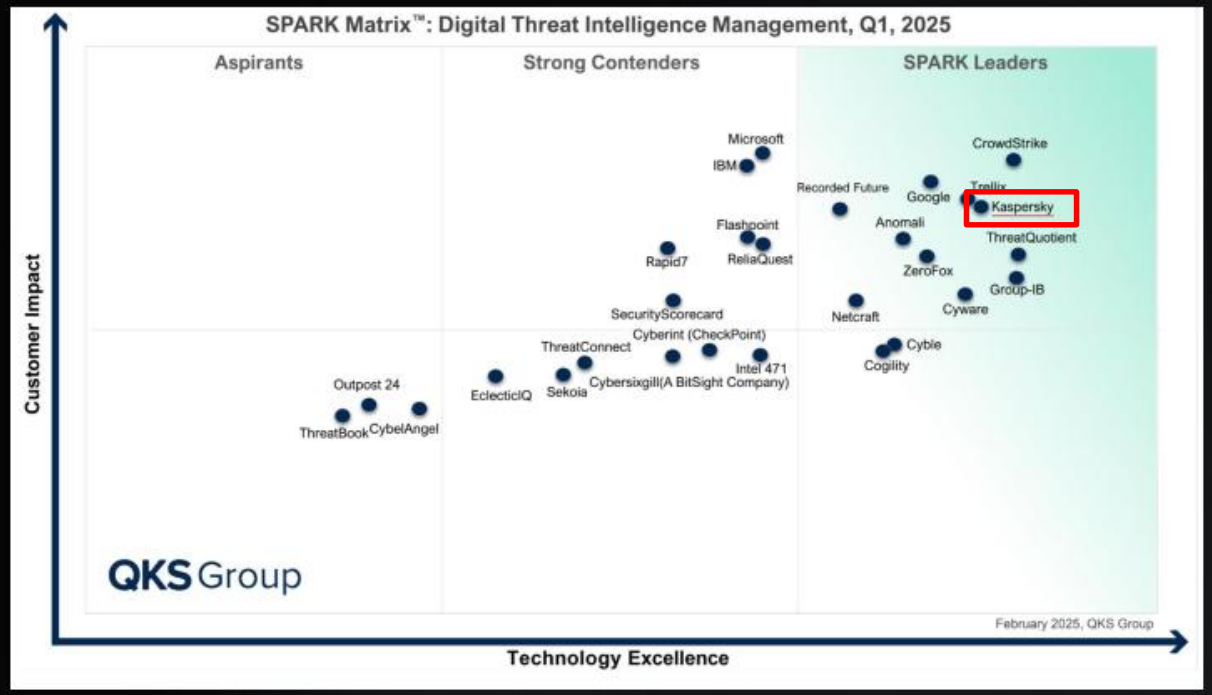
GIGAOM

"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

全球機構對卡巴斯基威脅情報的肯定

SPARK Matrix™: Digital Threat Intelligence Management, Q1, 2025*



QKS Group has named Kaspersky a Leader in the 2025 SPARK Matrix TM Digital Threat Intelligence Management

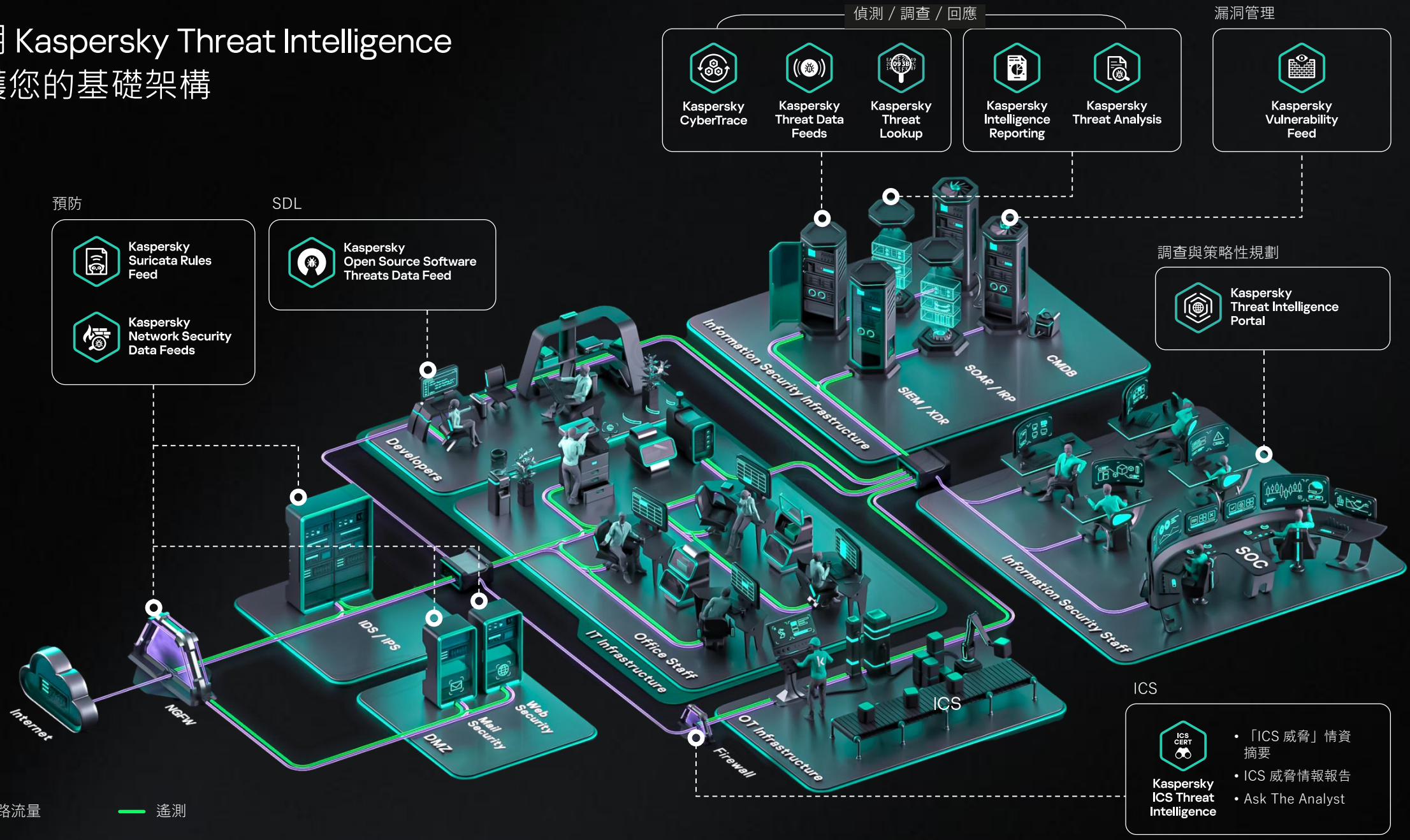
* February 2025, QKS Group

Frost Radar™

FROST & SULLIVAN

Frost&Sullivan has named Kaspersky a Leader in the Frost Radar : Cyber Threat Intelligence, 2024

利用 Kaspersky Threat Intelligence 保護您的基礎架構



Thank you!