落實校園資安和強化資安人才培育
接軌產業和國際

第2場
11:20~12:00

主持人：顏嗣鈞主任 / 國立臺灣大學計資中心
評論人：王永鐘主任 / 國立臺北科技大學計網中心
主講人：黃成弘 / Micro Focus 資深業務協理
案例分享人：陳啟煌博士 / 國立臺灣大學計資中心

今日議程

- Micro Focus 公司簡介
- 產業和國際的資安趨勢
- 落實校園資安的解決方案
- 強化資安人才培育的構想
- 案例分享

Micro Focus 專注於軟體 | 全球規模

> 40 億美元
年營收

FTSE 100
公司
FTSE 最大的科技公司

約 15,000 名
員工
覆蓋 50 個國家/地區

約 54,000 家
客戶
99 家財富 100 強企業

英國最大的科技公司

MICRO FOCUS

四大專注領域：協助客戶達成數位化轉型

在運行中
達成轉型目標

RUN and TRANSFORM

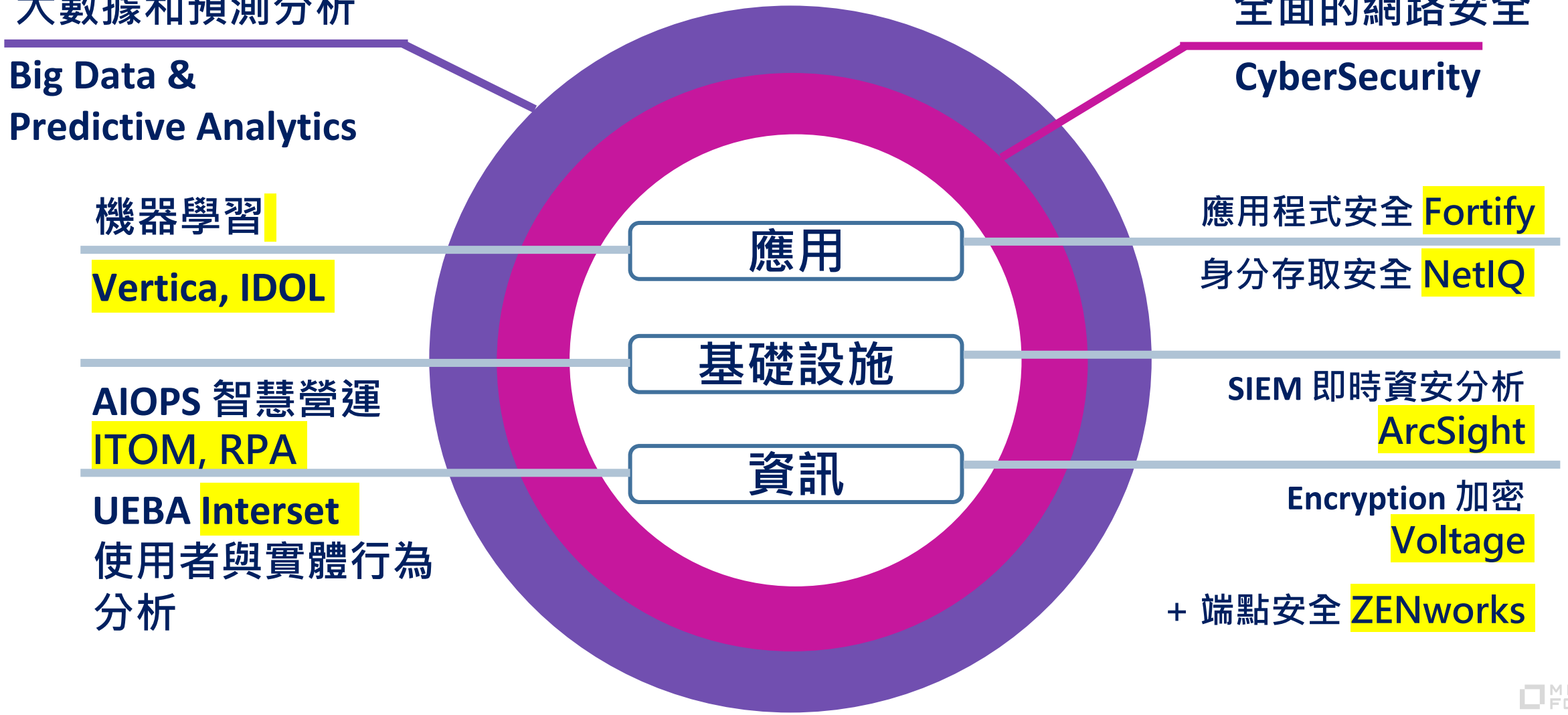
INNOVATE FASTER with LOWER RISK

用更低的風險
達成更快創新

Speed 速度	Agility 敏捷	Security 安全	Insights 洞察
1 Enterprise DevOps	2 Hybrid IT Management	3 Security, Risk & Governance	4 Predictive Analytics
企業 DevOps	混合式 IT 管理	安全風險和治理	大數據和預測分析

MICRO FOCUS

Micro Focus 獨特價值：全面、靈活的企業資安藍圖

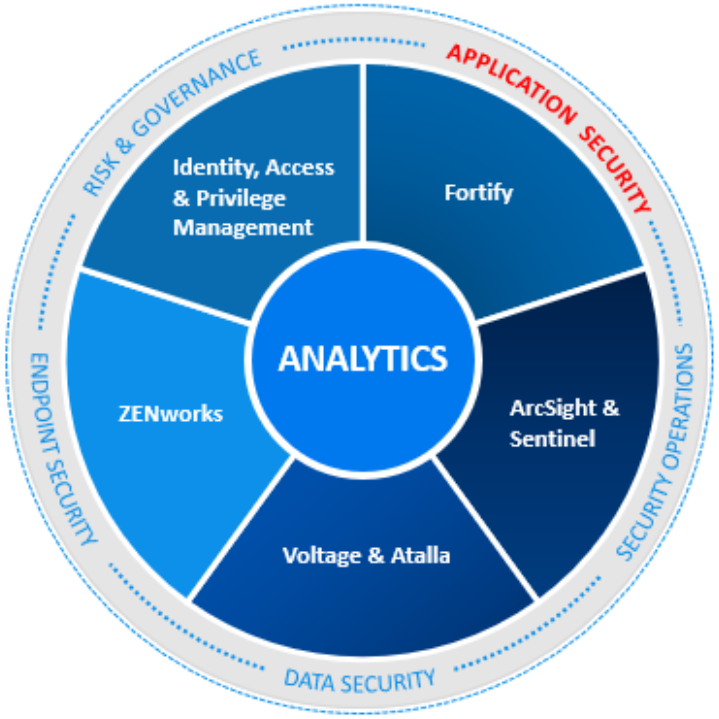


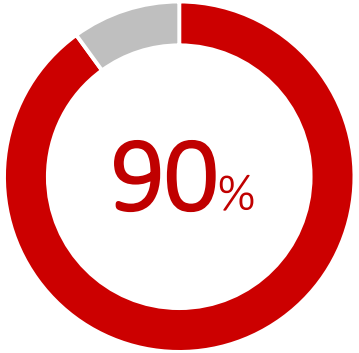
產業和國際的資安趨勢

Application security is more important than ever

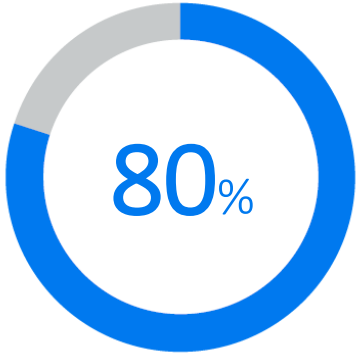
The majority of security breaches today are from application vulnerabilities

- Perimeter
- Network
- Endpoint
- Application
- Data





Percentage of security incidents from exploits against defects in the design or code of software.[1]



Percentage of applications containing at least one critical or high vulnerability.[2]

Source: [1]U.S. Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT)
[2]2017 Application Security Research Update" by the HPE Software Security Research team, 2017

243天
發現入侵的平均時間

2013 January February March April May June July August September October

84%
入侵發生在
應用程式層

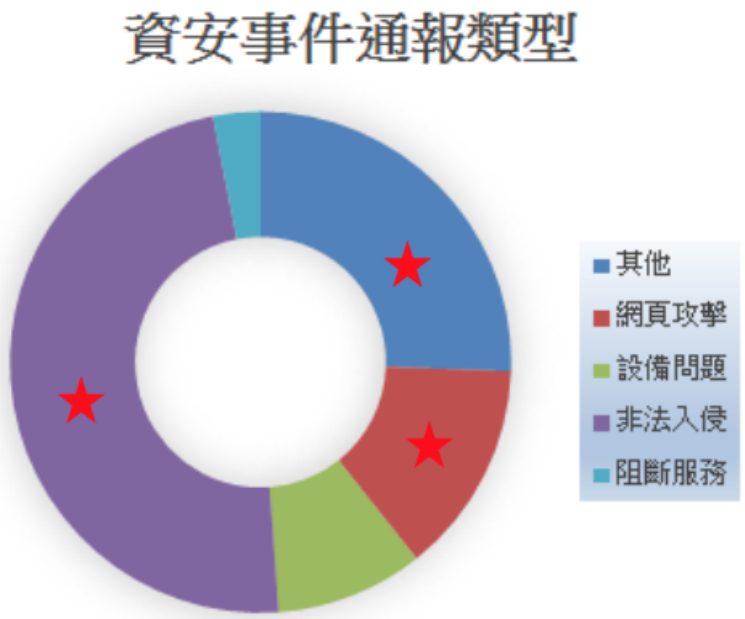
自從2010年，花費在解決入侵的時間越來越多

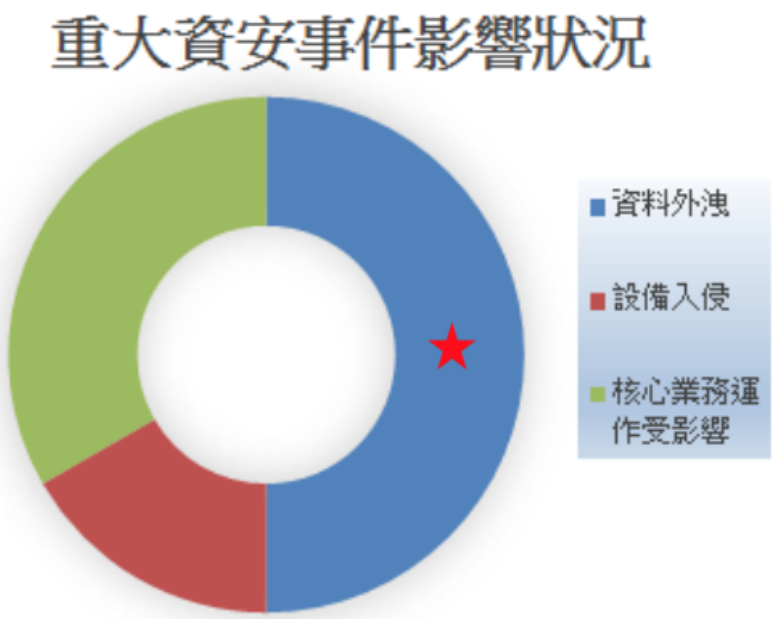
71%

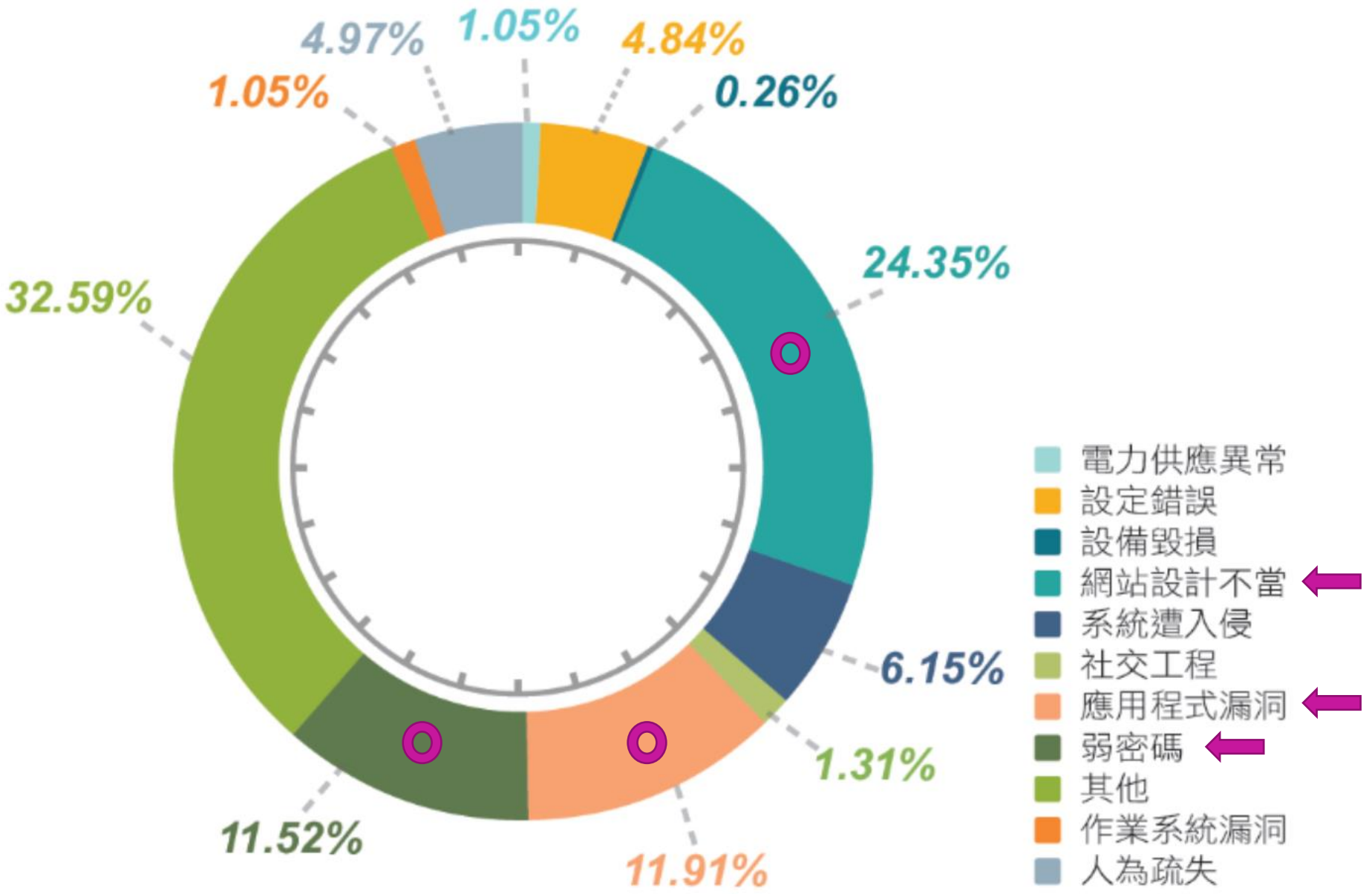
94%
入侵被第
三方披露

政府機關資安事件通報統計

- 107年接獲262件政府機關資安事件通報，事件類型以**非法入侵、網頁攻擊**為主
  - 重大資安事件影響狀況以資料外洩為主，占50.00%

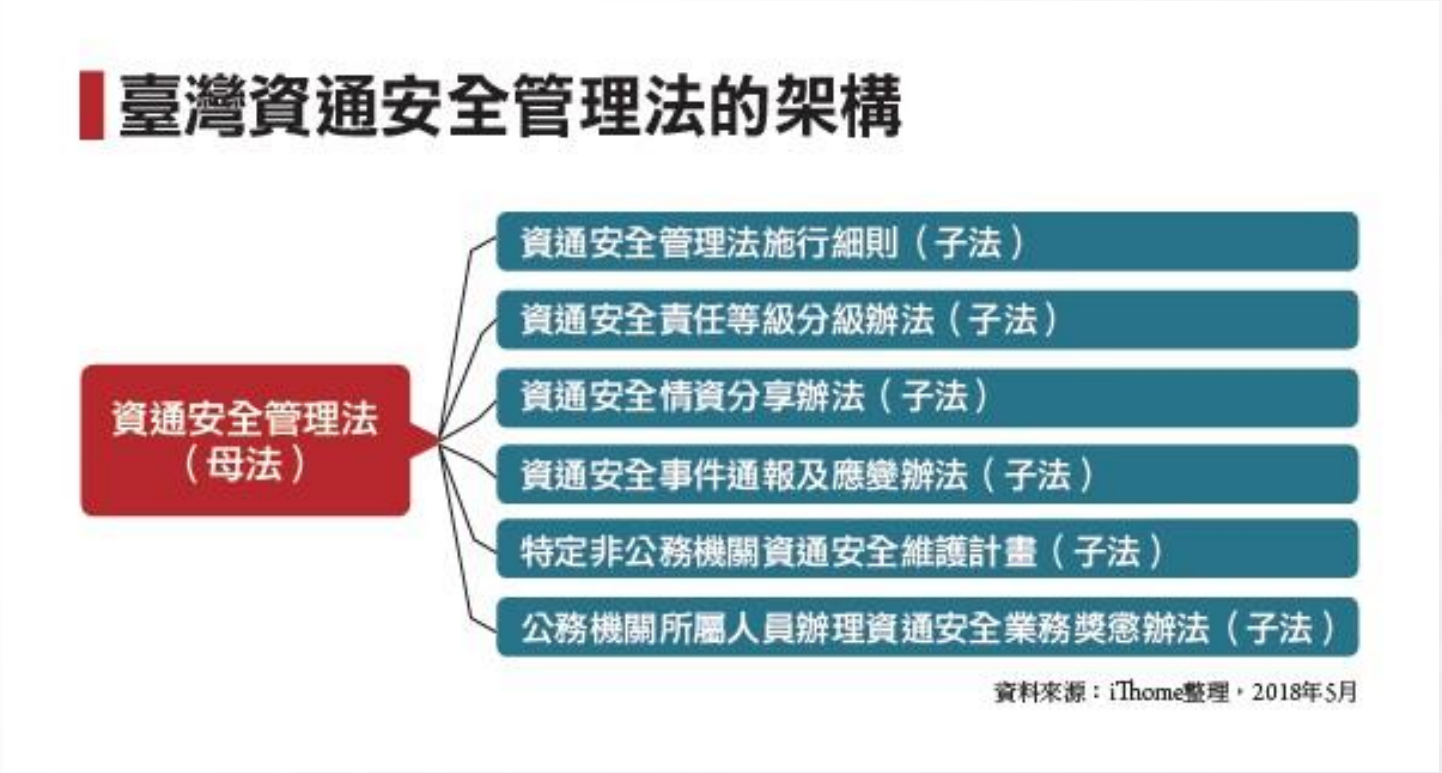





4.97%
1.05%
4.84%
1.05%
0.26%
24.35%
32.59%
6.15%
1.31%
11.52%
11.91%
電力供應異常
設定錯誤
設備毀損
網站設計不當
系統遭入侵
社交工程
應用程式漏洞
弱密碼
其他
作業系統漏洞
人為疏失

行政院通過資通安全管理法

- 107年5月11日 立法院院會中，《資通安全管理法》三讀通過
- 107年6月6日 總統令公告



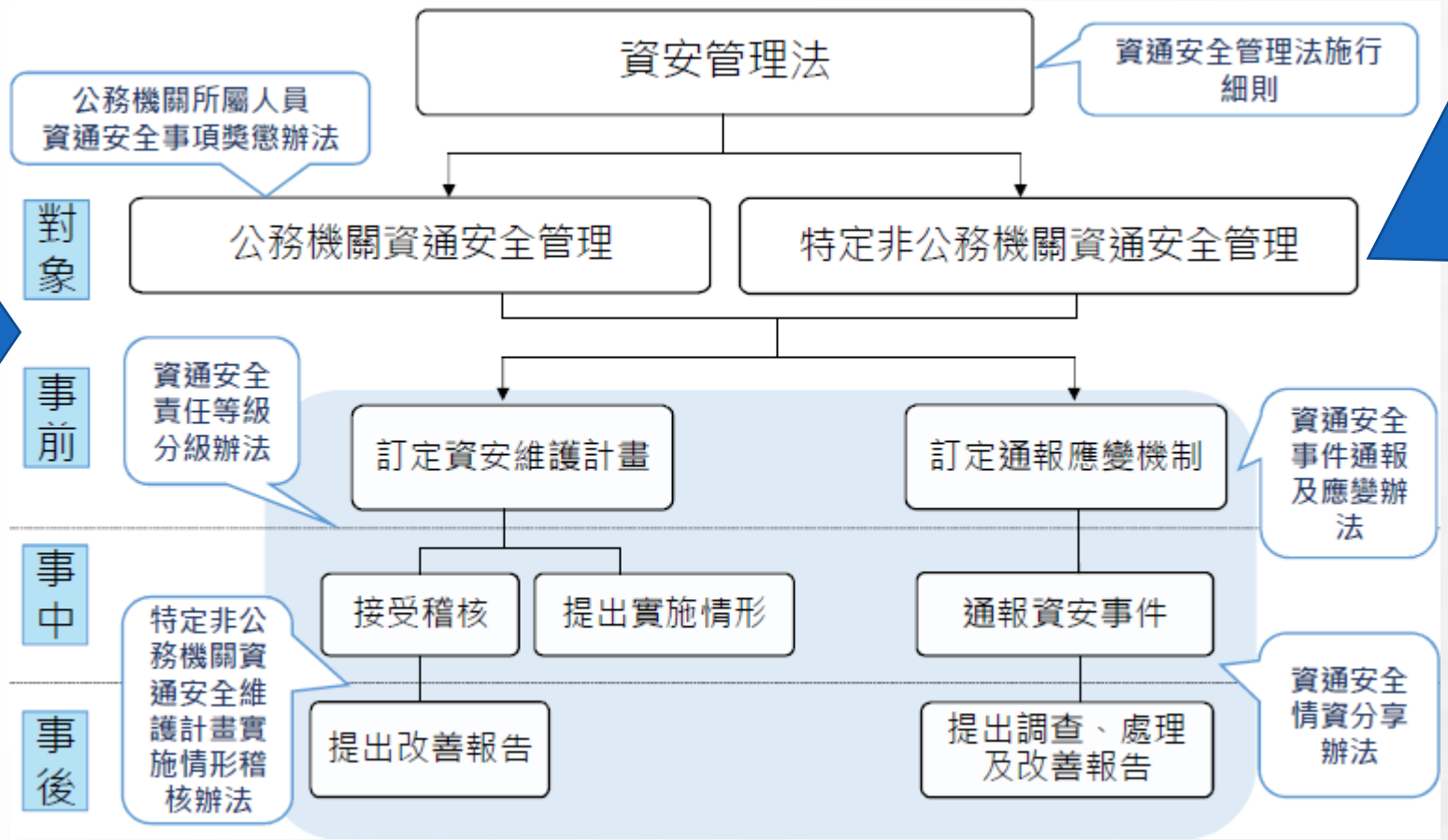
資安管理法架構

資通安全責任等級之公務機關**應辦事項**

- 應辦事項：詳附表一至附表八

資通系統分級及防護基準執行作業

- 資通系統防護分級及防護基準：詳附件九及附表十



未依規定制定資通安全計畫並且落實計畫者，依法可處10萬元以上100萬元以下罰鍰；

未依規定通報資通安全事件者，可處30萬元以上500萬元以下罰鍰，限期未改正者，按次處罰

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項
應辦事項_管理面

辦理項目	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內	1年內	2年內
資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入資訊安全管理系統，並於三年內完成第三方驗證；並持續維持其驗證有效性	2年內	2年內	2年內
業務持續運作演練	全部核心資通系統	每年1次	每2年1次	每2年1次
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專責人員(一年內)		專職(責)4人	專職(責)2人	專職(責)1人
資安治理成熟度評估(公務機關)		每年1次	每年1次	

A與B級機關初次受核定或等級變更後之**一年內**完成資通系統分級，並完成之控制措施。

C級機關若初次受核定或等級變更後之一年內完成資通系統分級，系統等級「高」者，應於初次受核定或等級變更後之**二年內**完成控制措施。

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項

應辦事項_技術面(1/2)

辦理項目	辦理內容	A	B	C
安全性檢測	全部核心資通系統網站安全弱點檢測	每年2次	每年1次	每2年1次
	全部核心資通系統系統滲透測試	每年1次	每2年1次	每2年1次
資通安全健診	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視	每年1次	每2年1次	每2年1次
資通安全威脅偵測管理機制	完成威脅偵測機制建置，並持續維運	1年內	1年內	
	依主管機關指定之方式提交監控管理資料(公務機關)	V	V	

Fortify
應用程式安全
原始碼掃描(白箱)
網站弱點檢測(黑箱)

ArcSight
日誌管理
即時資安分析

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項

應辦事項_技術面(2/2)

辦理項目	辦理內容	A	B	C
資通安全防護(啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	1年內	1年內
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆(WAF)	1年內	1年內	
	APT攻擊防禦	1年內		
政府組態基準	依主管機關公告之項目，完成政府組態基準導入作業，並持續維運(公務機關)	1年內	1年內	

ArcSight
日誌管理
即時資安分析

資料來源: 行政院資通安全辦公室

資通安全責任等級之公務(非)機關應辦事項

應辦事項_認知與訓練

辦理項目	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每年接受之資通安全專業課程訓練或資通安全職能訓練	4名各12小時	2名各12小時	1名12小時
	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	3小時	3小時	3小時
資通安全專業證照及職能訓練證書	初次受核定或等級變更後之一年內，資通安全專職(責)人員總計應持有之資通安全專業證照，並持續維持證照之有效性	4張	2張	1張
	資通安全專職人員總計應持有之資通安全職能評量證書，並持續維持證照之有效性(公務機關)	4張	2張	1張

→ 政府和產業界需才孔急

資料來源: 行政院資通安全辦公室

落實校園資安的解決方案

資安方案	產品名稱	已採購學校數	說明
應用程式安全	Fortify	10	網站設計不當 應用程式漏洞
即時資安分析	ArcSight	16	校園即時資安監控中心
身分存取安全	NetIQ IAM	33	雲端/地端身分整合與單一簽入
多因子驗證	NetIQ AA	0	弱密碼

108年工業局軟體標價格1080201

組別	項次	品項名稱	單套授權數	單位	投標價
4	42	PlateSpin Migrate 雲主機遷移	1	套	14,045
4	43	PlateSpin Protect 雲主機備援	1	套	77,193
15	38	Access Manager 網頁安控與單一登入	50	套	106,909
15	39	Advanced Authentication 多因素認證	50	套	178,605
15	40	CloudAccess 雲端認證管理	50	套	158,205
15	41	Identity Manager 帳號整合與自動化	50	套	149,904
15	42	Privileged Account Manager 主機特權帳號管理	1	套	54,525
17	101	ZENworks Asset Management 資產管理	50	套	88,992
17	102	ZENworks Configuration Management 組態管理	50	套	151,923
17	103	ZENworks Endpoint Security Management 端點安全管理	50	套	183,021
17	104	ZENworks Patch management 修補管理	50	套	30,850
18	106	Sentinel Enterprise 日誌管理暨即時資安事件管理平台	1	套	2,800,180
18	107	Sentinel for Log Management 日誌管理	1	套	1,006,300
19	49	Change Guardian 主機異動稽核軌跡管理	1	套	53,615
19	50	Change Guardian 工作站異動稽核軌跡管理	10	套	21,877
19	51	Change Guardian 網域異動稽核軌跡管理	50	套	3,713
22	13	ArcSight ESM Express 12.5GB/平均250EPS 事件關聯紀錄管理套件組	1	套	2,110,200
22	17	ArcSight User Behavior Analytics 使用者行為分析模組(1000U)	1000	使用者	3,287,285
22	18	ArcSight 通用日誌擴充模組 (擴充5GB日誌資料量)	1	套	170,945
22	20	Arcsight 通用日誌管理系統 (適用每日5GB日誌資料量)	1	套	484,370
22	23	Fortify SCA靜態程式碼分析工具(含軟體安全管理中心以及行動裝置源碼檢測)	1	套	1,784,835
22	24	Fortify WebInspect 動態網頁安全檢測工具 (含黑白箱交叉比對模組)	1	套	1,320,170

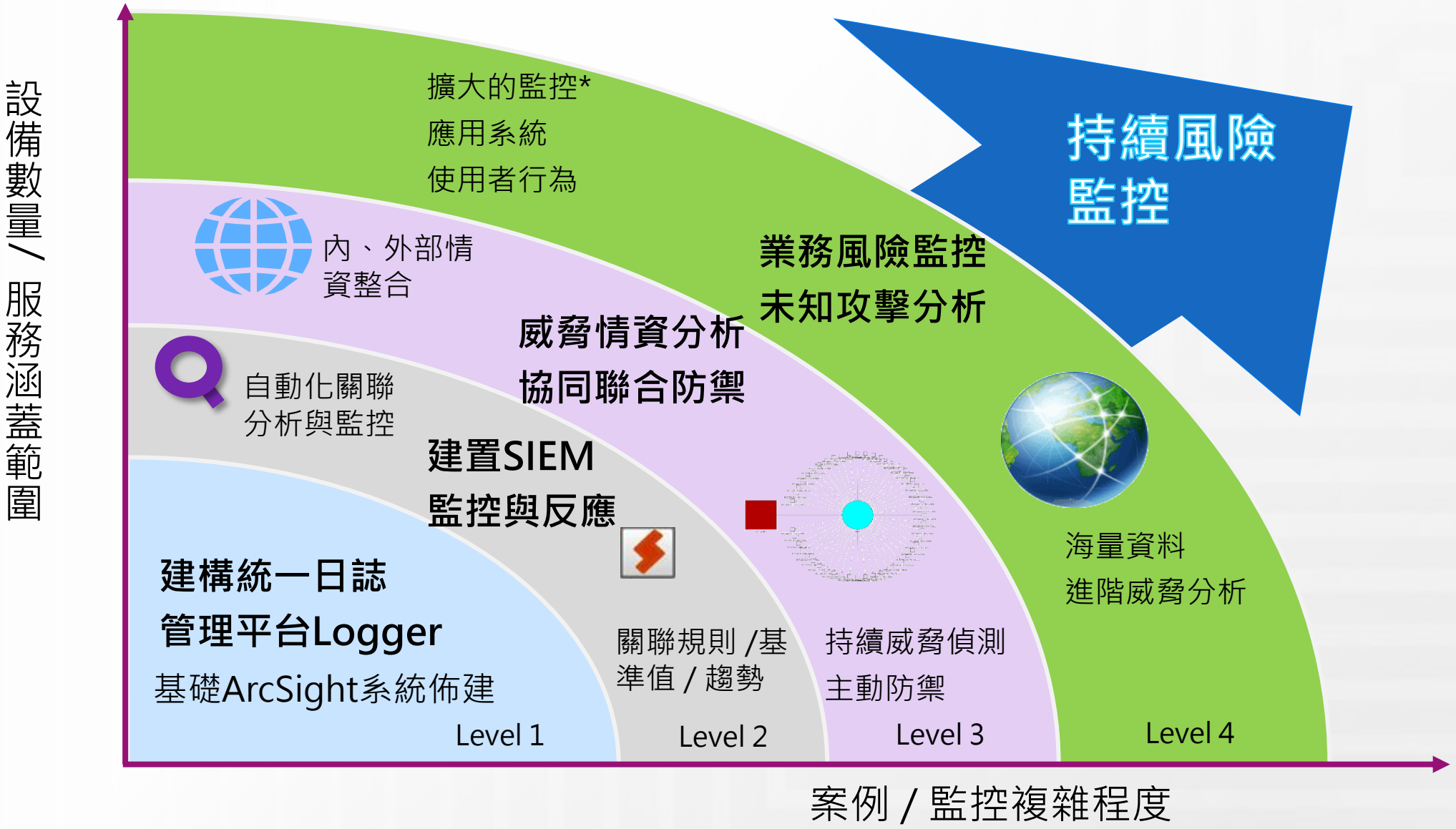
熱門方案：NetIQ Advanced Authentication (AA)

多因子驗證 Multi-Factor Authentication (MFA)

防止帳號被盜用，防止密碼被偷

傳統「密碼驗證」已不足以保護帳號使用的安全

ArcSight 防禦進階式威脅的安全方案



安全軟體發展生命週期(Secure Software Development Lifecycle，SSDLC)

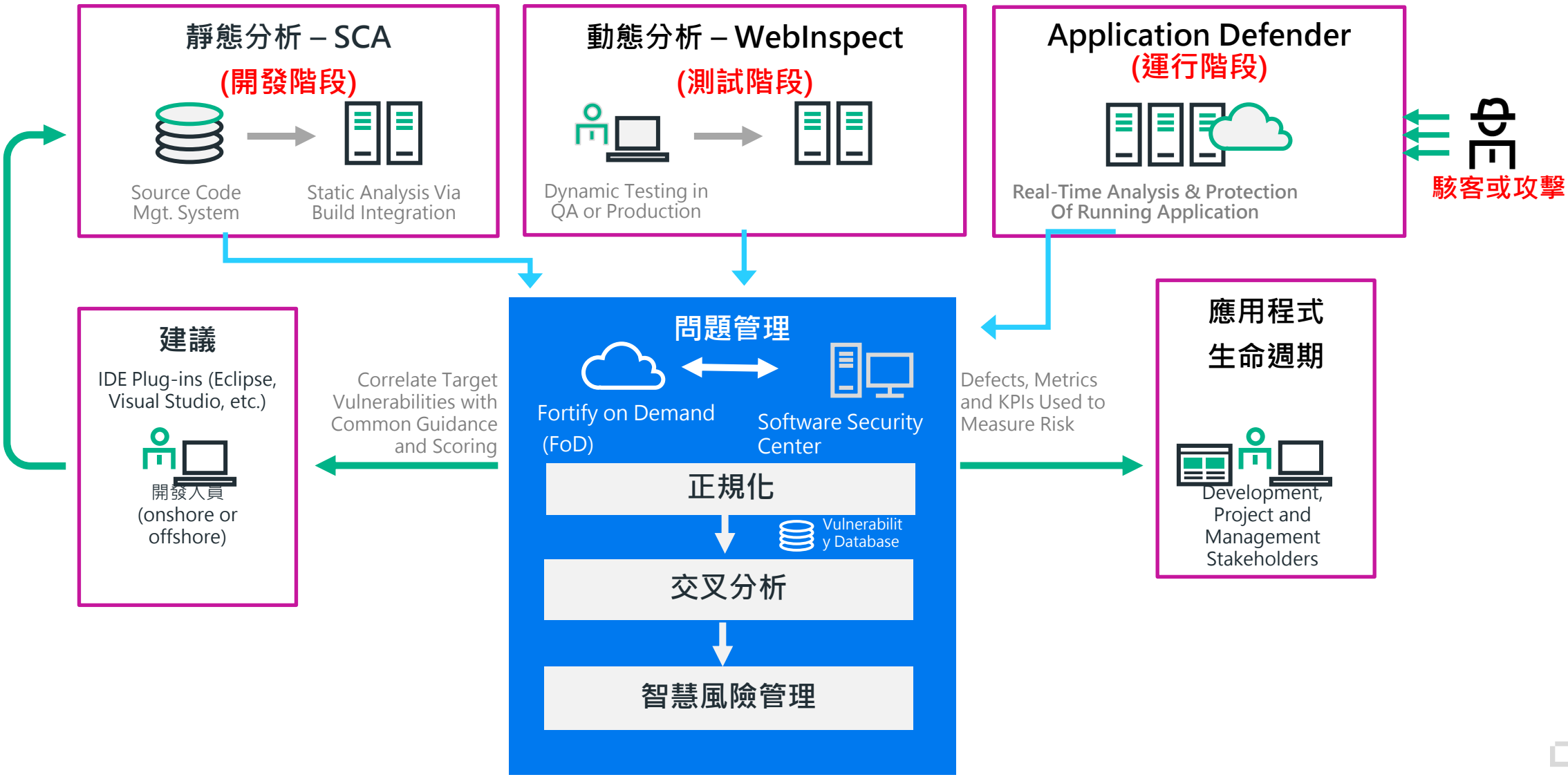
「安全性測試」驗證應用程式潛在安全性瑕疵，分為「源碼靜態分析」以及「動態測試」。「源碼靜態分析」可以在不執行軟體的狀況下，針對軟體的源碼內容進行分析，比對已知弱點模式，找出可能的缺陷或錯誤。「動態測試」則是將軟體在實際的環境中執行起來並進行分析的活動。

源碼靜態分析由於可以直接針對源碼進行檢視，故可被視為是「白箱測試」的一種，「動態測試」則是對執行的應用程式進行測試，故被視為「黑箱測試」。另外「灰箱安全性測試」，其針對黑箱及白箱的檢測結果進行交叉分析，目的在找出真正高風險的問題。

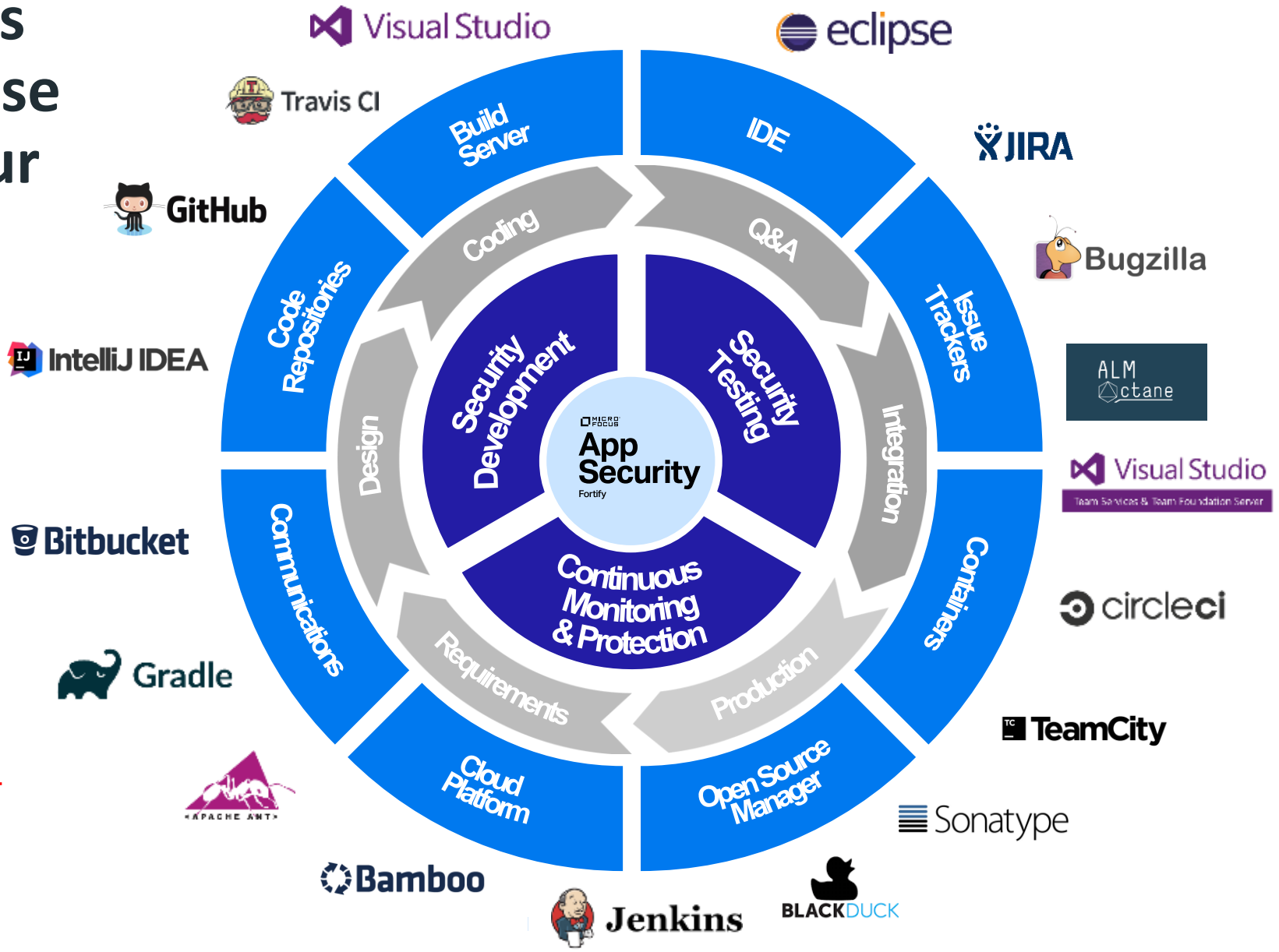
國家資通安全會報技術服務中心103年安全軟體測試參考指引.pdf

MICRO FOCUS

Fortify 解決方案 - 自建及雲端



Fortify integrates with what you use and protects your IT investments



可偵測709種漏洞
支援23種程式語言
涵蓋84萬個API

Gartner 2019

Application Security Testing

Figure 1. Magic Quadrant for Application Security Testing

Source: Gartner (April 2019)

為何選擇 Micro Focus Security Solution

- 10多年來Gartner評選業界領先之資訊安全解決方案
- 單一軟體公司可符合大1-7項資通安全管理法之防護基準要求
- 台灣與全球資安市場市佔率第一
- 台灣政府國安與府院高層均採用之資安風險控管平台
- 資訊安全事件通報整合機制完備
- 國內外資安專業服務團隊人數及資源最多

強化資安人才培育的構想

市場需求：政府及企業需才孔急
構想：開辦資安學程，培育資安人才
例如：

- Fortify
- ArcSight

徵求您的建議...
採用專案提報，取得資源，接軌國際

案例分享：Fortify應用程式安全

- 分享主題

  臺大弱點修補和DevOps上版平臺的建置經驗
- 分享人

  陳啟煌博士 / 國立臺灣大學計資中心

MICRO FOCUS

Micro Focus

感恩您的聆聽與建議

MICRO FOCUS