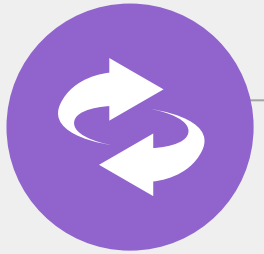
FortiDeceptor

DECEIVE | EXPOSE | ELIMINATE THREATS

Loco Hsu

Agenda



01

Deception Technology
是什麼?

02

FortiDeceptor
Technology

03

Deception Use Cases
欺敵誘捕技術使用案例

04

FortiDeceptor 在OT場景
的應用

© Fortinet Inc. All Rights Reserved.

什麼是 Deception Technology?

Deception Technology (欺敵誘捕技術) :

從攻擊者的角度或方法透過網路來檢視現有資訊系統上是否存有可被攻擊的漏洞。這個技術直接透過虛擬化的方式模擬各種現有IT環境常見元件作為誘餌，吸引攻擊者的注意。是一種強調即時、精準以及自動化防禦的手段。

Deception Technology 的運作方式 :

Deception Technology 通常以三個基本的動作運作 :

Deceive (設置陷阱與誘餌)
Expose (偵測威脅)
Eliminate (阻擋與隔離威脅)

為何需要 Deception Technology?

複雜的內部和外部攻擊的風險在過去幾年呈指數級增長。當今的安全技術主要尋求防禦邊界，但防火牆以及端點安全解決方案無法提供100%的安全保證。網絡攻擊者總是有辦法可以滲透網路，暢通無阻地潛伏數月，同時竊取數據及知識財產。

一般常見的資安解決方案可能會發現網路中的攻擊者，但有可能伴隨著又多又雜的事件紀錄，以至於錯過了關鍵的解決時間。

入侵活動監控是一項複雜的任務，特別是如果您不想要攻擊者知道正在被監視。我們需要一種隱秘的方法，讓攻擊者難以感知目前正被監控。

在防禦攻擊上沒有靈丹妙藥，只有在早期一開始偵測到入侵行為時盡可能的及早阻止。越早及時處理越過多層防禦的某種攻擊，越能有機會大幅降低企業風險。

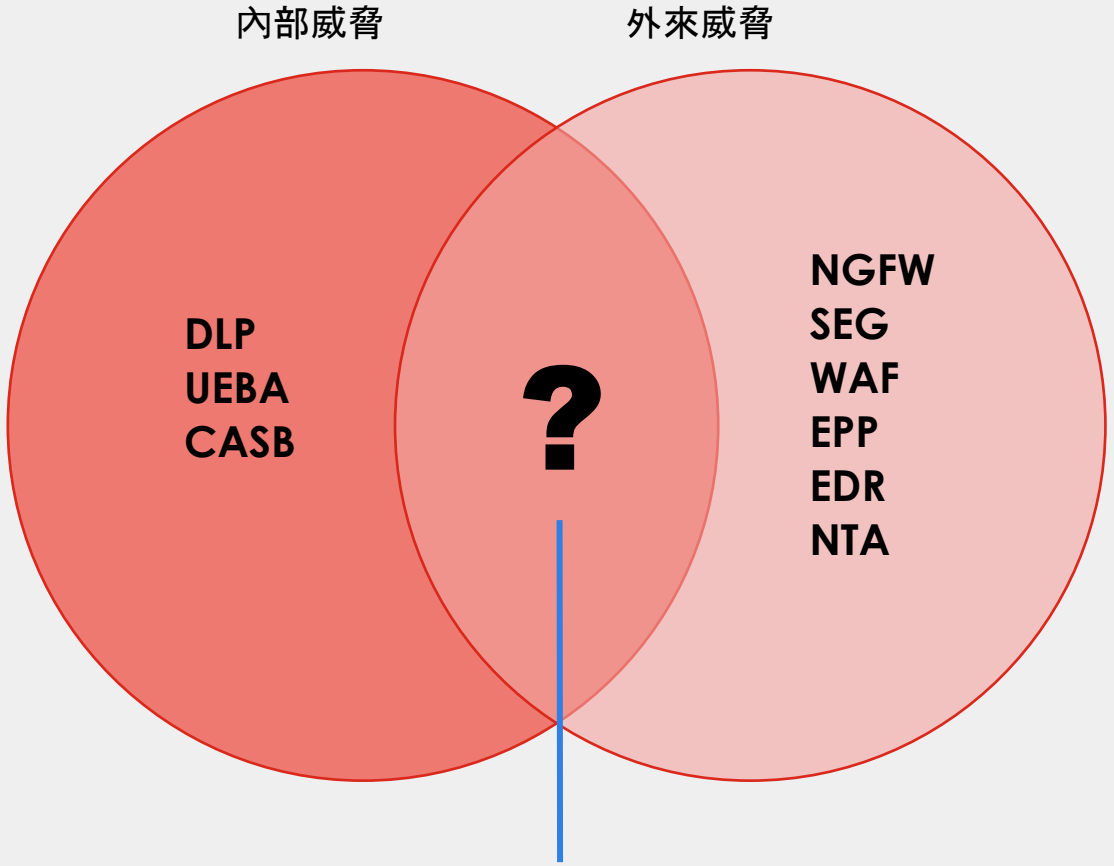
Honeypot vs. Deception

Deception Technology (欺敵誘捕技術)不是新名詞，早在 90 年代就出現了第一代的技術(Honeypot)。

Honeypot 透過模擬、或是直接採用真實的作業系統，減低其防護能力，讓它變的脆弱容易入侵後，放在防火牆外緣讓攻擊者入侵。藉以研究、觀察攻擊者的攻擊手法及策略。部署Honeypot 的管理者必須協同組織內的系統管理者或是資安管理者一起研究、分析這些蒐集到的資訊後，想辦法搭配資訊系統的設定或是變更，來達到防禦的目的。

Deception Technology 則是單一系統同時管理一群誘餌(類似早期單點運作的honeypot)，除了記錄以及分析攻擊者的攻擊手法之外，更進一步的直接與防火牆或是SIEM連動，做到即時自動隔離、阻絕這些攻擊者以達到保護資訊基礎建設的目標。

增強內外防禦解決方案之間的保護方法



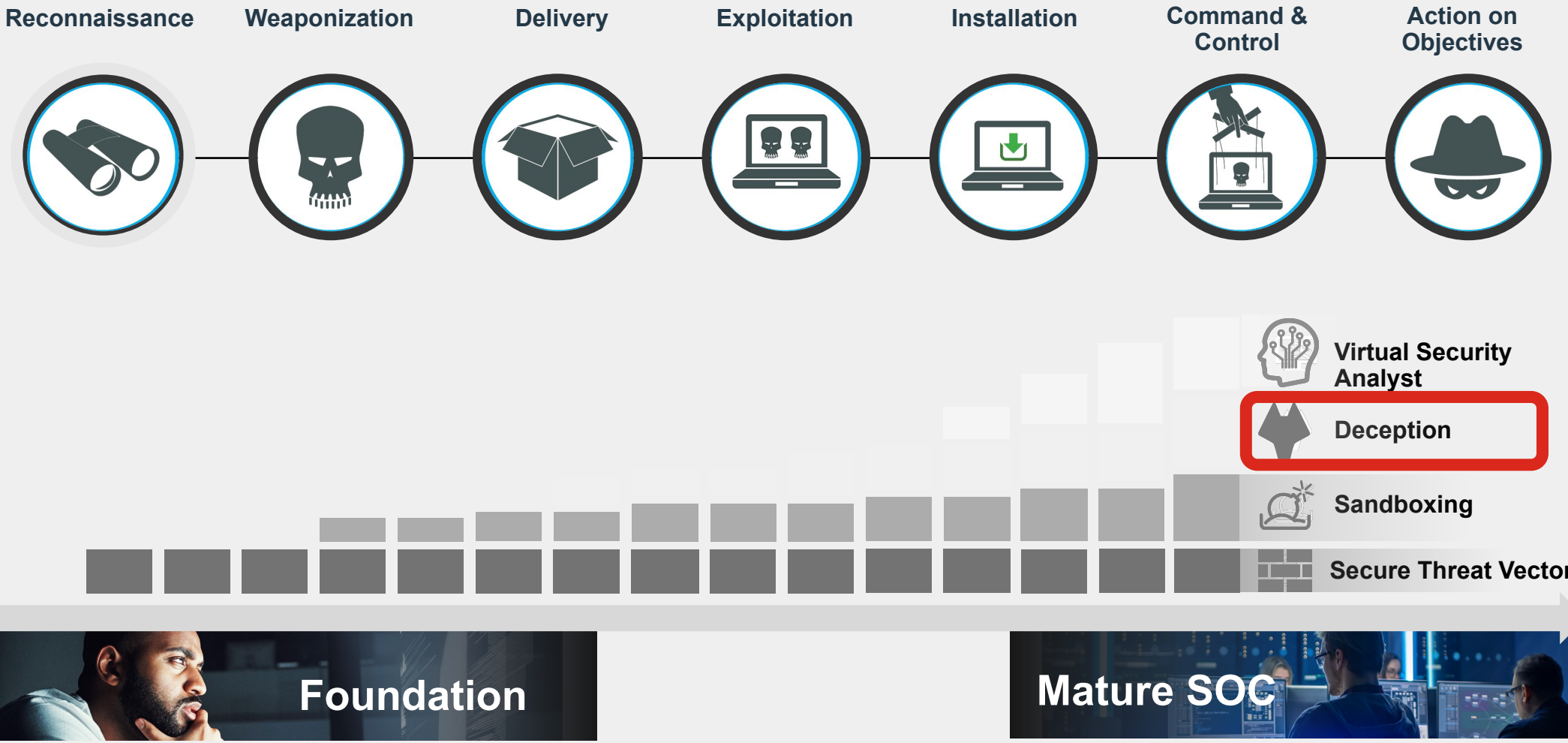
同常，資安解決方案的防禦目標分為兩個部分:

- External Threats (外來威脅)
- Internal Threats (內部威脅)

Deception is a solution for BOTH external AND internal threats

Deception 技術

SOC 成熟度模型



FortiDeceptor Technology

FortiDeceptor: Overview

FortiDeceptor 將honeypot的概念與威脅分析(threat analytics)和威脅緩解(threat mitigation)合二為一

FortiDeceptor 是一種進階威脅欺騙產品，旨在在攻擊鏈(Kill Chain)的早期，Deceive(欺騙)、Expose(暴露)和Eliminate(消除)外部和內部威脅，並在發生任何重大損害之前**主動**阻止這些威脅。

FortiDeceptor
Advanced Threat Deception

Appliance

Virtual Machine

Fabric Integration:

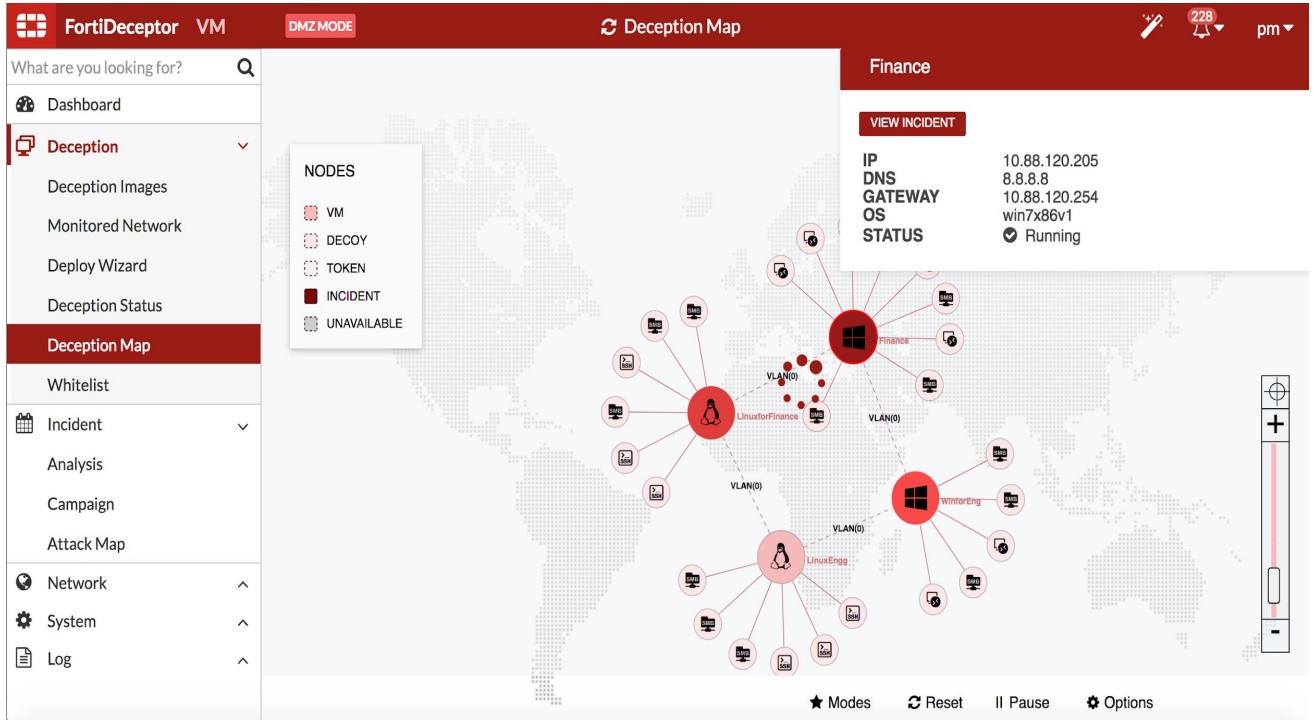
FortiGate

FortiSIEM

FortiSOAR

FortiNAC

FortiAnalyzer



FortiDceptor – 內多種建誘餌類型

Windows Decoy

- Windows 7
- Windows 10
- Windows Server 2016
- Windows Server 2019

Lures Available

- SMB
- RDP
- TCP Port Listener
- SQL (server)
- Cache Credentials
- Fake Network Connection

VPN Decoy

- FortiOS

Lures Available

- SSLVPN

Linux Decoy

- Ubuntu

Lures Available

- SSH
- SAMBA

Platform Decoys

- ERP
- POS
- PACS (medical)
- Infusion Pump (medical)
- DICOM (medical)
- GIT

SCADA Decoy & Lures

- HTTP
- FTP
- TFTP
- MODBUS
- S7COMM
- BACNET
- IPMI
- TRIXONEX
- GUARDIAN-AST
- IEC 60870-5-104
- EtherNet/IP (Rockwell)

FDC V.3.3

FortiDceptor – 內多種建誘餌類型

Windows Decoy
Windows 7
Windows 10
Windows Server 2016
Windows Server 2019

Lures Available
SMB
RDP
TCP Port Listener
SQL (server)
Cache Credentials
Fake Network Connection

Platform Decoys
ERP
POS
PACS (medical)
Infusion Pump (medical)
DICOM (medical)
GIT

VPN Decoy
FortiOS

Lures Available
SSLVPN

Linux Decoy
Ubuntu

Lures Available
SSH
SAMBA

SCADA Decoy & Lures
HTTP
FTP
TFTP
MODBUS
S7COMM
BACNET
IPMI
TRIXONEX
GUARDIAN-AST
IEC 60870-5-104
EtherNet/IP (Rockwell)

FortiDeceptor帶來好處

-AI驅動的安全營運作業

DECEIVE | EXPOSE | ELIMINATE

Decoys & Lures

- 提供豐富多樣的誘餌選擇(windows & Linux& FW & OT & IoT & ERP)
- 透過多樣的誘餌可有效拓展多種攻擊面向的防禦
- 支援自動化誘餌部署大幅降低攻擊防禦時間成本

Incident Analysis & Threat intelligence

- 自動化分析攻擊警報
- 自動化惡意軟體分析
- 自動產生有效可用的威脅情資

Fabric integration

- 透過整合Fortinet安全織網解決方案，及時針對現有攻擊或威脅進行防禦或緩解
- 提供通用性高的REST-API，可與任何支援REST-API的第三方資安解決方案整合

• System Features

- 企業中控管理平台集中分析安全報告
- 支援在Air-gapped網路中部署，不需連接Internet
- 支援SIEM整合方案

FortiDeceptor 核心技術

入侵偵測

- 以FortiGuard IPS技術為基礎
- 針對攻擊 “從”哪個誘餌或是”到” 那個誘餌進行分析

惡意軟體防護

- 針對可執行檔進行惡意軟體掃描
- 針對攻擊行為，提供PCAP檔下載

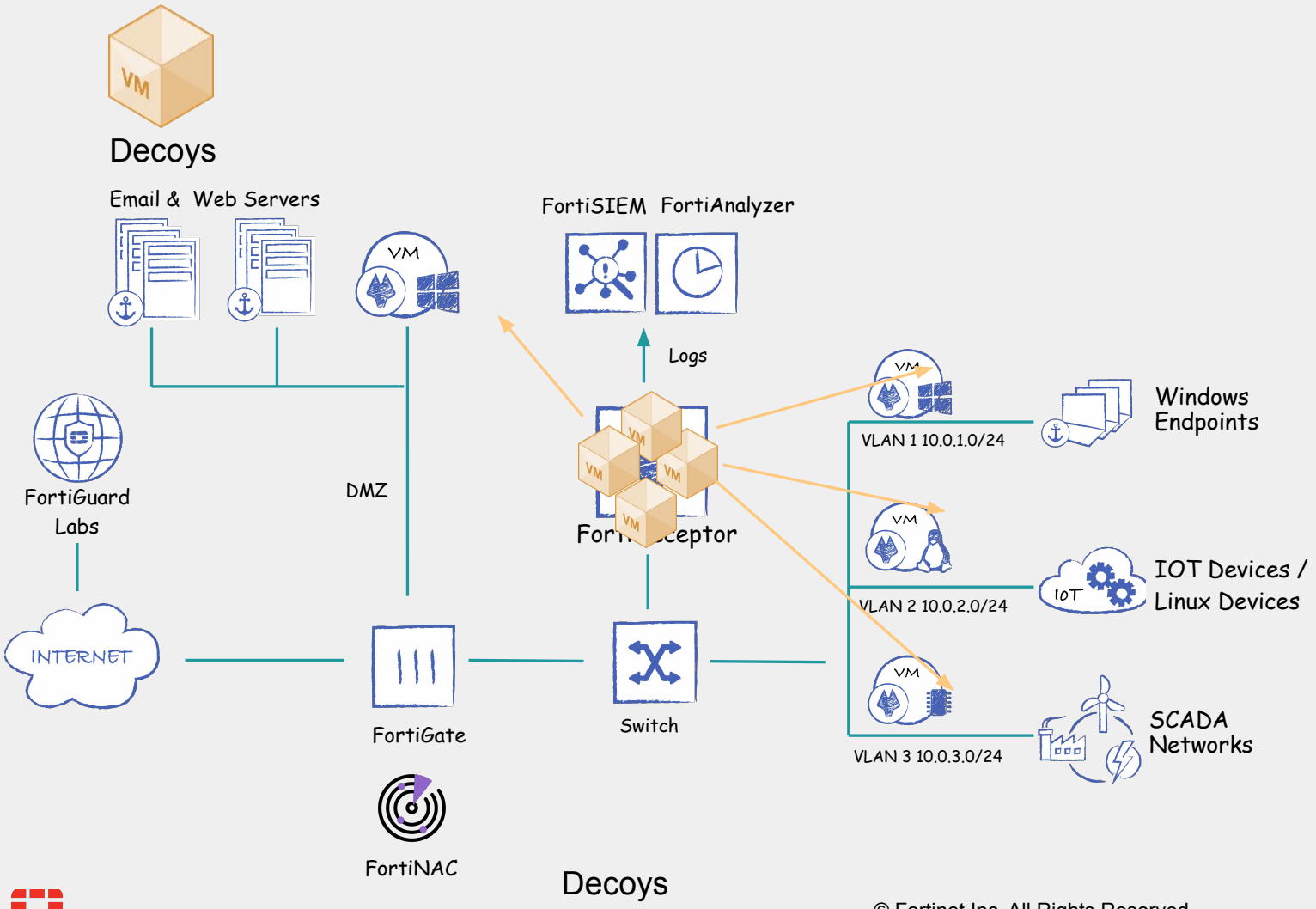
網頁威脅過濾

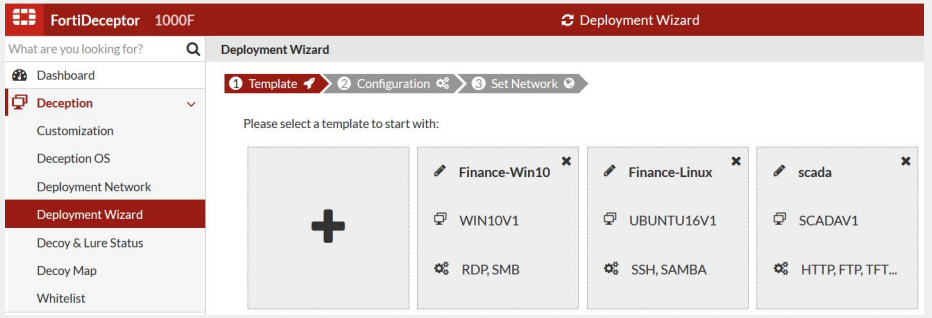
- 以FortiGuard網頁過濾引擎為基礎
- 分析誘餌到interne的網頁流量內容

- Anti-Reconnaissance Anti-Exploit Engine (ARAE) 反偵測反漏洞引擎
- Real-Time Tracking of Attackers Activities 即時追蹤攻擊者動態
- Correlate Campaigns 關聯入侵活動

FortiDeceptor 部署方式

- DECEIVE | EXPOSE | ELIMINATE

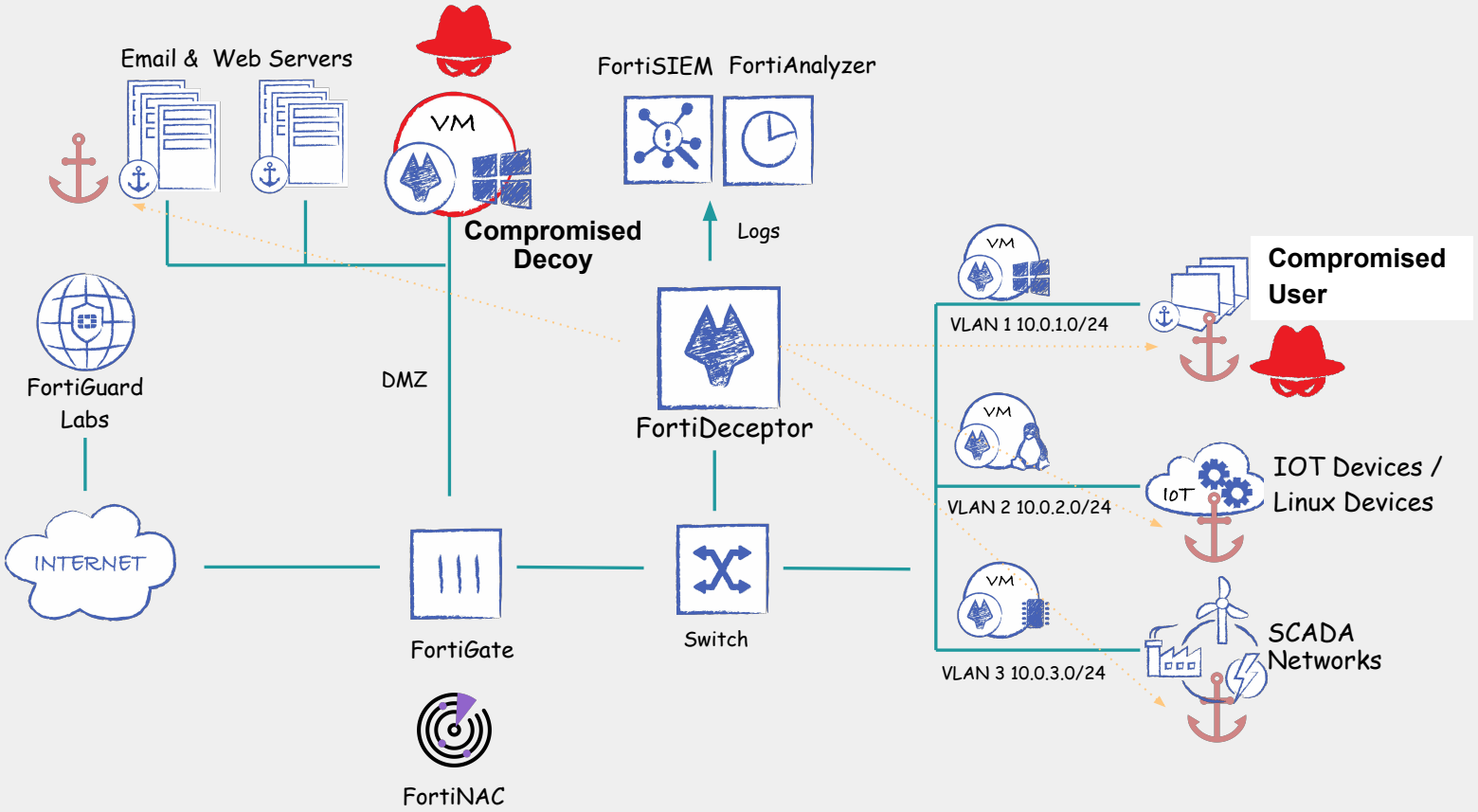


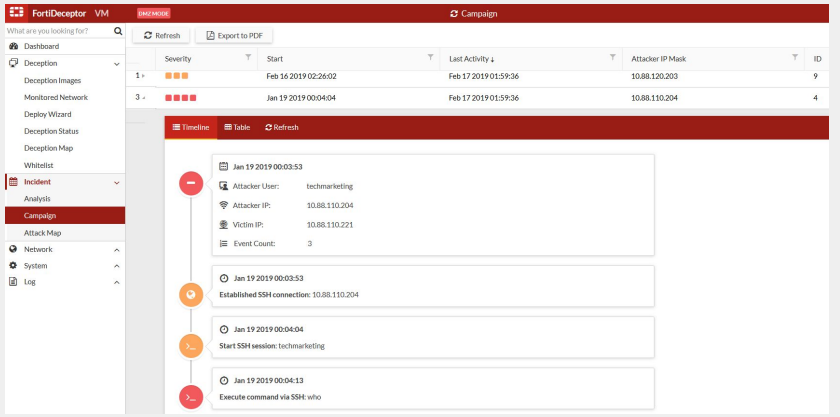


- ❑ 引誘攻擊者針對互動性高的 IT 和 OT 誘餌進行攻擊動作，且攻擊者無法區分其攻擊目標是誘餌或是真實設備
- ❑ 集中化管理並自動部署各種類型的作業系統(Windows, Linux, ICS/SCADA) 以及產生各種應用服務誘餌 (data, application /services*)
- ❑ 當應用於內網防禦時，支援 Air-gapped network，無須internet 連線

FortiDeceptor 部署方式

- DECEIVE | EXPOSE | ELIMINATE



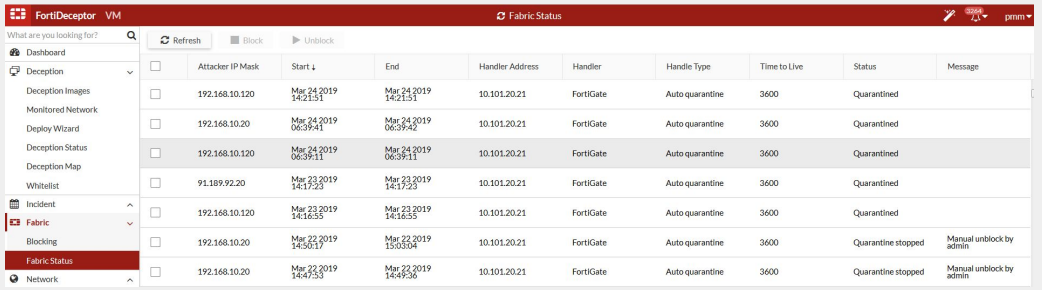


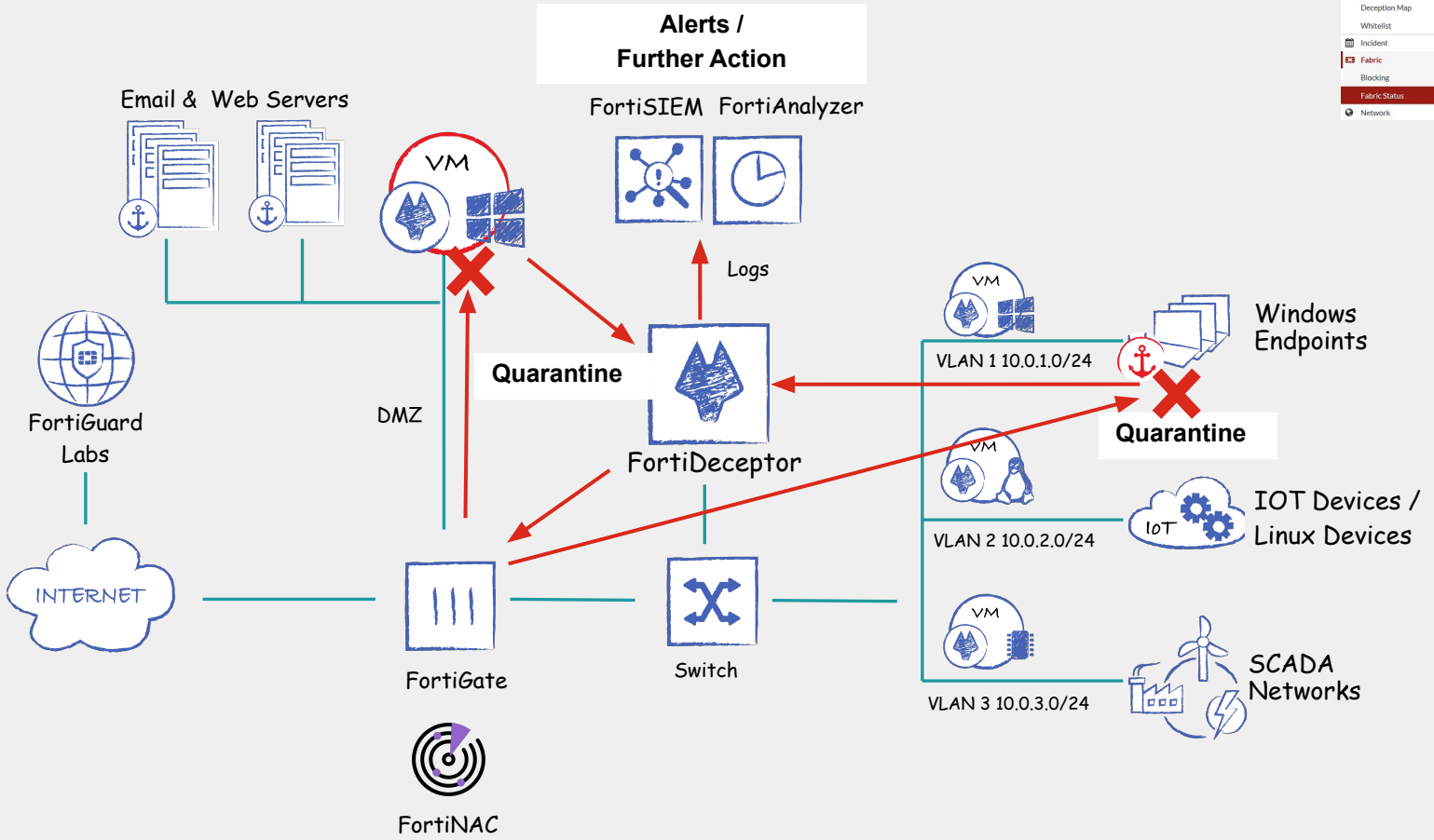
- ❑ 作為早期預警系統，並採用時間軸的模式記錄所有攻擊步驟，即時產生精準的警報
- ❑ 同時將偵測到的內外攻擊行為進行關聯分析，可於單一管理平台中顯示出更完整的威脅狀態

* Available v3.2 GA May 20

FortiDeceptor 部署方式

- DECEIVE | EXPOSE | ELIMINATE





- 依照攻擊事件的嚴重程度，在真實系統或應用服務遭受到攻擊前，可選擇手動或自動阻擋。
- 可透過與FortiGate整合，自動阻擋內部或外部惡意行為來源IP
- 與FortiNAC整合更可有效隔離有問題的設備
- 支援3rd Party以API的方式或是透過Fortinet Fabric Connector的方式整合

FortiDeceptor 使用Token技術提高保護覆蓋範圍

To increase “Deception Surface” or catch rate

Tokens For Example, RDP, SMB, SSH credentials installed on real endpoints

Example: Option 1:

假設我們的IT環境中有80台 PC/主機, 並且部署了**20個誘餌作業系統VM**

Deception Surface/Catch rate = 20/(20+80) = 20%

因此, 攻擊者有 20% 的機率會因為攻擊到誘餌進而被捕獲

Example: Option 2 (**建議做法**)

假設我們的IT環境中有80台 PC/主機, 在這80台主機上安裝了Token package, 並且部署了**20個誘餌作業系統VM**

Deception Surface/ Catch rate = (80+20)/(20+80) = 100%

100% catch rate – 只要任何攻擊者發起攻擊, 不管目標是誘餌還是真實的應用伺服器, 都會被抓到

除此之外, 任何被利用當跳板的內部電腦, 也無所遁形!

Thank you !

FortiDeceptor Use Cases

FortiDeceptor 使用情境

OT/ IoT 場域

- 透過被動足跡提供網路可視性和漏洞檢測
- 針對無法自行辨識威脅的資產，例如物聯網、SCADA 和醫療設備提供防護

東西向流量防護

- 檢測在內網橫向移動的威脅，而不是檢測出口/入口上的威脅
- 當作內網安全防護措施的最後一道防線(亦即檢視為何其他安全防護措施皆失效)
- 啟用縱深防禦和主動防禦策略

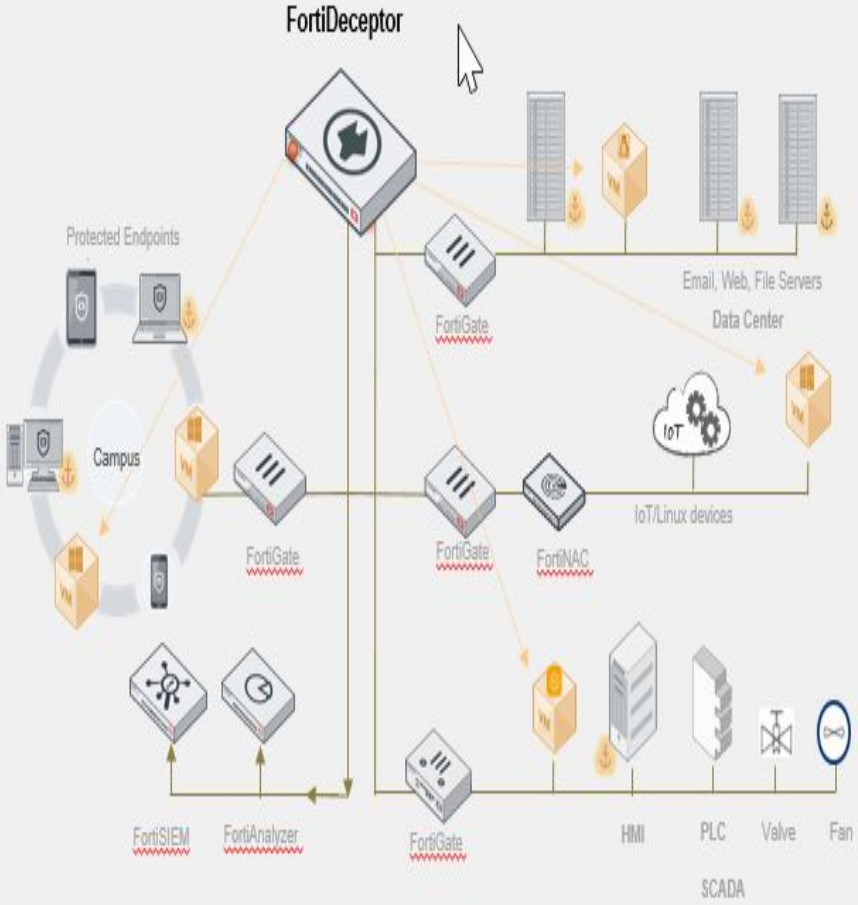
主動狩獵威脅

- 在網絡內部啟用噪聲更少的威脅檢測，以增強您的 SOC 團隊的能力
- 利用誘餌來追踪攻擊的起源
- 通過在高度監控的環境中在不被發現的前提下暗中觀察攻擊者，藉以了解攻擊者TTPs(Tactics, Techniques, and. Procedures)

Fortinet offering and business opportunity

Deception Use case – OT (Manufacture / Critical Infrastructure)

- Problem:
  - 實行用於保護 IT 資產的傳統安全防護措施非常困難
  - 現代 OT 設備具有更複雜且多樣的功能。這使它們成為惡意行為者的有吸引力的目標
- Solution:
  - 在基礎設施上部署誘餌（本質上是虛擬的設備）模擬傳統 IT 設備、OT 傳感器和控制系統。
  - 透過誘餌網路欺騙惡意攻擊者，引誘他們遠離關鍵資產並防止他們對目標網絡造成實際傷害
- Value:
  - 欺騙觸發了即時精準且簡潔有效的警報，提供了有價值的情報指標，而不是誤報，具有自動減輕威脅的能力。
  - 對現有產線網路零影響的被動解決方案，不需要任何代理或網絡拓撲更改，並且可以使用內置精靈自動化輕鬆部署。

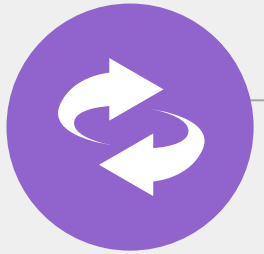


FortiDeceptor 與 FortiSIEM 的整合

Backup Slides

When Customer has no time for a real demo

Agenda



01

Deception Technology
是什麼?

02

FortiDeceptor
Technology

03

Deception Use Cases
欺敵誘捕技術使用案例

04

Deception as part of the
Fabric / ECO system
整合欺敵誘捕技術的
Fortinet解決方案介紹

05

FortiDeceptor 在OT
場景的應用

© Fortinet Inc. All Rights Reserved.

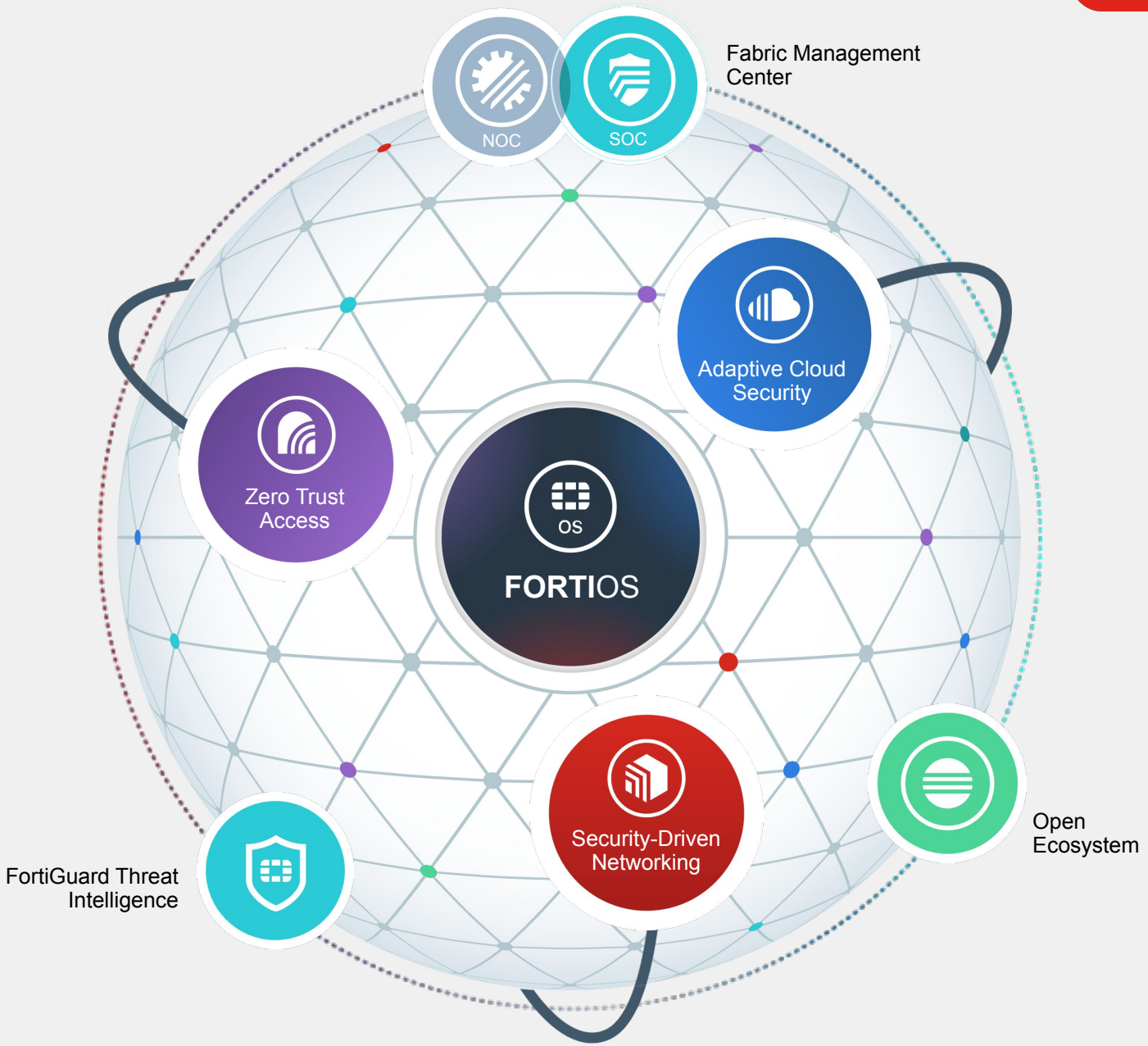
FortiDeceptor As Part of The Fabric

使用Deception的安全織網

Broad
部署在 IT 和 OT 領域的誘餌網絡以暴露攻擊者

Integrated
基於人工智能檢測的分析可作為阻礙威脅活動的早期預警

Automated
在發生不可挽回的損失之前，通過整合in-line的安全防護措施自動回應攻擊



FortiDeceptor提供良好的整合性

FortiGate

- 動態阻擋攻擊行為
- 針對OT/IoT攻擊行為提供防禦能力
- 隔離攻擊者

FortiNAC

- 自動隔離執行端點或是網路上的設備
- 針對OT/IoT攻擊行為提供防禦能力

FortiSIEM

- 可針對Token技術提供更進一步的歷史軌跡關聯分析
- 增強內部威脅的偵測能力
- 減少過多的事件資訊增強處理危機的效率

FortiSOAR

- 根據攻擊觸發矯正和補救回應
- 使用威脅情報增強MDR事件處理流程

FortiAnalyzer

- 配合IOC資料庫增強威脅感知
- 整合內建資安分析報表

Third-Party

- 透過API精靈可與任何第三方防護措施進行整合

FORTIDECEPTOR IMPROVE THE THREAT DETECTION OF THE FORTINET FABRIC

Summary

BREACHES
External and Internal threats

EARLY WARNING
High Fidelity Alerts, Redirect Attackers, Threat Analysis and Response

FABRIC INTEGRATION
Block Threats Automatically & Actionable Intelligence

BROAD COVERAGE
IT and IoT/OT Networks

EASE OF USE
Wizard-based provisioning and deployment, simple management

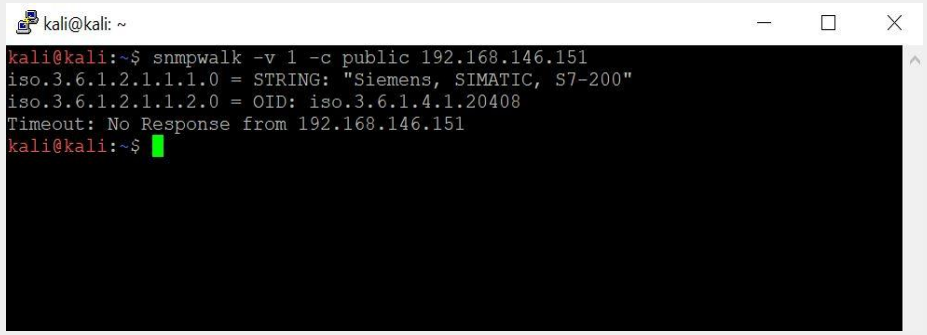
FortiDeceptor 針對 OT/IoT 場域的使用方式

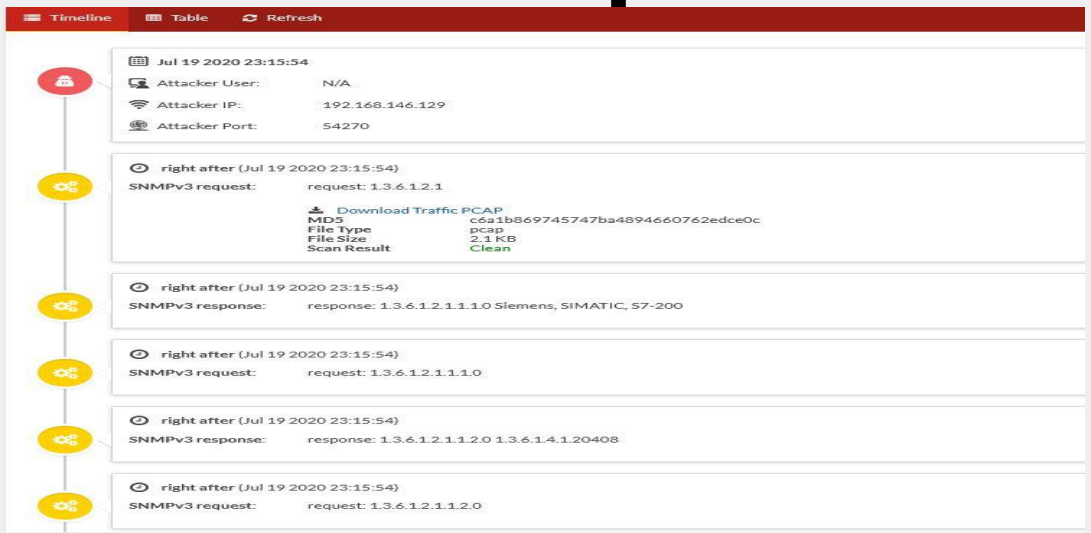
FortiDeceptor out of the box SCADA Traps

- Real-time visibility into industrial networks is the key to ICS security. To protect against external threats, malicious insiders, industrial organizations must monitor all activities - whether executed by an unknown source or a trusted insider, and whether authorized or not.
- Fortinet provides detection and mitigation capabilities to the SCADA environment by putting deception layers in both SCADA components, ICS Management & PLC side.
- SCADA Management Decoy:
  - Out of the box Real OS Decoys (Windows/Linux Server & endpoint)
  - Allow uploading your customize ICS image (ISO) and convert it automatically to an ICS decoy.
- **SCADA PLC Decoy Protocols:**
  - **HTTP**
  - **FTP**
  - **TFTP**
  - **SNMP**
  - **Modbus**
  - **S7Comm**
  - **Bacnet**
  - **IPMI**
  - **Triconex**
  - **Guardian-AST**
  - **IEC104**
  - **ENIP**

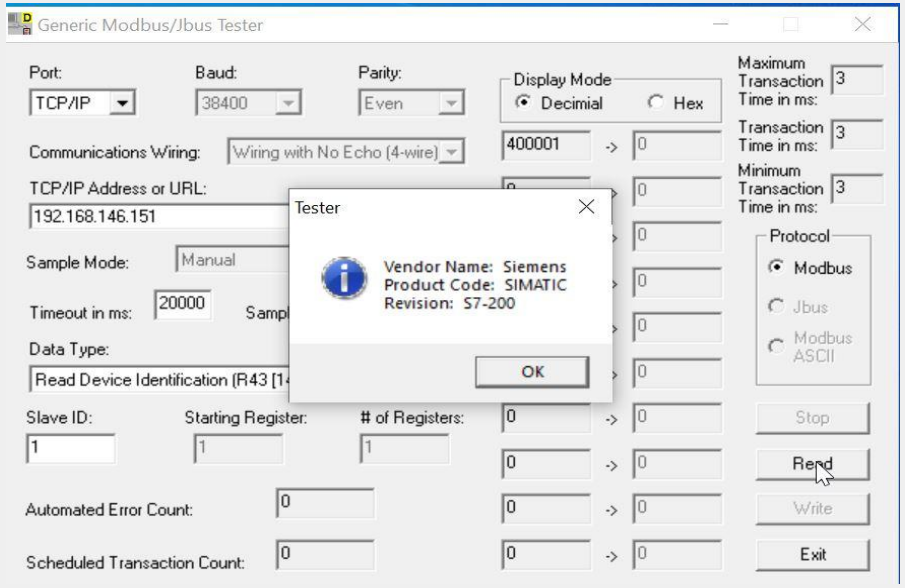
SCADA Attack Simulation – FortiDeceptor

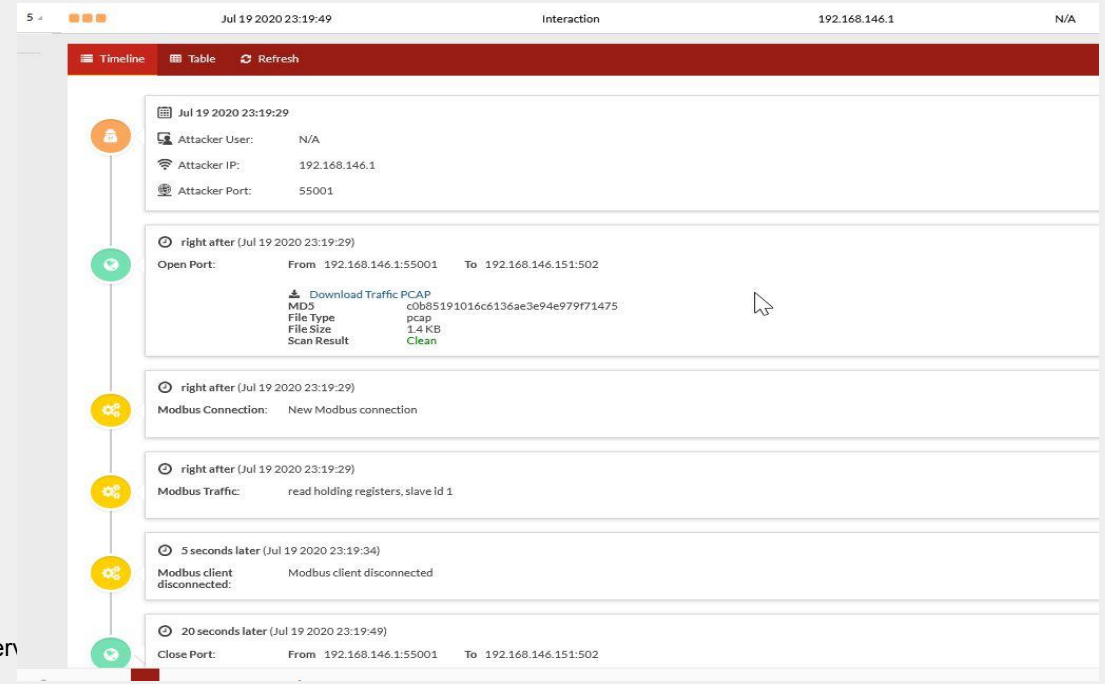
SNMP Query for stealth Device discovery





MODBUS RD/WR Query for retrieving and changing the configuration

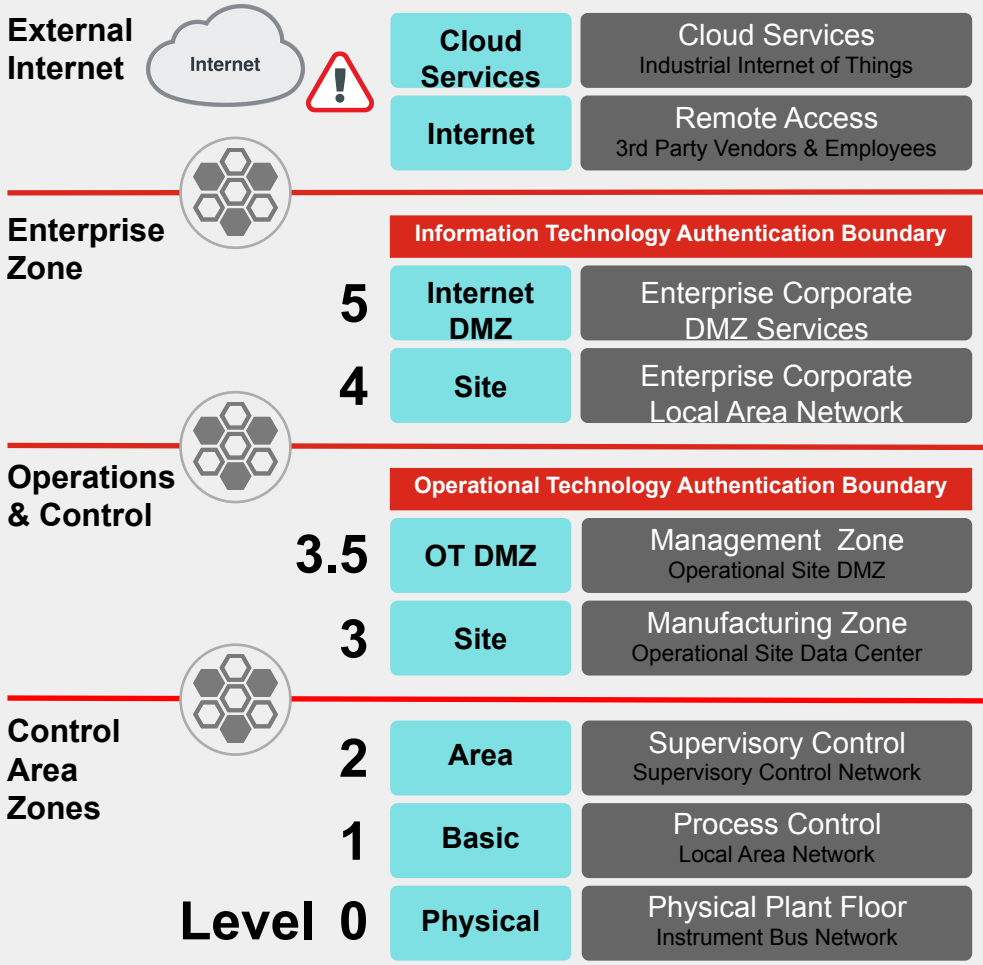




Protecting OT – Based on the Purdue Model

with the Fortinet Security Fabric

- Access Layer Segmentation
- L2/L3 NGFW Segmentation
- Web Server Protection
- Authentication and VPN
- Threat Protection
- Application Control
- Endpoint Protection
- Deception
- Sandboxing
- NOC/SOC



- Decoys in the **DMZ** infrastructure emulate **IT Servers with fake data and SSL VPN**
- **Deception Lures** deployed on the **real DMZ servers.**
- Expand the FortiEDR foot print on **assets** related to OT networks that located in the DMZ network
- Decoys emulate **IT Desktops & Servers, ERP/POS/DB/WEB critical apps** and **Deception Lures** deployed on the **real desktops & servers**.
- Expand the FortiEDR foot print on **assets** related to OT networks that located in the **IT network**
- **FortiAI** to improve **Threat analysis** and **Generate IOC**
- Decoys emulate **SCADA Management systems & application, IT Desktop & Server** with fake data and OT devices.
- Deploy FortiEDR agent on **SCADA Management systems & application, IT Desktop & Server**
- Decoys emulate **PLC, HMI, IoT sensors and legacy IT assets** such as Windows 7.
(Automation vendors such as Siemens, Rockwell, etc)

Deception Use case – Lateral Movement

- Problem:
  - Advanced attackers study the network carefully, as well as their security controls in place and learn their weaknesses until finding a way to evade detection.
- Solution:
  - Deception Decoys can be deployed in every network subnet (VLAN) across IT, Medical and OT networks
  - Deception Lures on endpoints to divert attackers to engage with decoys instead of a real asset.
- Value:
  - Rapidly detect APT & Malware & Human Threat actor post-breach activity
  - Improved productivity and reduced security manpower costs
  - Reduce time to detect and contain threats
  - NO False alarm

Deception Use case – Threat Hunting

- Problem:
  - The volume of alerts are increasing while organization facing talents shortage
  - Spending more time running after shadows than stopping real threats
- Solution:
  - Send compromised endpoint detection alerts to your SIEM for threat hunting automation using pre-configured policies.
  - Send compromised endpoint detection alerts to your SOAR for threat correlation analysis and mitigation based on high-confidence deception alerts
- Value:
  - Empowering the SOC team which alerts need to be triaged more quickly and accelerate a prompt response
  - Save time, money and resources

Discussion / Q&A