Kaspersky Next

新一代安全

Xavier Wang 王士皇
0955-770-299
xavier.wang@kaspersky.com.tw

為何要選擇卡巴斯基?

A. 產品效能

- AV-TEST 國際評測:
  防護 / 效能 / 可用性
  長年維持滿分

B. 偵測率表現

- 統計數據第一：多年來在惡意程式偵測率上，穩居全球領先地位。

C. 功能完整性

- 全方位端點行為管理：涵蓋惡意程式偵測、威脅防護、合規管理。
- 符合資安法規：幫助企業遵循政府與產業資安規範。

D. 信任保障

- 全球唯一透明中心：提供原始程式碼檢驗與透明中心服務，確保軟體可信度。
- 台灣註冊分公司 + 政府共同供應契約。

透明且受到獨立機構認可

Proven.
Transparent.
Independent.

Kaspersky Global Transparency 計畫內含可供執行的具體措施，可讓關係人驗證及確認我們產品、內部流程與業務營運的可信度。

13

個遍佈全球的透明度中心

定期獨立評估

- SOC 2 稽核
- ISO 27001 認證

深入瞭解

漏洞賞金計畫

超重要的認可

卡巴斯基產品定期接受頂尖研究機構的獨立評估，而我們的網路安全專業能力一致獲得頂尖產業分析師的認可。

經過最多測試。獲獎最多。

逾十年來，卡巴斯基產品參加了 1022 次獨立評測，其中有 771 次奪冠，871 次登上前三名，證明我們提供的防護領先業界。

2024 年

95	91	97%
次評測	次奪冠	登上前 3 名

深入瞭解

為什麼要推出新方案 ？

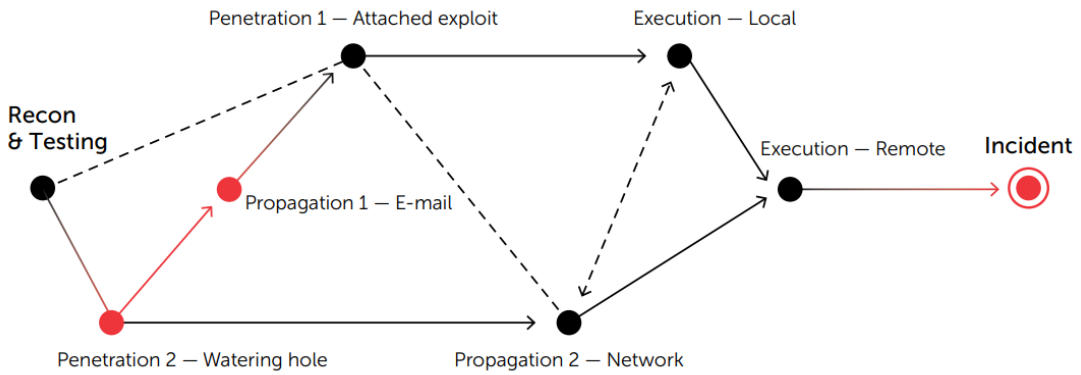
“新一代安全”

現今面對的挑戰

利用合法工具和無檔案式威脅 實施惡意攻擊 → 隱藏和躲避

需面對 有利益性的惡意攻擊（例如流行度高的勒索軟體） → 影響重大

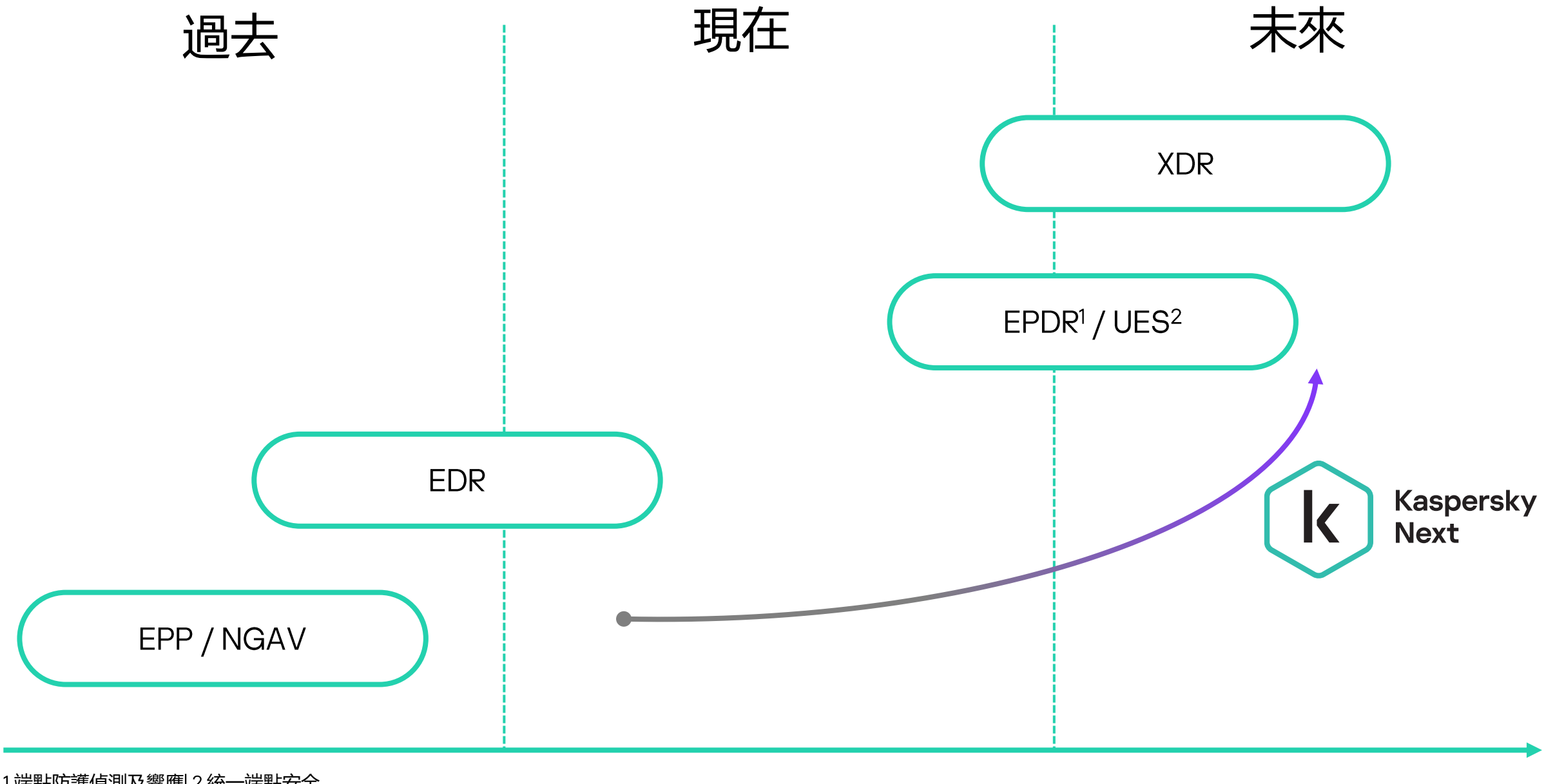
採用多重攻擊鏈階段 → 複雜持續性長



企業意識到：

- 威脅數量上升
- 攻擊場景日益複雜
- 威脅的財務影響
- 必須解決的合規性問題

端點防護（EPP）需要包含EDR的功能



1 端點防護偵測及響應| 2 統一端點安全

Kaspersky Next 產品價值定位

Kaspersky Next

在强大的端點防護機制下，利用 EDR 和 XDR 提高安全及優化維運

Kaspersky Next EDR Foundations

為每個人提供強大的安全防護

防護所有端點

1、提供企業基本安全需求
2、減少攻擊面威脅
3、增加可視性

Kaspersky Next EDR Optimum

加强防禦

通過必要的調查和響應措施提高對未知風險的安全性

1、提供企業自動化響應機制
2、定期清查內部可疑主機
3、提供主機安全加固功能

Kaspersky Next XDR Expert

擴展至其他安全防護範圍

防護您的企業免受最複雜，最新的網路威脅

1、提供整合端點及其他安全機制平台
2、整合端點外的安全防護機制

Kaspersky Next: 提供核心網路安全服務

第3階段

複雜和類似 APT 的攻擊

卡巴斯基專家安全

較高的 IT 安全能力或 SOC 團隊

Kaspersky Next

卡巴斯基 Next XDR 專家版

- Internal Expertise
  - Kaspersky Cybersecurity Training
- Intelligence
  - Kaspersky Threat Intelligence
- Extended Detection and Response
  - Native XDR
    - Kaspersky Anti Targeted Attack
  - Open XDR
    - Kaspersky Extended Detection and Response
- Assessment
  - Kaspersky Security Assessment
  - Kaspersky Compromise Assessment
- Expert guidance
  - Kaspersky SOC Consulting
- Investigation
  - Kaspersky Incident Response
- People
  - Kaspersky Security Awareness Ultimate

第2階段

規避性威脅

卡巴斯基最佳安全解決方案

IT 安全

卡巴斯基 Next EDR 優選版

- People
  - Kaspersky Security Awareness Advanced
- Detection Enrichment
  - Kaspersky Threat Intelligence Portal

第1階段

基礎威脅

卡巴斯基安全基礎

IT

卡巴斯基 Next EDR 基礎版

- Embedded
  - Kaspersky Embedded Systems Security
- Virtual server, VDI, cloud
  - Kaspersky Hybrid Cloud Security
- Network
  - Kaspersky Security for Mail Server
  - Kaspersky Security for Internet Gateway
- Data
  - Kaspersky Security for Storage
- People
  - Kaspersky Security Awareness Essential
- Support
  - Kaspersky Premium Support and Professional Services

Kaspersky Managed Detection and Response

威脅情報應用及案例分享

場景一：
提昇現有自動化阻擋及偵測機制：
Kaspersky Threat Data Feeds
威脅情報摘要

Kaspersky 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

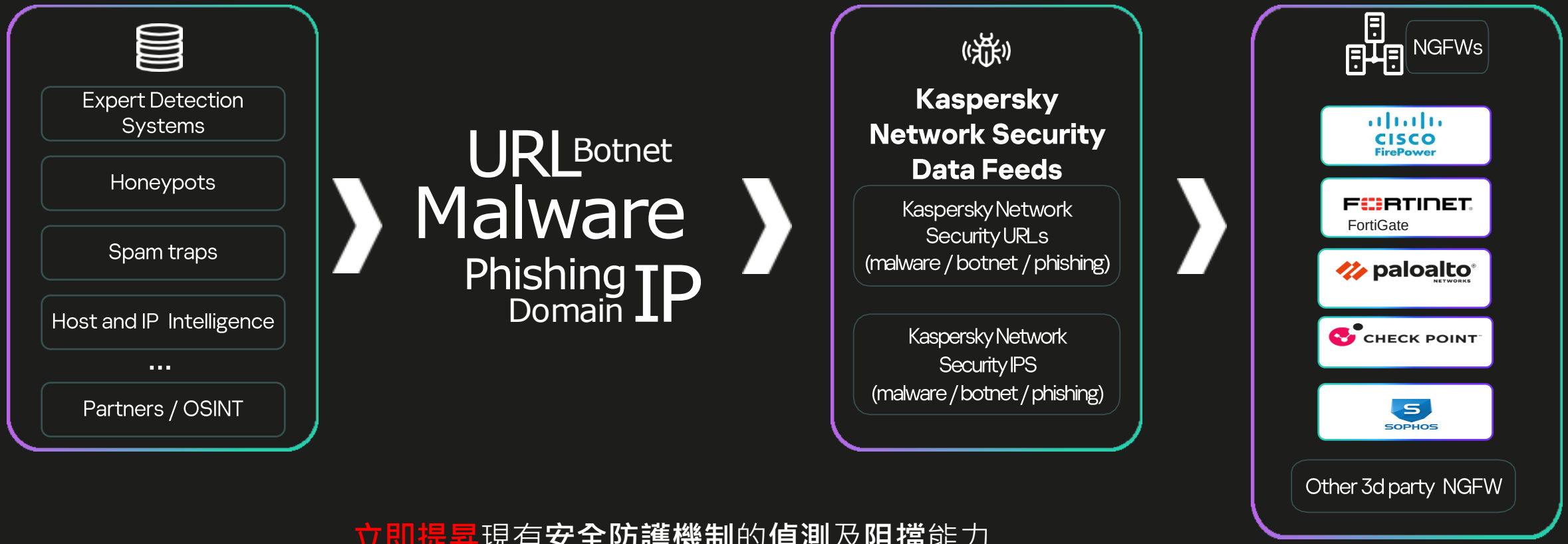
快速將各種威脅情報來源投入運作，並減輕 SIEM 的工作負載

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

透過網路安全 Data Feeds 整合應用案例分享

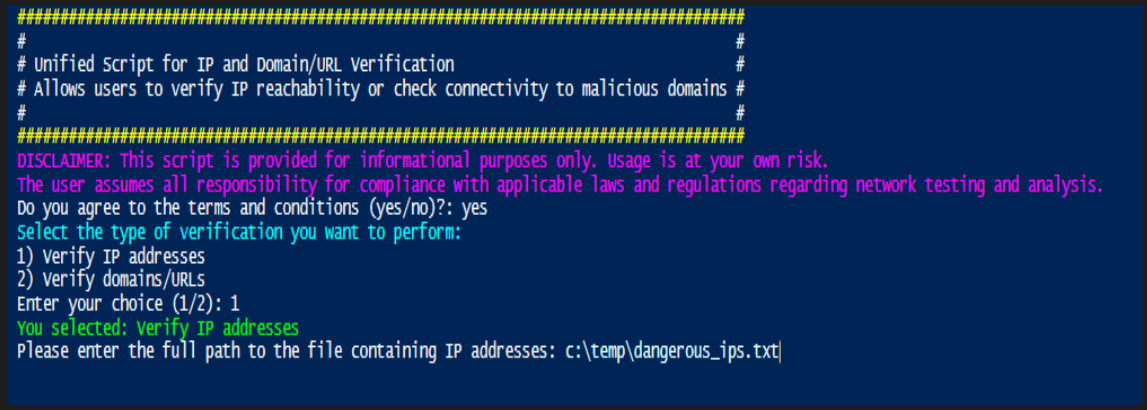


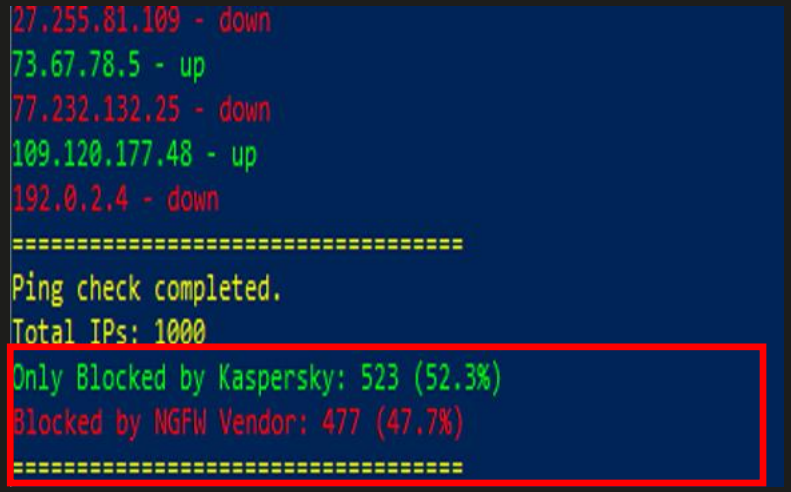
立即提昇現有**安全防護機制**的**偵測**及**阻擋**能力

kaspersky

檢驗方式

- 只需2個材料:
  - 只要有 NGFW + 卡巴 feeds (IP & URL)
- 提供現有威脅情報清單:
  - 提供現有惡意清單
- 隨插即用 Plug-and-Play :
  - 在被 NGFW保護的 Windows PC上 執行 PowerShell 腳本即可
- 4 種測試連線方式:
  - ICMP
  - Minimal TCP Handshake
  - HTTP HEAD request
  - TLS Handshake (443)
- 立即可看到的結果:
  - 統計有多少連線可被防火牆阻擋





可支援整合多種不同平台及多種應用

SIEM / SOAR / IRP

Radar, McAfee, ArcSight, RSA, splunk>, AlienVault, DFLABS, Microsoft, Fortinet, elastic, Resilient, Phantom, LogRhythm

Threat Intelligence Platforms

ThreatQ, ThreatConnect, Anomali, AlienVault, Arctic Security, MISP Threat Sharing, eclectic iq

Network Security Controls

paloalto networks, Fortinet, Suricata, Cisco FirePower

More...

有獎徵答!

www.kaspersky.com.tw

#kaspersky
#bringonthefuture