Active Directory 安全: 有時候真實比小說更加荒誕

ACYCRNF7

WHO ARE WE

- > John Jiang
- > Researcher @ CyCarrier
- >UCCU Hacker Co-Founder
- >Focus on
 - > Windows Security
 - Incident Response
- > Speaker of
 - >Black Hat USA
 - > HITB
 - > Code Blue
 - > ...

- >Boik Su
- >Researcher @ CyCarrier
- > CHROOT
- Focus on
 - > Windows Security
 - > Web Security
- > Speaker of
 - > OWASP Global AppSec
 - > ROOTCON
 - > HITCON

> ...



為什麼有這場 Talk

AD 令人又愛又恨

>AD 安全已成顯學,每年安全漏洞一直報

> PetitPotam (CVE-2021-36942)

- >sAMAccountName Spoofing (CVE-2021-42278, CVE-2021-42287)
- > Certifried (CVE-2022-26923)

>KrbRelayUp

>企業本身 AD 安全沒有正規化的檢查方式

> 難以得知 AD 健康狀況

>從實際案例出發,分享從中小型企業到大型企業,普遍存在哪些 AD 安全問題



不同場域大小的 AD 管理狀況

>小型企業 AD 少見特殊的 AD 攻擊手法

> 沒有權限分隔,較常發現高權限帳號被 Compromised

> 給予特殊權限的情況少見,取而代之的是大家權限給好給滿

> 安全性設定保持在預設狀態,較少調整過

- >常聽到的進階 AD 攻擊手法,在大型企業 AD 中較常出現
 - >因為資安要求較高,會設定管理分權,就可能出錯
 - >服務眾多,奇奇怪怪的軟體

> 歷史債很多,都是超過10年以上的AD

實際場域歸納出的常見管理問題分類

程度	管理群組	維運、日常帳號分隔	設定檢查	盤點帳號權限	核心資產範圍
沒在管理	×	×	×	×	×
嘗試管理	\checkmark			×	×
管理了,但還 是有一些失誤					
管很好	\checkmark		\checkmark		\checkmark

✗ 完全沒有實施▲ 實施但涵蓋不完全✓ 完整實施





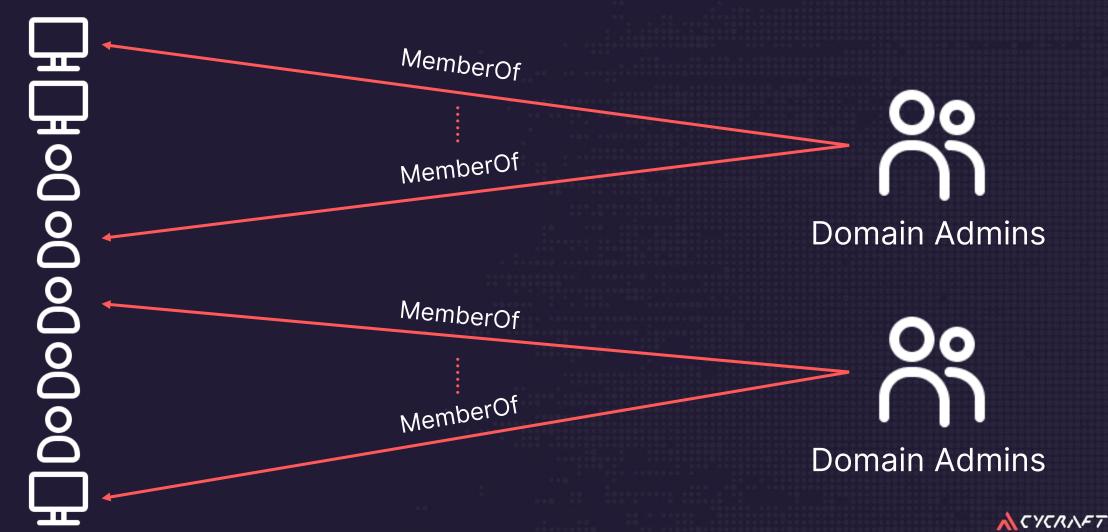
沒有管理群組

>只要是 IT 部門的員工帳號都是 Domain Admins

>預設群組用好用滿

- > Account Operator (不要加)
 - > As a best practice, leave the membership of this group empty, and do not use it for any delegated administration
- > Print Operators (謹慎加)
 - > Because members of this group can load and unload device drivers on all domain controllers in the domain, add users with caution
- >大部分的人根本不需要此權限,一人失守全部淪陷
- >建議動作:權限分隔、人員與維運帳號分開

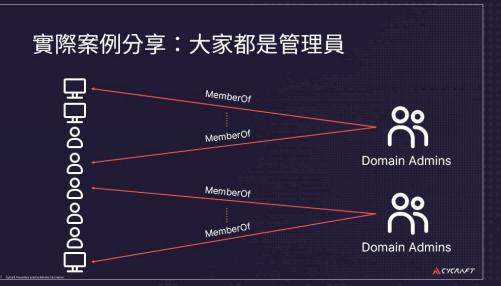
實際案例分享:大家都是管理員



10 CyCraft Proprietary and Confidential Information

案例檢討:大家都是管理員

>管理群組的成員組成通常關聯性強烈 >此案例中的成員組成大部分都來自不同 OU >除了使用者帳號,也有電腦帳號 >這狀況不只出現在主網域,子網域也有一樣問題 >代表並非一時權限委派出錯,而是管理群組在設計時存在觀念上的錯誤





設定了管理群組,但還是有問題

>常見幾種管理群組設定:

>開了額外的管理群組負責處理重設密碼請求,但成員組成不明
>開了很多額外的管理族群,層層迭代、嵌套,致權限模糊不清
>管理群組雖有權限分散,但其他帳號擁有群組操作之相關權限

>建議動作:

>建立一套機制審核管理群組的成員組成
>不要過度切割群組,並應適時審核複查
>帳號及群組權限盤點應定期執行、檢討



13 CyCraft Proprietary and Confidential Information



প



- >Pwd Mgmt 看起來是管理密碼的群組,卻對中間群組擁有 GenericAll 權限
- >中間的群組又對 Users Container 擁有 GenericAll 權限

> 權限設定問題 > 業務用途

>層層嵌套造成問題

實際案例分享:



ACYCRNF7

14 CyCraft Proprietary and Confidential Information





合維運、日常帳號分隔

設定檢查

盤點帳號權限



管理帳號不預期地到處留下蹤跡

>管理帳號沒切割,很容易造成 Credential Dumping >常見且重要的 AD 安全問題

>除了常見管理人員 AD 管理帳號登入並操作其他主機,還有:

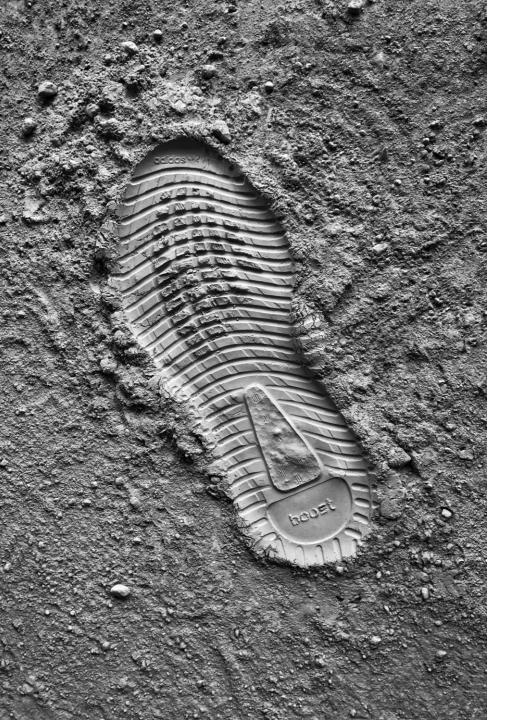
🔥 ር ሃር ጸ ለ F T

>軟體登入(e.g. 備份帳號)

> 排程事件

> 部署軟體帳號

>憑證遺留的問題比你想的還要嚴重



登入必留下足跡 也是駭客攻擊的機會

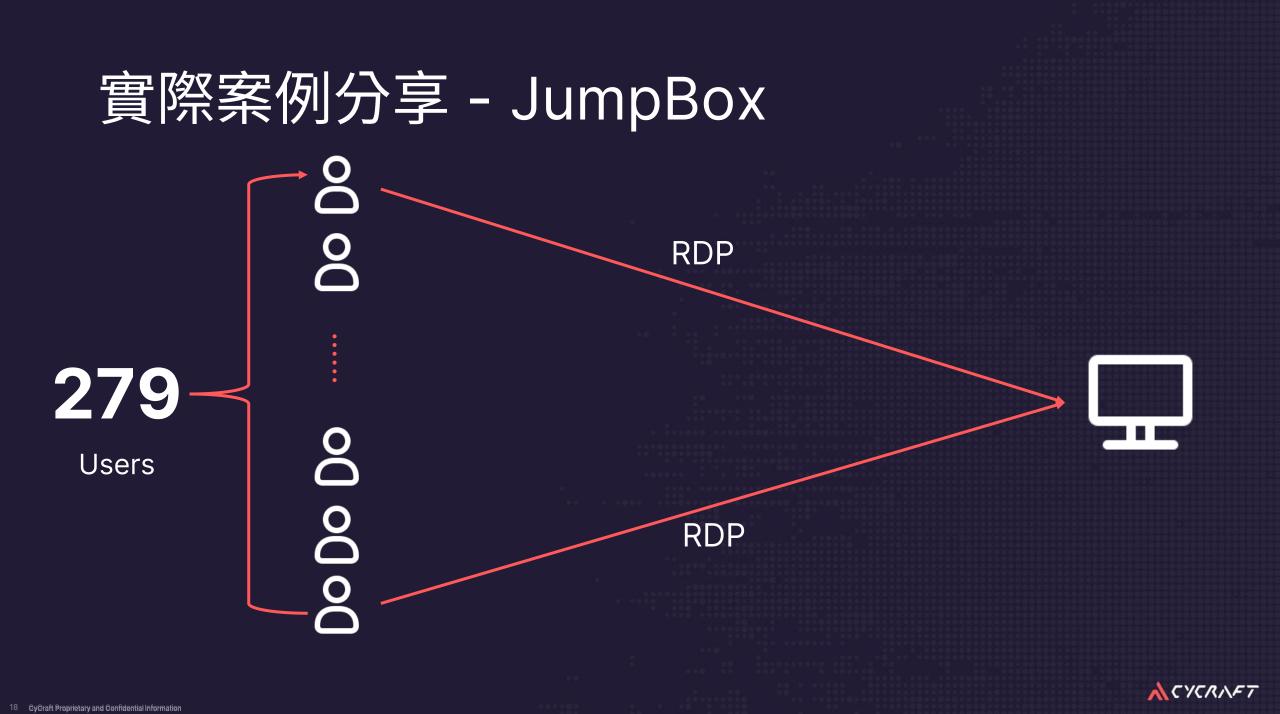
Cached Credentials

- > Mimikatz (Ticket/Hash)
- > Rubeus (Ticket)
- > mscash

Relay Auth

- > KrbRelay (Kerberos relay)
- > RemotePotato0 (NTLM relay)
- > Lsarelayx (NTLM relay + Downgrade)

ACYCRNFT



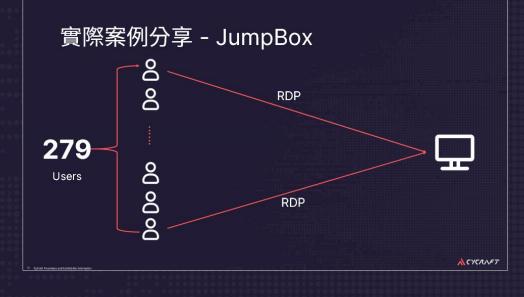
實際案例分享 - JumpBox

> 許多單位設定 Server 電腦讓員工共用主機 > 其中最常見的形式讓多個使用者(如: Domain Users) 可以 RDP 同一台 主機

>攻擊方式:

Cross-Session Attack

- > Relay Auth 到 ADCS 主機
- > Relay Auth 做 Shadow Credential



<u>∧</u>сус∧, г7

🔀 Windows PowerShell



– 🗆 🗙



¥



管理群組 維運、日常帳號分隔

合設定檢查

盤點帳號權限



AD 場域的各種設定錯誤

> Default Components:

- > Group Policy 讓不預期的人員修改 GPO
- > SPN on Users 被破解密碼的風險
- > Network Shares 權限開放過大

> ...

>Auth Related:

- >AD CS 權限、範本設定錯誤
- > Azure AD Connect 不預期的人員能夠影響雲端

> 2FA Service (<u>https://www.cisa.gov/uscert/ncas/alerts/aa22-074a</u>)

實際案例分享:"我們的"憑證

 > 錯誤設定憑證範本權限
 > 要賦予所有使用者註冊權限多給予修改權限
 > 所有使用者可以修改範本內容從而提權到 Domain Admins

Subject Name Server			Issuance Requirements				
Superseded Templa	ates	Exter	nsions	Security			
Group or user names:	Group or user pames:						
🎎 Authenticated Use	ers						
Administrator		-					
Service Communities (V				、			
Domain Computer & Enterprise Admins)			
Encoprise Adminis	(THEOMA	in third	nao numina)				
			Add	Remove			
Permissions for Authent	icated Users		Allow	Deny			
Full Control							
Read Write							
Enroll							
Autoenroll							
Autocritoli			;;				
Factor and a service in a			aliala 🗌				
For special permissions or advanced settings, click Advanced							
Advanced.							
Advanced.							
Advanced.							

Properties of New Template

 \times

實際案例分享: "我們的" 憑證

1

erOf

Domain Users

Modify Template

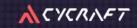
MemberOf

Any User

24 CyCraft Proprietary and Confidential Information

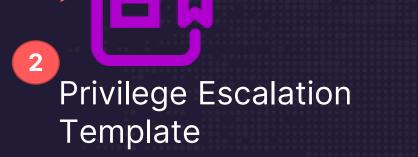
Misconfigure Template





實際案例分享: "我們的" 憑證

Modify Template





ACYCRNFT

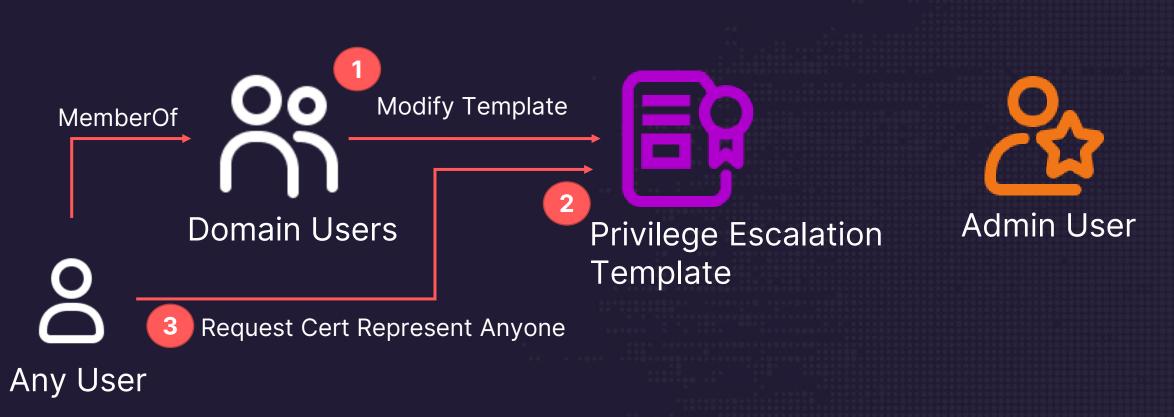
MemberOf

Domain Users

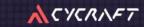
Any User

0





V # 4 50 4





27 CyCraft Proprietary and Confidential Informatio

實際案例分享:AAD Connect Service Account GetChangesAll GetChanges

Account Operators

MSOL_XXX

Password Hash Synchronization (PHS)

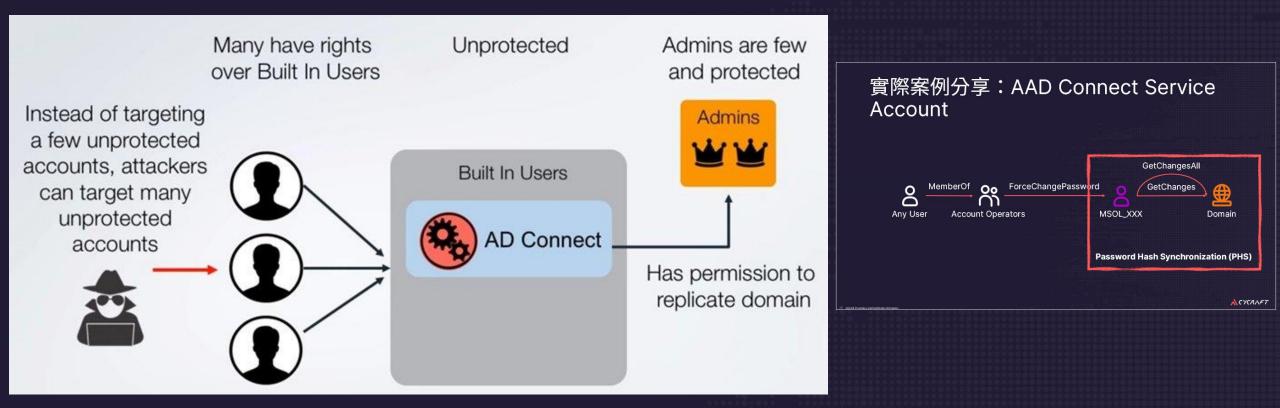


Domain

28 CyCraft Proprietary and Confidential Information

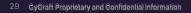
Any User

案例檢討: AAD Connect Service Account



https://www.youtube.com/watch?v=M_06E-MkKIQ

ACYCRNFT







維運、日常帳號分隔

設定檢查

分盤點帳號權限



企業中帳號權限設定的痛點

>對於特定資產應該有什麼權限沒有概念

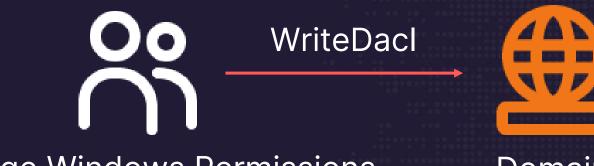
>不清楚權限帶來的功能與風險

>為了方便給定一組權限 (Property sets) 但沒有了解其賦與的權 限為何

🔥 CYCRNFT

>不曉得 AD 預設機制賦予的權限

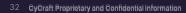
實際案例分享: Exchange AD Privesc



Exchange Windows Permissions

Domain

A CYCRNFT



案例檢討: Exchange AD Privesc

>不論是 Exchange Server 2010, 2013, 2016, 2019, 使用 RBAC Split 或是 Shared permissions 模型,都會在安裝過程 中引入高權限的安全群組

- > Organization Management
- Exchange Windows Permissions
- >Exchange Trusted Subsystem
- >這些高權限的安全群組
 - > 有些對於網域物件擁有 WriteDACL 權限 > 可以發動 DCSync 攻擊

實際案例分享:Exchange AD Privesc





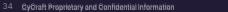
🔥 ርΎር ጸሊ 🕫 7

實際案例分享:我是你的主人

>給予負責加入網域人員對 OU 有權限建立電腦物件
 >透過負責加入網域人員的帳號讓電腦加入網域
 >負責加入網域的人員變成 Computer Owner
 >Owner 能夠透過設定 DACL 進行 RBCD/ShadowCred
 >較有資安意識的單位會設定
 >MachineAccountQuota = 0

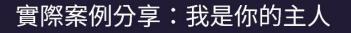


🔥 ርΎር ጸ.\.F7



案例檢討:我是你的主人

>加入網域人員是預期管理人員,無須修正 >如否,需定期回收 Owner 身分



- >給予負責加入網域人員對 OU 有權限建立電腦物件
 >透過負責加入網域人員的帳號讓電腦加入網域
 >負責加入網域的人員變成 Computer Owner
 >Owner 能夠透過設定 DACL 進行 RBCD/ShadowCred
- >較有資安意識的單位會設定 >MachineAccountQuota = 0

Delegation of Control Wizard	×
ative Directory Object Type Indicate the access of the task you want to delegate.	P
Datagete-control of	
O The folder, wanting objects in this folder, and creation of new objects in the	is folder
· Only the following stracts in the folder	
accuset elgents accuset elgents accuset elgents accuset elgents accuset accuset elgents constancionations constancionations constancionations constancionations	4
Conste assected dijects in this folder	
Culture adjusted algorits in this fulder	
c Back Next 3 Carvad	140





管理群組 維運、日常帳號分隔

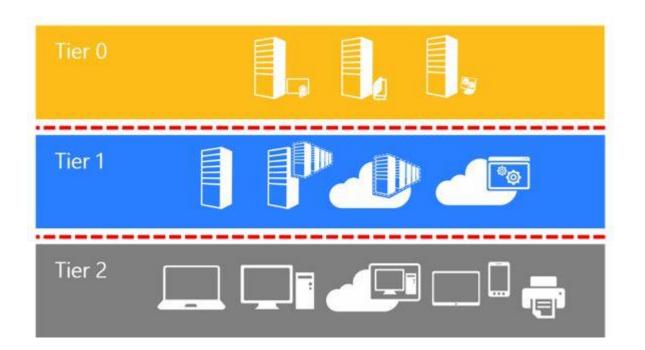
設定檢查

盤點帳號權限

合核心資產範圍

以往常見的三層架構(微軟提出)

- >雖然此架構並不是最新適合雲 的架構,但這令我們容易理解 分層的重要性
- >企業應該且必須有能力盤點出 核心資產是哪些
 - > Tier 0:影響整個網域的伺服器
 - > Tier 1: 企業伺服器
 - >Tier 2:標準使用者工作站



https://docs.microsoft.com/zh-tw/security/compass/privileged-access-access-model

常被忽略的核心資產種類

>常見系統:

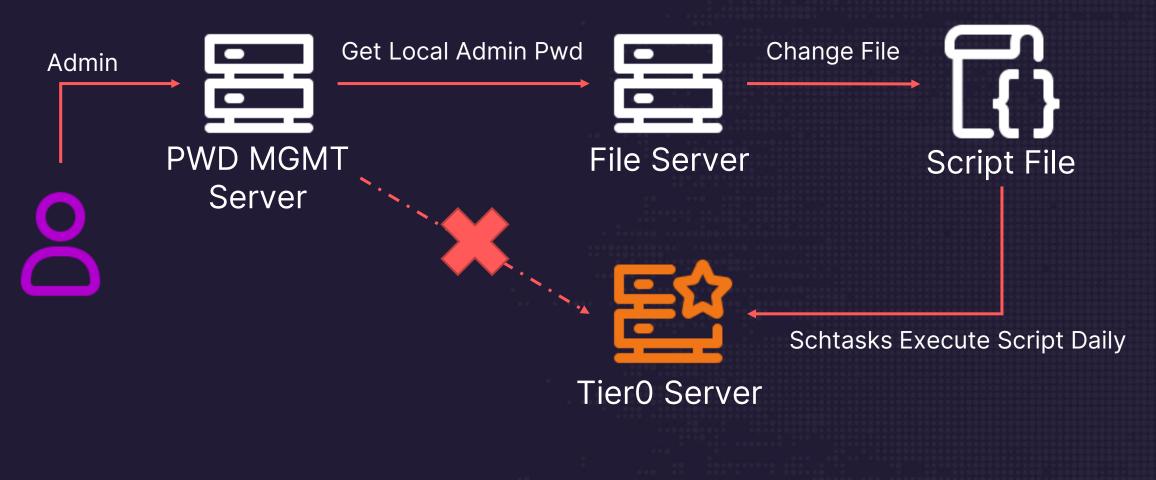
> Azure AD Connect ,直接雲端、地端一次掌握
> ADCS 主機,地端主機一次掌握
> ADFS 主機,雲端資源一手掌握
> LAPS Server

>其他核心:

- > 派送軟體 Server
- >核心資產會執行檔案的檔案伺服器
- > 特權管理系統 (常見於特權管理附加在 AD 身上)

>密碼管理平台

實際案例分享:你以為的核心資產





案例檢討:你以為的核心資產

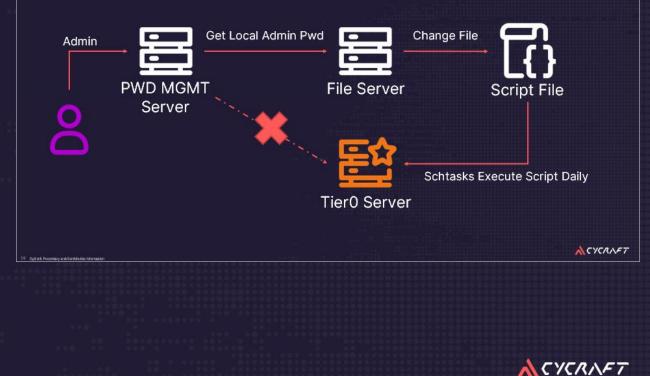
>被忽略的地方:

- > 不曉得 TierO 伺服器有下載外部 資源且執行的排程
- > 沒將密碼管理平台納入核心資產

>做的對的事

>將核心資產的管理與其他層分開

實際案例分享:你以為的核心資產



該如何解決 網管對於 AD 上核心資產為何不是很確定

- >對於重要帳號/電腦缺乏基本認識
 - > 可透過 Active Directory 帳號權限掃描建立基本盤點資料
- >缺乏對於帳號登入事件的監控、控管
 - >將前面建立的盤點資料作為目標,用端點/AD Log 監控重要帳號登入狀況
- >AD 攻擊過於複雜,網管不是短期能理解完的 >分享中有提到的資產,可以確認並詢問專業人士



如何評估自身場域

熱圖 – 不同大小場域遇到的威脅分布

* 1U = 1 使用者帳號 / 電腦帳號

場域大小 (U)	管理群組	維運、日常帳號分隔	設定檢查	盤點帳號權限	核心資產範圍
<1,000					
1000 ~ 10000					
> 10,000					

>大中型場域因服務多、權限控管複雜,常出現核心、權限問題
>中型場域通常缺乏分隔控管,容易出現憑證竊取問題
>設定檢查無論大小都可能出錯

100%

0%



- 參考我們的熱圖,找到與你同樣 大小的企業
 - 參考今天簡報並研究相關問題
 高掌握度(綠)的問題類型先解決
 棘手(紅)的問題類型需積極處理

熱圖 – 不同大小場域遇到的威脅分布



* 場域大小/新舊, 背負的營運安全風險不同



Thank You Any Question?



CyCraft Proprietary and Confidential Information