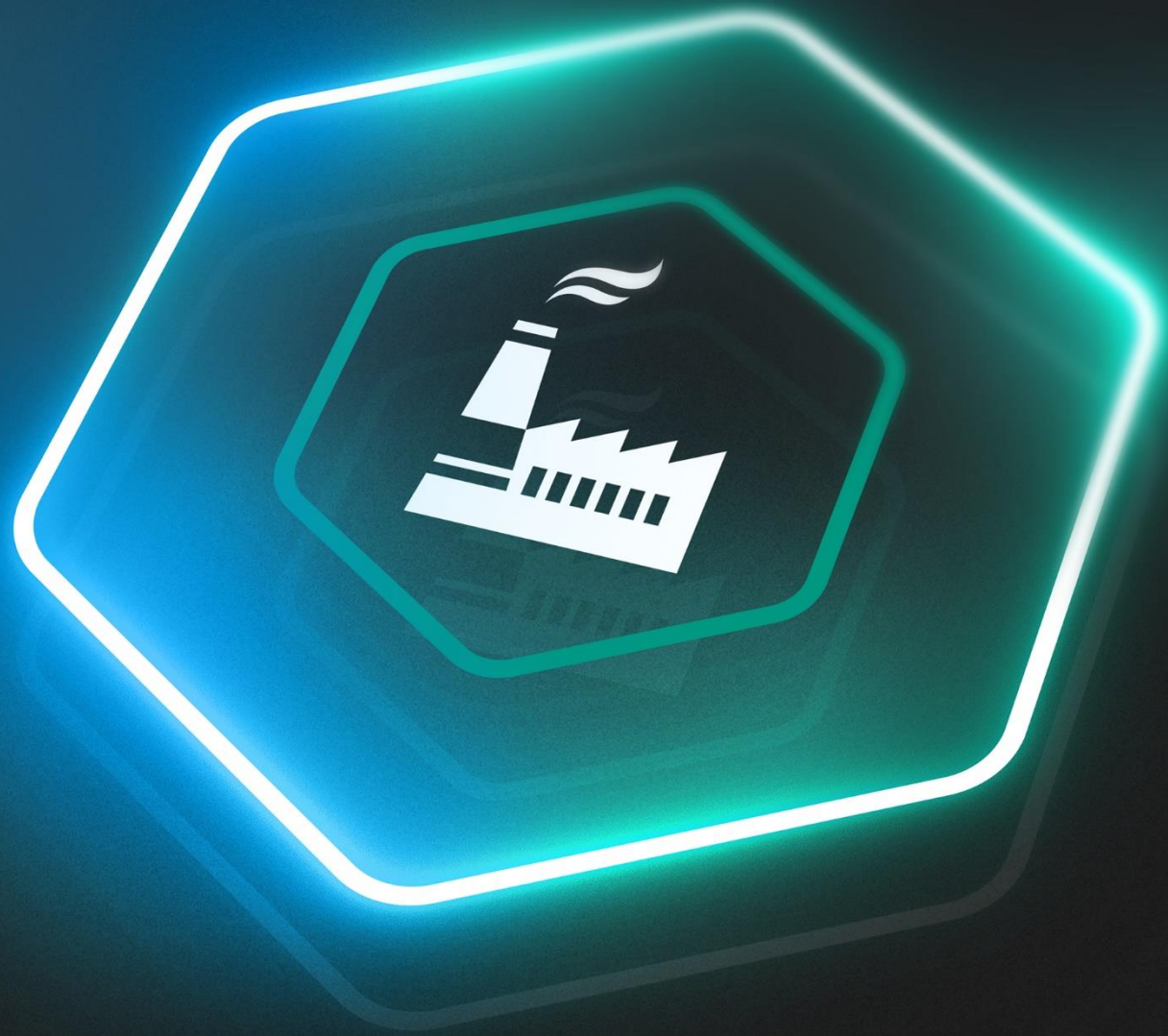
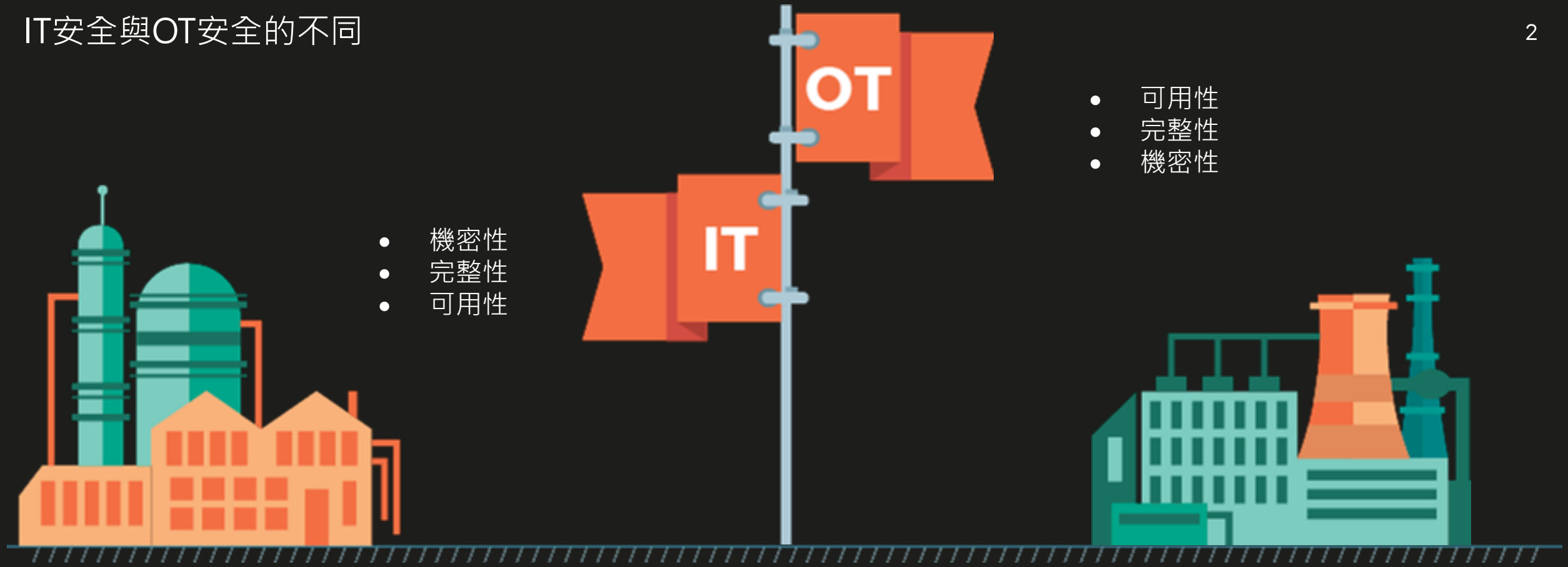
卡巴斯基工控安全規劃與案例分享



卡巴斯基 台灣技術總監
謝長軒 Chandler Hsieh
chandler.hsieh@kaspersky.com

IT安全與OT安全的不同

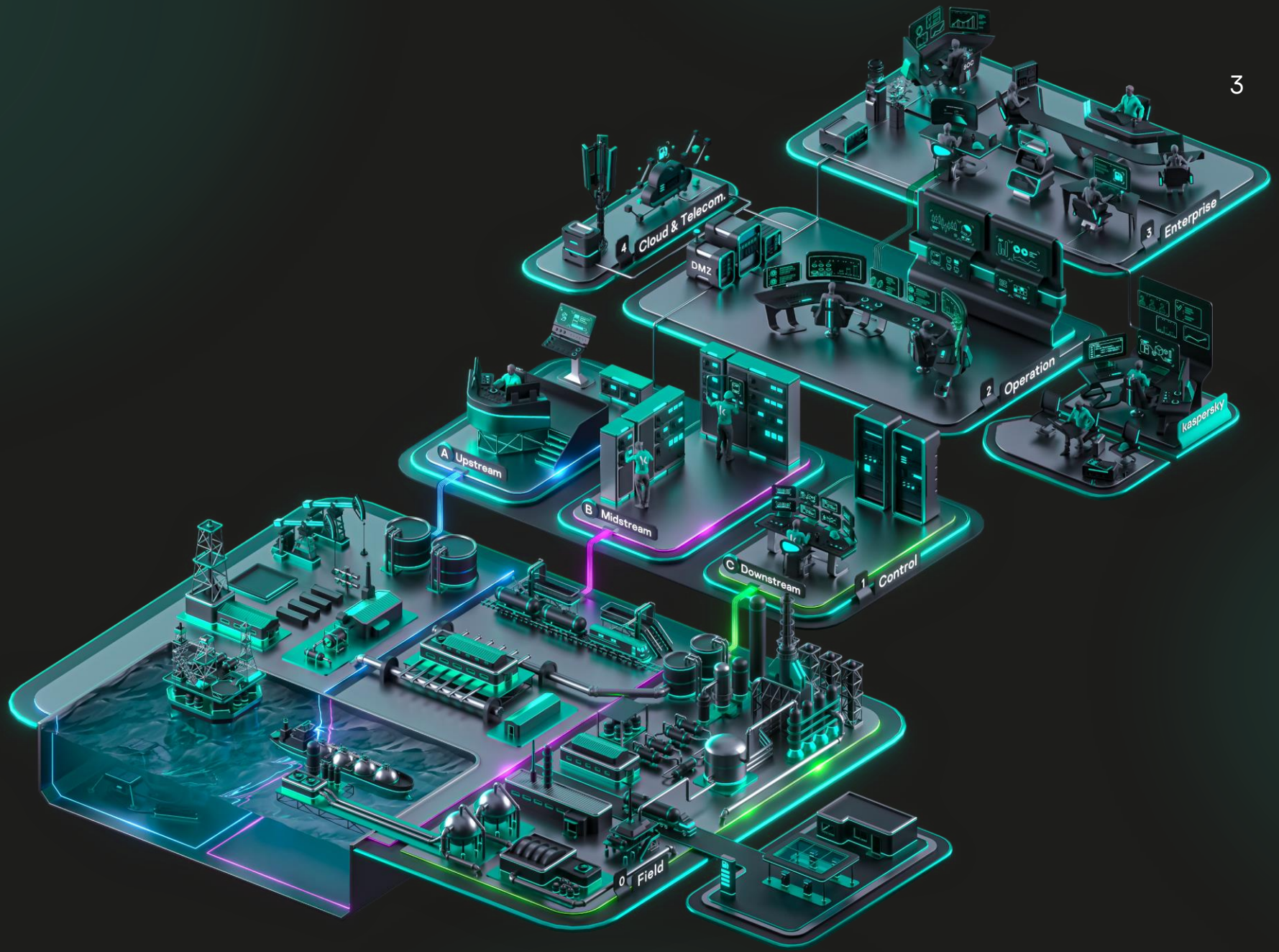


✓ IT安全關注在 資訊安全防護

✓ OT安全更關注在 生產過程安全防護

首先要確保生產過程的連續性

數位化場域示意

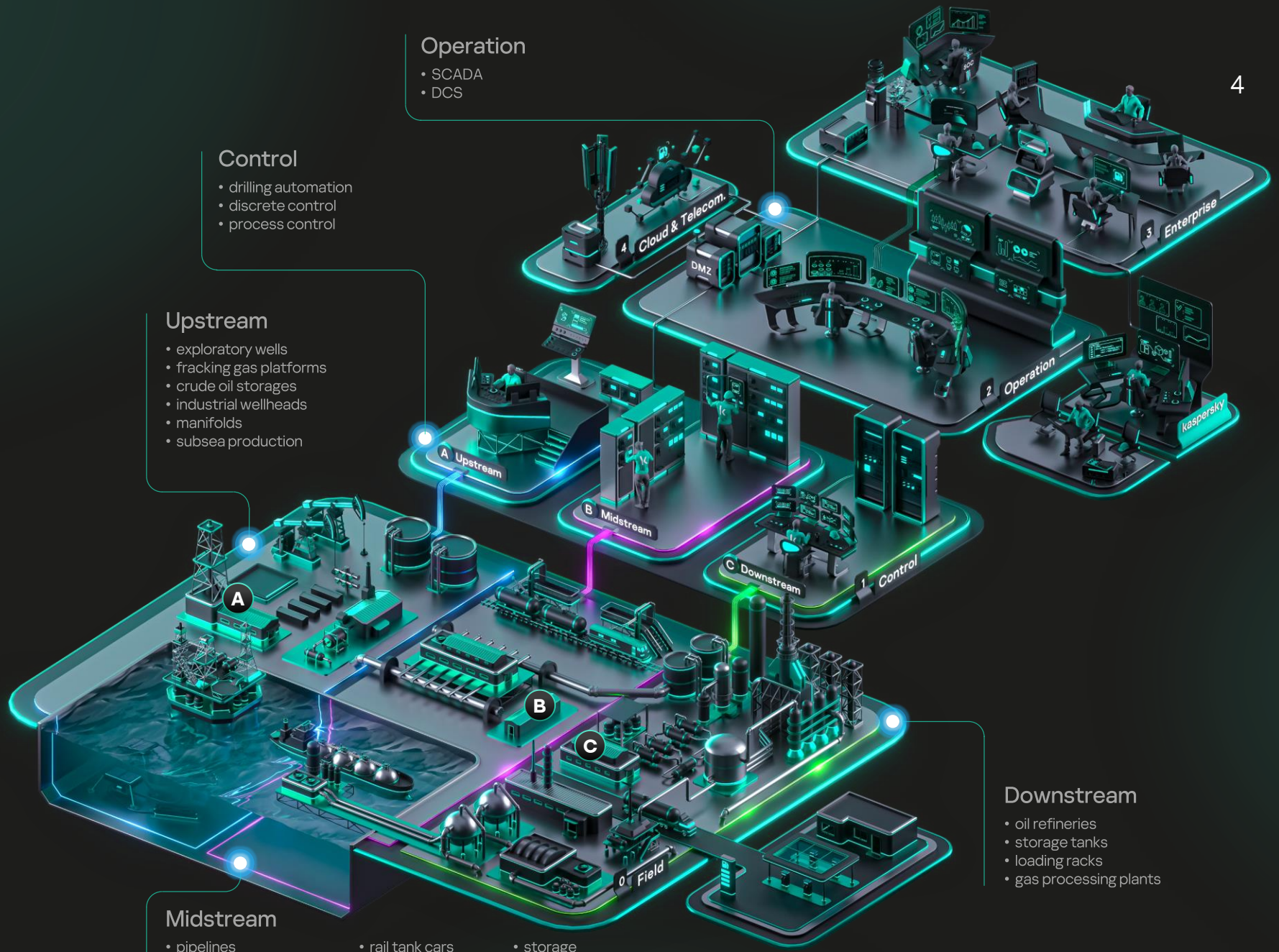

4 Cloud & Telecom.
DMZ
3 Enterprise
2 Operation
kaspersky
A Upstream
B Midstream
C Downstream
1 Control
0 Field

數位化場域示意

Operation
- SCADA
- DCS

Control
- drilling automation
- discrete control
- process control

Upstream
- exploratory wells
- fracking gas platforms
- crude oil storages
- industrial wellheads
- manifolds
- subsea production



Downstream
- oil refineries
- storage tanks
- loading racks
- gas processing plants

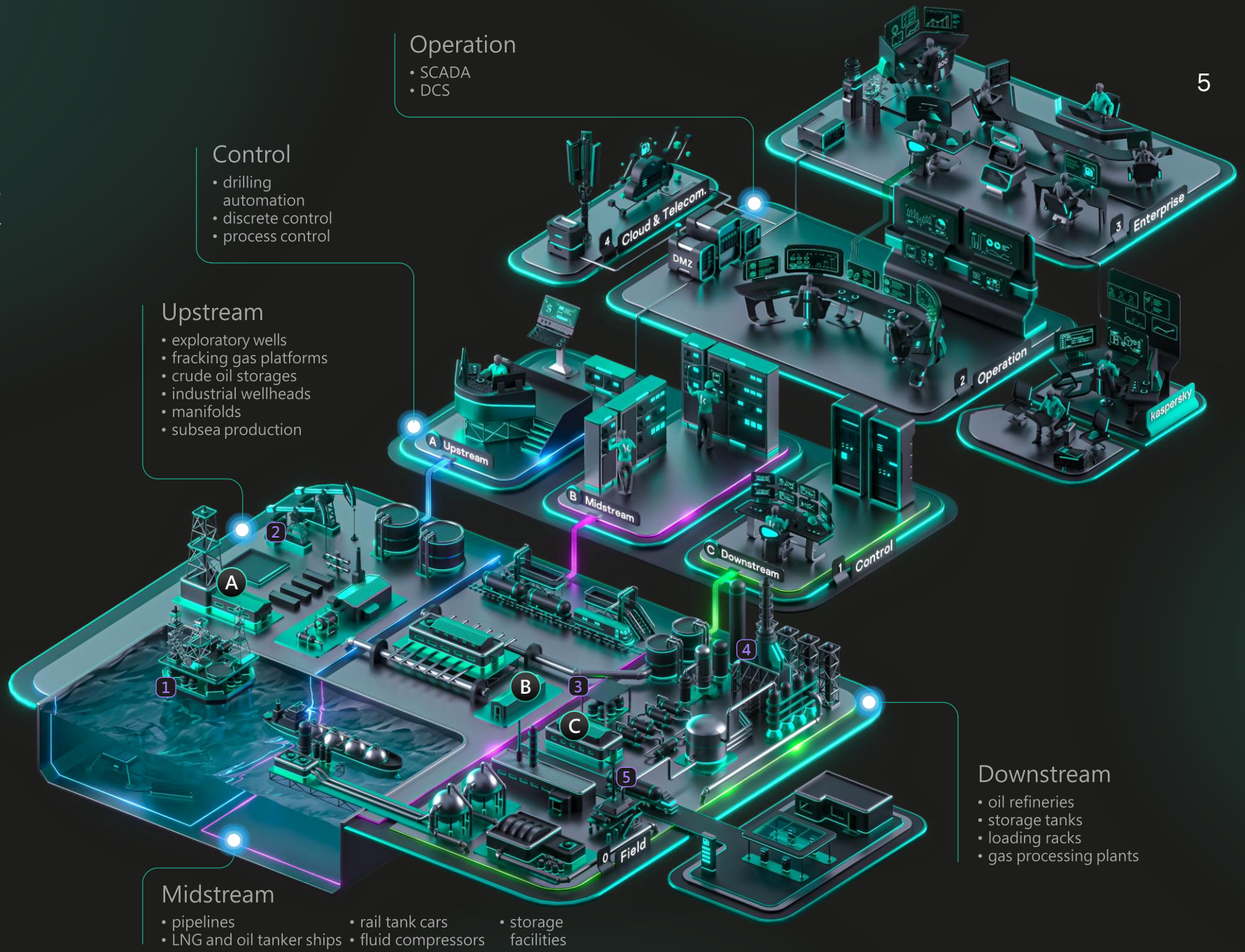
Midstream
- pipelines
- LNG and oil tanker ships
- rail tank cars
- fluid compressors
- storage facilities

數位化場域示意

數位化轉換使用科技

IIoT & Cloud

1. 現場資料獲取
2. 現場作業優化
3. 線路異常偵測
4. 傳感器監控
5. 線路優化及倉儲監控

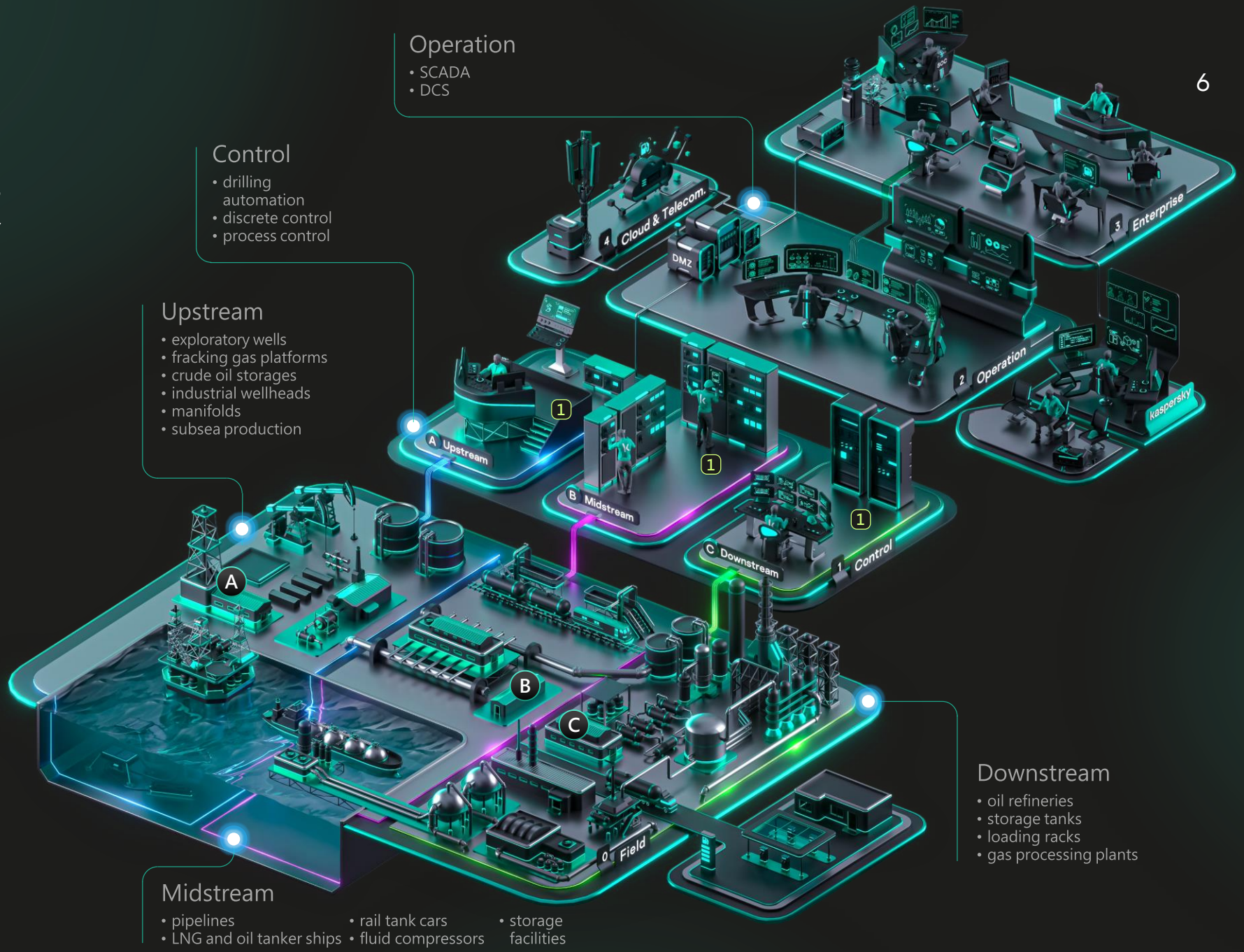


數位化場域示意

數位化轉換使用科技

工控場域元宇宙: AR, VR

1 新進人員教育訓練、協同訓練、維運訓練...等

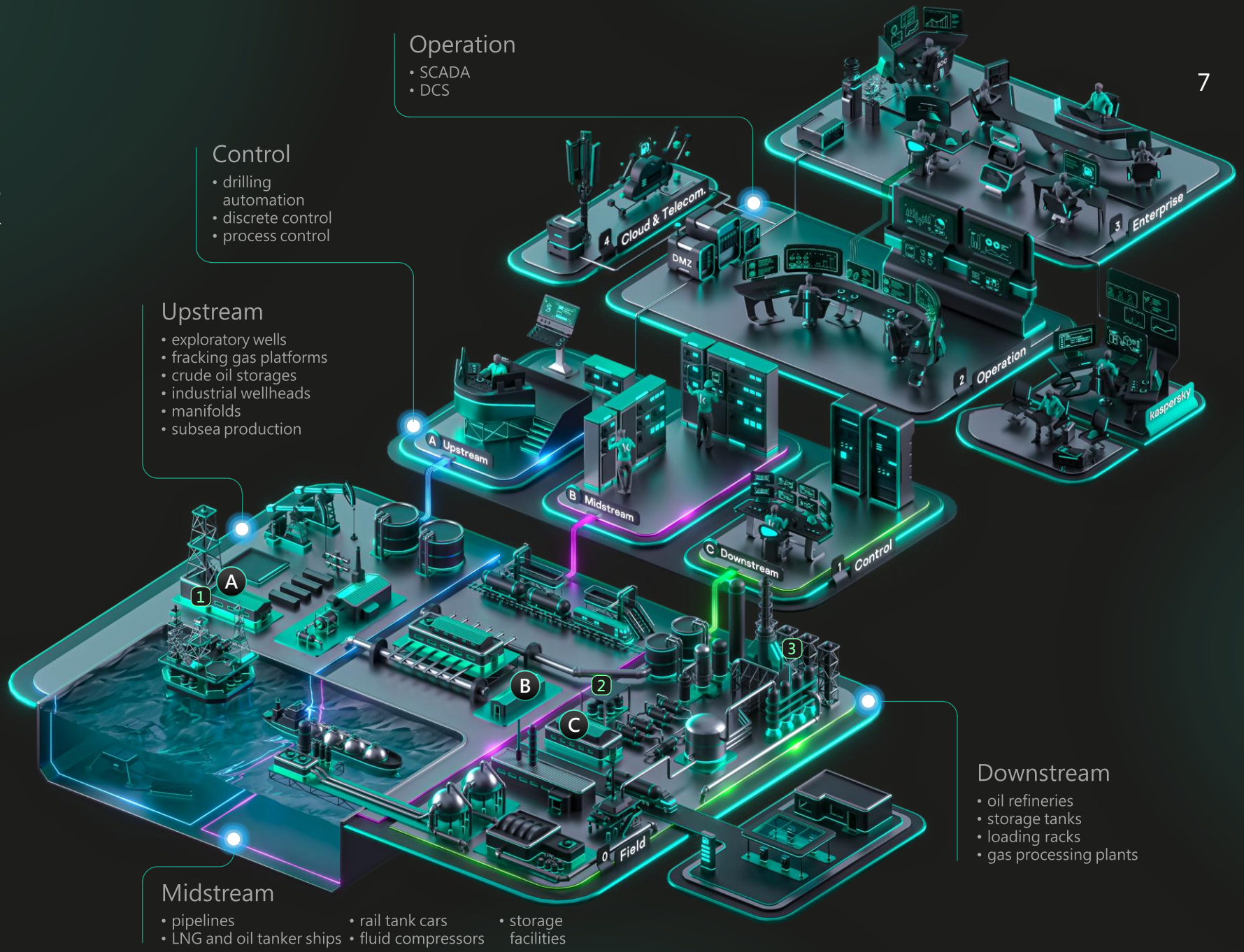


數位化場域示意

數位化轉換使用科技

機器化 及 5G

1. 危險場域機器人/無人機自動化處理
2. 監控人員無法到達的區域
3. 工廠檢查和出現問題時立即回應的能力

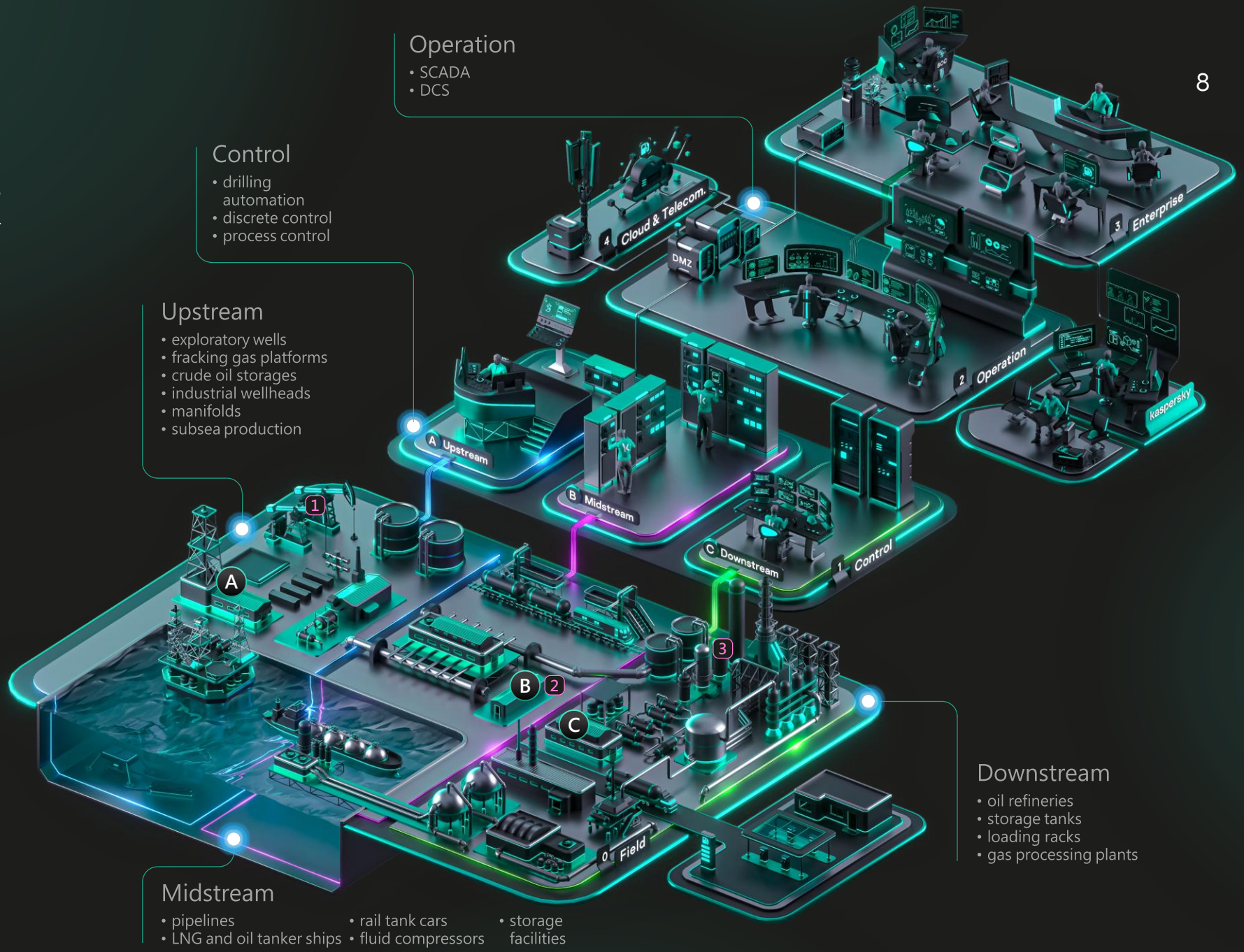


數位化場域示意

數位化轉換使用科技

數位韌性設計

1. 現代化設備替換
2. 雙線路及雙監控機制
3. 透過模擬數據找出可能問題

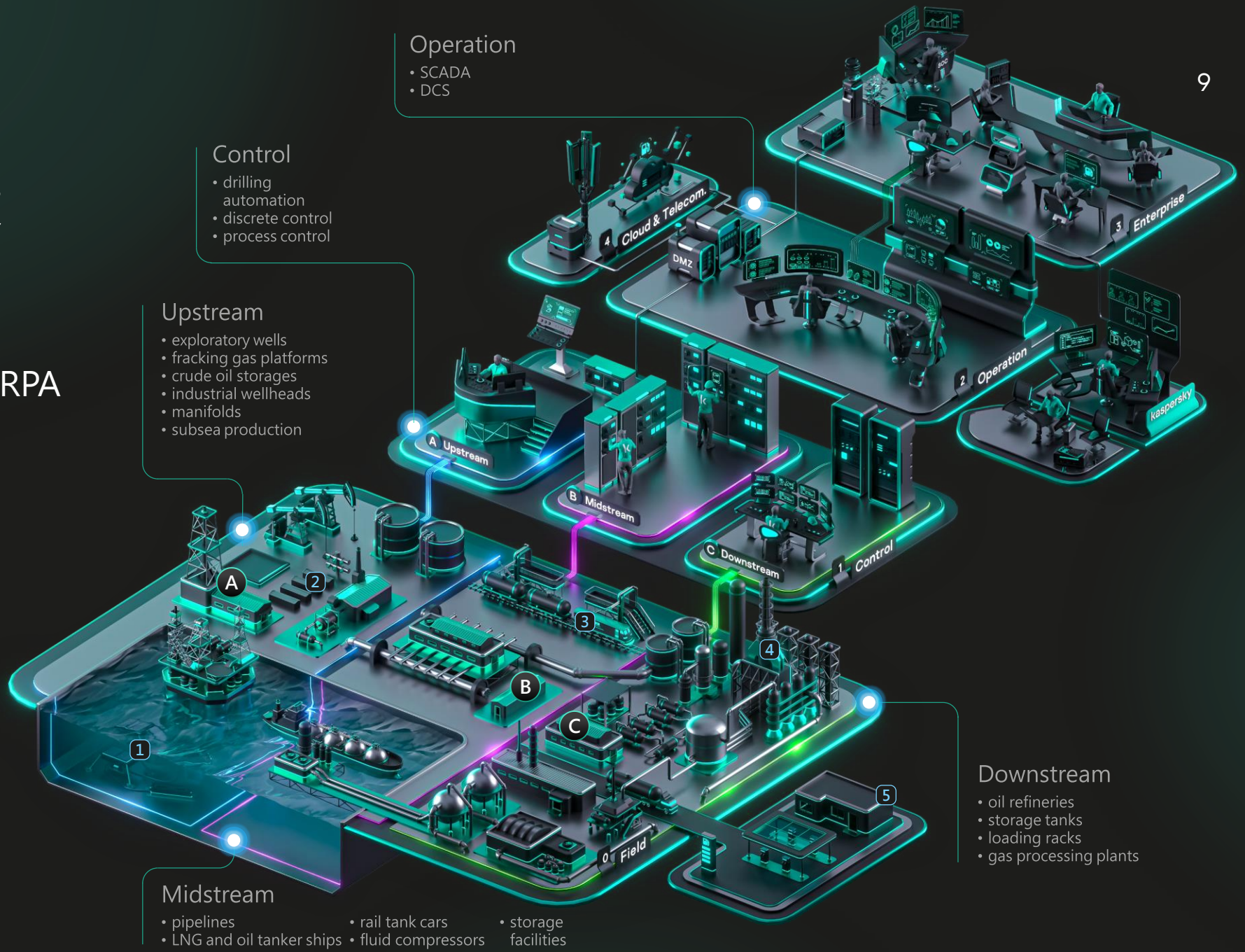


數位化場域示意

數位化轉換使用科技

混合式自動化應用, AI, ML, RPA

1. 現場環境定位
2. 端末訊號異常監控及預測
3. 資料收集及分析
4. 中繼設備故障預測
5. 客戶需求預測

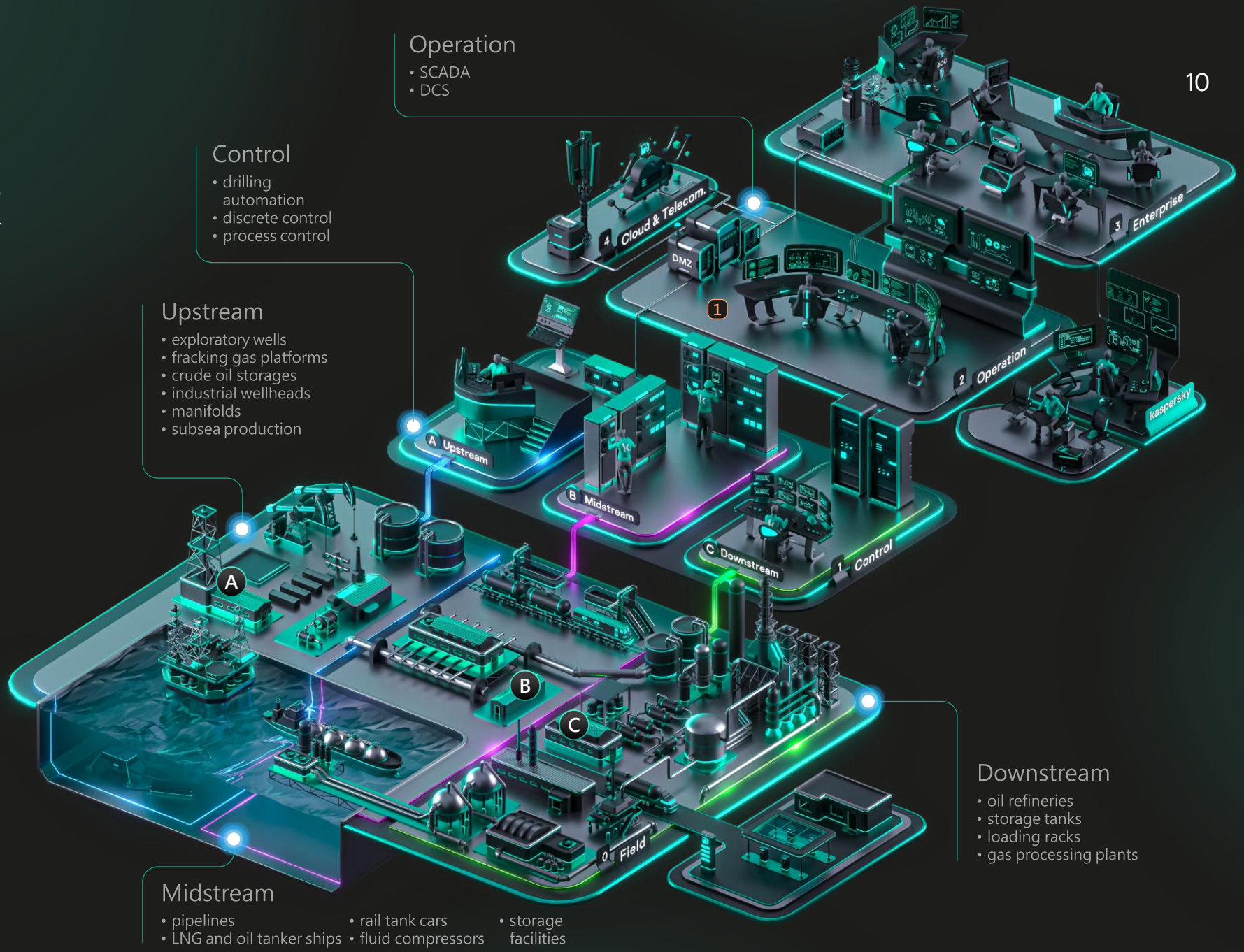


數位化場域示意

數位化轉換使用科技

IT/OT 融合運行

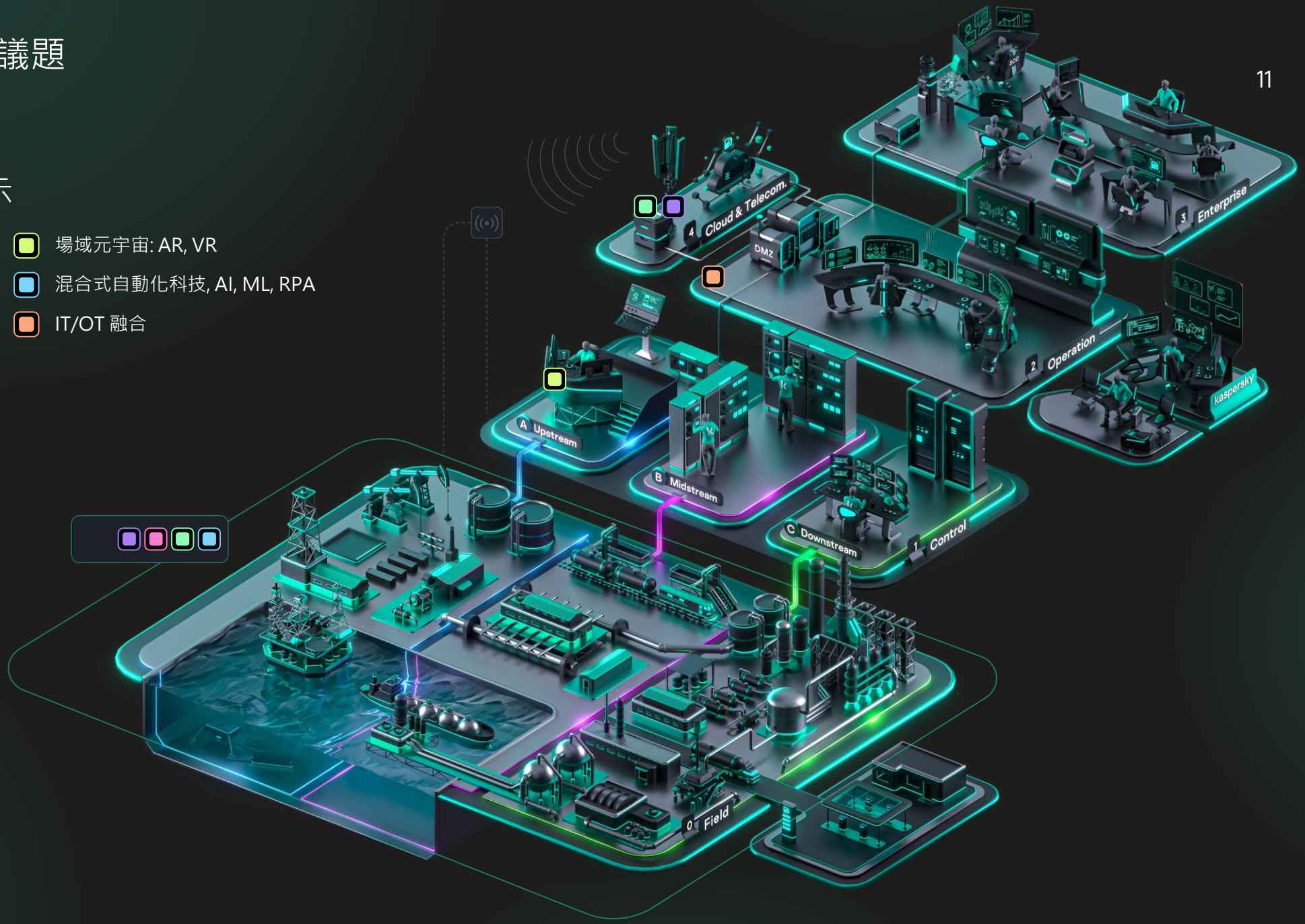
1 即時資料分析從端末傳感器到相關設備



新科技面對的資訊安全議題

數位化科技使用圖示

- IIoT & Cloud
- 數位韌性
- 機器化 及 5G
- 場域元宇宙: AR, VR
- 混合式自動化科技, AI, ML, RPA
- IT/OT 融合



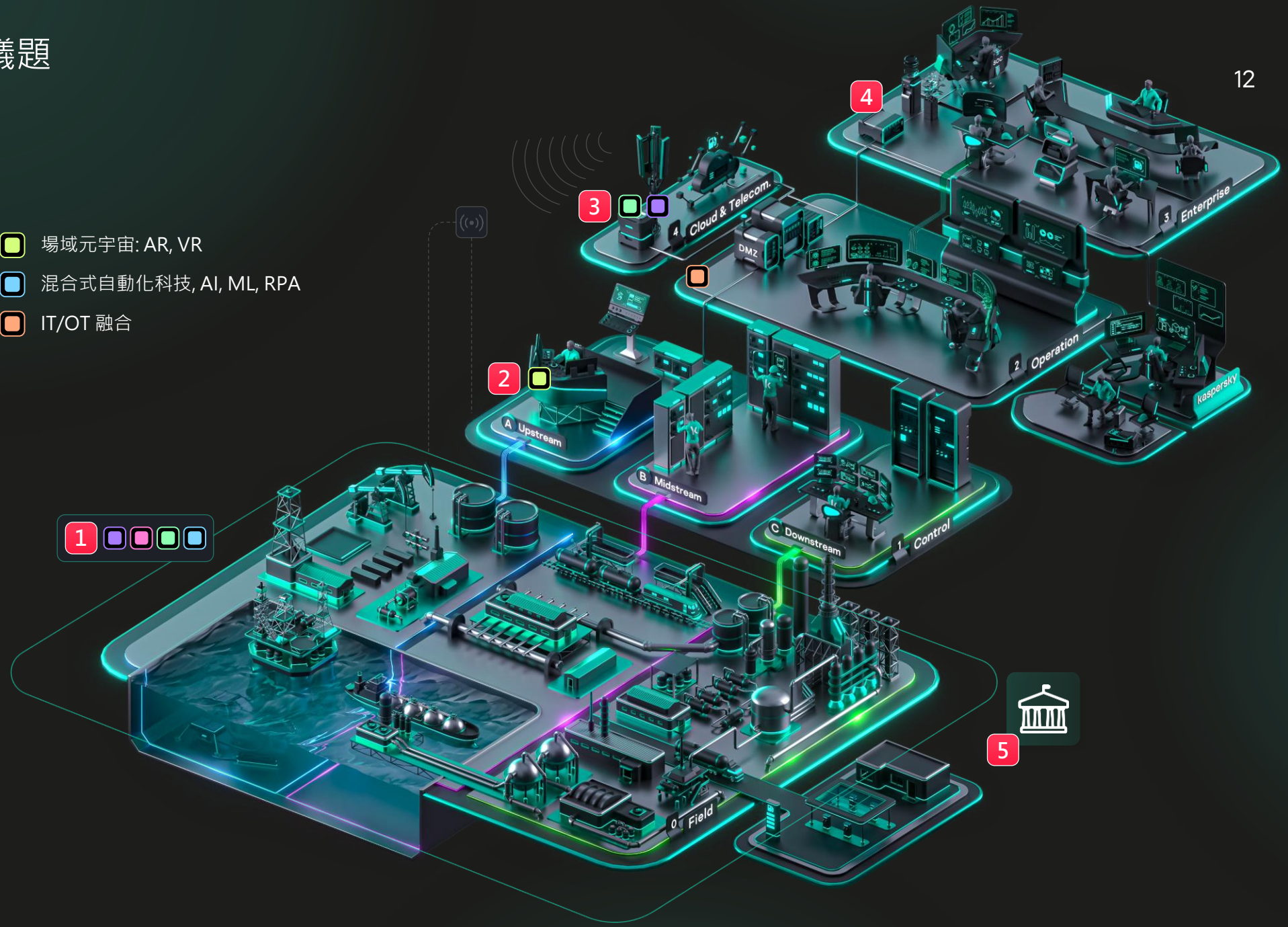
新科技面對的資訊安全議題

數位化科技使用圖示

- IIoT & Cloud
- 數位韌性
- 機器化 及 5G
- 場域元宇宙: AR, VR
- 混合式自動化科技, AI, ML, RPA
- IT/OT 融合

常見的安全風險及挑戰

1. 攻擊面擴大
2. 無法管控過舊的基礎設施影響 IT/OT 的維運
3. 透過外部存取至 OT 基礎設施
4. 人員失誤
5. 關鍵基礎設施的合規需求



Click on item 1-5 to continue

1. 攻擊面擴大

IIoT & Cloud　數位韌性　混合式自動化科技　機器化 及 5G

Upstream process example

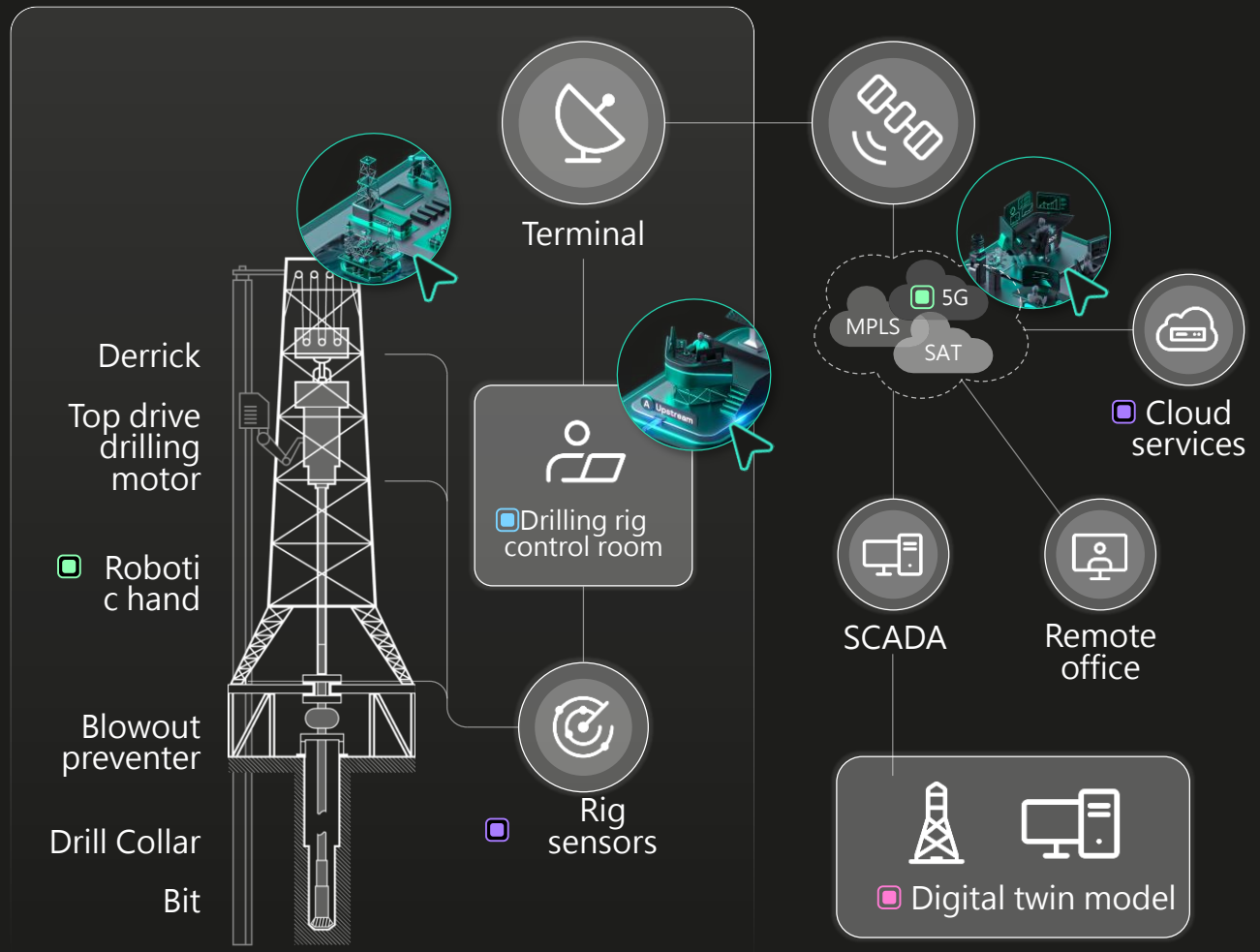
How Kaspersky can help

Kaspersky Industrial CyberSecurity

Ecosystem of supporting services

Kaspersky ICS Security Assessment

Kaspersky Managed Detection and Response



Click to learn more

1.攻擊面擴大

How Kaspersky can help

Kaspersky Industrial CyberSecurity

- 端至端 OT/IIoT 基礎設施融合運用
- 系統及網路可視性
- 定期深度安全稽核

Ecosystem of supporting services

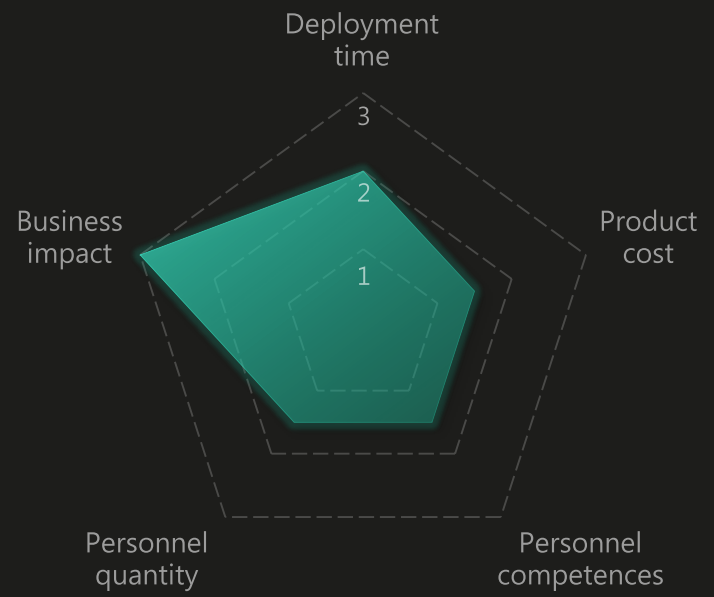
Kaspersky ICS Security Assessment

- 檢視 ICS 基礎設施及相關安全流程是否完善
- 檢核關鍵元件的安全性

Kaspersky Managed Detection and Response

- 主動式威脅偵測
- 自動化及響應指導
- ICS 安全專家團隊

解決方案特性



ICS 監控自動化設備能連接不同系統，導致若其一設備有已知風險。攻擊者就可以利用破口進行相關入侵行為。增加管理人員找到源頭的困難性

Click on product to learn more

2.過舊的基礎設施

IT/OT 融合

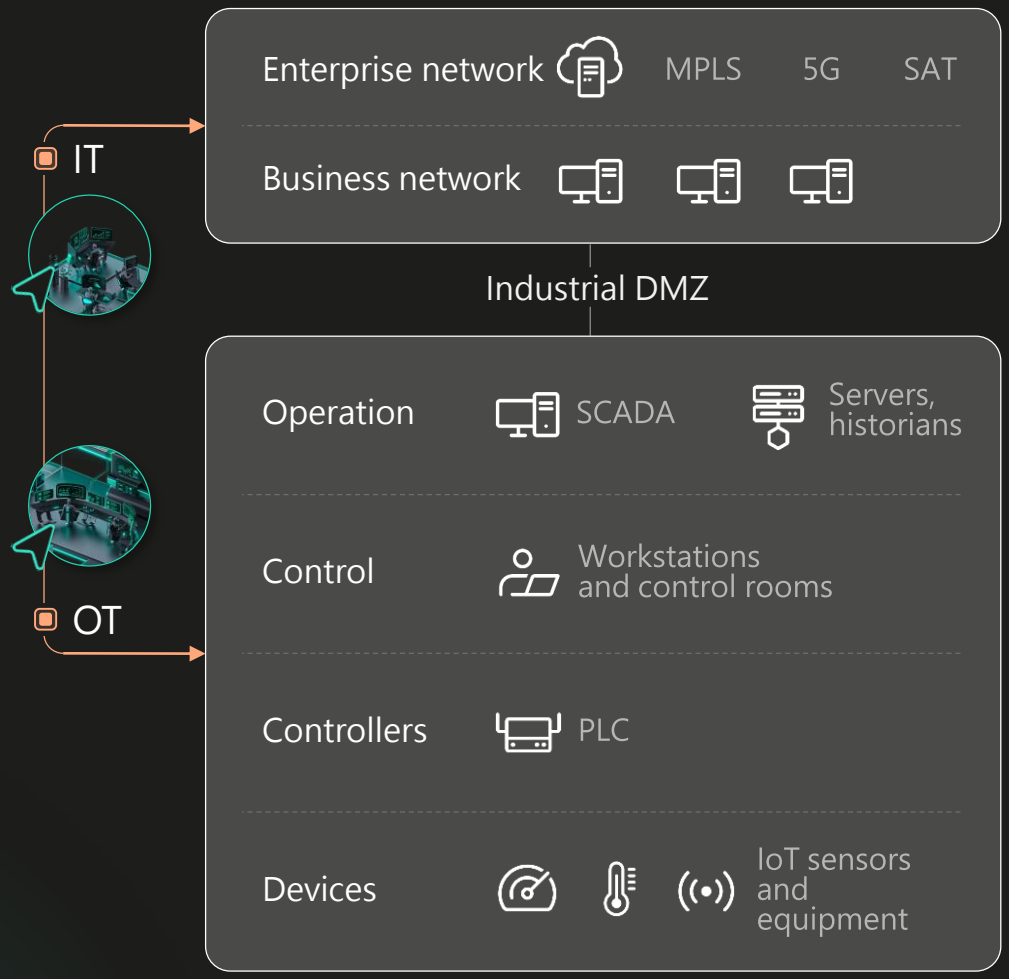
How Kaspersky can help

Kaspersky Industrial CyberSecurity

Kaspersky Extended Detection and Response

Ecosystem of supporting services

Kaspersky Threat Intelligence



Click to learn more

2.過舊的基礎設施

How Kaspersky can help

Kaspersky Industrial CyberSecurity

- 偵測各種威脅及異常行為
- 提供不中斷的安全處理建議
- 集中化管理包含安全政策、資產管理....

Kaspersky Extended Detection and Response

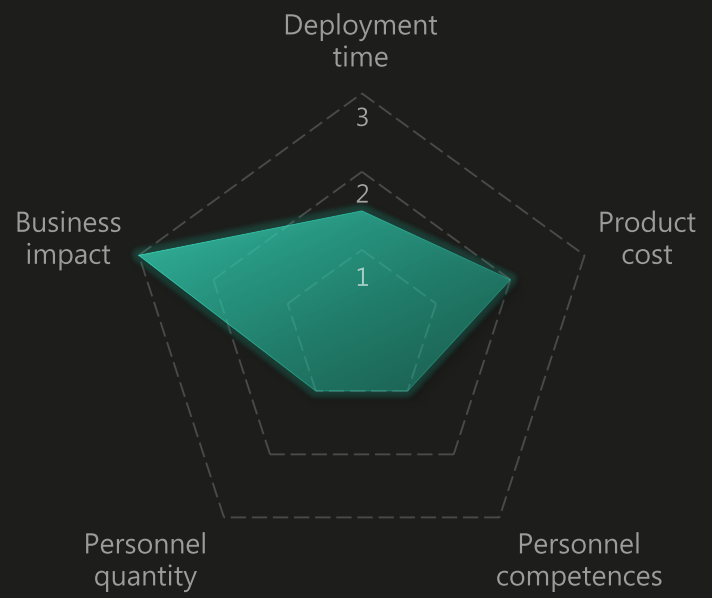
- 強大的勒索病毒、惡意威脅、無檔案式威脅及 APTs
- 跨組織 IT 基礎架構的全面可視性和響應能力

Ecosystem of supporting services

Kaspersky Threat Intelligence

- 提昇事件調查及主動式威脅查找
- 全面的威脅和漏洞資訊

解決方案特性



越來越多的工控設備整合 IT/OT相關資料，成為了新的安全風險。

Unsecured legacy infrastructure with outdated technology

針對資訊安全需求，不同角度要求的安全機制也不同

- IT 關注在資料保密性及完整性
- OT 關注在即時的可用性及維運及可用性。

Click on product to learn more

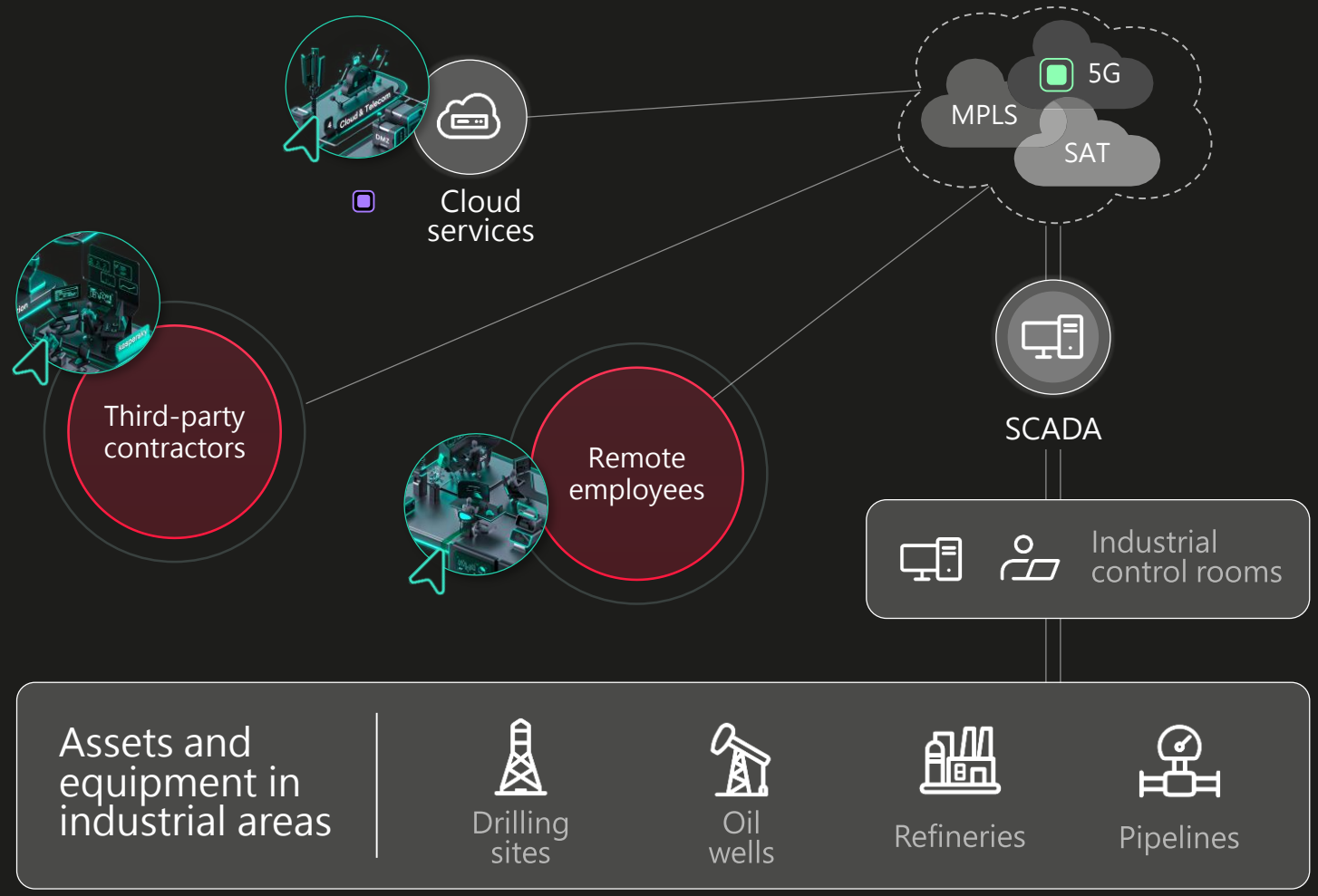
3.從外部存取 OT場域設備

IIoT & Cloud 機器化 及 5G

How Kaspersky can help

Kaspersky SD-WAN

Kaspersky Thin Client



Click to learn more

3.從外部存取 OT場域設備

How Kaspersky can help

Kaspersky SD-WAN

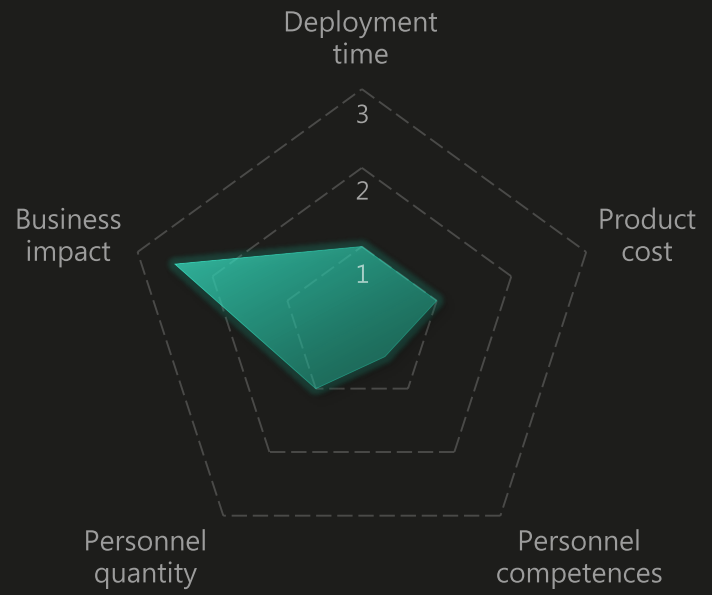
Rapid deployment of distributed network

- Easy scalability
- Convenient management
- Centralized security

Kaspersky Thin Client

- Cyber immune thin clients for secure remote access
- Centralized management for simple administration of the thin client infrastructure

解決方案特性



開放透過遠端連線維護方式，連到場域的相關設備進行維護。因為對 OT 基礎設施具有更廣泛存取權限的用戶可能會使其面臨重大的網路攻擊風險

Click on product to learn more

4.人員失誤

場域元宇宙　IT/OT 融合

How Kaspersky can help

Kaspersky Industrial CyberSecurity

Kaspersky Extended Detection and Response

Ecosystem of supporting services

Kaspersky Security Awareness

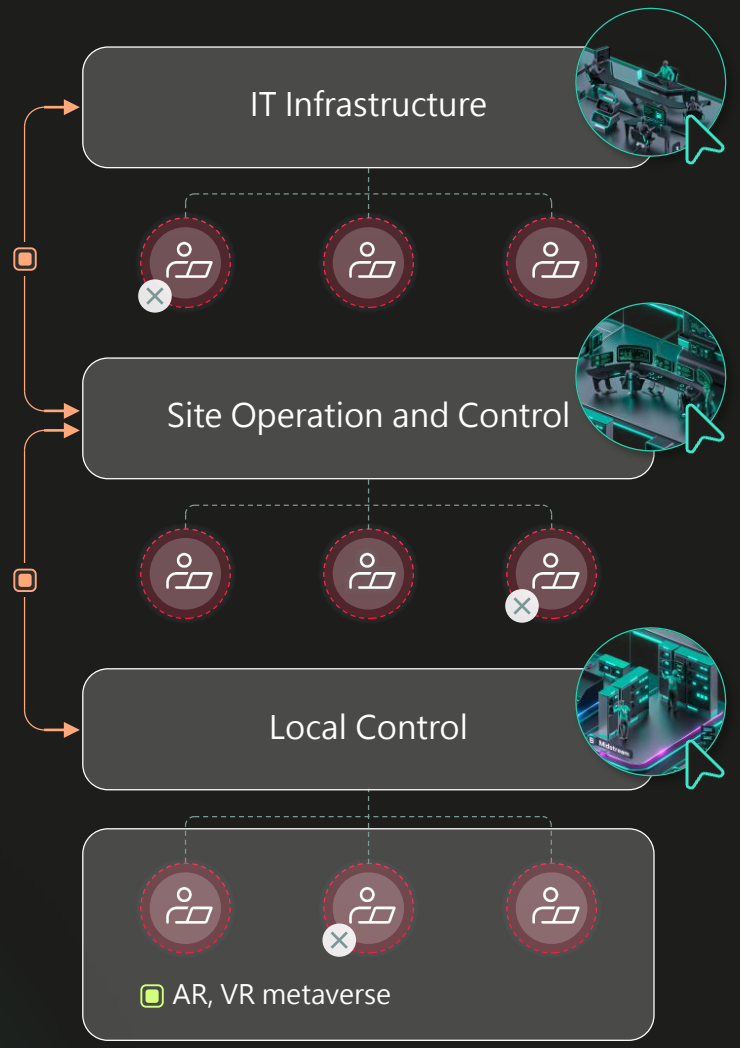
Kaspersky ICS CERT

43%

of workers

surveyed globally in 2020 wanted to leave the energy sector in the next five years

Spring 2022 outlook



Click to learn more

4.人員失誤

How Kaspersky can help

Kaspersky Industrial CyberSecurity

- 減少負責安全維運人員的工作負載，可提供更快的威脅定位及威脅響應

Kaspersky Extended Detection and Response

- 單一管理平台
- 可統一整合管理 IT 及 OT 不同場景的環境

Ecosystem of supporting services

Kaspersky Security Awareness

- 培訓材料
- 遊戲式互動內容
- 釣魚郵件模擬

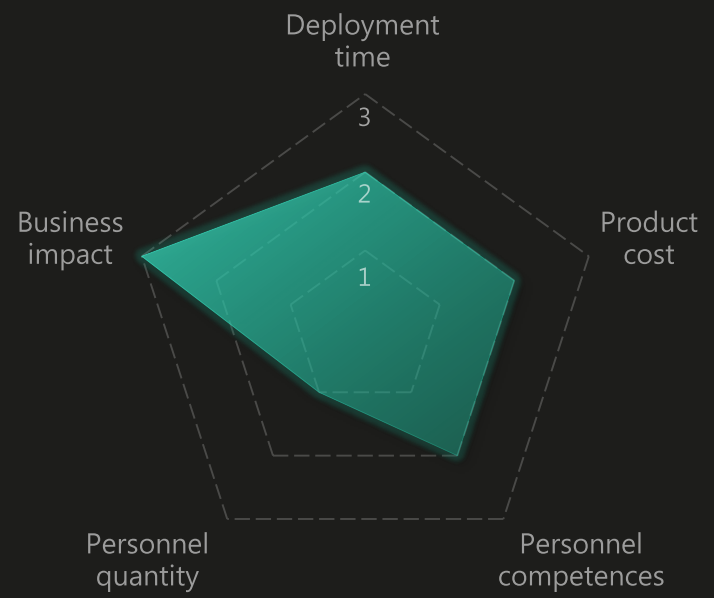
Kaspersky ICS CERT

與 ICS 專家們學習

- Digital forensics and incident response
- Exploring vulnerabilities
- Cross-functional training programs

Click on product to learn more

解決方案特性



5. CIP 合規性

Cybersecurity regulations for the energy, and in particular oil and gas sector, address emerging threats, vulnerabilities and set the industry benchmark for securing OT systems. Countries across the globe imply particular standards and directives which commonly include:

Risk management and assessment | Policies and procedures | Systems security | Incident response and reporting | Workforce training

- ISA / IEC 62433
- ISO / IEC 27001
- ISA99

- NIS2 Directive
- ENISA Guidelines on Cybersecurity for OT and ICS
- EU Cybersecurity Strategy
- EU Cybersecurity Act
- EU Cyber Resilience Act

- NIST CSF
- NIST SP 800-82
- TSA Pipeline Security Directive
- API Standard 1164
- DOE Cybersecurity Capability Maturity Model

- Government Cyber Security Strategy
- NCSC’ s Cyber Assessment Framework

- IT Security Act 2.0
- BSI KritisV
- BSI ICS Security Compendium
- DVGW
- VDMA 66418

- National Cybersecurity Strategy
- ANSSI Cybersecurity Framework for ICS
- Critical Information Infrastructure Protection Law

- The Netherlands Cybersecurity Strategy (NLCS)
- Network and Information Systems Security Act (WBNI)
- NSCS Guide to Cyber Security Measures

- The National Security Framework
- CNPI Royal Decree 704/2011
- CCN-STIC Security Guides

- Swedish Cybersecurity Act
- Swedish Protective Security Act
- MSB Guidance

- National Cybersecurity Strategy
- Romanian Cybersecurity Law No. 362/2018
- National Energy Regulatory Authority Regulations

- National Cybersecurity Strategy and Action Plan
- BTK CIPR
- EPDK Cybersecurity Regulation

- Estratégia Nacional de Cibersegurança
- PNSI Framework
- ANP Regulations

- NCIIPC Guidelines
- Information Technology (IT) Act, 2000

- GB/T 44462.1-2024
- GB/T 22239-2019
- GB/T 32919-2016
- GB/T 25070-2019

- BSSN National Cybersecurity Strategy
- BSSN Regulation No. 4/2021
- Presidential Regulation No. 82/2022

- UAE Information Assurance Standards
- UAE Cybersecurity Council Framework
- UAE IoT Security Standard
- UAE CIIP Policy

- NCA OTCC-1:2022
- NCA ECC-2-2024
- NCA CGIoT-1:2024

Contact us to know more about your regional standards and regulations

How Kaspersky can help

Kaspersky provides services and solutions following policy “defense in depth” which is recommended by industrial security solution providers as well as regulatory bodies in different countries

Kaspersky Industrial CyberSecurity

The products are designed to make oil and gas companies compliant with IEC 62443, NIS2, NERC CIP, SOC 2 Type2, ISO / IEC 27001

通過相容性測試:

Schneider Electric
YOKOGAWA
B&R
SIEMENS
Honeywell
EMERSON
Baker Hughes

>130 systems from 50+ vendors

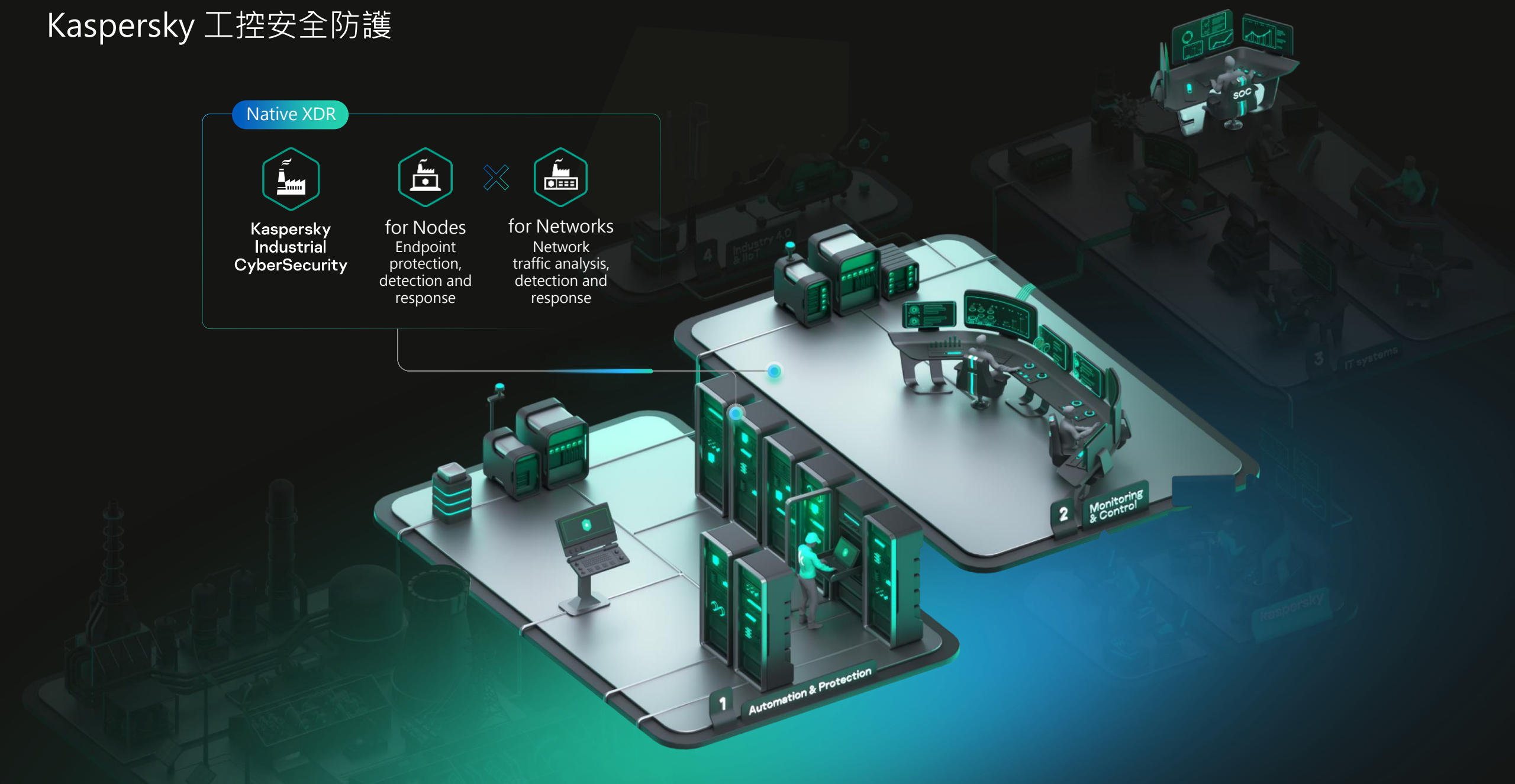
Click to learn more

Kaspersky Security Awareness and Expert Trainings

Solution designed to empower employees with essential cybersafety skills thereby complying with the requirements of the NIS 2 Directive

Read more about NIS 2 Directive and our products compliance

Kaspersky 工控安全防護



Kaspersky Industrial CyberSecurity

XDR

- 工控端點防護偵測及響應
- OT 網路異常及入侵偵測
- 集中化資產盤點、風險及安全合規性稽核

針對關鍵基礎設施
專用的安全防護平台

關鍵功能

- Asset inventory & management, compliance audit and risk management
- Deep packet inspection and machine-learning for anomaly detection
- PLC integrity checker and risk-oriented vulnerability detection
- Industrial-grade network and host-based intrusion detection
- Kaspersky ICS CERT intelligence and vulnerabilities database
- Non-invasive, effective ICS protection with light footprint
- Open API, and integration to Kaspersky Single Management Platform

工控專家市場的認可及評測

FROST & SULLIVAN

VDC Resear

industrial internet CONSORTIUM

稽核及合規性

IEC 62443-4-1

AICPA SOC SOC 2 Type 2

TÜV AUSTRIA CERTIFIED ISO/IEC 27001

相容性

OEM agreements and certifications with:

Schneider Electric · YOKOGAWA · B&R · GE · SIEMENS · Honeywell · EMERSON · Baker Hughes

Over 130 certified systems from 50+ vendors

如何更好的保護好OT生產系統?

- **資產盤點和風險管理**
  - 先了解現況及可能的風險
- **系統/網路加固及有效的管控**
  - 可視性/管控覆蓋性/零信任
- **安全監控/定期稽核**
  - 集中化/自動化處理
  - 異常處理流程設計
- **人員安全意識培養**
  - 員工教育訓練
  - 異常處理演練/事件響應演練

如何更好的保護好OT生產系統？工具/流程/人員

- **資產盤點和風險管理**
  - OT 基礎設備清單和漏洞檢測
  - 網路威脅檢測
  - 以風險為導向的風險檢測和報告
- **網路威脅檢測與響應**
  - 網路流量分析及端點探針，用來偵測入侵流量（工控DPI 和 IDS）
- **端點安全分析、威脅防護、檢測和響應**
  - 反惡意程式、應用程序白名單、設備控制等
  - 端點事件根本原因分析及響應

kaspersky

Kaspersky Industrial CyberSecurity for Networks

網路流量分析 及 異常偵測及響應

KICS for Networks 針對 OT 環境整合的**關鍵功能**

網路流量分析

- **深層式封包分析技術可深入分析各種工控相關特殊通訊協定**
  - 遙測資料、指令及參數/數值的控制
- 網路可視性
  - 提供流量傳輸的流程及設備間溝通的架構圖
  - 協助提供工控網路設備間溝通的技術拓撲圖
  - 網路可視性及連線過程的記錄

網路入侵及網路異常的偵測機制

- 利用由 卡巴斯基 ICS-CERT專家所收集的各種 IDSI 規則，提供給使者的相關証據。
- **網路完整性監控**
  可偵測未知或新的設供
- 透過內建基於用戶端提供的歷史數據，可偵測到異常流量的發生

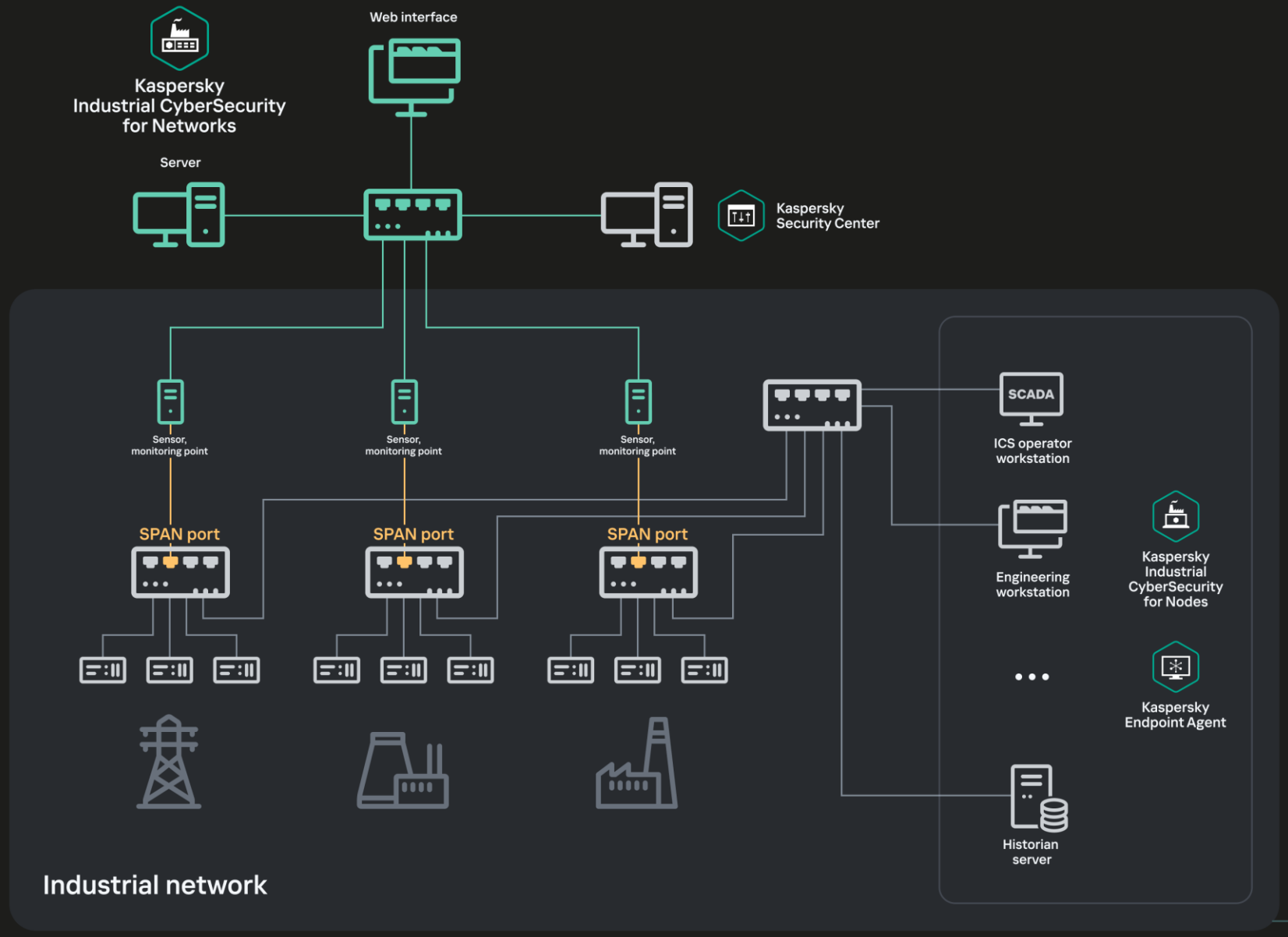
資產盤點、漏洞偵測及風險評估

- 集中化被動式收集資產資訊及可透過主動式輪詢方式收集
- **風險評估偵測**及可提供延申性的報告
- 可自動更新的各種專家模組及內容
  - **OT 資產類型**
  - 針對 ICS CERT 相關的弱點資料庫
  - **偵測 PLC** 設定完整性控制
  - 滿足各種安全合規性

整合性

- **支援階層式及分散式部署架構**
- 可整合卡巴斯基 XDR安全平台
- 也支援建立 OT 安全平台生態鏈，可透過下列方式整合介接：CEF, OPC, 104, Syslog, API

KICS for Networks 導入架構

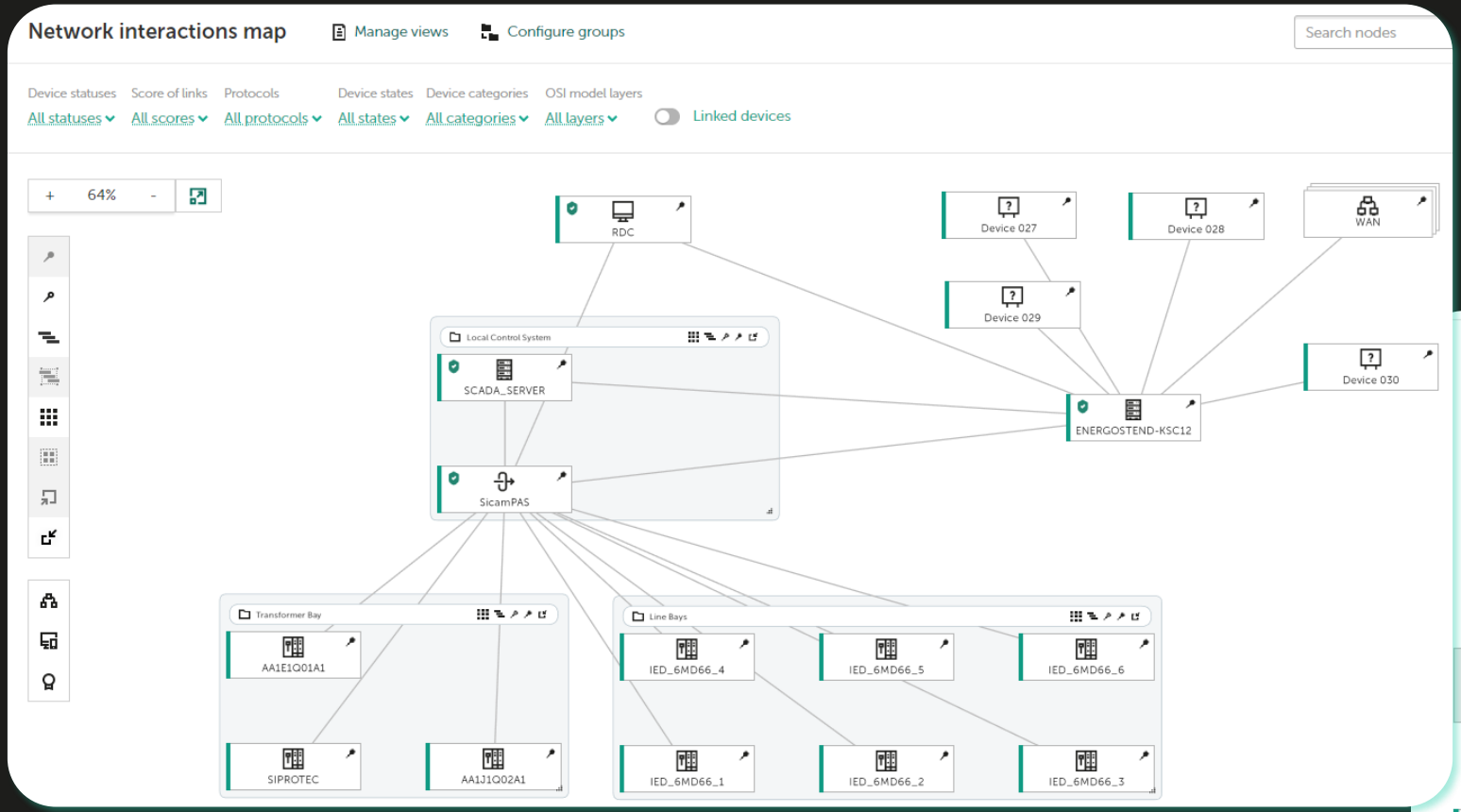


KICS for Networks

透過接入工業網路交換機鏡像流量進行旁接監測

- **資產盤點**– OT 設備辨識及資產盤點
- **風險評估及漏洞偵測** –工控設備上的軟體或裝置漏洞偵測
- **工控網路異常及入侵偵測** –工控網路威脅入侵偵測
- **網路完整性監控** – 對未授權的網路設備及網路流量進行監控
- **網路設備可視性**– 資料可視化顯示功能
- **DPI, Deep Packet Inspection** –工控協議深度分析
- **Command Control** – 工控協議指令監測審記

KICS for Networks. 網路可視性

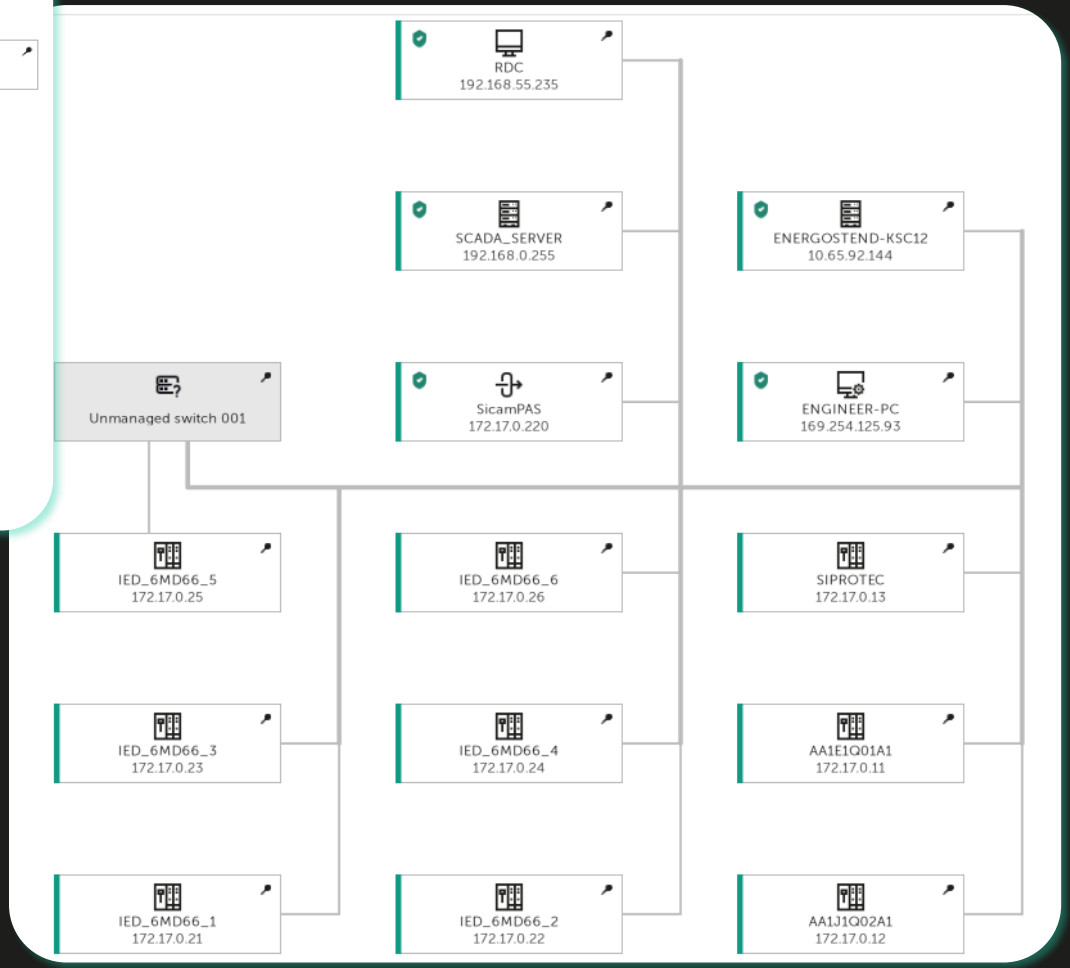


網路拓撲圖

- 實體網路連接圖示
- 可設定交換機的連接埠與設備間的關係
- 可依主動輪詢的結果產生
- 設備安全狀態可直接顯示在相關圖示中

網路通訊協定關聯圖

- 設備間連線關聯圖
- 使用的通訊協定及流量記錄
- 可支援分群、搜尋及過濾的應用
- 可依時間軸的變化市追蹤狀態



KICS for Networks. OT 漏洞、風險評估

安全事件 | 怎麼發生?

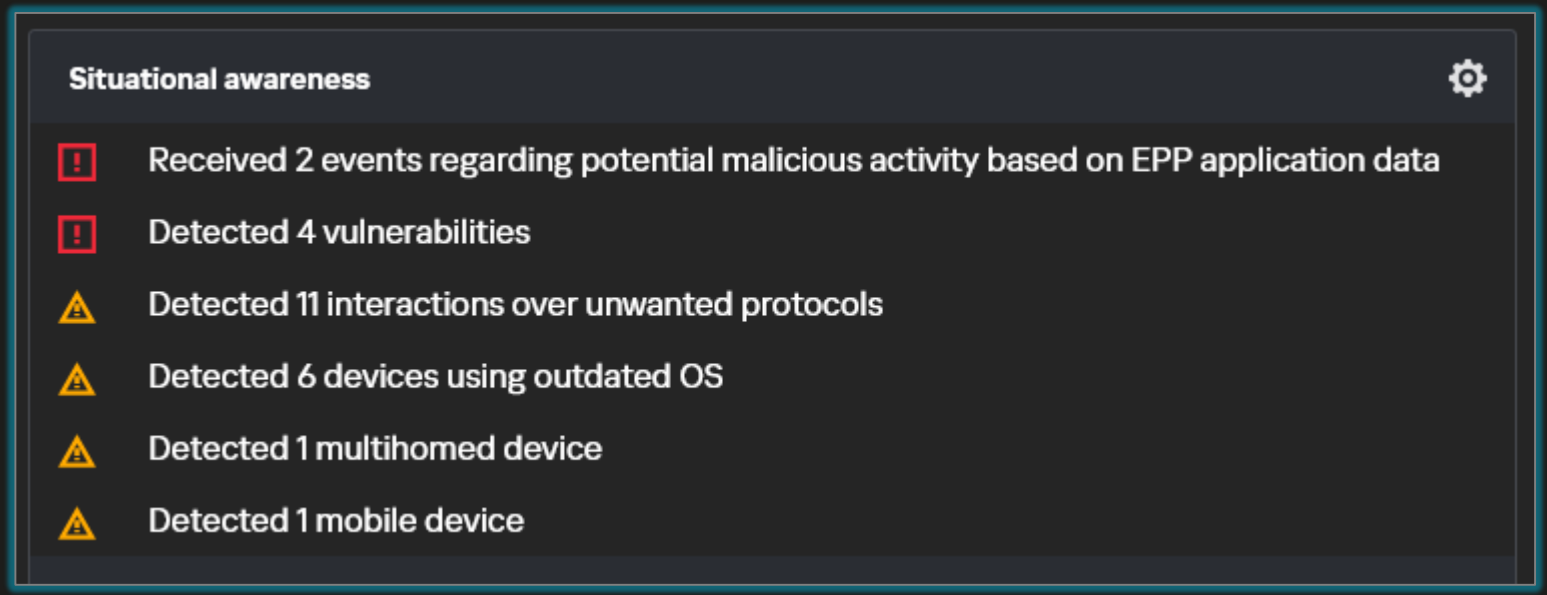
提供風險評分方便辨識優先級

可基於資產重要性、網路連線方式及漏洞的動態評分

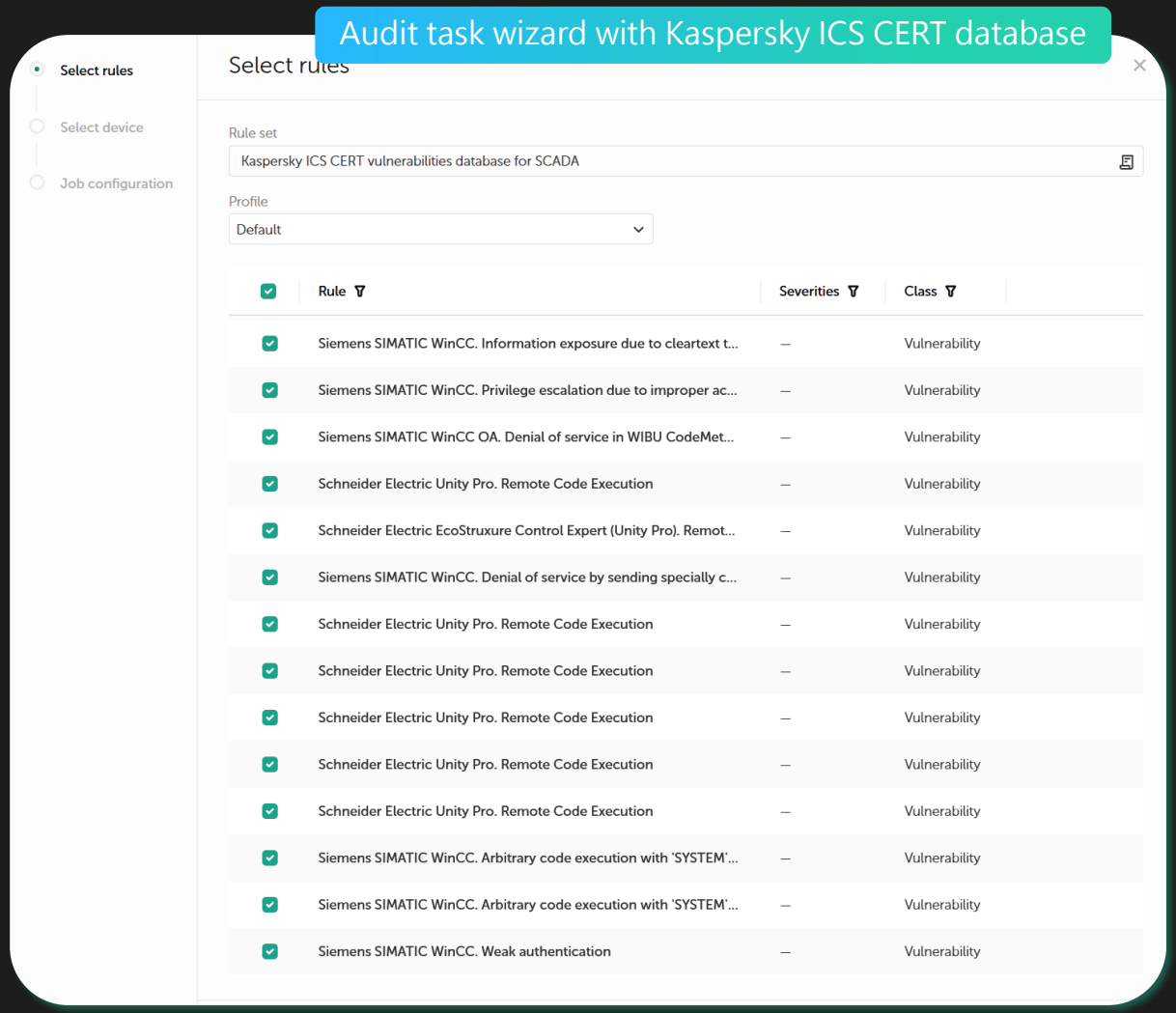
可自訂的基本風險評分

風險 | 為什麼會發生?

- 網路端的漏洞
- 端點不安全的設定
- 系統過舊、漏洞未修補、不安全的存取及異常的網路通訊
- 過舊的作業系統、未經授權的連接裝置
- 具有漏洞的工控設備



KICS for Networks. 安全稽核及檢視規則



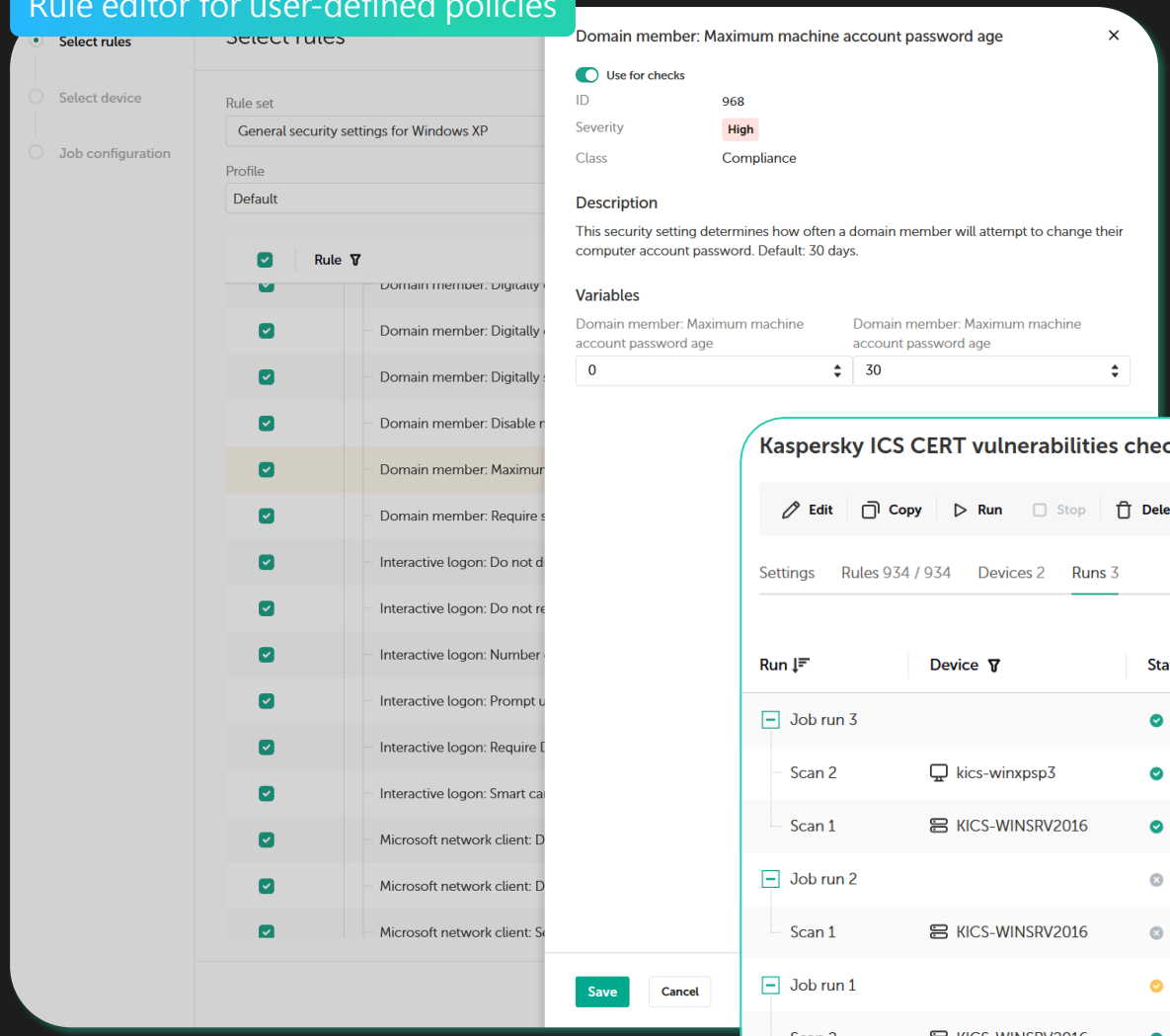
提供可以立即使用的安全稽核規則

- **Kaspersky ICS CERT vulnerabilities database for SCADA**
- General security settings for Windows XP/7/8.1/10/11
- General security settings for Window Server 2012/2012 R2/2016/2019/2022
- General security settings for Debian
- General security settings for Red Hat Enterprise Linux, CentOS, Oracle Linux
- General security settings for Ubuntu
- General security settings for SUSE Linux Enterprise, openSUSE
- Security Level -1 for Cisco routers and switches
- Security Level -2 for Cisco routers and switches
- General security settings for FortiGate

規則會隨著產品更新持續更新相關規則*

KICS for Networks.安全稽核及檢視規則

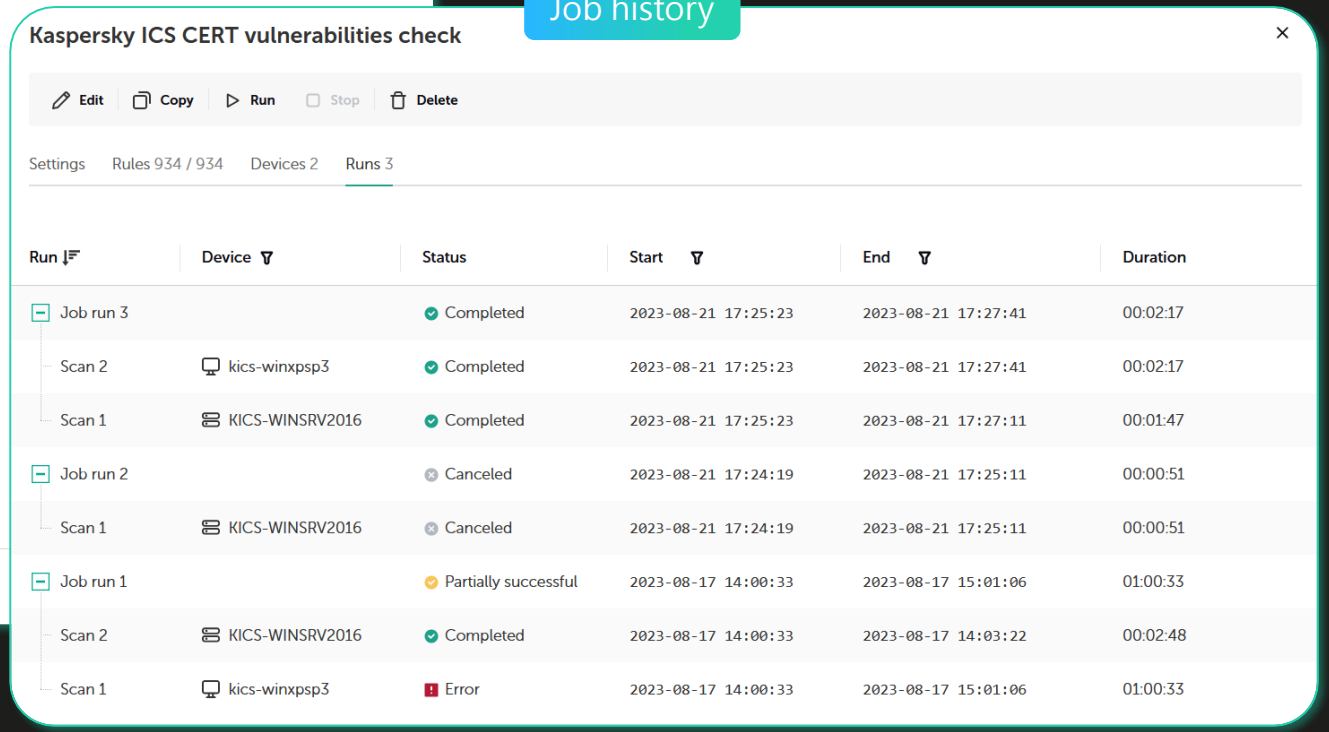
Rule editor for user-defined policies



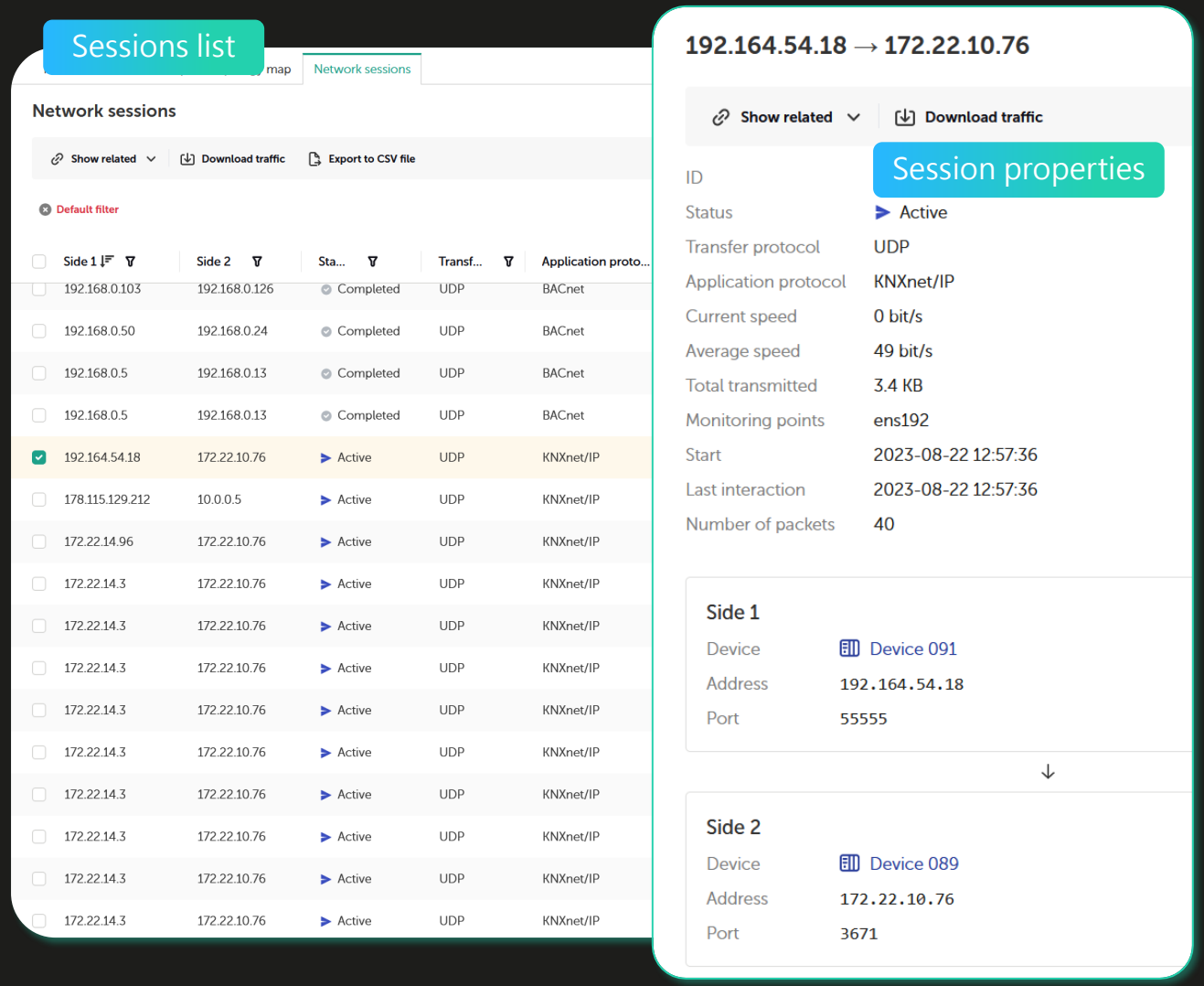
Audit Tasks

- Task manager permits flexible control of task settings, including single or group tasks for scheduled or manual execution with traceable change history
- Compatibility with 3rd party OVAL-based rules makes it possible to use configuration checkups against preferable custom rules

Job history



Network Traffic Analysis: 網路連線資訊



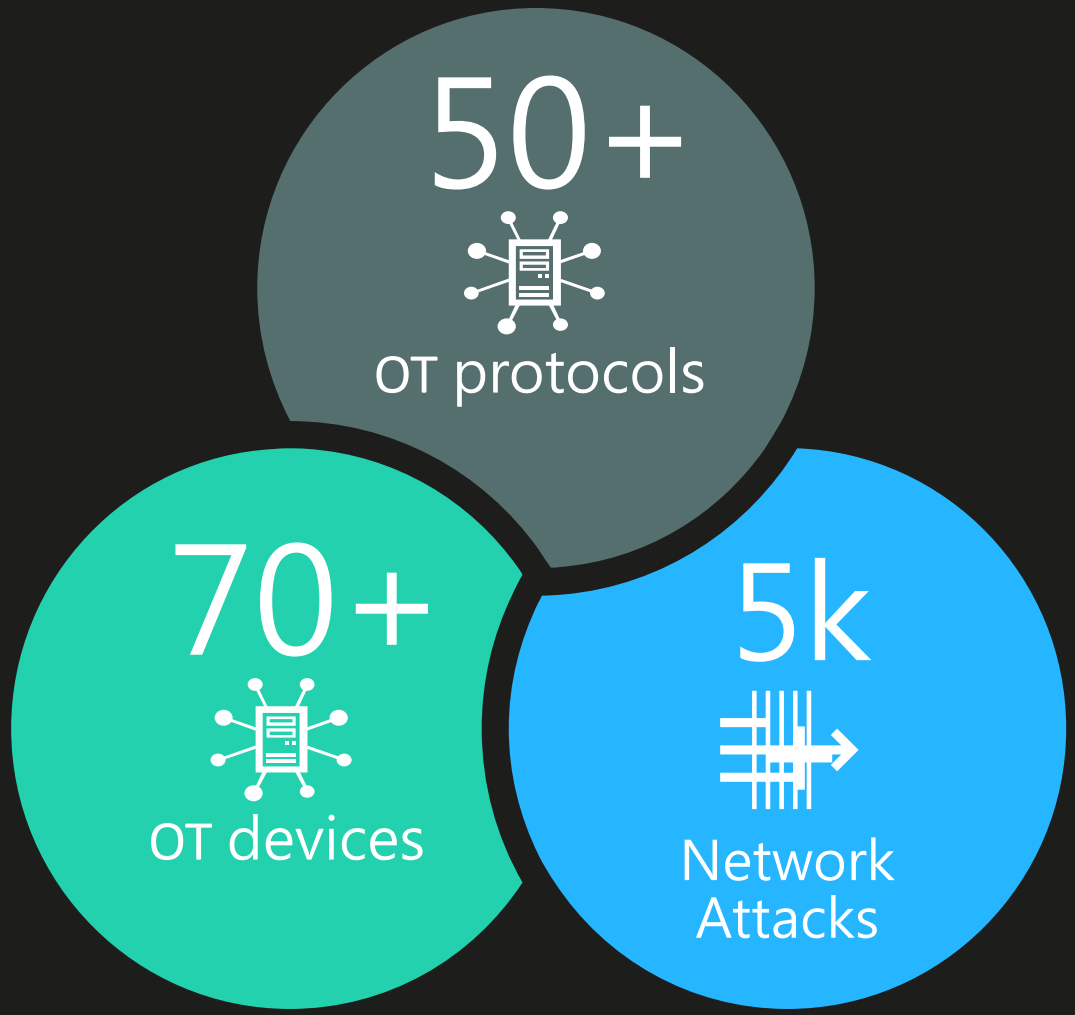
網路連線資訊

- Session status (Active/Completed)
- Communication direction
- Transport and application protocols
- Sessions statistics (speed, bytes)

常用場景

- 觀察特殊進行中的連線行為及使用的特殊網路協定
- 分析連線發生時間
- 下載需要深入調查的連線資訊

KICS for Networks. 支援多種工控設備及協議



- 深度封包檢測技術，包含 OT及IT 相關協定
- 更新DPI不需要重新安裝產品及升級
- 可自動化偵測及建立相關流量監控規則
- 支援匯入SCADA及參數關聯資訊與特定工控設備整合
- 可提供被動式 PLC 完整性監控

KICS for Networks.支援多種工控設備及協議

支援解析的工控協議

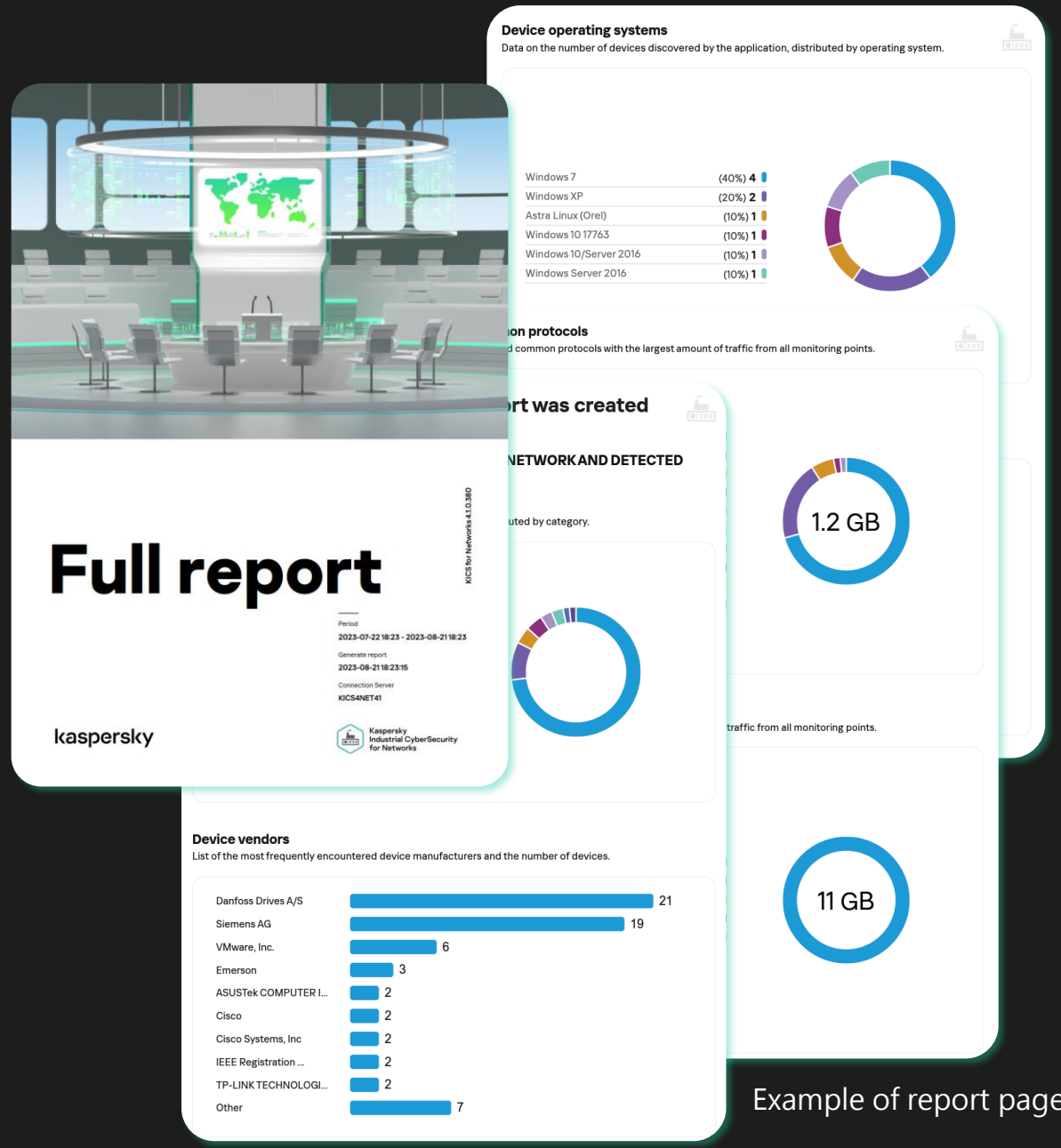
- ABB DMS
- ABB SPA-Bus
- Bacnet
- Beckhoff
- CODESYS V3 Gateway
- Digsi4
- DNP3
- Ekra243 system protocol
- Emerson ControlWave Designer
- Emerson ControlWave data exchange protocol
- Emerson DeltaV
- EtherNet/IP
- Honeywell ControlEdge
- Honeywell ControlEdge Discovery
- Honeywell Experion EpicMo
- Honeywell Experion CdaComm
- Honeywell Experion NameServer
- Honeywell Experion Discovery
- FTP
- Foxboro HPS
- GE SRTP
- GOOSE
- IEC 60870-5-101
- IEC 60870-5-104
- Mitsubishi MELSEC System Q
- MMS
- Modbus TCP
- Moxa NPort Ia5000a system protocol
- Micom C264
- Omron FINS
- OPC DA (DCE/RPC)
- OPC UA Binary
- ProsoftSystems DeviceDiscoveryProtocol
- Profinet IO
- Profinet RPC
- DirectLogic Ecom
- Relematika BDUBus
- S7Comm over Industrial Ethernet
- S7Comm over TCP
- S7Comm Plus
- Sampled Values
- Schneider UMAS
- TASE2 (ICCP/IEC 60870-6)
- Yokogawa Vnet/IP
- Feu
- Yard
- Cos
- Valmet

支援識別的工控設備

- Mitsubishi System Q E71
- Micom C264
- Micom P545
- Moxa NPort Ia5000a
- Omron CJ2M
- ProsoftSystems Regul R500
- Relematika TOR 300
- Schneider Electric MiCOM P545
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Schneider Electric Modicon Momentum
- Schneider Electric SEPAM S81 NPP
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIMATIC S7-200
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIPROTEC 4 7SA52
- Siemens SIPROTEC 4 7SJ64
- Siemens SIPROTEC 4 7SS52
- Siemens SIPROTEC 4 7UM62
- Siemens SIPROTEC 4 7UT63
- Siemens SIPROTEC 5 7SJ86
- Siemens SIPROTEC 6MD66
- TASE2 Server
- Yokogawa AFV10, AFV30, AFV40
- Yokogawa Centum VP
- Yokogawa PROSAFE-RS
- Ipu950
- YCL/ECL
- Valmet
- ABB AC 700F
- ABB AC 800M
- ABB RED 670, REL 670, RET 670, REF 615
- ABB RTU 560
- Allen-Bradley CompactLogix Series
- Allen-Bradley ControlLogix Series
- BACNet device
- Beckhoff Cx
- Devices with CODESYS V3
- Devices with DNP3
- Devices with IEC 60870-5-101
- Devices with IEC 60870-5-104
- Devices with IEC 61850-8-1: GOOSE, MMS
- Devices with IEC 61850-9-2: Sampled Values
- EKRA 200 Series
- EKRA BE2502
- EKRA BE2704
- Emerson ControlWave Micro 33
- Emerson DeltaV MD, MD Plus, MQ
- Honeywell ControlEdge 900
- Honeywell Experion C300
- Foxboro FCP 200 Series
- General Electric MULTILIN B30
- General Electric MULTILIN C60
- General Electric RX3i

KICS for Networks. 內建自動化報告

- OT network inventory
- Network baseline
- Risk summary
- Adjustable time period
- Scheduling and e-mail delivery

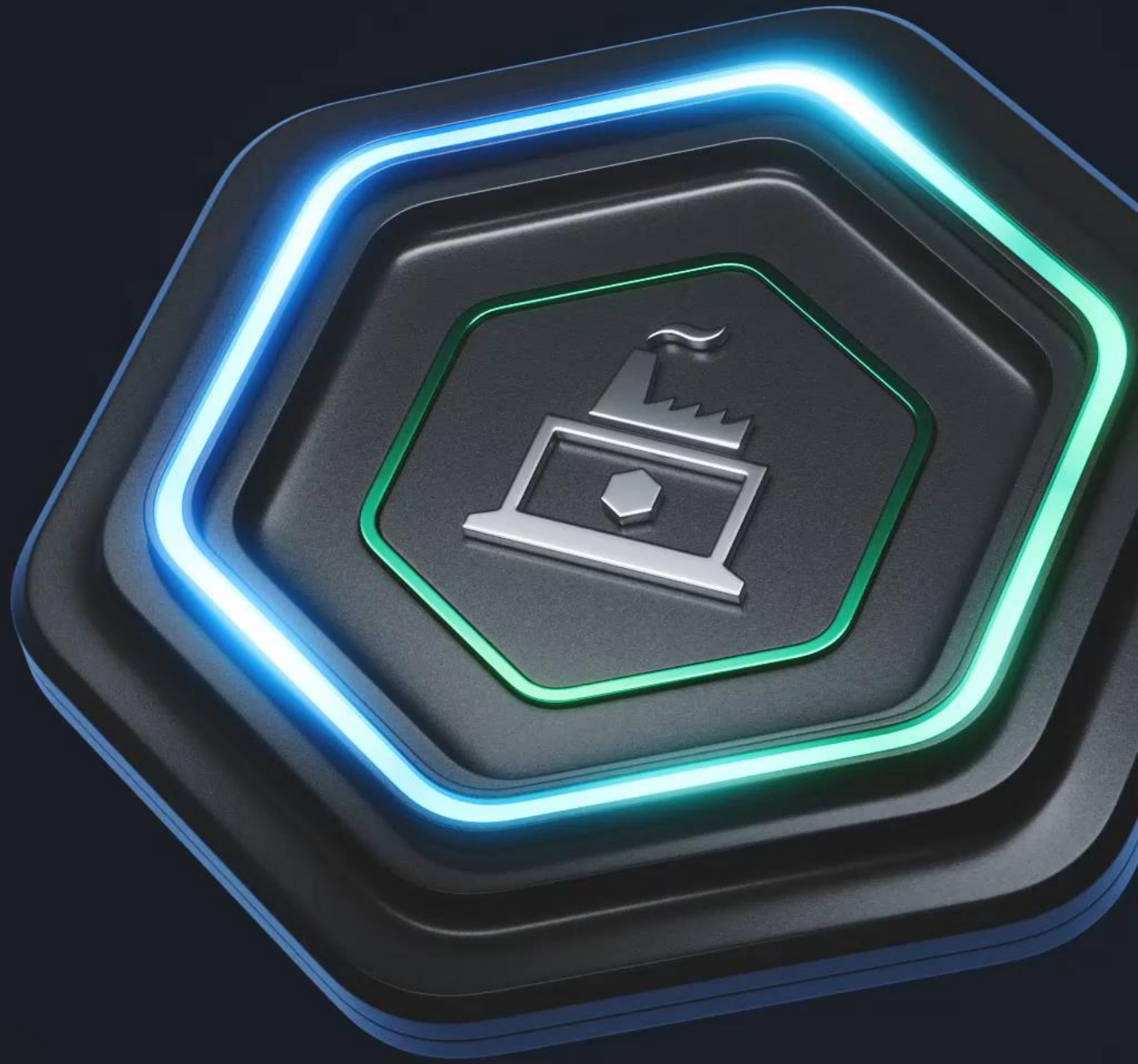


Example of report pages

kaspersky

Kaspersky Industrial CyberSecurity for Nodes

端點防護 偵測及響應



KICS for Nodes. 功能選項

Windows

Portable Scanner

Linux

Audit Agent

Gateway

Engineering workstation

Historian Server

System management workstation

SCADA server

Embedded systems

Operation workstation

主要特色

Kaspersky Industrial CyberSecurity for Nodes

- 通過工控自動化控制廠商相容性測試*
- 提供 Windows XP/Server 2003 的防護
- 支援 非阻擋模式 (statistic mode)
- 安裝/更新/升級 無需重新啟動
- 支援隔離網路環境更新場景
- 針對 OT 設計的功能及設定
- 功能模組化架構 – 可自行選擇要使用的元件

* Learn more: certification

KICS for Nodes. 安全元件

Windows Nodes Linux Nodes

Industrial Endpoint Protection

防護
- 惡意程式防護 Linux
- 漏洞利用防護（內存進程）windows
- 網路威脅防護 Linux
- 反加密 Linux

管控
- 應用程式白名單 Linux
- 外接設備控制 Linux
- Wi-Fi 管控（windows）
- 本機防火牆管理

審查
- Windows Log 異常監控
- 檔案完整性監控 Linux
- PLC 完整性監控

溯源
- EDR Agent
- 端點傳感器(與KICS for Network 整合) Linux

KICS for Nodes. 客戶效益

效益

管控 全面降低行為安全風險

防護 強化安全防護能力

審查 了解業務

安全風險及弱點

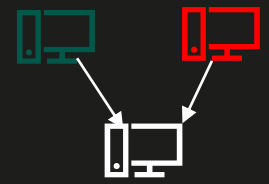
濫用

隨意安裝與生產不相關應用程序

USB 設備隨意使用

對工業主機的存取缺乏控制

生產部門 非生產部門



脆弱

主機系統老舊
很少升級
漏洞多

缺少對惡意程式防護能力

缺少對網路威脅防護能力

缺少對勒索軟體防護能力

未知

端點事件根本原因分析和響應

系統關鍵安全事件缺乏記錄

工控系統檔案變更缺乏記錄

PLC程序變更缺乏記錄

處理方式

- 應用程式白名單 ★
- 外接設備管控
- 防火牆
- 檔案即時防護 ★
- 網路威脅防護 ★
- 漏洞利用防護 ★
- 反勒索加密 ★
- EDR Agent
- Windows事件記錄
- 檔案完整性監控 ★
- PLC程序監控

★卡巴斯基優勢功能

ICS 廠商相容性測試


Honeywell
ROSATOM
PROSOFT SYSTEMS
EKRA
Valmet FORWARD
Système electric
kaspersky
EMERSON
BOSCH
PcVue Solutions
SIEMENS
MITSUBISHI ELECTRIC
B&R
RTSoft
YOKOGAWA

Worldwide clients

滿足合規性要求

IEC-62443 3-3 requirements covered by KICS and organizational measures (all requirements and all security levels)

- FR1
- FR2
- FR3
- FR4
- FR5
- FR6
- FR7

符合安全認証 Level 3 to 62443 4-1

KICS is the world's first industry standard certified XDR platform.

Confidence in the security of the solution	Best programming practices
Vulnerability risk minimized	Comprehensive testing and documentation

KICS for Networks was the first in the world in its category to reach the ML-3 trust level

https://www.kaspersky.com/enterprise-security/industrial-cybersecurity/certification

卡巴斯基工控安全解決方案可解決OT最關心的問題

痛點

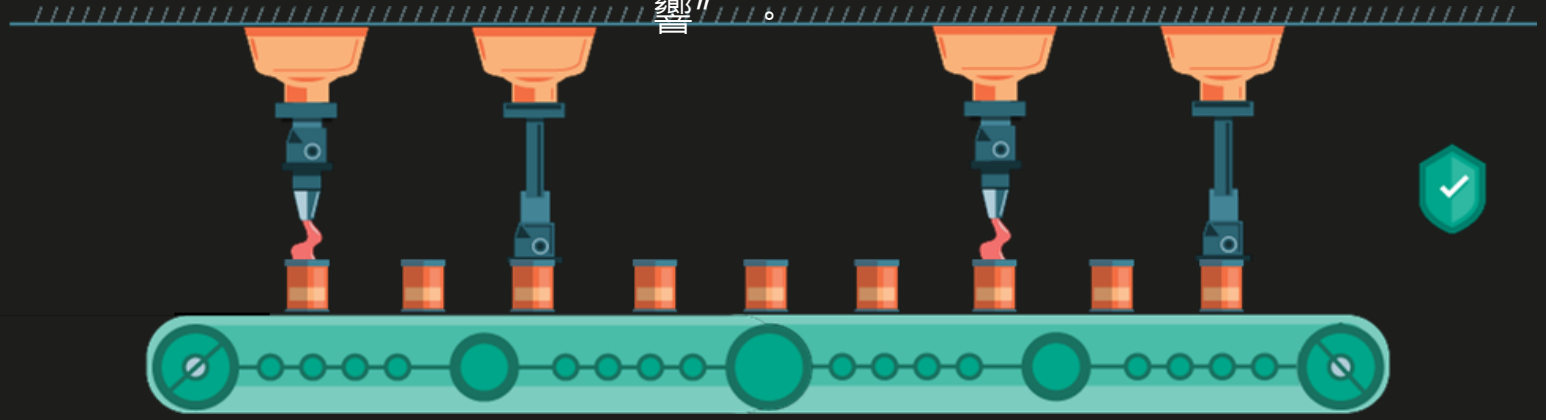
安全威脅與
日俱增

IT安全產品
不適用

安全建議
極待推進

卡巴斯基工控安全防護 – 不影響系統性能，不影響生產過程。

1. KICS4Nodes安裝部署無需重啟或停止生產系統的運行。
2. KICS4Nodes佔用系統資源級小，不影響生產系統運行。
3. KICS4Nodes 專為工業生產環境設計，兼容多種工業應用及通過多種工控廠商兼容性檢測報告。
4. KICS4Networks 採用旁路監測方式對生產系統運行”零影響”。



kaspersky

Learn more about KICS

https://www.youtube.com/playlist?list=PL6BzPT9XO1o4ERqB_cwRe7fhxbIJIecP9