

AD 安全與維運： 累積的安全問題與擴大的安全邊界

此議程為系列議程，建議先聽過去年的

- > 網管的資安迷思：Windows AD 的安全冷知識
- > 權限、信任、地雲端串接的可攻擊點



總結

- 重設密碼並非萬用解，要**了解受災範圍**
 - 了解真的需要重設的帳號是甚麼
 - **注意 AD 架構中不為人知隱藏的帳號**(e.g., krbtgt...)
- 大型 AD 環境經常給予過多的權限、過度信任
 - **了解使用者獲得的是甚麼樣的權限**
 - SIDHistory 可以造成跨樹系提權，需要重新**注意 AD 樹系的信任關係**
- **重新看待雲端與地端關聯，地端是能夠影響雲端的**
 - 任何雲端與地端整合的地方(ADFS/ADConnect...)，也會是重點保護的目標

EVERYTHING
STARTS FROM CYCRAFT

萬能新網 Proprietary and Confidential Information



其他技術細節

- > HITCON PEACE 2022
 - > HITCON YouTube 頻道

- > Blue Team Summit 2022
 - > 10/04 Online Free

Active Directory 安全：有時候真實比小說更加荒誕

中文 現場演講 企業藍隊

Windows Active Directory (AD) 一直都是讓人們又愛又恨的服務，由於 AD 的高市佔率，各家廠商與各式軟體都搶著與它相容，但另一方面，當大量的新舊服務都高度依賴與 AD 的整合時，在複雜場域之下或許相得益彰，然而維運人員過於依賴也將導致解耦困難，在維運過程中不敢對部分的安全性設置動手。基於上述這些問題以及 AD 維運的歷史性因素，在過往的調查中，我們時常在場域中發覺許多地下網管 (Shadow Admins) 的存在，伴隨著近年來層出不窮的 AD 安全性問題，企業資訊安全正面臨極大的考驗。

本議程將是與過往截然不同的 AD 安全議題分享，我們將從實際分析過的企業案例中，挑選出誇張的錯誤範例，並對其進行詳細的技術分享、探討可能形成安全破口的因素，例如未確實執行設定檢查、缺乏帳號與資源間的權限盤點、核心資產遭到忽略，以及因實作權限分隔而導致的更多安全問題等。最後，我們將依據這些 AD 場域的資安程度做分類，以提供會眾了解自己企業 AD 的相對安全程度，透過實際案例反思自己還能做哪些事情來加強 AD 場域的安全。

Mon, October 3

Tue, October 4

2:00 pm - 2:45 pm PT

9:00 pm - 9:45 pm UTC

Add to Calendar

Plenary Session

Don't Relay Me: Empirically Diagnose Privilege Escalation via Active Directory Account Sighting

Shand-De "John" Jiang, Cybersecurity Researcher, CyCraft Technology

Gary Sun, Cybersecurity Researcher, CyCraft Technology

Show More



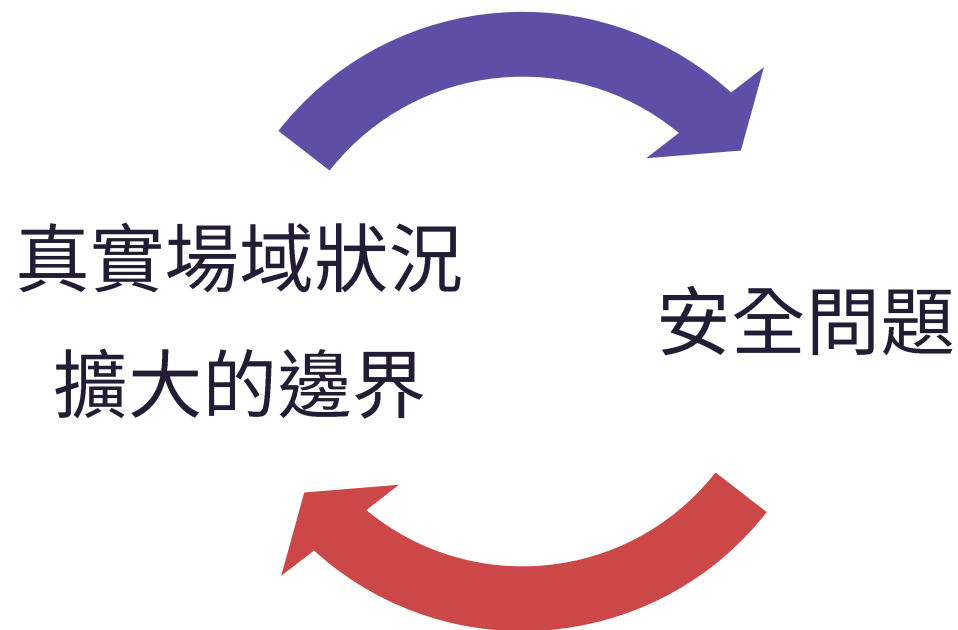
自介

- > 奧義智慧 – 資深資安研究員
- > UCCU Hacker 共同創辦人
- > 多場國際資安研討會講者
 - > BlackHat
 - > HITB
 - > HITCON
 - > CodeBlue
 - > ...
- > 專注於事件調查、Windows Security



議程綱要

- > 累積的安全問題
- > 利用你忽略的功能
 - > 潛伏/提權
 - > 竊取密碼
- > To The Cloud !



An abstract graphic on the left side of the slide. It consists of several overlapping, semi-transparent shapes in shades of red and dark blue. A prominent white outline of a right-pointing chevron is positioned to the left of the main title text.

累積的複雜權限

快速介紹 AD 權限的複雜的狀況

- > 歷史因素，就像你的前任留下的爛攤子
 - > 測試帳號權限沒移除
 - > 密碼寫在敘述上
- > 對於權限的不熟悉導致的錯誤設定
 - > 賦予管群組權限，結果連使用者都變成可管
- > 軟體自動幫你設定的權限
 - > 例如: SQL Server 幫你帳號設定 SPN 導致密碼可能被破解
 - > 有些軟體會自動幫你建立群組

歷史因素 – 案例(前人留下的奇怪權限)



> 任何人都能讀取伺服器的擴充許可權(Extended Right)欄位

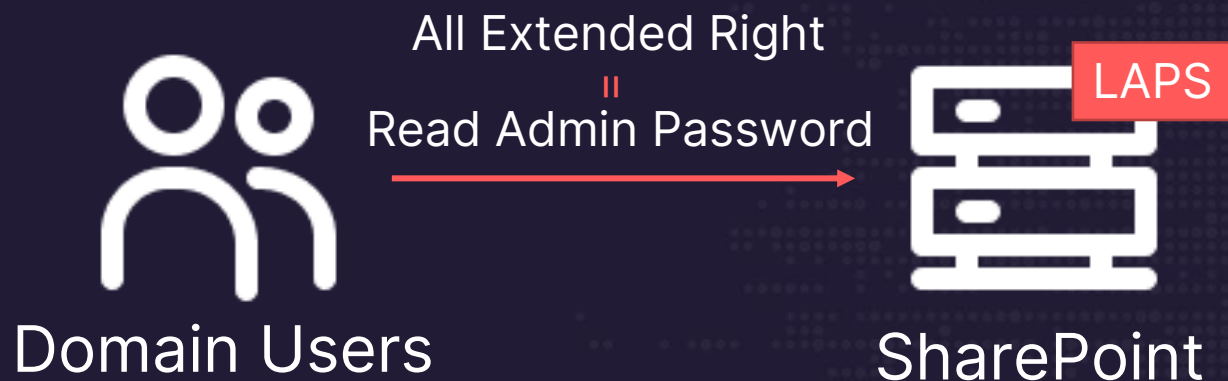


| Extended Right Example | Description |
|--|---|
| Change Password {ab721a53-1e2f-11d0-9819-00aa0040529b} | Permits changing password on user account. |
| Reset Password {00299570-246d-11d0-a768-00aa006e0529} | Permits resetting password on user account. |
| Receive As {ab721a56-1e2f-11d0-9819-00aa0040529b} | Exchange right: allows receiving mail as a given mailbox. |
| Send As {ab721a54-1e2f-11d0-9819-00aa0040529b} | Exchange right: allows sending mail as the mailbox. |

歷史因素 – 案例(前人留下的奇怪權限)

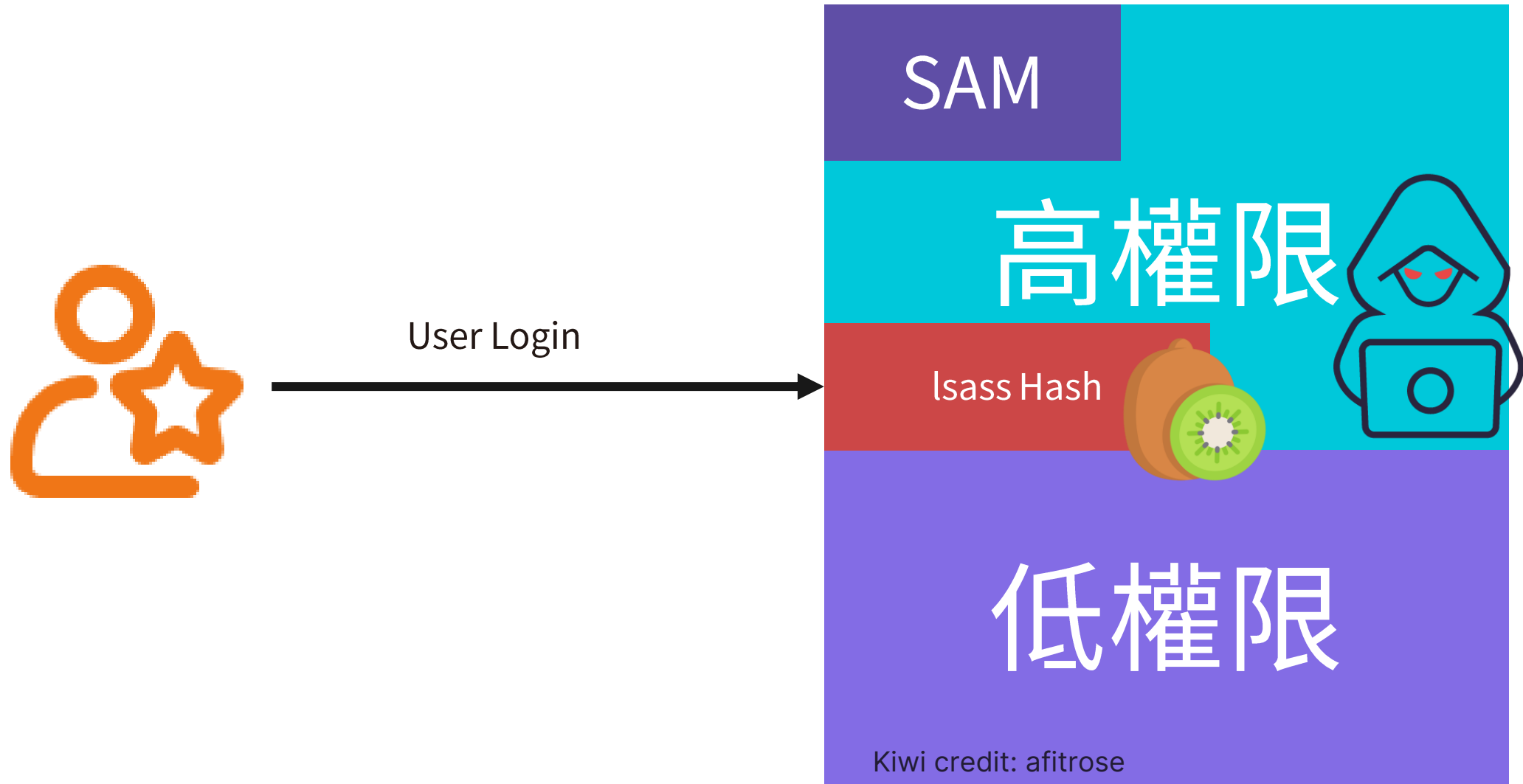


- > 任何人都能讀取伺服器的擴充許可權(Extended Right)欄位
- > 後來引入 LAPS 後，組合成可利用的攻擊



上述問題基本上是靜態的
但配上動態的資料
安全 AD 評估就更複雜了

違規操作 – 駭客有高權限有機會竊取憑證

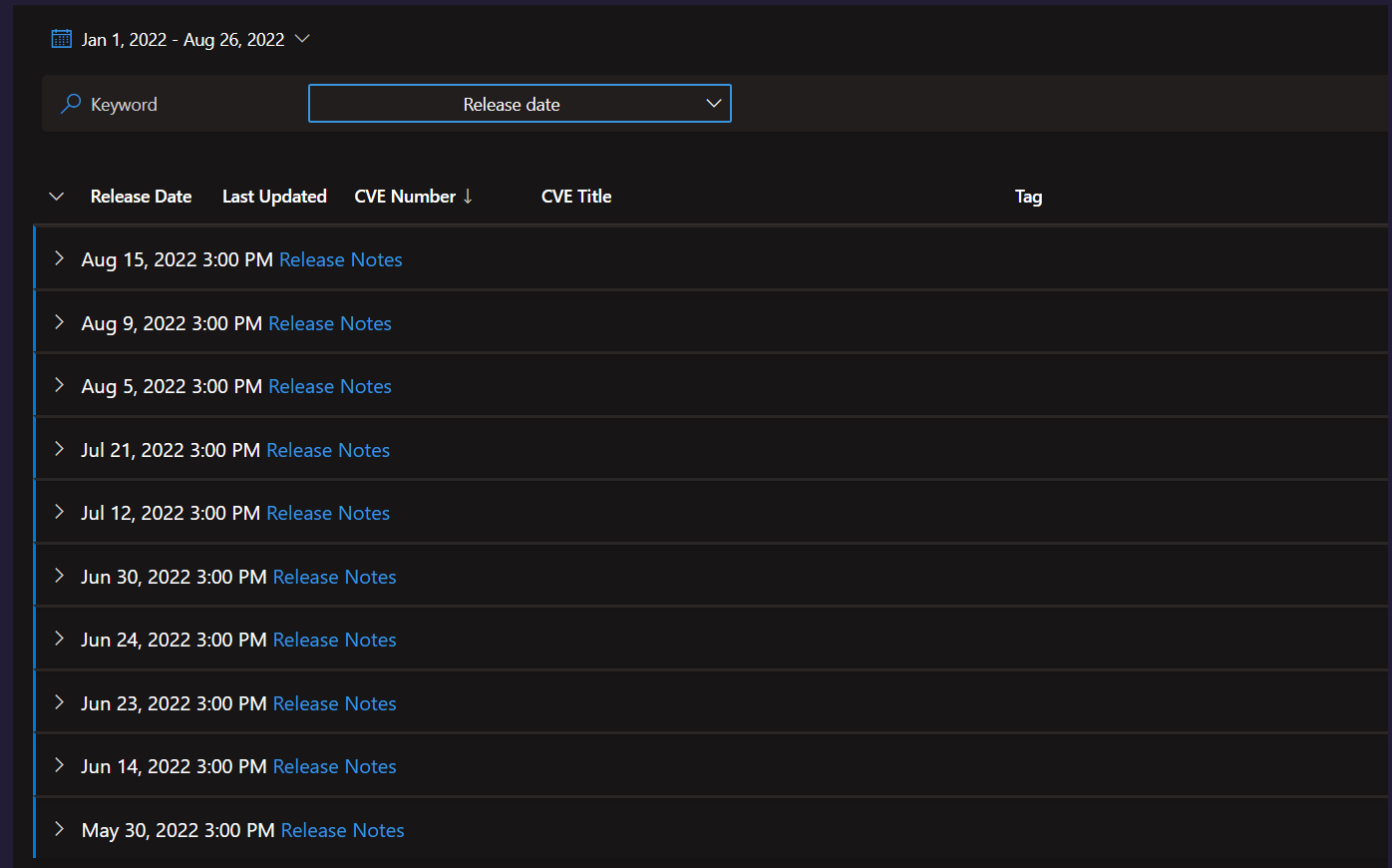


駭客哪那麼容易提權？

2022年 01~08 月

Windows 提權 CVE

966 個



| Release Date | Last Updated | CVE Number ↓ | CVE Title | Tag |
|------------------------|--------------|--------------|-------------------------------|-----|
| > Aug 15, 2022 3:00 PM | | | Release Notes | |
| > Aug 9, 2022 3:00 PM | | | Release Notes | |
| > Aug 5, 2022 3:00 PM | | | Release Notes | |
| > Jul 21, 2022 3:00 PM | | | Release Notes | |
| > Jul 12, 2022 3:00 PM | | | Release Notes | |
| > Jun 30, 2022 3:00 PM | | | Release Notes | |
| > Jun 24, 2022 3:00 PM | | | Release Notes | |
| > Jun 23, 2022 3:00 PM | | | Release Notes | |
| > Jun 14, 2022 3:00 PM | | | Release Notes | |
| > May 30, 2022 3:00 PM | | | Release Notes | |

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/Relay Auth
 - > 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：
 - > 軟體登入(e.g. 備份帳號)
 - > 排程事件
 - > 部署軟體帳號
- > 不管是 RDP, WINRM, Network Share Access，都可能被利用，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)



登入必留下足跡 也是駭客攻擊的機會

Cached Credentials

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

不用碰到
Lsass

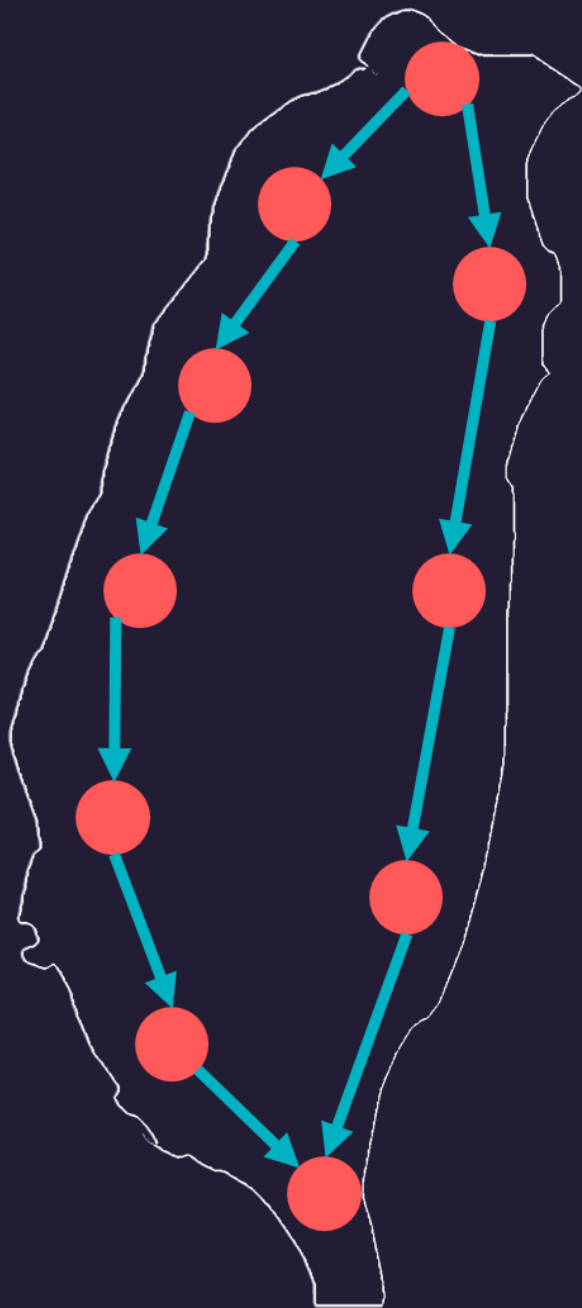
Relay Auth

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

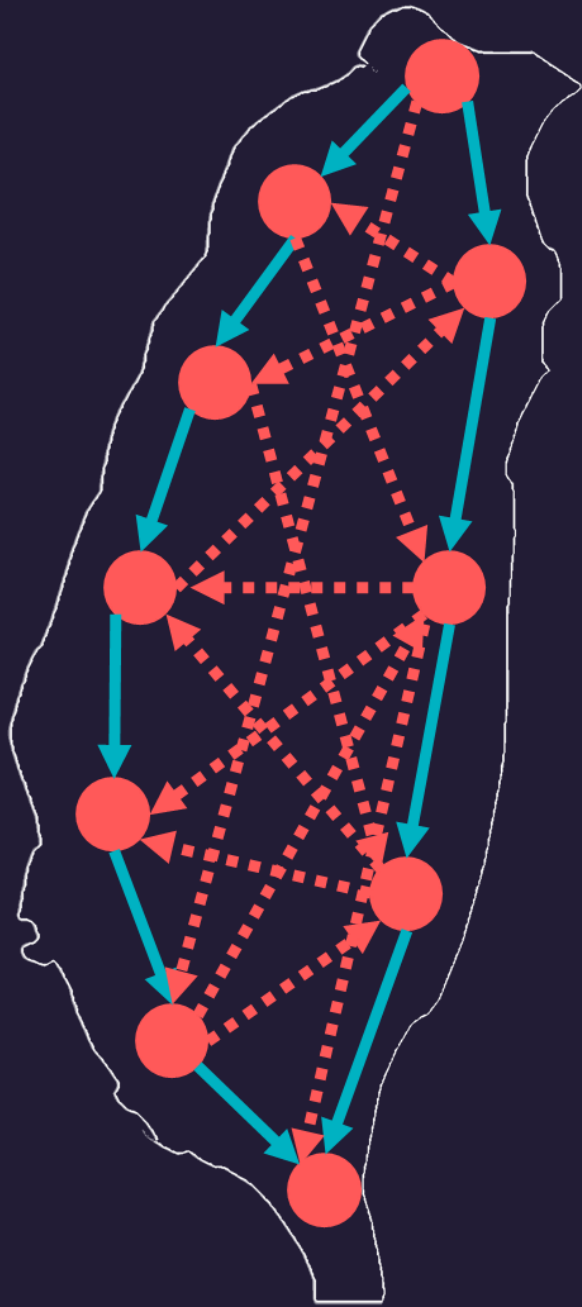
跨 Session
攻擊

單純 network
logon 的登入
也可以攻擊

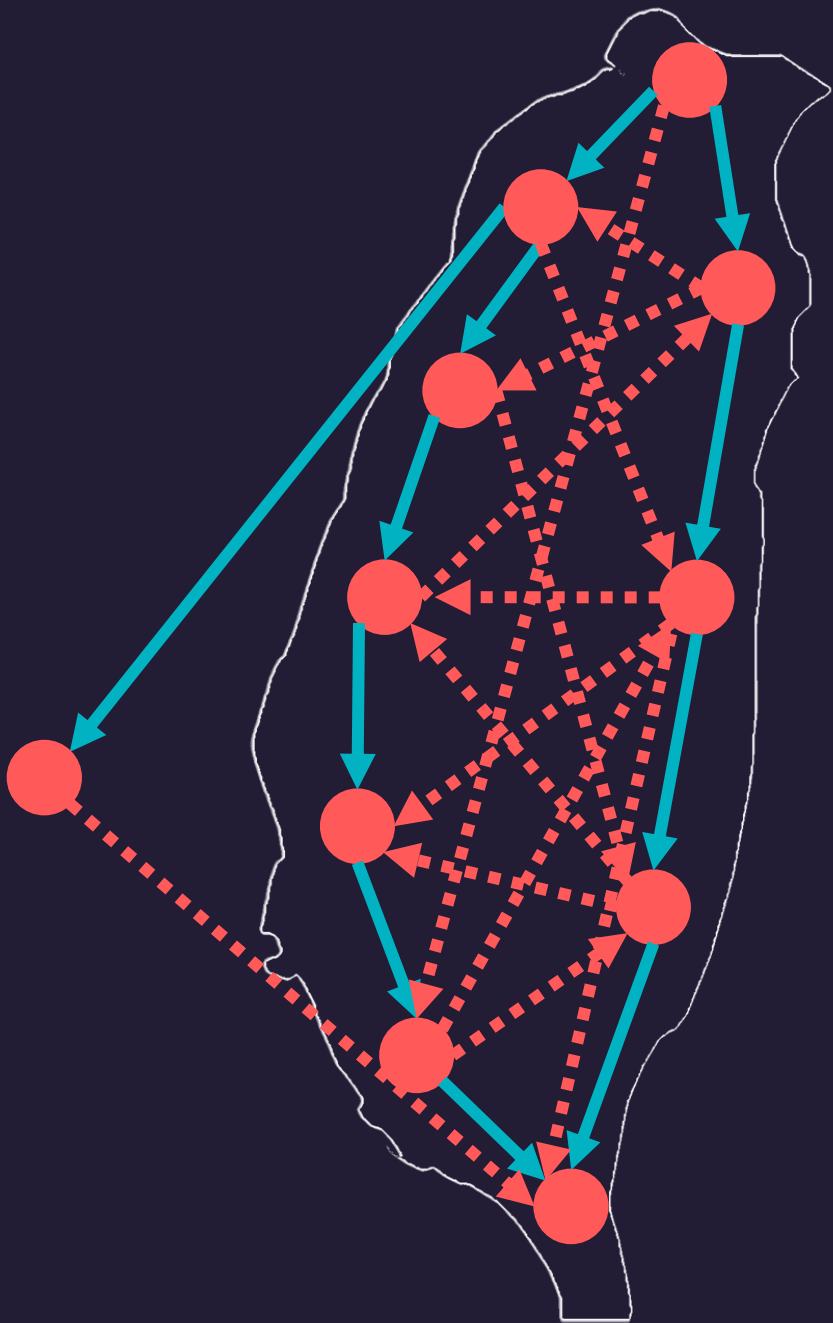




AD 權限資料
只有兩條路可以從北到南



但加上違規操作
就像是有人打通了
中央山脈的傳送門



同時也增加了
需要防禦的邊界

The background on the left side of the slide is composed of several overlapping geometric shapes. There are dark blue and black angular forms, some with a fine grid pattern, set against a solid red background. A white outline of a chevron or arrow shape points towards the right, framing the title text.

疊加的安全功能

你可能會用過無密碼登入 但他 AD 這種環境怎麼動的？

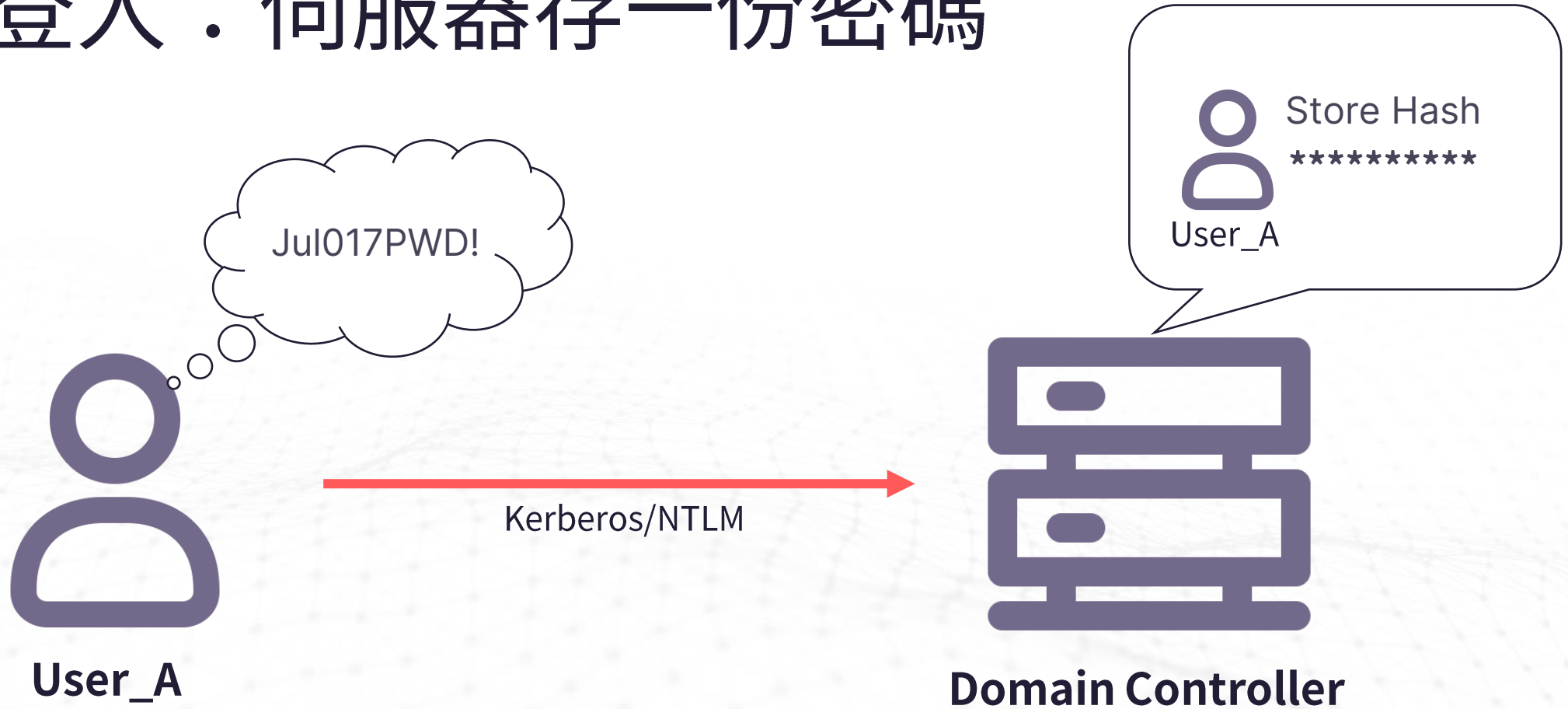
Your organization requires Windows Hello

What takes seconds to create and gives you fast and secure sign-in? A Windows Hello PIN! It only works on your device, so it stays off the web.

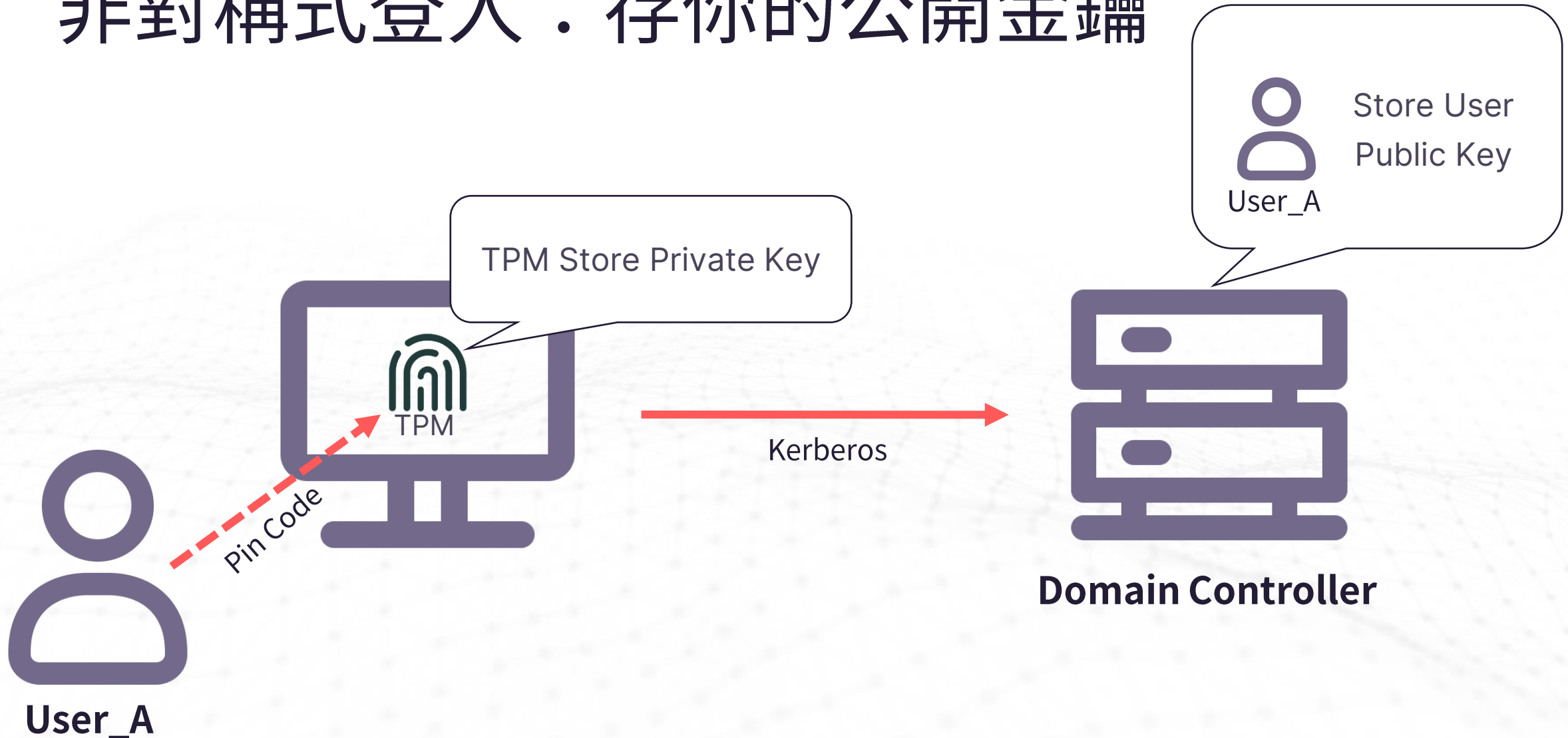


Set up PIN

密碼登入：伺服器存一份密碼

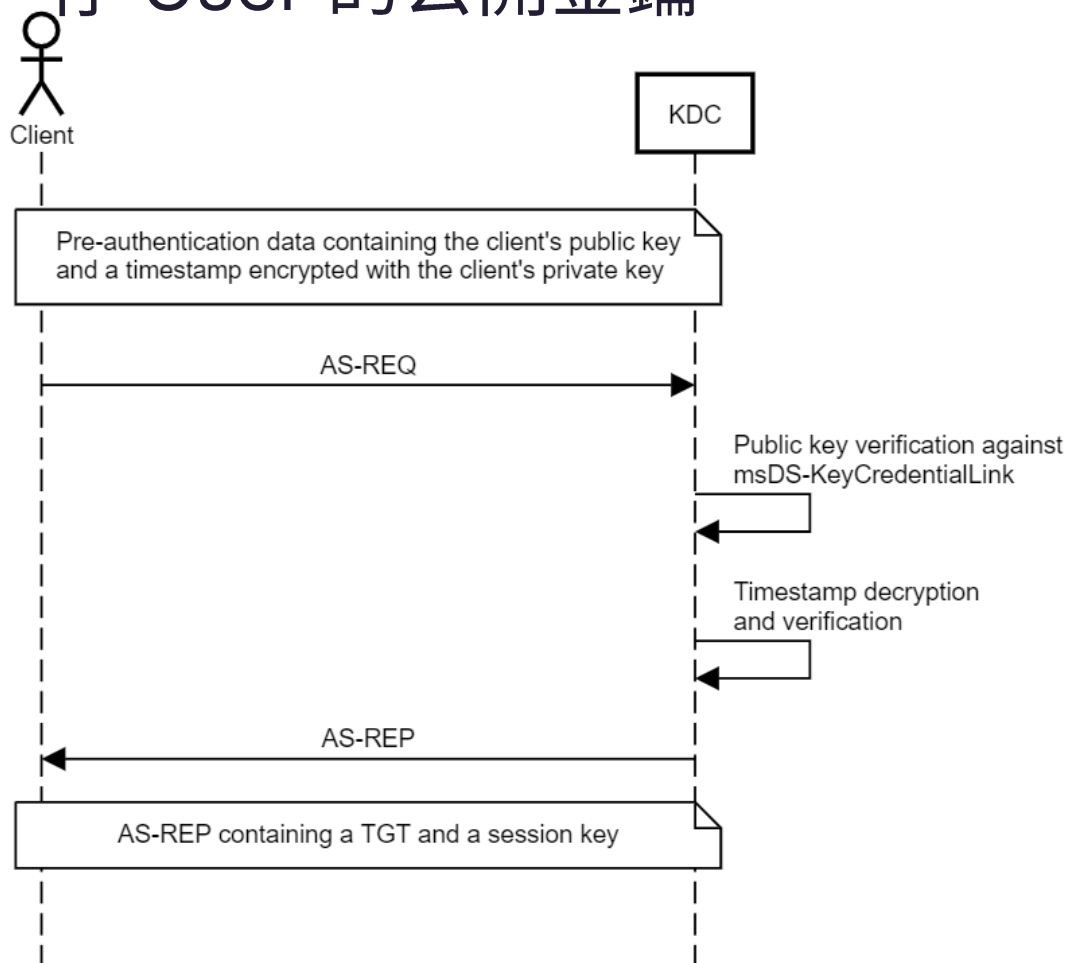


非對稱式登入：存你的公開金鑰

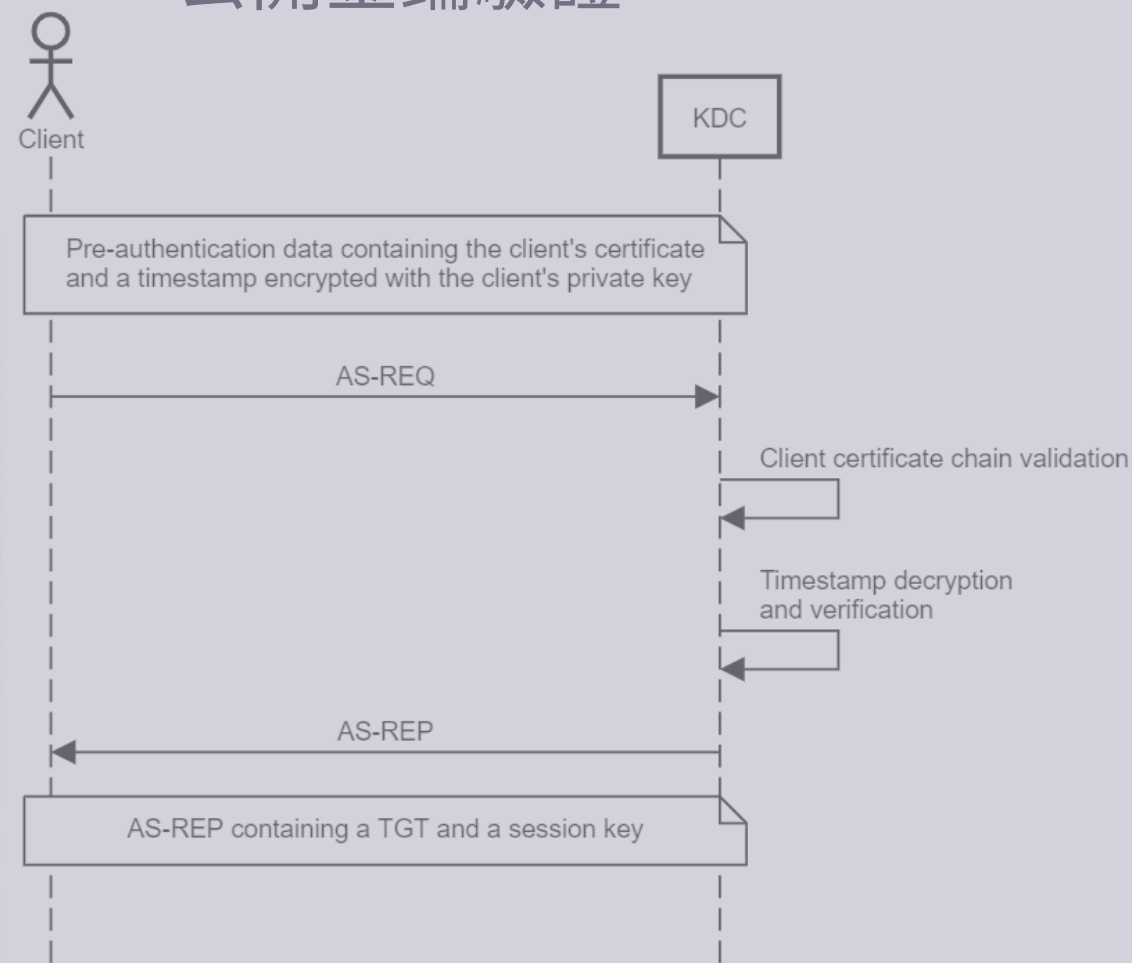


Kerberos PKINIT

msDS-KeyCredentialLink
存 User 的公開金鑰



透過 AD CS 主機
公開金鑰驗證



來源: <https://posts.specterops.io/>

攻擊介紹: Shadow Credentials

- > 利用前述的驗證方式，自己寫入 Public Key
- > 攻擊需求:
 - > Domain Functional Level Windows Server 2016 or above
 - > DC 有自己的 Key Pair (e.g. 通常是有設置 ADCS or CA)
 - > 攻擊者可以寫入 msDS-KeyCredentialLink

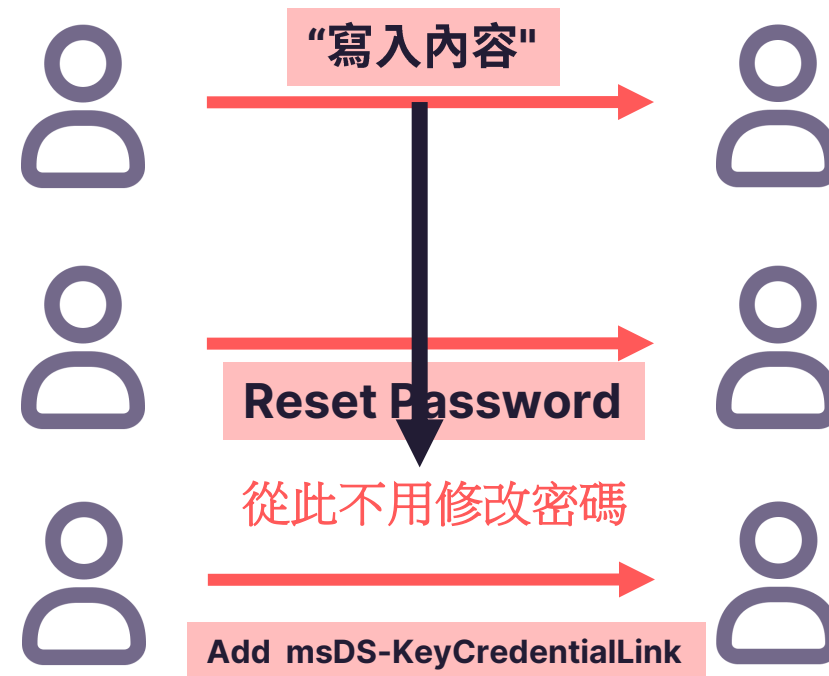
攻擊介紹: Shadow Credentials

- > 寫入 msDS-KeyCredentialLink
 - > Active Directory 中儲存 Public Key 的欄位
- > 適用於 User/Computer



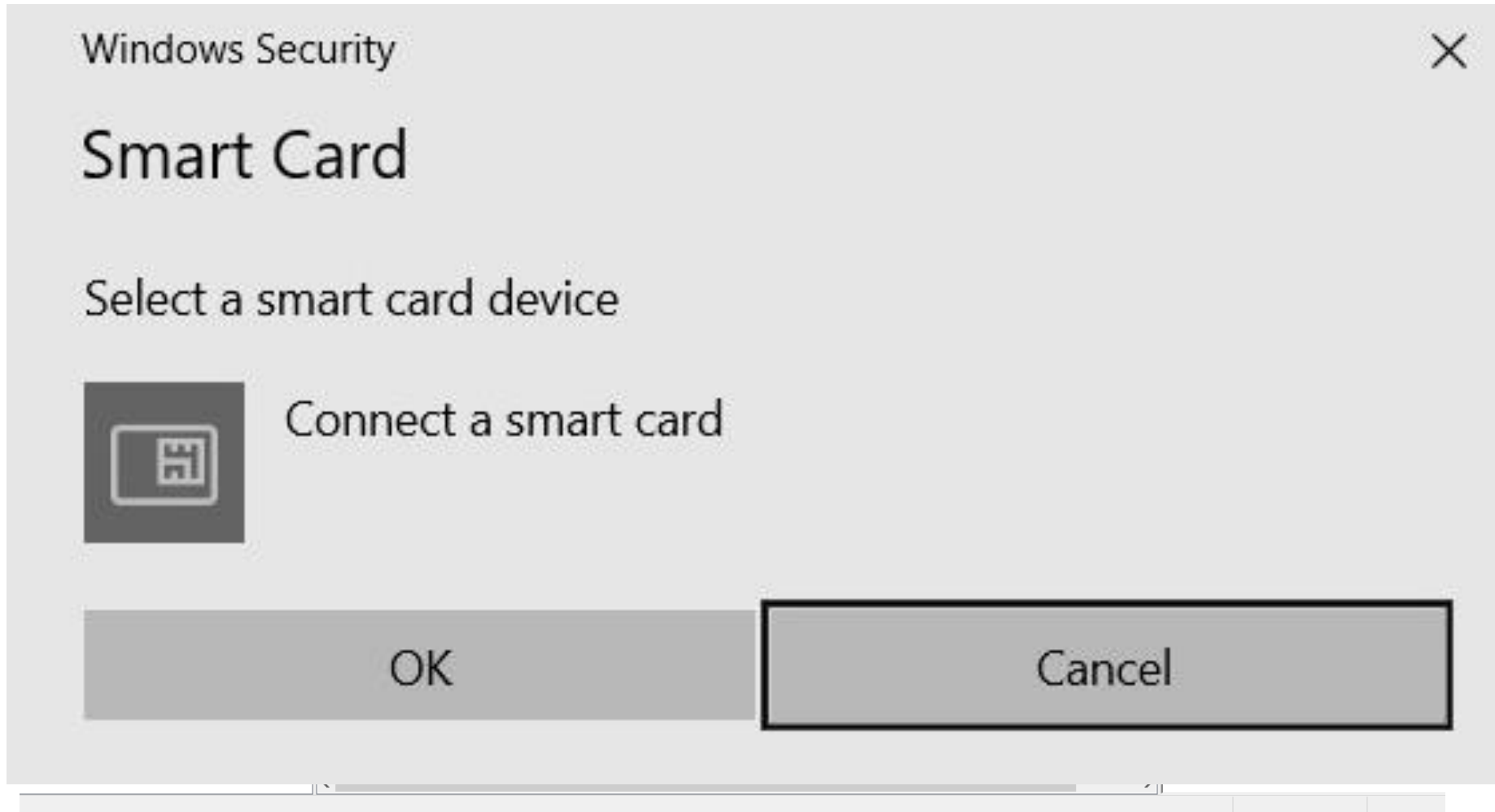
攻擊介紹: Shadow Credentials

- > 寫入 msDS-KeyCredentialLink
 - > Active Directory 中儲存 Public Key 的欄位
- > 適用於 User/Computer



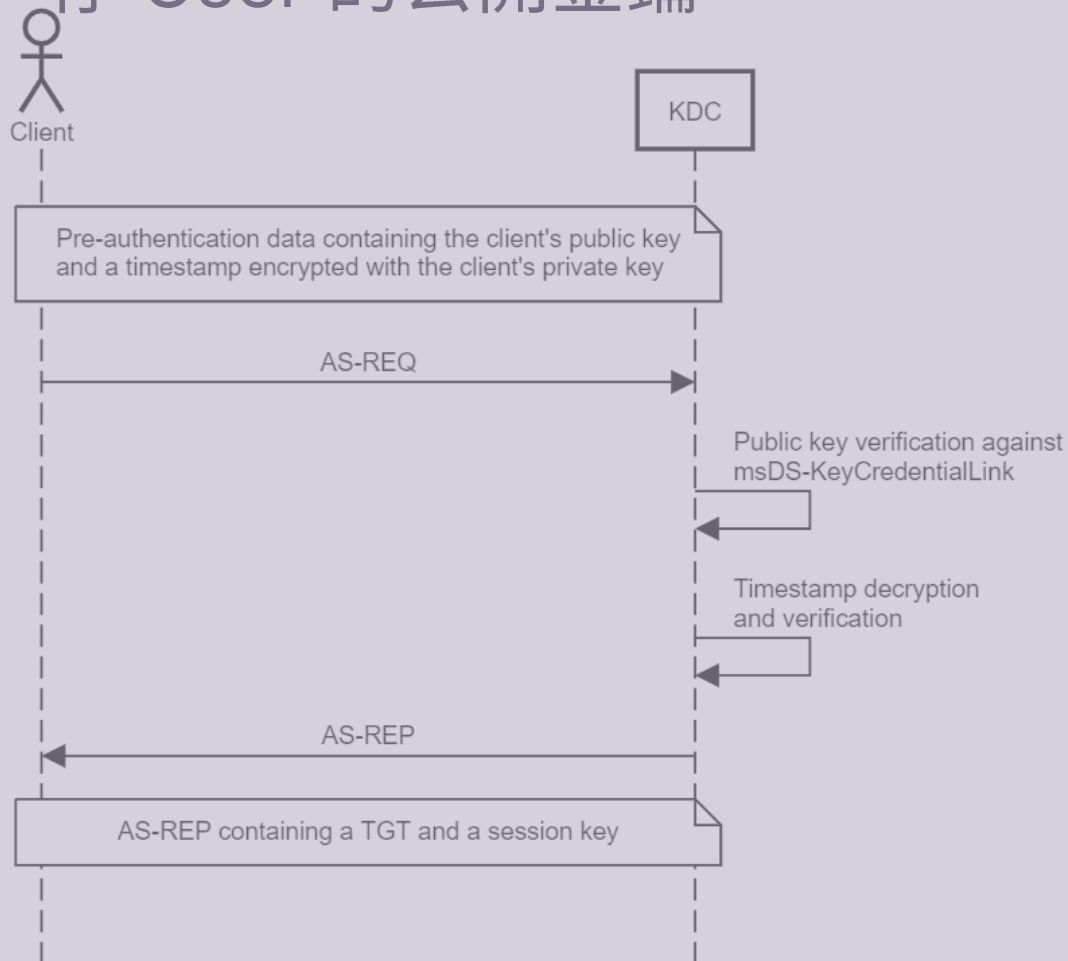
msDS-KeyCredentialLink
是 Windows Server 2016 才有的
那以前 Win7 怎麼做到呢？

另外一種憑證驗證 (ADCS)

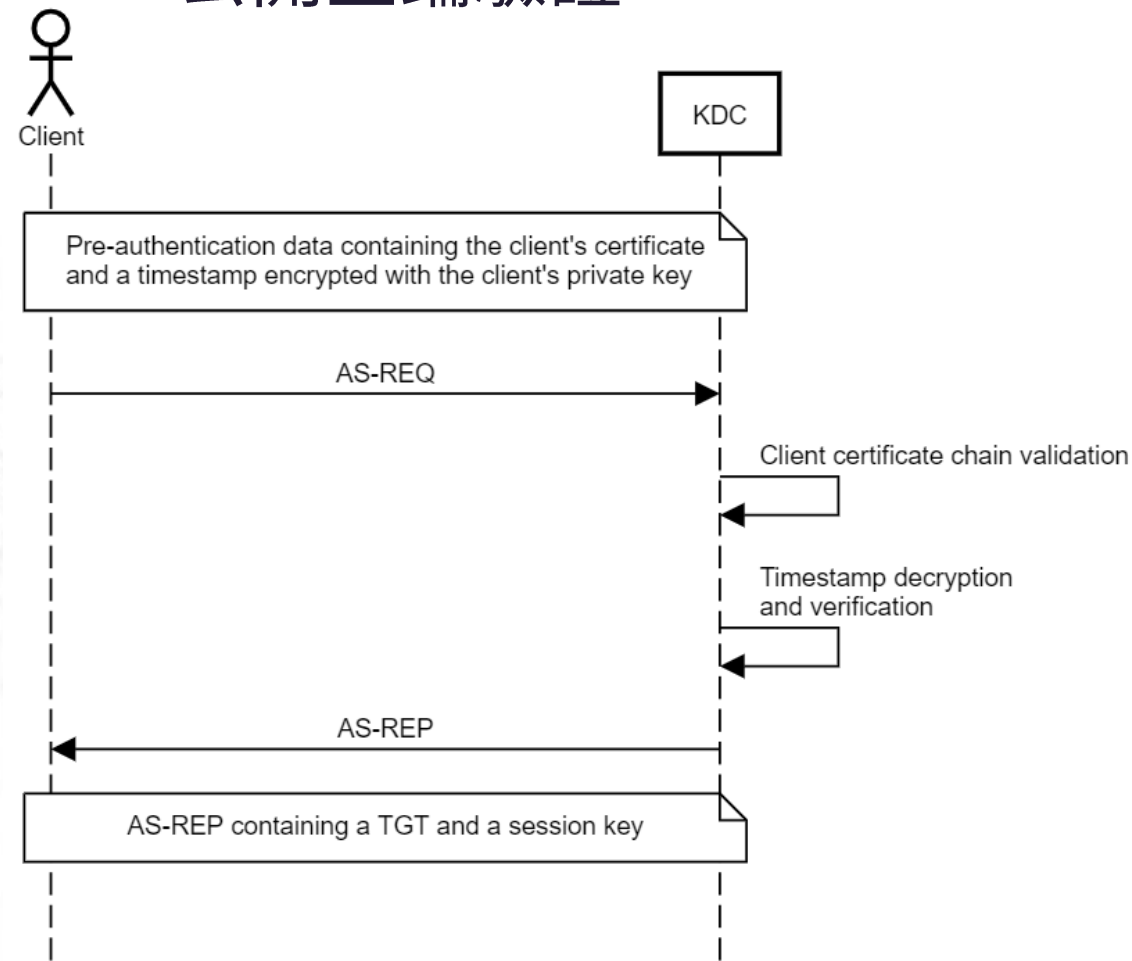


Kerberos PKINIT

msDS-KeyCredentialLink
存 User 的公開金鑰



透過 AD CS 主機
公開金鑰驗證



ADCS 介紹

- > Active Directory Certificate Services (AD CS)
- > 微軟提供的 public key infrastructure (PKI)
- > 功能分為:
 - > 憑證授權單位(CA)
 - > 憑證授權單位網頁註冊
 - > OCSP
 - > 憑證註冊原則資訊
 - > ...

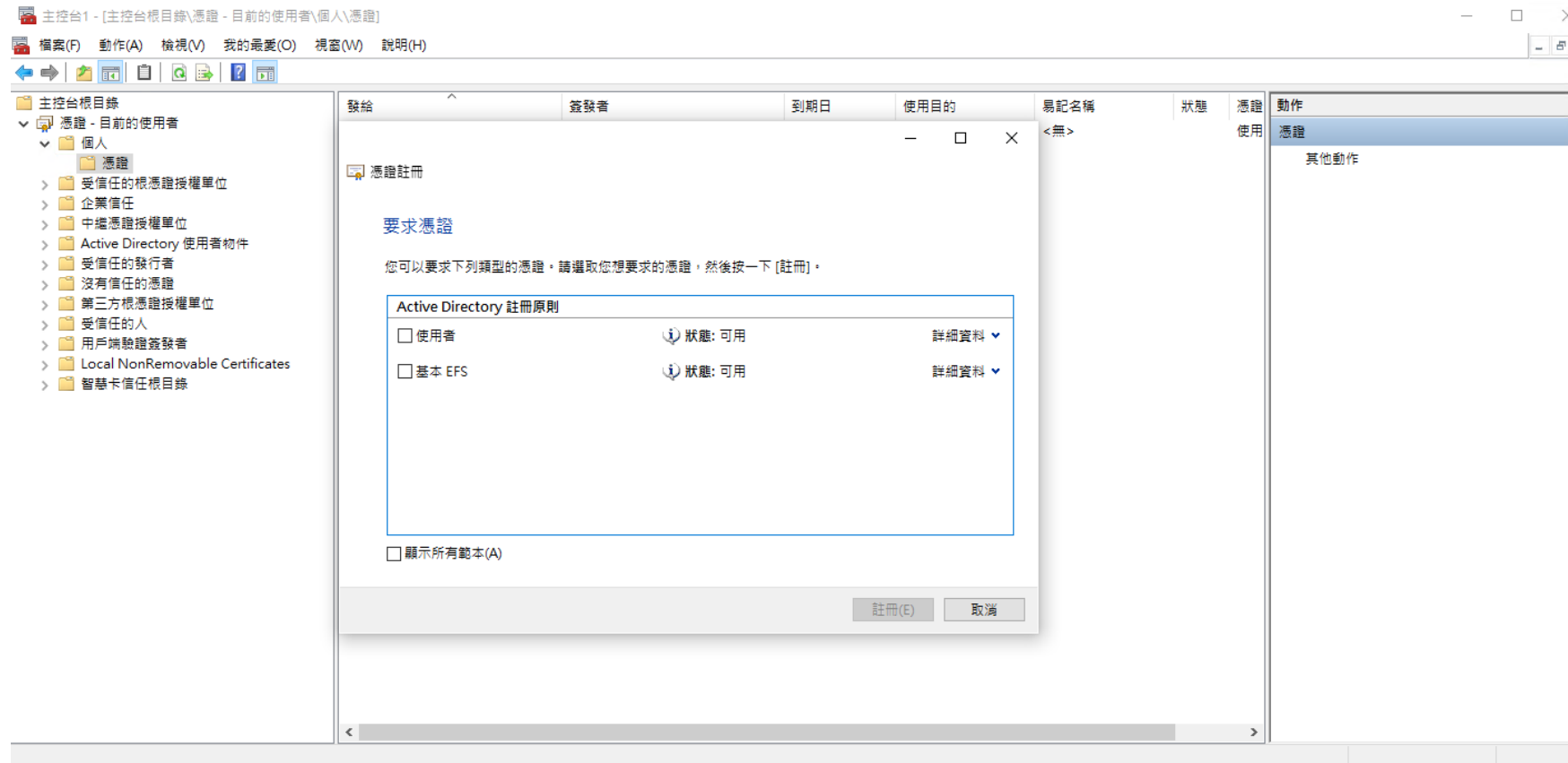
ADCS 可做以下利用

| | |
|---|---|
| User Credential Theft (1 year +) | Stealing existing user certificates capable of domain authentication or actively requesting a new certificate from a user's context. <i>Survives user password changes and can be done without elevation or touching LSASS!</i> |
| Machine Persistence (1 year +) | Stealing existing system certificates capable of domain authentication or actively requesting a new certificate from a system's context, combined with resource-based constrained delegation (or just S4U2Self). <i>Survives machine password changes and can be done without touching LSASS!</i> |
| Domain Escalation Paths | Misconfigured certificate templates that allow Subject Alternative Name (SAN) specification, vulnerable Certificate Request Agent templates, vulnerable template ACLs, the EDITF_ATTRIBUTESUBJECTALTNAME2 flag being set, vulnerable CA permissions, or NTLM relay to web enrollment endpoints. |
| Domain Persistence | Stealing the certificate authority's private key and forging "golden" certificates. |

Ref: specterops

預設所有電腦/使用者都能申請自己的憑證

> User/Computer Persistence



小節整理:

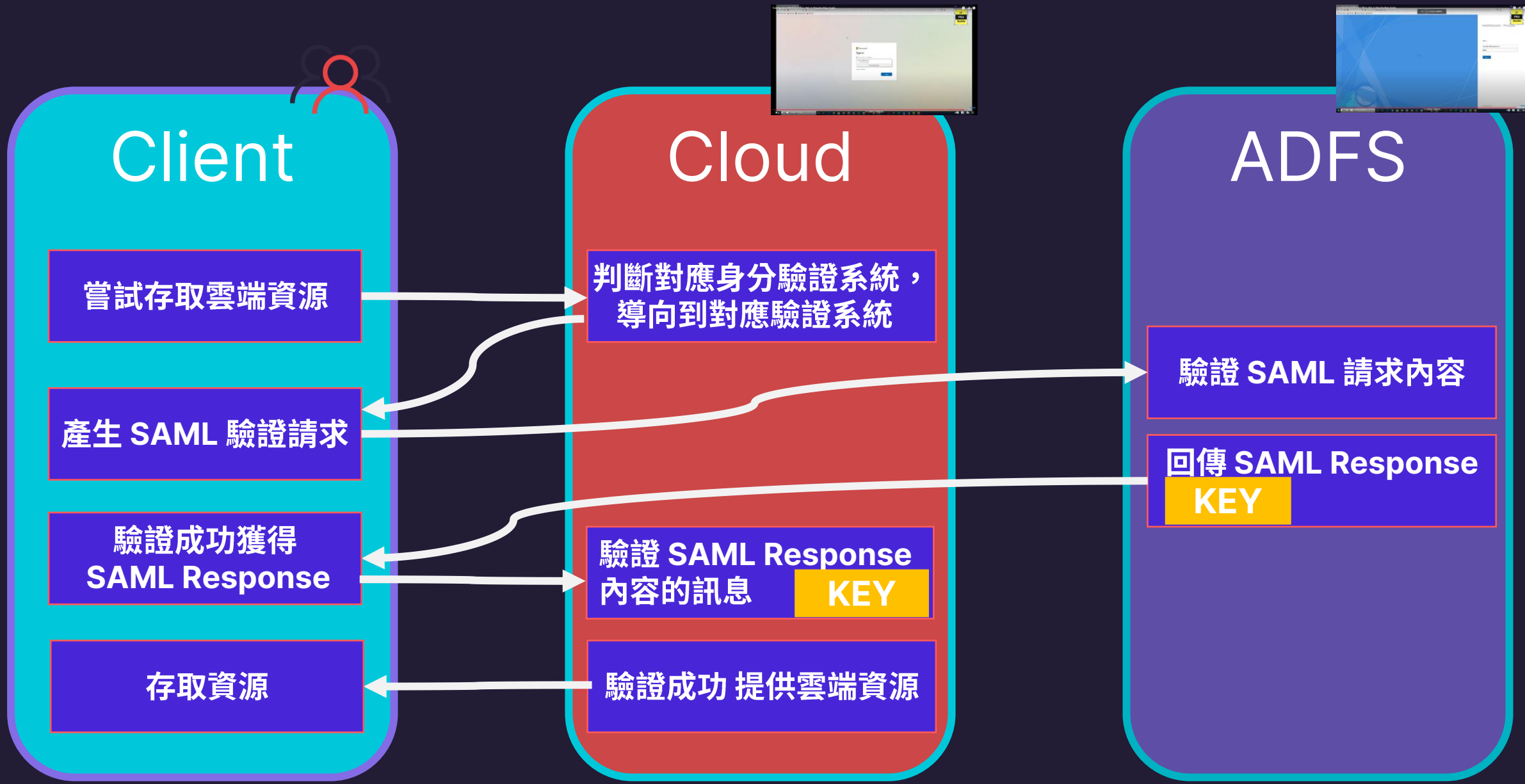
- > 權限的濫用配上 msDS-KeyCredentialLink
 - > 可以讓駭客獲取帳號控制權並潛藏在環境
 - > 還是回歸到權限盤點好、檢查是否有非預期啟用此功能的帳號
- > ADACS 伺服器與其功能是一個重要的防守邊界
 - > 盤點已經發出去的憑證
 - > 檢查憑證原則是否有權限設定問題，駭客可以透過錯誤設定做到提權

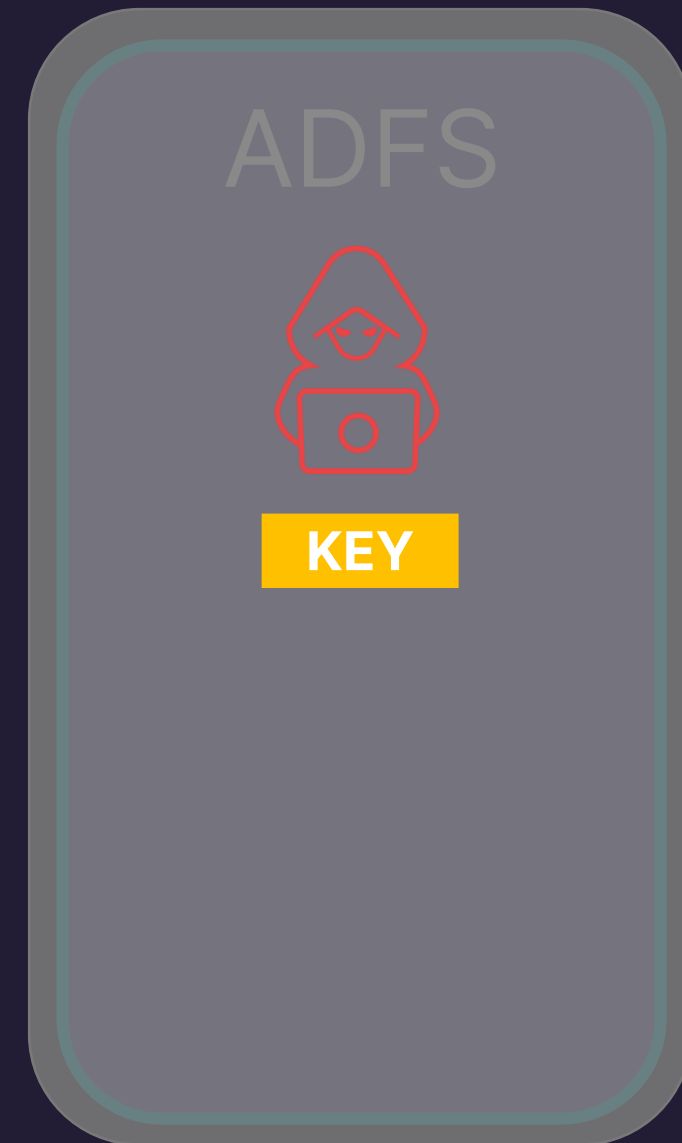
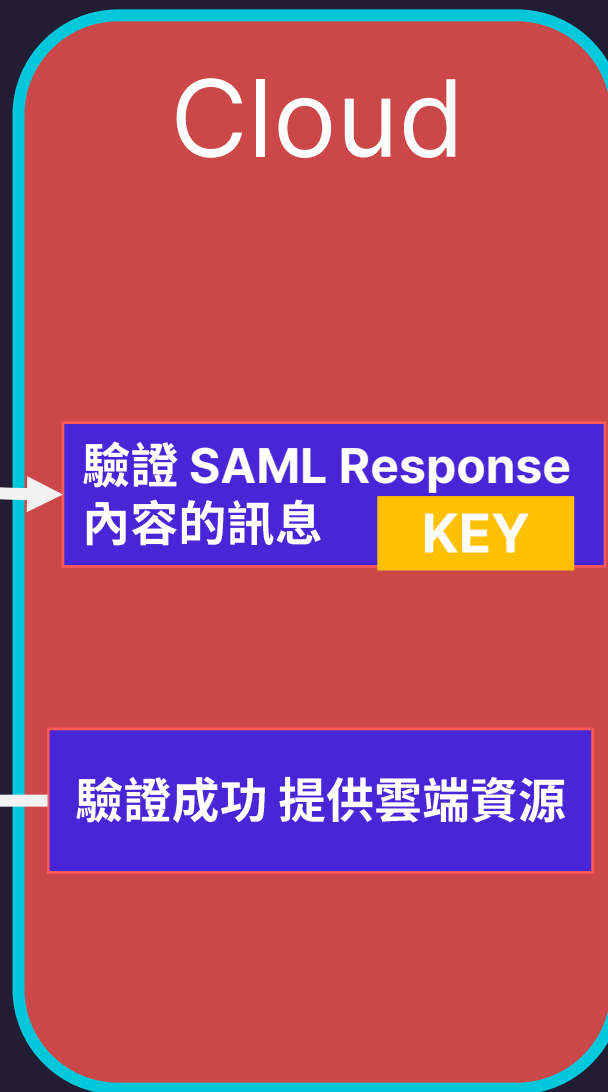
An abstract graphic on the left side of the slide. It consists of several overlapping geometric shapes: a large dark blue shape with a white outline, a smaller orange shape, and a white outline of a larger shape. The background is a solid red color.

To The Cloud !

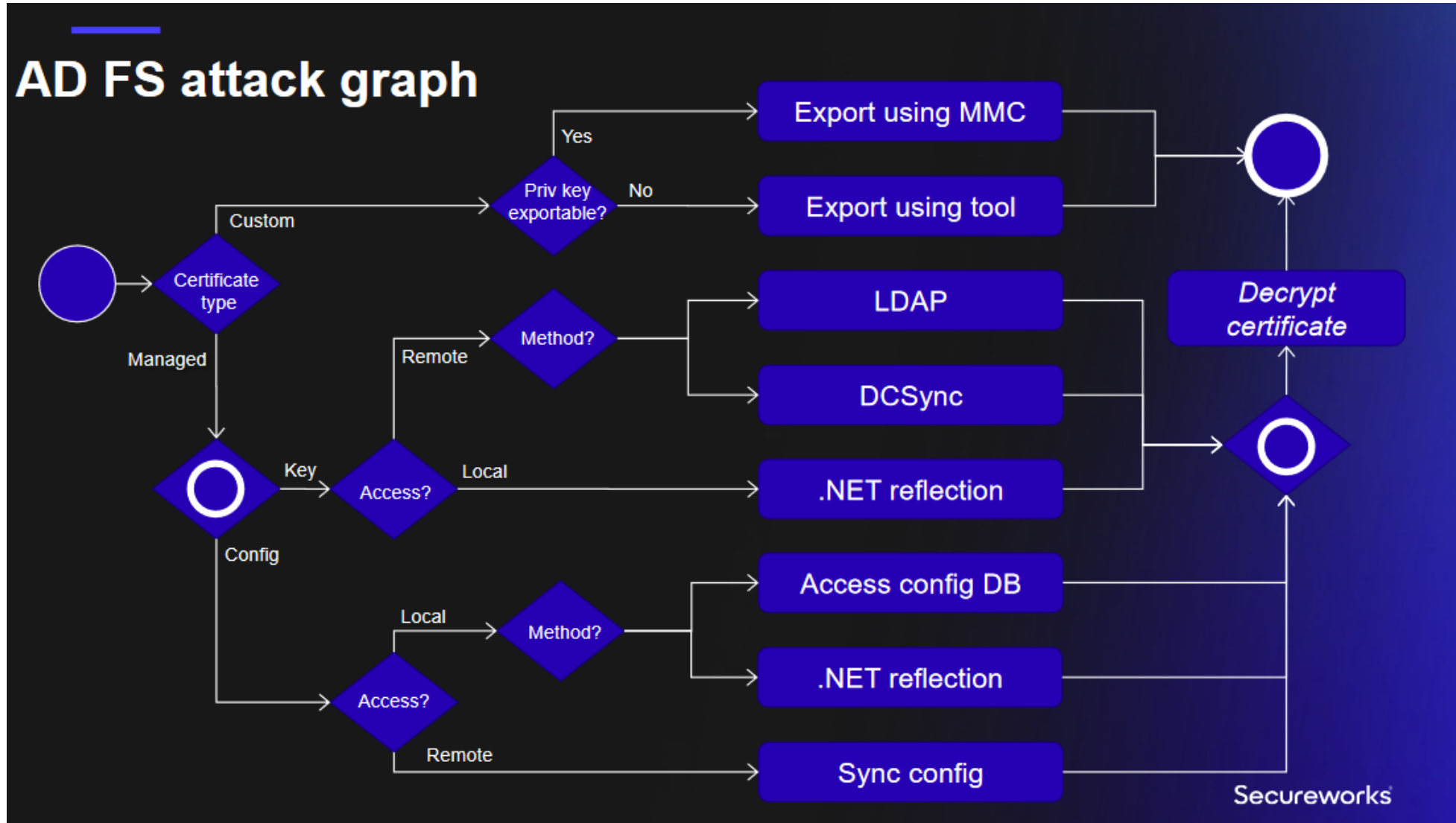
Hybrid Identity

- > Federation
 - > ADFS
- > AD with Cloud Sync
 - > Password Hash Sync (PHS)
 - > Pass-Through Authentication (PTA)
 - > Other Cloud Platform





AD FS 偷 Key 大全



<https://o365blog.com/talks/Eight%20ways%20to%20compromise%20AD%20FS%20certificates.pdf>

Hybrid Identity

- > Federation

- > ADFS

- > Azure AD Connect

- > Password Hash Sync (PHS)

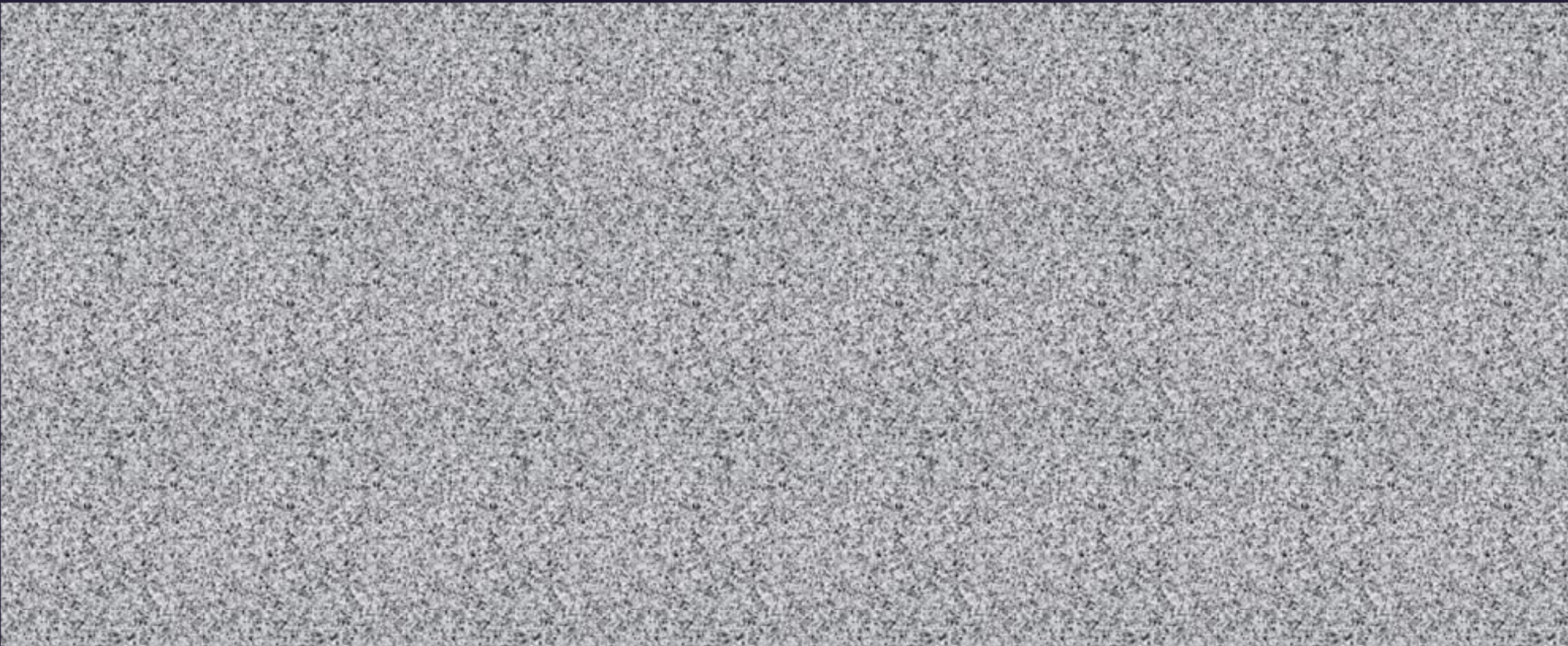
- > Pass-Through Authentication (PTA)

Azure AD Connect

AAD 與地端的攻擊管道之一

- > Azure AD Connect
- > Server 上安裝 Azure AD Connect 應用程式
- > 安裝會在系統設定 MSOL_ 開頭的帳號
- > 預設安裝會用到 SQL
- > 驗證模式：
 - > PTA
 - > PHS

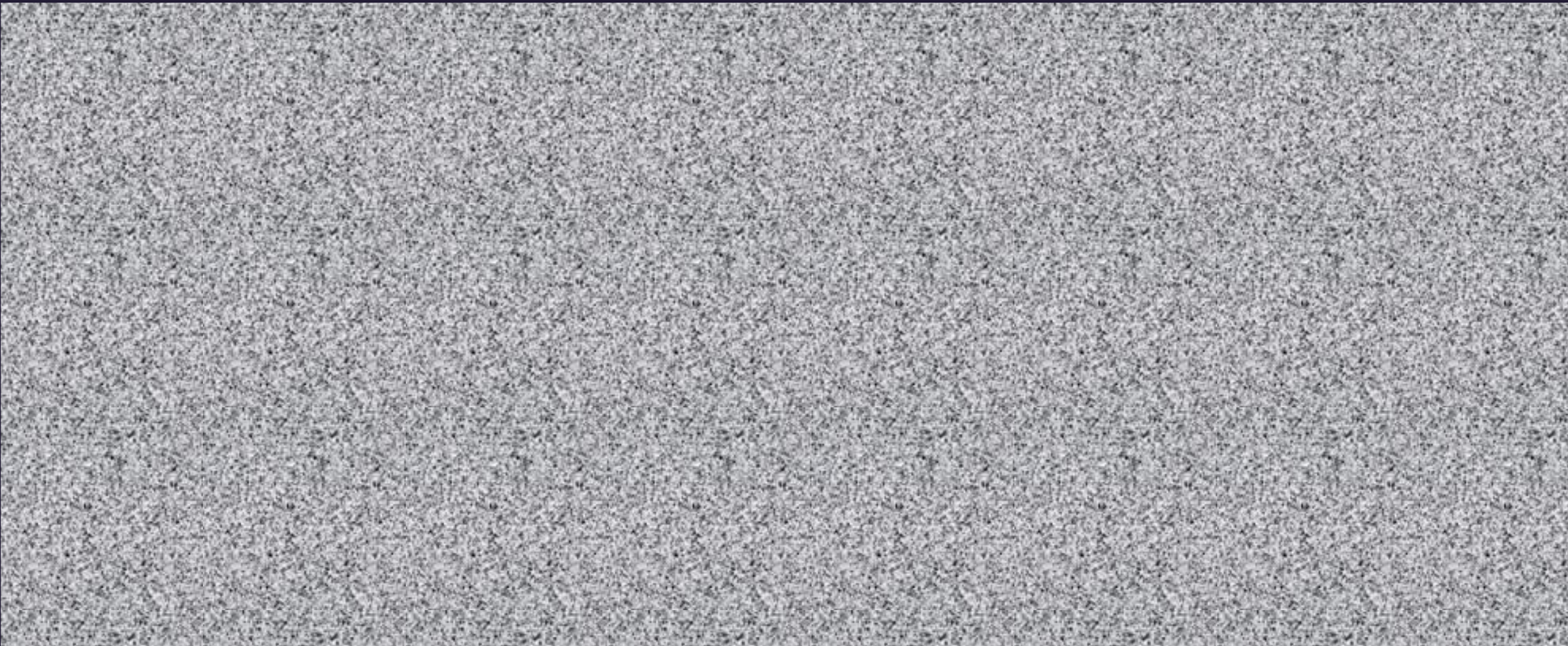
Azure AD Connect - PTA



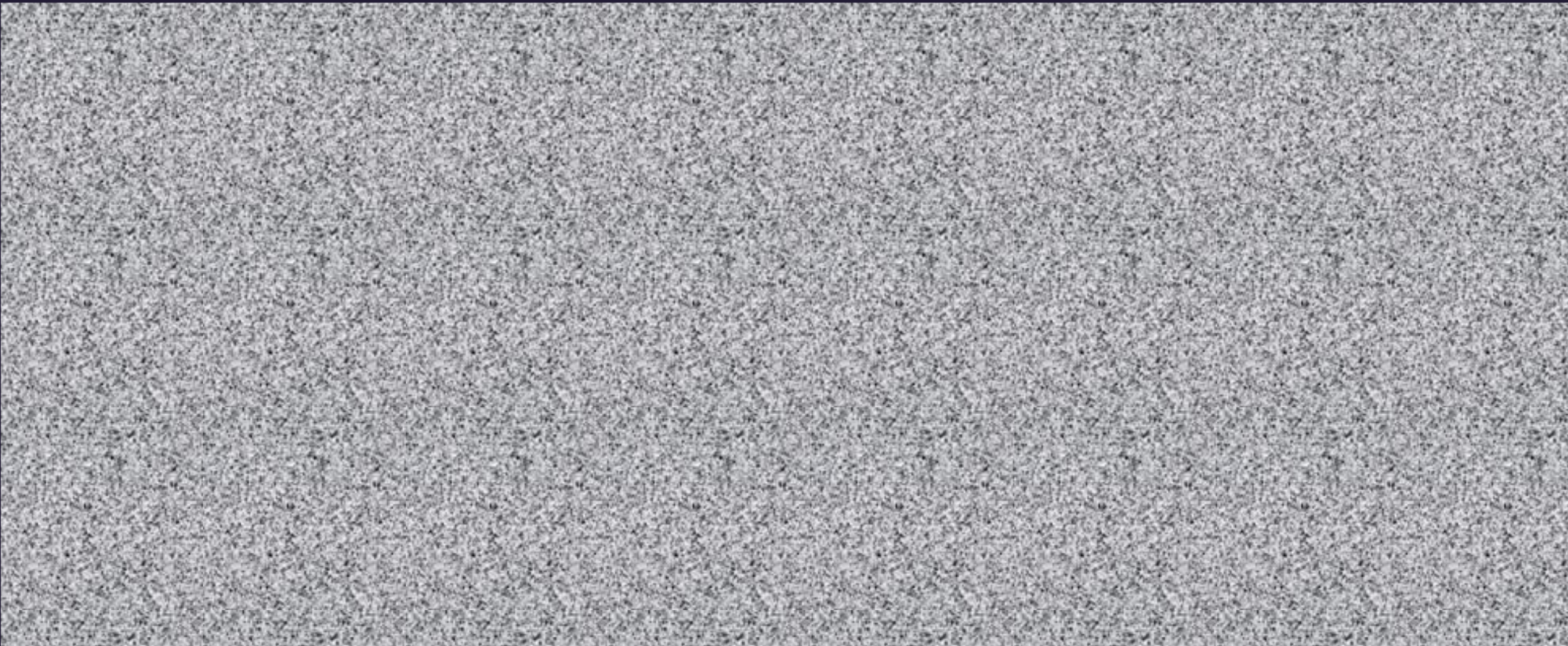
PTA 攻擊方式

- > 當設定 PTA 模式時，地端 AD 會出現 **MSOL_** 開頭帳號，用做帳號資訊同步，但權限不大
- > 在 Azure AD Connect 所在的主機安裝後門 Agent
 - > E.g. AADInternals 的 AADIntPTASpy
- > 透過攻擊用的 Agent 攔截驗證封包
 - > 強制驗證通過，無須輸入正確密碼
 - > 獲得其他正常登入使用者的密碼

Azure AD Connect - PHS

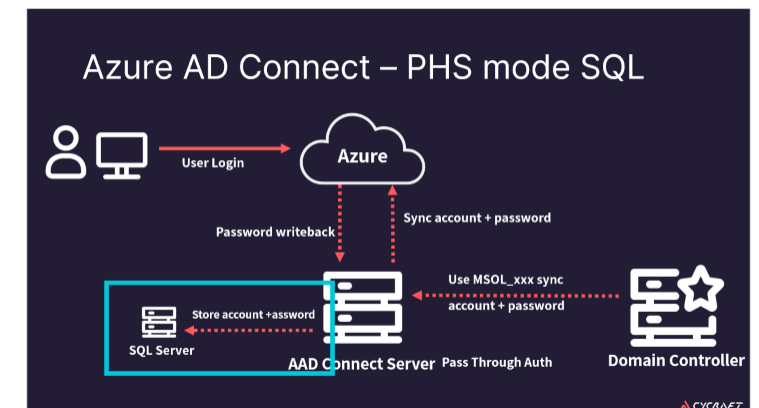


Azure AD Connect – PHS + writeback



PHS 攻擊方式

- > 當設定 PHS 模式時，會設定兩個帳號
 - > 地端 AD 會出現 **MSOL_** 開頭帳號，用做 DCSync 同步密碼
 - > 雲端 AAD 會建立雲端帳號 **Sync_** 開頭的帳號，用作重設地端或是雲端帳號用
- > **密碼存於 SQL Server**，但預設 AAD Connect 用 SQL Express



Azure 以外的平台呢？

- > AWS Active Directory Connector
 - > 透過 VPC 對接使用自建服務帳號
 - > 保護服務帳號、定期更換密碼
- > Google Cloud Directory Sync
 - > 安裝軟體於伺服器
 - > 保護安裝軟體的伺服器、服務帳號



議程總結



EVERYTHING
STARTS FROM
SECURITY



接下來，行動！

- > 短期：保護雲端平台與地端帳密界接處
 - > 各家雲端平台類似概念的界接處都應注意，不只是 Azure
 - > 增加控制項目且添加核心資產控制措施
- > 短期：檢查場域中是否有憑證登入這類型的功能
 - > 檢查其安全設定還有目前發出去的憑證
- > 中長期：對累積的權限問題、違規登入進行盤點
 - > 掌握帳號登入狀況、定期盤點確認場域是否有變更