FORTINET

Secure OT Summit 2023
保衛工控 即刻守護

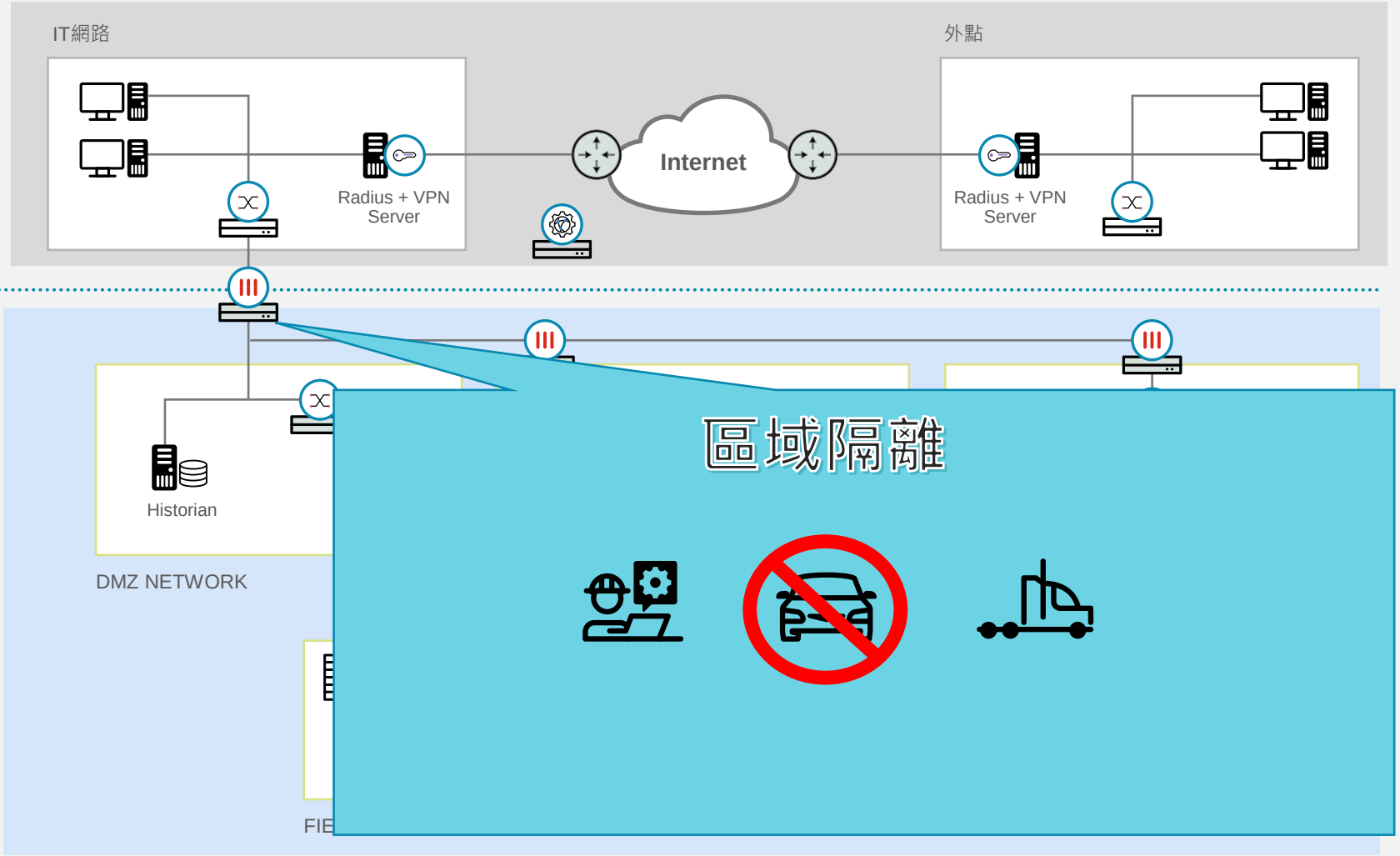
快速打造工控營運的資安防禦堡壘

Degas / 曹仁賢
Security Consultant

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

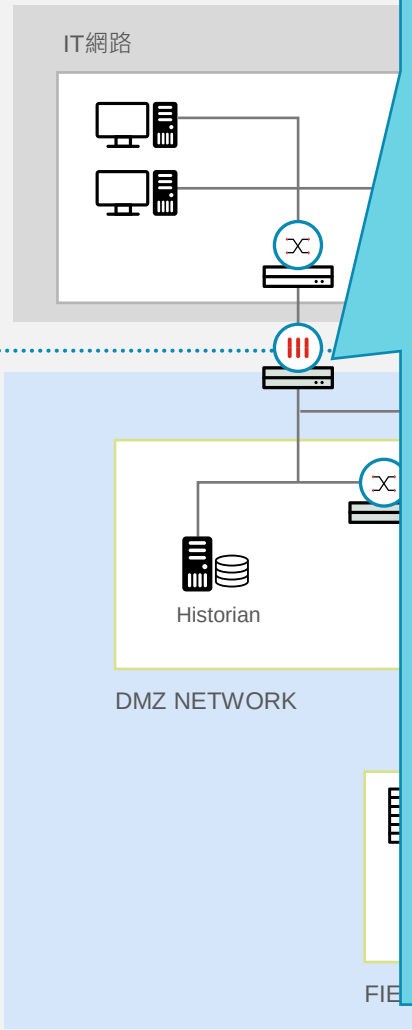


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

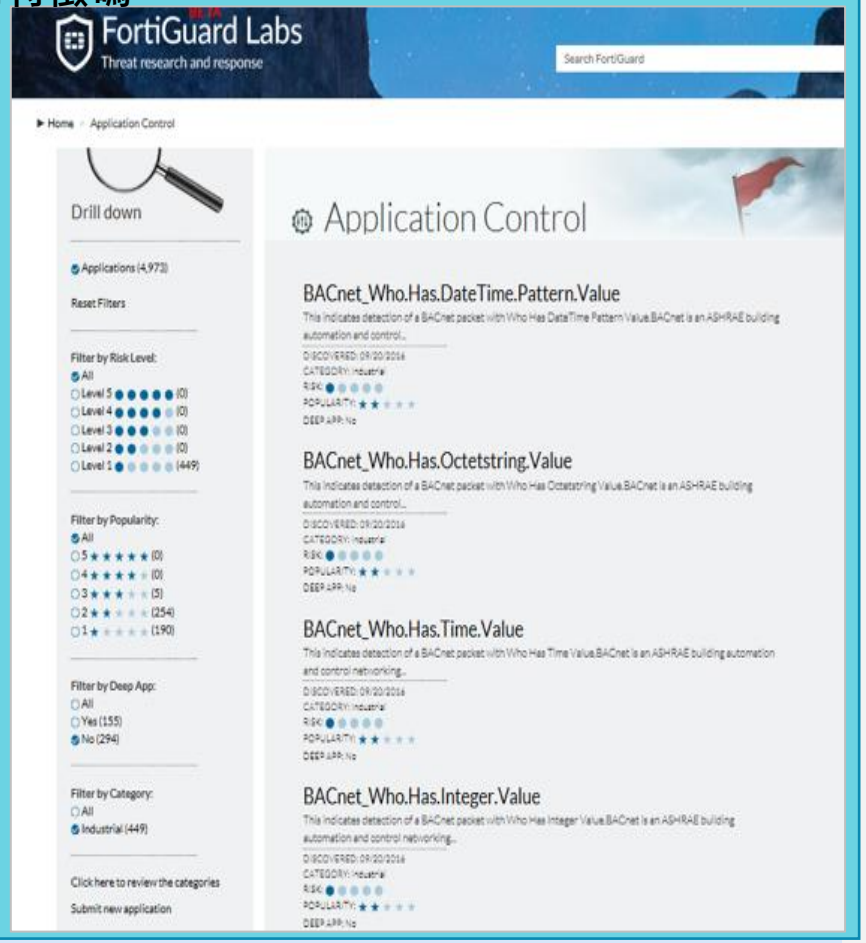
Operational Technology (OT)



安檢/IPS/虛擬補丁

接近2000個工業應用特徵碼
為工業應用保駕護航

- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- HART
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor

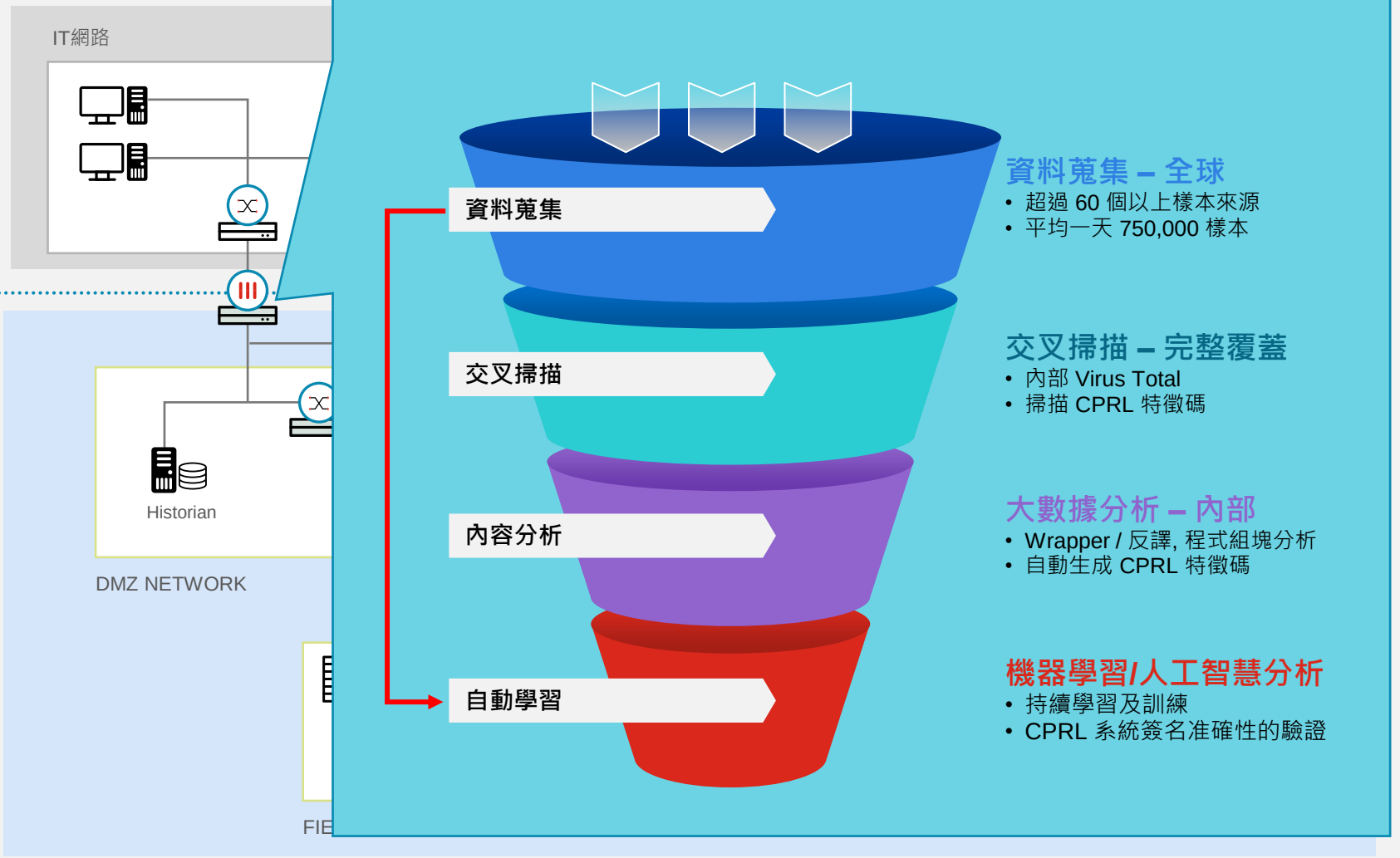


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

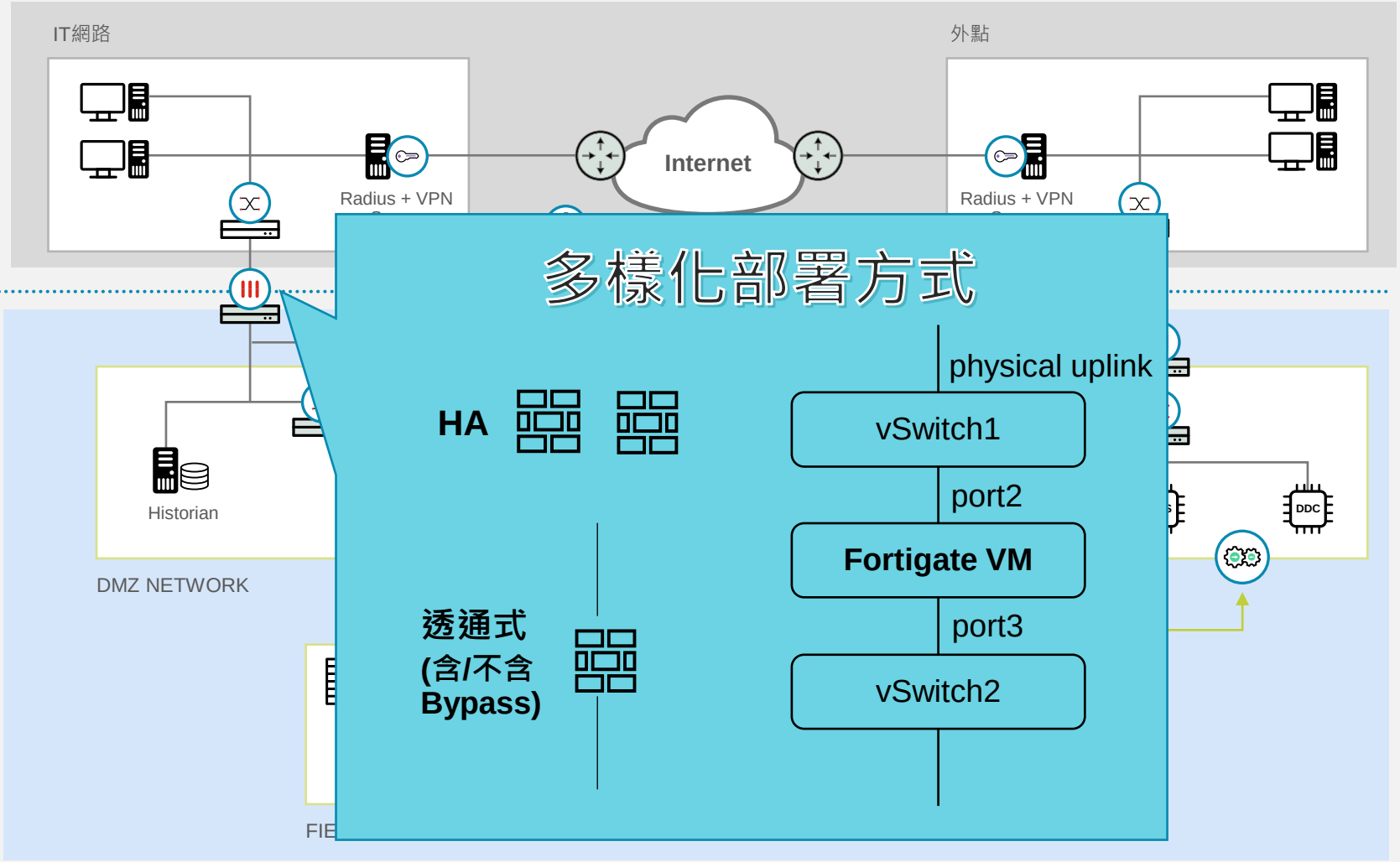


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

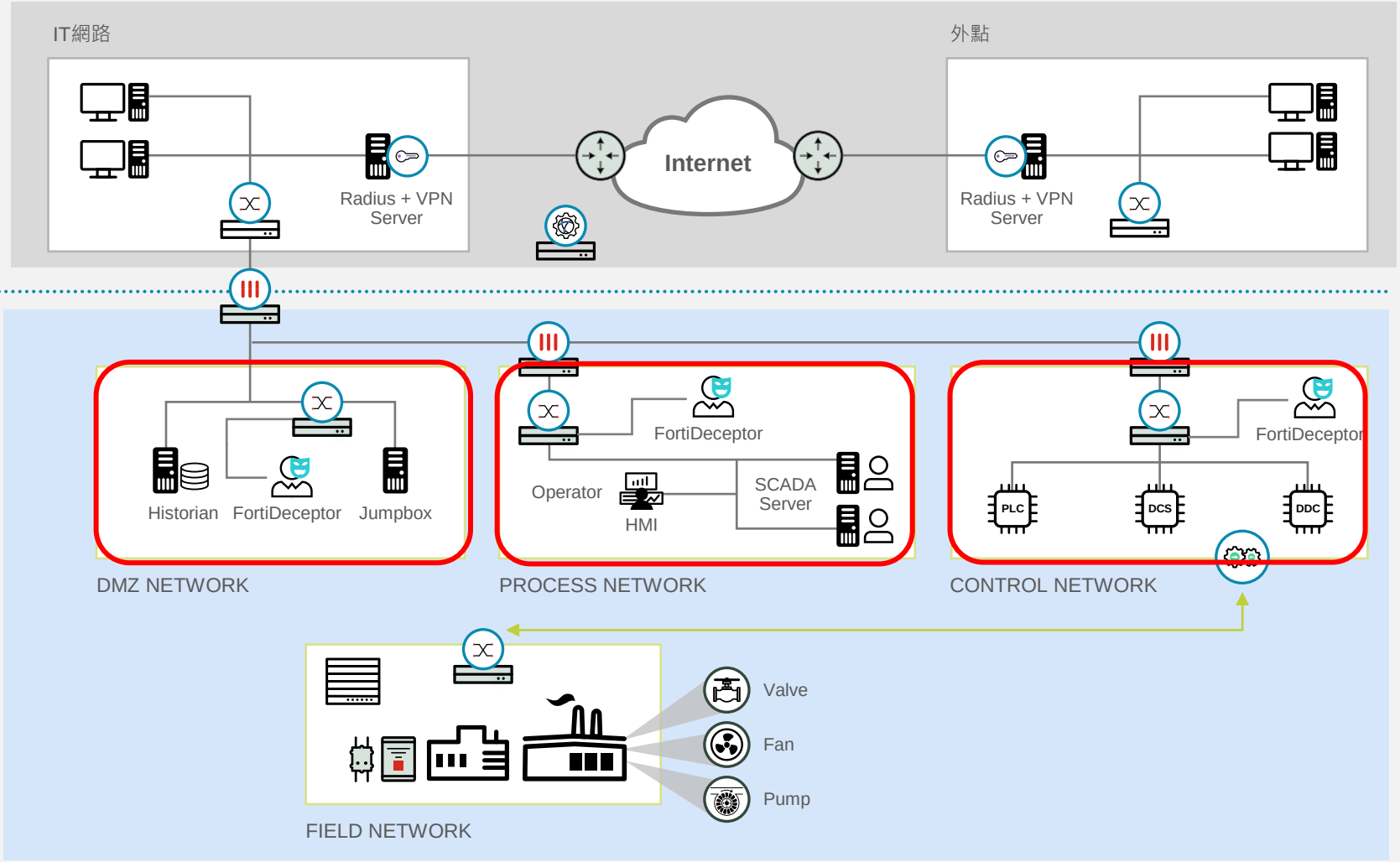


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

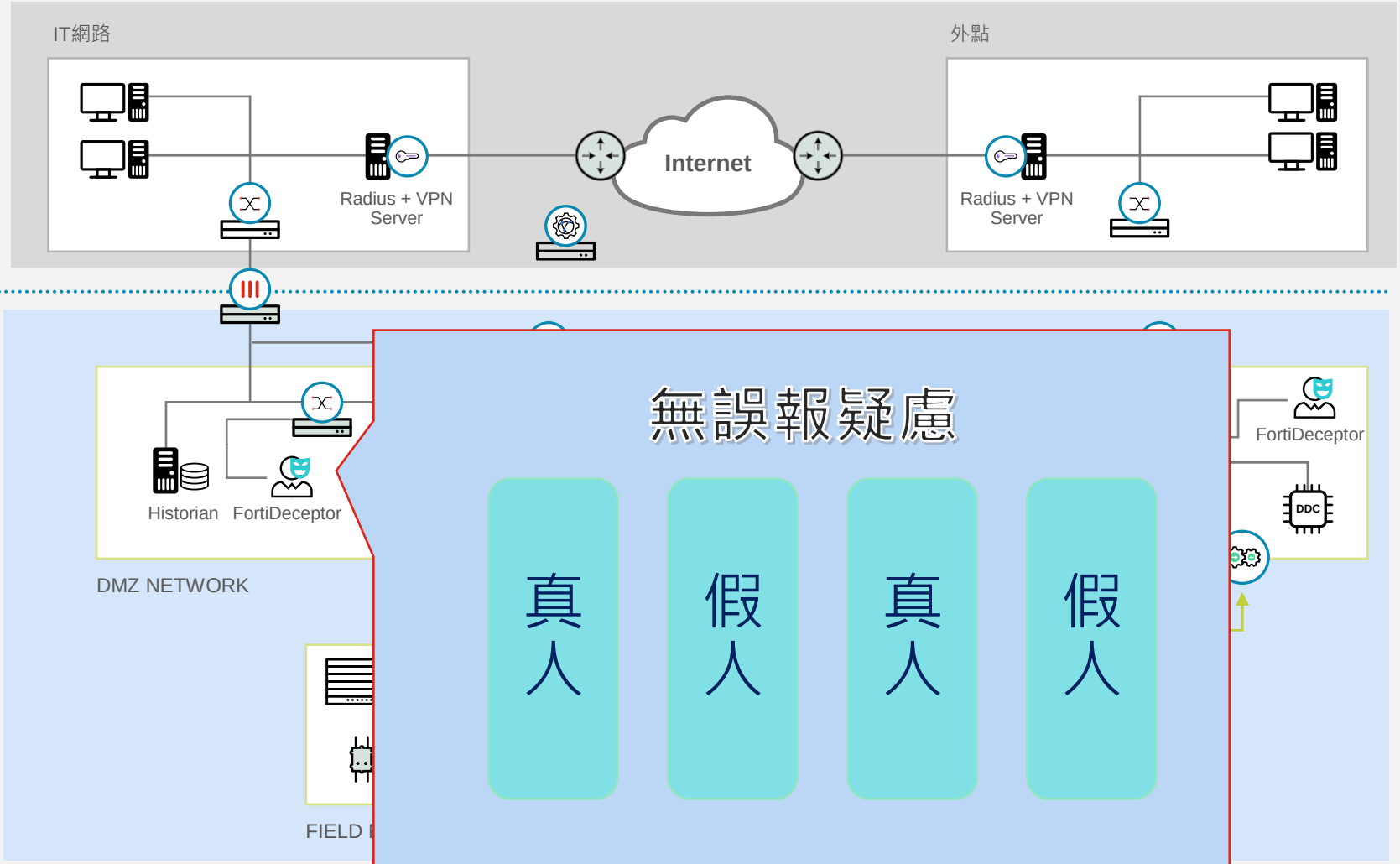


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

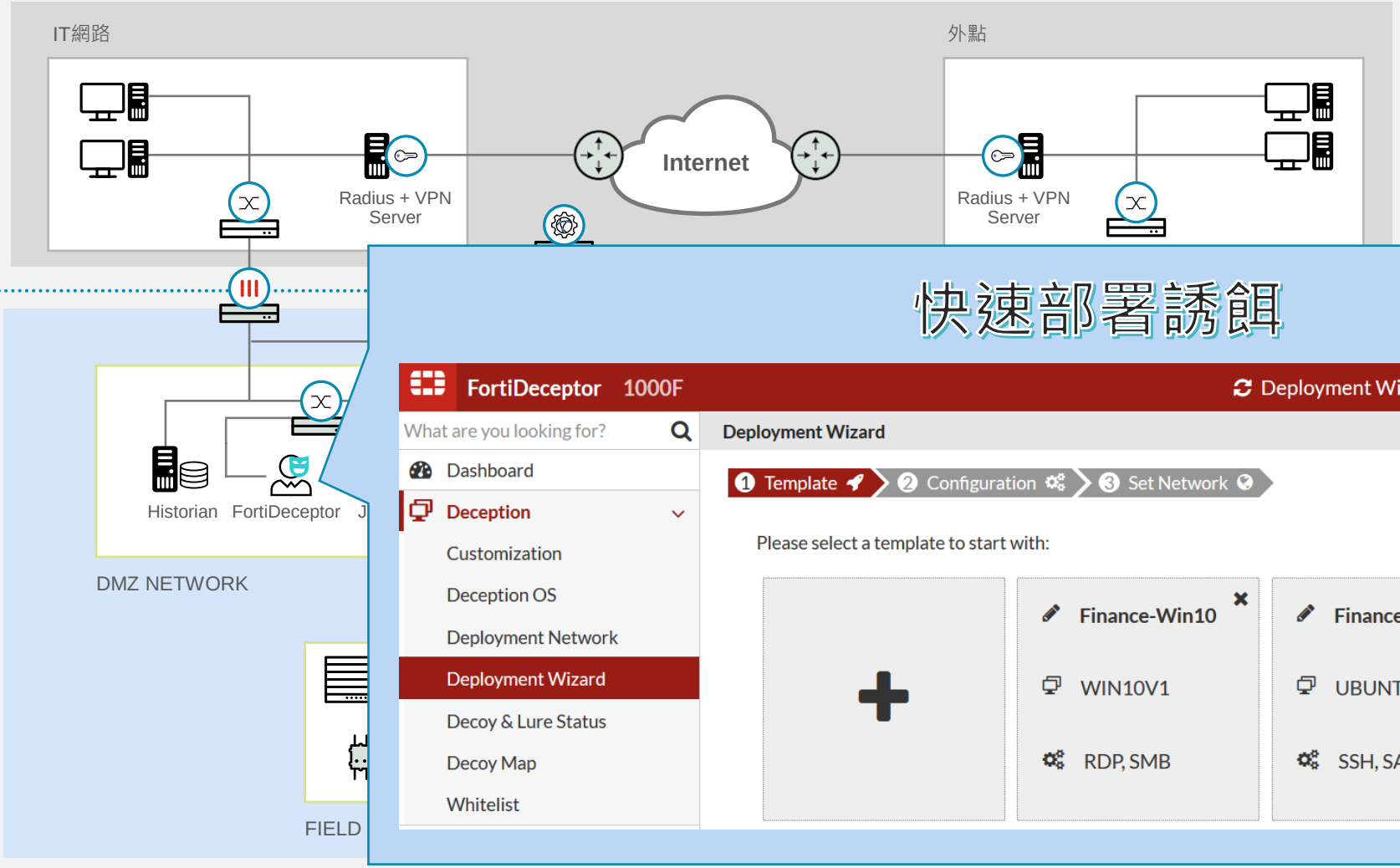


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

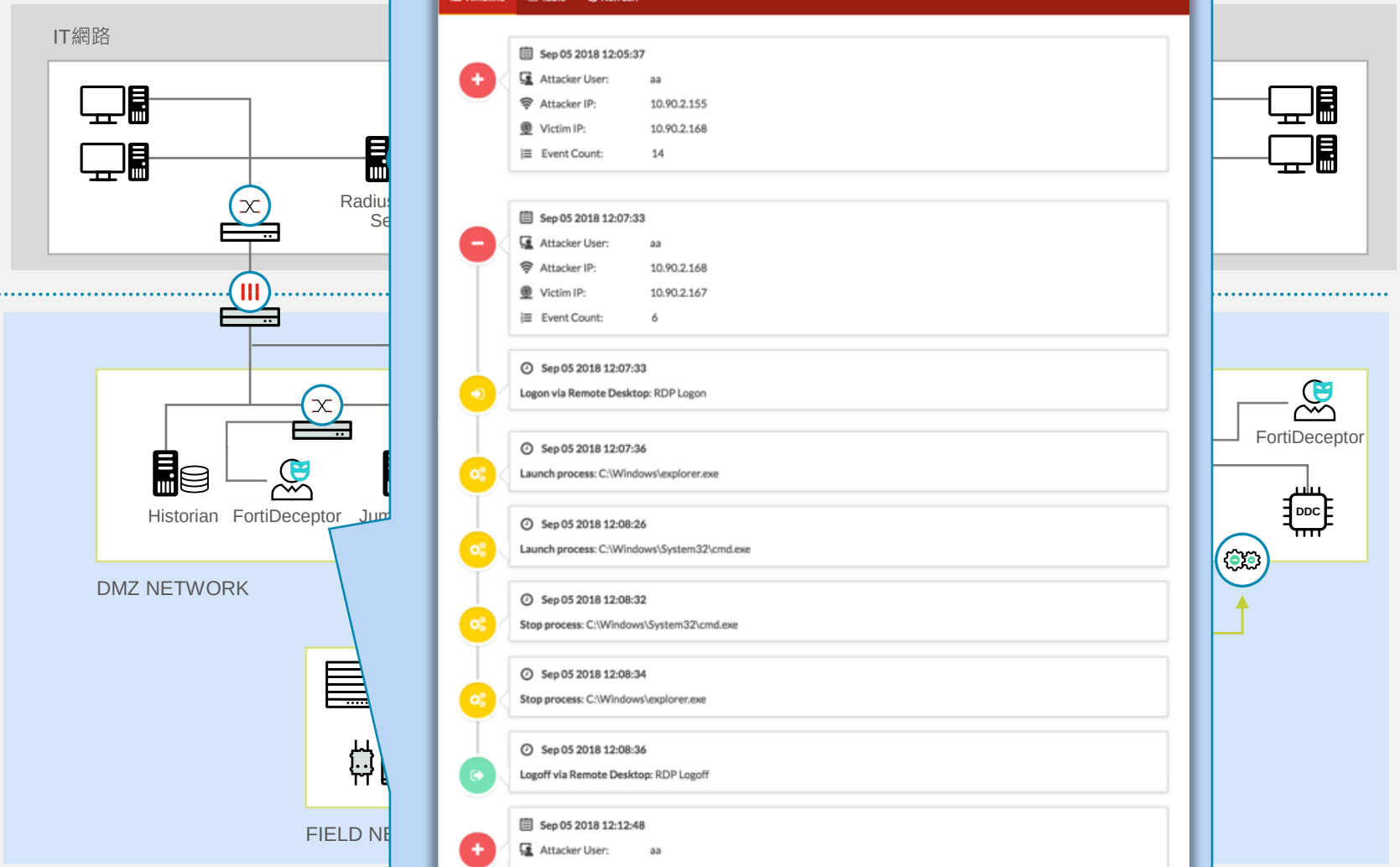


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)



完整足跡

Timeline | Table | Refresh

Sep 05 2018 12:05:37
Attacker User: aa
Attacker IP: 10.90.2.155
Victim IP: 10.90.2.168
Event Count: 14

Sep 05 2018 12:07:33
Attacker User: aa
Attacker IP: 10.90.2.168
Victim IP: 10.90.2.167
Event Count: 6

Sep 05 2018 12:07:33
Logon via Remote Desktop: RDP Logon

Sep 05 2018 12:07:36
Launch process: C:\Windows\explorer.exe

Sep 05 2018 12:08:26
Launch process: C:\Windows\System32\cmd.exe

Sep 05 2018 12:08:32
Stop process: C:\Windows\System32\cmd.exe

Sep 05 2018 12:08:34
Stop process: C:\Windows\explorer.exe

Sep 05 2018 12:08:36
Logoff via Remote Desktop: RDP Logoff

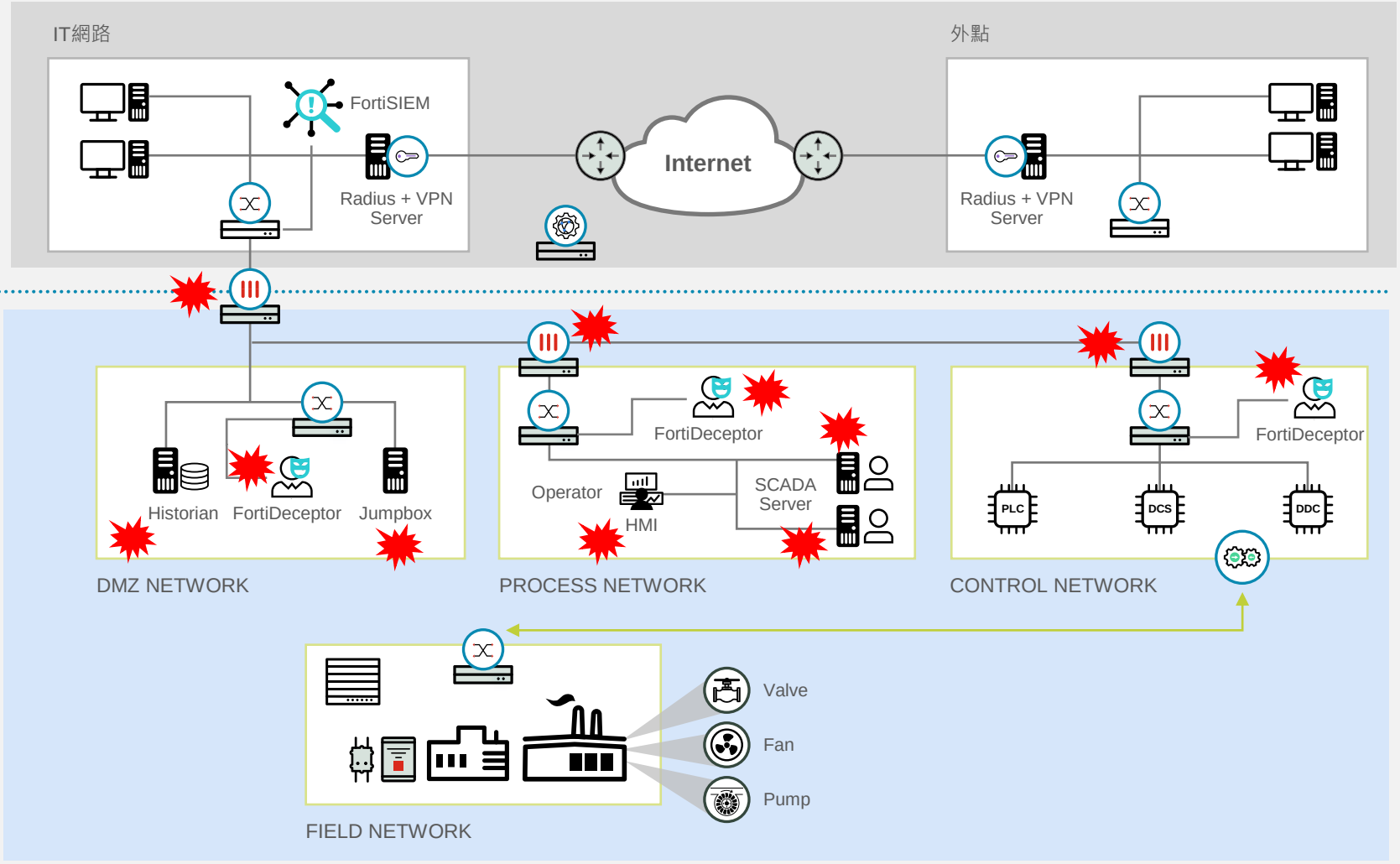
Sep 05 2018 12:12:48
Attacker User: aa
Attacker IP: 10.90.2.155
Victim IP: 10.90.2.168
Event Count: 12

© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)

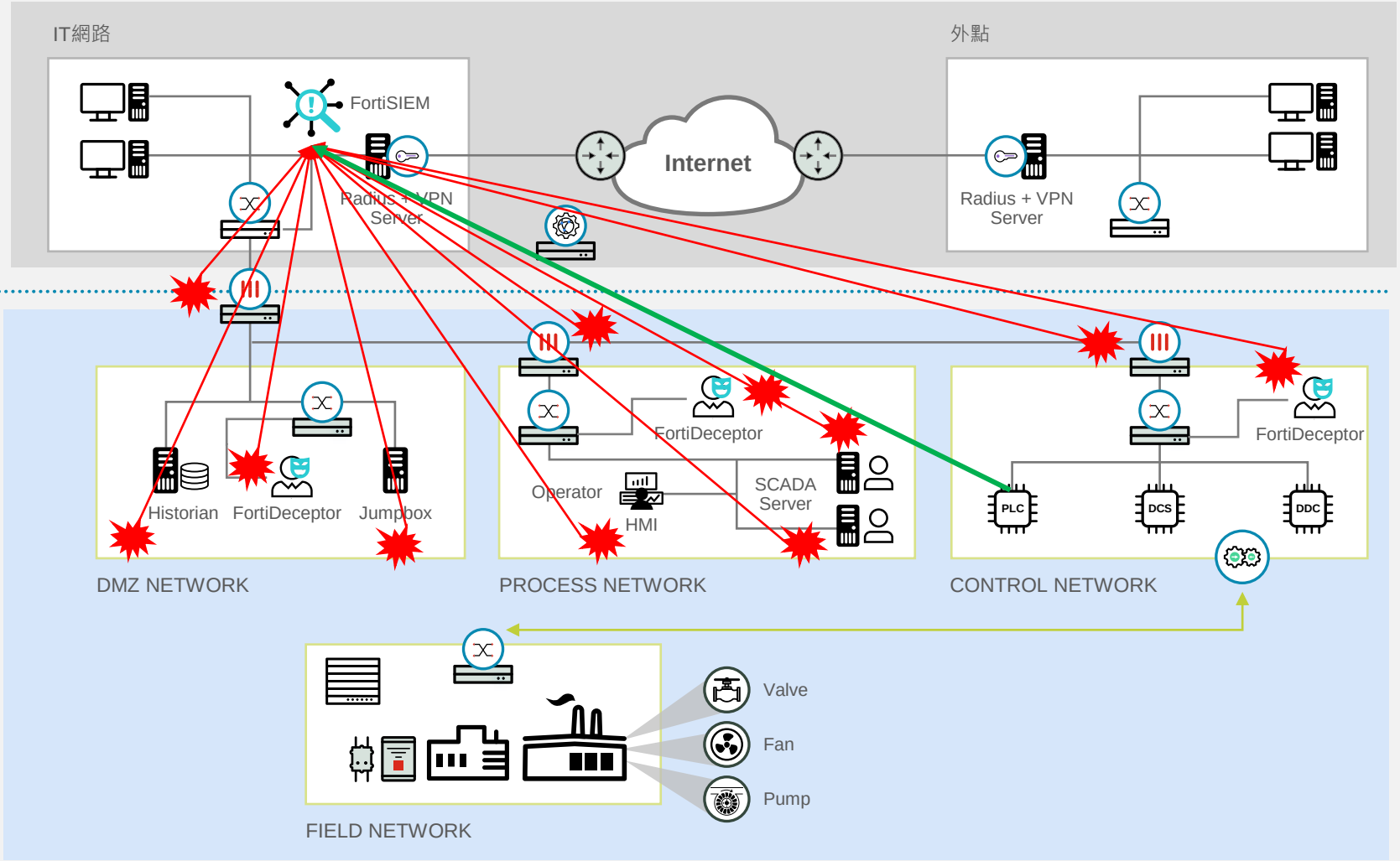


© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

Operational Technology (OT)



© Fortinet Inc. All Rights Reserved.

按部就班做資安

Information Technology (IT)

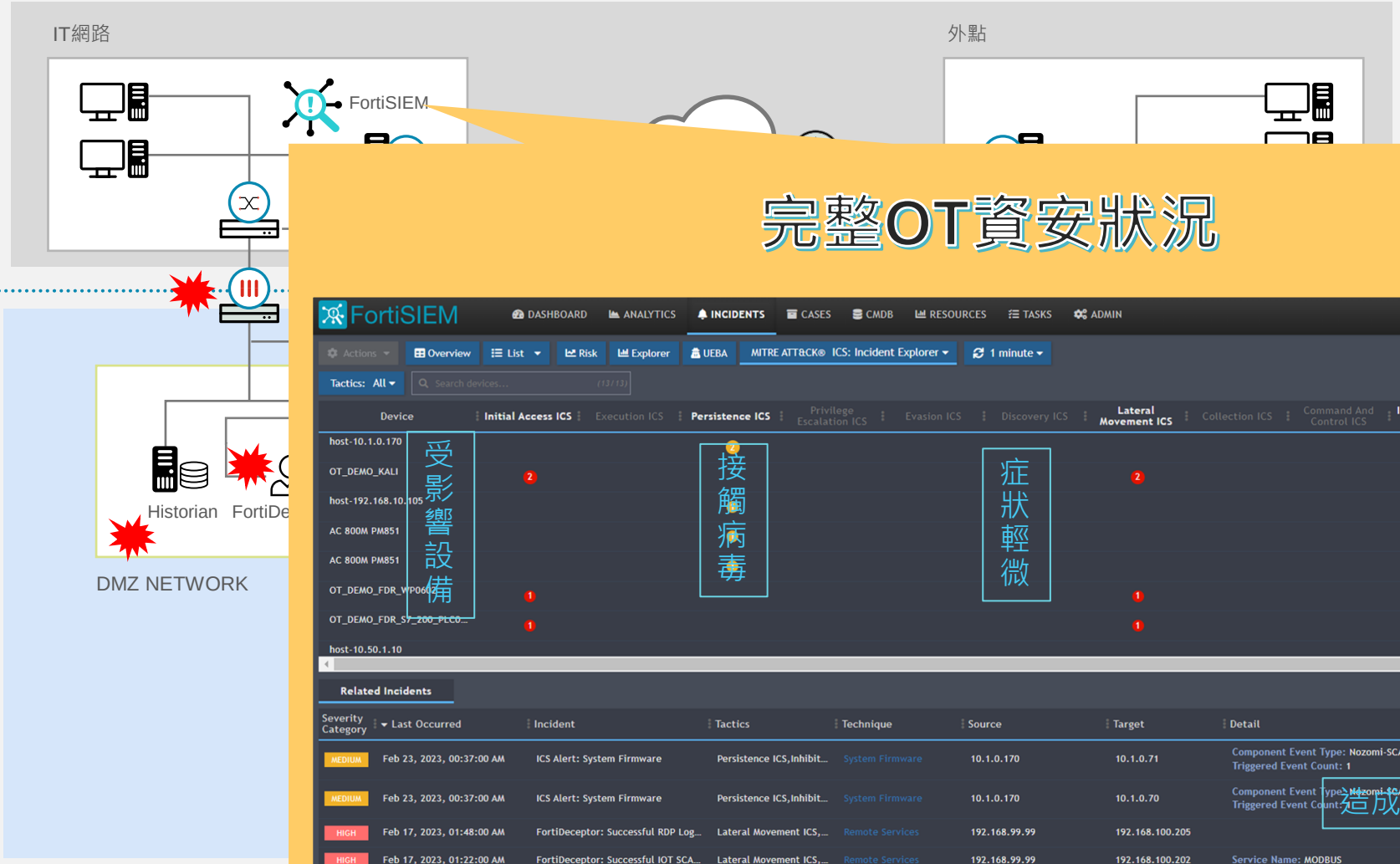
Operational Technology (OT)

完整資安狀況

按部就班做資安

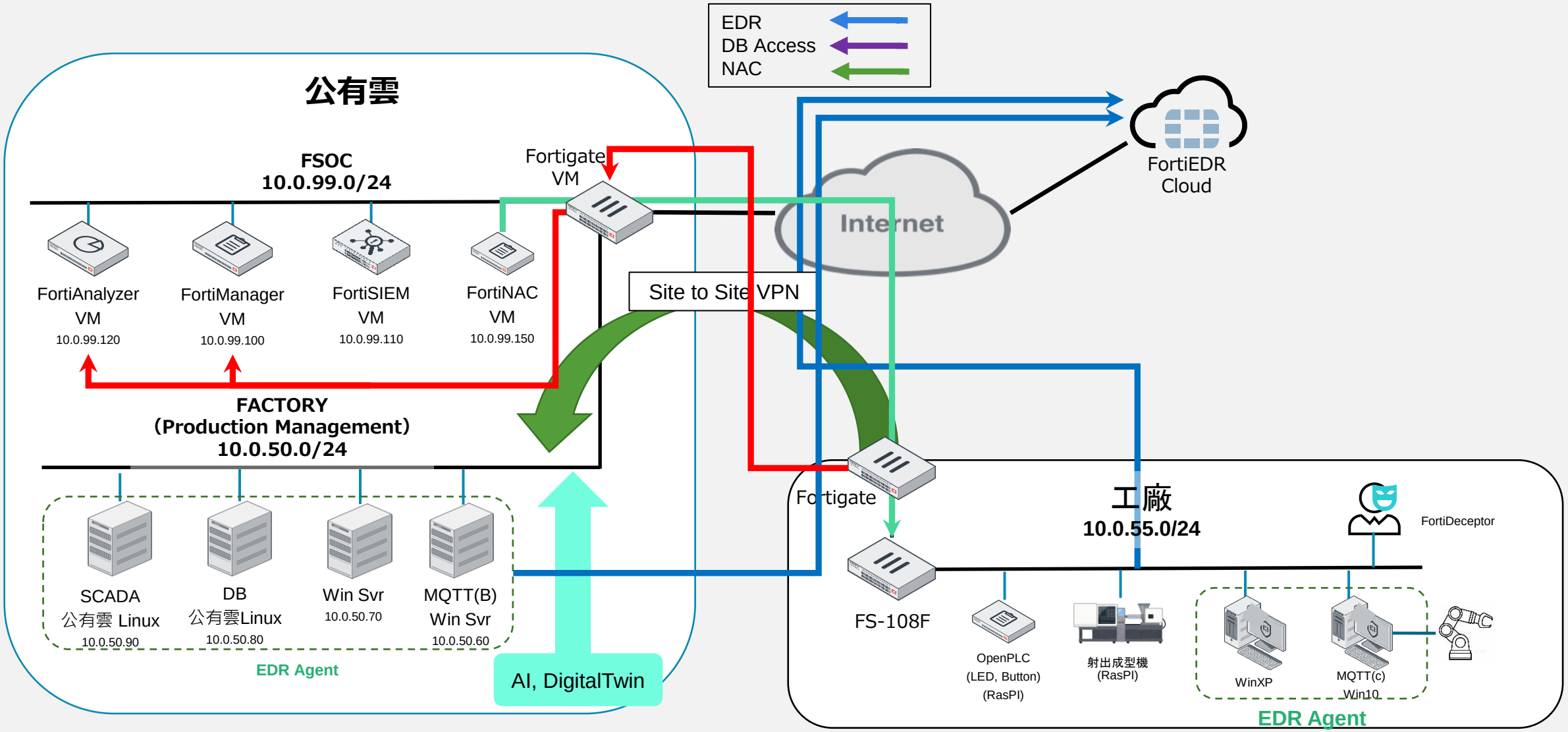
Information Technology (IT)

Operational Technology (OT)



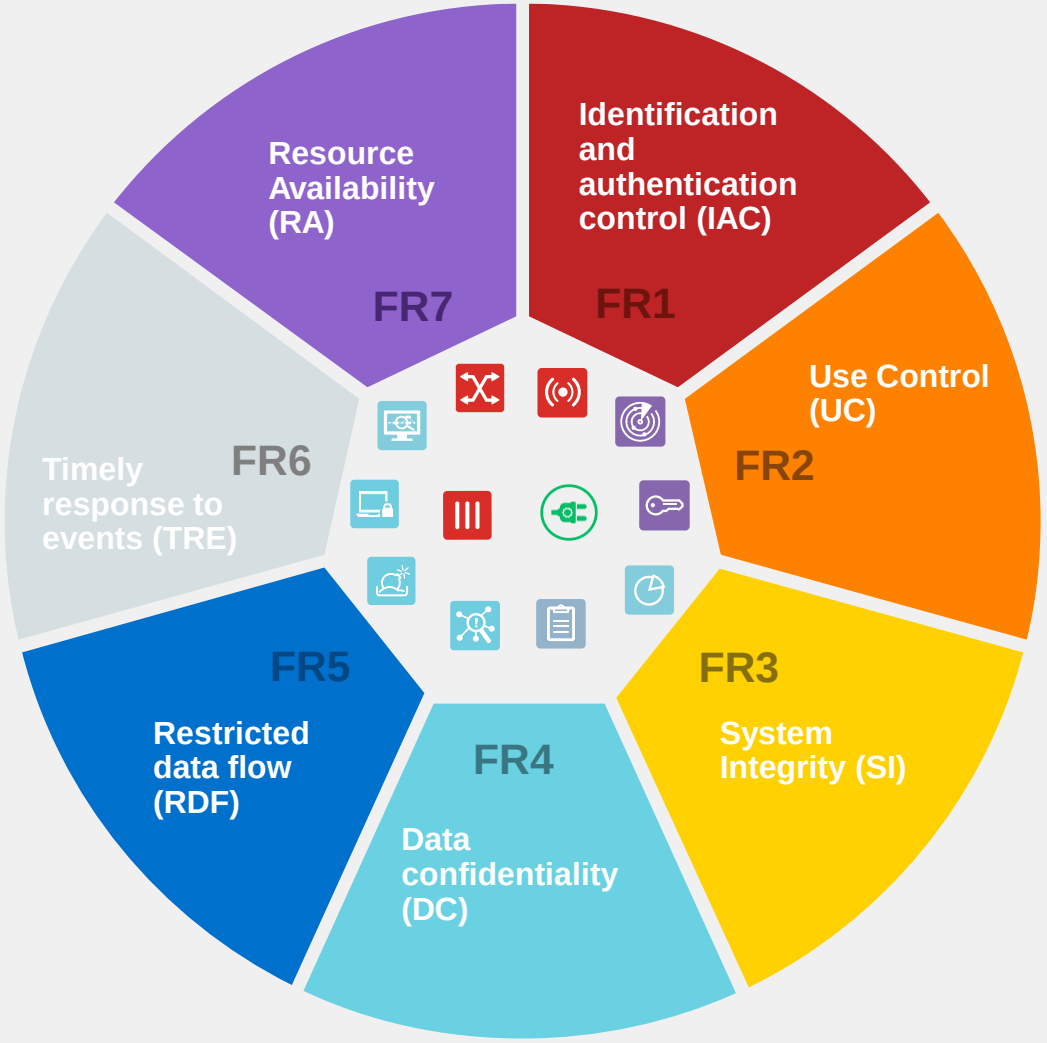
完整OT資安狀況

Fortinet OT 公有雲方案



© Fortinet Inc. All Rights Reserved.

IEC 62443 – 對應方案



1 FortiGate, FortiWiFi/FortiAP, FortiNAC FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSIEM

2 FortiGate, FortiWiFi/FortiAP, FortiNAC, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandobox, FortiSIEM

3 FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandobox, FortiSIEM, FortiTester, FortiResponder

4 FortiGate, FortiSwitch, FortiAP, FortiEDR

5 FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer

6 FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiSIEM, FortiManager

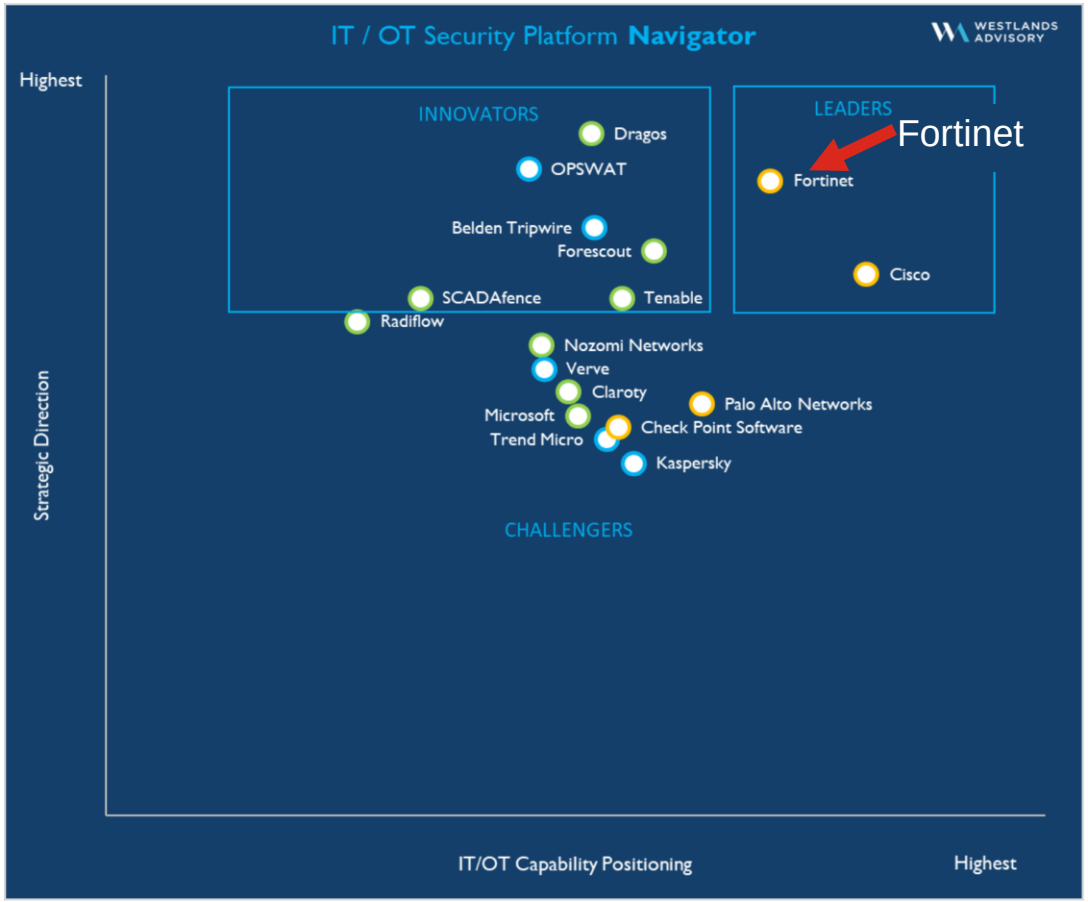
7 FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions

© Fortinet Inc. All Rights Reserved.

Fortinet OT 安全織網

網路安全	▪ 網路分割 ▪ 網路微分割 ▪ 安全 SD-WAN / SD-Branch ▪ 網頁安全
零信任存取	▪ 網路存取控制 ▪ 角色存取控管 ▪ 安全遠程連接
網路維運	▪ 登入、監控和報告 ▪ 網路運維中心(NOC)
安全維運	▪ 資安自動協作系統 ▪ 資安運維中心(SOC)
情資與回應	▪ 端點偵測與回應 ▪ 進階威脅防禦 ▪ 工控安全情資 ▪ 自動 IoT 設備識別
開放式生態鏈	▪ ICS/OT 安全合作夥伴 ▪ 安全織網合作夥伴
OT方案	▪ 工規級別硬體 ▪ 虛擬機器 ▪ 3G/4G/5G 無線設備

IT/OT Security Platform Navigator 2022



- Primarily NGFW & Zero Trust
- Mixed Capabilities
- Primarily Vulnerability Management & Threat Detection

WESTLANDS ADVISORY

Appliance
Virtual
Hosted
Cloud
Agent
Container

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

Secure OT Summit 2023

保衛工控 即刻守護