Consulting Service – Workshop

自由系統資安解決方案—身分識別與存取管理(IAM)

Identity and Access Management Security

Microsoft

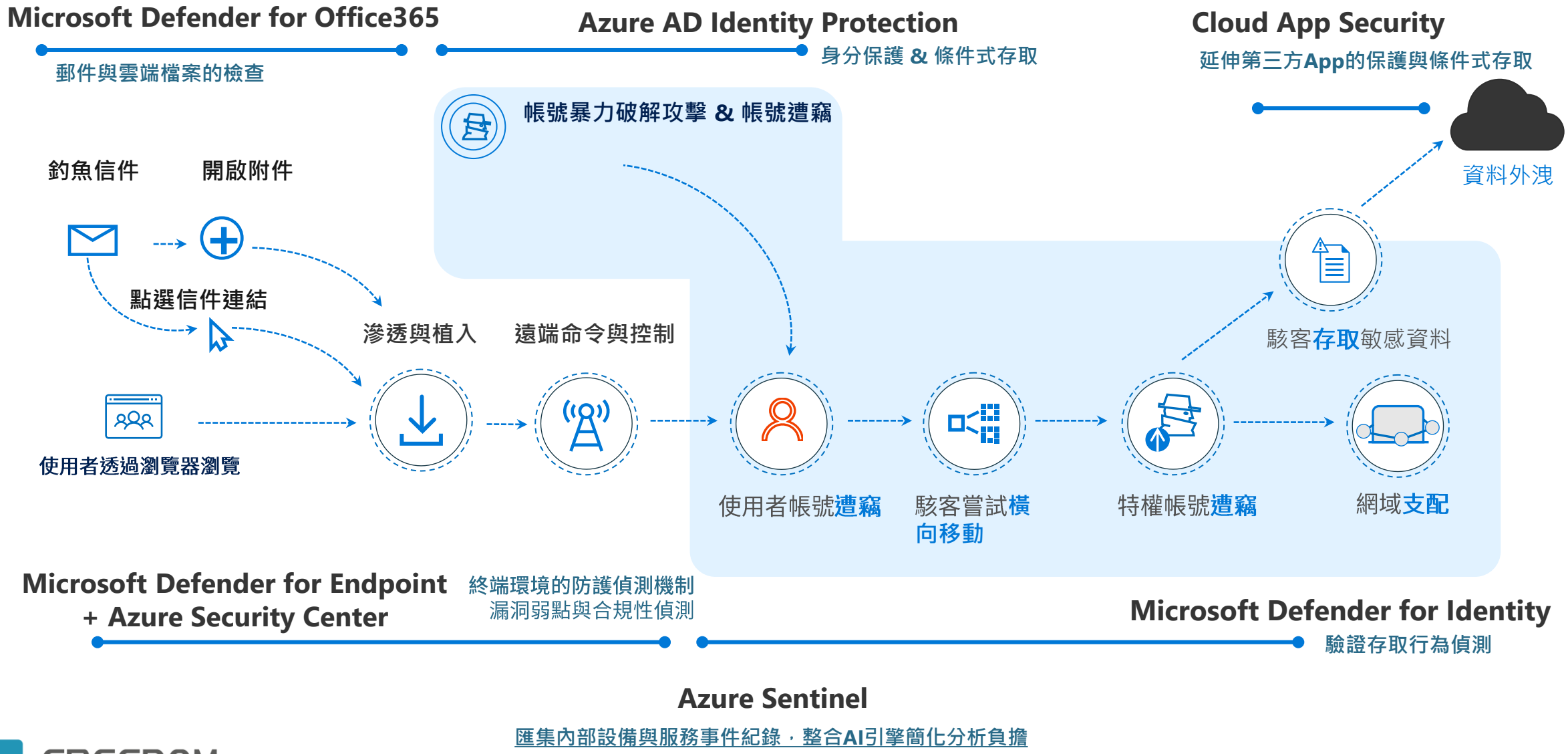
FREEDOM SYSTEMS

自由系統資訊安全服務團隊
Freedom Systems Inc.

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions

智慧化身分保護運行情境流程



FREEDOM SYSTEMS

自由系統如何建構安全的資訊環境

資料 Data

保障**資料本身**受到完善的保護與掌控

裝置 Device

保障資料與身分運行在**高安全性環境**

身分 Identity

保障員工身分**僅由本人**持有與使用

登入的人是否是對的人？若遭駭客竊取身分該如何發現？

網路 Network

保障網路傳輸都是**合規流量**

FREEDOM SYSTEMS

規劃全方位的身分防護

多因素驗證 (MFA)

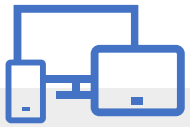
透過多項檢驗、確保端點、雲端、地端環境的身分可信度

登入整合 (SSO)

透過企業系統間信任與連動，減少密碼使用與曝光風險

風險行為保護

透過經驗與人工智慧，視察可疑行為，防範未然



端 點

雲 端

地 端

FREEDOM SYSTEMS

實際案例分享 - 身分安全

FREEDOM SYSTEMS

專業服務
Managed Service

×

Microsoft

雲端資安平台
Cloud Sec. Platform

身分安全	裝置安全	資料安全
身分異常偵測	防毒與端點防護	資料治理與加密
身分存取管理與防護	弱點威脅偵測管理	備份與災難還原
電子郵件社交工程防護		
	更新管理與安全性基準	

資安管理政策		
資安事件管理	變更與組態管理	法遵合規性管理

#身分安全 - 身分異常偵測

此為某台灣工業網通大廠於2020年下半年遭到勒索事件攻擊的後續處理案例

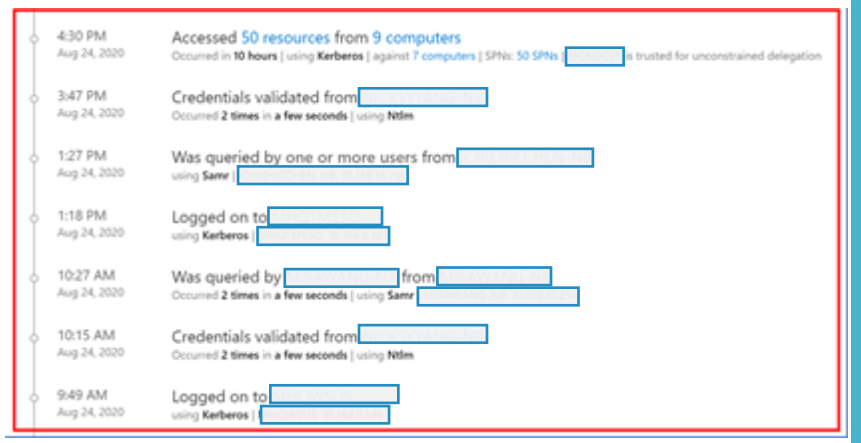
該企業最高權限的網域管理員帳號權限外洩，被用來登入其他台設備進行橫向移動

自由系統透過 Microsoft Defender for Identity 偵測異常AD帳戶行為，以下為事件過程節錄

2020/08/23 下午3點44分
偵測到該帳號有潛在被橫向移動風險

2020/08/23 下午5點至凌晨
透過傳統NTLM驗證嘗試密碼破解

2020/08/24 上午9點~
駭客已成功獲取網域控制權



FREEDOM SYSTEMS

#身分安全 - 身分異常偵測

此為某台灣工業網通大廠於2020年下半年遭到勒索事件攻擊的後續處理案例

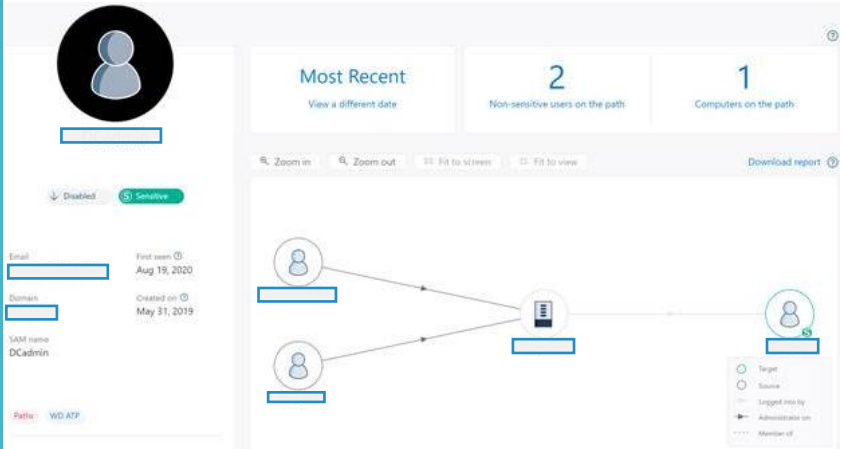
該企業最高權限的網域管理員帳號權限外洩，被用來登入其他台設備進行橫向移動

自由系統透過 Microsoft Defender for Identity 偵測異常AD帳戶行為，以下為事件過程節錄

得知網域管理者遭竊後立即停用帳號
橫向移動路徑，評估潛在衝擊範圍

透過內建橫向移動報告
針對可能影響之特權帳號進行稽查

透過LDAP明碼驗證提示報告
若干特權帳戶密碼可能已外洩



Lateral movement paths to sensitive accounts

Period: 8/20/2020 - 8/25/2020

Lateral movement graphs displayed in the user profile ar

Details

Sensitive Account	Sensitivity Reason
[redacted]	Member of Account Operators
[redacted]	Member of Account Operators
Join	Member of Account Operators
DCadmin	Member of Schema Admins
VMUser	Member of Domain Admins,Enterprise Admins,Administrators,Administrators
[redacted]	Member of Account Operators
ExOrgAdmin	Member of Account Operators,Organization Management,Schema Admins
[redacted]	Member of Administrators,Account Operators,Domain Admins
VMAdmin	
[redacted]	Member of Account Operators
[redacted]	Member of Account Operators
panrunner	Member of Server Operators

Cleartext passwords exposed using unencrypted LDAP authentications

Period: 8/19/2020 - 8/25/2020

Authentications

Last Seen (UTC)	Source Computer	Exposed Account
8/20/2020 12:40:36.395 AM	[redacted]	[redacted]
8/20/2020 12:30:13.628 AM		
8/20/2020 12:29:45.954 AM		
8/19/2020 11:58:24.614 PM		
8/19/2020 11:56:27.525 PM		
8/19/2020 11:38:53.776 PM		
8/19/2020 11:27:02.399 PM		
8/19/2020 11:26:56.727 PM		
8/19/2020 3:25:52.670 PM		
8/19/2020 2:41:48.761 PM		
8/19/2020 2:27:08.154 PM		
8/19/2020 2:23:44.999 PM		
8/19/2020 2:01:00.637 PM		
8/19/2020 1:25:29.032 PM		
8/19/2020 1:24:22.065 PM		
8/19/2020 12:37:26.860 PM		
8/19/2020 12:33:39.209 PM		
8/19/2020 11:52:41.171 AM		
8/19/2020 11:46:54.988 AM		

FREEDOM SYSTEMS

#身分安全 - 身分異常偵測

此為某台灣竹科半導體IC設計公司於2020年下半年內部資安事件攻擊的處理過程

自由系統透過 Microsoft Defender for Identity 偵測異常AD帳戶行為，以下為事件過程節錄

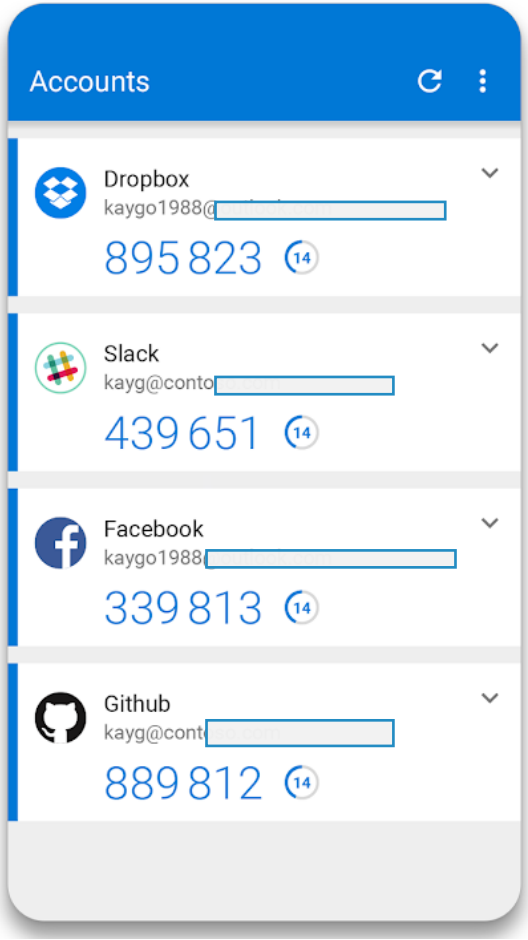
Zerologon被通用漏洞評分系統 (CVSS) 評為風險最高的 10 分，可直接透過漏洞直接駭入網域控制站

黃金票證(Golden Ticket)代表駭客可能已獲得網域控制權，可任意製作Kerberos Ticket登入任何網域內系統

FREEDOM SYSTEMS

#身分安全 - 身分存取管理與防護

Azure MFA 多因素驗證



Azure AD PIM 特權帳戶管理

XX公司

XXX(姓名) is assigned the Global Administrator role for XX公司 Directory

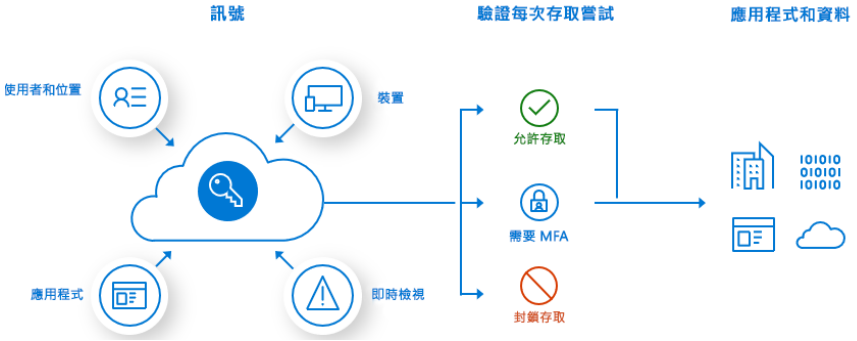
The details of this assignment appear below.
View the details of this assignment in the Privileged Identity Management (PIM) portal.

View details >

Settings	Value
User or Group	XXX(姓名)
Role	Global Administrator
Resource name	XX公司
Resource type	Directory
Updated by	XXX(指派者)
Assignment type	Eligible
Assignment start	February 19, 2021 2:11 UTC
Assignment end	January 1, 0001 0:00 UTC
Justification	-

Privileged Identity Management protects your organization from accidental or malicious activity by reducing persistent access to Azure resources, providing just-in-time or time-limited access when needed.

Azure AD 條件式存取

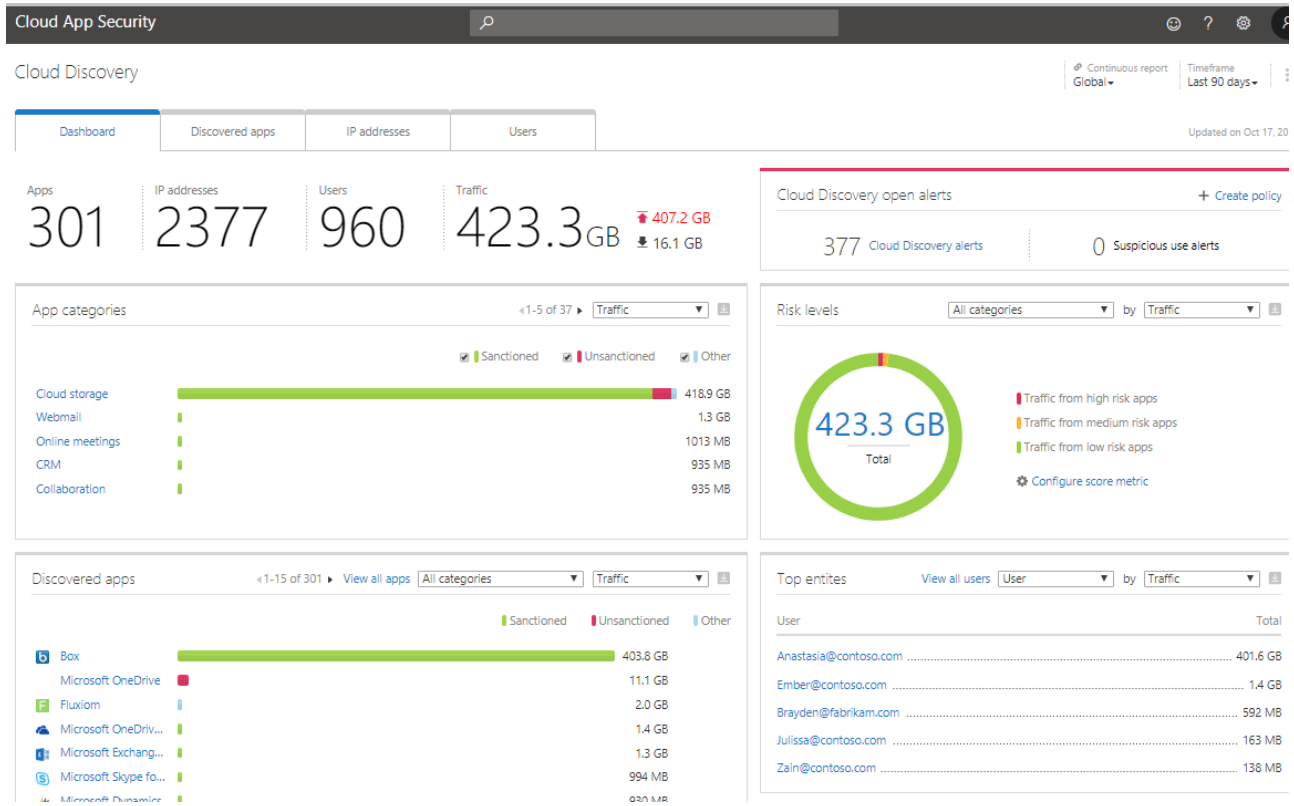


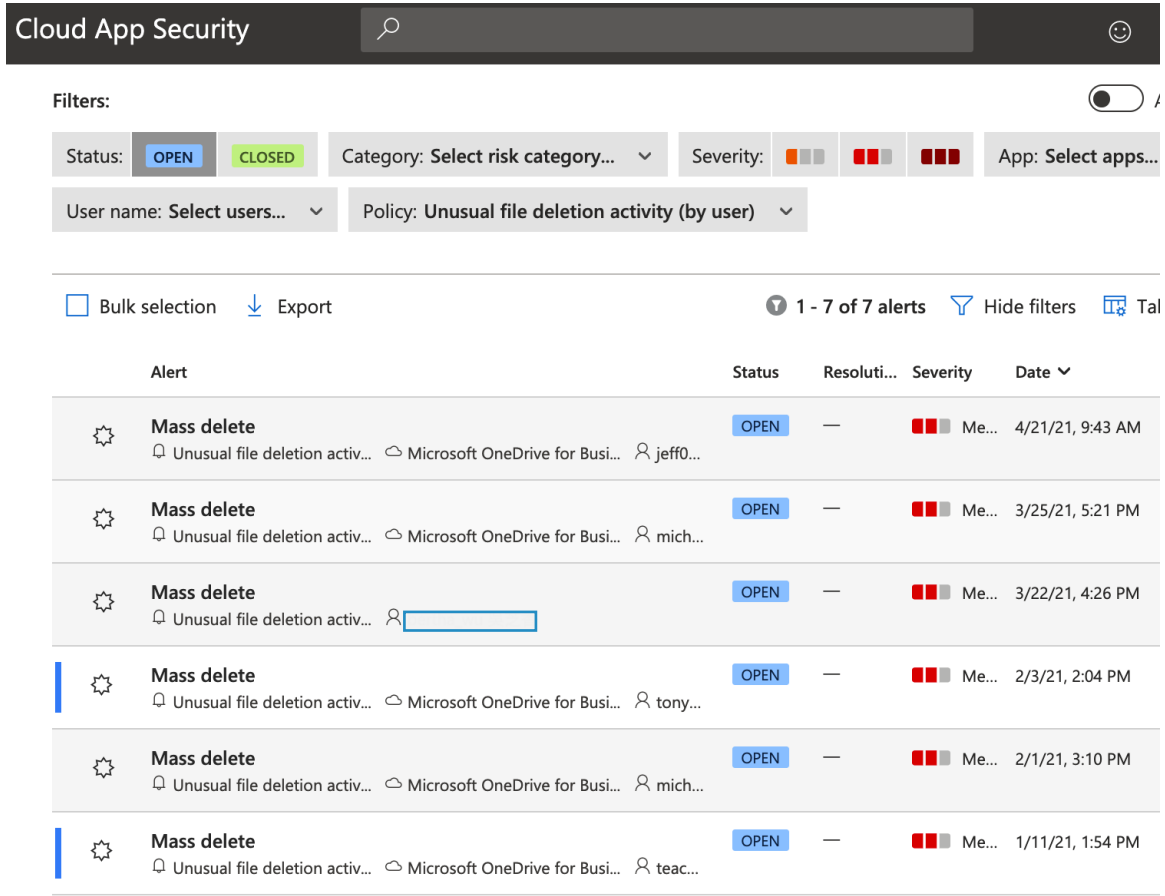
FREEDOM SYSTEMS

#身分安全 - 身分存取管理與防護

Microsoft Cloud App Security 探索組織內雲端應用程式使用，阻絕影子IT不當行為

針對雲端應用程式內的資料與操作行為進行控管，防範潛在威脅與異常狀況





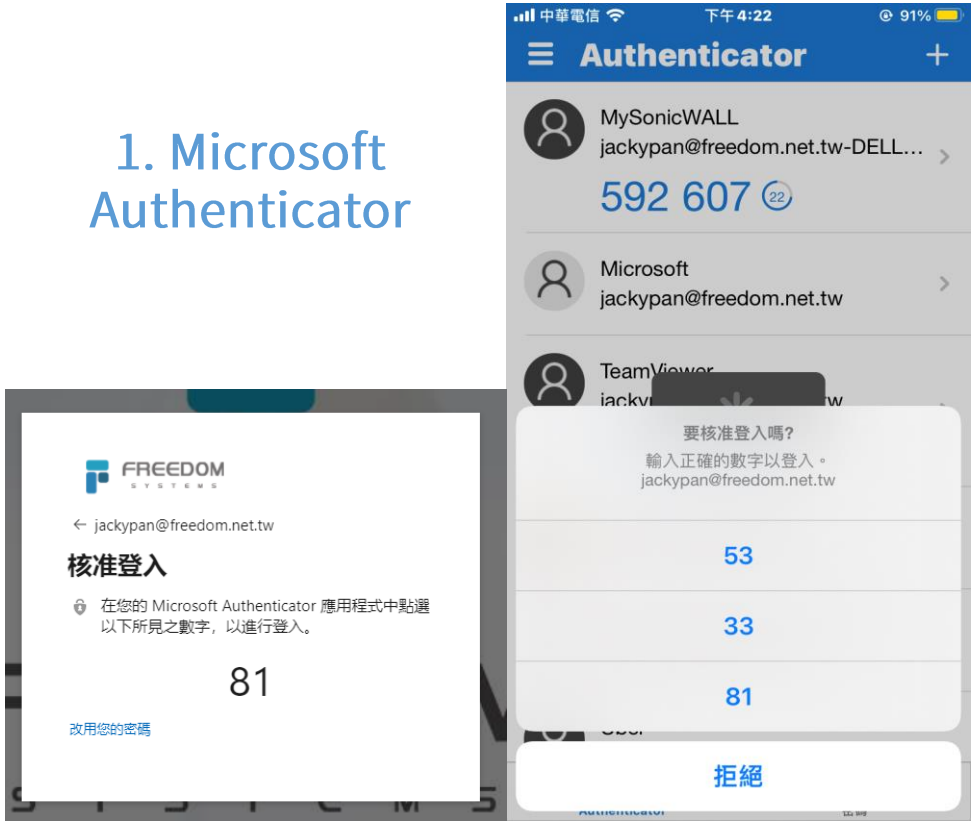
FREEDOM SYSTEMS

#身分安全 - 身分存取管理與防護

自由系統內部已導入無密碼驗證(Password-less Authentication)機制

適合有高機密性需求的產業 (e.g., 半導體、工業產線、生技醫藥…等)

1. Microsoft Authenticator



2. FIDO 2 硬體安全性金鑰

3. Windows Hello 生物辨識 (臉部 & 指紋)

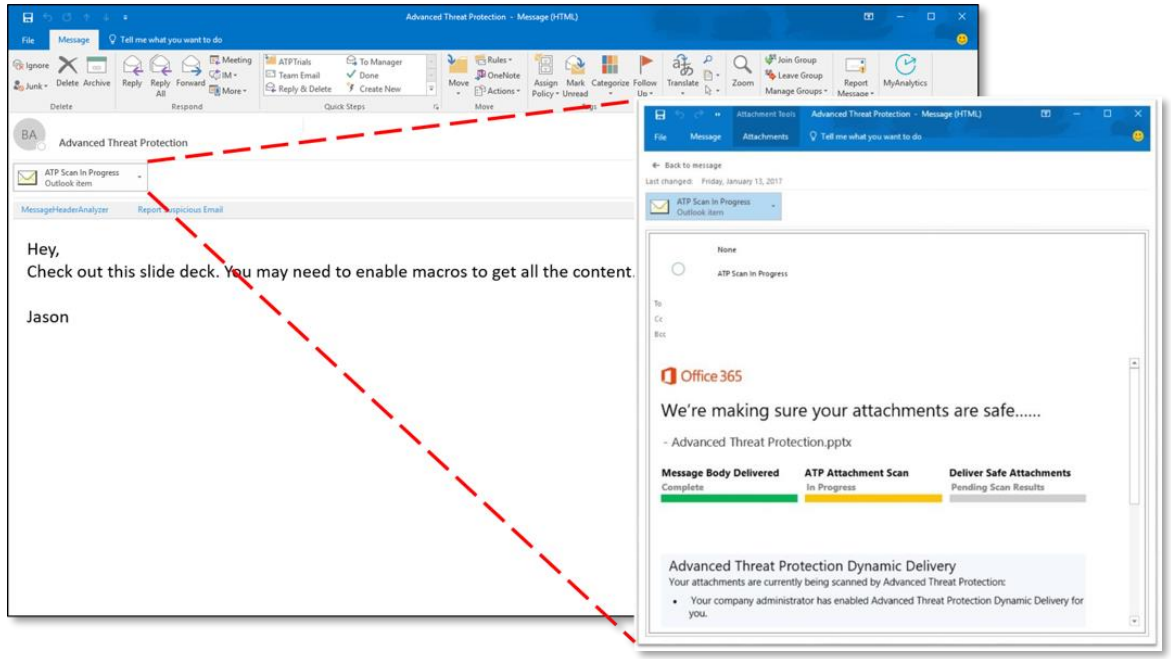
#身分安全 - 電子郵件社交工程防護

攻擊者通常使用電子郵件中的連結引導用戶連到這些極為相似的釣魚網站

騙取電子郵件帳號、密碼及信用卡資訊等機密個資，或將惡意程式（例如勒索軟體）直接下載到用戶的電腦

自由系統的既有客戶有將近80%已透過導入 Microsoft Defender for Office 365 來減緩此網路釣魚攻擊

沙箱掃描



AI 防偽冒分析技術

安全連結沙箱掃描

FREEDOM SYSTEMS

身分安全顧問諮詢服務範圍

Microsoft Defender for Identity 服務項目:
- Health Center 警示解讀分析
- Health Center 警示威脅排除
- Scheduled Reports 解讀分析
- Scheduled Reports 威脅排除

Azure AD Identity Protection 事件回應服務項目:
- 使用者異常行為告警與風險解讀分析
- 設定定期寄出使用者風險報告信件
- 使用者風險自動因應規則訂定(e.g.,強制停用或MFA)

管理者教育訓練與諮詢服務項目:
- Agent代理程式部署操作教學
- 微軟資訊安全管理後台操作諮詢服務
- 提供技術部署文件

高級警示事件(非立即性攻擊)處理:
- 事件偵查與定義
- 依定義層級進行應變處理
- 提供調整建議

中級警示事件(非立即性攻擊)處理:
- 事件偵查與定義
- 依定義層級進行應變處理
- 提供調整建議

緊急攻擊事件回應及處理:
- 回應及遠端連線處理、到場處理
- 攻擊阻斷處理、災情控制應變
- 營運復原計畫及執行
- 攻擊源頭分析
- 漏洞修補與優化建議

定期告警事件檢視:
- 定期蒐集內部正常之事件回報並調整告警設定
- 第三方軟體事件統整及政策調整
- 警報通報機制建立與維護

自由系統的獨到之處與服務效益

即時且高效率地調查、遏制並修補重大資安事件

危機管理與即時應變

事件發生當下，沒有應對經驗的企業容易無所適從。您需要具有豐富處理經驗的團隊進場協助、主導陣營，能就事件相關的溝通事宜給予建議，包含與主管溝通、與IT及其他廠商協作。

蒐集調查威脅情報

若企業沒有資安團隊，往往當事件噴發時無法有效判讀威脅，也無從排除。專家就像解籤師，能透過工具比對數據紀錄、第三方資源等情報，進行有效率的調查、定義問題，找出攻擊的源頭。

以顧問式服務為本位

解決問題才是我們與客戶的共同目標。您不需要擔心廠商銷售不適用的產品，或是解決方案難以在組織落地。從問題洞察到技術維運全部交予一站式的服務，將資安管理納入企業永續經營方針。

專業解籤

判讀事件內容、定義緊急優先程度

即時處理

事件回應及應變處理

動態優化

環境結構調整、工具設定調整

FREEDOM SYSTEMS

資訊安全服務流程

Security Workshop
Estimated Time: 3-5 weeks

針對需求進行部分規模PoC Workshop

■ 工具測試佈署：
基本方案以 Microsoft Defender for Endpoint 及 Defender for Identity 為主要工具，可依照客戶需求調整配置與報價。

■ 資安健檢服務：
於3-5周內佈署後持續監控環境、處理告警並提交結果報告，如過程中發現重大資安漏洞將主動且即時通知客戶處理。

■ 方案價格：
- 約NT$ 10萬 (Estimated Price)

(※依照企業部署規模與客製化程度不同，將影響報價)

Implementation
Estimated Time: 4-5 weeks

確認企業資安需求逐步導入資安產品

■ 完整導入解決方案：
依據Workshop結果報告與客戶溝通需求與現況，進行完整的資安架構規劃，以及完成產品佈署。

■ 佈署後監控與障礙排除：
完成Onboarding後，自由系統將進行短期的監控測試，以及障礙排除，確保工具上線後的正常運作。

■ 方案價格：
- 客製化報價，包含授權費用與專案費用

(※依照企業部署規模與客製化程度不同，將影響報價)

Managed Service
Estimated Time: Pay per mth

自由系統成為委外資安維運夥伴

以訂閱制服務 協助企業動態優化

■ 資安監控服務：
與客戶端協議監控範圍，以及所部署之工具定期監控，並參與定期會議報告

■ 資安改善建議：
定期根據 OS Patch、App Patch 等提交總體資訊環境或資安報告建議

■ 方案價格：
- 月訂閱或年訂閱制付費
- 客製化報價，請洽自由系統

(※依照企業部署規模與客製化程度不同，將影響報價)

※本項服務名目為Workshop，不含正式Implementation及Managed Service。詳細請洽自由系統。

自由系統資安服務客戶案例

Learn More→

研華在2020年底決定開始重新檢討既有資安管理，加強己身的資訊架構體質、降低被攻擊的風險，與縮短被攻擊後的反應時間。自由系統憑藉專業實力在眾多優秀Security Partners之中脫穎而出，成為研華的資安顧問，並分成三步驟確實進行資安健檢：1. 協助分析現況之風險，與現存之攻擊 2. 導入資訊安全工具，並提供資安維運服務3. 提出架構改善建議(AD、Email、Firewall)，並協助執行。

有察於地端server版本老舊，除了日常使用與維運問題，更擔心造成系統資安漏洞。自由系統的首要之務是協助艾訊評估比較升級地端server或上雲端的資訊成本、風險和生產效益，並規劃並執行地端email server移轉上雲端。除了Microsoft 365授權及導入，交給自由系統支援每月技術維運及教育訓練，更與微軟合作進行Security Workshop PoC，使用Microsoft Defender For Endpoint為艾訊降低端點資安風險。

台灣人壽為了因應大量資料處理，並有效從中發掘潛在資安事件，委託自由系統及微軟聯手抵禦資安潛在風險。導入Azure Sentinel後，藉由AI的高度學習及運算能力，以及視覺化的儀表板，將台灣人壽每日60十億位元組的資料，壓縮在半小時內檢視、回應及處理完成，協助內部資安人員更有效進行資源分配及利用。

為確保產業領先地位，瑞昱決心積極佈局資訊安全規劃，以降低經營風險及可能面臨的災損。自由系統透過佈署Microsoft Defender for Identity，優化企業內部的監控機制，若偵測到可疑的駭客橫向移動或攻擊行為，將可在第一時間示警並進行停權及環境檢查，搶在駭客發動更嚴重的攻擊前阻斷其動作。後期陸續使用Azure Security及Microsoft Defender來強化鞏固安全防護，也強化風險警示。

資訊安全與原廠合作認證

自由系統具有全球知名資訊安全組織(ISC)2的專業資格證照
提供的資安服務能更切身協助企業制定資安管理政策，評估風險範圍與有效控制

(ISC)²®

CISSP® | Certified Information Systems Security Professional

CISSP®認證被譽為資訊安全界的最高標準，偏重資安管理概念，主要訴求對象是中高階資安主管，例如CSO(安全長)、CISO(資安官)，或者是資安顧問等

SSCP® | Systems Security Certified Practitioner

SSCP®認證是針對具有資訊安全技術能力且具實務經驗者而設，此證照以公正客觀的標準，界定了企業組織中實際負責運作及落實資安政策相關從業人員的實務工作範圍、角色與職務

Microsoft Partner
Microsoft
Gold Security
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions

Winner Microsoft Partner
2021 Partner of the Year
Taiwan
Microsoft

Hewlett Packard Enterprise Business Partner
Business Partner

cisco Select Partner

vmware PARTNER
PROFESSIONAL SOLUTION PROVIDER

VEEAM GOLD pro partner

DELL PartnerDirect Preferred

Adobe Certified Reseller

Symantec. Specialist Partner
Small and Midsize Business Segment

FireEye Product Specialist

(ISC)²國際資訊系統安全核準聯盟為非營利性的全球知名資訊安全組織，成立於1989年。
(ISC)²開發資訊系統安全核準認證計畫，並為資訊安全人員提供專業資格認證、教育及考試服務。(ISC)²的認證是一張保持中立、客觀的證照，獨立於任何軟體或廠商之外，(ISC)²頒發的專業人員認證受到全世界的認可(符合ISO/IEC 17024全球人才認證評估標準)

FREEDOM SYSTEMS

讓自由系統陪伴您成長，共同打造IT績效

IT is not an issue, call us!

FREEDOM SYSTEMS

02-2655-0668

sales@freedom.net.tw

www.freedom.net.tw