

# Oracle Webinar

## 啟動OODA資安防禦戰略

動力安全 林正榮



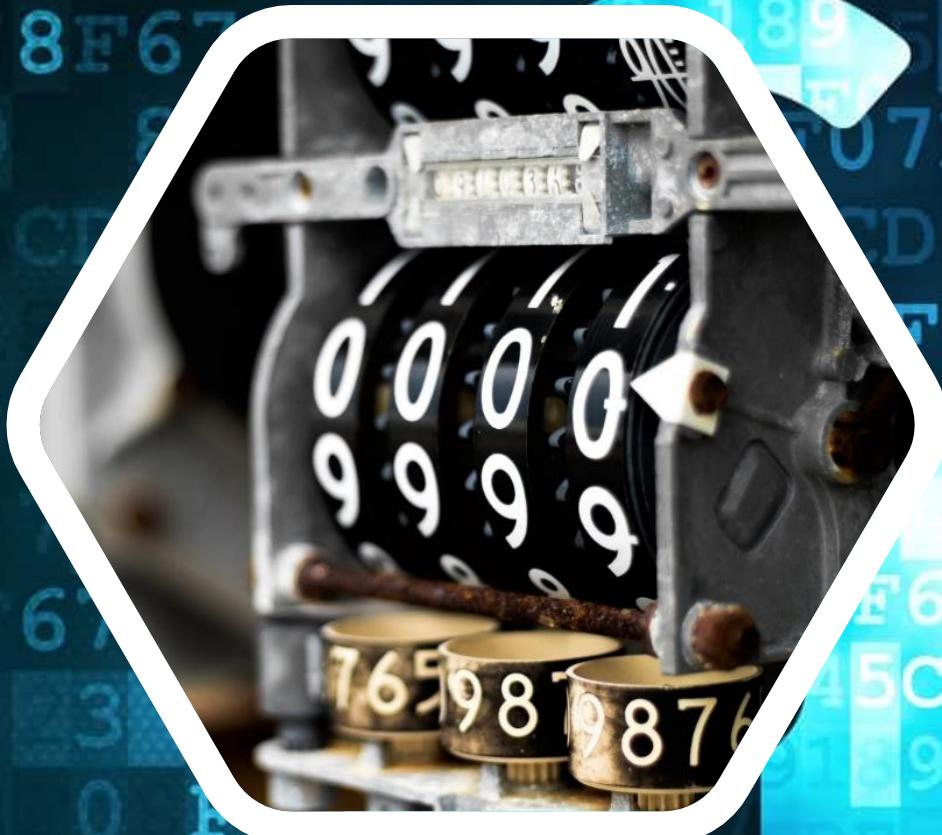
融合創新的科技夥伴



# 企業面臨的衝擊



POWER  
OUTAGES



Hacker

Covid-19



# 駭客攻擊從未停止

資安攻擊頻傳 從政府到企業都受駭

公共部門  
金融服務業  
科技業

2018年4月 高雄果菜公司  
駭客鎖住交易電腦，威脅48小時之內付贖金；果菜公司最後以比特幣支付贖金

2018年12月 台灣高鐵  
台灣駭客用手機駭入高鐵票務系統成功

2019年1月 台北市衛生局  
298萬筆台北市民個資外流

2019年6月 銓敘部  
59萬筆資安外派公務員個資遭竊

An official website of the United States government Here's how you know ▾

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > Kaseya VSA Supply-Chain Ransomware Attack

Kaseya VSA Supply-Chain Ransomware Attack

Original release date: July 02, 2021

瑞典連鎖超市COOP遭駭 全國800家實體店面暫關閉

The Central News Agency 中央通訊社  
2021年7月3日 週六 下午6:51 · 1分鐘 (閱讀時間)

Dynasafe

- 已曝光的業者就包括：
  - 臺灣電腦大廠
  - 封測大廠某集團旗下孫公司Asteelflash Group
  - 筆電代工大廠廣達
- 快訊／科技業遭駭客病毒攻擊！公司拒絕勒索 出貨些微延誤
- 美國再生能源業者 Invenergy遭勒索軟體REvil攻擊
- Evil攻擊美核武外包商
- 南韓核子研究室被北韓駭客從VPN漏洞駭入
- Colonial Pipeline 支付 1.23 億元贖金，美國政府追回逾一半

Microsoft MSRC | 安全性更新 致謝 開發人員

MSRC > 客戶指引 > 安全性更新導覽 > 弱點 > CVE 2021 34527

Windows Print Spooler Remote Code Execution Vulnerability

CVE-2021-34527

於此頁面 安全性弱點

已發行：2021/07/01 Last updated: 2021年7月3日

Assigning CNA: Microsoft

MICROPATCHES AVAILABLE

Oday: CVE-2021-34527  
„PrintNightmare“  
Print Spooler Remote Code Execution  
MICROSOFT WINDOWS  
Patch size: 1 instruction PATCH

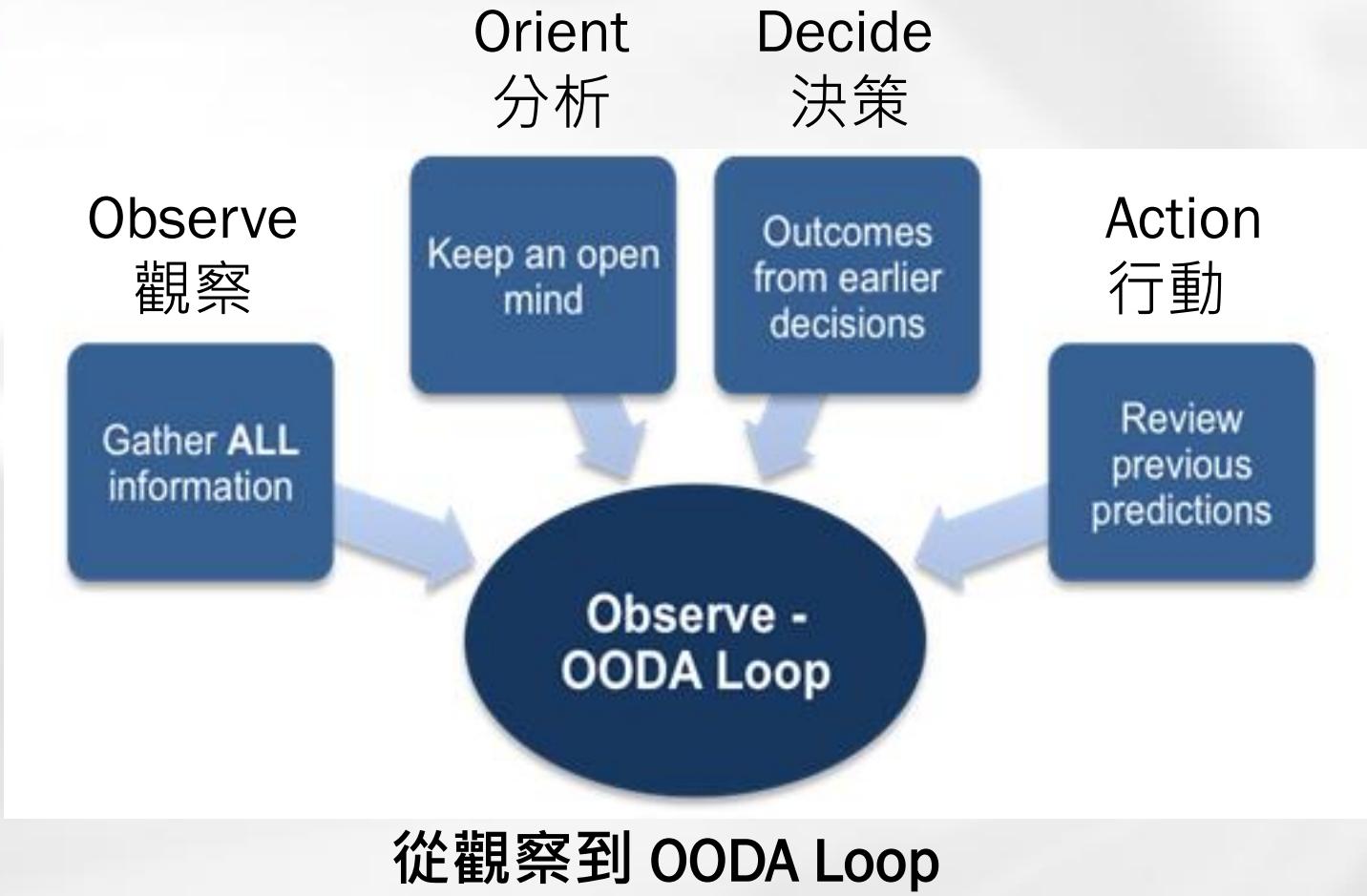
# John Boyd上校的OODA



## John Boyd' OODA：如何贏得無處不在的競爭與對抗

**Observe:** 弄清楚什麼會贏  
**Orient:** 確定自己目標  
**Decision:** 切斷對手一切聯繫  
**Action:** 在敵方的OODA循環內採取行動，使敵人最終陷入戰略性癱瘓；對於己方的OODA循環；通過實現決策力與執行力的整合來獲得競爭優勢，提高與複雜環境的互動能力。

## OODA 改變傳統SOC運行結構



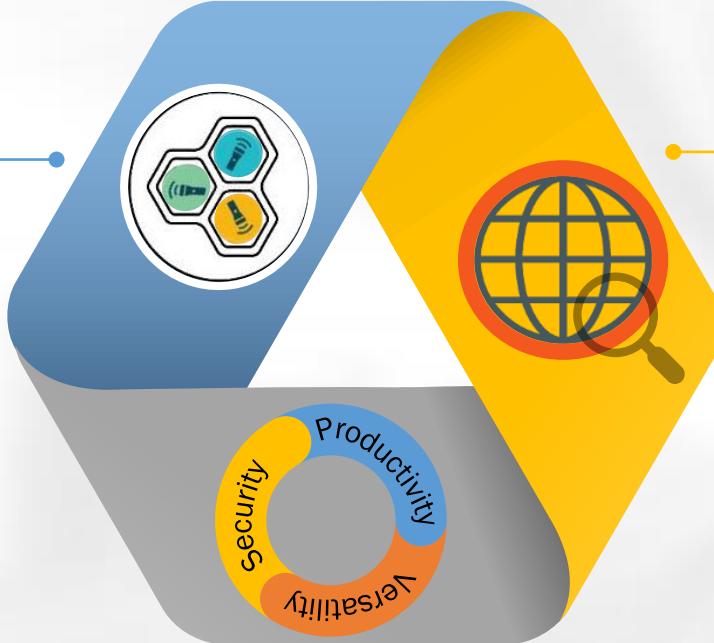
- Trigger  
有防毒還是會中毒
- Scope  
駭客總是知道誰沒補丁
- Sensors  
多少偵測點才夠
- Historical Data  
歷史資料難查
- Threat Intelligence  
威脅情資無從比對

# OODA Loop 是快速調整資安策略的方法

# OBSERVE – DynaEyes 持續及自適切風險評估

## 內眼監控- 即時掌控

- IOT/OT 安全性
- 即時斷網隔離



## 外眼監控-風險評估

- 自我檢視由外而來網路資安風險
- 隨時修復風險

## Dynasafe Managed Detection & Response Service

- 端末資安防護
- 動安 Security 團隊

# ORIENT – DynaDI Security & Purple Team

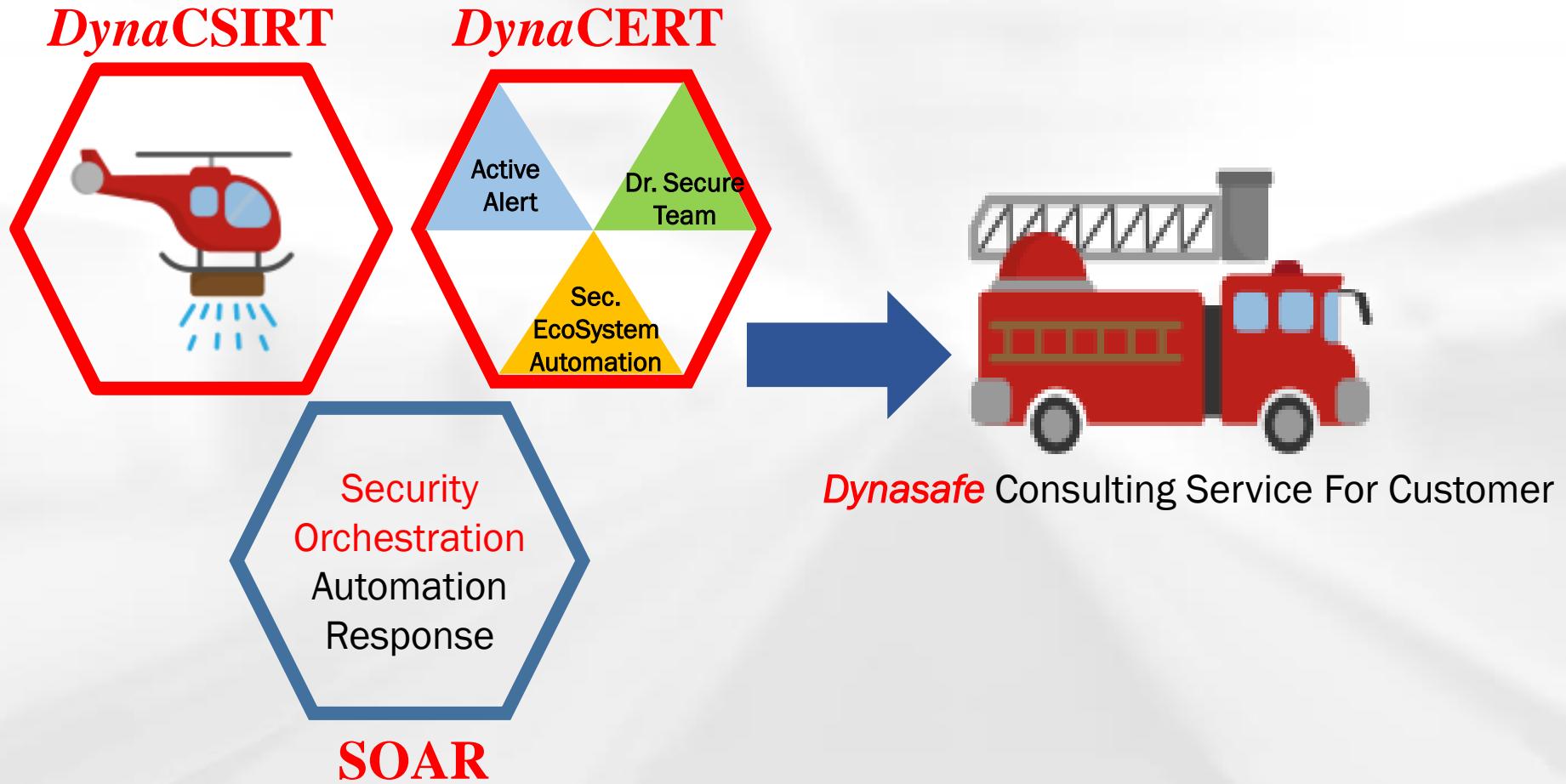
Security Big Data-  
*DynaDI* Security  
Team



Dynasafe Purple Team



# DECIDE – DynaCSIRT & DynaCERT



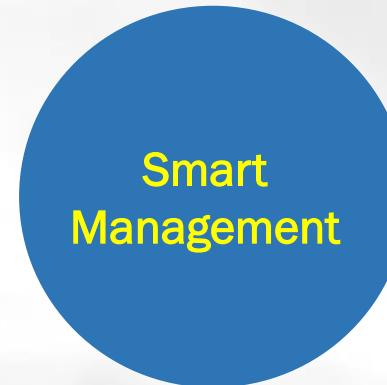
# ACTION – DynaECP & DynaCONSULT



- 用戶自助服務，減少IT維運負擔
- 流程標準化及自動化，



維運可視化



高可用、自動化、及易於管理。

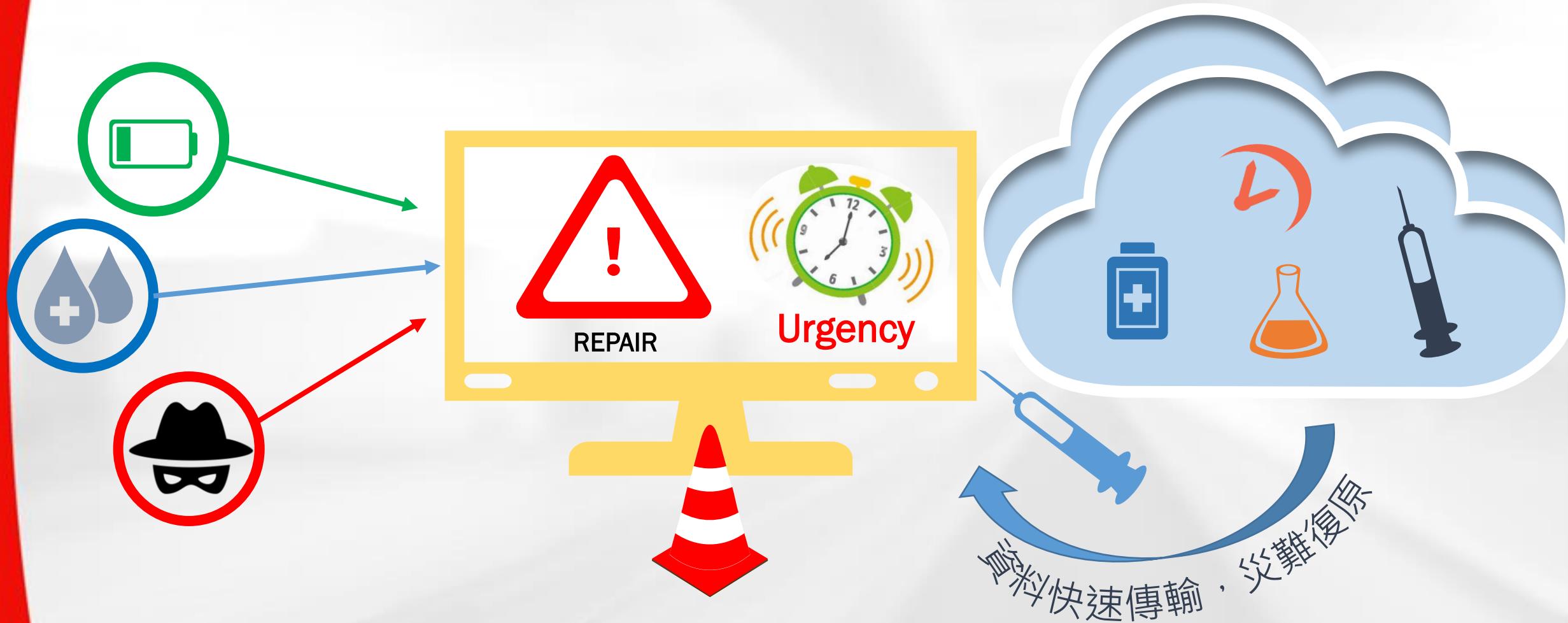


- 服務目錄減少了交付服務的時間和成本
- 達成IT與企業目標一致
- 收益最大化



Consulting Service

# 營運不中斷-避風港計畫·災難復原



科技戰略・智能防禦・掌握未來

## Dynasafe OODA

