Digi Win TV

ESG"碳盤"查了沒？

企業"減碳"必備良方

EP11

LIVE 2023/9/08 PM15:00-15:40

保護客戶、生產與營運安全，企業
永續經營不能失守的資安基礎建設！

講師: 鼎新電腦 數位科技運營中心 林崇裕 副理

2023年ESG必修課 守護之章 8/25起雙周五下午15:00~15:40

鼎新電腦 40

保護客戶、生產與營運安全
企業永續經營不能失守的資安基礎建設!

數位科技運營中心

林崇裕

2023.09.08

資安治理被重視程度…

資安廠商 Delinea 針對位於澳洲、紐西蘭、新加坡、馬來西亞、印度、台灣、香港的 2,000 名企業資安決策人員進行問卷調查，發現**多數企業並未將資安視為公司業務策略的一部分**。

畫面及內容取自TWCERT/CC 2023.05.15 發佈資料

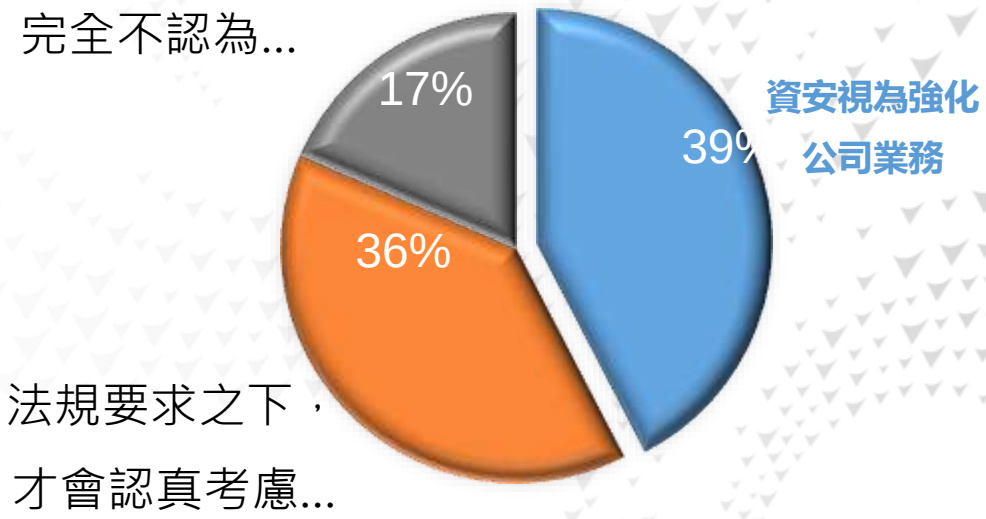
…資安治理被重視程度…

企業資安決策人員中，只有

39% 認為所屬公司的領導階層，將資安視為強化公司業務的一環；

有 36% 的公司更是只在監管與法規要求之下，才會認真考慮資安。

也有 17% 的公司完全不認為資安是該公司的工作重點。



資料內容取自TWCERT/CC
2023.05.15 發佈資料

…未重視資安造成的危害

導致

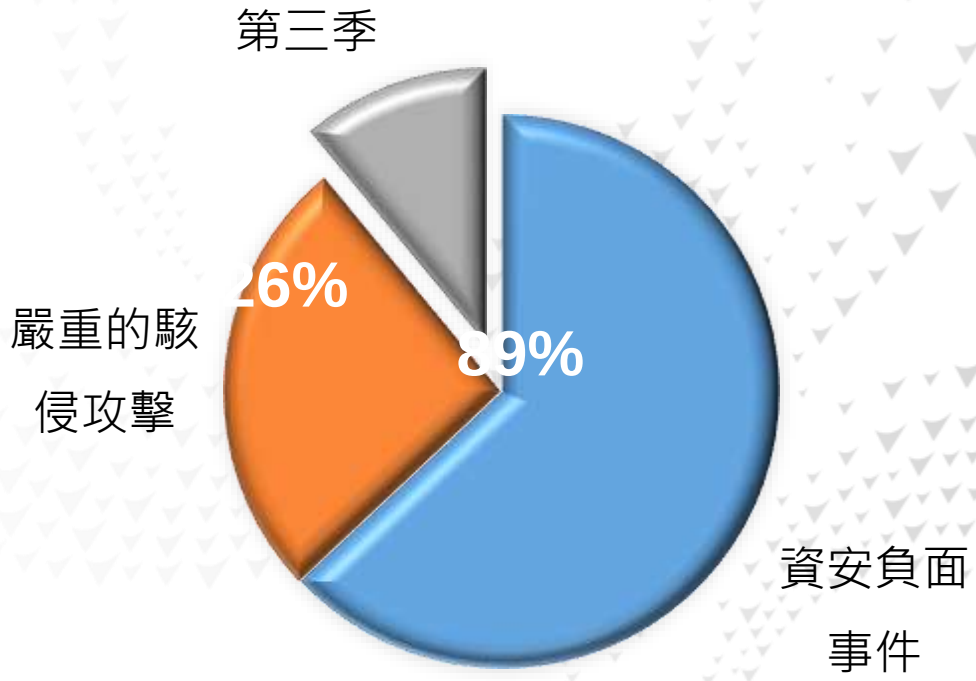
35% 公司延遲在資安人員與軟硬體設備方面的投資、

34% 公司發生資安策略決策的延遲，

更有 27% 公司因而增加了非必要的費用。

有 **89% 的企業因而發生了資安負面事件**，也

有 **26% 公司遭到更為嚴重的駭侵攻擊。**



資料內容取自TWCERT/CC
2023.05.15 發佈資料

供應鏈資安事件

iThome

新聞

汽車大廠Toyota宣布日本14家工廠停工，起因疑似零件供應商遭到網路攻擊

日本汽車大廠豐田（Toyota）宣布於3月1日當地14家工廠停工，原因是零件供應商小島工業（Kojima Industries）遭駭

文/ 周峻佑 | 2022 03 01 發表

288 分享

TOYOTA 企業情報 ニュースルーム モビリティ サステナビリティ 投

2022年02月28日

2022年3月 国内工場の稼働について（2/28時点）

お知らせ, 工場稼働

印刷

国内仕入先（小島プレス工業株式会社）におけるシステム障害の影響を受け、3/1（火）（1直・2直ともに）国内全14工場28ラインの稼働を停止することを決定いたしました。お客様及び関連仕入先の方々には、様々なご不便をおかけすることをお詫び申し上げます。

畫面及內容取自ITHOME 2022年報導

員工洩密事件

iThome

前員工意圖爆料，特斯拉7.5萬員工個資外洩

意圖向媒體爆料特斯拉自駕系統問題內幕的特斯拉前員工，卻也導致這家電動車大廠員工陷入個資外洩風險

文/ 林妍溱 | 2023-08-22 發表

讚 52 分享

畫面及內容取自ITHOME 2023.08.22日報導

勒索軟體攻擊事件

iThome

四分之一曾遭勒索病毒襲擊的醫療機構營運被迫全面停擺

趨勢科技研究指出供應鏈是資安風險的主要來源

文/ 廠商新聞稿 | 2022-10-26 發表

趨勢科技研究指出，全球57%的醫療機構曾在過去三年中遭到勒索病毒襲擊，其中更有四分之一的醫療機構營運被迫全面停擺。

畫面及內容取自ITHOME 2022.10.26日報導

資安治理需要由上往下紮根，植入企業根本

經營決策層支持

給錢、給人、給支持

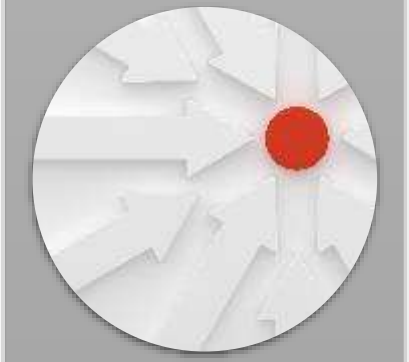
製訂並落實管理程序

各項計畫、辦法、作業程序之擬訂及執行

技術措施

導入設備、系統、工具、平台，協助識別、保護、偵測、回應、復原等管理機制，並協助收集量化指標

企業的資安治理該如何

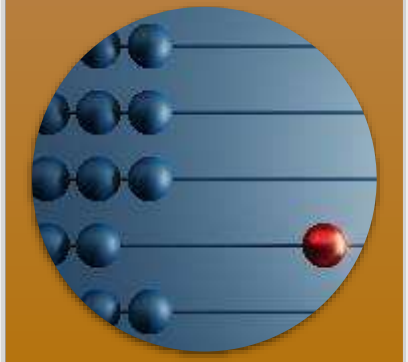


建立組織及政策

- 可參考 ISO27001
- 及 上市櫃資安管控指引
- 制定政策及作業程序

合規及法遵盤點

- 企業應遵守的
- 合約的資安要求
- 應遵守的法律
  - 營業秘密法
  - 個資法
  - GDPR
  - …..



風險評估及管理

- 面對可能風險
- 面對新的攻擊方式
- 既有防護機制，當風險發生時，是否為可接受損害
- 需改善項目之管理

教育訓練及供應鏈要求

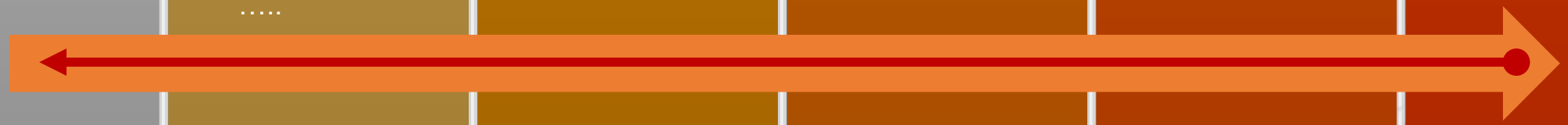
- 資安政策佈達
- 資安意識提升
- 機敏保密機制說明
- 各作業程序說明

技術性措施

- 可參考 ISO27002
- 及 上市櫃資安管控指引
- 導入適合之技術方案

稽核審查

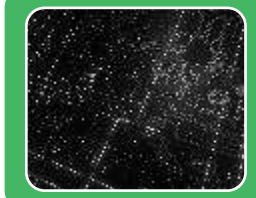
- 資安目標審查
- 作業程序遵守稽核
- 供應鏈廠商資安稽核
- 缺失發現及提報



企業資安常見不足

資安訓練

高風險弱點偵測及修補



網路分割及防護

傳輸加密

特殊存取權限管理

雲服務之資訊安全

資安維運

資安訓練

資安通識訓練

執行時機:

.新人到職

.定期執行

訓練內容可包含:

.公司資安政策及各項規範

.網路及各項服務之資安認知

.駭客攻擊手法及危害

.....

資安專業訓練

執行時機:

.定期執行

訓練內容可包含:

.認證課程(ISMS、PIMS、...)

.資安專業研習課程

.....

高風險弱點偵測及修補


弱點掃描
初次掃描
IP清單
客戶修補
讓高風險的弱點消失
(YES or NO)
重複掃描
確認修補完成
(YES or NO)


滲透測試
初次檢測
資通系統 網站
✓ 弱點掃描
✓ 手動指令入侵
✓ 攻擊工具
客戶修補
讓高風險的弱點消失
(YES or NO)
重複掃描
確認修補完成
(YES or NO)

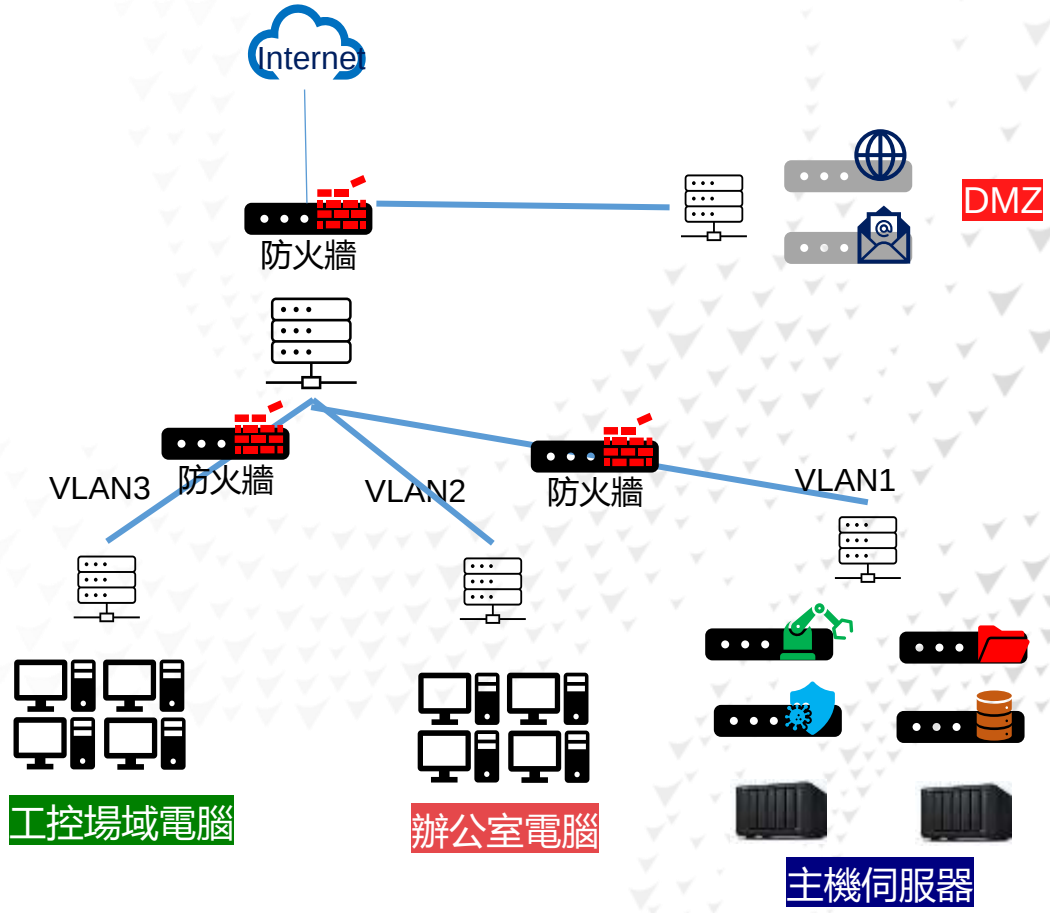
網路分割及防護

分割防禦基本分割原則：

對外服務需分割，風險較高的主機服務，應獨立於DMZ區，並加以控制、防止被入侵後快速內部擴散。

重要服務需分割，重要服務應該網路分割，並加以控制措施，增加防禦縱深。

工控場域需分割，重要生產場域，應網路分割，並加以控制措施，防止辦公室網路遭滲透後，快速內部感染至工控場域。



傳輸加密

對外部提供的服務，需以加密方式進行傳輸，常見的服務，如：

網頁服務：

HTTP → HTTPS

郵件服務：

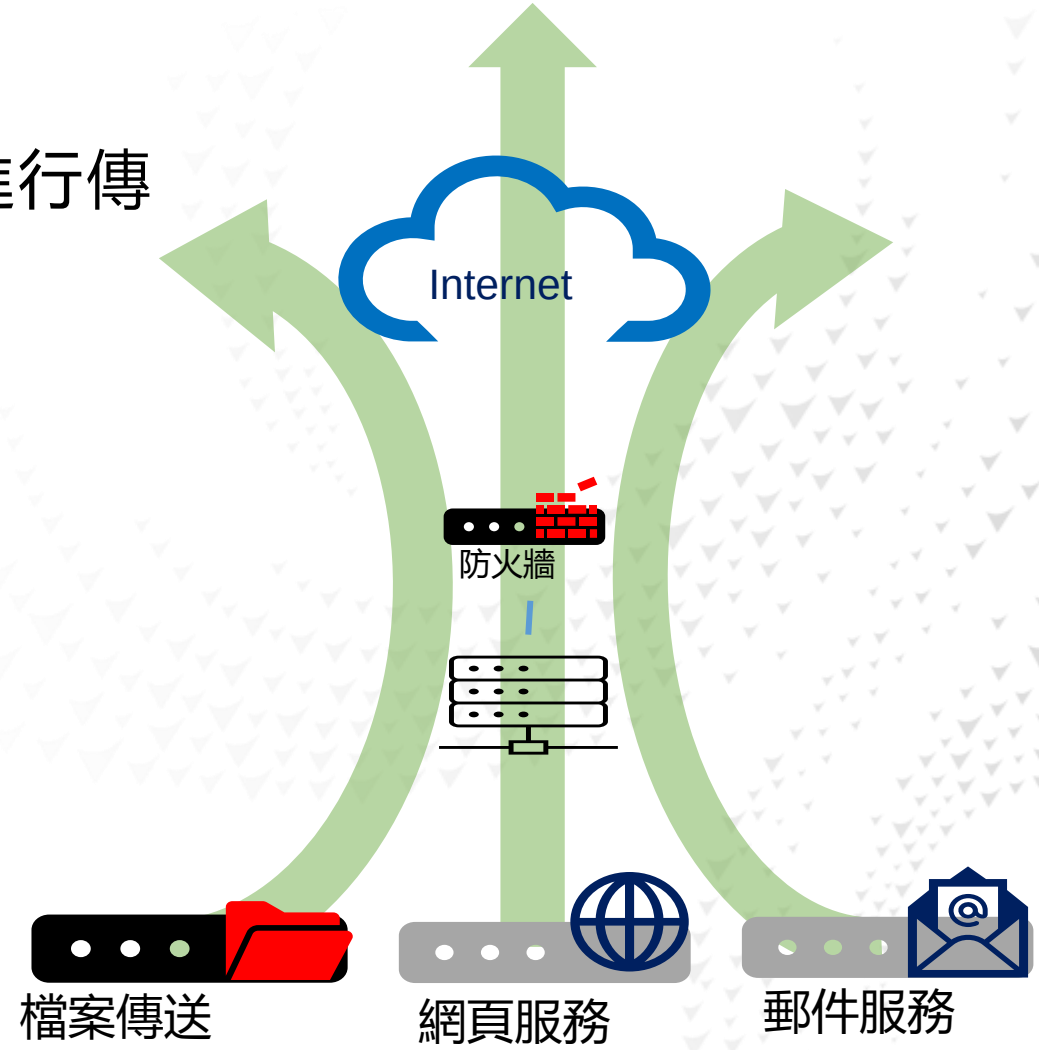
SMTP→SMTPS

POP3 → POP3S

IMAT → IMAPS

檔案傳送：

FTP → FTPS、SFTP



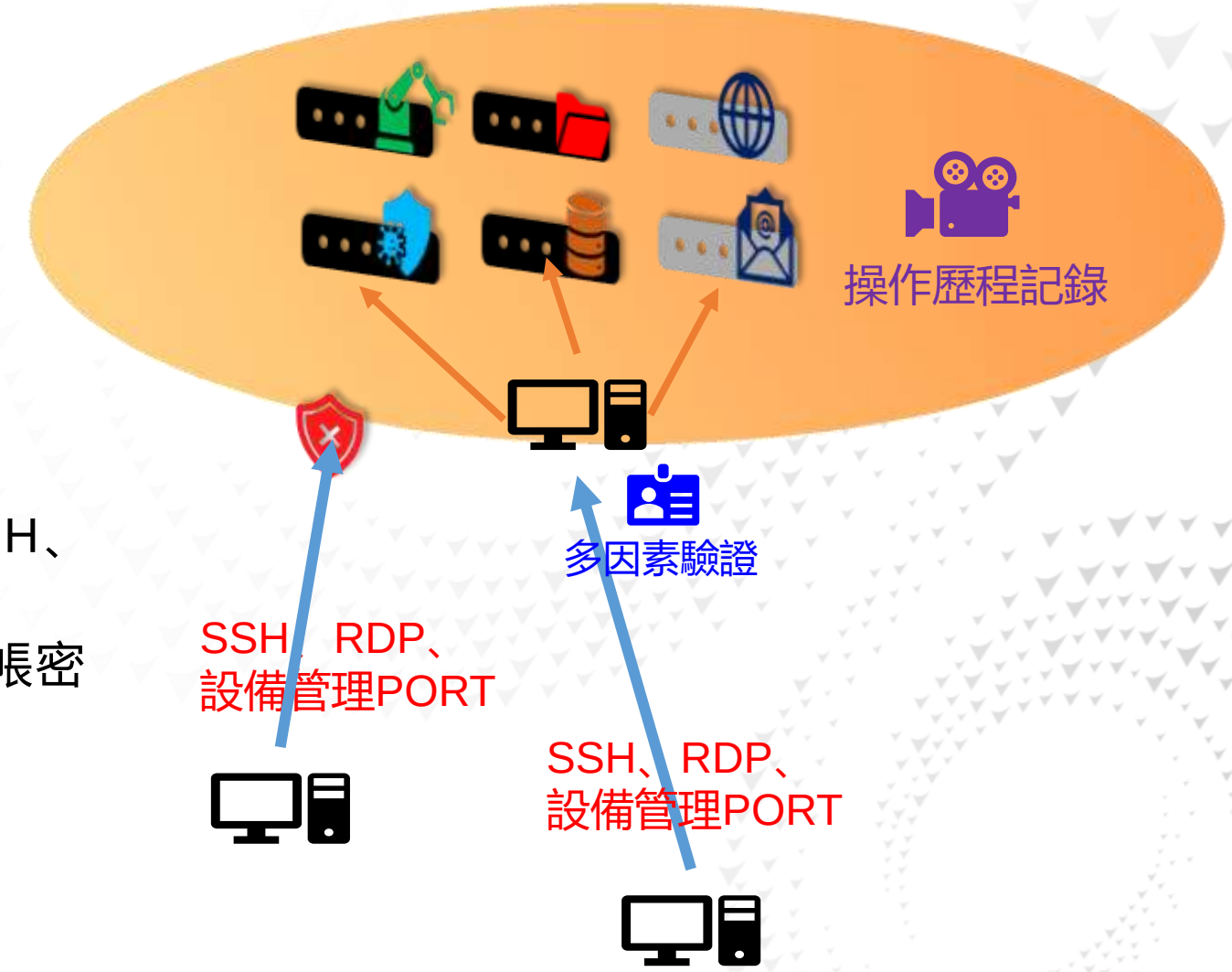
特殊存取權限管理

特權帳號:

- 網域管理帳號
- 網路服務管理帳號
- 應用程式管理帳號

管控方法:

- 限制管理存取 (限制管理服務連接，SSH、RDP、設備管理PORT)
- 管理權限帳密保護 (主機代登入，管理帳密不外洩)
- 多因素身份驗證 (管理人員身確認)
- 操作歷程記錄 (事後稽核查證)



雲服務之資訊安全

不同類型的雲端服務（SaaS、PaaS 和 IaaS），不同的資安防禦考慮因素：

SaaS （軟體即服務）	PaaS （平台即服務）	IaaS （基礎設施即服務）
身份驗證：強化身份驗證，帳密外加多因素驗證。 **數據加密**：加密存儲的數據。 **服務商提供之安全標準和合規性** **監控和日誌**	**應用程式安全：**確保適當的安全性，包括編碼審查、漏洞掃描和安全測試。 **環境隔離：**隔離應用程式和環境，以防止安全漏洞在不同的應用程式之間擴散。 **安全開發：**遵守安全開發，並使用強化的身份驗證方法。 **服務商提供之安全標準和合規性** **監控和日誌**	**網絡安全：**包括防火牆、入侵檢測系統和虛擬私人網絡（VPN）等。 **主機安全：**確保虛擬機器和主機受到保護，包括及時應用安全更新和漏洞修補。 **存儲安全**：環境中的數據存儲進行加密和適當的存取控制。 **服務商提供之安全標準和合規性** **監控和日誌**

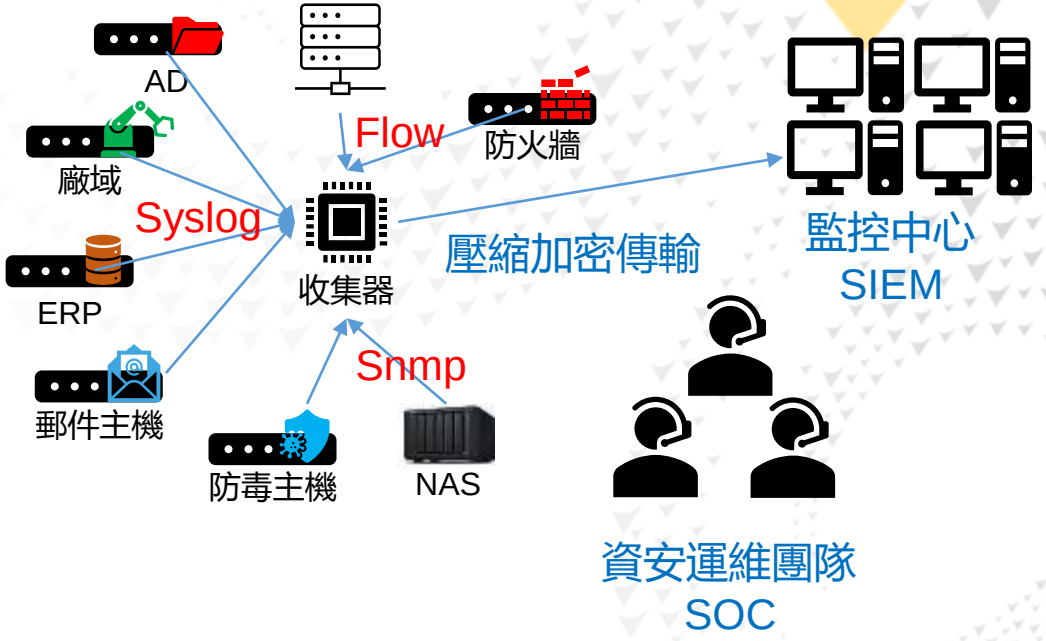
資安維運

資安維運的工作內容：

狀態監控、組態管理，持續監控組織的資訊系統和網絡，以檢測異常活動、不尋常的流量或潛在的攻擊跡象。。

情資掌握、事件調查，參與威脅情報分享和合作，以瞭解最新的威脅趨勢，負責進行調查，以確定事件的性質、影響範圍和可能的起因。

威脅通報、應對,提交資安事件的報告，向組織的高級管理階層和相關當局提供必要的資訊，並採取措施來應對檢測到的威脅。。



企業永續經營不能失守的資安

資安是為保護企業重要之資訊資產，使其**遭受風險威脅甚至是攻擊**時，能有**足夠**的保護、偵測、回應，以及復原機制、一旦資產之 機密性、完整性、可用性 遭受破壞時，能適時的被控制及因應。

不同產業、規模、會面臨不同程度的資安威脅以及利害關係人的期望。

在面對契約、法規及供應商要求時，把資安植入企業根本文化 才是負責任的做法。

鼎新電腦 40

匯報完畢敬請指教

Thanks

數 智 問 鼎 ▼ 捷 足 先 登

就享知 DigiKnow 平台，新會員掃碼註冊

新會員 掃碼註冊

邀請碼：00970

會員專享： 重點精華與回看，講義下載

訂閱頻道

[ESG碳盤查全攻略]

鼎新提供全方位解決方案
支持企業整合規劃ESG三面向需求

鼎新LINE好友每月抽好禮

一對一
諮詢服務

活動消息
隨時掌握

產業資訊
一把抓

每月抽
專屬好禮

掃碼掃起來

抽好禮5選1的即享券耶!!
(王品、家樂福、百貨、7-11等)