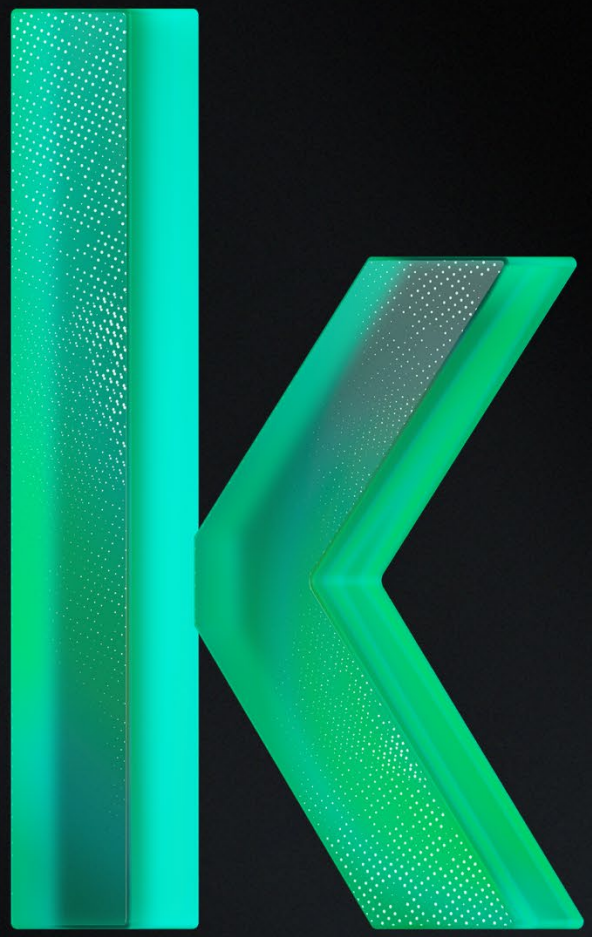
# Kaspersky 大型企業 (Enterprise) 網路安全

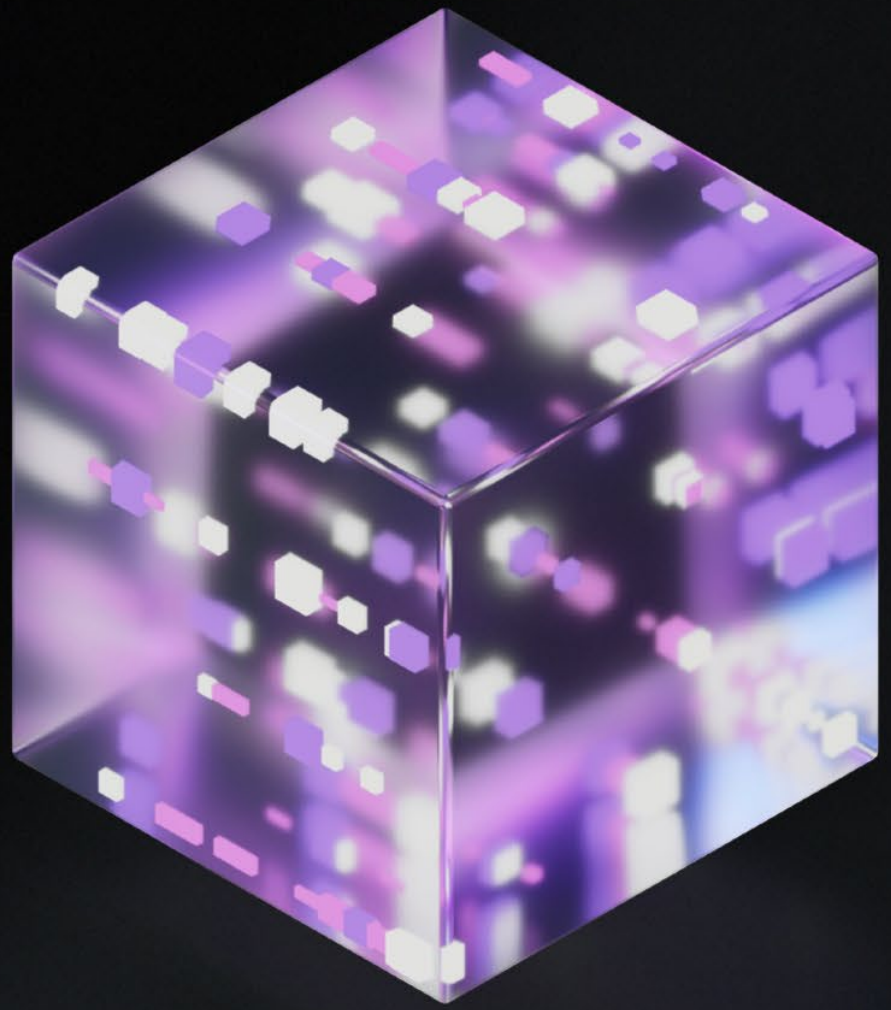


kaspersky 引领未来

# 為何要選擇卡巴斯基?

發現卡巴斯基的
世界級專業知識
以及 AI 驅動式產品組合
正如何改寫企業
網路安全的定義。

卡巴斯基不僅是網路安全提供商，更是備受信賴的全球合作夥伴，集數十年豐富經驗、不懈的創新以及對透明的堅持於一身。我們先進的解決方案經過嚴謹的研究、真實世界的測試，並採用 AI 驅動式做法，可為企業提供毫不妥協的防護。



## 為何要選擇卡巴斯基?

### 企業產品組合可:

01 提供從 IT 與 OT 風險中恢復的能力

02 引導您的 SOC 達致大師級的精確度與效率

03 利用威脅情報管理風險

04 建立安全的 DevOps 環境，並保護您的雲端工作負載

05 訓練您整個團隊以更安全、更受保護的方式工作

06 在外部專家的指導與支援下管理您的安全事件

### 個案研究

# 以全球專業知識與 AI 驅動式創新為基礎建立起的技術領先地位

## 研究與調查

我們的產品組合是以領先世界的威脅研究與事件調查為核心。

我們擁有無與倫比的全球專業知識，可幫助我們的客戶預先防範不斷演變的威脅，並在整個事件回應過程中獲得完整支援。

## 安全的 AI 驅動式做法

我們將人工智慧內嵌到解決方案中時，是採用安全的做法，

無論是以 AI 加強的威脅偵測與警示分類，還是由生成式 AI 驅動的威脅情報，多年來，我們一直是在網路安全領域應用 AI 的先鋒，並持續引領潮流。

## 安全的軟體開發方式

從安全的軟體開發生命週期，到安全設計型原則，

我們在產品的每個開發階段都顧及了安全性。我們嚴謹的做法可確保系統具備恢復能力與安全性，能夠隨時保護客戶的安全。

**~5,000**
名高度合格的專家

**50%**
名研發人員

**50+**
名全球公認的網路安全專家

**5**
個一流的專業知識中心

# 無與倫比的專業知識

我們有一流的專家團隊跨**五個專業知識中心**來相互合作，結合彼此的專門知識與技能來應對最複雜、最危險的網路威脅。這種相互合作的做法強化了我們最先進的防護技術，確保我們產品與解決方案的安全性與可靠性能夠成為業界的典範。

# 在卡巴斯基產品組合核心使用的 AI

## 逾 20 年來，

卡巴斯基一直在使用機器學習和 AI
預先防範不斷演變的網路威脅


我們專門的 AI 技術研究中心在推動創新的同時，還會確保 AI 和機器學習是以安全且合乎道德的方式受到使用。

主要重點領域：

- 將 AI 整合到網路安全解決方案中
- 開發技術來加強以安全、負責任的方式使用 AI
- 追蹤以 AI 實現的威脅來預測新興攻擊媒介
- 使用卡巴斯基的大型語言模型 (LLM) 基礎架構進行生成式 AI 研究
- 建立安全部署 AI 系統的指導方針

深入瞭解

50,000
檔案

100,000
名使用者 / 天

以整合式機器學習模型訓練的靈活雜湊

~1000
個偵測到的網路釣魚網頁 / 天

機器學習式網路釣魚偵測引擎

15,000
檔案

7,000
名使用者 / 天

以機器學習實現的偵測記錄產生方式

100,000
個檔案 /天

實驗室中作為偵測惡意軟體之用的大型神經網路

我們透過對 AI 的五大應用，帶給客戶較別家更優異的防護：

1. AI 與機器學習驅動式威脅偵測
2. 透過 AI 提升安全程序效率
3. 對威脅情報與安全程序使用的生成式 AI
4. 安全的 AI 做法與方法學
5. IT 與作業科技 (OT) 環境中的 AI 式行為分析與異常偵測

# 業界活躍的貢獻者

我們是全球威脅情報領域的主要活躍參與者，與外界的廣大網路安全社群密切合作來打擊全球網路犯罪

INTERPOL

PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE 11 • 12 • 2018

industrial internet CONSORTIUM

AFRIPOL

Coalition Against Stalkerware

我們與國際刑警組織 (INTERPOL)、執法機構、電腦緊急應變小組 (CERT) 及全球 IT 安全社群等國際組織合作，進行聯合網路犯罪調查與行動。

MITRE | ATT&CK®

我們向包括 MITRE 在內的全球倡議組織提供重要的網路威脅情報，提升 ATT&CK 架構的準確性。

我們的工作力求合乎道德原則，以負責任的方式揭露弱點。

卡巴斯基透過為 Adobe、Microsoft、Google、Apple 等頂尖公司識別並協助修復零日漏洞，強化了該產業的安全性。

# 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 次評測

91 次奪冠

97% 登上前 3 名

深入瞭解

# 持續推動創新，隨時都能迎接明日的挑戰

專利、發明、機器學習 / AI、自家作業系統 (OS)

**1,500+**

項成功註冊的專利

**500+**

項發明（2005 到 2024 年）

**20+ 年**

推動機器學習與 AI 創新的經驗；我們將 AI 工具內嵌到自家的流程與網路安全解決方案架構中

KasperskyOS
Be Immune

我們透過突破性的 KasperskyOS，實現從網路安全到「網路免疫」的轉變。

## 關於 KasperskyOS

將網路安全要求做了加強的微核心作業系統

- 微核心架構可大幅減少攻擊面以及弱點風險，而安全監視器則令未經授權的操作變得不可能
- 由卡巴斯基從零開發，核心不含任何第三方程式碼！
- 「網路免疫」產品與解決方案的建立基礎

kaspersky cyber immunity

「網路免疫」是我們開發安全設計型解決方案的做法與方法學

「網路免疫」系統乃專門設計成連不明威脅都能抵禦，並且能在受到攻擊時保持穩定運作。

# 設計「網路免疫」的未來

KasperskyOS 作業系統的「網路免疫」解決方案先天就內建了防護能力，可抵禦惡意程式碼與駭客入侵，從核心就開始保護您的重要系統。

Kaspersky Thin Client

Kaspersky IoT Secure Gateway

Kaspersky Automotive Secure Gateway

KasperskyOS Mobile

KasperskyOS 作業系統的解決方案有全方位的生態系統合作夥伴計畫支持，該計畫旨在鼓勵透過共同發展來推動創新與成長。透過 Kaspersky Appicenter 這個專為應用程式開發人員與全球硬體供應商而設的一站式商店，合作夥伴可取得所需的工具與支援來成功發展。

Kaspersky Appicenter


深入瞭解

# 為您企業打造的網路安全

我們擁有經驗、專業知識、情資以及調改能力，可滿足您目前需求，並可保護您安全成長。

# 產品組合

## 為何要選擇卡巴斯基?

### 企業產品組合可:

01 提供從 IT 與 OT 風險中恢復的能力

02 引導您的 SOC 達致大師級的精確度與效率

03 利用威脅情報管理風險

04 建立安全的 DevOps 環境，並保護您的雲端工作負載

05 訓練您整個團隊以更安全、更受保護的方式工作

06 在外部專家的指導與支援下管理您的安全事件

## 個案研究

# 提供從 IT 與 OT 風險中恢復的能力

網路犯罪不斷在演進。我們也是。我們的解決方案無論是在 IT、OT 還是兩者交會型環境中運作，都能緩解網路犯罪所造成最嚴重的影響。

## 企業環境

網路犯罪可能會引發財務下滑、運作停擺、資料外洩以及詐欺，導致客戶流失、信譽嚴重受損。

+

## 工業環境

攻擊可能會令生產中斷、財務損失、智慧財產遭竊，進而危及技術穩定性與業務持續性。

## 挑戰

- 日益擴大的攻擊面
- 合規性
- 舊有系統
- 新興及不斷演變的威脅與弱點
- 專業人士與技能短缺
- 預算限制

01

# 開啟您的網路防禦

前來探索我們的產品組合，其中每樣產品都是以三大支柱為核心打造，旨在每個階段強化您的防禦。

## 技術

1

讓您的內部專家配備所需的工具與能力，來對網路威脅進行偵測與回應

## 知識

2

隨時獲知最新的威脅演進、持續提升您團隊有效處理事件的能力，並且促進安全意識

## 專業知識

3

取得來自外部專家的評估、即時事件回應和策略指引

# 卡巴斯基為 IT 環境提供的防護

1

| | 基本防護 | 進階資產型安全 |
|---|---|---|
| 端點 | Kaspersky Next EDR Foundations | Kaspersky Next EDR Expert |
| 網路 | Kaspersky Security for Mail Server | Kaspersky Anti Targeted Attack |
| 工作負載 | Kaspersky Hybrid Cloud Security | Kaspersky Cloud Workload Security |

全方位的防禦以及最佳化的安全程序

XDR 企業

Kaspersky Next XDR Expert

集中化的資訊安全監視

Kaspersky Unified Monitoring and Analysis Platform

目標式解決方案

- Kaspersky Container Security
- Kaspersky SD-WAN
- 卡巴斯基詐騙防護
- 卡巴斯基掃描引擎
- Kaspersky DDoS Protection

2

- 意識：Kaspersky Security Awareness
- 威脅情報：Kaspersky Threat Intelligence
- 培訓：Kaspersky Cybersecurity Training

3

- 評估：Kaspersky Security Assessment
- 代管式安全：Kaspersky Managed Detection and Response
- 事件回應：Kaspersky 事件回應
- 漏洞評估：Kaspersky Compromise Assessment
- SOC 諮詢：Kaspersky SOC 諮詢
- 支援服務：卡巴斯基專業服務

# 卡巴斯基為 OT 環境提供的防護

Open
Single Management
Platform

1 技術

2 知識

3 專業知識

深入瞭解

1

全方位的防禦以及最佳化的安全程序

XDR
工業

Kaspersky
工業
網路安全

- 進階資產管理
- 全系統偵測與預防
- 安全稽核

進階資產型安全

Kaspersky Industrial CyberSecurity for Nodes
端點、SCADA

Kaspersky Industrial CyberSecurity for Networks
網路通訊裝置
控制器與 IIoT

專門解決方案

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

「網路免疫」解決方案

- Kaspersky IoT Secure 閘道
- Kaspersky Thin client
- Kaspersky Automotive Secure Gateway

2

- 意識: Kaspersky Security Awareness
- 威脅情報: Kaspersky ICS Threat Intelligence
- 培訓: Kaspersky ICS CERT Training

3

- 評估: Kaspersky ICS Security Assessment
- 代管式安全: Kaspersky Managed Detection and Response
- 回應: Kaspersky 事件回應
- 專業服務: 卡巴斯基專業服務

# IT、OT 與兩者混合型情境適用的 Open Single Management Platform

企業
網路安全

XDR

Kaspersky Next
XDR Expert

深入瞭解

Open
Single Management
Platform

**網路安全**
於 IT 與 OT 環境交會處

工業
網路安全

XDR

Kaspersky
Industrial
CyberSecurity

深入瞭解

Open Single Management Platform 會針對組織的基礎架構，提供全方位的安全態勢檢視。它簡化了事件管理、系統管理與安全維護工作。

這個平台是一個內嵌於 Kaspersky Next XDR Expert 和我們統一化 IT-OT XDR 技術堆疊當中的重要元件，可協助抵禦可在 IT 與 OT 環境之間游移的複雜網路攻擊。

- 從單一主控台進行事件管理
- 自動化與整合協調
- 部署工具包

- 集中化資產與個案管理
- 劇本
- 調查圖表

Kaspersky Next

# 一個適用於企業環境的核心網路安全提案

Kaspersky Next 是為了防止如今複雜與新興的企業網路威脅造成「大屠殺」而打造的新一代產品線，可提供頂尖的端點防護 (EPP)、端點偵測和回應 (EDR) 以及延伸偵測和回應 (XDR)，以便阻斷攻擊進行。

深入瞭解

# Kaspersky Next：將您的企業安全提升到新的等級

## Kaspersky Next EDR Optimum

### 對進階威脅的優質防護

小型網路安全團隊適用的 EDR

- 強大端點防護
- 進階安全控制
- 加強 EDR 功能
- 延伸雲端安全
- IT 管理員網路安全培訓

## Kaspersky Next XDR Expert

### 對最複雜威脅的專家防護

大型網路安全或 SOC 團隊適用的
終極 XDR

- 強大端點防護
- 進階安全控制
- 強力 EDR 功能
- 跨整個基礎架構的進階威脅偵測和回應
- 調查圖表、個案管理與劇本
- 無縫的第三方整合

## Kaspersky Next EDR Foundations

### 對大規模威脅的基本防護

無與倫比的端點防護

- 強大端點防護
- 基礎安全控制
- 基礎 EDR 功能
- 最大程度自動化

# 有助抵禦複雜網路威脅的開放式 XDR 平台

Kaspersky Next XDR Expert

專為加速威脅偵測、提供即時檢視能力以及自動做出回應而設計，可提供主動式網路防禦所需的全方位網路安全。

## 可帶來的幫助

以更短的平均偵測時間 (MTTD) 以及能加快平均回應時間 (MTTR) 的自動化作業，識別複雜且持續的威脅。

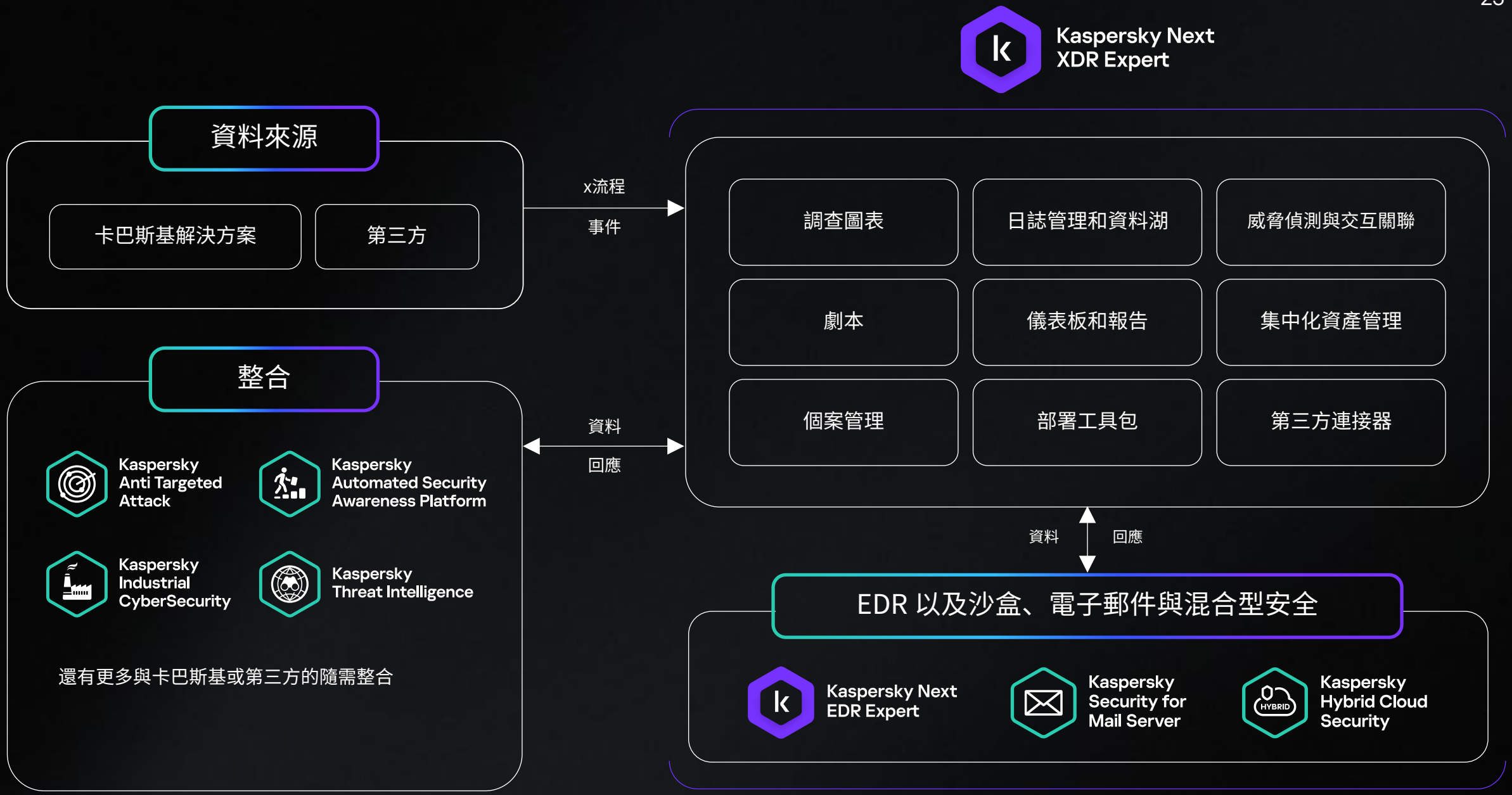
在 AI 輔助下，進行監視、偵測、威脅搜捕以及調查。

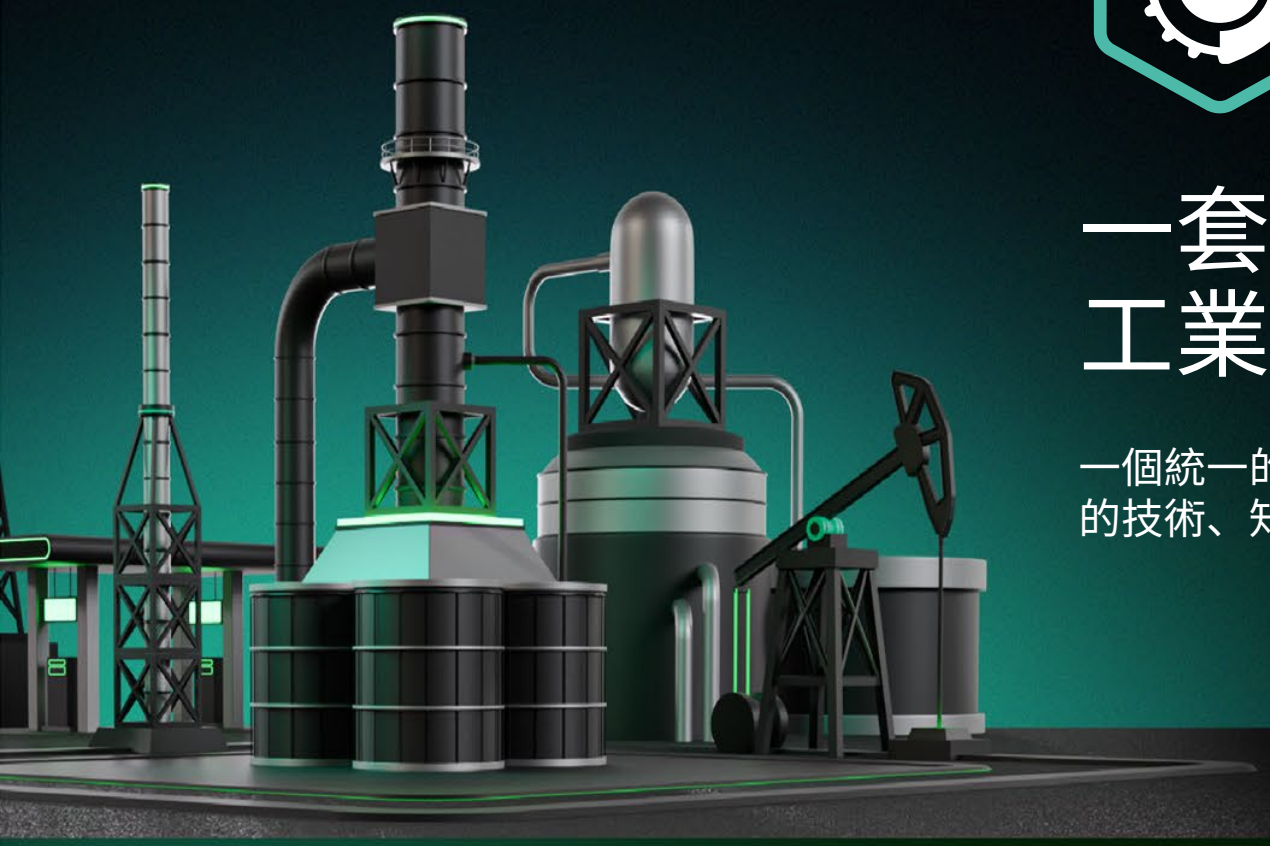
端點、混合型雲端與郵件防護。

以進階個案管理功能增加效率。

卡巴斯基已連續第二年在 XDR 類別獲評為領導者


深入瞭解


Kaspersky Next
XDR Expert
資料來源
卡巴斯基解決方案
第三方
x流程
事件
調查圖表
日誌管理和資料湖
威脅偵測與交互關聯
劇本
儀表板和報告
集中化資產管理
個案管理
部署工具包
第三方連接器
整合
資料
回應
Kaspersky
Anti Targeted
Attack
Kaspersky
Automated Security
Awareness Platform
Kaspersky
Industrial
CyberSecurity
Kaspersky
Threat Intelligence
還有更多與卡巴斯基或第三方的隨需整合
資料
回應
EDR 以及沙盒、電子郵件與混合型安全
Kaspersky Next
EDR Expert
Kaspersky
Security for
Mail Server
Kaspersky
Hybrid Cloud
Security
HYBRID



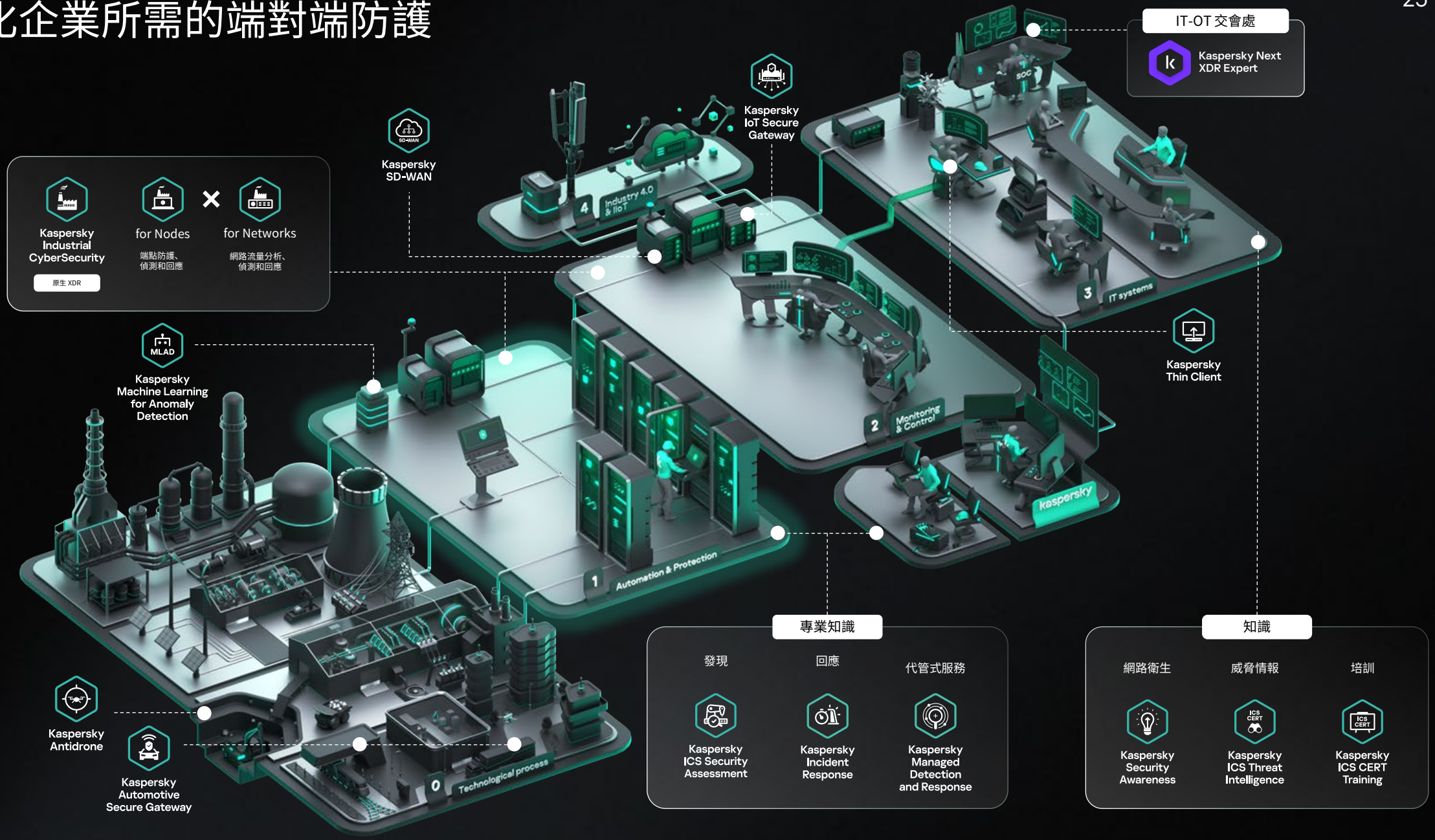
Kaspersky
OT CyberSecurity

# 一套將網路與實體相結合的工業安全生態系統

一個統一的工業安全概念，集在每個層面保護工業化企業所需的技術、知識與專業能力於一身。

深入瞭解

# 工業化企業所需的端對端防護



# OT XDR 平台提供重要基礎架構防護

Kaspersky Industrial CyberSecurity

OT 生態系統的核心，以 XDR 平台的形式運作。它的特色是以原生整合的節點與網路安全產品來保護工業自動化與控制系統 (IACS)。

## 可帶來的幫助

揭露隱藏的威脅。遠在異常、弱點和入侵企圖變得危險之前，就加以偵測到。

管理複雜的基礎架構。將回應和管理自動化，確保能對事件迅速做出反應。

在不影響技術工作流程的情況下運作，確保不會造成任何不可接受的損壞。

利用我們經認證的解決方案，達到符合工業網路安全的最高標準。

深入瞭解


Kaspersky
Industrial CyberSecurity
for Nodes
端點防護、偵測和回應
硬體
軟體
弱點
姓名
使用者
FQDN
MAC
IP
伺服器
工作站
攜帶型掃描機
Kaspersky
Industrial
CyberSecurity
合規性稽核、
風險及資產管理
Kaspersky
Industrial CyberSecurity
for Networks
網路流量分析、偵測和回應
OC
軟體
弱點
FQDN
MAC
IP
伺服器
感測器
SD-WAN
遠端採集器
資料補足
防護狀態
安全性稽核
網路社群
主機遙測
硬體管理
警報和事件

# 引導您的 SOC 達致大師級的精確度與效率

02

## 今日 SOC 面臨的最大挑戰

網路威脅的演變速度快過防禦

技能的取得與保留

對合規性的影響

# 卡巴斯基可協助組織建立強大的 SOC，並提升其有效性和效率

## 執行

### 代管式安全

**MDR**

Kaspersky Managed Detection and Response

- 享受自有 SOC 的所有主要好處

### 調查

**事件回應**

Kaspersky Incident Response

- 事件回應約定服務
- 事件緊急應變

## 組建

### 核心技術堆疊

**SIEM**

Kaspersky Unified Monitoring and Analysis Platform

**XDR**

Kaspersky Next XDR Expert

**NDR**

Kaspersky Anti Targeted Attack

**EDR**

Kaspersky Next EDR Expert

### 架構與流程

**諮詢服務**

Kaspersky SOC Consulting

- SOC 架構開發
- 網路威脅情報架構
- 事件回應整備

## 改善

### 威脅情報

**情資摘要**

Kaspersky Threat Data Feeds

**威脅情報平台**

Kaspersky CyberTrace

**威脅情報入口網站**

Kaspersky Threat Intelligence Portal

**威脅情報洞察分析**

Kaspersky Ask the Analyst

### 技能與表現

**培訓**

Kaspersky Cybersecurity Training

- 安全程序及威脅搜捕
- 事件回應
- 惡意軟體分析
- 數位鑑識

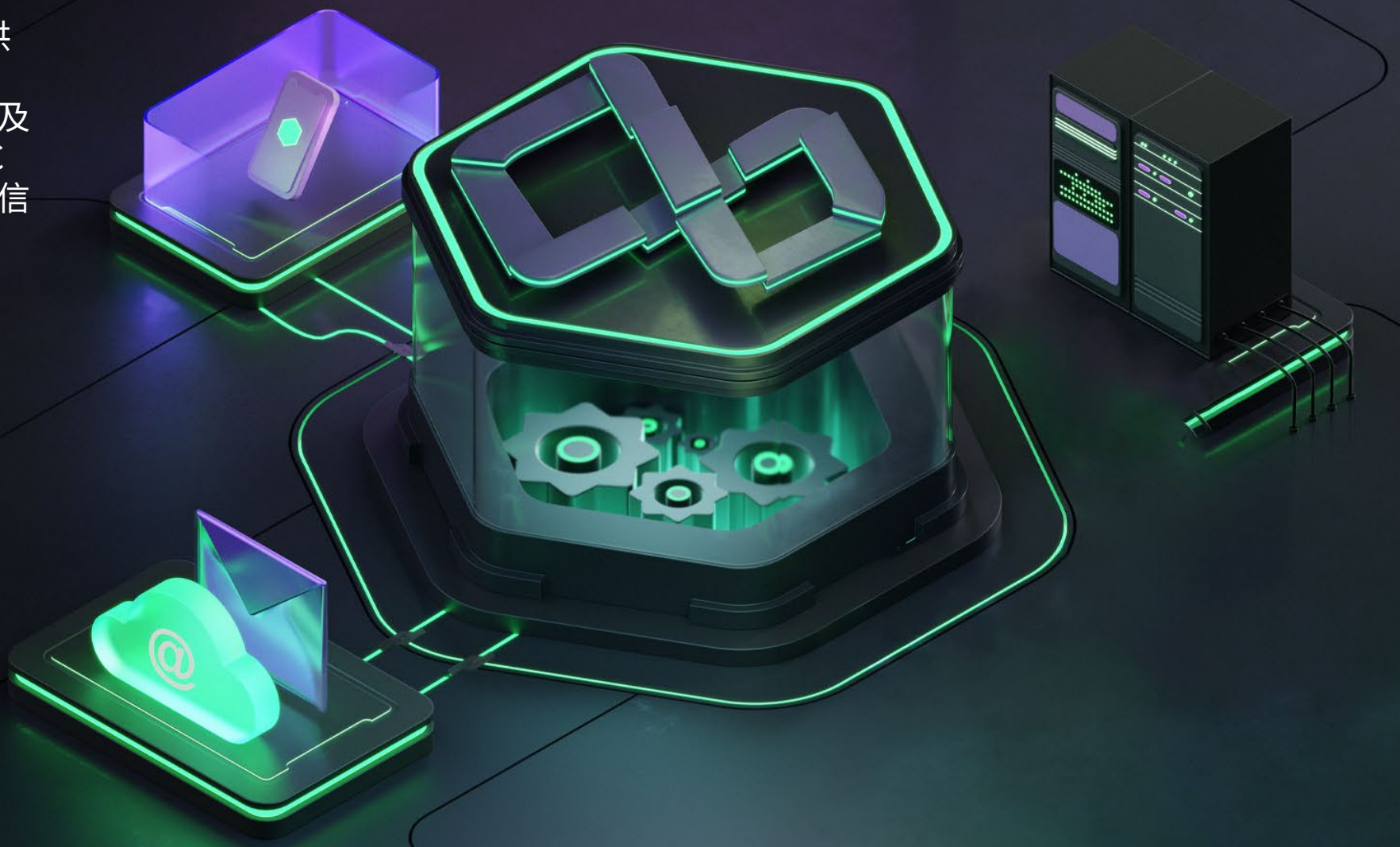
**諮詢服務**

Kaspersky SOC Consulting

- SOC 成熟度評估
- 桌面演練
- 對手攻擊模擬

# 卡巴斯基 SOC 諮詢如何使您的企業受益

卡巴斯基 SOC 諮詢服務可為企業提供 SOC 建立、支援或加強方面的協助。我們擁有數十年網路安全專業知識以及跨全球數百個基礎架構經營自有 SOC 的經驗，可協助組織以更高的效率與信心來偵測、回應及緩解網路威脅。



深入瞭解

1. **建立或加強您的 SOC：**將網路安全風險降至最低，保護您的企業運作免於中斷。

2. **享受世界級的專業知識：**在高層次的引導下，快速有效地適應不斷演變的威脅。

3. **減少網路威脅的影響：**改善威脅偵測效果並加快回應時間，以便獲得更好的結果。


4. **將資源最佳化：**簡化流程，以便在不過度支出的情況下，達致更好的 IT 安全結果。

5. **隨著您的業務來擴展：**確保 SOC 會隨著您業務的成長來演進，在您的業務擴大時，仍維持強大的防護能力。

6. **享受量身打造的 SOC 設計：**在顧及監管要求的情況下，解決您業務特定的網路安全威脅。

# 您的 SOC 所需、以 AI 加強的先進 SIEM 平台

Kaspersky Unified Monitoring and Analysis Platform

一套新一代安全資訊與事件管理 (SIEM) 解決方案，可管理安全資料與事件來協助實現全方位防禦。卡巴斯基 SIEM 會在向所有安全控制來源收集日誌並即時關聯資料後，彙整所有資訊並提供給 SOC，供其進行深入事件調查及回應。

## 可帶來的幫助

具有資料主權的日誌管理。

即時串流傳送資料進行交互關聯。

在 AI 輔助下，進行威脅偵測、事件回應以及威脅搜捕。

立即提供對您安全態勢的檢視能力，支援合規性。

深入瞭解

# 以含有 NDR 與 EDR 的反 APT 解決方案強化您的 SOC

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack 是一套先進的反 APT 解決方案，可抵禦複雜的網路威脅。從網路偵測和回應 (NDR) 到原生 XDR 功能，它什麼都提供，可在網路與端點層級保護主要攻擊入口點。它可提供跨您整個 IT 基礎架構的完整檢視能力，強化您的 SOC 抵禦目標式攻擊的能力。

## 可帶來的幫助

- 保護您的企業基礎架構與業務免受複雜攻擊。
- 透過單一介面，簡化對網路流量和端點的控制操作。
- 提供跨網路流量、電子郵件、端點的一體化安全性來保護您的業務。
- 將威脅偵測與回應任務自動化，減少事件偵測與回應時間。

深入瞭解

03

# 利用威脅情報管理風險

整合供機器讀取的情報、人類專業知識以及策略指引，以便主動應對不斷演變的威脅。

# 快速演變的網路攻擊

隨著新的弱點與攻擊媒介快速冒出，組織要預先防範潛在風險也變得具有挑戰性。使用以威脅情報加強的工具，可更精確地管理風險。

## **此外**，企業往往面臨新的挑戰：

### 缺乏背景脈絡

原始未經處理的威脅情報往往缺乏必要的背景脈絡，使得組織難以評估特定威脅會如何影響自家的運作與資產。

### 資訊超載

來自多個來源的大量威脅資料會令識別哪些威脅真正與您的環境切身相關變得具有挑戰性。

組織需要的是已彙整好且切身相關的最新威脅情報，以便對鎖定自家業務的網路威脅有深入瞭解，並確保自家做好準備並受到保護。

**Kaspersky Threat Intelligence**

Kaspersky Threat Intelligence 會提供 360 度全方位的全球威脅情勢檢視，包括威脅執行者所用的工具與手法。它會透過結合情報來源與威脅情資摘要，即時奉上手法、操作與策略方面的威脅情報；如此等於是將所有擷取的網路威脅知識全都整合到一處來提供。

# Kaspersky Threat Intelligence — 比攻擊者早一步

## 供機器讀取的威脅情報

- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

## 威脅情報專家支援

- Kaspersky Takedown Service
- Kaspersky Ask the Analyst

## Kaspersky 威脅情報

- 手法
- 操作
- 策略

## 供人類讀取的威脅情報

- Kaspersky Threat Lookup
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Analysis
  - 沙盒
  - 歸因
  - 相似性
- Kaspersky Threat Intelligence Reporting
  - APT
  - 犯罪軟體
  - ICS
- Kaspersky Threat Infrastructure Tracking

# 供人類讀取的威脅情報

Kaspersky Threat Intelligence Portal

我們供人類讀取的威脅情報既是為了 IT 也是為了 OT 而設計。Kaspersky Threat Intelligence Portal 提供了單一存取點，其中整合了各項服務來互相補足及強化。

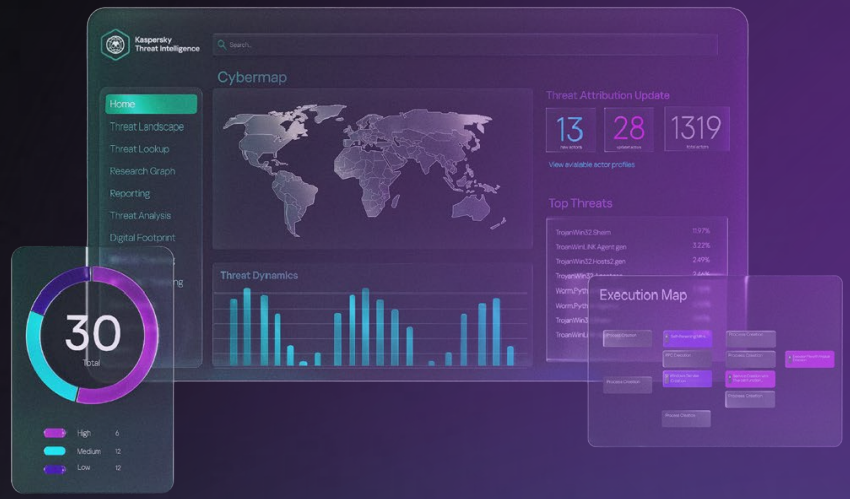
## 可帶來的幫助

透過跨所有使用中威脅情報產品與外部來源運作的強大主搜尋工具，提供完整的網路威脅情報與關係分析。

使用沙盒以及最先進的歸因與相似性技術，自動對可疑檔案進行例行分析。

針對您的數位足跡提供全方位檢視，包括任何可能容易受到攻擊或外洩的資產。

提供多個專為您特定需求量身打造的商業報告管道。




由 Kaspersky Threat Landscape 提供：地區與產業特定的威脅情報可協助組織瞭解所面臨的確切威脅。

試試我們領先業界的威脅情報

# 供機器讀取的威脅情報

Kaspersky Threat Data Feeds

超過 30 個專為各種安全需求量身打造、範圍涵蓋 IT 與 OT 的威脅情資摘要。

## 可帶來的幫助

以持續更新的 IoC 以及可供執行的背景脈絡，強化您的安全解決方案（包括 SIEM、NGFW、IPS / IDS、安全代理伺服器等）。

自動執行初步分類來改善事件回應，同時為安全分析師提供所需的背景脈絡。

預防威脅，並且管理與所有產業以及特別是工業化組織相關的弱點。

彈性靈活的傳遞格式與機制可供輕鬆整合到安全控制中。

## 一般威脅情資摘要

- 惡意 URL
- 勒索軟體 URL
- 網絡釣魚 URL
- 殭屍網絡 C&C URL
- 行動殭屍網路 C&C URL
- 惡意雜湊
- 行動惡意雜湊
- IP 信譽
- IoT URL
- ICS 雜湊
- APT 雜湊
- APT IP
- APT URL
- 犯罪軟體雜湊
- 犯罪軟體 URL

傳遞給：SIEM、SOAR、IPR、TIP、EDR、XDR 等

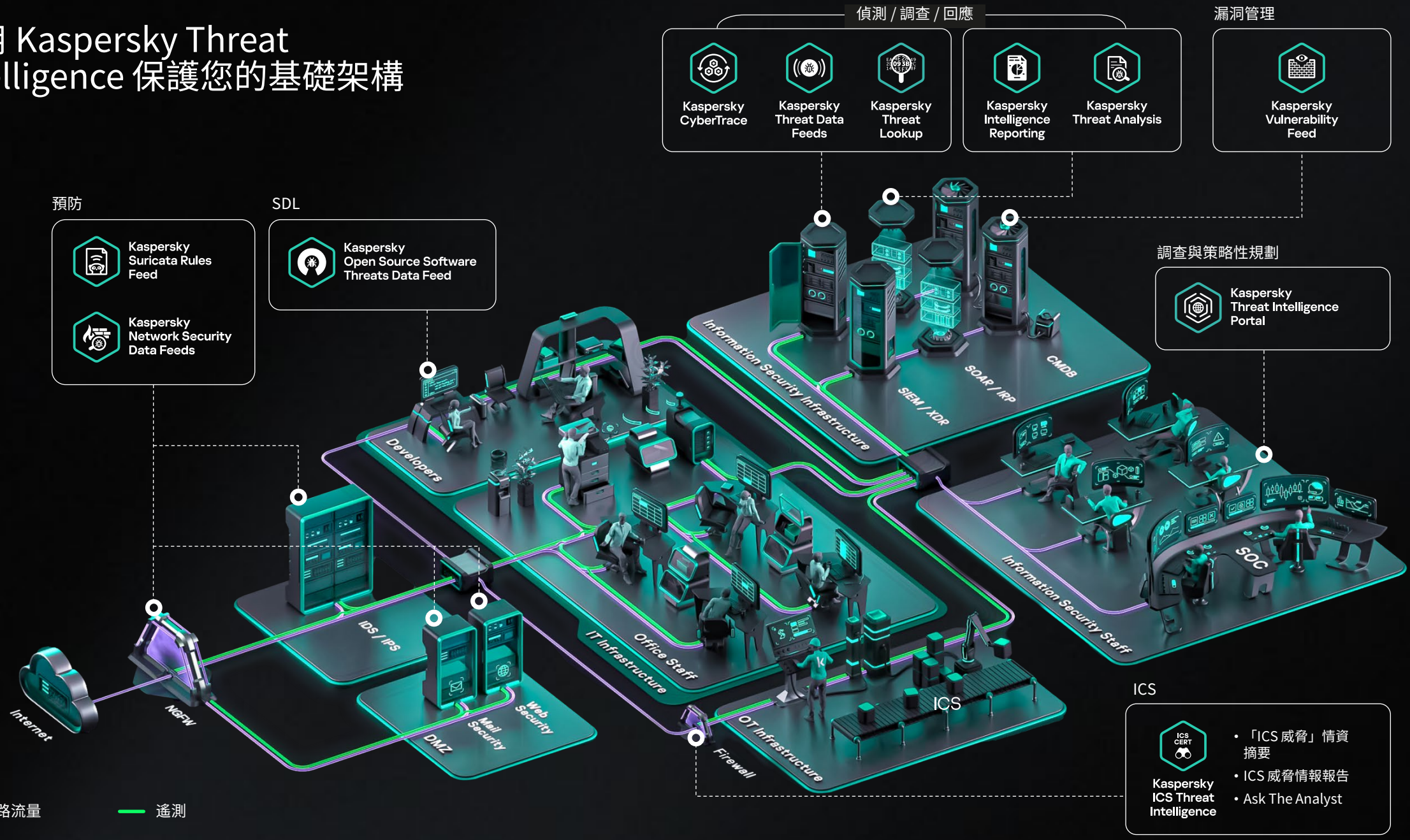
Kaspersky CyberTrace

Kaspersky Threat Data Feeds 可以與第三方威脅情報平台以及我們自家的 Kaspersky CyberTrace 整合。

## 特定威脅情資摘要

- 「網路安全」情資摘要（適用於 NGFW）
- 「Suricata 規則」摘要（適用於 IDS / IPS）
- 「Sigma 規則」情資摘要（適用於 SIEM/EDR）
- 「Yara 規則」情資摘要（適用於 YARA 掃描器）
- 「弱點 / ICS 弱點」摘要 (SBOM /CMDB)
- 「開放原始碼軟體威脅」情資摘要 (OSA /CSA / ASOC)
- 「雲端存取安全代理程式」情資摘要 (CASB)

# 利用 Kaspersky Threat Intelligence 保護您的基礎架構



04

# 建立安全的 DevOps 環境，並保護您的雲端工作負載

雲端移轉與容器化強化了企業的敏捷性、恢復能力與競爭力，但同時也帶來了新的網路安全挑戰：

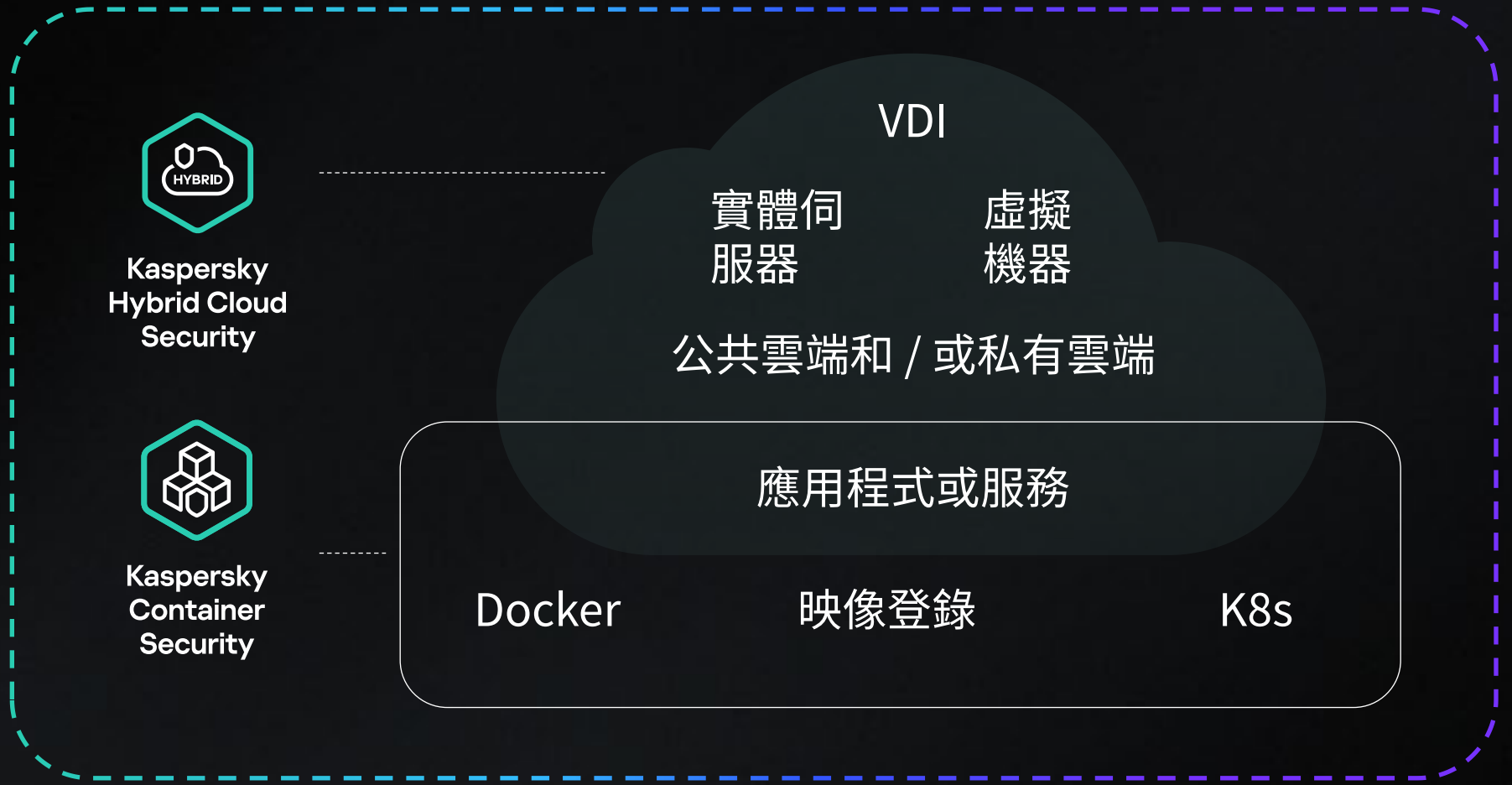
## 挑戰

不安全的第三方資源

對混合型雲端環境的檢視與控制能力有限

不安全的軟體開發（包括容器映像與執行階段）

# Kaspersky Cloud Workload Security




開發人員仰賴容器化，而企業需要擴展自家雲端環境。不過，這些環境的特定安全風險可能會造成重大損害，因此需要專門的防護解決方案。

Kaspersky Cloud Workload Security 是專為保護 DevOps 與雲端環境而設計。它是利用多層式威脅防護來降低雲端風險，同時確保跨私有雲端、公共雲端與混合型雲端的完整監視能力。它會藉由在整個開發生命週期保護重要元件，保護 CI/CD 管道以及容器化的應用程式。

深入瞭解

# 混合型雲端安全

Kaspersky Hybrid Cloud Security

保護您整個混合型基礎架構，
以便抵禦最廣泛的雲端相關網路攻擊，
同時卻減少您資源的消耗。

## 可帶來的幫助

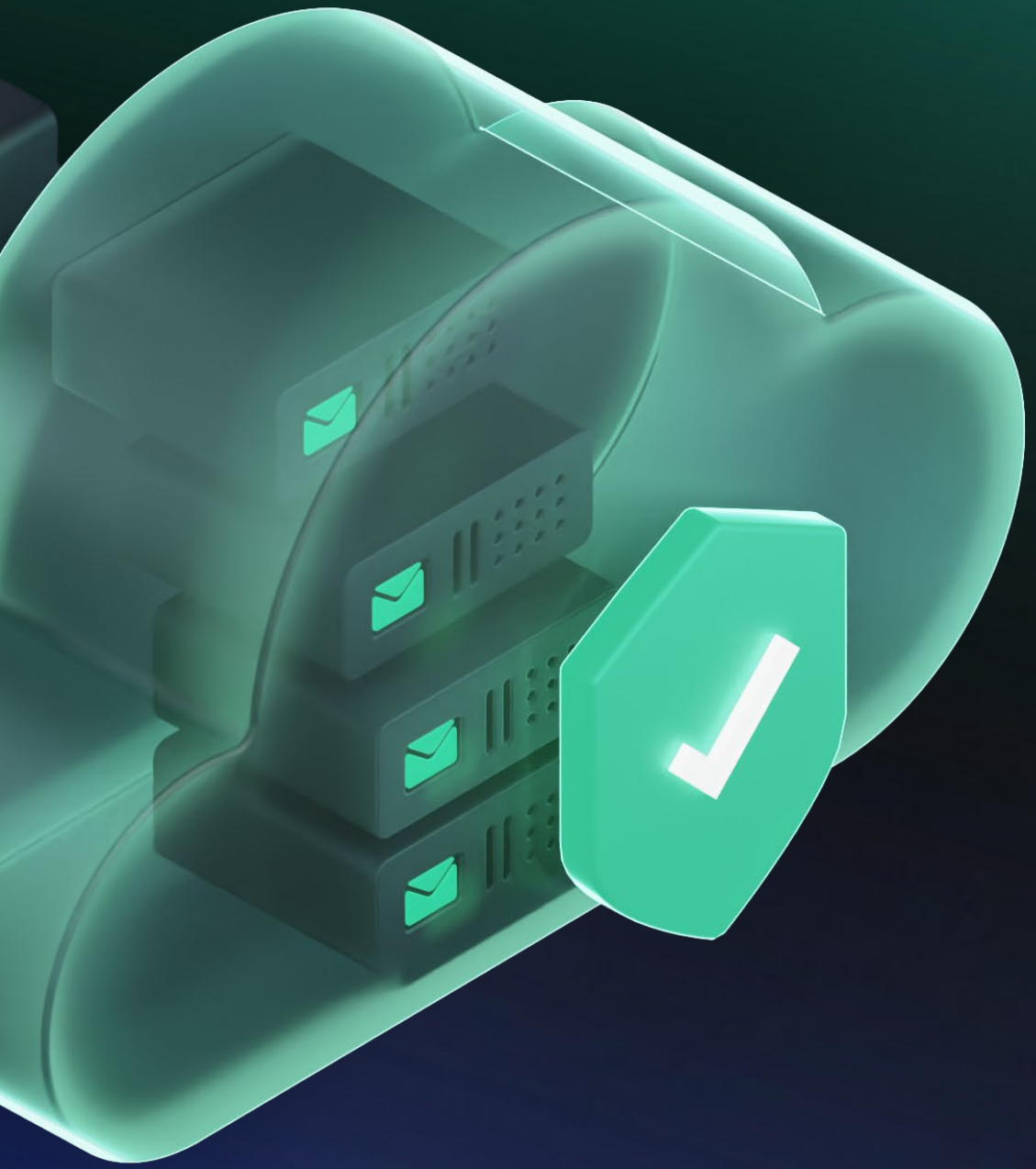
跨所有工作負載類型與雲端平台來保護混合型環境

維持符合監管要求

增加對混合型基礎架構的檢視能力，進而減少 IT 事件

以 AI 驅動式防護將誤報降至最低

# 容器安全防護



Kaspersky Container Security

保護您的容器化應用程式從開發到運作的整個生命週期。

## 可帶來的幫助

在每個開發與運作步驟保護應用程式

提高開發環境與流程的透明度

稽核基礎架構與應用程式來確保合規性

加快發佈客戶導向的應用程式與服務

# 05


# 訓練您整個團隊以更安全、更受保護的方式工作

組織讓自家的 IT 人員和非技術員工具備必要的知識與技能，一方面可以強化 IT 安全團隊，一方面可以在全體員工之間培養具有強烈安全意識的文化。如此有助於保護重要資產、確保合規性並且維持信任。

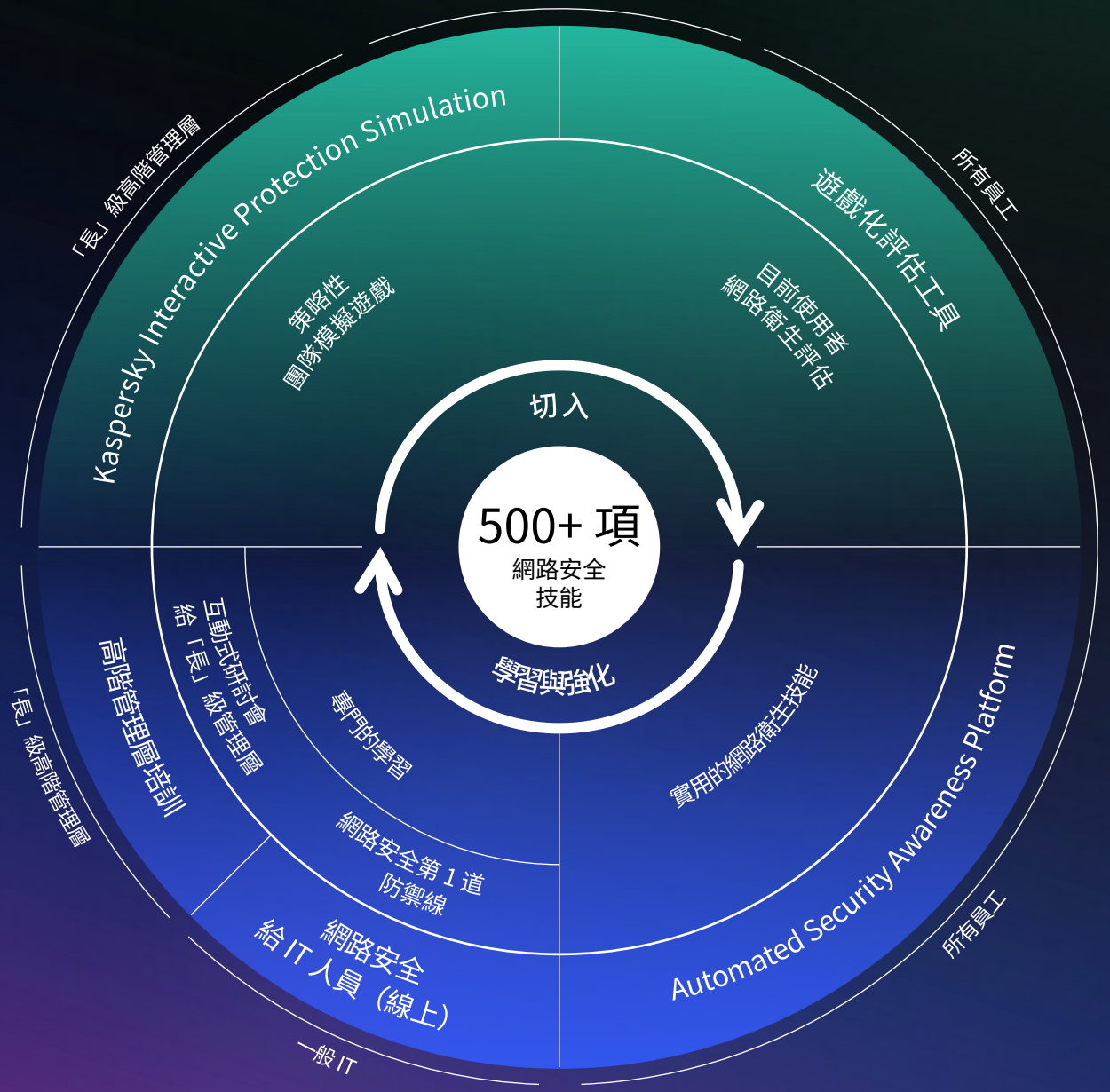
# 以下是企業在處理安全問題時所面臨的挑戰：

缺乏安全意識

缺乏合格的技術人員

員工知識與技能的鴻溝

我們協助組織建立的網路安全架構會具有恢復能力，同時又能解決人員相關挑戰，並減少與人相關的事件。我們會加強 IT 與安全團隊的能力，解決合格人員短缺的問題，培養對網路警覺的文化，教導員工認出及避免威脅，同時賦予技術團隊能力來將安全解決方案的有效性推升到最高。




# 卡巴斯基安全意識

我們的安全意識可在組織內促進網路安全文化，影響上至高階管理層、下至一般員工的每個人。卡巴斯基特有的遊戲式培訓可協助高階管理層與主管做出有效的網路防禦策略，而自動化平台則可賦予員工能力來主動抵禦威脅。這種做法可減少與人相關的事件，並加強組織整體的恢復能力。

Kaspersky Automated Security Awareness Platform 免費試用

# 卡巴斯基培訓課程組合

我們的培訓課程組合包括了網路安全以及產品方面的培訓，可提供資訊安全專家所需的技能來有效使用複雜的安全解決方案，以及根據您獨特的需求加以自訂。網路安全培訓所涵蓋的領域像是惡意軟體分析、威脅搜捕以及事件回應等，可協助組織充分利用其安全投資，同時維持強大的安全態勢。

卡巴斯基網路安全培訓

卡巴斯基產品培訓

## 網路安全培訓

### 主題

- 反向工程
- 事件回應
- 主動威脅搜捕
- 工業網路安全培訓

### 培訓形式

- 線下
- 線上
  （由講師帶領）
- 自學

# 在外部專家的指導與支援下管理您的安全事件

06

全方位的網路安全服務可協助您的組織應對複雜的威脅。在我們專業知識的支援下，您的企業將受到保護並準備好應對任何安全挑戰。

# 卡巴斯基安全服務

**Kaspersky Managed Detection and Response**

持續地監視、偵測及回應

**Kaspersky Incident Response**

數位鑑識、事件回應以及惡意軟體分析

**Kaspersky Compromise Assessment**

偵測漏洞以及過去攻擊的痕跡


**Kaspersky SOC Consulting**

自建 SOC 或是加強現有安全程序

**Kaspersky Security Assessment**

透過實用的演練，找出攻擊者會如何利用您的安全漏洞

**Kaspersky Digital Footprint Intelligence**

監視您的數位資產以偵測外部威脅

深入瞭解

# MDR 與事件回應

Kaspersky Managed Detection and Response

全天候的代管式防護，可抵禦網路威脅以及傳統的自動化安全措施所無法偵測的複雜攻擊。

## 可帶來的幫助

確保迅速偵測到威脅並加以應變，以便將可能造成的停擺時間與財務損失降至最低。

享受自有 SOC 的所有主要好處，但沒有自行建立 SOC 的麻煩與花費。

減少您的安全成本以及雇用與訓練多名昂貴的 IT 安全專業人員來做出完整安全防護的需要。

讓您的內部 IT 安全資源能夠將注意力轉移到其他對業務至關重要的問題。

Kaspersky Incident Response

這項服務涵蓋了從最初的應變與證據收集，到識別主要攻擊媒介並準備攻擊緩解計畫，整個事件調查與回應週期。

## 可帶來的幫助

快速遏制並解決事件，以便將造成的業務中斷降至最低，並減少營運停擺時間。

由專家帶領進行調查。由卡巴斯基的網路安全專業人員進行深入的事件分析。

我們經濟實惠的事件管理功能可減少安全漏洞所帶來的相關財務損失。

以量身打造的安全性加強功能，強化未來對類似攻擊的防禦能力，享受更強的網路恢復能力。

# 探索 MDR 與事件回應如何在 2024 年成為數位王國的守護者

靜默護盾與數位惡龍：MDR 的主動式防護



惡龍時刻：事件回應如何將結局從毀滅改成復活

數十年來，我們的 MDR 與事件回應服務保護了各行各業的安全。如今，世界各地的組織都仰賴我們久經考驗的專業知識以及不懈的創新來保衛他們的數位前線。探索我們專家所出的最新報告，預先防範新興威脅。

取得報告

# 全球信賴、久經考驗的解決方案

我們為全球逾 200,000 個各行各業的企業客戶提供防護，能為各種規模與複雜度的組織提供有效的安全解決方案。

**200**
個國家與地區

**30+**
個區域代表辦公室

卡巴斯基觸角遍布全球又懂在地需求，能在任何地方提供受信賴的防護。

| 為每個產業量身打造 | 各板塊的商業客戶 | 國家/地區 |
|---|---|---|
| 金融服務 | ~3,500 | 130 |
| 政府機關 | ~6,300 | 125 |
| 能源業 | ~1,600 | 93 |
| 製造業 | ~38,000 | 171 |
| 零售 | ~12,700 | 125 |
| 醫療照護 | ~4,900 | 89 |

還有更多

交通運輸 | 石油與天然氣 | IT | 教育 | 電信業

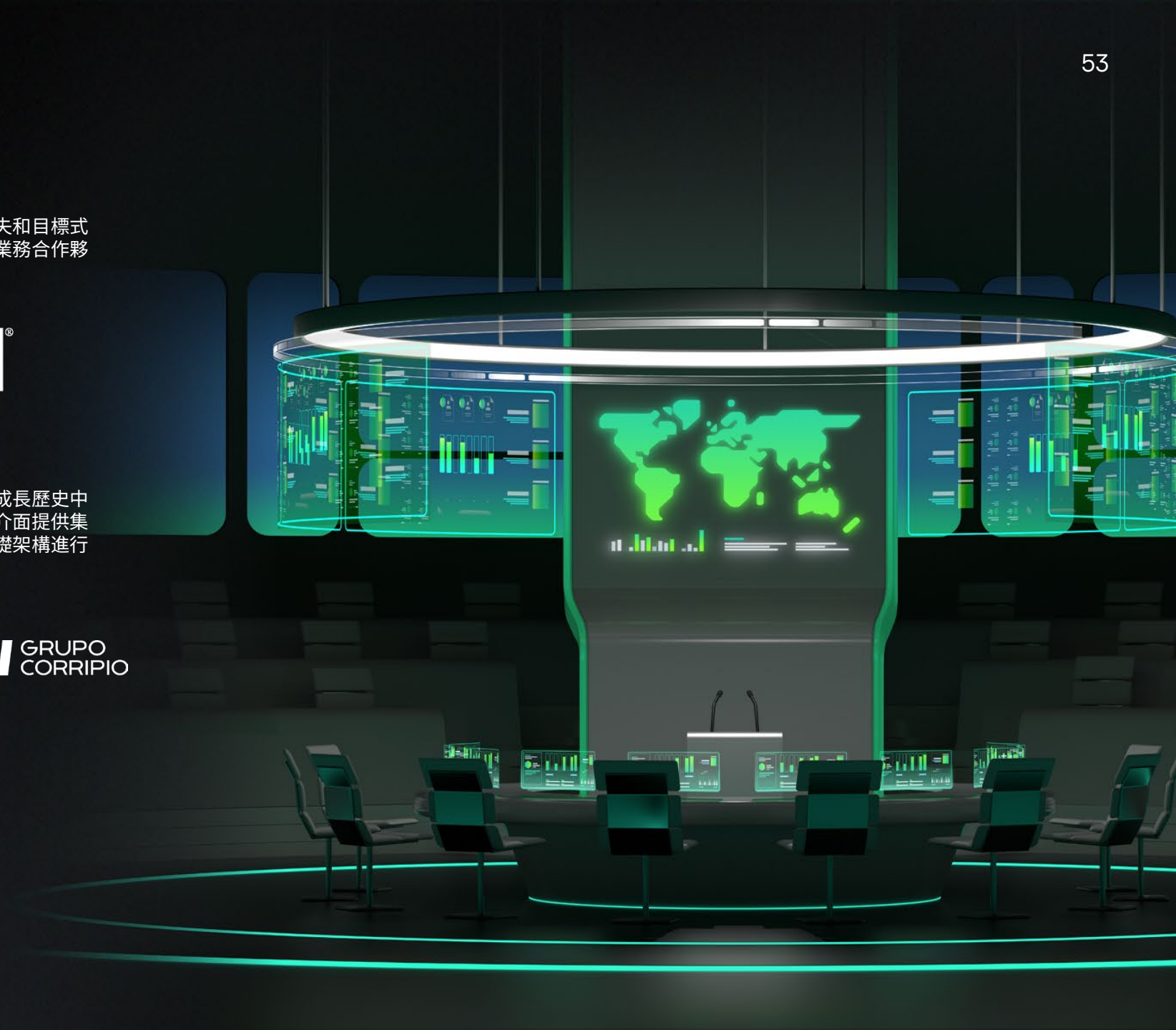
# 個案研究

> 卡巴斯基讓我們能夠保護自家免受網路威脅、資料遺失和目標式攻擊。我們還能夠達到最高安全標準，增加我們全球業務合作夥伴的信心。

**Lijun Zhong**
IT 經理，建溢集團有限公司

> 多年來，卡巴斯基一直是我們的戰略盟友，也是我們成長歷史中重要的一部分。卡巴斯基透過直覺、對使用者友善的介面提供集中化監視與管理功能，讓我們能對自家的網路安全基礎架構進行更完整詳細的檢視與控制。

**Radhames Mendez**
資深業務持續性經理，Grupo Corripio



閱讀所有個案研究

# 為卡達奧林匹克委員會提供的進階防護

多哈，
卡達

代表卡達的國家
奧林匹克委員會

閱讀案例

## 挑戰

面對日益增多的網路安全威脅，卡達奧林匹克委員會 (QOC) 需要一套強大且可擴展的安全架構。鑑於有多種數位資產以及重要的 IT 基礎架構，他們需要一套主動式解決方案來保護敏感資料並確保無縫的運作。

## 解決方案

所施作的卡巴斯基解決方案在經整合後，提供了全方位的防護。

- Kaspersky Anti Targeted Attack
- Kaspersky CyberTrace
- Kaspersky Threat Data Feeds
- Kaspersky Threat Lookup
- Kaspersky Next EDR Expert

## 成果

卡達奧林匹克委員會利用卡巴斯基解決方案，顯著提升了網路威脅偵測成效、快速回應速度以及 SOC 效率。加強的安全控制、無縫的擴展能力以及主動式更新確保了恢復能力。卡巴斯基在實施及事件回應期間所提供的支援，讓 QOC 更加能夠有效緩解不斷演變的全球網路威脅。

> 卡巴斯基提供的功能還有他們聆聽我們的需求，超出了我的期待。他們使我們對產品以及背後的人員充滿信心，並讓我們擁有更安全的網路。

**Rashid AlNahlawi**

卡達奧委會 IT 安全顧問

# 加強的集中化 IT 與 OT 安全防護 Condor Carpets

哈瑟爾特，荷蘭

歐洲最大的地毯製造商

閱讀案例

## 挑戰

Condor Carpets 希望確保其龐大的工業網路受到強大且可擴展的防護。面對網路威脅的不斷發展，Condor Carpets 需要有一套解決方案來保護其 IT 系統，還有特別就是其作業科技 (OT) 網路。

## 解決方案

卡巴斯基解決方案協助為 IT 與 OT 領域打造了集中化安全防護：

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Threat Data Feeds
- Kaspersky Next EDR Optimum

## 成果

與卡巴斯基合作後，Condor Carpets 抵禦網路威脅的能力大幅增加了，不僅整體安全態勢增強，同時還確保了製造流程能無縫運作。在日益數位化的工業環境中，此次成功的施作為 Condor Carpets 的持續成長與恢復能力奠定了強大的基礎。

> 卡巴斯基解決方案為我們的網路以及網路安全組成帶來了革新。我們有信心他們能夠保護我們複雜的作業。

**Patrick de Haan**

IT 經理，Condor Carpets

www.kaspersky.com.tw



#kaspersky
#bringonthefuture