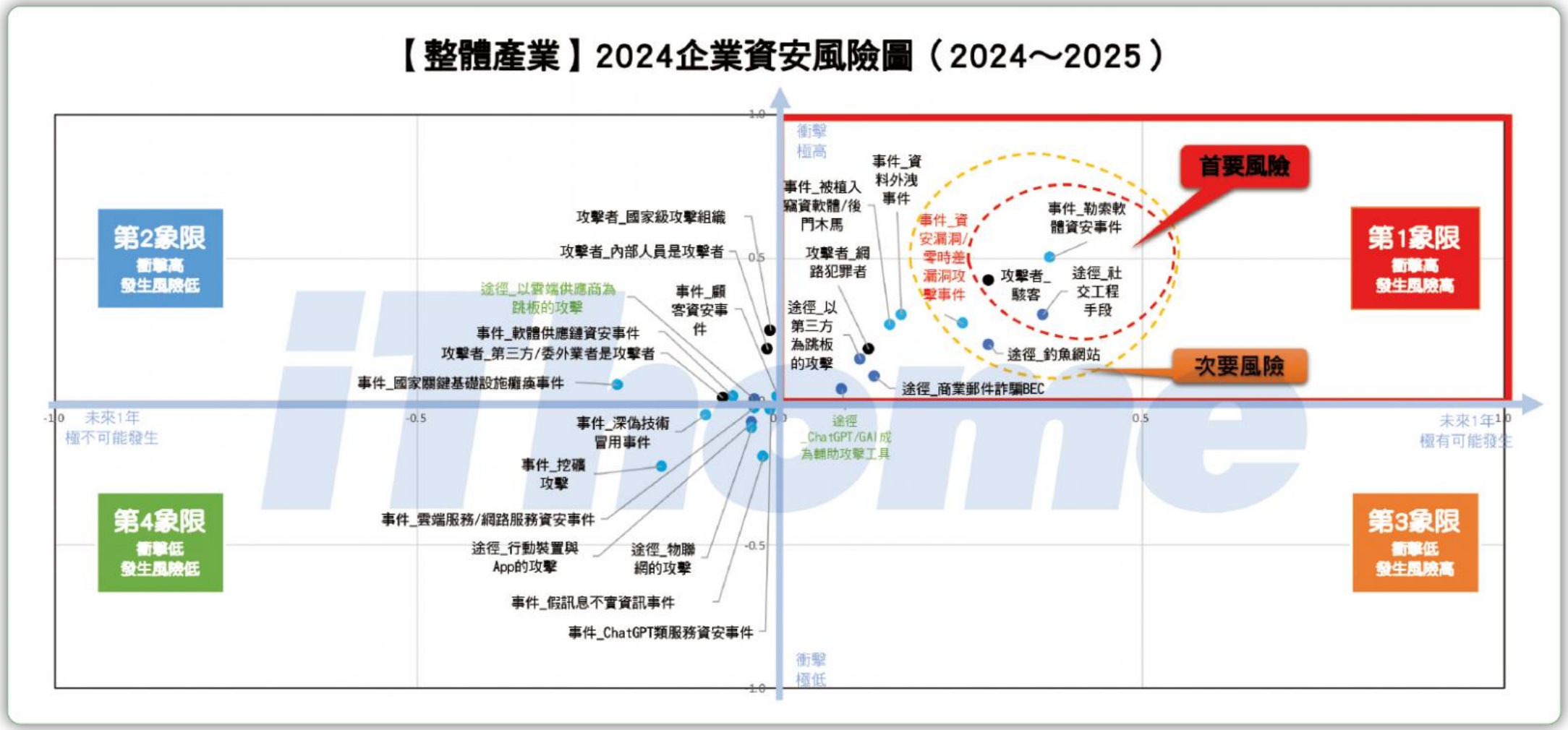
資安事件案例分享與實作

微智安聯 魏宏吉 技術長

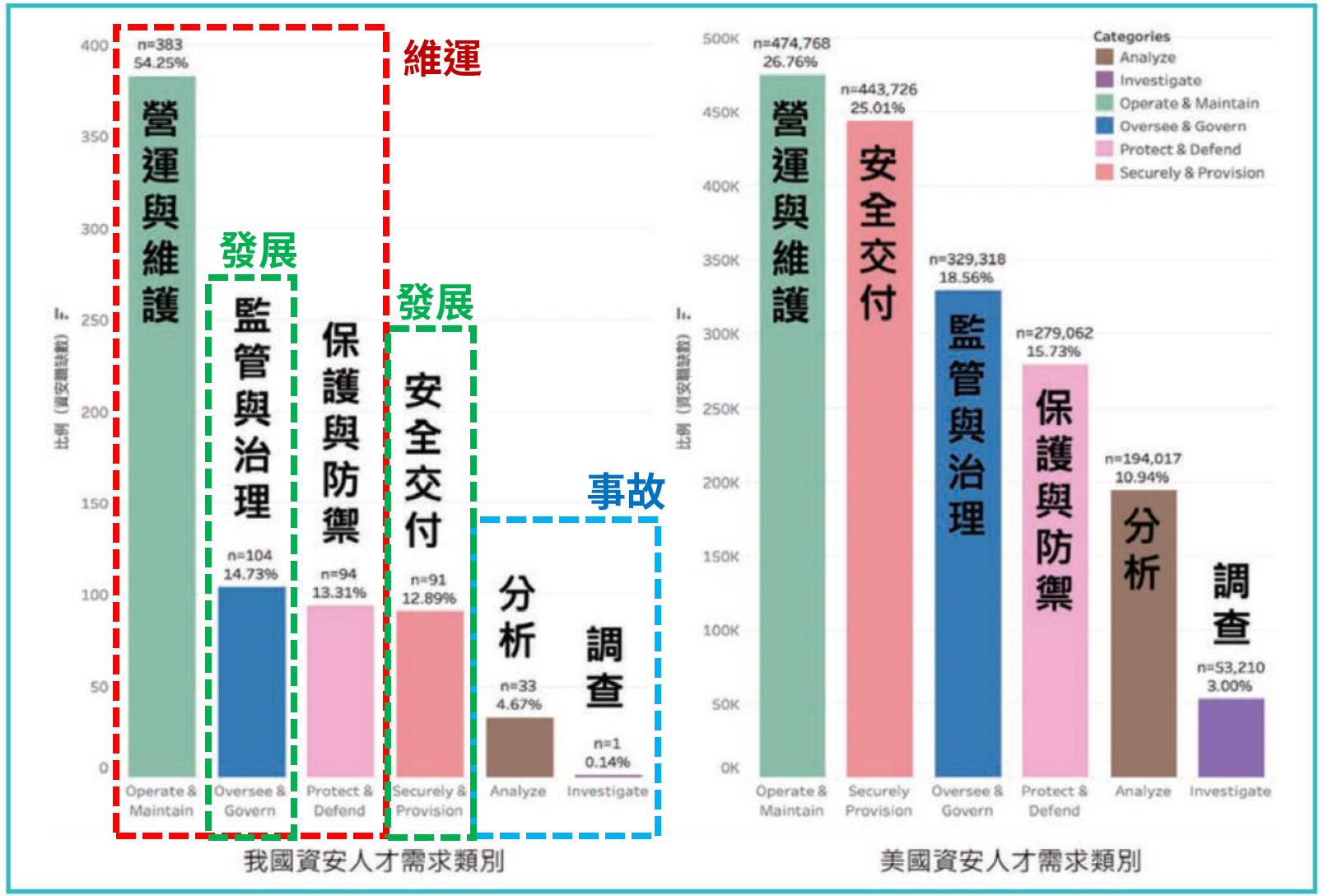
SHIELDXTREME
微智安聯

企業普遍面臨的資安風險與困境



資料來源：iThome CIO大調查

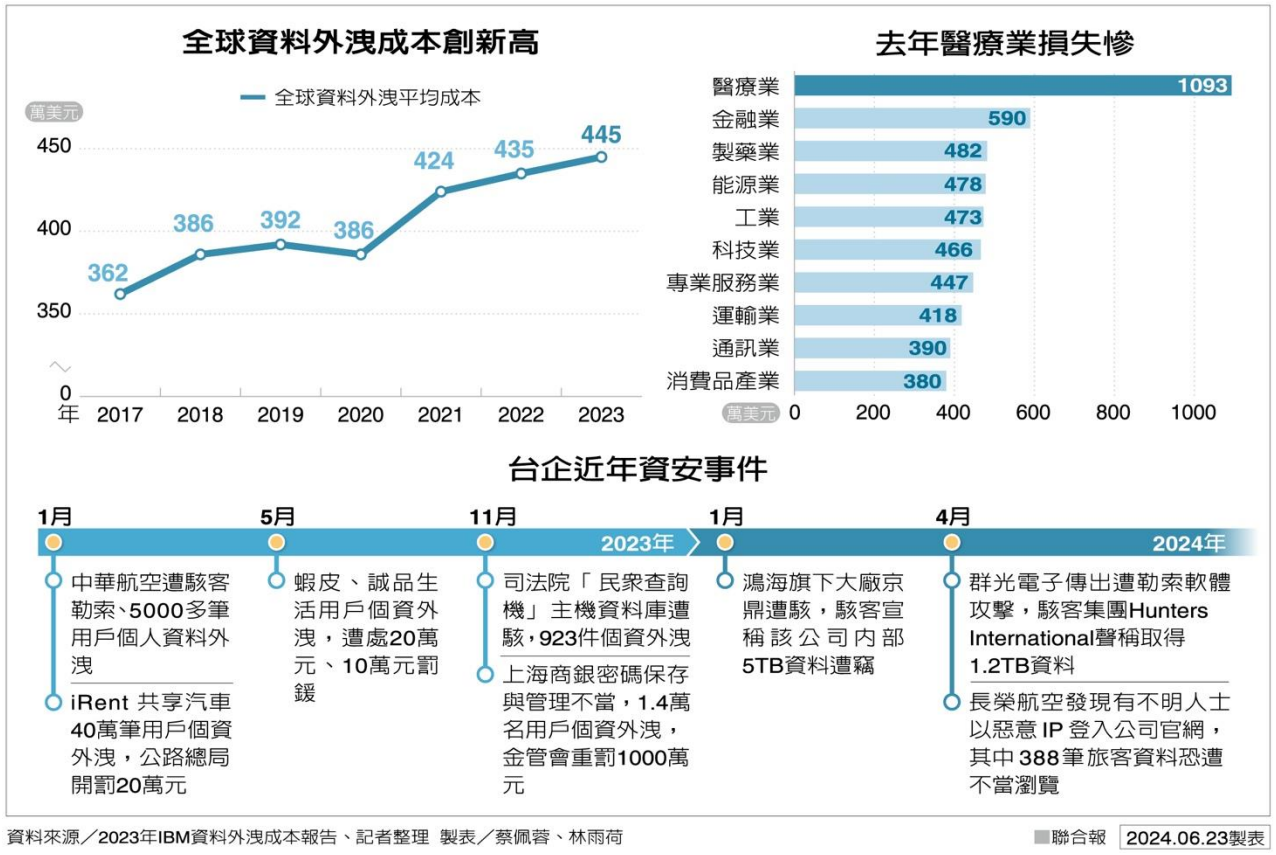
資安人才現況與需求



- 台灣 1 年遭駭 7420 萬次，全球之冠
- 台灣遭駭次數為各國平均值 2.7 倍、網路勒索全球第 4 多
- 資安人才缺口，企業維運類資安人才為大宗
- 資安設備買越多，資安維運越吃力
- 資安人力重實戰，資安防護設備無法取代
- 資安人才養成刻不容緩

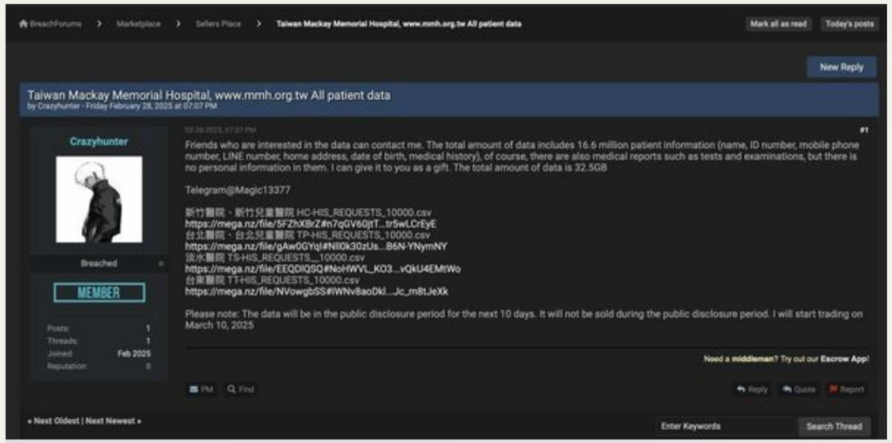
資料來源：資安院台灣資安人才培力研究報告

歷史事件不斷發生



資料來源／2023年IBM資料外洩成本報告、記者整理 製表／蔡佩蓉、林雨荷

■聯合報 2024.06.23製表



▲一名駭客在論壇「Breach Forums」拍賣馬偕病患個資。(圖 / 翻攝李欣穎臉書)

記者趙于婷 / 台北報導

馬偕醫院上月遭駭客入侵，導致醫院門急診系統500多台電腦當機，病人檔案遭到加密勒索，而有一名自稱「Crazy Hunter」的駭客上月28日把個資放到論壇上拍賣，稱資料有1660萬筆，傳有詐騙集團用10萬美元（約新台幣328萬元）買下。對此，衛福部表示，檢調單位已介入調查，目前並不能百分之百確認資料是否為馬偕流出。

資料來源：聯合報、ETtoday新聞雲

駭客眼中的金流？

- 博客來、誠品、萊爾富、家樂福等國內多家知名商場，近來陸續發生駭客攻擊事件，嫌犯藉此取得會員綁定的信用卡資料盜刷商品變賣，目前至少有上百人受害。
- 刑事局警方發動6波搜索，逮捕共15人，發現陳姓主嫌竟和中國駭客聯手，駭商場個資盜刷牟利

https://ynews.page.link/eJpjF

老司機：慈母手中線，來看看最純真的社交工程

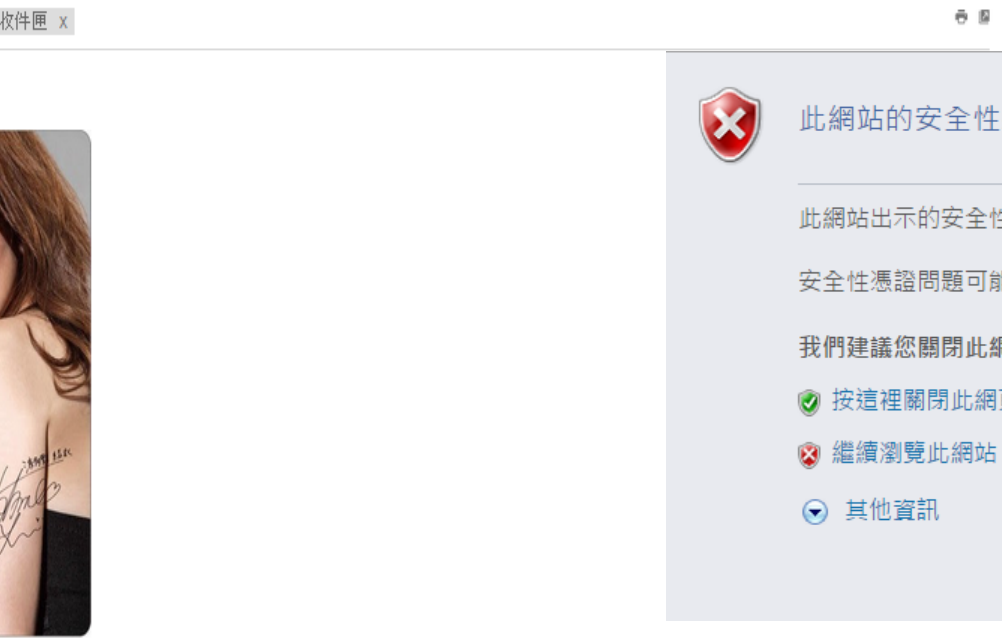
波多野結衣登上悠遊卡　卡公司：清純的跟「天使」一樣　收件匣 x

愛優子 <iroironohana@gmail.com>
寄給 我

「暗黑林志玲」波多野結衣在台灣人氣超高，不只多次代言網路遊戲，還曾拍攝國片《沙西米》，儼然是台灣AV女優第一人。近日連台北悠遊卡公司也找上波多野結衣，推出「天使」與「惡魔」悠遊卡，悠遊卡公司林筱淇表示，「**這次推出的卡樣風格清新又唯美，而且盈餘將會捐給公益團體，非常正面！**」

波多野結衣公益悠遊卡分為「天使」、「惡魔」兩種款式，「天使」款的卡面的設計風格以清純為主題，**波多野結衣穿著白色洋裝，面露甜美微笑，慵懶的姿態配合溫暖的光線**，彷彿置身天堂一般；而「惡魔」卡面則以冷豔為主題，波多野結衣**穿著黑色洋裝，眼中透著一股成熟氣息，十足的冰山美人**。

波多野結衣悠遊卡事件懶人包
如無法連結 請複製網址 http://goo.gl/hBN6BE



SHIELDXTREME 微智安聯

天下沒有白吃的午餐...只有ooxx

網站名稱	網址	件數
TikTok	www.asosss-tkkp.com	11
Tradivio	wap.tradiviovvo.cc	8
數位雲端	www.annbdd.com	8
FLIX	www.flixwonderful.com	7
bete-dex	bete-dex.today	7
Celestia	www.celestiia.com	7
Crze	cryzeneq.com	7
MaxCoin	es.maxi.it.com	7
POYA	www.poyabuyinc.com	6
imToken	imtoke.qpon	6
BitCoit	www.bitcoittw.com	5
Yscle	yscle.top	5
YPLW	www.yplw-win.com	5
全方位智能策略	chaosnrx.com	5
GRGC	grtrade.pro	5
Gold	www.twxauxjpsn.com	5

https://165.npa.gov.tw/#/article/9/1677

比特幣漲📈什麼？

https://crypto.cnyes.com/BTC/1y

公開資訊觀測站

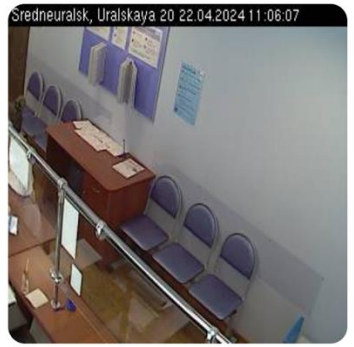
公告日期時間	市場產業別	公司代號	公告簡稱	公告項目	公告主旨	詳細資料
114/04/30 15:22:48	上市 鋼鐵工業	2029	盛餘	M26 遭受重大損失或資安事件	本公司網路資安事件進一步補充說明	
114/04/07 15:32:58	上市 光電業	3051	力特	M26 遭受重大損失或資安事件	說明本公司發生網路資安事件	
114/03/31 17:02:09	上市 資訊服務業	6214	精誠	M26 遭受重大損失或資安事件	本公司網路資安事件說明	
114/03/30 21:09:22	上市 鋼鐵工業	2029	盛餘	M26 遭受重大損失或資安事件	本公司網路資安事件說明	
114/03/25 17:49:55	上市 建材營造	2505	國揚	M26 遭受重大損失或資安事件	本公司網路資安事件說明	

https://mopsov.twse.com.tw/mops/web/ezsearch

杰哥不要！來~讓我看看

Live camera in Bucharest, Romania

Live camera in Meguro-ku, Japan



Live camera in Moscow, Russian Federation

Welcome to Insecam project. The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams. Now you can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other network video cams available online without a password. Mozilla Firefox browser is recommended to watch network cameras.

The following actions were made to Insecam for the protection of individual privacy:
- Only filtered cameras are available now. This way none of the cameras on Insecam invade anybody's private life.

- Any private or unethical camera will be removed immediately upon e-mail complaint. Please provide a direct link to help facilitate the prompt removal of the camera.

http://www.insecam.org

您以為很安全的網站？

https://daxxxg1xx1.com.tw

您以為很安全的網站？

https://mexxx.com.tw/

您以為很安全的網站？

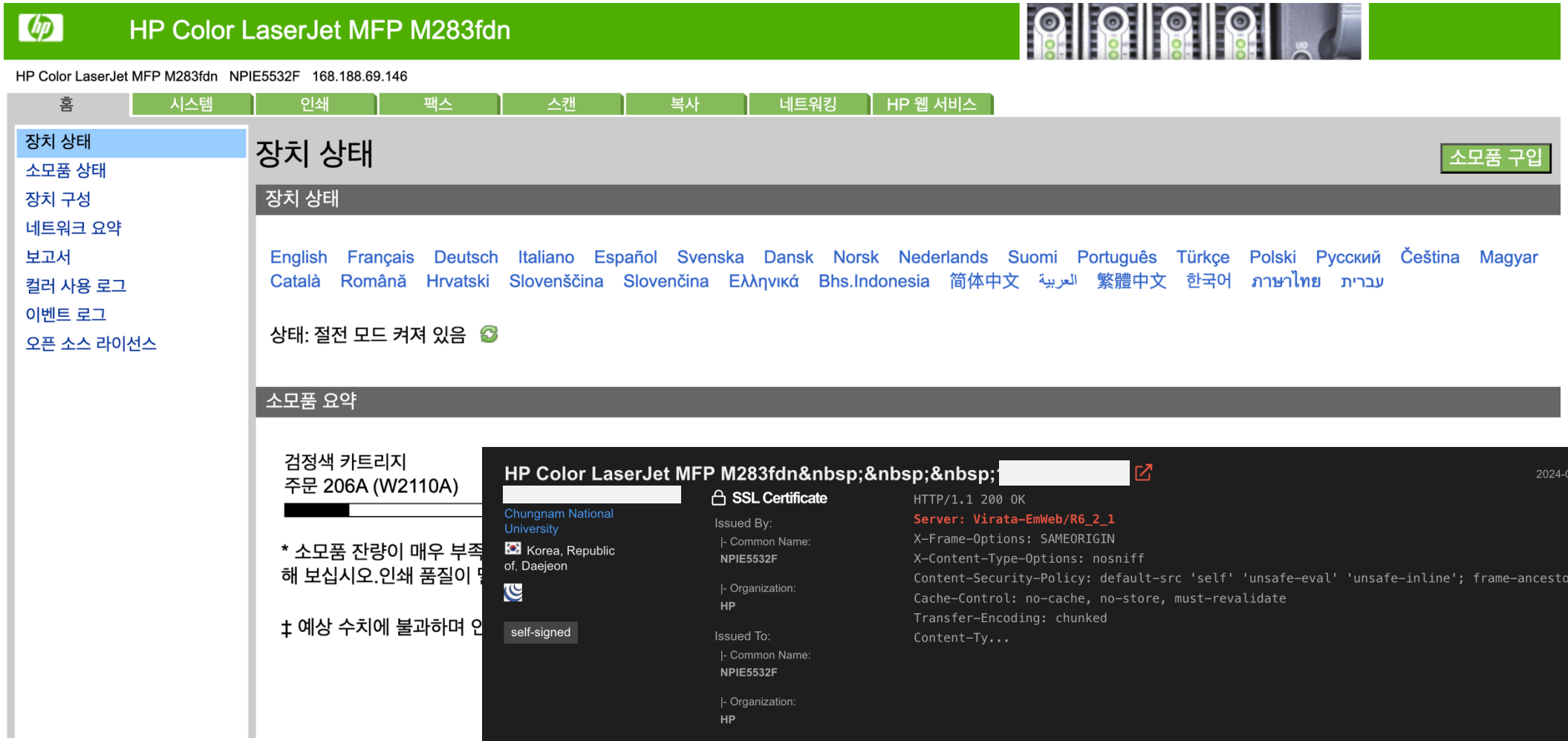
https://lvxxx.com.tw/

印啦！哪次不印？


HP OfficeJet Pro 8710
Embedded Web Server（內嵌式 Web 伺服器）
搜尋
首頁
掃描
傳真
Web 服務
網路
工具
設定
掃描到電子郵件
設定「掃描至電子郵件功能」的目標電子郵件設定檔。
掃描到網路資料夾
設定「掃描至資料夾」功能的目標網路資料夾。
HP 數位傳真
設定印表機，以將傳真儲存到網路資料夾或轉寄到電子郵件地址。
節能模式
在以下時間後進入節能模式
5 分鐘
Web 服務
設定 Web 服務並開啟 HP ePrint。
印表機更新
檢查有無新的印表機更新。
預估墨匣墨水存量*
C
M
Y
K
*實際墨水存量可能有所不同。
網路摘要
已連接
IP 位址:
主機名稱:
HPFA24E0
HP 建議採用 ColorLok(R) 紙張，以取得最佳列印結果


Web 服務
網路
工具
設定
安全
密碼設定
為防止未經授權的使用者從內嵌式 Web 伺服器 (EWS) 遠端設定印表機或檢視印表機設定，可以設定密碼。一旦設定密碼，從 EWS 變更或檢視許多印表機設定時，都需要此一密碼。
管理員密碼只能由下列可列印的 ASCII 字元：A-Z, a-z, 0-9，及特殊字元組成：!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
將本方塊保留為空白，即可停用密碼。
使用者名稱
admin
密碼
確認密碼
套用
取消

好想贏韓國！今晚吃泡菜...


HP Color LaserJet MFP M283fdn
HP Color LaserJet MFP M283fdn NPIE5532F 168.188.69.146
홈
시스템
인쇄
팩스
스캔
복사
네트워킹
HP 웹 서비스
장치 상태
소모품 상태
장치 구성
네트워크 요약
보고서
컬러 사용 로그
이벤트 로그
오픈 소스 라이선스
장치 상태
소모품 구입
장치 상태
English Français Deutsch Italiano Español Svenska Dansk Norsk Nederlands Suomi Português Türkçe Polski Русский Čeština Magyar
Català Română Hrvatski Slovenščina Slovenčina Ελληνικά Bhs.Indonesia 简体中文 العربية 繁體中文 한국어 ภาษาไทย עברית
상태: 절전 모드 켜져 있음
소모품 요약
검정색 카트리지
주문 206A (W2110A)
* 소모품 잔량이 매우 부족
해 보십시오.인쇄 품질이
‡ 예상 수치에 불과하며 인
HP Color LaserJet MFP M283fdn
2024-04-22T07:17:07.441561
Chungnam National University
Korea, Republic of, Daejeon
self-signed
SSL Certificate
Issued By:
|- Common Name:
NPIE5532F
|- Organization:
HP
Issued To:
|- Common Name:
NPIE5532F
|- Organization:
HP
Supported SSL Versions:
TLSv1.2
HTTP/1.1 200 OK
Server: Virata-EmWeb/R6_2_1
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' 'unsafe-eval' 'unsafe-inline'; frame-ancestors 'self'
Cache-Control: no-cache, no-store, must-revalidate
Transfer-Encoding: chunked
Content-Ty...

老闆說：這批貨很純

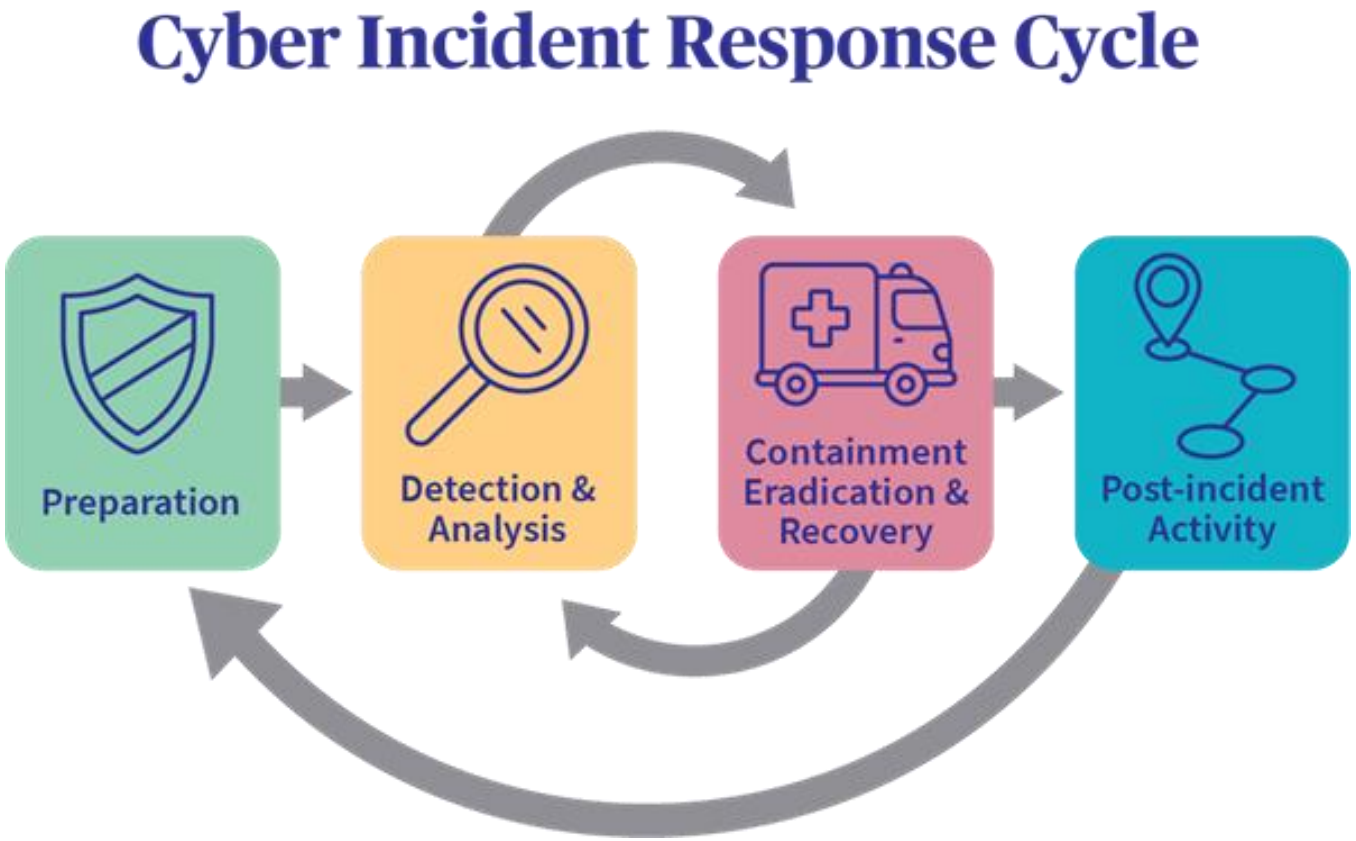
- 11110.pdf
- 111年學校勞務委託書附件.pdf
- 11205–1.pdf
- 11206.pdf
- 113年學校勞務委託書–1.doc
- 113年學校勞務委託書附件資料–保險.pdf
- 113年學校勞務委託書附件資料.pdf
- 113招生簡章.pdf
- 13屆第23次理事會–1.pdf
- 13屆第23次理事會–2.pdf
- 13屆第23次理事會–3.pdf
- 13屆第24次理事會.pdf
- 13屆第25次理事會.pdf
- 13屆第26次理事會.pdf
- 14屆第1次理事會.pdf
- 1517870344.jpg
- 1_1.jpg
- 200805010008_0001.jpg
- 2011.03.03.pdf
- 2011.03.09.pdf
- 2011.03.09複驗.pdf
- 2011.03.10.pdf
- 2011.03.11.pdf
- 2011.03.15–複驗.pdf

- 招標會議記錄發文111–03.pdf
- 招標會議記錄發文111–04.pdf
- 招標會議記錄發文111–05.pdf
- 招標會議記錄發文111–06.pdf
- 招標會議記錄發文111–09.pdf
- 招標會議記錄發文111–10.pdf
- 招標會議記錄發文111–11.pdf
- 招標會議記錄發文111–12.pdf
- 招標會議記錄發文111–1~2.pdf
- 招標會議記錄發文112–03.pdf
- 招標會議記錄發文112–04.pdf
- 招標會議記錄發文112–05.pdf
- 招標會議記錄發文112–06.pdf
- 招標會議記錄發文112–09.pdf
- 招標會議記錄發文112–1–2.pdf
- 招標會議記錄發文112–10.pdf
- 招標會議記錄發文112–11.pdf
- 招標會議記錄發文112–12.pdf
- 招標會議記錄發文113–03.pdf
- 招標會議記錄發文113–04.pdf
- 招標會議記錄發文113–1–2.pdf
- 旭臨蛋11月份.pdf
- 業者供應學校午餐食材追溯流向管制自主管理紀錄月報表.xls
- 樂寶商行.pdf
- 樂寶商行10月.pdf
- 決標公告(202303).pdf
- 決標公告11201–02.pdf
- 決標公告急202304).pdf

如何做好備份？

- 如何有效的備份？3-2-1備份原則
  - 既然我們已經知道了數據資產的重要性，也了解資料應做好備份以降低災害衝擊，更知道**「雞蛋不要放在同一個籃子」**分散風險的道理，那麼我們可以採用業界盛行且有效的備份方式，也就是**「3-2-1備份原則」**。
- 3-2-1備份原則，能提供資料備份與災難復原最好的準備，即使設備損壞或內部資料遺失，也能確保資料仍有備份可使用，如以下：
  - **至少備份三份** (一份原始檔，兩份備份檔)：
    可在原本備份的資料受損時，及時將資料還原。
  - **使用兩種不同的備份方式** (光碟、外接硬碟或其他)：
    備份的設備及媒體儲存裝置有各自的優缺點，耐用程度與可承受的環境都有所不同。
  - **其中有一份要放在異地** (放在網頁設計公司、分公司或其他)：
    避免當天災、火災或水災發生時，一次將設備都全數破壞。

NIST 事件回應四階段生命週期指南 (SP 800-61 R2)



1. 準備階段

- 建立事件回應團隊（如 CSIRT）。
- 擬定政策、流程，並定期演練。
- 準備工具、培訓人員，提升應變能力。

2. 偵測與分析

- 監控系統、發現異常行為。
- 快速分類事件、評估影響與優先順序。
- 收集日誌與證據資料，協助判斷真實性。

3. 遏制、根除與恢復

- **遏制**：阻止事件擴大（如隔離設備）。
- **根除**：移除惡意程式與入侵者。
- **恢復**：修復系統、恢復服務並加強防護。

4. 事後分析

- 回顧事件處理過程，找出根本原因。
- 更新制度與防禦機制，避免重蹈覆轍。
- 整理報告，分享經驗以提升整體資安成熟度。

https://medium.com/@bhavin200/nist-incident-response-800-61-a-comprehensive-guide-to-the-four-phase-lifecycle-for-identifying-3c79b9b0a993

資安事件分析的不同角度

從檔案角度

-惡意程式
-時間
-建立者
-隱藏/刪除
-惡意程式屬性
-連線

從封包角度

-IP
-Domain
-Url
-行為

從日誌角度

- 時間
- 來源/目的
- 行爲分析
- 關聯分析

從情資角度

-IP
-Domain
-Url
-行為

Wireshark

- **分析**
  - Follow TCP Stream
  - 透過 TCP Stream 觀察到應用程式層 (Application Layer) 流量
  - 流量資料的瑞士刀！
- **統計**
  - Conversations
  - 分別將資料、時間、通訊埠 (protocol) 區分顯示
- **過濾**

Wireshark Cheat Sheet

Logical Operators

OPERATOR	DESCRIPTION	EXAMPLE
and or &&	Logical AND	All the conditions should match
or or ||	Logical OR	Either all or one of the conditions should match
xor or ^^	Logical XOR	Exclusive alterations - only one of the two conditions should match not both
not or !	Not (Negation)	Not equal to
[n] [...]	Substring operator	Filter a specific word or text

https://www.stationx.net/wireshark-cheat-sheet/

日誌格式 — Apache Combined Access Log

- 資料範例

```
236.184.27.219 - - [10/Sep/2016:18:27:10] "GET /product.screen?productId=FL-NYC-44
&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1" 200 3930 "http://www.yahoo.com"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 797
```

- 欄位說明

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

✓ 236.184.27.219 (%h)
  - 發出請求的 client IP (remote host)

✓ - (%l)
  - Remote logname，因為容易偽造，所以通常沒人用

✓ - (%u)
  - 對網頁發起要求的 user，因為容易偽造，所以通常沒人用

✓ [10/Sep/2016:18:27:10] (%t)
  - Web server 收到 request 的時間

✓ "GET /product.screen?productId=FL-NYC-44&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1" (\"%r\")
  - Client 端發出的要求字串

日誌格式 — Apache Combined Access Log

- 資料範例

```
236.184.27.219 - - [10/Sep/2016:18:27:10] "GET /product.screen?productId=FL-NYC-44
&JSESSIONID=CA10MO3AZ7USANA5006 HTTP 1.1" 200 3930 "http://www.yahoo.com"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 797
```

- 欄位說明

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

  - ✓ 200 (%>s)
    - Server 端回覆的狀態碼
  - ✓ 3930
    - 回覆給 client 端的資料大小
  - ✓ "http://www.yahoo.com" (\"%{Referer}i\")
    - 這次呼叫的前一個網頁
  - ✓ "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" (\"%{User-agent}i\")
    - 使用者使用的瀏覽器資訊
  - ✓ 797 (?)
    - 標準規範以外的其他資訊

網頁攻擊日誌範例

- 192.168.1.101 - - [20/May/2025:14:23:45 +0800] "GET /index.php?id=1%20OR%201=1 HTTP/1.1" 200 532 "-" "sqlmap/1.4.10#stable"
- 192.168.1.102 - - [20/May/2025:14:24:03 +0800] "GET /search.php?q=<script>alert('xss')</script> HTTP/1.1" 403 1234 "-" "Mozilla/5.0 (X11; Linux x86_64)"
- 192.168.1.103 - - [20/May/2025:14:25:11 +0800] "POST /upload.php HTTP/1.1" 500 768 "-" "curl/7.64.1"
- 192.168.1.104 - - [20/May/2025:14:26:09 +0800] "GET /etc/passwd HTTP/1.1" 404 234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
- 192.168.1.105 - - [20/May/2025:14:26:47 +0800] "GET /index.php?page=../../../../etc/passwd HTTP/1.1" 200 674 "-" "Mozilla/5.0 (Windows NT 6.1)"
- 192.168.1.106 - - [20/May/2025:14:27:33 +0800] "GET /admin HTTP/1.1" 401 89 "-" "Nikto/2.1.6"
- 192.168.1.107 - - [20/May/2025:14:28:10 +0800] "GET /api/user?id=1;DROP TABLE users;-- HTTP/1.1" 403 1900 "-" "Mozilla/5.0 (Macintosh)"

ISO27001：2022 版新增的要求

- ✓ 企業現況掌握
- ✓ 關鍵服務持續監控

A5.30
營運持續之資
通訊準備

A8.10 資訊刪除
A8.11 資料遮罩
A8.12 防範資料外洩

- ✓ 端點預警
- ✓ 異常行為監控

A5.23
雲端服務之
資訊安全

A5.7 威脅情報
A7.4 實體安全監控
A8.9 組態管理
A8.16 活動監控
A8.23 網頁安全防護
A8.28 程式開發安全

- ✓ API 安全
- ✓ 網站安全
- ✓ 應用服務安全

- ✓ 情資運用
- ✓ 風險持續監控
- ✓ 弱點掃描、滲透測試
- ✓ 紅隊演練

SHIELDXTREME 微智安聯

上市櫃公司資通安全管控指引

技術面

設置系統監控及技術檢測平台

- 資安要求納入資通系統開發及維護需求規格
- **定期安全性檢測**並完成**系統弱點修補**
- 資通安全**威脅偵測管理機制**
- 資通安全防護與控制
- 實體安全控管

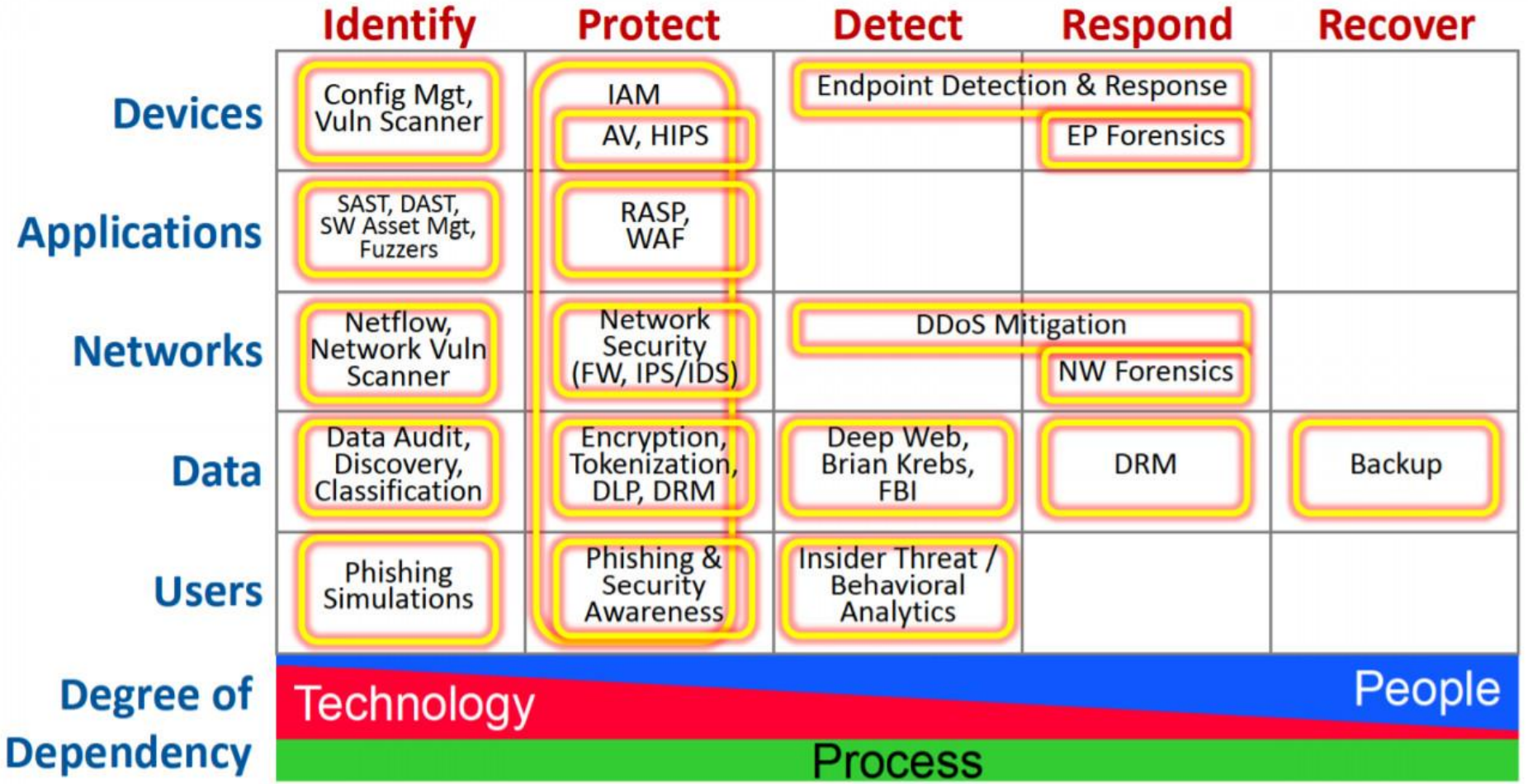
資安素養

資安認知訓練與演練

- 資通安全教育訓練
- 資通安全**專業課程訓練**
- 每年定期辦理電子郵件**社交工程演練**

SHIELD XTREME 微智安聯

Cyber Defense Matrix (CDM)

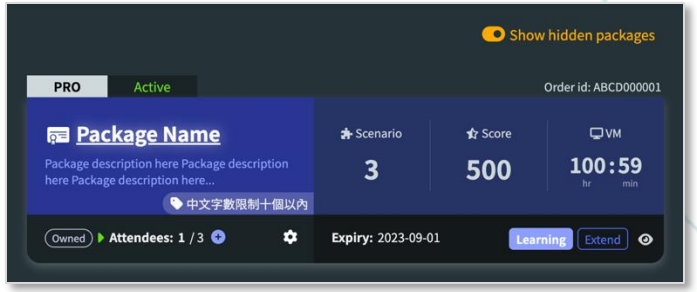


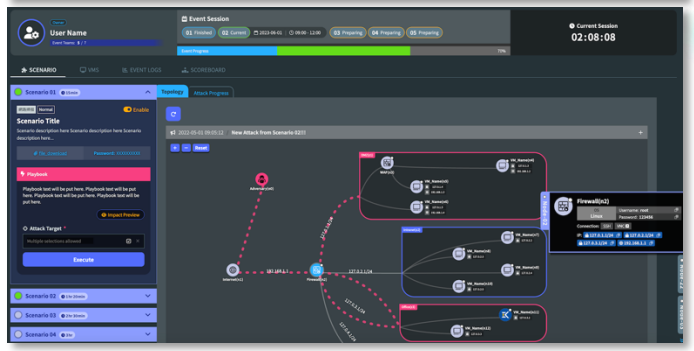
https://www.jcic.org.tw/main_ch/fileRename/fileRename.aspx?fid=1143&kid=1

微智安聯的產品及服務

X-Range
資安攻防演訓服務

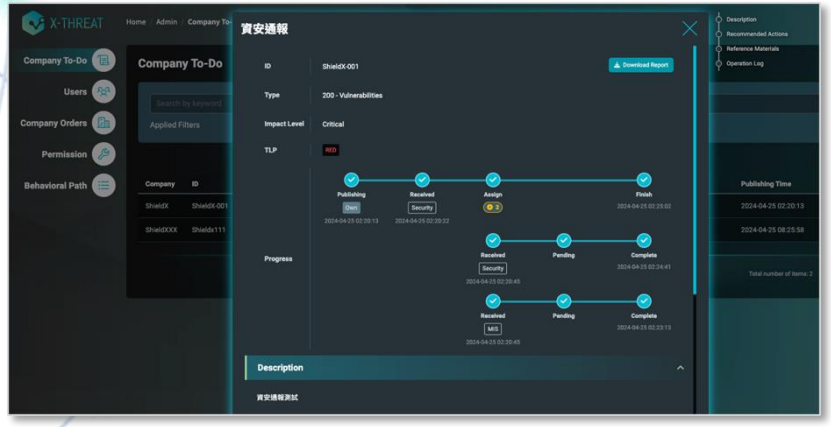
-符合**NICE**、**ECSF**、資安人培框架
-個人紅藍隊資安技術實作
-真實體驗**擬真情境**與環境
-企業網路架構團隊**攻防演練**
-資安人員技能評估與考核





X-Threat
資安威脅情資服務

-符合**ISO 27001:2022** 版本之程序要求：蒐集、分析、溝通與管理
-整合企業資安防護系統，**自動派送**阻擋清單
-支援**ISAC**組織情資管理作業要求與分享機制
-支援國際商用情資，單一訂閱與整合介面



X-Village
資安風險檢測服務

-**外部曝險**即時分析與持續監控服務
-企業**弱點及漏洞**掃描與滲透測試
-**企業內部**資安健康狀態檢查服務
-供應鏈**資安評級分數合規改善**服務

SHIELDXTREME 微智安聯

Hackers are anywhere, any time!
Are you READY ?

Welcome to Shieldx.io

SHIELDEXTREME