Kaspersky Industrial CyberSecurity：解決方案概要

kaspersky 引領未來

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity：解決方案概要

簡介

根據過往的經驗，全球的工業公司對其 IT 和 OT (營運技術) 網路的網路安全處理方式不盡相同。多數公司的企業基礎結構具備成熟的入侵偵測和事件回應措施，但是在 OT 方面經常仰賴傳統的隔離網閘方法。工業公司變得越來越「數位化」，在智慧技術、新型自動化系統，以及採用工業 4.0 方面的投資越來越多。這些實際上消除了 IT 和 OT 之間可以用來防止網路威脅影響工業控制系統的環境落差。根據卡巴斯基 ICS CERT 的資料，在 ICS 電腦上偵測到惡意物件的比例，在 2019 年上半年達到 41.2%[1]。

這些威脅是什麼？

首先，這些威脅包括傳統惡意程式意外感染的風險。您不必從目標變成受害者。內含銀行木馬程式或勒索軟體的單一快閃磁碟機或網路釣魚電子郵件在無意間帶入 ICS 環境，可能會對公司的核心業務造成嚴重影響。即使意外感染並不會經常發生，但心懷不軌的駭客明顯也有可能滲透 OT 網路，並且對昂貴的設備或生產造成可觀的損害，或是竊取貴重的資訊。

什麼是適當的 ICS 網路安全措施？

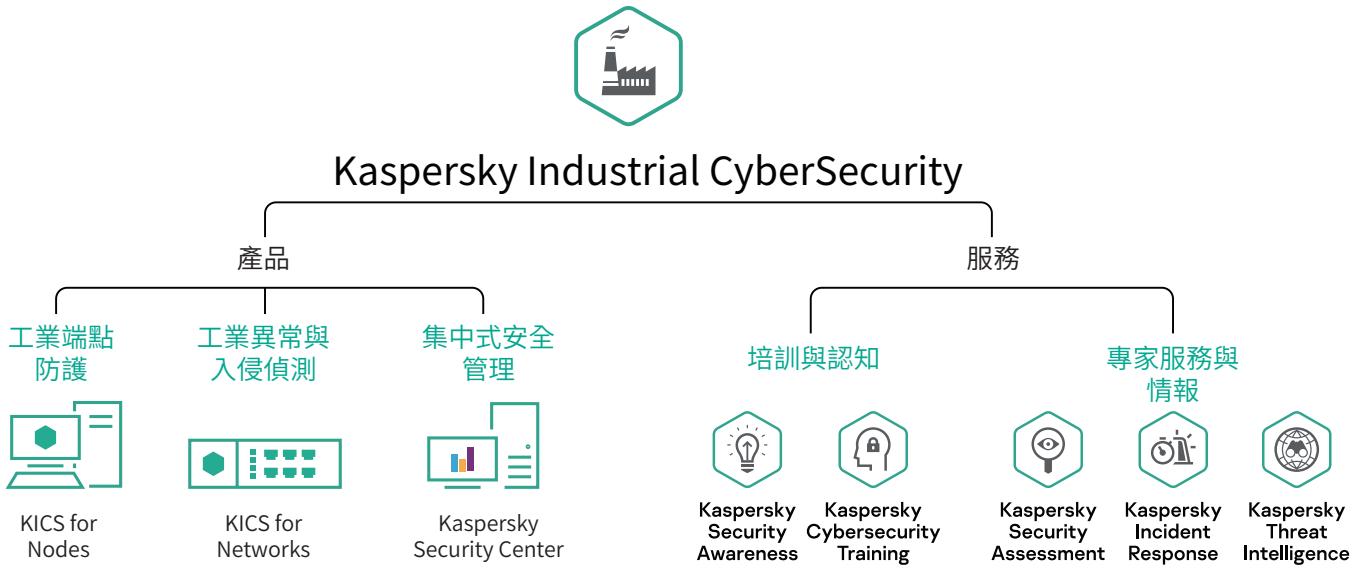
1.工業端點防護，可以防止意外感染，以及讓心懷不軌的人更難入侵。
2.OT 網路監控和異常偵測，可以識別可程式邏輯控制器 (PLC) 層級上的惡意行動。
3.員工培訓計畫，可以減少意外，並將人為因素減到最少。
4.專屬的專家服務，可以調查基礎結構、進行專家分析，或是緩解事件的影響。

1 2019 年上半年工業自動化系統的威脅現況，卡巴斯基 ICS CERT

卡巴斯基提供哪些產品？

卡巴斯基的 Kaspersky Industrial CyberSecurity (KICS) 產品組合可以解決工業企業組織的所有網路安全需求。KICS 可以提供工業網路安全整體式的方法，為客戶 OT 資訊安全流程的任何階段提供價值，從網路安全評估和培訓，到先進技術與事件回應。

Kaspersky Industrial CyberSecurity 元件



在 Gartner 2020 年的報告「競爭現況：營運技術資訊安全」[2] 中提到，卡巴斯基是以下 4 種產品類別的代表性供應商，包括：

- OT 端點安全；
- OT 網路監控和可視性；
- 異常偵測、事件回應和報告；
- OT 安全服務。

Arc 顧問集團強調，卡巴斯基將威脅情報、機器學習和人類專業知識完美的結合，可以提供防止任何類型威脅的靈活防護[3]。

此外，Forrester 的研究[4]證實使用 Kaspersky Industrial CyberSecurity 的公司可以獲得 368% 的投資報酬率，以及專家支援和安心使用等其他優勢。

2 Gartner：競爭現況：營運技術資訊安全，2020 年 3 月
https://ics.kaspersky.com/KICS-cited-in-Gartnercompetitive-landscape-OTsecurity

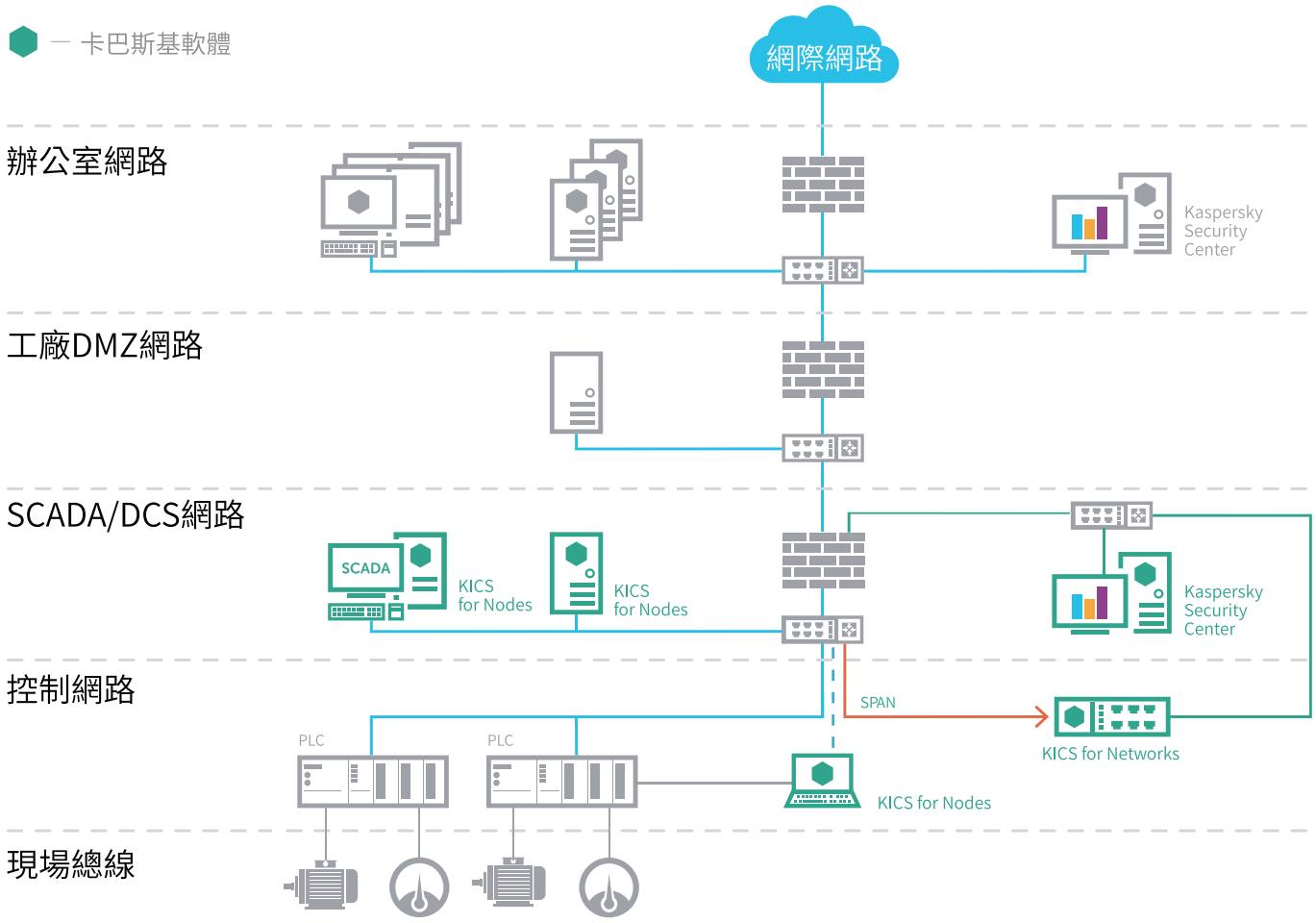
3 Arc Advisory：卡巴斯基發展更強大的網路安全解決方案，2018 年

4 Forrester Research：Kaspersky Industrial CyberSecurity 的整體經濟影響 (Total Economic Impact ™)，2019 年 4 月。
https://www.kaspersky.com/forrester-tei-for-kics

產品

KICS 產品是為了完整保護貴企業組織的工業要素所設計：KICS for Nodes 的目標在於保護工業端點，而 KICS for Networks 則是監控工業網路安全。

Kaspersky Industrial CyberSecurity 產品部署



KICS for Networks

KICS for Networks 是一款 OT 網路監控和可視性解決方案，以軟體或虛擬裝置的形式提供，可以被動連線至 ICS 網路。

優勢：

- ✓ **資產探索**
  被動 OT 資產識別和盤點
- ✓ **深度封包檢測**
  幾乎即時的技術流程遙測分析
- ✓ **網路完整性控制**
  偵測未經授權的網路主機和流量
- ✓ **入侵偵測系統**
  傳送惡意網路活動的相關警示
- ✓ **命令控制**
  檢查工業通訊協定上的命令
- ✓ **外部系統**
  透過 API 整合的外部偵測功能
- ✓ **異常偵測的機器學習 (MLAD)**
  透過即時遙測和歷史資料探勘尋找網路或實體異常 (循環神經網路)

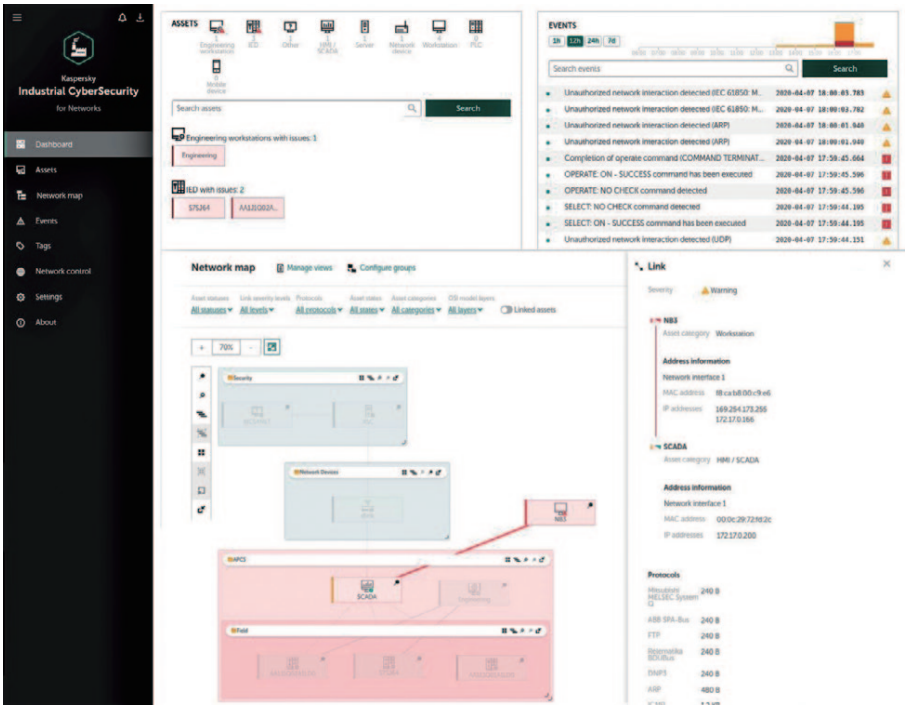
KICS for Networks 可以在其早期階段偵測 ICS 網路內部的異常訊號和入侵行為並確保採取必要行動，以防止對工業流程的任何負面影響。

KICS for Networks 是一種與裝置無關的解決方案，可以讓客戶選擇他們最信任的工業運算裝置供應商。

KICS for Networks 的介面會顯示一個即時儀表板和網路地圖，可以處理資產和安全事件。

KICS for Networks 裝置的範例

KICS for Networks 的介面



KICS for Nodes

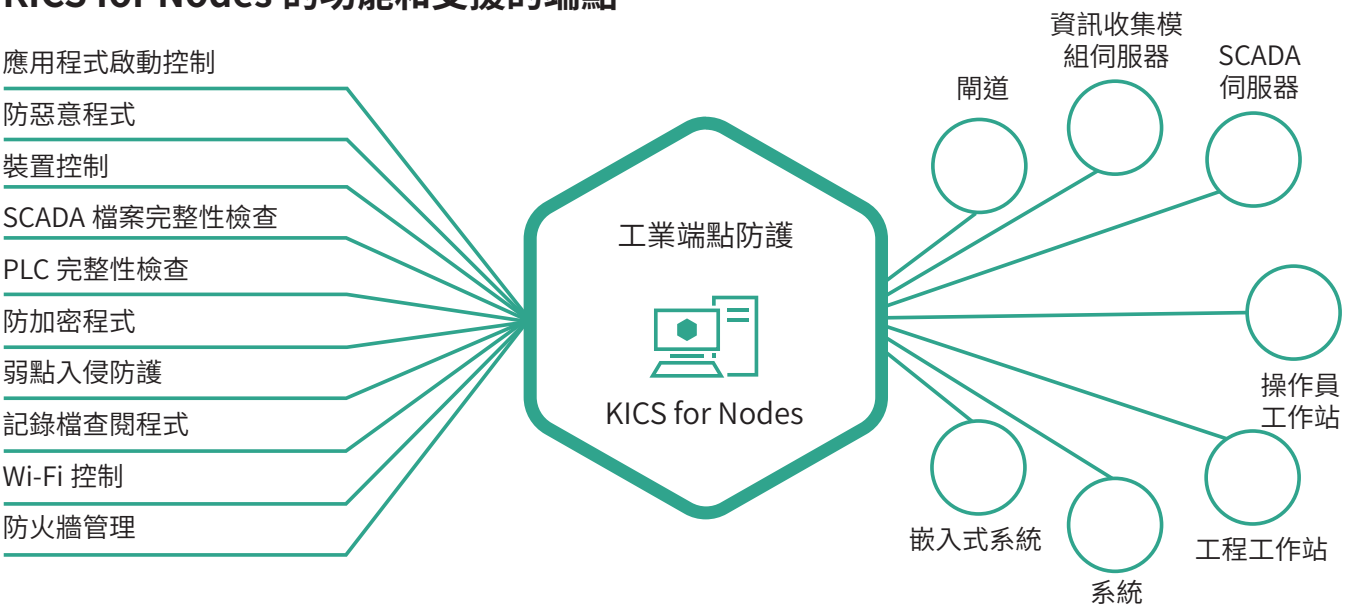
KICS for Nodes 是一款 OT 端點安全產品，以 Windows 和 Linux 電腦軟體的形式提供。

優勢：

- ✓ **對受保護的裝置影響較小**
- ✓ **相容性最高**
- ✓ **進階惡意程式防護**
- ✓ **環境控制**

KICS for Nodes 是專為消耗最少資源所設計。這款產品建立在安全和嵌入式系統中，其模組化的架構代表您只要安裝所需的防護元件即可。防護元件可以設定成威脅防護模式或僅限偵測模式。這個方法非常適合效能低落、需要最多可用運算能力的舊型電腦。

KICS for Nodes 的功能和支援的端點



「我們決定和卡巴斯基合作，因為我們可以在作業仍在繼續運作的同時執行 Kaspersky Industrial CyberSecurity，而且該解決方案和我們使用的控制系統相容」

AGC Glass Germany GmbH
的工廠經理 Jan Houben

KICS for Nodes 可以保護工業節點，防止人為因素、一般惡意程式、針對性攻擊或破壞所造成的各種不同類型網路威脅影響。KICS for Nodes 相容於工業自動化系統的軟體及硬體元件，例如 SCADA、PLC 和 DCS。

Kaspersky Security Center

Kaspersky Security Center 是一款集中式安全管理解決方案。它可以在多個站台以及整個企業網路提供工業防護層的控制和可視性。

優勢：

✓ **系統管理**
- 集中式系統資料收集
- 集中式軟體部署
- 弱點偵測與修補程式管理
- 延伸的用戶端管理功能

✓ **原則管理**
- 集中式安全原則管理
- 遠端工作排程與執行

✓ **報告與通知**
- 事件記錄
- 儀表板和報告
- SMS/ 電子郵件通知

✓**SIEM 整合**
- Arcsight、Splunk、Qradar
- Syslog 伺服器

✓**HMI 整合**

✓**MES 儀表板整合**
- 安全狀態與資訊會傳送到 IEC 104/OPC 2.0 相容的主機

Kaspersky Industrial CyberSecurity：服務

我們的服務套件構成 KICS 產品組合的重要部分 - 我們提供從工業網路安全評估到事件回應的全方位資訊安全服務。

專家服務

「相較於其他供應商，其解決方案在 ICS 網路安全領域、專業水準，以及複雜度方面的體驗，可以為我們帶來更高的價值，以及確保我們公司安全策略的大好未來」

Plzeňský Prazdroj 的 C&A 經理 Ondřej Sýkora

- **工業網路安全評估：**卡巴斯基提供侵入性極低的工業網路安全評估，其中包括外部和內部滲透測試、OT 安全評估，以及自動化解決方案安全評估。卡巴斯基的專家會提供對於公司基礎結構的重要見解，以及如何強化 ICS 網路安全結構的建議。

- **威脅情報：**卡巴斯基專家所收集的最新分析有助於強化客戶的防護，防止客戶遭到針對性的工業網路攻擊。這些資訊會以 TI 即時摘要或量身訂做報告的形式提供，可以根據地區、產業和 ICS 軟體參數來滿足特定客戶的需求。

「透過練習並學習卡巴斯基團隊的知識，我們提高了我們對網路安全威脅的防護。」

PacificLight 的執行長 Yu Tat Ming。

「卡巴斯基是為我們 ICS 集團提供專業工業網路安全技術培訓的最佳公司」

Ezenta 的首席技術長 Søren Egede Knudsen

- **事件回應：**當網路安全事件發生時，我們的專家會收集和分析資料、重新建構事件的時間軸、判斷可能的來源和動機，以及擬定修復計畫。此外，在卡巴斯基提供的惡意程式分析服務中，卡巴斯基的專家會將提供的任何惡意程式樣本進行分類、分析這些惡意程式的功能和行為，以及提出將這些惡意程式從您的系統中移除並將任何惡意行動復原的建議和計畫。

培訓與認知

- **工業網路安全認知培訓：**現場和線上互動式培訓模組以及網路安全遊戲，可以讓員工和工業電腦化系統及其管理員進行互動。學員可以獲得特別針對工業環境的目前威脅現況以及攻擊方式的最新見解、探索實際情況並獲得網路安全的工作技能。現場的課程可以自訂或調整為一或兩天。

- **專家培訓計畫：**ICS 滲透測試和 ICS 數位鑑識培訓模組是針對網路安全專家所設計。學員可以獲得在工業環境中執行完整滲透測試或數位鑑識所需的進階技巧。包括認證。

進一步了解 KICS：
https://ics.kaspersky.com

卡巴斯基
引領未來

www.kaspersky.com

台灣聯繫人：台灣銷售總監 黃茂勳
eden.huang@kaspersky.com

* 第三屆世界網際網路大會中的全球頂尖的網際網路科技成果獎
** 中國國際工業博覽會 (CIIF) 2016 年特別獎