

運用「高階情資」與「專家檢測服務」 建構安全中心

卡巴斯基 謝長軒

chandler.hsieh@kaspersky.com.tw

兵不厭詐，這是戰爭



故知兵者，動而不迷，舉而不窮。
故曰：知彼知己，勝乃不殆；
知天知地，勝乃不窮。

知彼知己，勝乃不殆
知天知地，勝乃可全
- 孫子兵法

準備好面對各種威脅挑戰嗎？



安全團隊應該有多快的響應速度才夠？



Ransomware cases

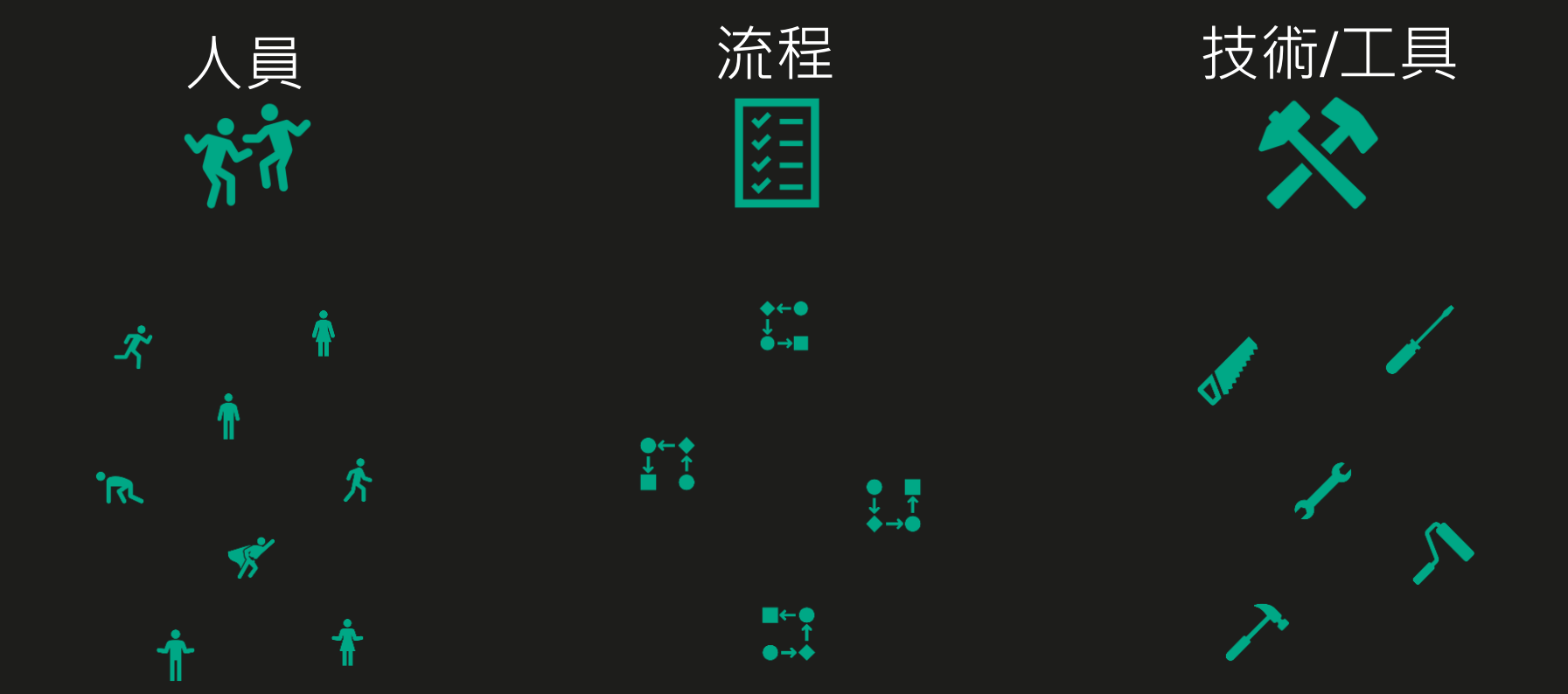
Distribution of attacks by duration based on initial vector

Initial attack vector	Attack duration					Grand total
	Hours	Days	Weeks	Months	Years	
Compromised accounts	9.52%	2.38%	4.76%	7.14%	0.00%	23.81%
Exploitation of public-facing applications	4.76%	14.29%	9.52%	11.90%	2.38%	42.86%
External remote services	2.38%	4.76%	2.38%	0.00%	0.00%	9.52%
Malicious email	2.38%	2.38%	2.38%	4.76%	0.00%	11.90%
Trusted relationships	0.00%	2.38%	0.00%	2.38%	0.00%	4.76%
Hardware additions	2.38%	0.00%	0.00%	0.00%	0.00%	2.38%
Other	2.38%	2.38%	0.00%	0.00%	0.00%	4.76%
Grand total	23.81%	28.57%	19.05%	26.19%	2.38%	100.00%

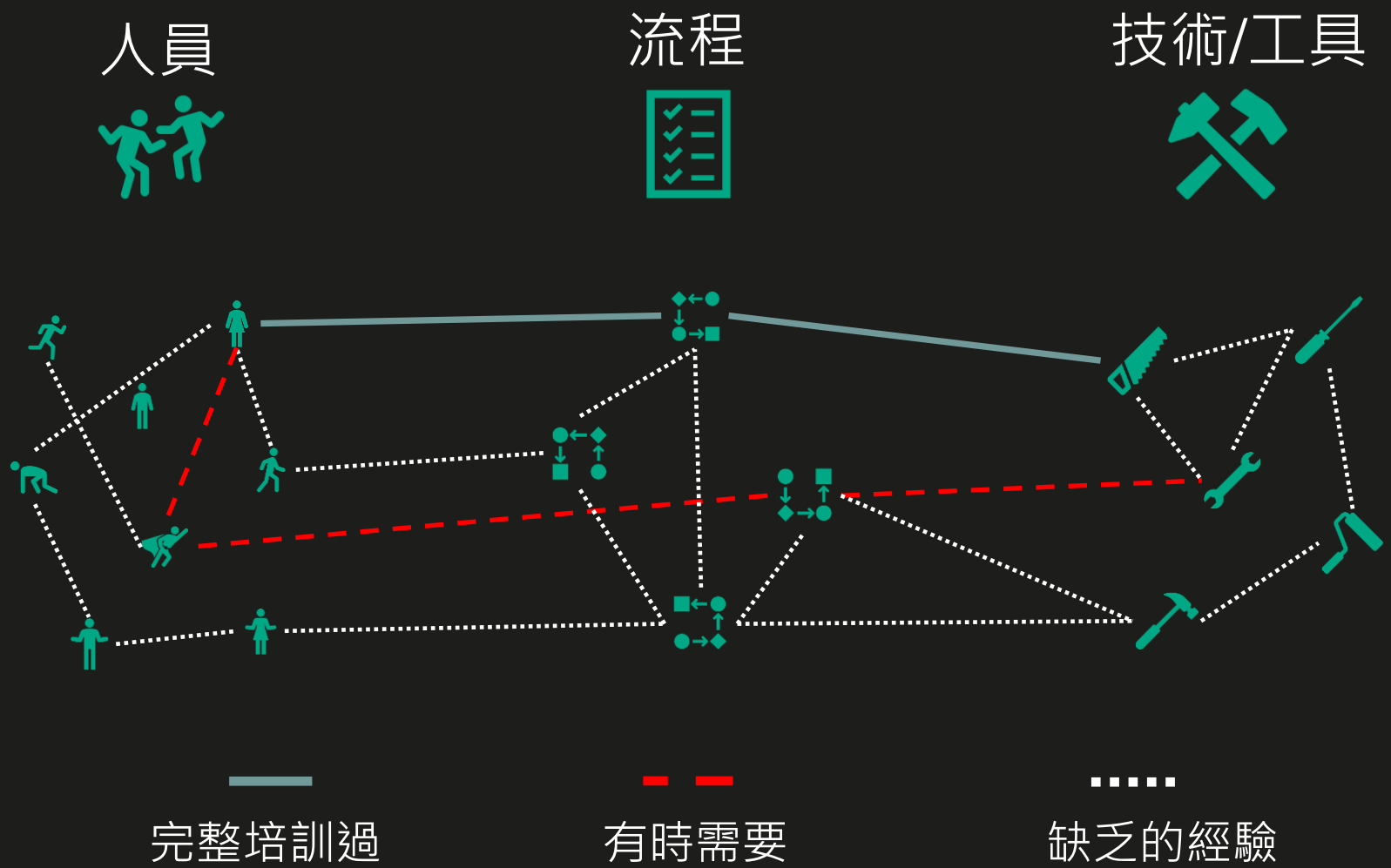
威脅響應統計數據

	造成影響時間 Mean time to impact	偵測時間 Mean time to detect Kaspersky MDR service	響應時間 Mean time to respond IR service from initial request to restored timeline
快速攻擊 >50% 幾小時 到 幾天 譬如: Ransomware	1 天	41.45 分鐘	29.4 小時
現代化攻擊 超過 7 天 勒索病毒及資料竊取	14 天	34.8 分鐘	48.3 小時
持續性攻擊(APT) >幾個月 資料外洩 及 勒索病毒	94.5 天	40.24 分鐘	60.13 小時

SOC 安全團隊



目標：訓練前



目標：訓練後

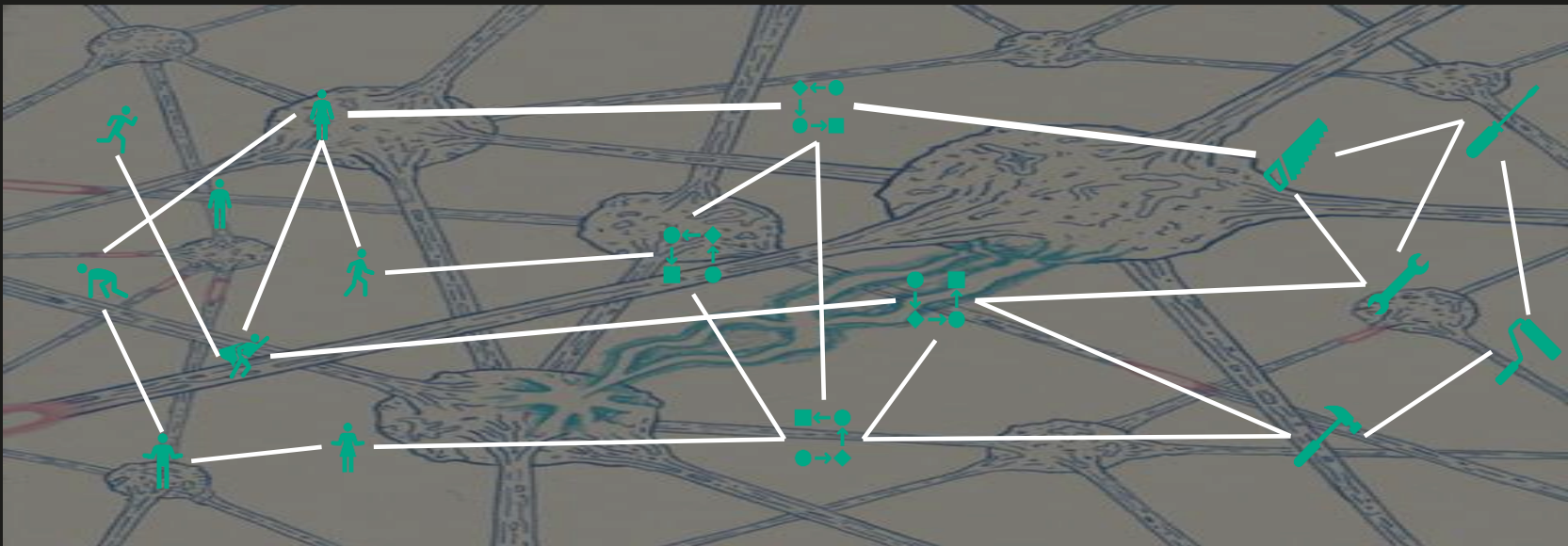
人員



流程



技術/工具



成為DNA的一部份

SOC 能力評估



服務

- 安全事件監控
- 事件響應
- 威脅情資
- 記錄管理
- 惡意程式分析



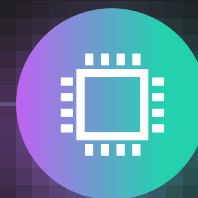
團隊人員

- Team size
- Shift rosters
- Roles
- Profiles, skillsets
- Assistance with hiring
- Training
- Onboarding



流程

- Alert Registration
- Incident Handling
- Use Case Management
- Threat Hunting
- Threat Intelligence
- Engineering
- Management



技術/工具

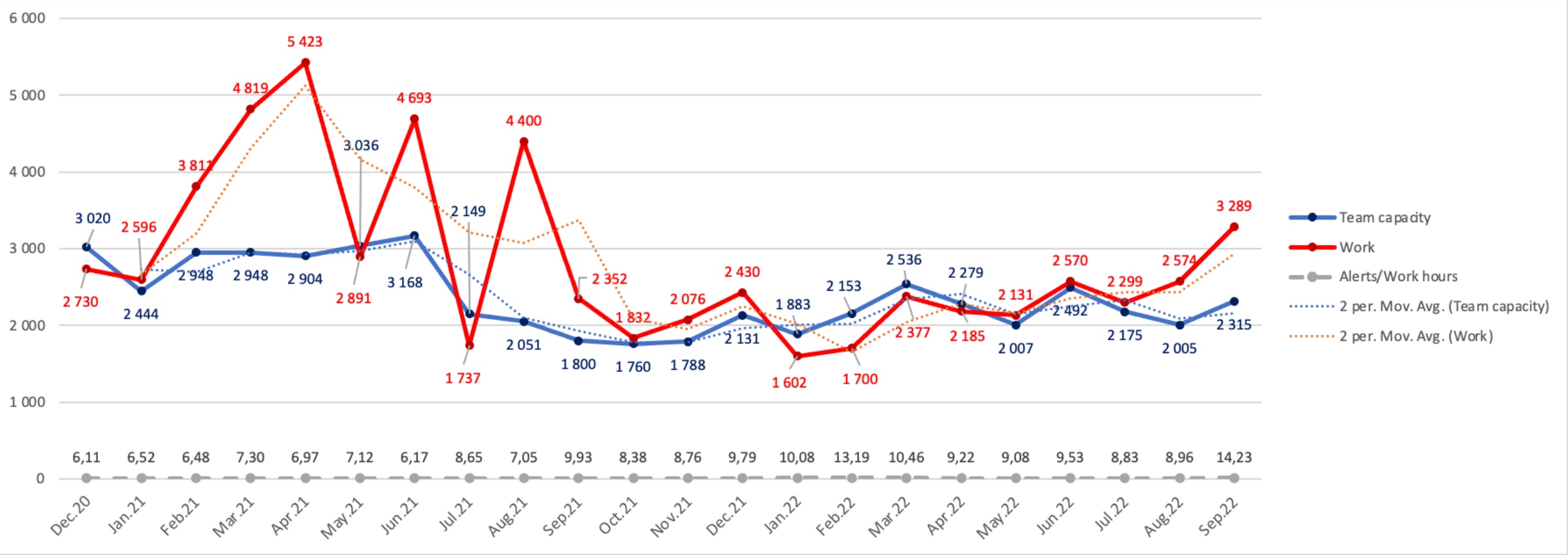
- SIEM
- Ticketing
- IRP / SOAR
- Threat Intel
- Forensics
- Knowledge Base

是維運soc或是僅做事件記錄的保存

常見情形: 未定義清楚，只好先保存所有記錄

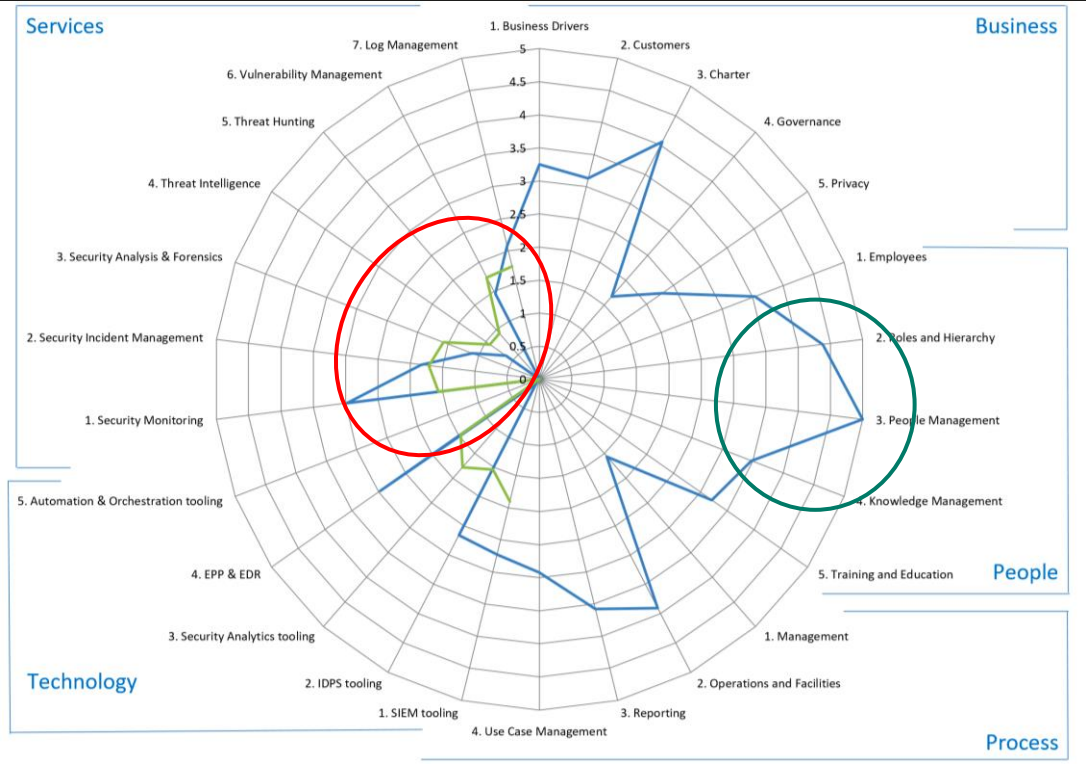


檢視現有SOC處理能力的評估及升級計劃



團隊能處理的能力 = Metrics + Forecasts = MTT{D,R}

SOC 成熟度評估、架構開發、流程設計



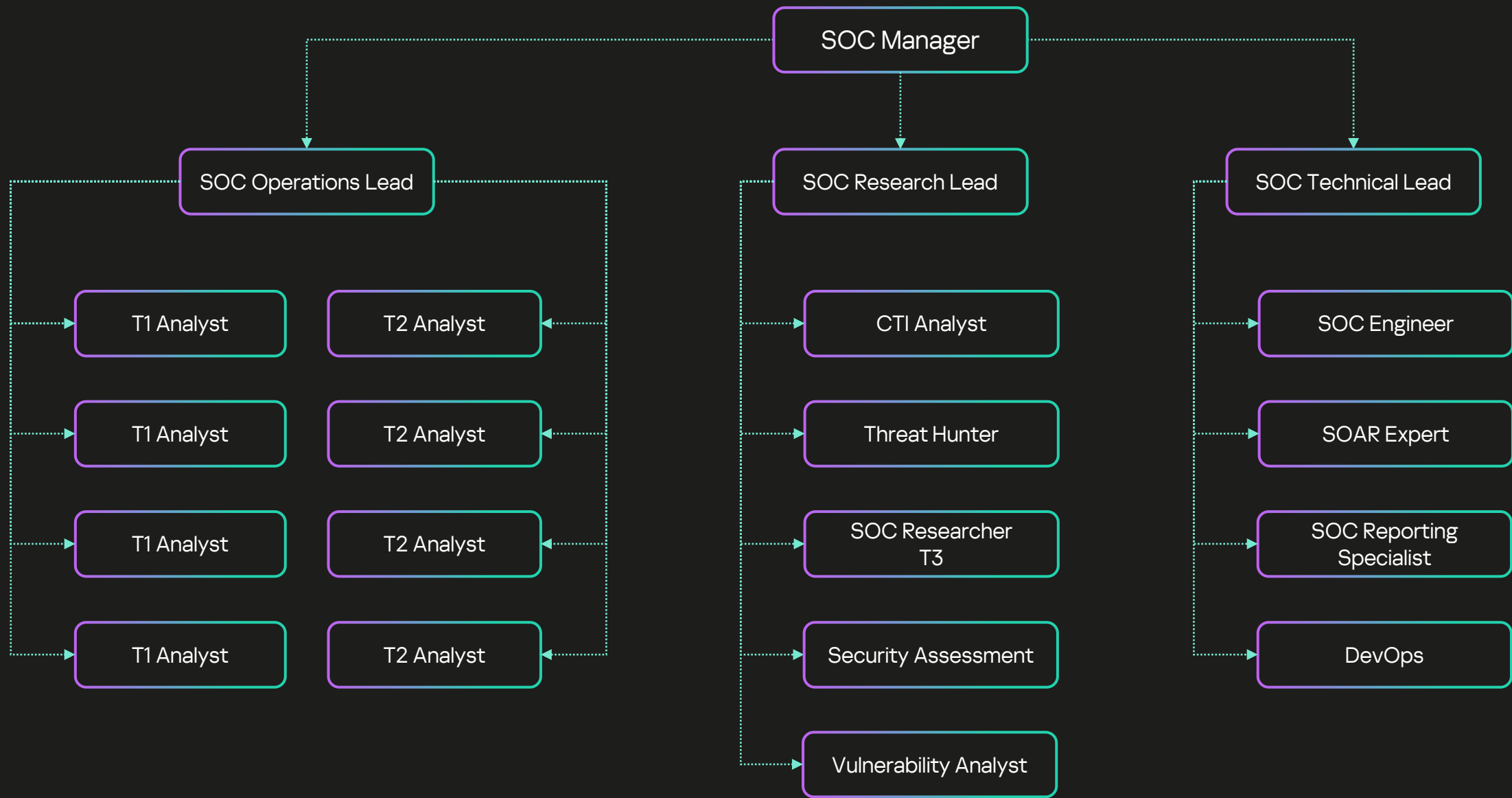
Weak domains

Strong domains

Current

Target

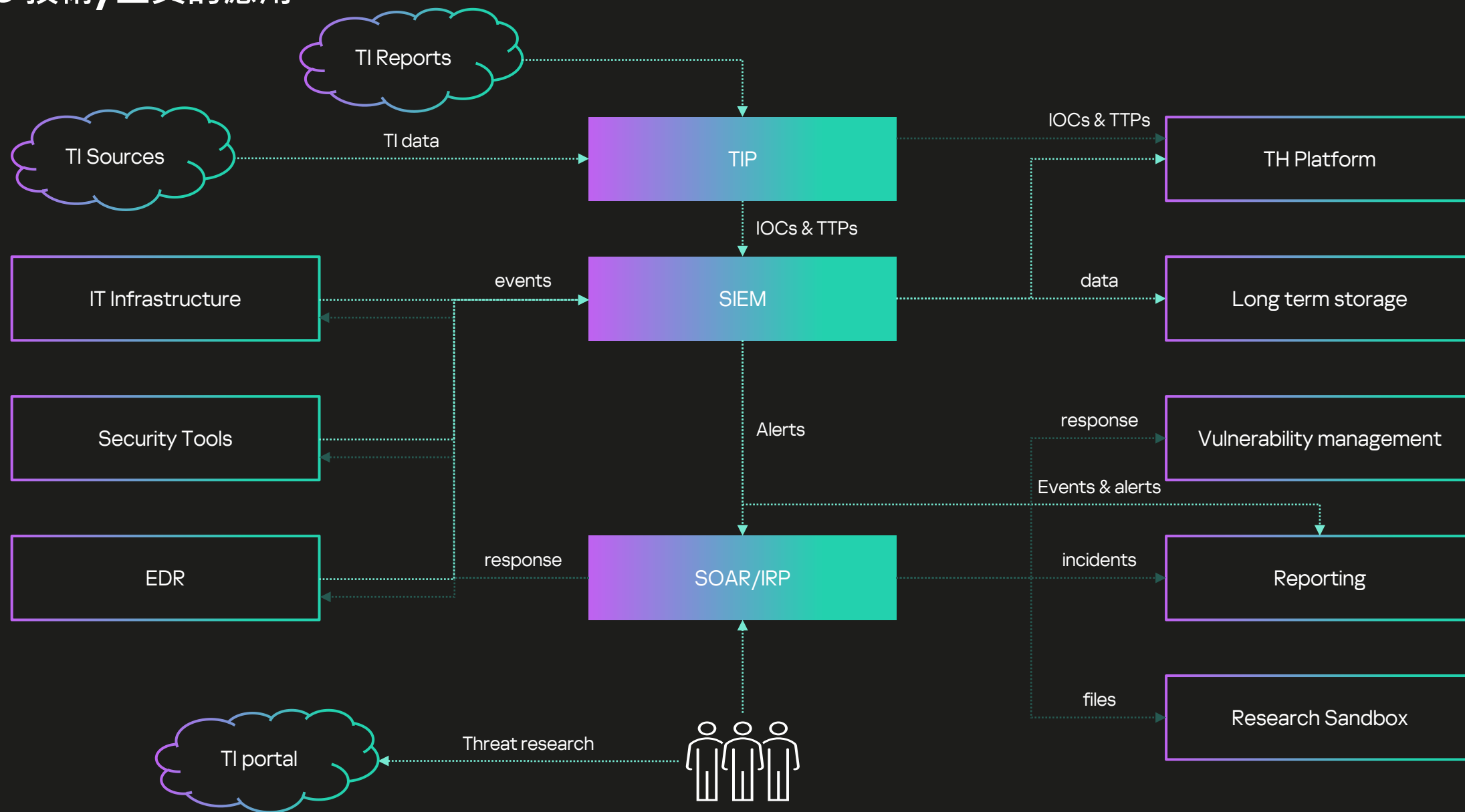
SOC 團隊建立



SOC 程序/流程設計



SOC 技術/工具的應用



常見SOC安全團隊的挑戰

- 如何了解組織可能受到入侵威脅的管道?
- 面對威脅的反應時間是否足夠?
- 是否了解當發生事件時的響應步驟?

三種提昇企業安全維運能力的方式



武裝化

提升內部專家團對面對複雜
威脅事件處理及優化調查流
程時的相關工具



知識化

提升及豐富對抗進階安
全威脅的知識水平



實戰演習

透過外部專家單位進行實
際演練確保面對複雜威脅
時的相關響應工作及流程

三種提升企業安全維運能力的方式



武裝化

提升內部專家團對面對複雜
威脅事件處理及優化調查流
程時的相關工具



知識化

提升及豐富對抗進階安
全威脅的知識水平



實戰化

透過外部專家單位進行實
際演練確保面對複雜威脅
時的相關響應工作及流程

Kaspersky 安全平台

知識化

威脅情報分享

- Threat Data Feeds
- 威脅情報平台 (CyberTrace)
- 威脅查找
- 威脅溯源引擎 (KTAE)
- APT 威脅報告
- 雲端分析沙箱
- 數位軌跡情報 (Digital Footprint Intelligence)
- 特定行業威脅情報 (Financial, ICS, Transport)
- 詢問專家服務 (Ask the Analyst)

專家培訓

- 事件響應培訓
- 數位取證培訓
- 惡意分析及逆向工程培訓
- YARA 規則撰寫培訓
- 威脅情境討論

提升內部
處理知識及
能力

武裝化

原生式 XDR
開放式 XDR



關鍵任務
支援團隊

實戰化

安全評估

- 對手攻擊模擬 (Adversary Attack Emulation)
- 入侵檢測安全評估 (Targeted Attack Discovery)
- 滲透測試
- 紅隊演練 (Red Teaming)
- 應用程式安全評估服務
- 特定行業安全評估服務 (ICS, Payment Systems, Transportation, IoT)
- SOC 顧問
- 事件調查準備顧問服務

響應服務

- Managed Detection and Response (MDR Expert)
- 事件響應
- 惡意程式分析
- 數位取證

三種提升企業安全維運能力的方式



武裝化

提升內部專家團對面對複雜
威脅事件處理及優化調查流
程時的相關工具



知識化

提升及豐富對抗進階安
全威脅的知識水平



實戰演習

透過外部專家單位進行實
際演練確保面對複雜威脅
時的相關響應工作及流程

Kaspersky 安全平台

知識化

威脅情報分享

- Threat Data Feeds
- 威脅情報平台 (CyberTrace)
- 威脅查找
- 威脅溯源引擎 (KTAE)
- APT 威脅報告
- 網路犯罪威脅報告
- 雲端分析沙箱
- 數位軌跡情報 (Digital Footprint Intelligence)
- 特定行業威脅情報 (Financial, ICS, Transport)
- 詢問專家服務 (Ask the Analyst)

專家培訓

- 事件響應培訓
- 數位取證培訓
- 惡意分析及逆向工程培訓
- YARA 規則撰寫培訓
- 威脅情境討論

提升內部
處理知識及
能力

武裝化

原生式 XDR
開放式 XDR

Kaspersky
Anti Targeted
Attack Platform

Kaspersky
Endpoint Detection
and Response Expert

關鍵任務
支援團隊

實戰演習

安全評估

- 對手攻擊模擬 (Adversary Attack Emulation)
- 入侵檢測安全評估 (Targeted Attack Discovery)
- 滲透測試
- 紅隊演練 (Red Teaming)
- 應用程式安全評估服務
- 特定行業安全評估服務 (ICS, Payment Systems, Transportation, IoT)
- SOC 顧問
- 事件調查準備顧問服務

響應服務

- Managed Detection and Response (MDR Expert)
- 事件響應
- 惡意程式分析
- 數位取證

Kaspersky 安全平台

知識化

威脅情報分享

- Threat Data Feeds
- 威脅情報平台 (CyberTrace)
- 威脅查找
- 威脅溯源引擎 (KTAE)
- APT 威脅報告
- 網路犯罪威脅報告
- 雲端分析沙箱
- 數位軌跡情報 (Digital Footprint Intelligence)
- 特定行業威脅情報 (Financial, ICS, Transport)
- 詢問專家服務 (Ask the Analyst)

專家培訓

- 事件響應培訓
- 數位取證培訓
- 惡意分析及逆向工程培訓
- YARA 規則撰寫培訓
- 威脅情境討論

提升內部
處理知識及
能力

武裝化

原生式 XDR
開放式 XDR



Kaspersky
Anti Targeted
Attack Platform



Kaspersky
Endpoint Detection
and Response Expert

關鍵任務
支援團隊

實戰演習

安全評估

- 對手攻擊模擬 (Adversary Attack Emulation)
- 入侵檢測安全評估 (Targeted Attack Discovery)
- 滲透測試
- 紅隊演練 (Red Teaming)
- 應用程式安全評估服務
- 特定行業安全評估服務 (ICS, Payment Systems, Transportation, IoT)
- SOC 顧問
- 事件調查準備顧問服務

響應服務

- Managed Detection and Response (MDR Expert)
- 事件響應
- 惡意程式分析
- 數位取證

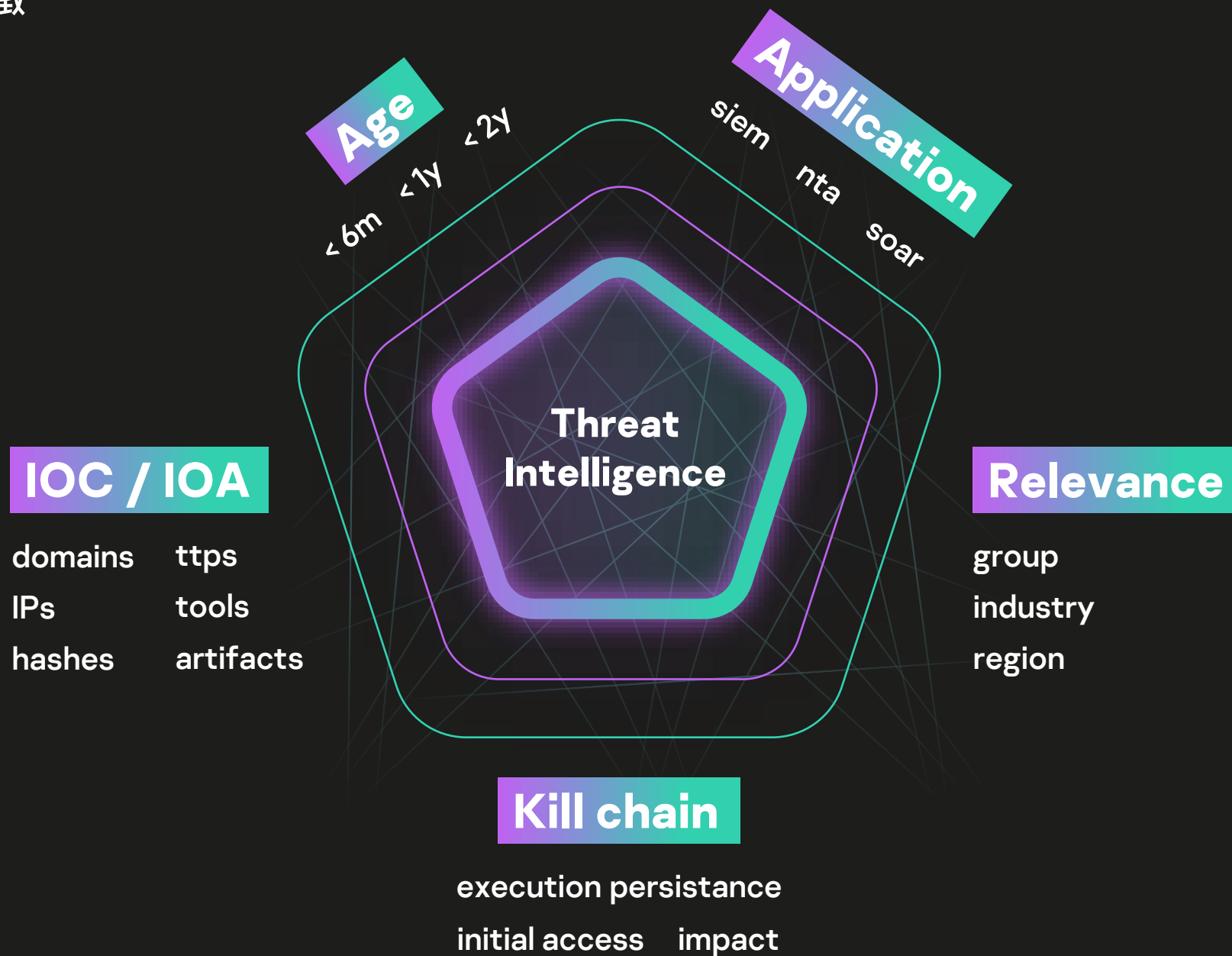
Kaspersky Threat Intelligence



不斷變化的網路安全挑戰



主要威脅情報特徵



Threat intelligence 類型

Technical



#Feeds
#MRTI
#Correlation

Operational



#Investigations
#Research

Tactical



#TTPs
#Actors

Strategic



#Trends
#Targeted TI

Plan

- Build CTI Framework
- Stay up to date with threat landscape

Respond

- Reduce response time
- Response automation
- Malicious domains takedown

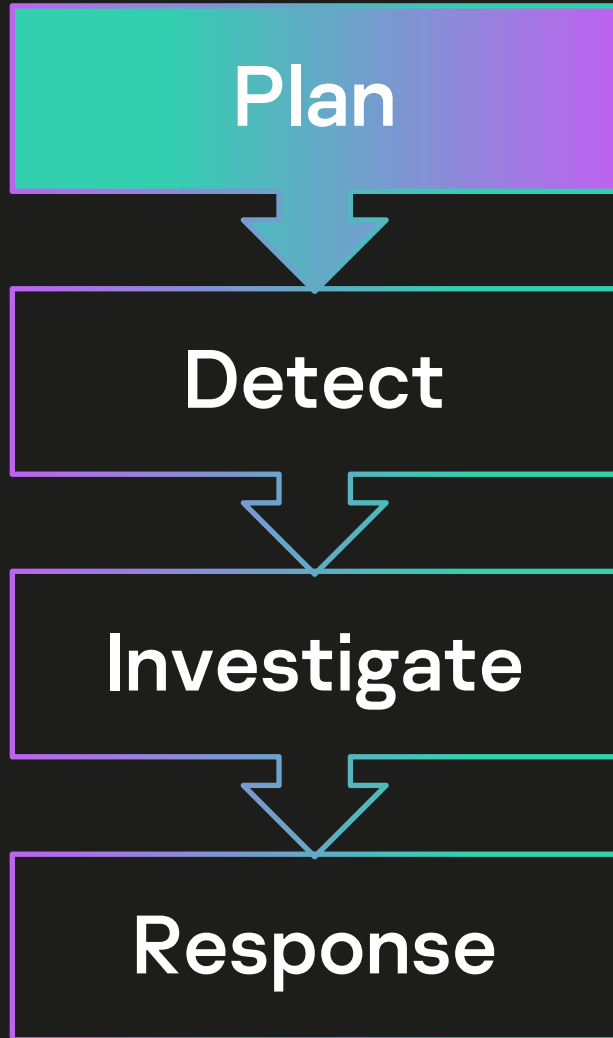


Detect

- Improve detection rate
- Reduce detection time
 - Dark web monitoring

Investigate

- Context enrichment
 - Attacks attribution
 - Malware detonation

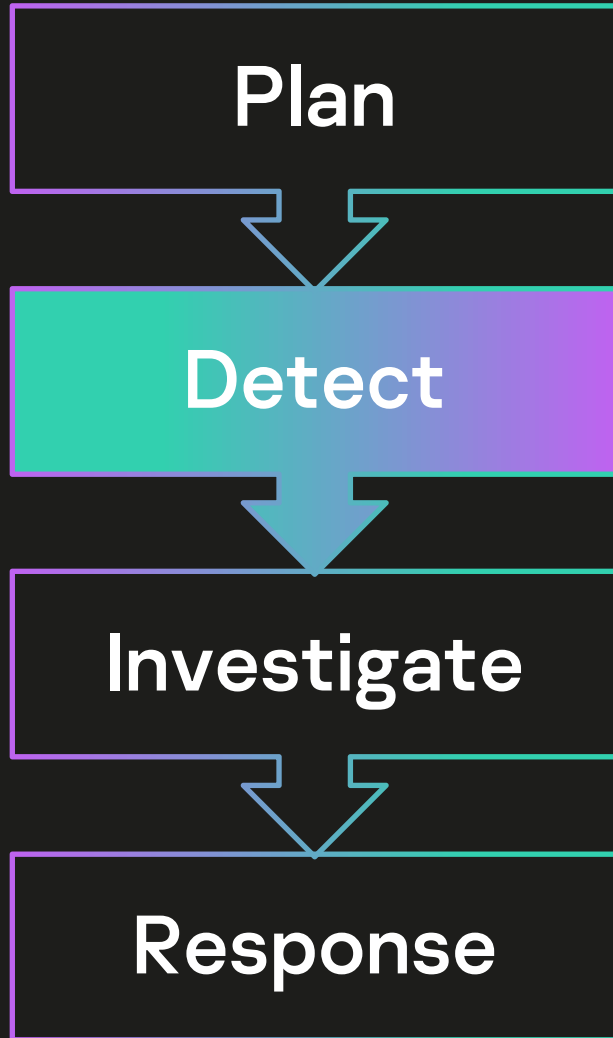


- Issues:**
- Too many threats
 - Not enough resources to prevent all

Stage goal: Structure and systemize cyber security approach

TI role: Threat landscape identification

- Outcomes:**
- Attack surface is visible
 - Attack vectors are identified
 - Actors profiles are clear
 - Processes are established

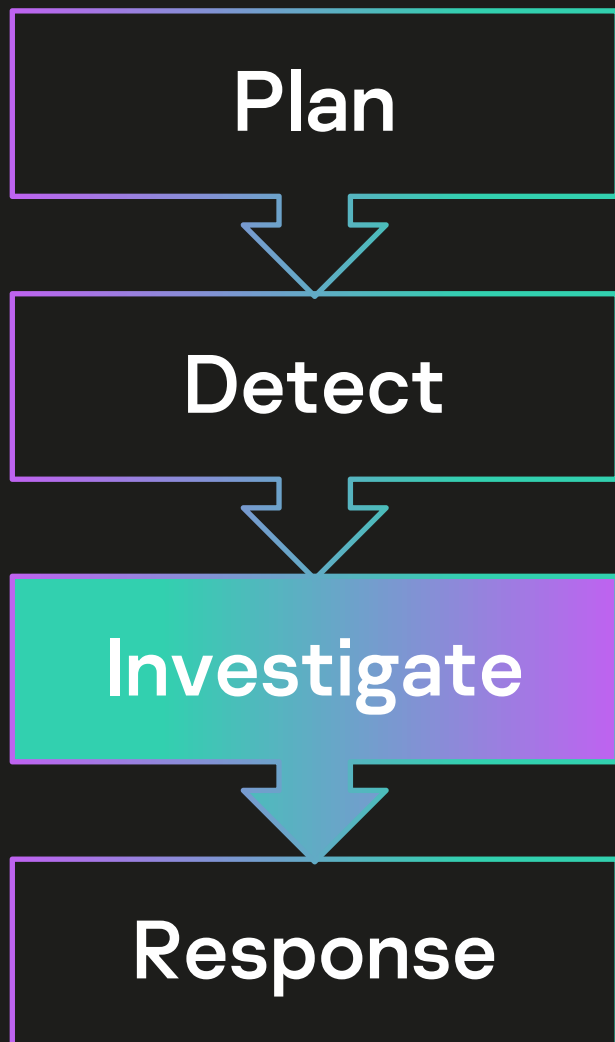


- Issues:**
- Poor detection level
 - Lurking threats in customers infrastructure

Stage goal: Detect malicious activities as early as possible

TI role: Detection capabilities improvement

- Outcomes:**
- Traditional detection technologies are reinforced with TI data
 - Incident card enrichment: Feeds (IOC) -> SIEM (Alert) -> SOAR (Request) -> TIP (Threat Data)
 - Additional sources of information are added (researchers reports, data from surface/dark web)

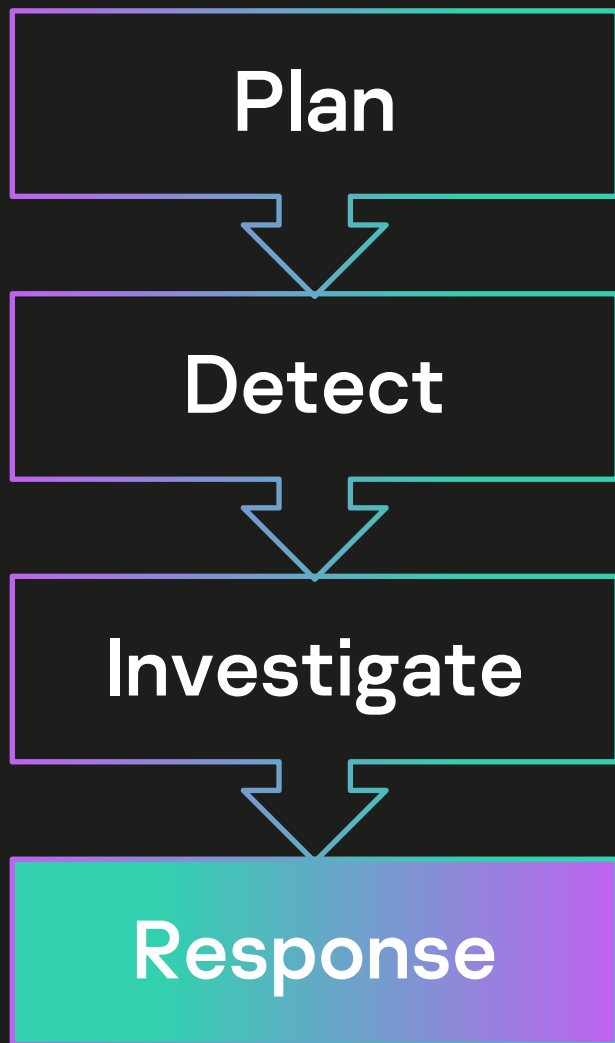


- Issues:**
- Too much information to analyze
 - Lack of information to take decision

Stage goal: Get clear picture of situation

TI role: Incident analysis process enrichment with context information about incident's artifacts such as hash, IP, domain

- Outcomes:**
- Detailed understanding of what happened and how
 - Incident context and scope is clear
 - Other potential related issues are evaluated



- Issues:**
- Not enough competence
 - Some actions need to be done externally

Stage goal: Incident consequences elimination

TI role: Expert support of the process

- Outcomes:**
- Incident response is done effectively
 - Malicious and phishing domains are stopped
 - Fake accounts in social network are deleted

Kaspersky 威脅智能情報



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 來源

KSN

Web crawlers

BotFarms

Spam traps

Sensors

Passive DNS

Partners

OSINT

GREAT

Kaspersky
APT Research
team



Kaspersky
SOC



Kaspersky
Red Team



Kaspersky
ICS CERT



Kaspersky
Threat
Intelligence



用戶

Kaspersky 威脅資料提供 (Data Feed)

IP REPUTATION FEED

HASH FEED (WIN / *nix / MacOS / AndroidOS / iOS)

ICS HASH FEED

INDUSTRIAL VULNERABILITY

FEED IN OVAL

URL FEEDS (Malicious, Phishing and C&C)

RANSOMWARE URL FEED

APT IOC FEEDS

CRIMEWARE FEEDS

VULNERABILITY FEED

PASSIVE DNS (pDNS) FEED

IoT URL FEED

SURICATA RULES

TRANSFORMS

FOR MALTEGO

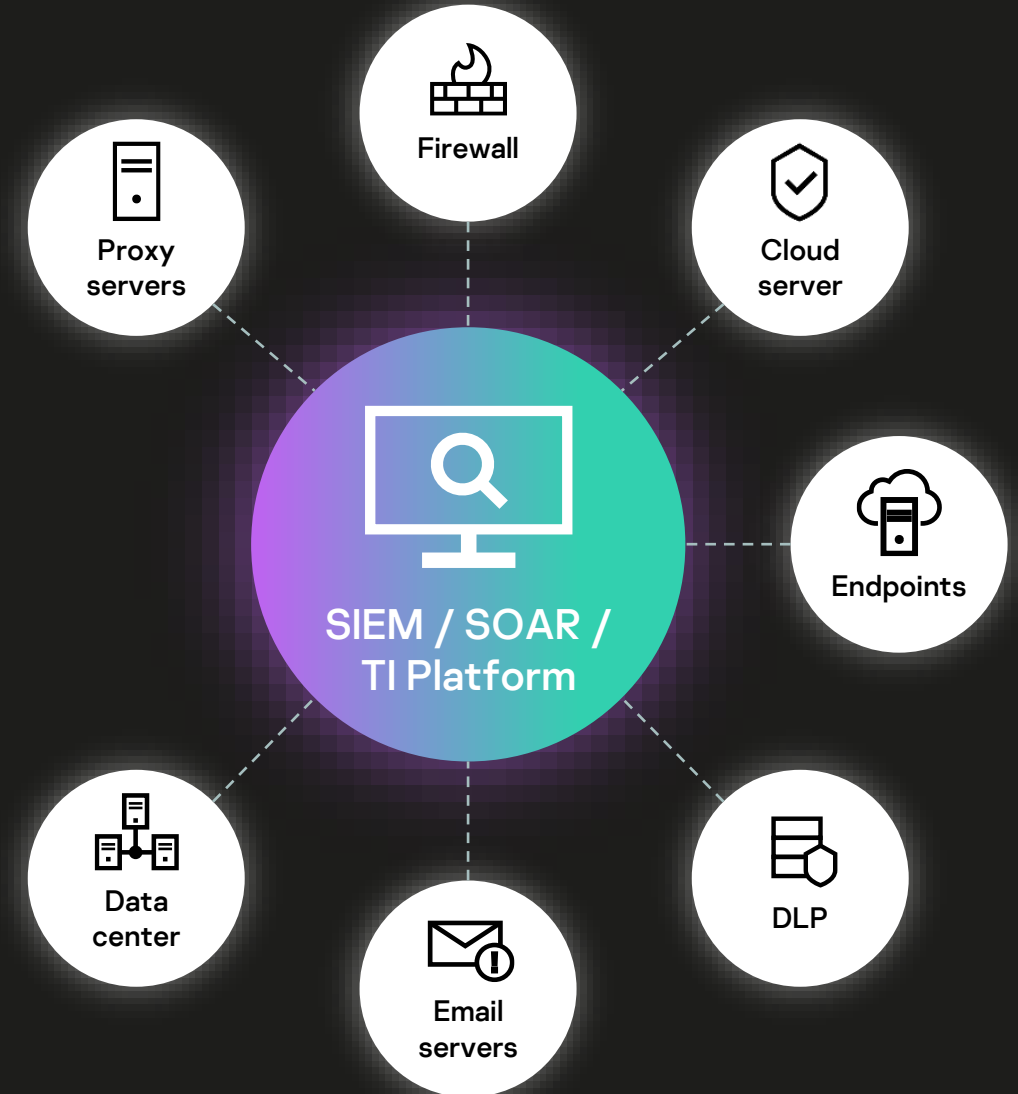
CLOUD ACCESS SECURITY BROKER (CASB) FEED

OPEN SOURCE SOFTWARE THREATS

REGION-SPECIFIC FEEDS



**Kaspersky
Threat Data
Feeds**



Kaspersky APT/網路犯罪/工控安全 Threat Intelligence Reporting

TLP: AMBER

Kaspersky APT Intel

kaspersky

Researcher Notes – Operation Triangulation: iOS devices targeted with previously unknown malware

Report Id: 20230602

Version: 1.0 (01.Jun.2023)

Executive Summary

This report is an early-warning regarding a long-standing campaign we are currently tracking under the name “Operation Triangulation”. It involves a previously unknown iOS malware platform distributed via zero-click iMessage exploits. Kaspersky employees were affected by this threat.

This release constitutes our first public announcement about this campaign, as we are in the process of getting in touch with industry partners to assess the prevalence of this threat. In addition, we provide a forensic methodology in the hopes that it will help readers determine whether their organization is targeted by the unknown group behind these attacks.

Our findings in a nutshell:

- A previously unknown actor has been infecting iOS devices since 2019 using zero-click iMessage exploits, by sending specially crafted messages with attachments;
- The malicious toolset consists of several stages, including parts that disable installation of iOS updates and also remove most of the traces of infection;
- The final payload, that is a fully-featured APT platform, runs in-memory without persistence, and devices are reinfected after reboot if needed.

This Report is composed of Kaspersky researchers’ findings. Although it has been peer reviewed to ensure its quality, it’s aimed towards sharing actionable, partial intelligence in a timely manner and therefore may not contain all the information we usually provide. For more information please contact: intelreports@kaspersky.com

This Report has been compiled by AO Kaspersky Lab (“Rightholder”) in accordance with the terms and conditions set forth in the Service Agreement with the User. Information in this Report is solely for informational purposes and cannot be used for other purposes or deemed as official proof. The Rightholder shall not be held liable to anyone in relation to this Report, including for any inappropriate or improper use of the Service by the User. Information in this Report is confidential and is intended solely for internal use by the User. No information in the Report may be shared with third parties unrelated to the User and/or made available to the public.

Threat actor profiles

Mapping to 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

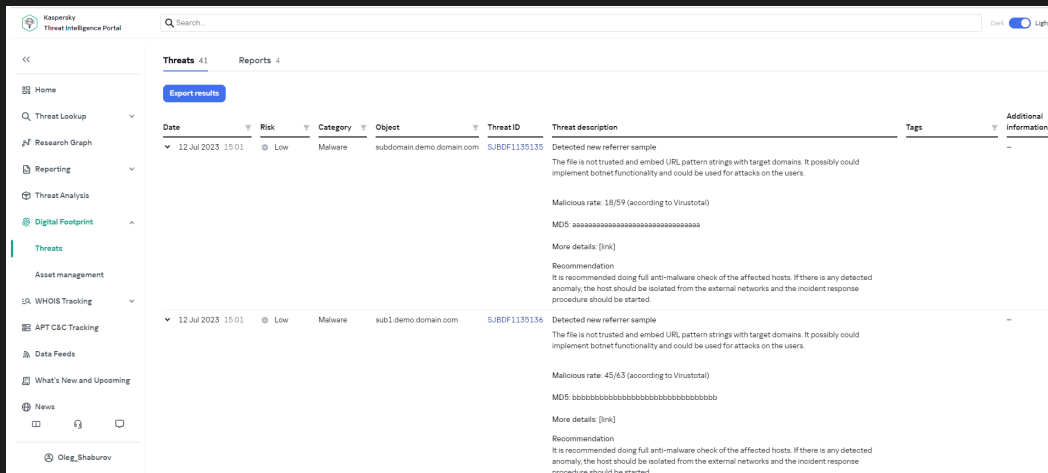
Conclusions and recommendations

Indicators of Compromise (iOCs) and YARA rules

數位軌跡情報 **Digital Footprint Intelligence** – 外部攻擊面風險管理



- Network Reconnaissance
- Dark Web Monitoring
- Discovery of Data Leakages



The screenshot displays the Kaspersky Threat Intelligence Portal. The left sidebar contains navigation links: Home, Threat Lookup, Research Graph, Reporting, Threat Analysis, Digital Footprint (highlighted), Threats, Asset management, WHOIS Tracking, APT/C&C Tracking, Data Feeds, What's New and Upcoming, and News. The main content area shows a table of threats with columns for Date, Risk, Category, Object, Threat ID, Threat description, Tags, and Additional information. Two threat entries are visible, both dated 12 Jul 2023 15:01, categorized as Malware, and originating from subdomain.demo.domain.com. The first threat has a risk level of Low and a threat ID of SUBDF1130135. The second threat has a risk level of Low and a threat ID of SUBDF1130136. Both threats are described as 'Detected new referer sample' and include a recommendation to perform a full anti-malware check.

Date	Risk	Category	Object	Threat ID	Threat description	Tags	Additional information
12 Jul 2023 15:01	Low	Malware	subdomain.demo.domain.com	SUBDF1130135	Detected new referer sample The file is not trusted and embed URL pattern strings with target domains. It possibly could implement botnet functionality and could be used for attacks on the users. Malicious rate: 18/59 (according to VirusTotal) MD5: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa More details: [link] Recommendation It is recommended doing full anti-malware check of the affected hosts. If there is any detected anomaly, the host should be isolated from the external networks and the incident response procedure should be started.		
12 Jul 2023 15:01	Low	Malware	sub1.demo.domain.com	SUBDF1130136	Detected new referer sample The file is not trusted and embed URL pattern strings with target domains. It possibly could implement botnet functionality and could be used for attacks on the users. Malicious rate: 45/63 (according to VirusTotal) MD5: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbb More details: [link] Recommendation It is recommended doing full anti-malware check of the affected hosts. If there is any detected anomaly, the host should be isolated from the external networks and the incident response procedure should be started.		



Home

Threat Lookup

Research Graph

Reporting

Threat Analysis

Digital Footprint

Threats

Asset management

WHOIS Tracking

APT C&C Tracking

Data Feeds

What's New and Upcoming

News

Oleg_Shaburov

Search...

DarkLight

Threats 41Reports 4

Export results

Date	Risk	Category	Object	Threat ID	Threat description	Tags	Additional information
12 Jul 2023 15:01	Low	Malware	subdomain.demo.domain.com	SJBDF1135135	<p>Detected new referrer sample</p> <p>The file is not trusted and embed URL pattern strings with target domains. It possibly could implement botnet functionality and could be used for attacks on the users.</p> <p>Malicious rate: 18/59 (according to Virustotal)</p> <p>MD5: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</p> <p>More details: [link]</p> <p>Recommendation</p> <p>It is recommended doing full anti-malware check of the affected hosts. If there is any detected anomaly, the host should be isolated from the external networks and the incident response proeedure should be started.</p>		
12 Jul 2023 15:01	Low	Malware	sub1.demo.domain.com	SJBDF1135136	<p>Detected new referrer sample</p> <p>The file is not trusted and embed URL pattern strings with target domains. It possibly could implement botnet functionality and could be used for attacks on the users.</p> <p>Malicious rate: 45/63 (according to Virustotal)</p> <p>MD5: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbb</p> <p>More details: [link]</p> <p>Recommendation</p> <p>It is recommended doing full anti-malware check of the affected hosts. If there is any detected anomaly, the host should be isolated from the external networks and the incident response procedure should be started.</p>		

威脅類型

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

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

品牌冒充

- 假冒網站
- 假冒社群帳號
- 假冒手機 apps

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

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

先了解自己有哪些弱點是被別人掌握的

三種提升企業安全維運能力的方式



武裝化

提升內部專家團對面對複雜
威脅事件處理及優化調查流
程時的相關工具



知識化

提升及豐富對抗進階安
全威脅的知識水平



實戰演習

透過外部專家單位進行實
際演練確保面對複雜威脅
時的相關響應工作及流程

三種提升企業安全維運能力的方式



武裝化

提升內部專家團對面對複雜
威脅事件處理及優化調查流
程時的相關工具



知識化

提升及豐富對抗進階安
全威脅的知識水平



實戰演習

檢視安全團隊響應效率

防患未然 而且便宜

	真實事故(Real incident)	安全演練(Ethical exercise)
財務影響(Financial impact)	Millions* 造成損失	50-250k USD 一種投資
無壓力(Stress-free)	No	Yes
名譽損失 (Reputational damage)	Yes	No
是否有罰則 (Regulatory fines)	Yes	No
時間可控制 (Controlled timing)	No	Yes

* - average cost of cyber security incident from various sources is 4-9 millions USD

Kaspersky 安全評估

知識化

威脅情報分享

- Threat Data Feeds
- 威脅情報平台 (CyberTrace)
- 威脅查找
- 威脅溯源引擎 (KTAE)
- APT 威脅報告
- 網路犯罪威脅報告
- 雲端分析沙箱
- 數位軌跡情報 (Digital Footprint Intelligence)
- 特定行業威脅情報 (Financial, ICS, Transport)
- 詢問專家服務 (Ask the Analyst)

專家培訓

- 事件響應培訓
- 數位取證培訓
- 惡意分析及逆向工程培訓
- YARA 規則撰寫培訓
- 威脅情境討論

提升內部
處理知識及
能力

武裝化

原生式 XDR
開放式 XDR



關鍵任務
支援團隊

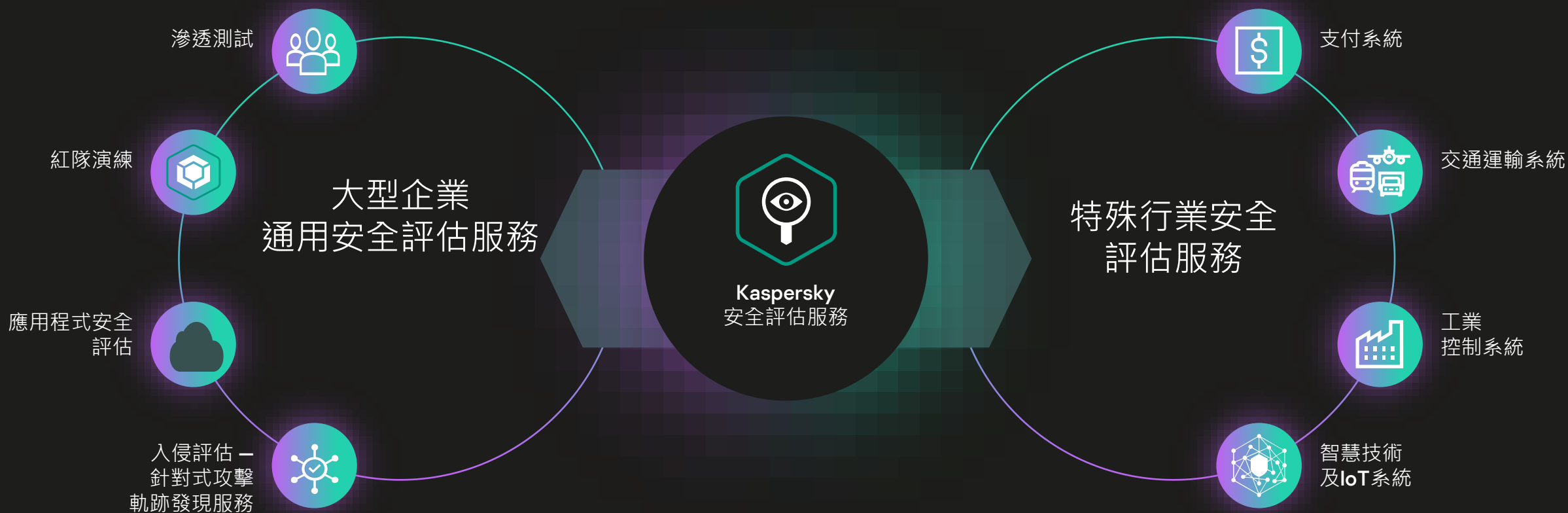
實戰演習

安全評估

- 對手攻擊模擬 (Adversary Attack Emulation)
- 入侵檢測安全評估 (Targeted Attack Discovery)
- 滲透測試
- 紅隊演練 (Red Teaming)
- 應用程式安全評估服務
- 特定行業安全評估服務 (ICS, Payment Systems, Transportation, IoT)
- SOC 顧問
- 事件調查準備顧問服務

響應服務

- Managed Detection and Response (MDR Expert)
- 事件響應
- 惡意程式分析
- 數位取證



辨識



分析



消除



管理

安全評估服務覆蓋範圍

	Penetration Testing /Application Assessment	Adversary Attack Emulation/Blue Team Exercise	Red Teaming	TTX
事件響應能力的演練				
Prevention	✓		✓	
Detection		✓	✓	
Response			✓	✓

搭配持續更新的威脅情報設計實際攻擊的劇本演練

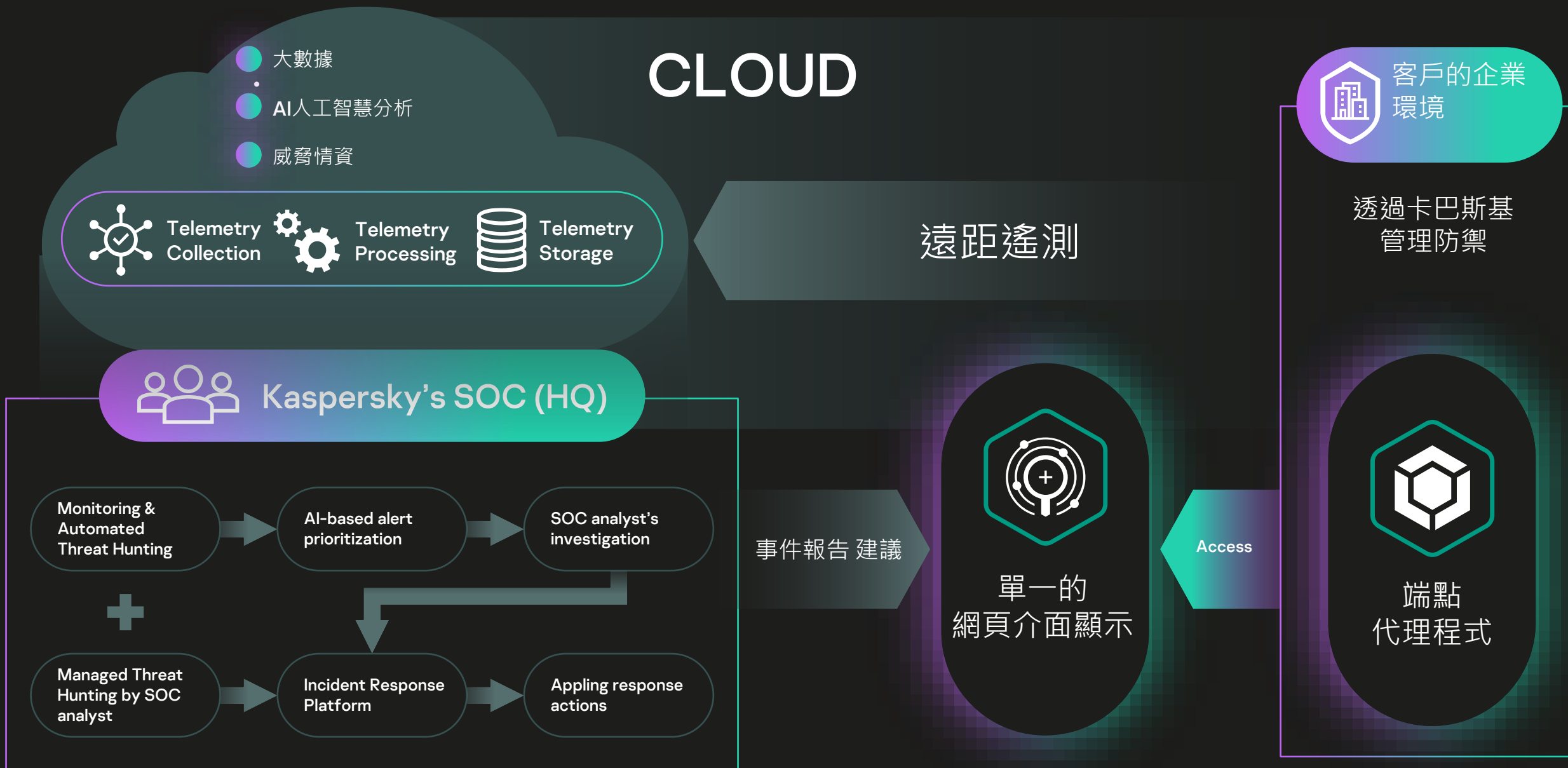
總結

常見SOC安全團隊的挑戰及解決建議

- 如何了解組織可能受到入侵威脅的管道?
 - 數位軌跡情報
 - 利用威脅情報收集內容，了解已曝露的風險進行相關的響應措施
 - 安全評估服務
 - 利用不同深度的安全評估服務，找出可能入侵的管道
- 面對威脅的反應時間是否足夠?
 - 攻防演練/安全評估服務
 - 透過演練，檢驗安全團隊響應能力可優化的部份
- 是否了解當發生事件時的響應步驟?
 - 事件響應演練
 - 透過各種威脅事件場景做為，內部測試、培訓及提昇相關的安全意識及檢視相關事件響應的流程及權責

Kaspersky MDR 託管服務

54



國際認證 威脅獵捕

我們的專家團隊皆有通過各種專家認證並專注在 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



700+

追蹤威脅組織數量

80mln

全球數據收集探針數量

200+

全球領先知名的分析人員數量

Thank you!

kaspersky