CYBERSEC 2022 臺灣資安大會

NOW CHANGE

數位轉型　資安升級

SEP. 20-22 臺北南港展覽二館

工業技術研究院
Industrial Technology Research Institute

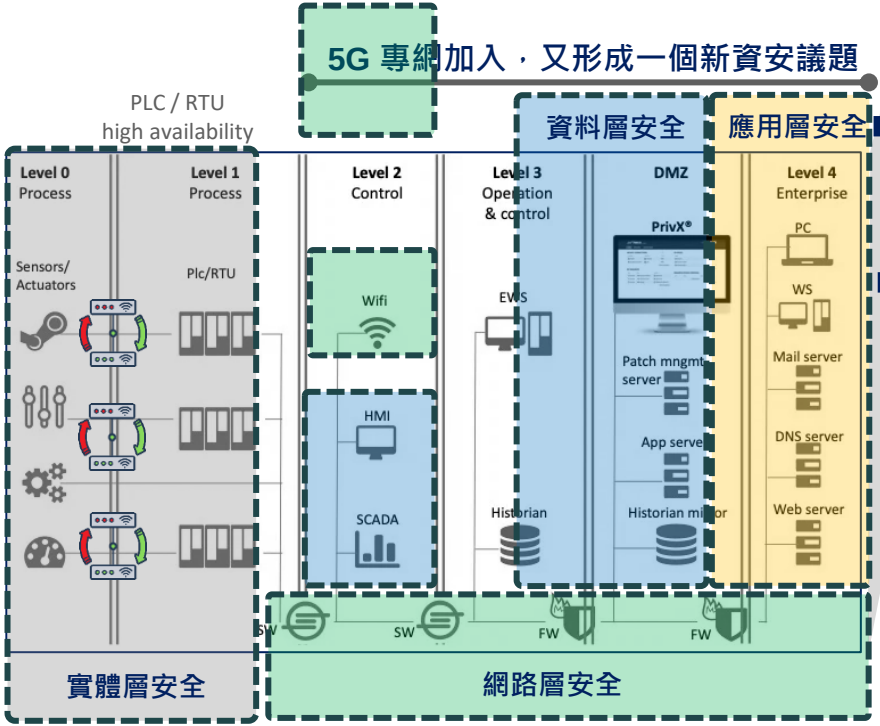
零信任下的智慧工廠資安技術與應用

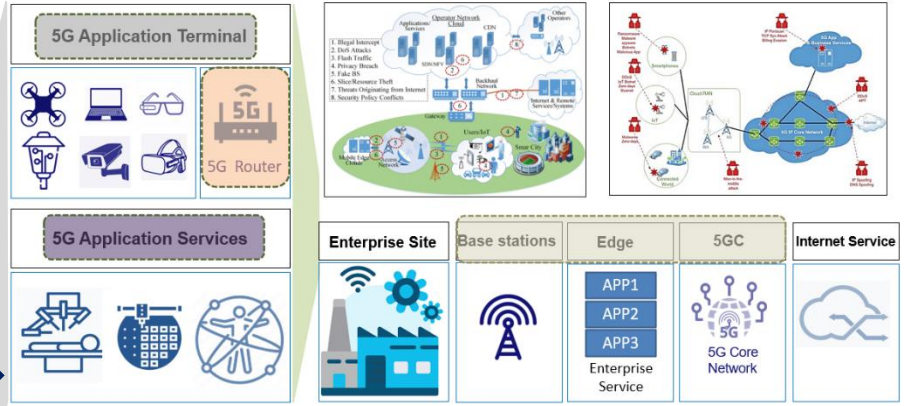
工研院 資通所
副所長 黃維中 & 經理 陳伯榆

2022/9/21

1、解構智慧工廠與資安威脅 (1/2)

對環境干擾最小，不影響營運效能或干擾以致中斷，在智慧工廠資安防護重中之重





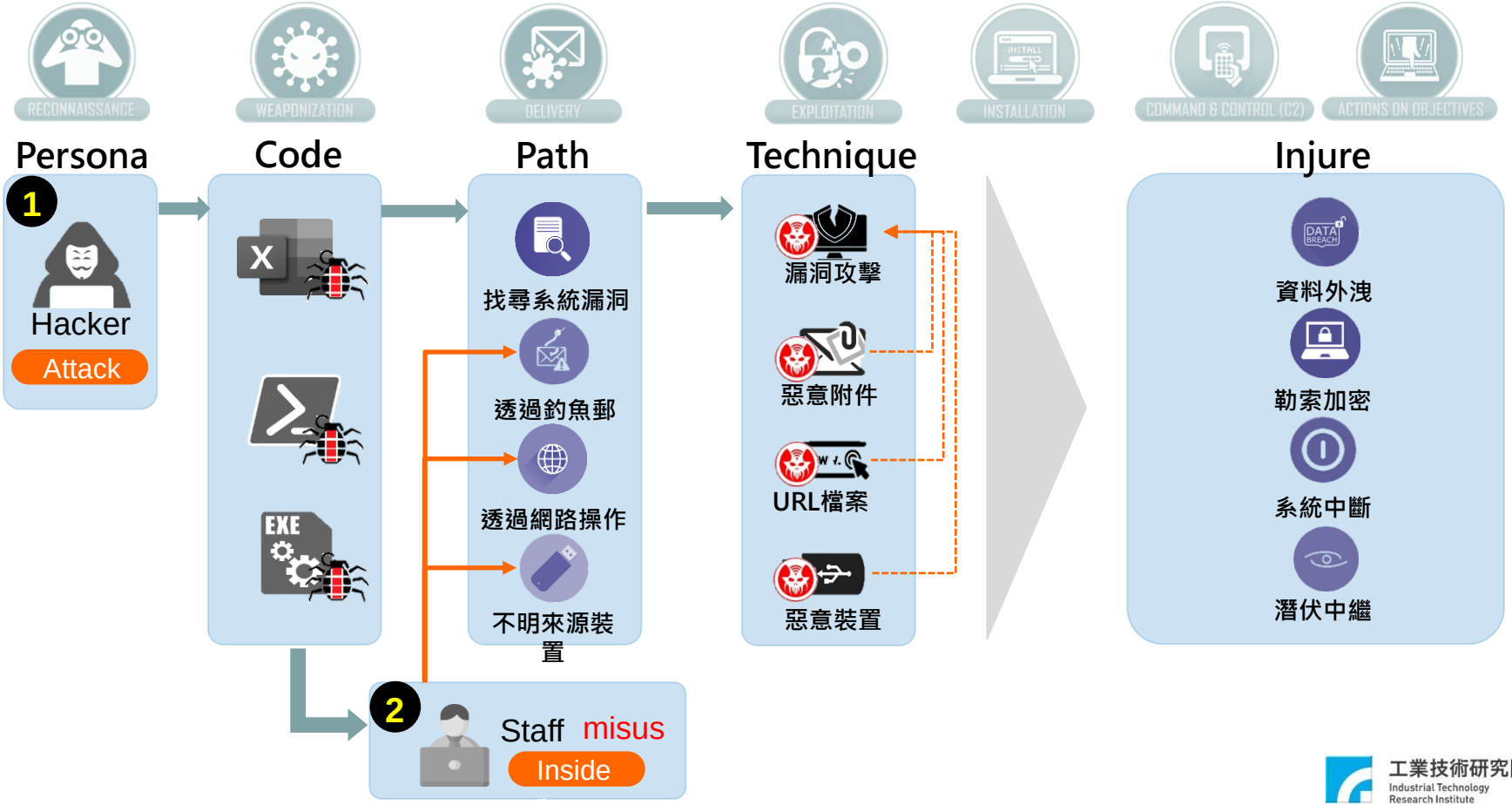
從駭客思維下攻擊想定：

- 惡意軟體或是惡意程式碼
- 利用智慧工廠網路設計與配置的缺陷
- 阻斷服務
- 應用層信息外洩
- 利用遠程存取
- 軟體或硬體漏洞
- 攻擊身份驗證機制
- 資料外洩、盜竊(入侵系統後)
- 未經授權存取操作
- 駭客利用供應鏈、供應商和服務提供商
- 竊聽/攔截/劫持
- 駭客勒索加密攻擊(內部威脅)
- 操作上意外損壞（意外）
- 社交工程與釣魚
- Web Based 系統攻擊
- API攻擊
- 雲端服務系統脆弱點
- 資安機制導致營運中斷或系統故障
- 實體層攻擊
- 攻擊 AI 演算法

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

常見駭客入侵攻擊 (2/2)

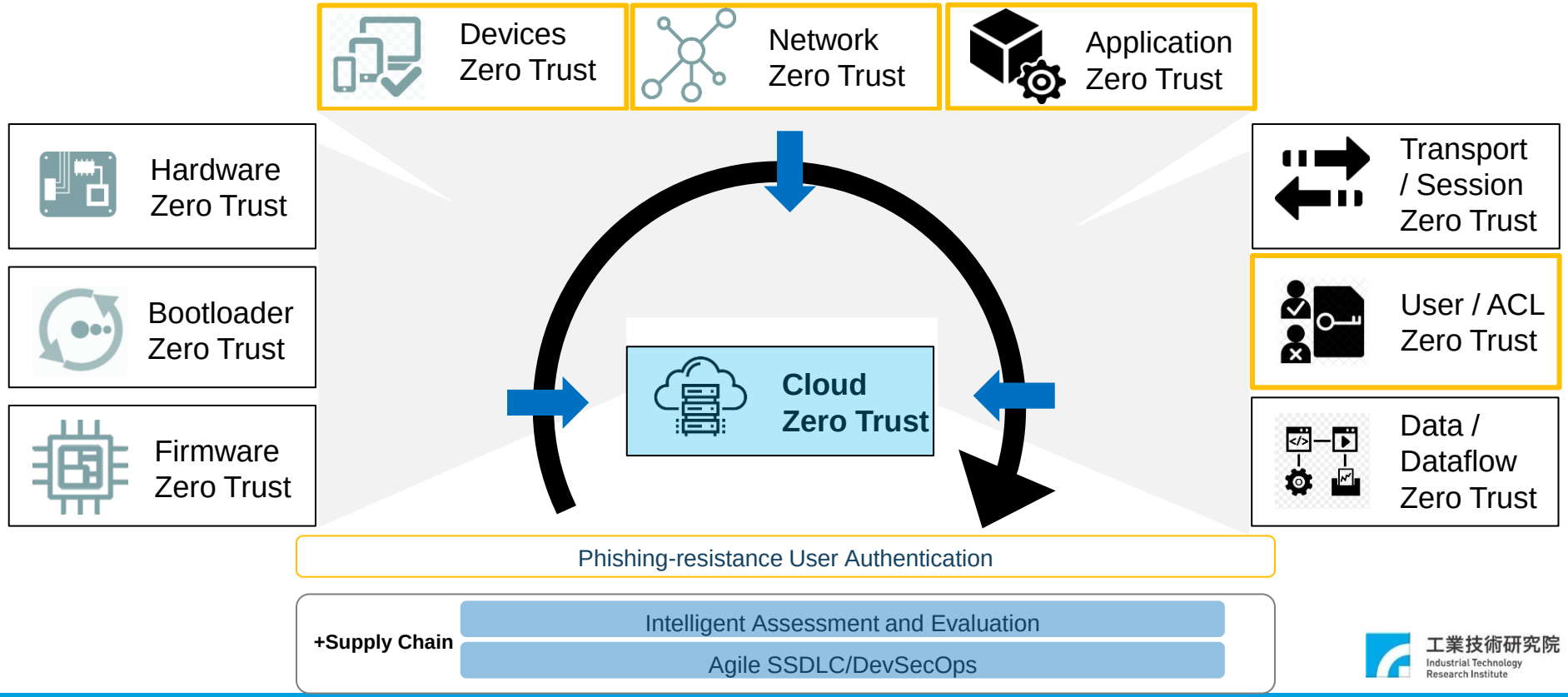


工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

2、對策：從多層次零信任出發

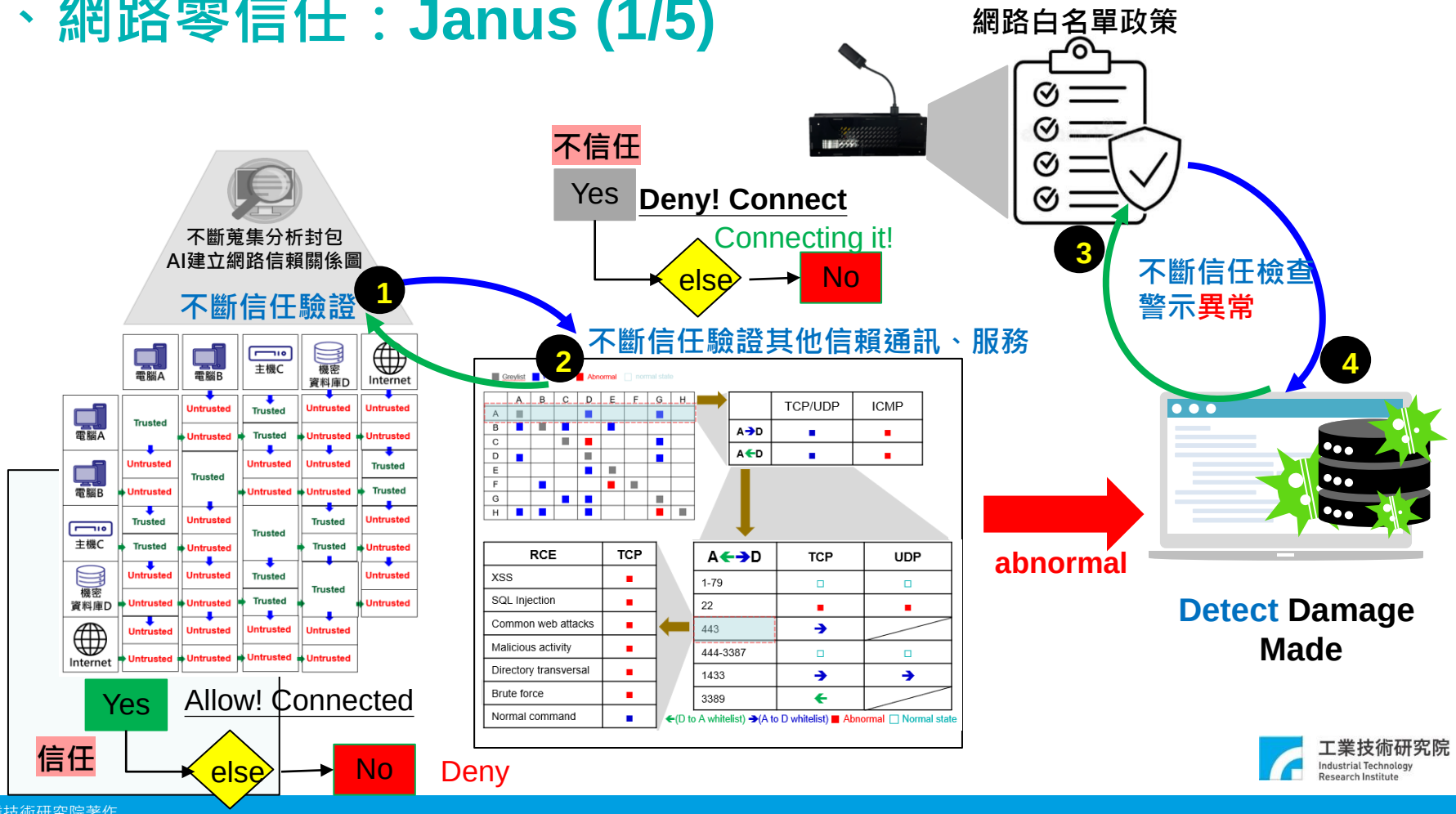
零信任是一種基於「從不信任，始終驗證」的前提的緩解措施，意味著所有用戶必須經過身份驗證、授權並持續驗證安全配置，然後才能被授予或保持對應用程式和資料的存取權限



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

3、網路零信任：Janus (1/5)



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

Janus適用的場域與特殊性考量 (2/5)

- 適用在架構變異性小，且具高度機敏性環境 例如：智慧工廠、IoT場域、封閉型網路系統。
- 外部保護防禦方法在未來威脅環境並不真正有效。
- 可以有效抑制駭客突破疆界後，阻斷橫向穿透入侵。
- 可以解決舊系統無法立即更新的風險危害。
- 不適用在高變動性系統環境前緣防護，例如：內容結構高變動網站系統。

Reduce abnormality

降低減緩升級後異常事件

lack of mastery

解決掌握度不足的修補升級風險

End of life cycle

產品生命週期結束無法修補

Stability

升級更新，維持業務運作穩定性

Buffer time

爭取到緩衝時間

Overly frequent

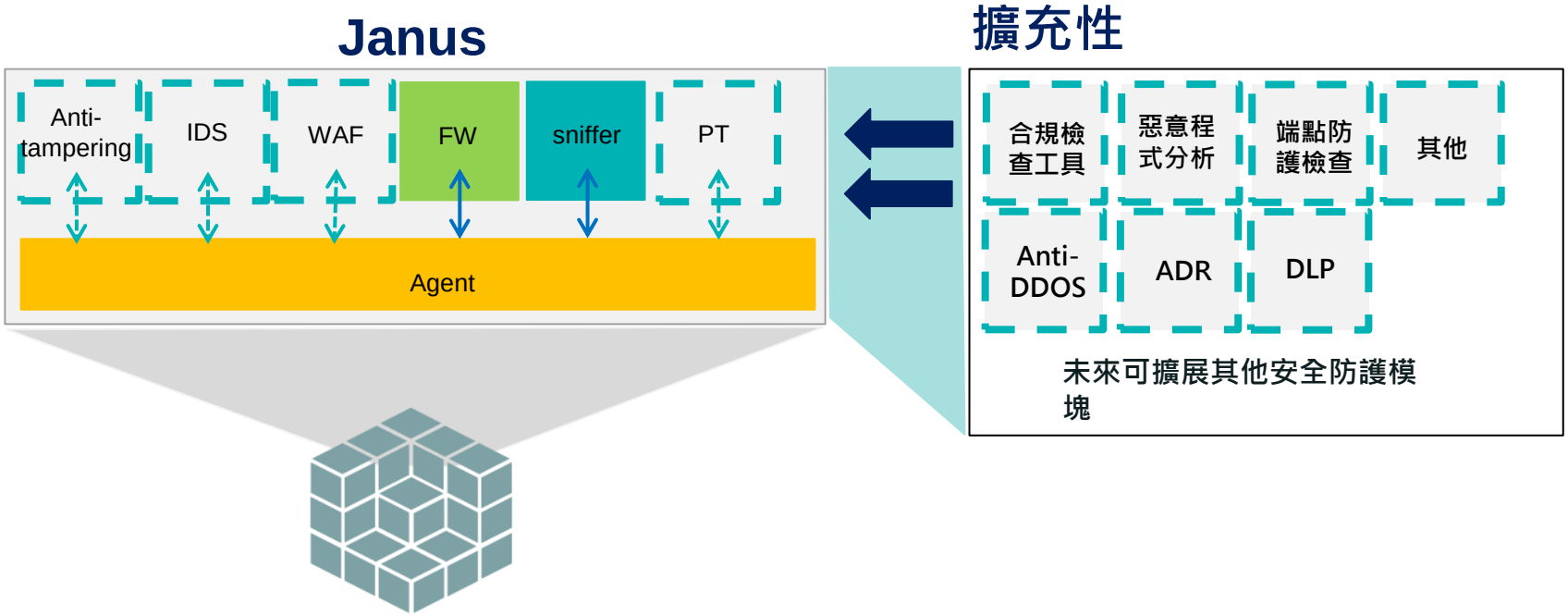
修補過度頻繁的營運干擾

解決升級修補Patch Management遇到痛點

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

Janus 防禦倉儲模塊擴充設計，解決未來需求 (3/5)



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

Janus應用架構圖 (4/5)

Management Center

Hosting in Cloud

Hosting on Local

Janus

Defensive target

HealthCare Device

Industrial & IoT Device

VM & Container

PC & Laptop

network segment Devices

Server Farm

工業技術研究院
Industrial Technology Research Institute

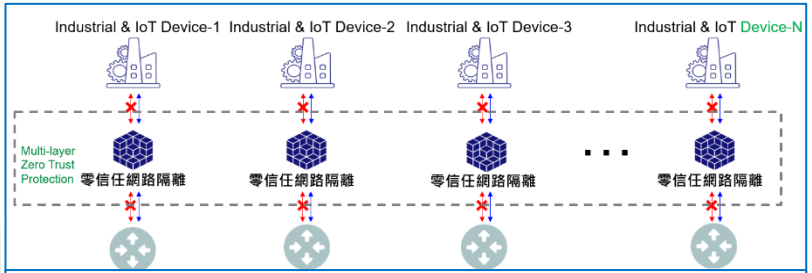
©ITRI. 工業技術研究院著作

Janus應用架構漏與解決EOS痛點與零信任需要 (5/5)

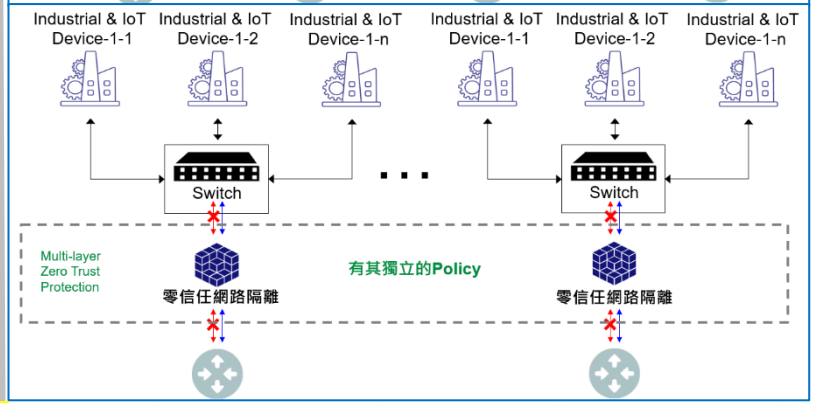
產品生命週期結束無法修補

採用網路零信任機制

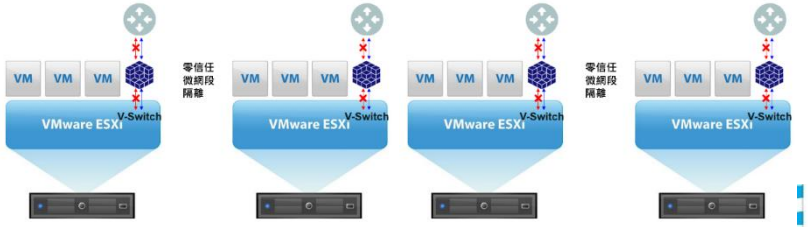
(IoT獨立設備防護架構下)



(IoT 隔離網段防護架構下)



隔離虛擬網段防護架構下)



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

4、駭客利用OS白名單工具迴避資安檢查 (1/3)

LOLBAS

☆ Star 4,403

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

Search among 160 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At (Windows)
Atbroker.exe	Execute	Binaries	T1218: Signed Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	T1202: Indirect Command Execution
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries	T1564.004: NTFS File Attributes T1105: Ingress Tool Transfer T1218: Signed Binary Proxy Execution
CertOC.exe	Execute Download	Binaries	T1218: Signed Binary Proxy Execution
Cmstp.exe	Execute AWL bypass	Binaries	T1218.003: CMSTP
ConfigSecurityPolicy.exe	Upload	Binaries	T1567: Exfiltration Over Web Service
Conhost.exe	Execute	Binaries	T1202: Indirect Command Execution
Control.exe	Alternate data streams	Binaries	T1218.002: Control Panel
Csc.exe	Compile	Binaries	T1127: Trusted Developer Utilities Proxy Execution
Cscript.exe	Alternate data streams	Binaries	T1564.004: NTFS File Attributes
DataSvcUtil.exe	Upload	Binaries	T1567: Exfiltration Over Web Service
Desktopimgdownldr.exe	Download	Binaries	T1105: Ingress Tool Transfer
Dfsvc.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
Diantz.exe	Alternate data streams Download	Binaries	T1564.004: NTFS File Attributes T1105: Ingress Tool Transfer
Diskshadow.exe	Dump Execute	Binaries	T1003.003: NTDS T1202: Indirect Command Execution
Dnscmd.exe	Execute	Binaries	T1543.003: Windows Service
	Copy		T1105: Ingress Tool Transfer

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

零信任對策：AWL軟體白名單零信任解決方案 (2/3)

期望能解決非白名單程式與駭客植入惡意程式痛點

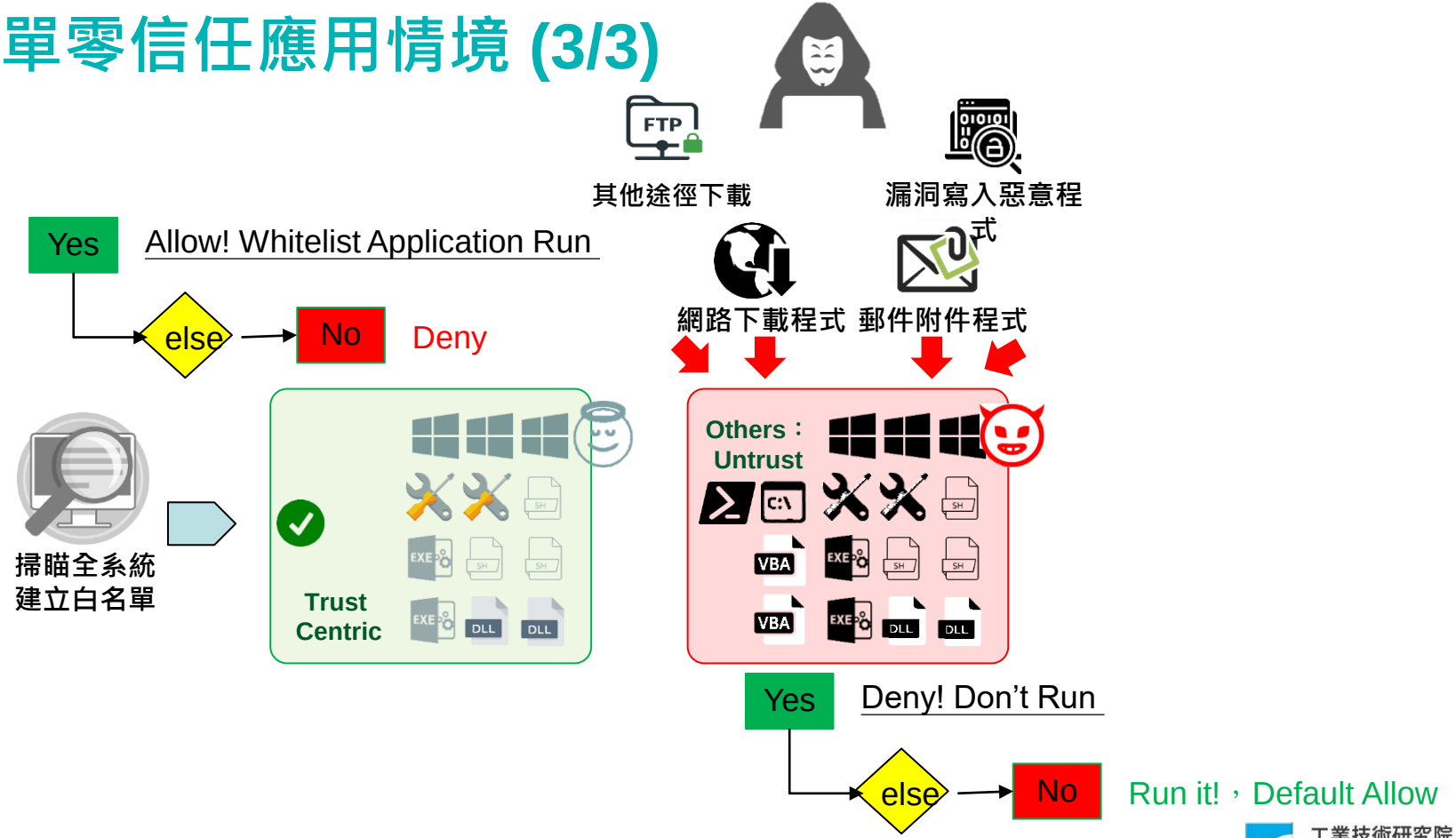
1. 從風險四個渠道上，把非白名單程式阻斷
2. 適用在標準化公務電腦的安全防護
3. 減輕IT與資安的壓力，搭配其他成為完整防護

阻斷駭客惡意程式進入系統執行所有管道	網路下載程式	郵件附件程式	其他網路途徑下載程式	系統漏洞寫入之惡意程式
阻斷駭客惡意程式類型	Not Trust Executable File	Not Trust Shell Scripts	Not Trust Command	Not Trust Macro File
防護的效益	無法執行非白名單程式	即時通知資安管理者		

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

白名單零信任應用情境 (3/3)



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

5、社交工程與釣魚依然發生 (1/3)

電子郵件攔阻始終不是100%，員工資安教育訓練永遠無法阻止去開啟疏於防備的各類惡意附件與連結

魚叉式網路釣魚（Spear Phishing

針對特定人員、公司、組織的發送，目標為釣取特定人員機敏資料或於其電腦植入木馬

複製型釣魚 (Clone

攻擊者使用某方法密切監視受害者收件匣，偽造郵件進行這類型網路釣魚。

鯨釣（Whaling）

直接瞄準大型公司、重要人物發送特定釣魚郵件的攻擊

語音簡訊釣魚（voice

攻擊者會假冒為受害者信任的個人或單位，利用語音通話與各種話術，取得機敏資訊。

商業信件妥協 (Business Email

這類信件詐騙沒有惡意鏈接或附件，規避安全檢查，冒充 CEO 或任何有權電彙的高管

雪鞋釣魚 (snowshoein g phishing)

使用不同提供商和服務器相關聯的Domain分類進行傳播垃圾郵件。雪鞋垃圾郵件發送者通常使用匿名域難追捕

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

疏於與難以防備的各類惡意附件(2/3)

駭客設計出針對性釣魚惡意附件，隱藏各類漏洞利用與程序武器化來躲避層層檢查

不在釣魚情資庫

出現空窗期

逃脫迴避檢查

線上沙箱檢查時間差

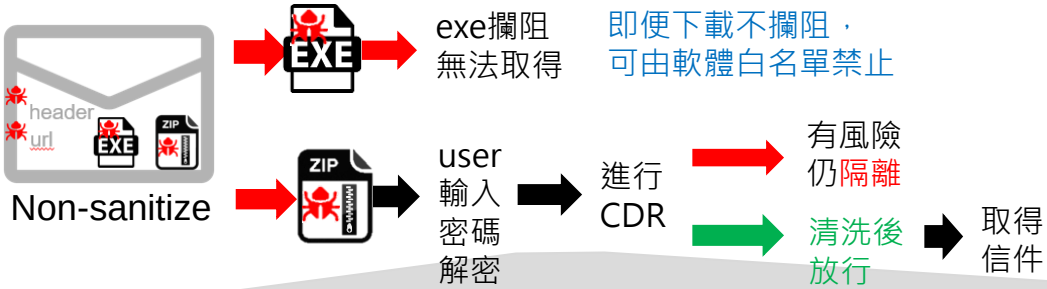
惡意圖片	HTA文件	RTLO	LNK快捷文件	漏洞利用
BMP內嵌惡意壓縮檔	HTML存成HTA (HTML Application)	RIGHT-TO-LEFT	LNK快捷文件藏惡意程式	CVE-2021- 40444
手觸發	**新版Office巨集**	**惡意HTML**	**舊版EXCEL巨集**	**無檔案式攻擊**
滑鼠移動觸發 (ppt撥放模式)	Macro 藏惡意程式	HTML內嵌惡意Scripts	EXCEL4.0 惡意巨集	不落地在記憶體執行惡意程式

工業技術研究院 Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

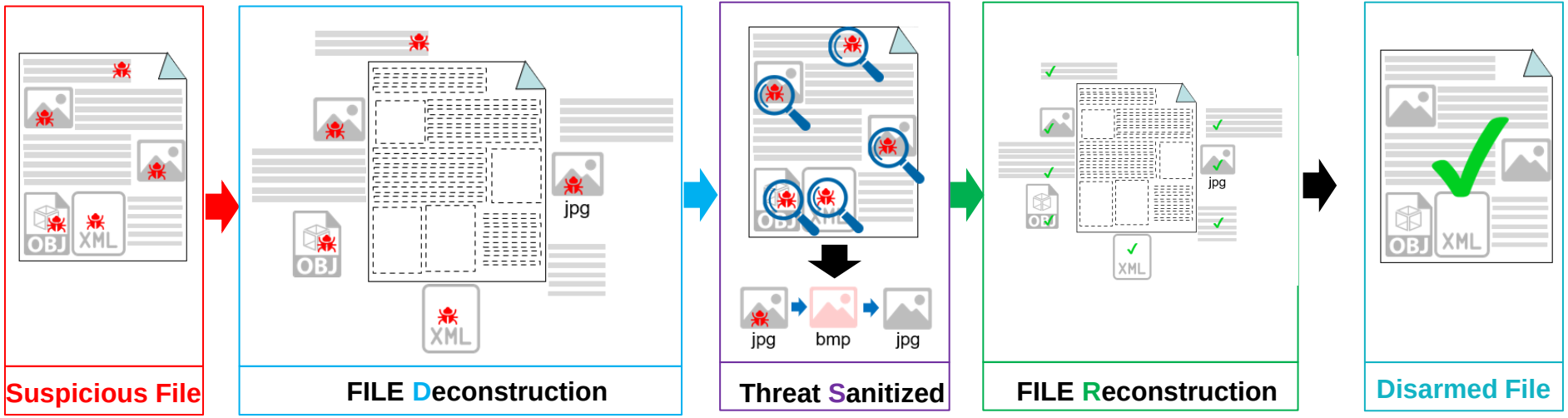
零信任對策：郵件與附件清洗 (3/3)

Content disarm and reconstruction



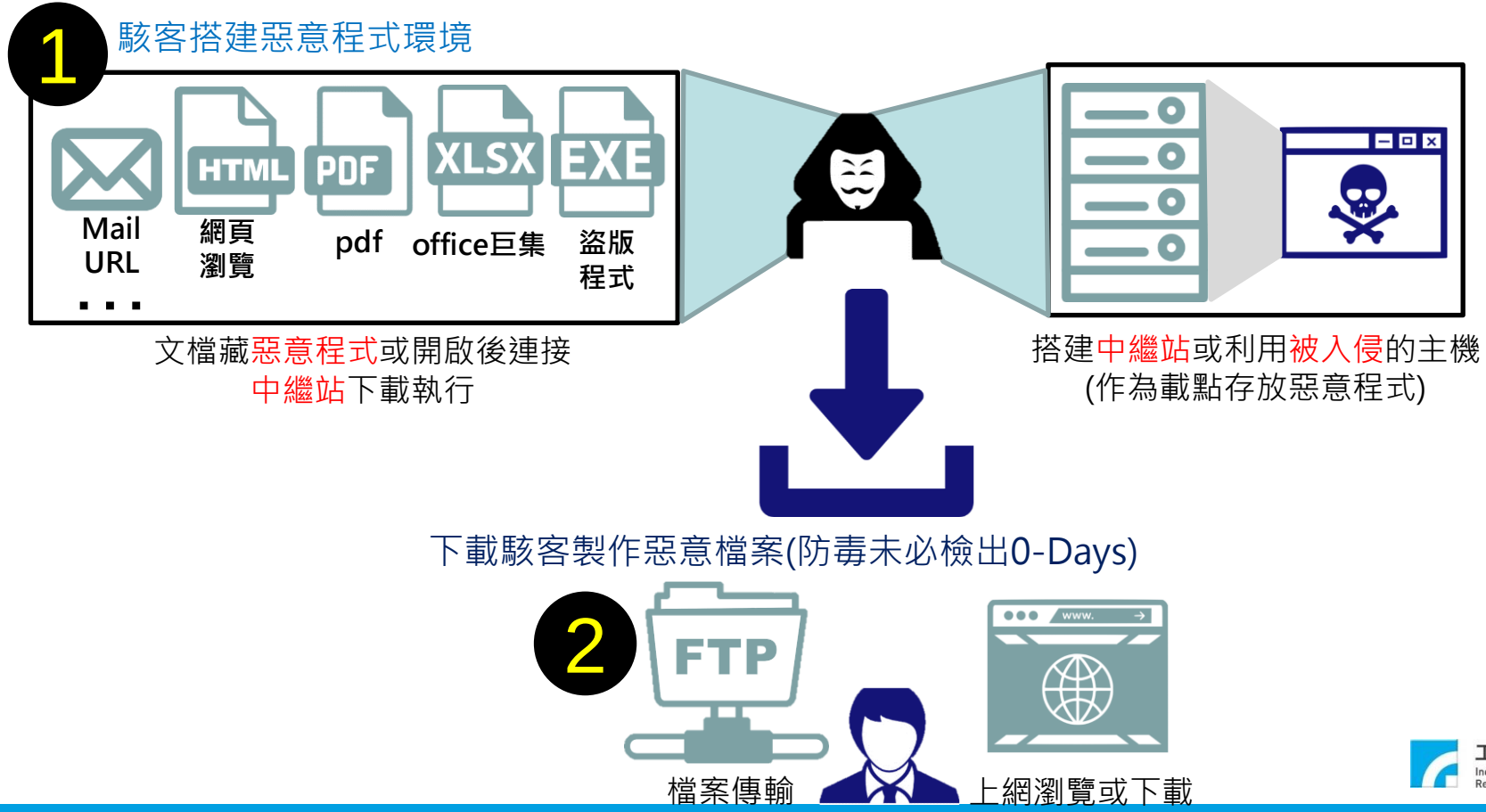
分析相關安全機制，還結合：

- 多套防毒掃描引擎交叉比對
- 防釣魚資料庫
- 防垃圾郵件機制
- 檔案沙箱檢核
- …



©ITRI. 工業技術研究院著作

6、員工上網永遠無法得知網站與檔案藏哪些風險(1/4)



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

從現場到電視觀看，解構上網風險問題(2/4)

企業主管可能會問? 網路有防火牆+沙箱，端點有EDR+防駭防毒難道不夠嗎?

風險：

- ~~突發事件觀眾踩踏~~
- ~~舞台倒塌~~
- ~~煙火施放導致火災~~
- ~~病毒快速傳播~~
- 地震疏散傷亡

透過電視觀看直播演場會

隔離上網

VS.

現場參加演場會

直接連網

風險：

- ✓ 突發事件觀眾踩踏
- ✓ 舞台倒塌
- ✓ 煙火施放導致火災
- ✓ 病毒快速傳播
- ✓ 地震疏散傷亡

取決於：

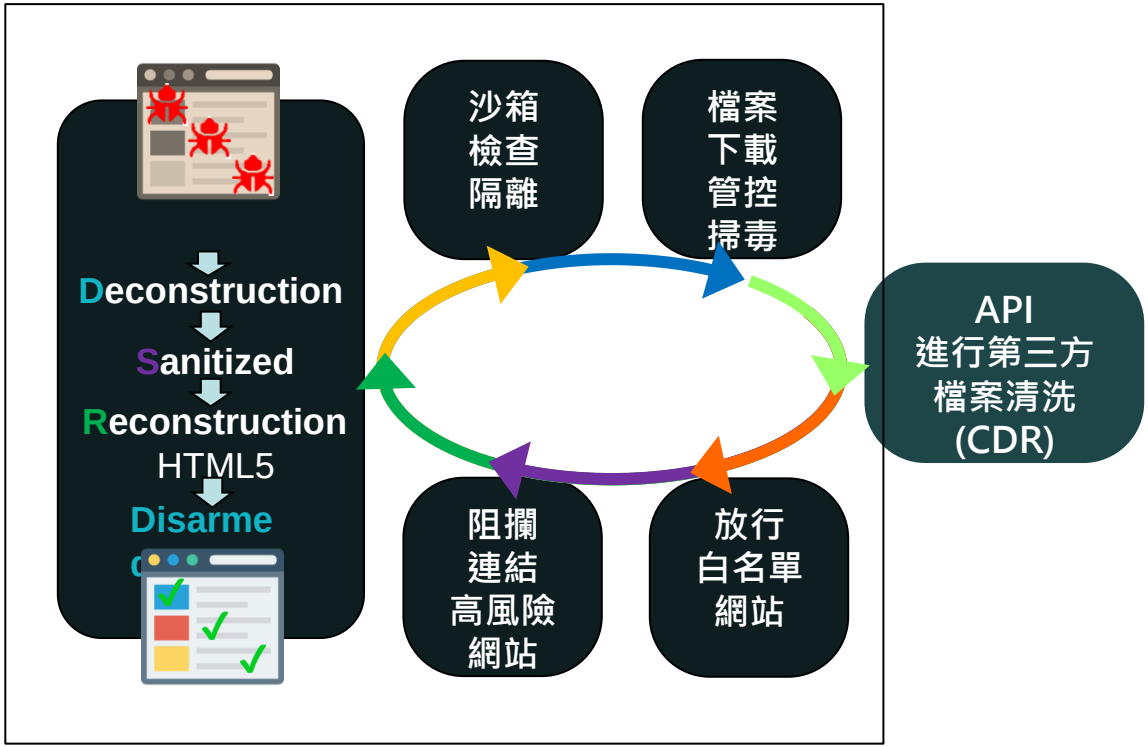
面對風險類型不同、零信任價值未落實、公司上網活動vs.駭客破壞竊取支出分析、沒將駭客手法精進算入與產業適型性

工業技術研究院 Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

零信任對策：人員隔離上網(3/4)

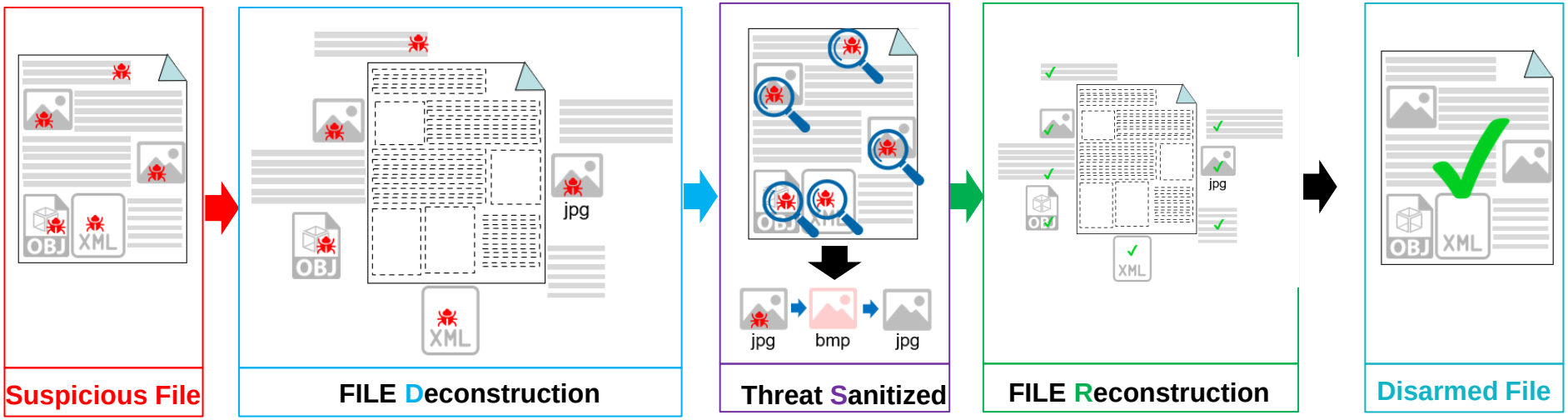
URL / Web



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

下載檔案進行清洗 (4/4)



工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

7、資料與隱私保護

1.盤點與數據分類

Inventory and data classification of cloud data and on-premises data can protect data.

2. 授權管控

Authorized users are restricted from reading, transmitting, deleting, modifying, and printing data under control, and create usage records

3. 預防資料外洩

Use DLP technology to filter content, control transmission and storage. Even if the data is authorized and circulated externally, it should be tracked with DRM technology.

4. 隱私與保密設計

Privacy Enhancement Technologies:

- Federated learning,
- Homomorphic encryption,
- zero-knowledge proof,
- Secure Multi-Party Computation

Multi-level De-identification:

- K-anonymity,
- differential privacy

5.資料治理

- Continuous monitoring of alert data
- Correction of violations
- Audit risk user usage take revocation access
- Block unauthorized users
- Continually update the data usage policy

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

8、裝置零信任

Smart Phone	1. The company has issued a special mobile phone, and the camera lens and data transmission function have been cancelled 2. DLP (Manage MTP transmission)
HID	1. No private entry is allowed 2. DLP
Cable	1. No private entry is allowed 2. DLP
Wi-Fi	1. Wi-Fi is authenticated 2. Using company-approved AP 3. DLP
Portable storage device	1. No private entry is allowed 2. DLP
video camera	1. Concessionary use of meeting rooms 2. DLP
Bluetooth	1. Bluetooth device disabled 2. Using company-approved AP 3. DLP

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

9、5G 核心和邊緣安全設計和已知漏洞 (1/5)

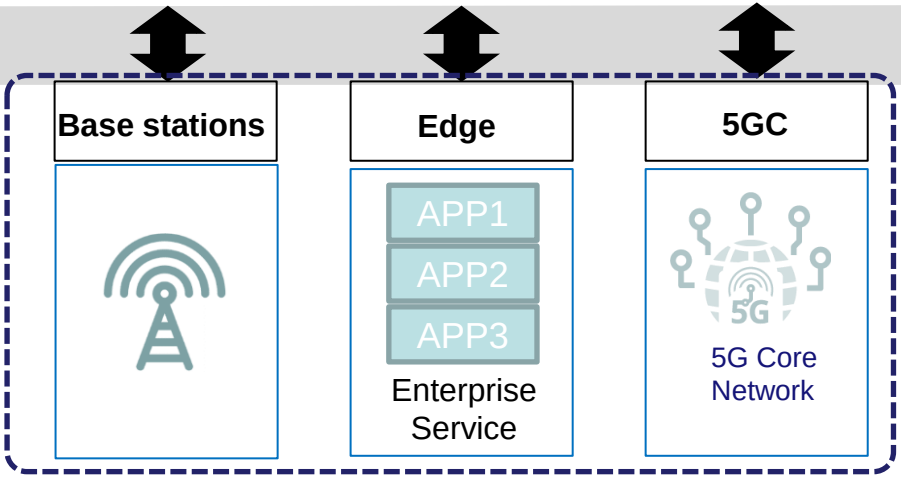
從駭客思維可見的攻擊想定：

- Chip Design Safety
- buffer overflow
- 5GC code vulnerability

- potential vulnerability
- Malicious Container
- APP vulnerabilities
- Slice/Resource Theft

- Fake base stations
- Impersonate users
- MiTM
- Attack PWS

- DOS & DDOS
- Cloud Application Vulnerability
- bottom layer attack on POD or Containe
- POD attack POD



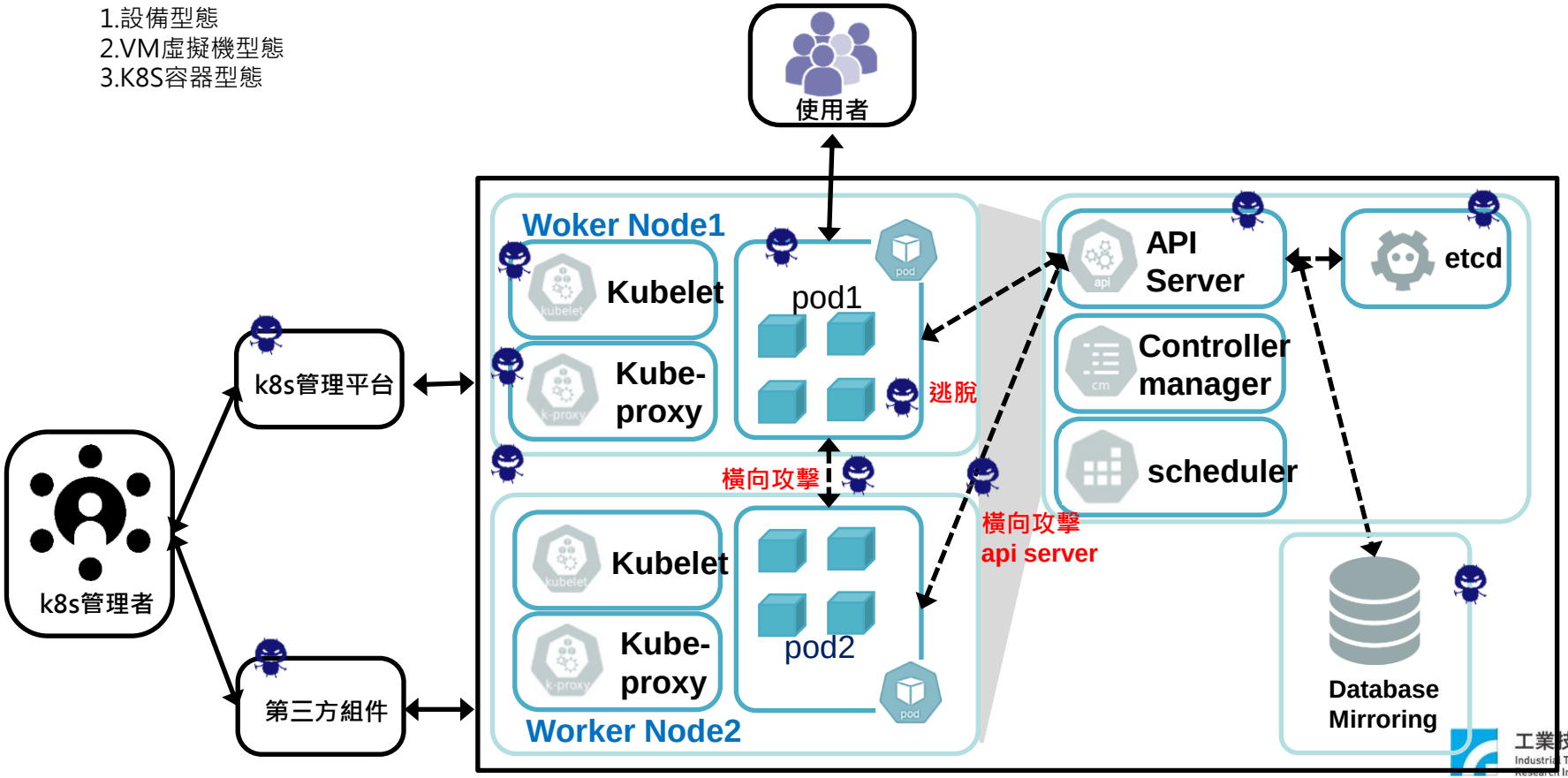
**「災防告警細胞廣播訊息系統（Public Warning System，PWS）」

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

攻擊者對 5GC & Edge 的思考： k8s型態(2/5)

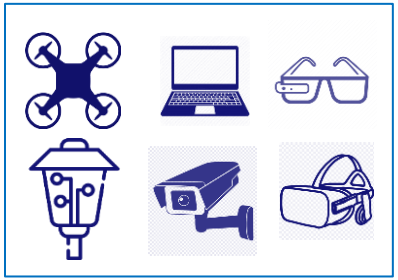
1.設備型態
2.VM虛擬機型態
3.K8S容器型態

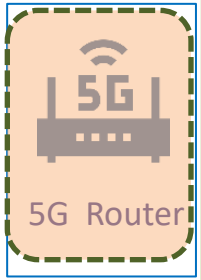


©ITRI. 工業技術研究院著作

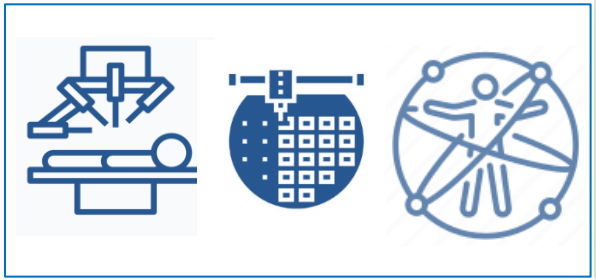
5G 路由器安全問題(3/5)

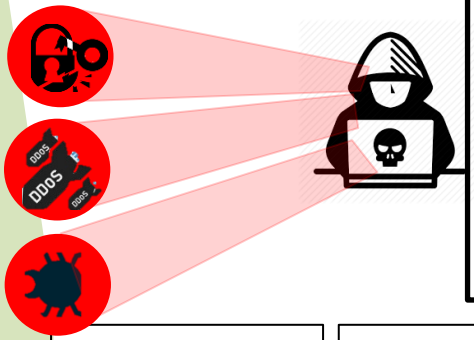
5G Application Terminal





5G Application Services





1. Brute force Password
2. Lack of 2FA
3. OpenSSL vulnerability
4. Lack of self-defense
5. Ignore firmware update
6. Difficulty passing OWASP requirements
7. Sim card security issues
8. 0-Day Vulnerability
9. Engineer act as one sees fit

Enterprise Site	Base stations	Edge	5GC	Internet Service
		APP1 APP2 APP3 Enterprise Service	 5G Core Network	

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

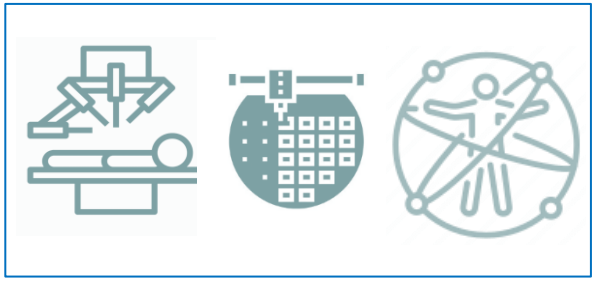
5G應用終端安全問題(4/5)

5G Application Terminal

- Brute force Password
- Lack 2FA
- OpenSSL vulnerability
- Lack of self-defense
- Ignore firmware update
- Difficulty passing OWASP requirements
- Sim card security issues
- 0-Day Vulnerability
- Engineer act as one sees fit

- Ransomware
- Threats originating from Internet
- Privacy Breach
- DOS / DDOS
- IoT Botnet
- Billing Evasion (計費規避)
- APT
- Phishing

5G Application Services



Enterprise Site	Base stations	Edge	5GC	Internet Service
		APP1 APP2 APP3 Enterprise Service	 5G Core Network	

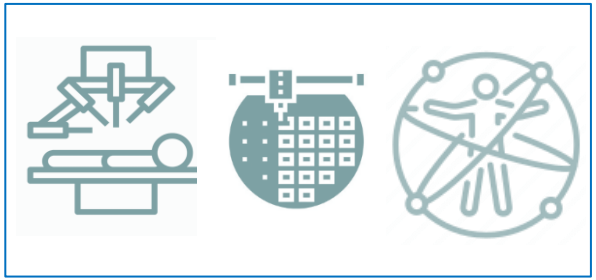
工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

對策

5G Application Terminal

5G Application Services



安全驗證

- Source Code Analysis
- Black Box Testing
- Penetration Testing
- Vulnerability Assessment

產品設計

- Application Zero Trust
- Transport / Session Zero Trust
- User / ACL Zero Trust
- Firmware Zero Trust
- Bootloader Zero Trust
- Hardware Zero Trust
- Network Zero Trust
- Cloud Zero Trust
- Devices Zero Trust
- Data / Dataflow Zero Trust

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

10、還有兩個重要議題，與智慧工廠安全息息相關

- AI 安全議題 (人工智慧資安論壇)

- 供應鏈安全 (供應鏈安全論壇)

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作

感謝聆聽

Thank You!

工業技術研究院
Industrial Technology Research Institute

©ITRI. 工業技術研究院著作