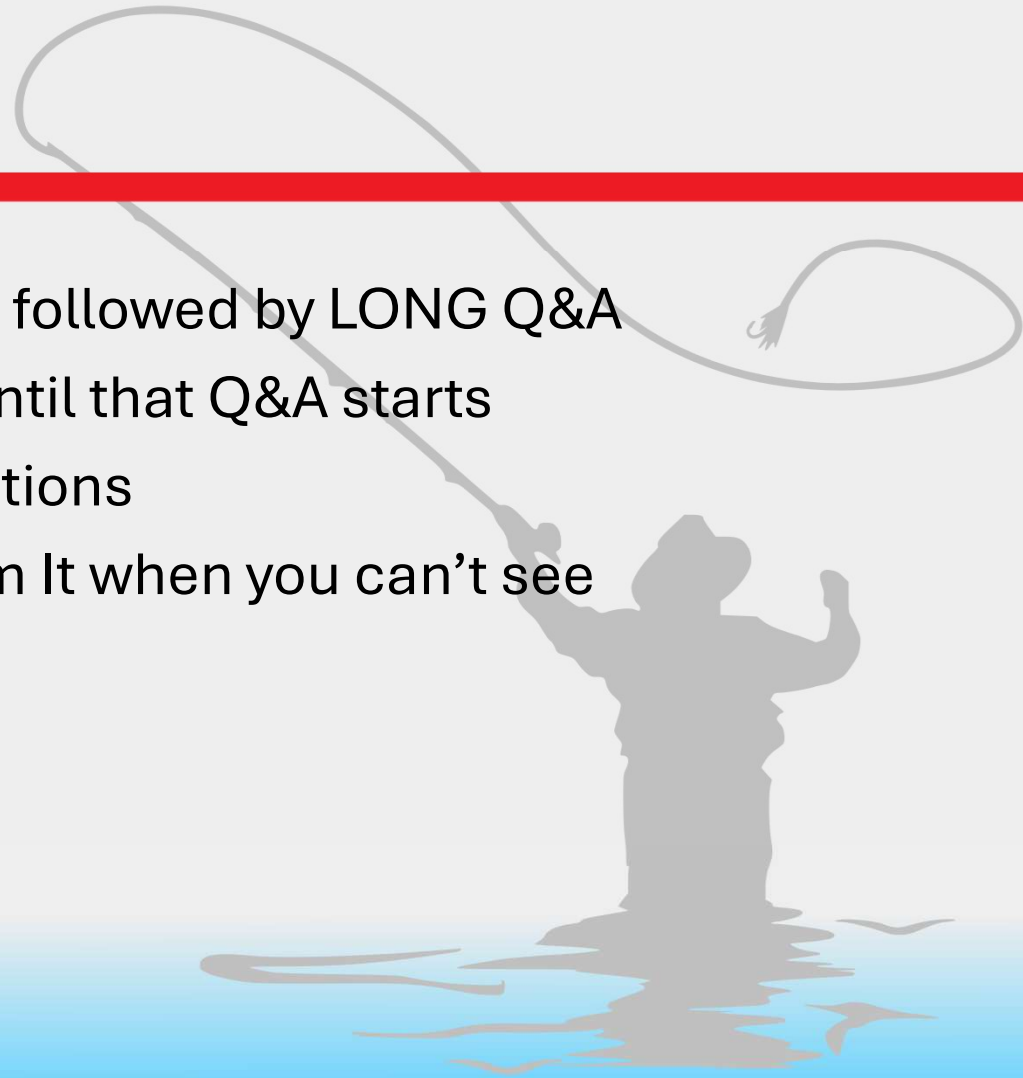


The Admin's Guide to Preventing SCCM Attacks



Attention

- MMS sessions are 60-75 minutes followed by LONG Q&A
- Please hold detailed questions until that Q&A starts
- Feel free to ask clarification questions
- Remind the speakers to use Zoom It when you can't see



Speakers



Tom Degreeef

Defending your castle since '19

Extraordinary Consultant, AppControl

 @tomdegreeef

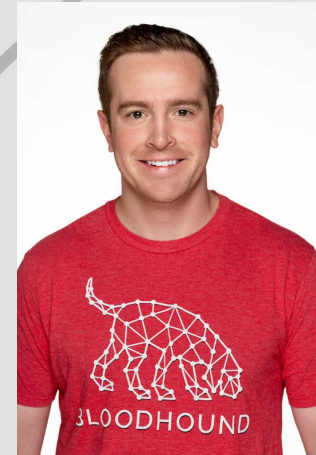


Kim Oppalfens

You know him, you love him

CIO @ AppControl.ai

 @thewmiguy



Chris Thompson

Attacking your castle since '21

Sr. Security Researcher @ SpecterOps

 @_Mayhem



Can't see our slides? Can't hear? Need to repeat the question? Call us out!



What this talk is not about:

- SCCM fundamentals
- Attack path detection



What this talk is about:

- Attack surface
- Attack execution **demons**
- **Attack path prevention**
- Step-by-step reference guide
- Potential pitfalls (and **bypasses**)

Agenda

- SCCM attack surface
 - Hierarchy TAKEOVER
 - ELEVATE privileges
 - Gathering CREDs
- Attack demos
- Remediation guidance and walkthroughs
- Automating issue identification

Misconfiguration Manager



SCCM Attack Path Management Knowledge Base

- Co-authored with Duane Michael (@subat0mik) and Garrett Foster (@unsigned_sh0rt)
- Step-by-step foundational, **offensive**, and **defensive write-ups** for known techniques
- A **taxonomy** to simplify and demystify concepts
- Based on MITRE ATT&CK
- **Scripts** and **tools** to identify misconfigurations



<https://misconfigurationmanager.com>



Shoutouts / Prior Work

- Garrett Foster (@unsigned_sh0rt)
- Duane Michael (@subat0mik)
- Andy Robbins (@_wald0)
- Jonas Bülow Knudsen (@Jonas_B_K)
- Elad Shamir (@eladshamir)
- Zach Stein (@synzack21)
- Erik Hunstad (@badsectorlabs)
- Dylan Bradley (@slygoo)
- Nick Powers (@zynergy)
- Matt Creel (@Tw1sm)
- Lee Chagolla-Christensen (@tifkin_)
- Will Schroeder (@harmj0y)
- Adam Chester (@_xpn_)
- Christopher Panayi (@Raiona_ZA)
- Carsten Sandker (@0xcsandker)
- Josh Prager (@Praga_Prag)
- Mehdi Elyassa



Misconfiguration Manager Taxonomy

Because "Hierarchy takeover via NTLM coercion and relay to MSSQL on remote site database" doesn't roll off the tongue...

Attack Techniques



RECON



CRED



ELEVATE

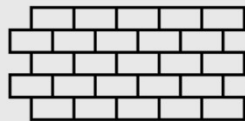


TAKEOVER



EXEC

Defense Techniques



PREVENT



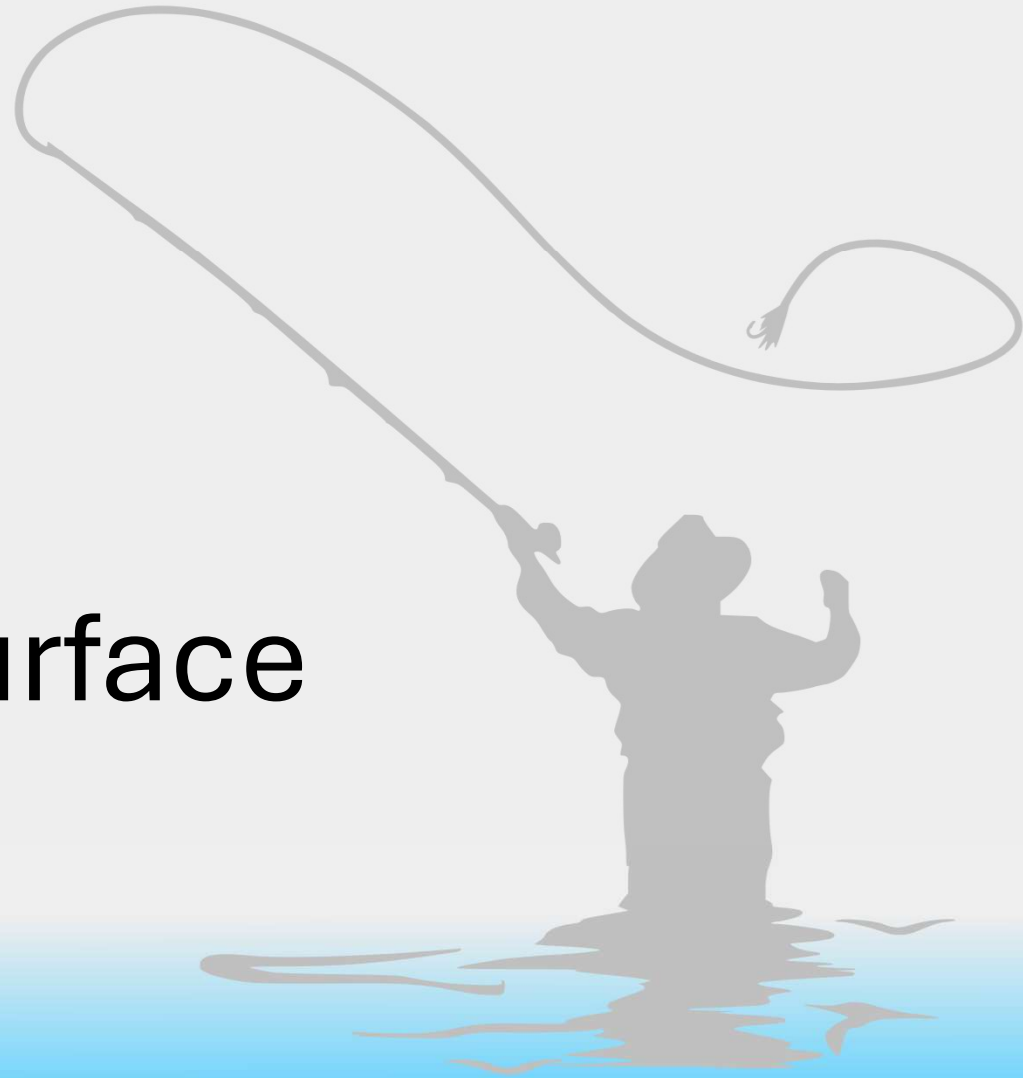
DETECT



CANARY



SCCM Attack Surface



SCCM Hierarchy

- One installation of SCCM
- Contains one or more primary sites
- This is the **security boundary**

SITE DATABASE



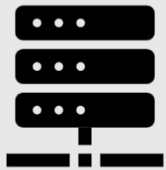
PRIMARY SITE



SITE SERVER



SMS PROVIDER



MANAGEMENT
POINT



CLIENTS



DISTRIBUTION
POINT



Hierarchy TAKEOVER



Hierarchy TAKEOVER

Gaining complete control of all client devices in the SCCM hierarchy

- How can attackers take over a hierarchy?
 - Obtain the **Full Administrator** role in **ANY** primary site

Hierarchy TAKEOVER

Gaining complete control of all client devices in the SCCM hierarchy

- How can attackers take over a hierarchy?
 - Obtain the **Full Administrator** role in **ANY** primary site
- Security roles in the site database are replicated to **ALL** sites
 - **Own one primary site, own them all**

Hierarchy TAKEOVER

Gaining complete control of all client devices in the SCCM hierarchy

- How can attackers take over a hierarchy?
 - Obtain the **Full Administrator** role in **ANY** primary site
- Security roles in the site database are replicated to **ALL** sites
 - **Own one primary site, own them all**
- Why do we care?
 - Insanely high success rate on red team operations and pentests
 - Allows **command execution, CMPivot, Run Script** on clients
 - Allows the ability to impact the availability of software



Real World Example

CMPivot (Connected to 123 - Primary Site - All Desktop and Server Clients)

Entities

Search

- DriverVxD
- EmbeddedDeviceInformati
- Environment
- EPStatus
- EventLog()
- File()
 - Device
 - FileName
 - Mode
 - LastWriteTime
 - Size
 - Version
 - SHA256Hash
 - MD5Hash
- FileContent()
- FileShare
- Firmware
- IDEController
- InstalledExecutable
- InstalledSoftware
- IPConfig
- IRQTable
- Keyboard

Home Query

Run Query

Create Collection Export

File('C:\Users*\aws*')

Device	FileName	Mode	LastWriteTime	Size	Version	SHA256Hash
SCCM-SITESRV	C:\Users\domainadmin\aws\config	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-SITESRV	C:\Users\domainadmin\aws\credentials	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-DISTRO	C:\Users\domainadmin\aws\config	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-DISTRO	C:\Users\domainadmin\aws\credentials	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-SQL	C:\Users\domainadmin\aws\config	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-SQL	C:\Users\domainadmin\aws\credentials	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-MGMT	C:\Users\domainadmin\aws\config	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00
SCCM-MGMT	C:\Users\domainadmin\aws\credentials	-a----	3/31/2025 12:05 PM	4		9F86D081884C7D659A2FEAA0C55AD015A3BF4F1B2B0B822CD15D6C15B0F00

Query Results Query Summary

Query completed on 5 of 8 clients (3 clients offline and 0 failures) id(16778562) | All Desktop and Server Clients | 8 objects

Hierarchy TAKEOVER

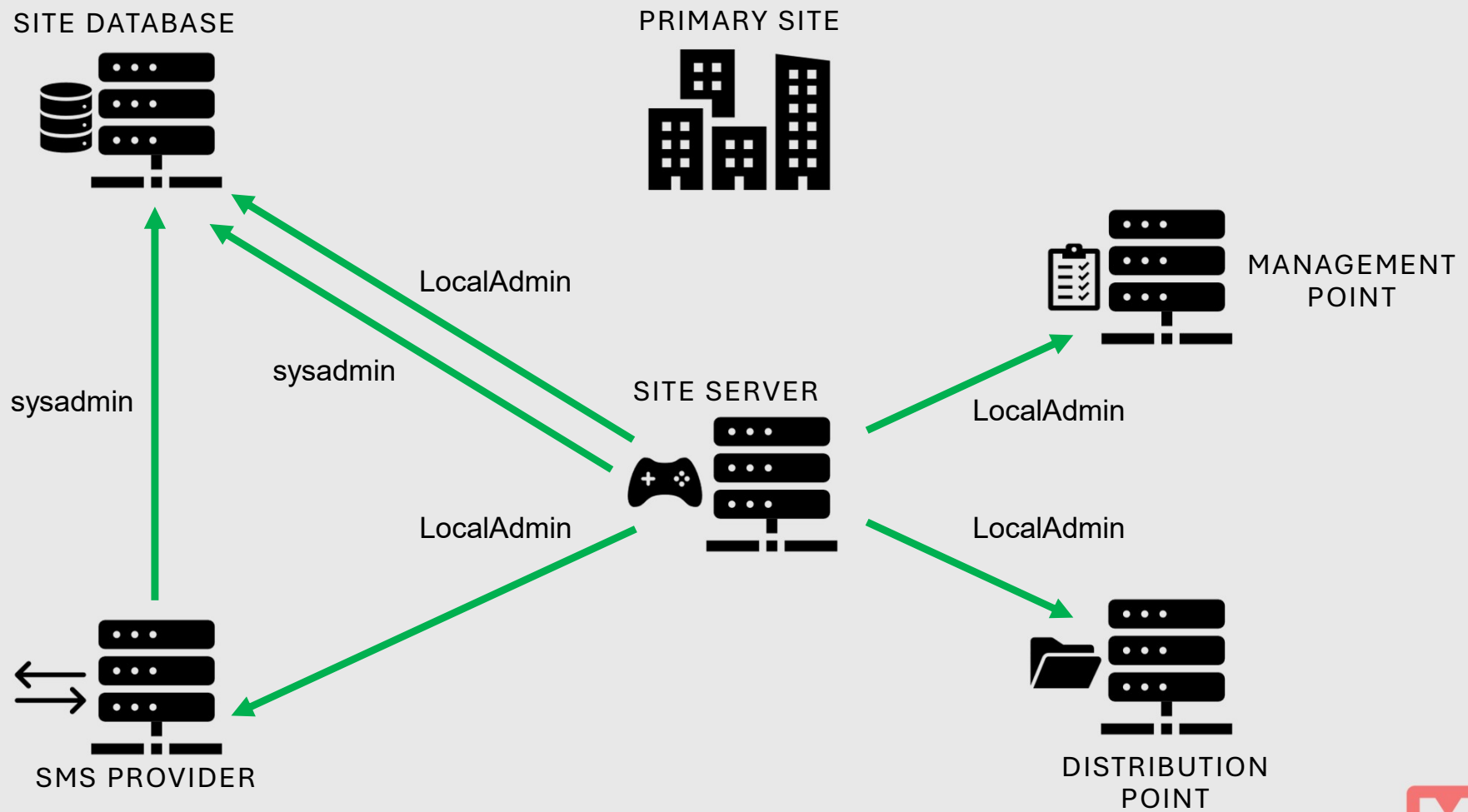
Key concepts

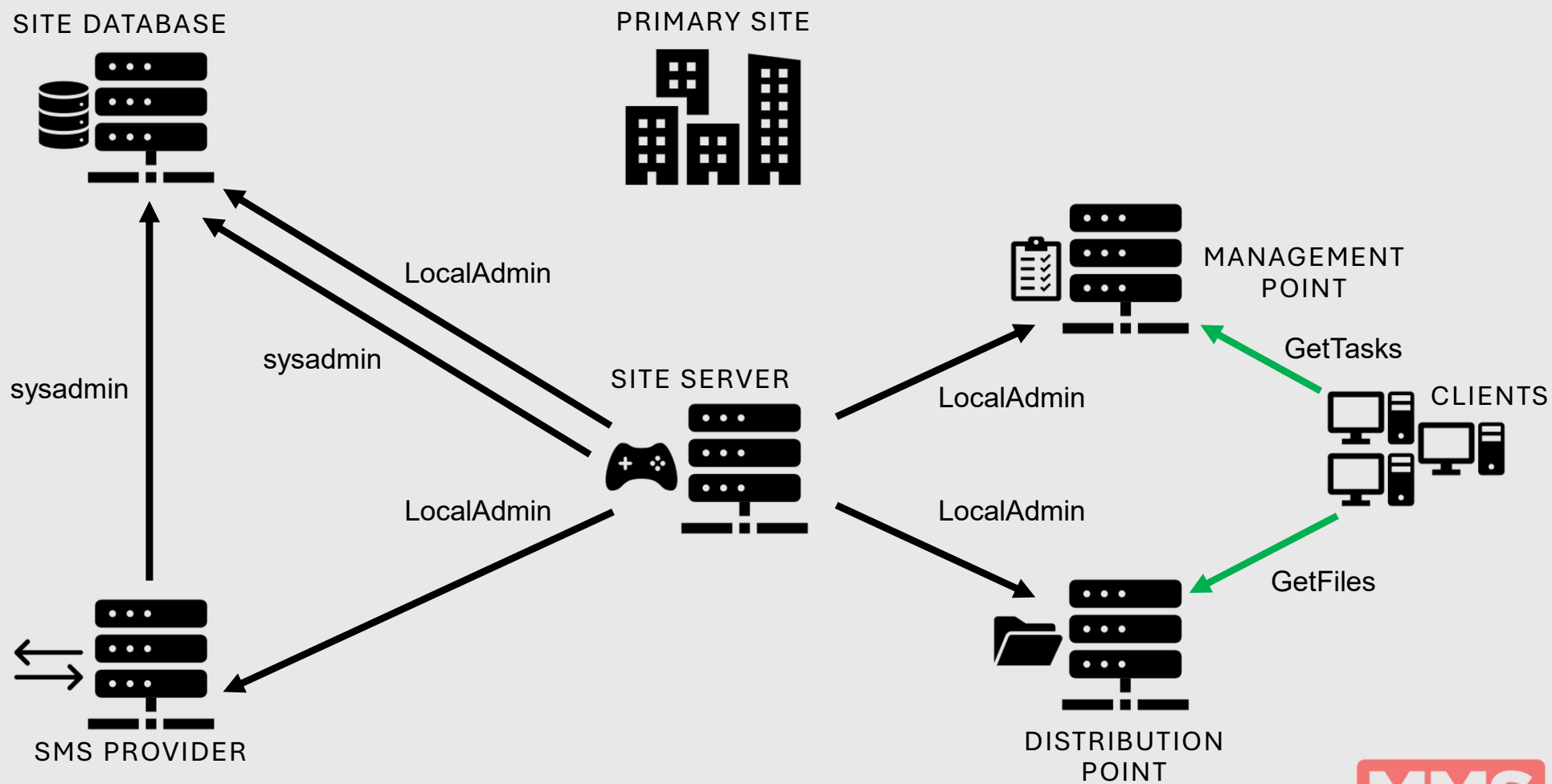
- The primary site server's domain computer account **must** be:
 - a member of local **Administrators** on every site system role
 - **sysadmin** in the site database

Hierarchy TAKEOVER

Key concepts

- The primary site server's domain computer account **must** be:
 - a member of local **Administrators** on every site system role
 - **sysadmin** in the site database
- A remote SMS Provider's domain computer account **must** be:
 - **sysadmin** in the site database





SITE DATABASE



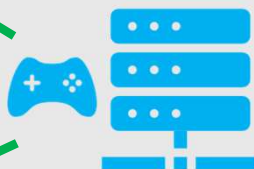
PRIMARY SITE



LocalAdmin

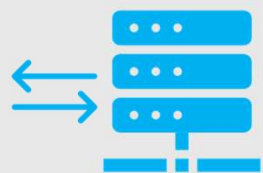
sysadmin

SITE SERVER



LocalAdmin

sysadmin



SMS PROVIDER



MANAGEMENT
POINT

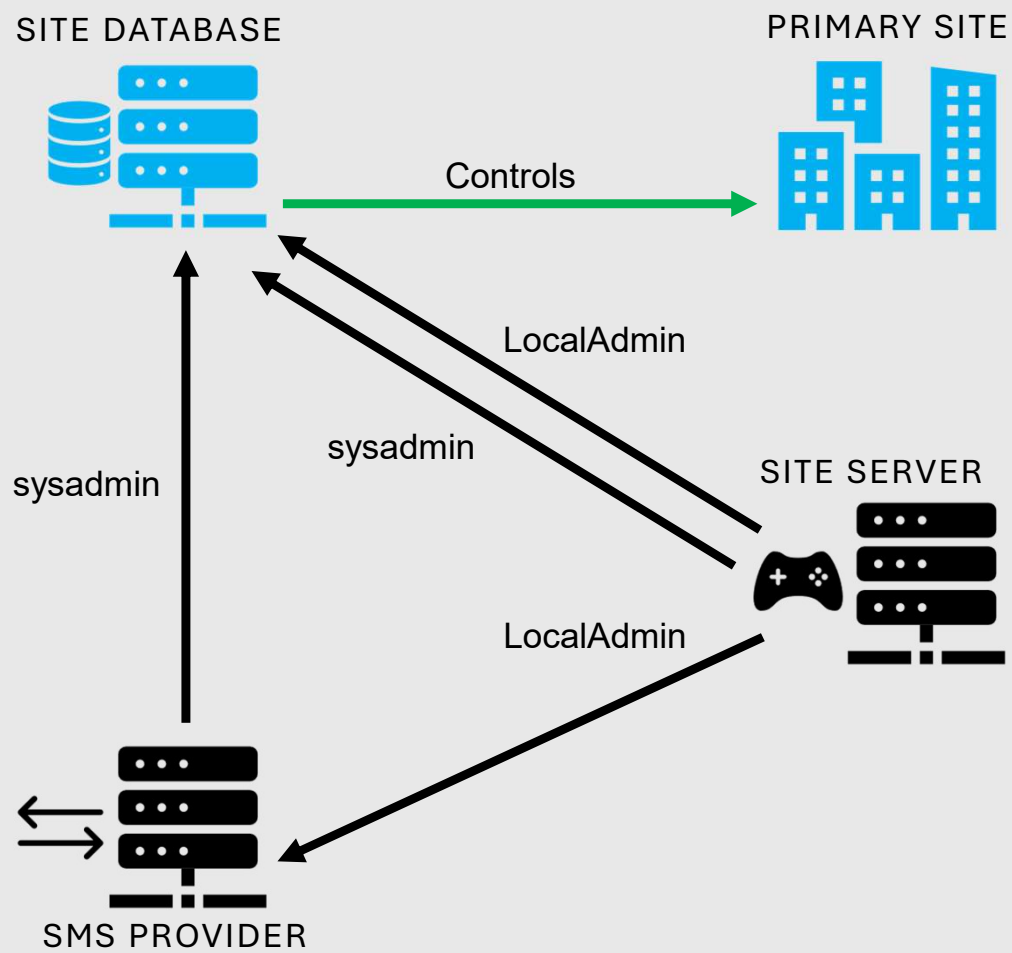


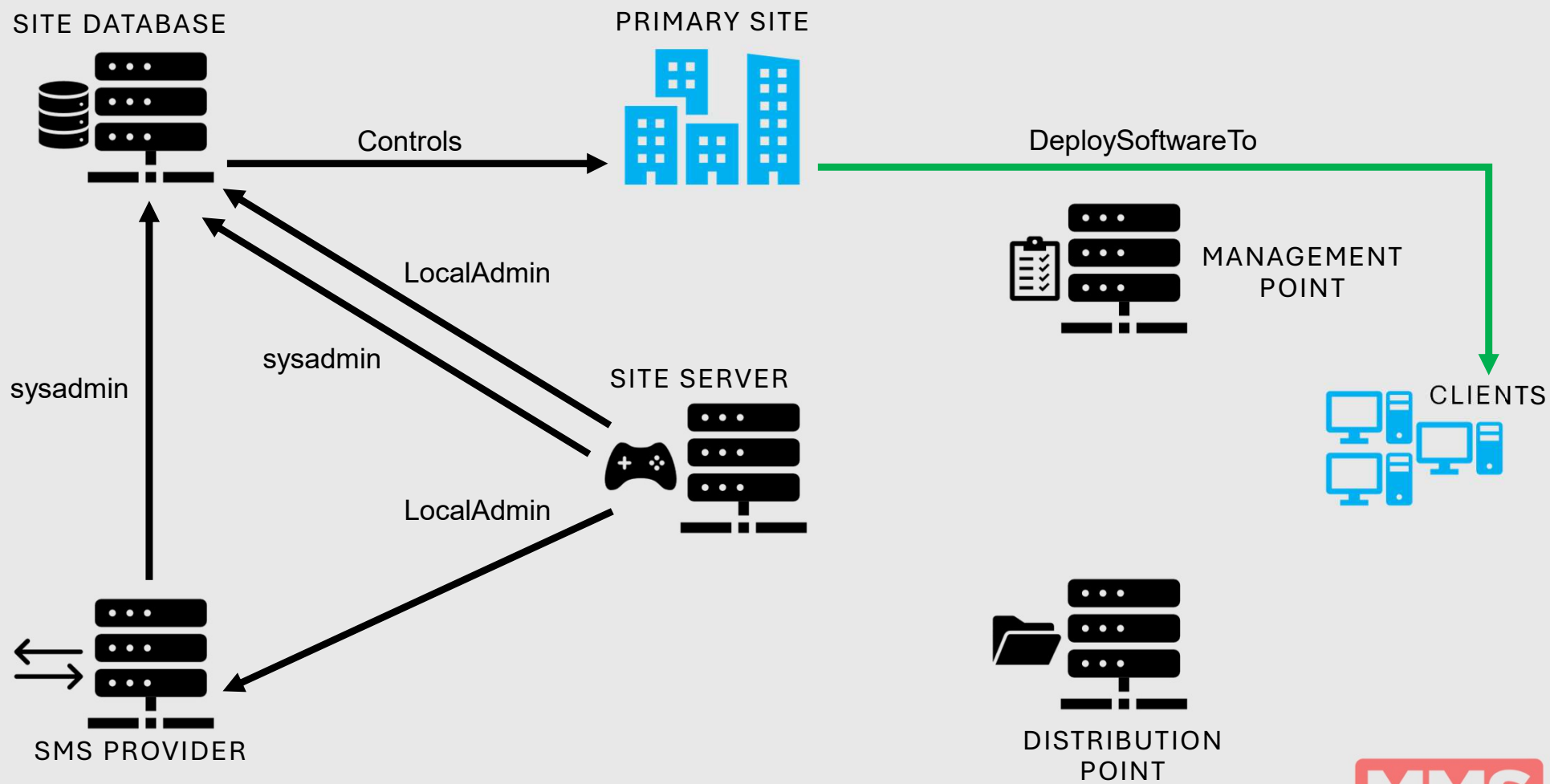
CLIENTS



DISTRIBUTION
POINT







NTLM

- One protocol that Windows users and computers use to **authenticate over the network** without a password

NTLM Relay

- Attackers can **coerce** computers into authenticating to their machine and **relay** the NTLM messages to another machine where that computer has privileges
- Allows **impersonation** of the coerced computer

NTLM Relay in SCCM

site servers

- Attackers can **coerce** computers into authenticating to their machine and **relay** the NTLM messages to another machine where that computer has privileges...
- Allows **impersonation** of the coerced computer

NTLM Relay in SCCM

site servers

- Attackers can **coerce** computers into authenticating to their machine and **relay** the NTLM messages to another machine where that computer has privileges... such as the **site database**
- Allows **impersonation** of the coerced computer

NTLM Relay in SCCM

- Won't-fix Windows issues like Printerbug, **PetitPotam** make coercion from site servers trivial

NTLM Relay in SCCM

- Won't-fix Windows issues like Printerbug, **PetitPotam** make coercion from site servers trivial
- NTLM can also be coerced when automatic client push installation is enabled with NTLM fallback (ELEVATE-2/ELEVATE-3)

NTLM Relay in SCCM

- Won't-fix Windows issues like Printerbug, **PetitPotam** make coercion from site servers trivial
- NTLM can also be coerced when automatic client push installation is enabled with NTLM fallback (ELEVATE-2/ELEVATE-3)
 - Site server authenticates with ALL configured accounts, then its domain account, which requires local admin privileges to install client

NTLM Relay in SCCM

- Susceptible when hosted **remotely** from the site server:
 - site database - MSSQL/SMB
 - SMS Provider - AdminService/WMI/SMB
 - passive/active site servers - SMB
 - other site system roles - SMB

NTLM Relay in SCCM

Cross-protocol compatibility

SMB

- > SMB
- > MSSQL
- > HTTP(S)

HTTP (WebDAV Redirector / WebClient)

- > LDAP(S)
- > HTTP(S)

Questions so far?



SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to
MSSQL on remote site database



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database



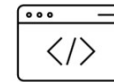
TAKEOVER-3

NTLM coercion and relay
to HTTP on ADCS



TAKEOVER-4

NTLM coercion and relay from
CAS to origin primary site server



TAKEOVER-5

NTLM coercion and relay to
AdminService on remote SMS Provider



TAKEOVER-6

NTLM coercion and relay
to SMB on remote
SMS Provider



TAKEOVER-7

NTLM coercion and relay
to SMB between primary
and passive site servers



TAKEOVER-8

NTLM coercion and relay
HTTP to LDAP
on domain controller

SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to
MSSQL on remote site database

TAKEOVER



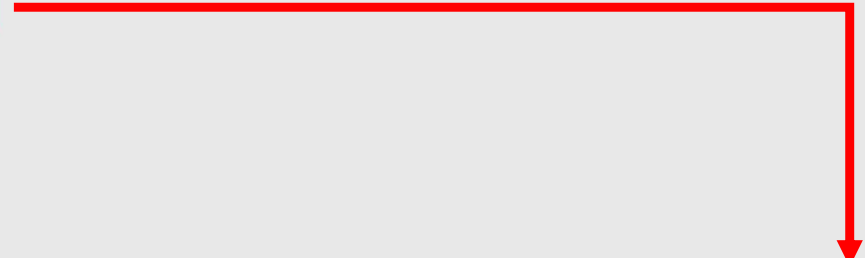
SITE DATABASE



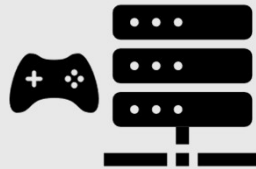
PRIMARY SITE



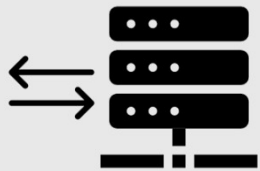
DeploySoftwareTo



SITE SERVER



CLIENTS



SMS PROVIDER



SITE DATABASE



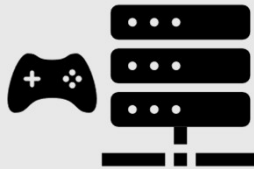
Controls

PRIMARY SITE

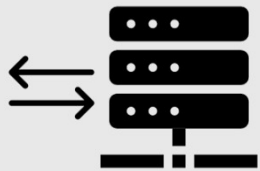


DeploySoftwareTo

SITE SERVER



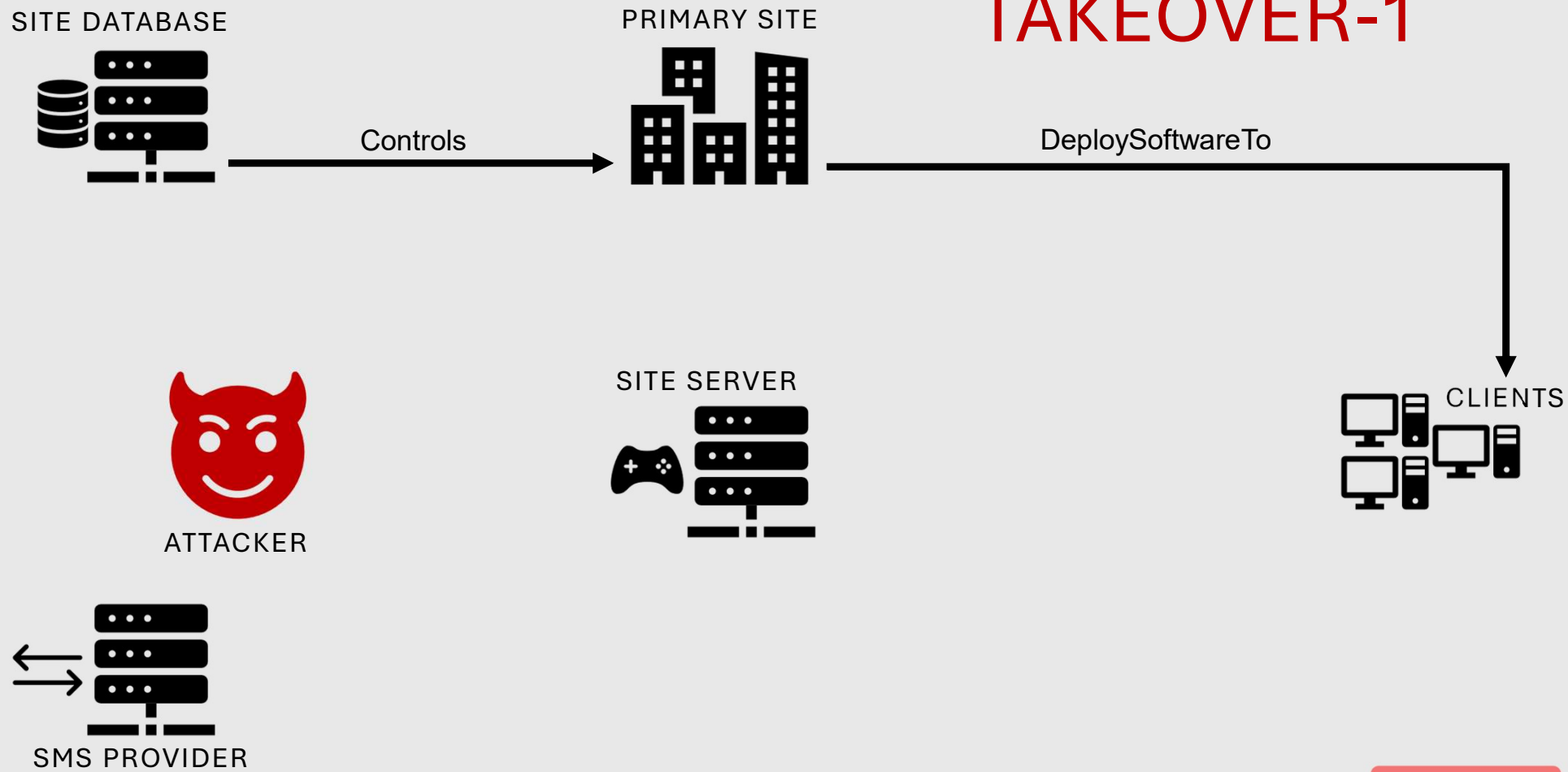
CLIENTS



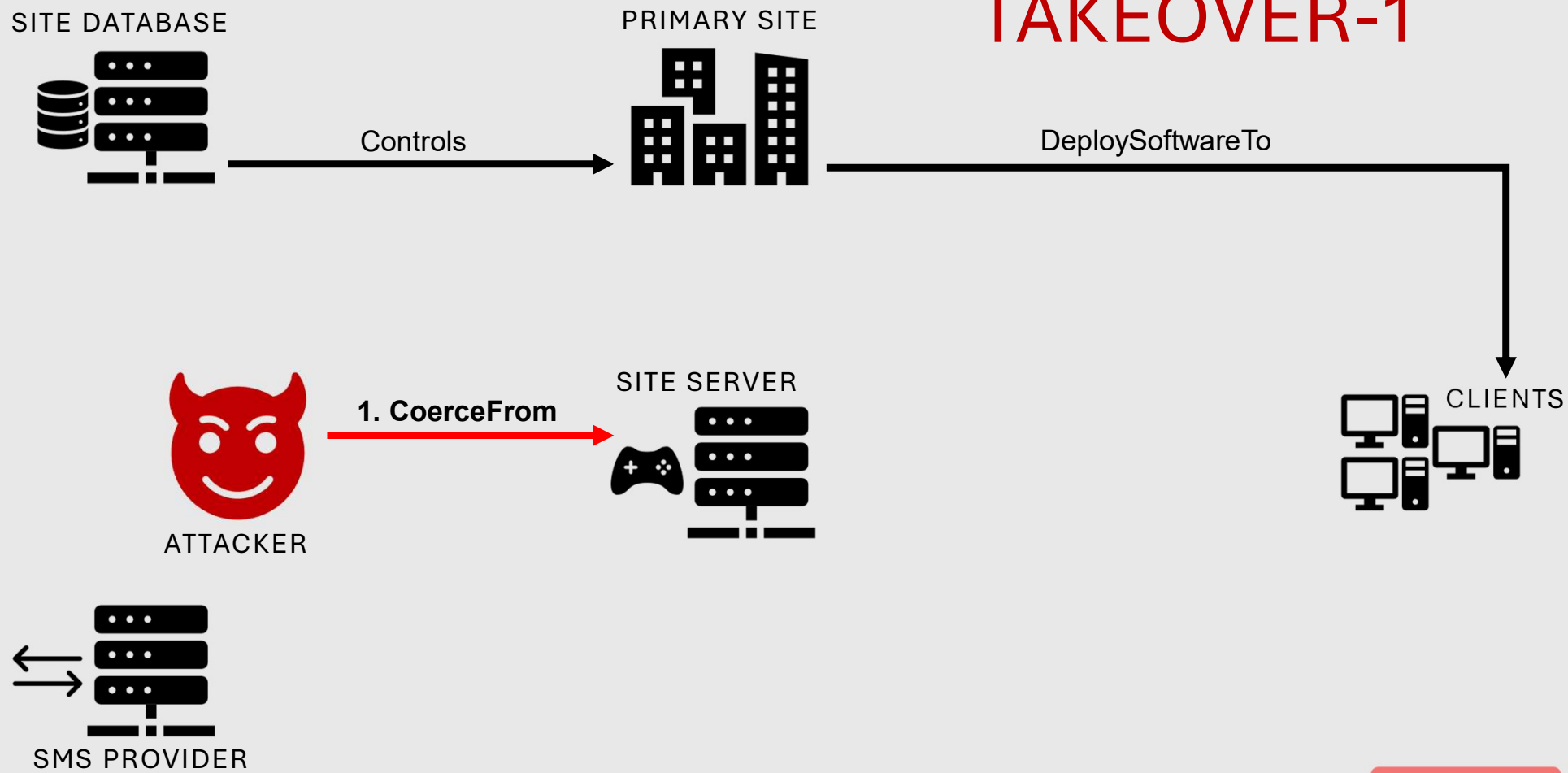
SMS PROVIDER



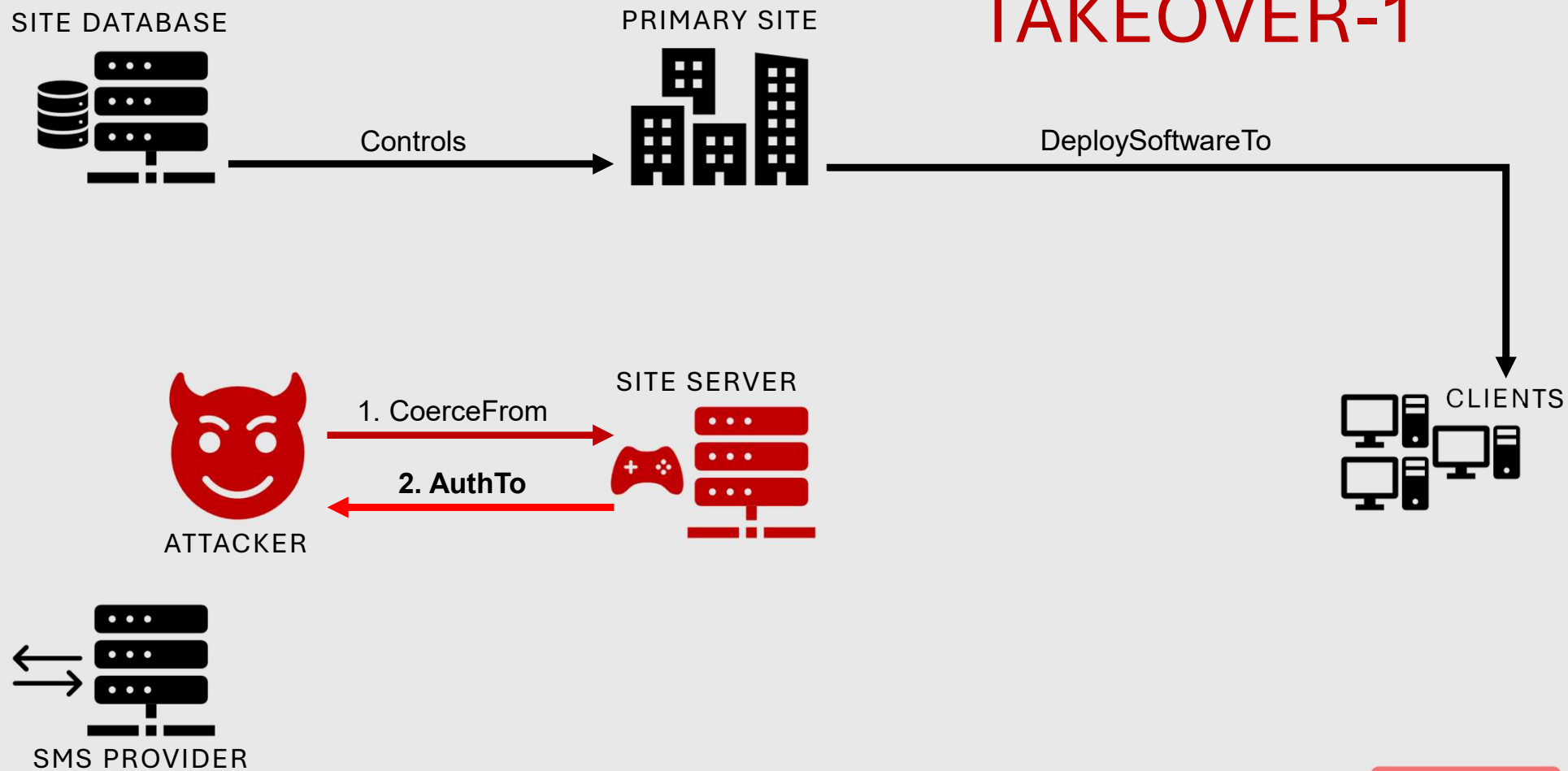
TAKEOVER-1



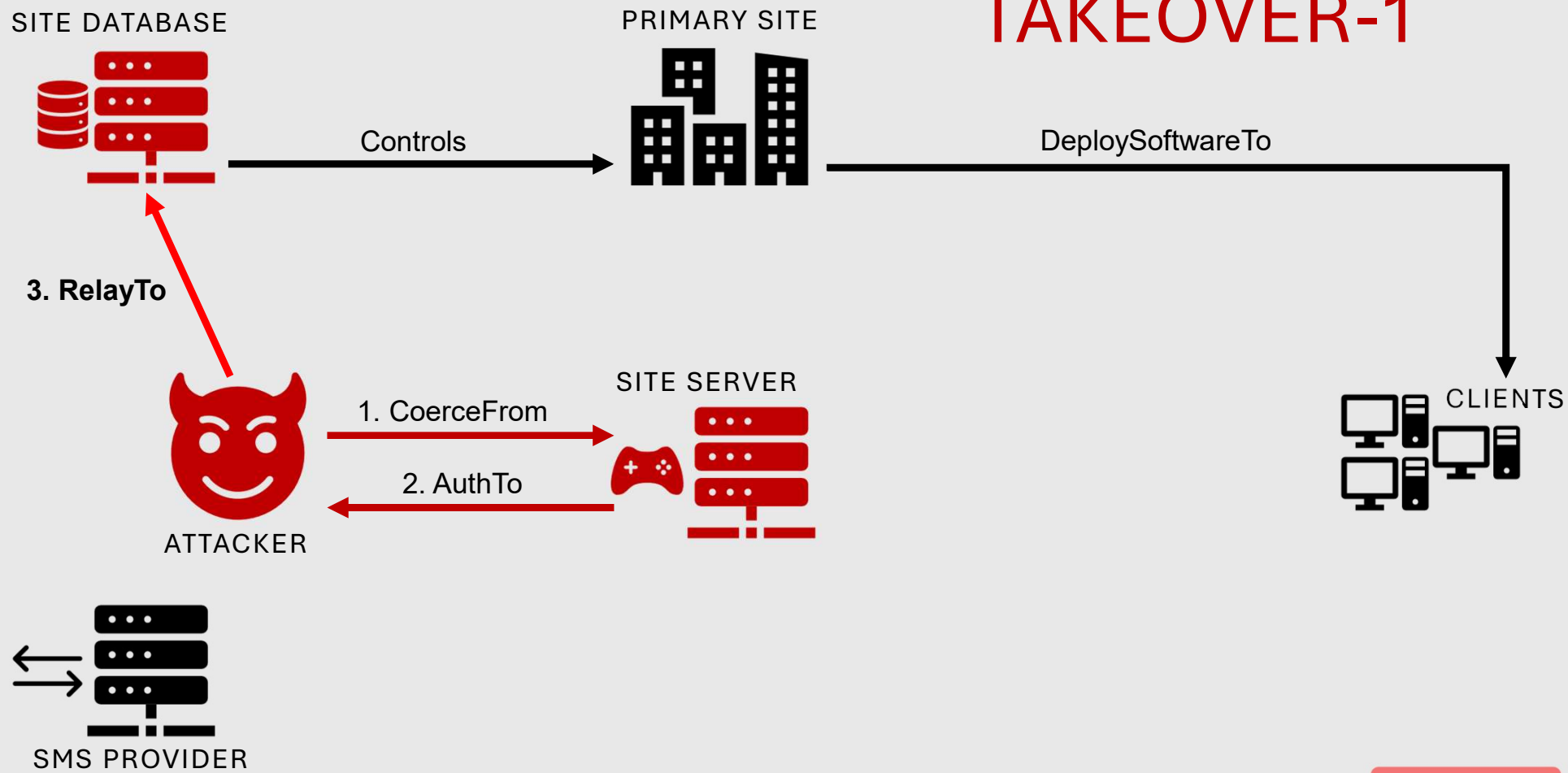
TAKEOVER-1



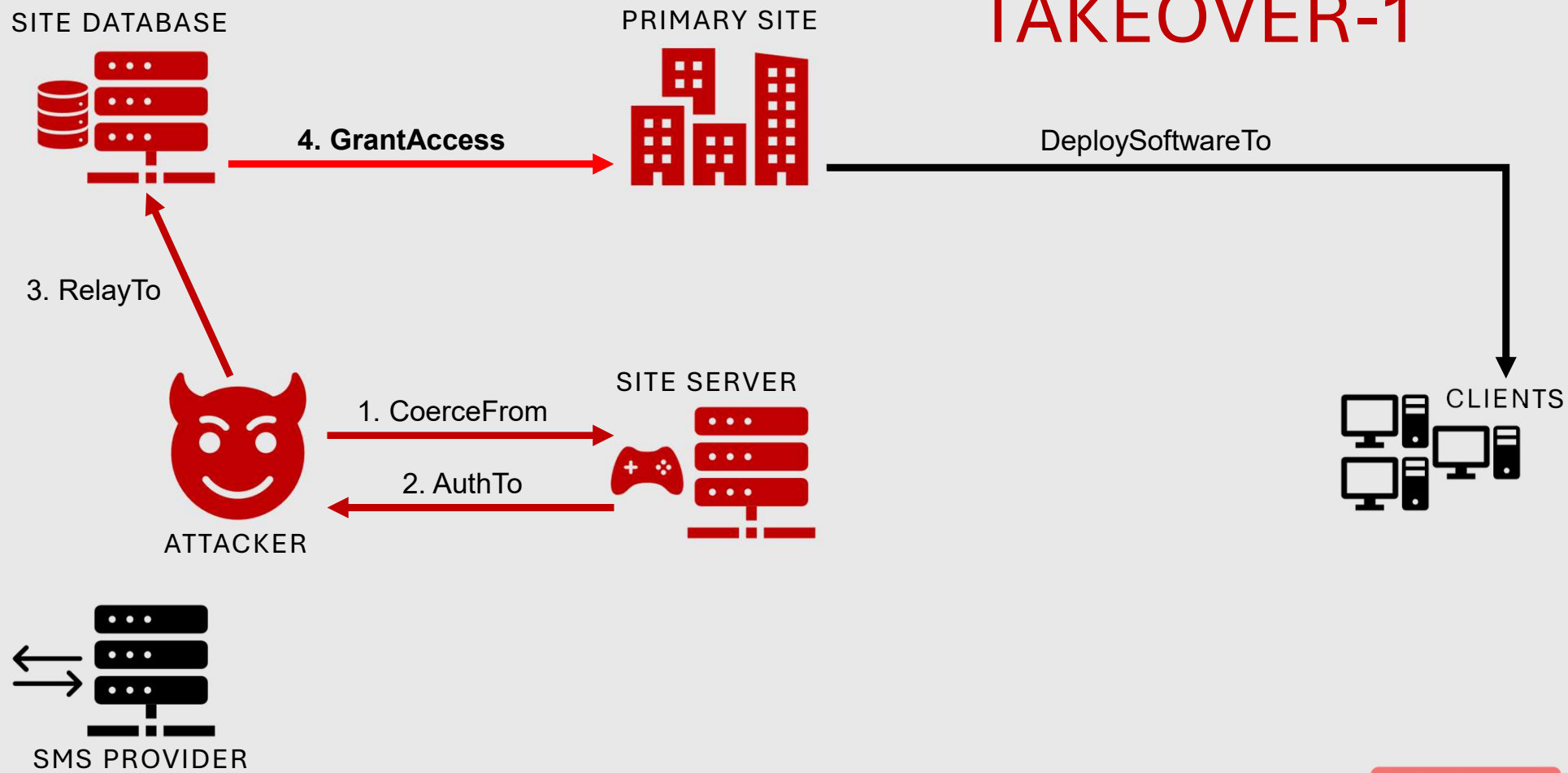
TAKEOVER-1



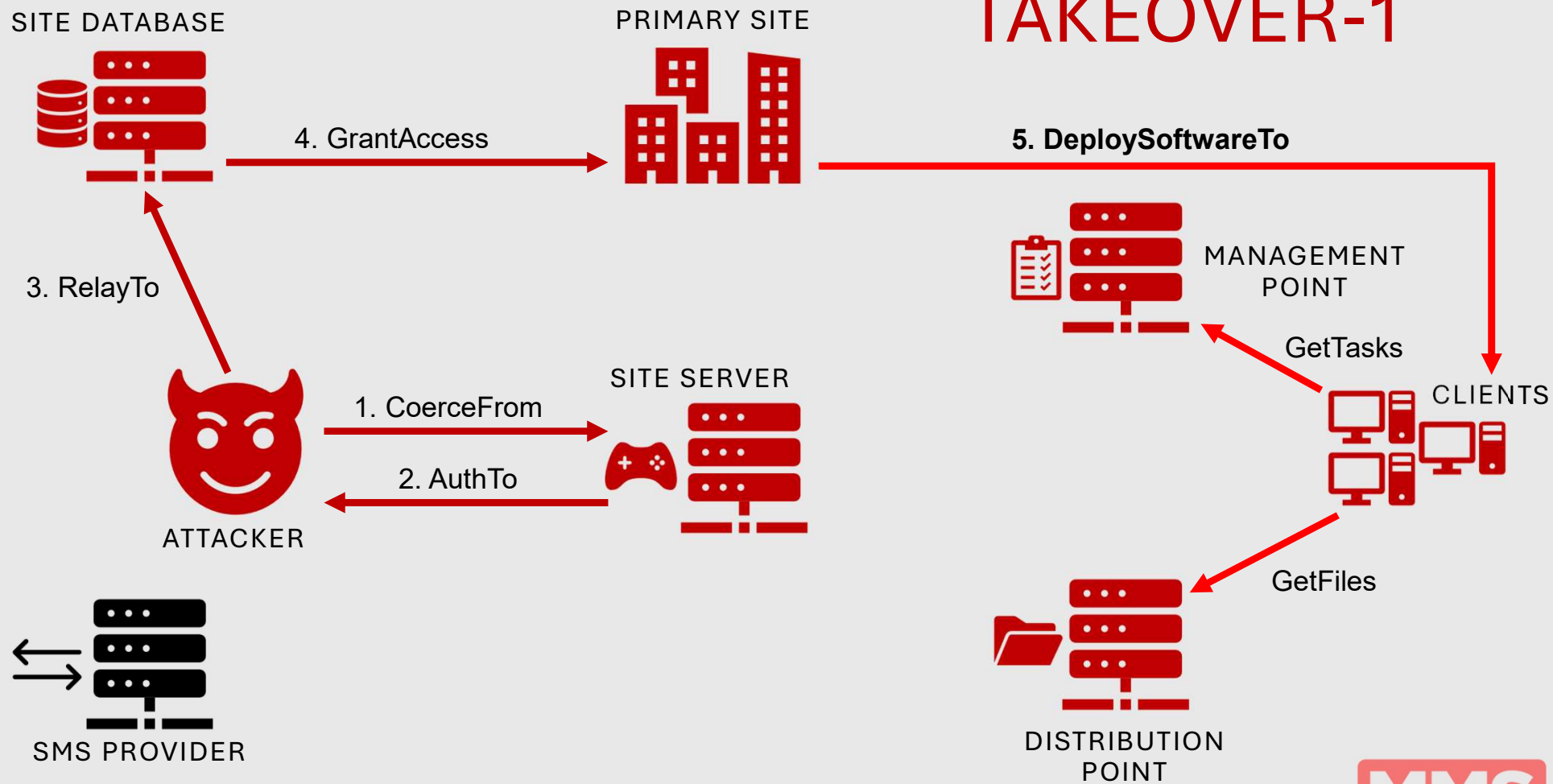
TAKEOVER-1



TAKEOVER-1



TAKEOVER-1



DEMO

Hierarchy TAKEOVER-1



NTLM Relay Prevention

Just **disable NTLM** for the domain, it's easy!

- Only kidding, please don't do this
- This recommendation is common (Chris is guilty of making it) but it isn't feasible to just flip the switch in most organizations
- Careful monitoring must take place beforehand to identify clients that don't support Kerberos
- However, **this doesn't account for Kerberos relay attacks**

NTLM Relay Prevention

Message Signing (SMB, LDAP/S)

- A digital signature of each message is attached to the NTLM authenticate message, preventing tampering
- Uses a shared session key (based on the user's password hash, which the attacker-in-the-middle does not know) to hash message

NTLM Relay Prevention

Channel Binding (MSSQL, LDAPS, HTTPS)

- Part of extended protection for authentication (EPA)
- Server checks that the TLS certificate hash embedded in the NTLM authenticate message from the client matches its own certificate

<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>



NTLM Relay Prevention

Service Binding (MSSQL)

- Part of extended protection for authentication (EPA)
- Server checks that the service principal name (SPN) embedded in the NTLM authenticate message from the client matches its own SPN
- **Weaker than channel binding**, because the SPN is based on network information that can be manipulated by an attacker, such as DNS records or resolution
 - e.g., MSSQLSvc/hostname.domain.com:1433

NTLM Relay Prevention

Firewalls!

- **Disable/block unnecessary connectivity** to protocols that don't support **enforcement** of signing, channel binding, or service binding



TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Require EPA on site databases

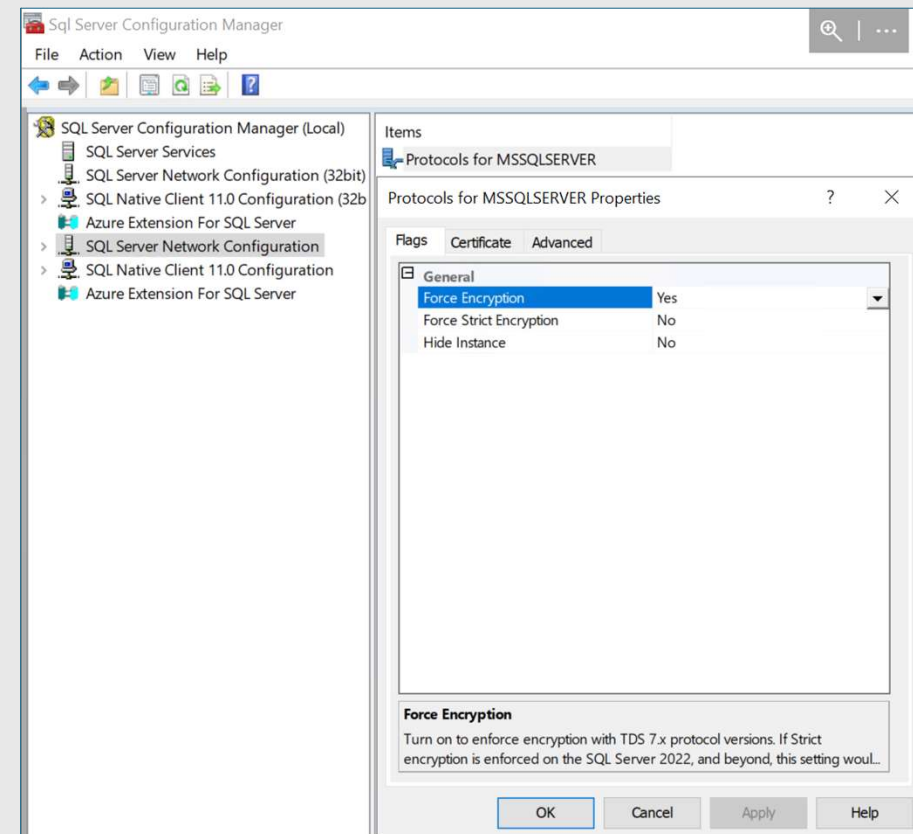
PREVENT-14

On **remote** site database servers:

1. Open Sql Server Configuration Manager
2. Click “Sql Server Network Configuration”
3. Right click “Protocols for MSSQLSERVER”, then click “Properties”
4. Set “Force Encryption” to “Yes”

If this setting is not configured, only service binding is enforced (not channel binding)

<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/connect-to-the-database-engine-using-extended-protection?view=sql-server-ver16>



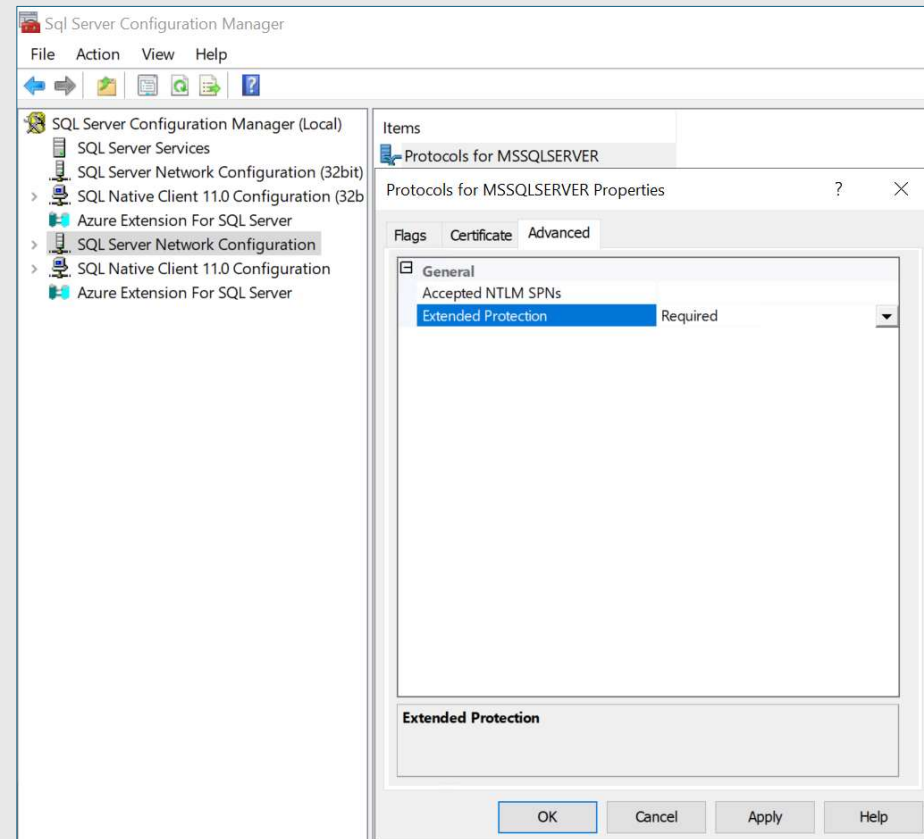
Require EPA on site databases

PREVENT-14

5. Navigate to the “Advanced” tab
6. Set “Extended Protection” to “Required”
7. Click “Apply”, then “OK”
8. Restart the “SQL Server (MSSQLSERVER)” service

Setting to “Allowed” will not prevent NTLM relay attacks if the coerced client doesn’t support channel binding

<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/connect-to-the-database-engine-using-extended-protection?view=sql-server-ver16>



SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to
MSSQL on remote site database



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database



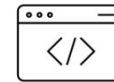
TAKEOVER-3

NTLM coercion and relay
to HTTP on ADCS



TAKEOVER-4

NTLM coercion and relay from
CAS to origin primary site server



TAKEOVER-5

NTLM coercion and relay to
AdminService on remote SMS Provider



TAKEOVER-6

NTLM coercion and relay
to SMB on remote
SMS Provider



TAKEOVER-7

NTLM coercion and relay
to SMB between primary
and passive site servers



TAKEOVER-8

NTLM coercion and relay
HTTP to LDAP
on domain controller

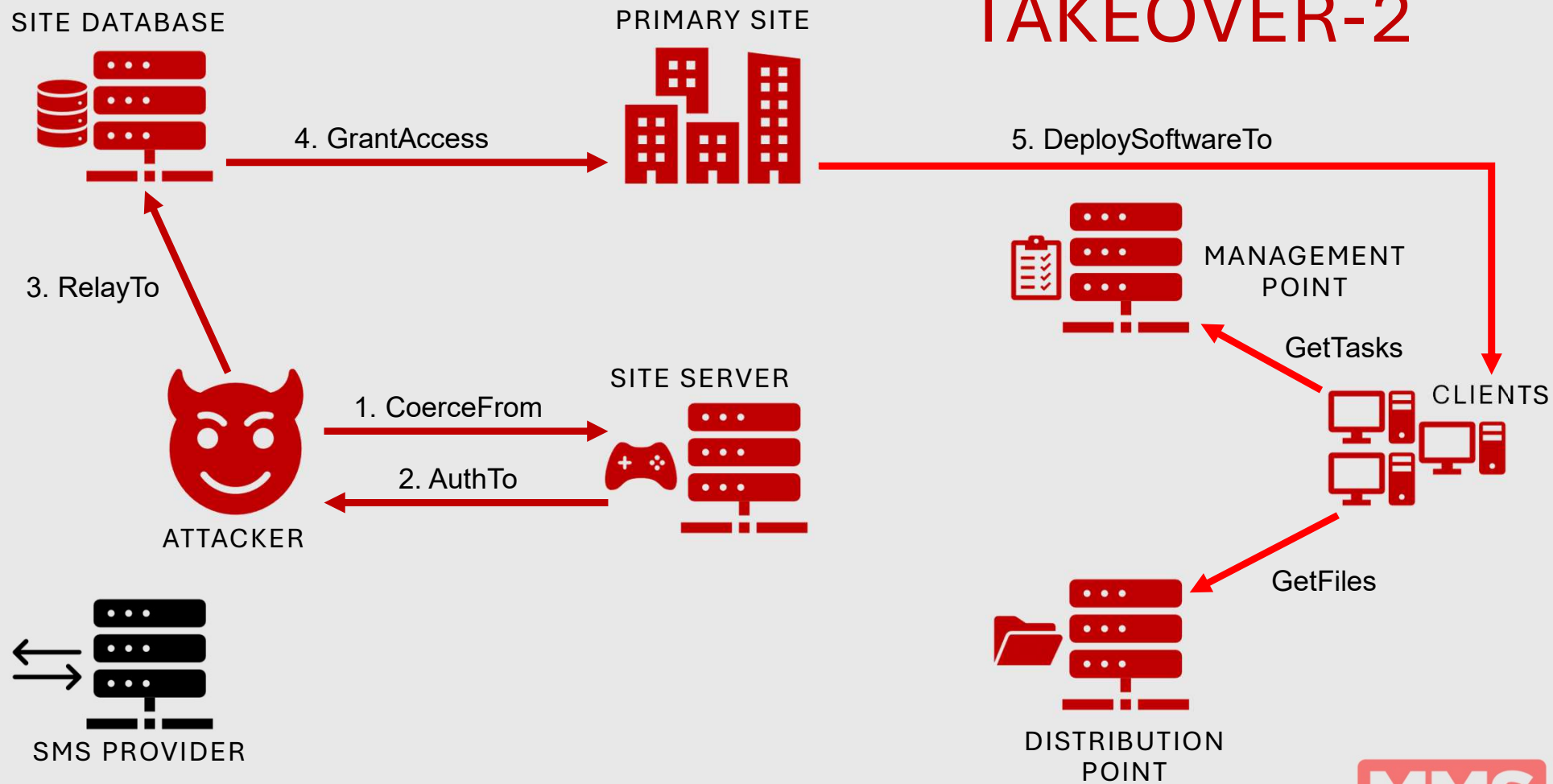
SCCM Hierarchy Takeover Attack Paths



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database

TAKEOVER-2



DEMO

Hierarchy TAKEOVER-2



SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to
MSSQL on remote site database



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database



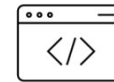
TAKEOVER-3

NTLM coercion and relay
to HTTP on ADCS



TAKEOVER-4

NTLM coercion and relay from
CAS to origin primary site server



TAKEOVER-5

NTLM coercion and relay to
AdminService on remote SMS Provider



TAKEOVER-6

NTLM coercion and relay
to SMB on remote
SMS Provider



TAKEOVER-7

NTLM coercion and relay
to SMB between primary
and passive site servers



TAKEOVER-8

NTLM coercion and relay
HTTP to LDAP
on domain controller

SCCM Hierarchy Takeover Attack Paths



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database



TAKEOVER-4

NTLM coercion and relay from
CAS to origin primary site server



TAKEOVER-6

NTLM coercion and relay
to SMB on remote
SMS Provider



TAKEOVER-7

NTLM coercion and relay
to SMB between primary
and passive site servers

ELEVATE-1



ELEVATE-1

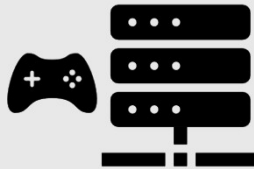
SITE DATABASE



PRIMARY SITE



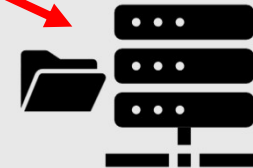
SITE SERVER



MANAGEMENT
POINT

LocalAdmin

LocalAdmin



DISTRIBUTION
POINT



CLIENTS



ATTACKER



SMS PROVIDER



ELEVATE-1

SITE DATABASE



PRIMARY SITE



ATTACKER

1. CoerceFrom

SITE SERVER



LocalAdmin

LocalAdmin



MANAGEMENT
POINT



CLIENTS



DISTRIBUTION
POINT



SMS PROVIDER



ELEVATE-1

SITE DATABASE



PRIMARY SITE



ATTACKER

1. CoerceFrom

2. AuthTo

SITE SERVER



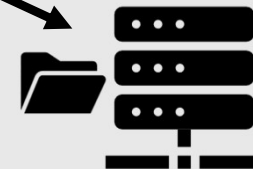
MANAGEMENT
POINT

LocalAdmin



CLIENTS

LocalAdmin



DISTRIBUTION
POINT



SMS PROVIDER



ELEVATE-1

SITE DATABASE



PRIMARY SITE



3. RelayTo

1. CoerceFrom

2. AuthTo

SITE SERVER

LocalAdmin

LocalAdmin

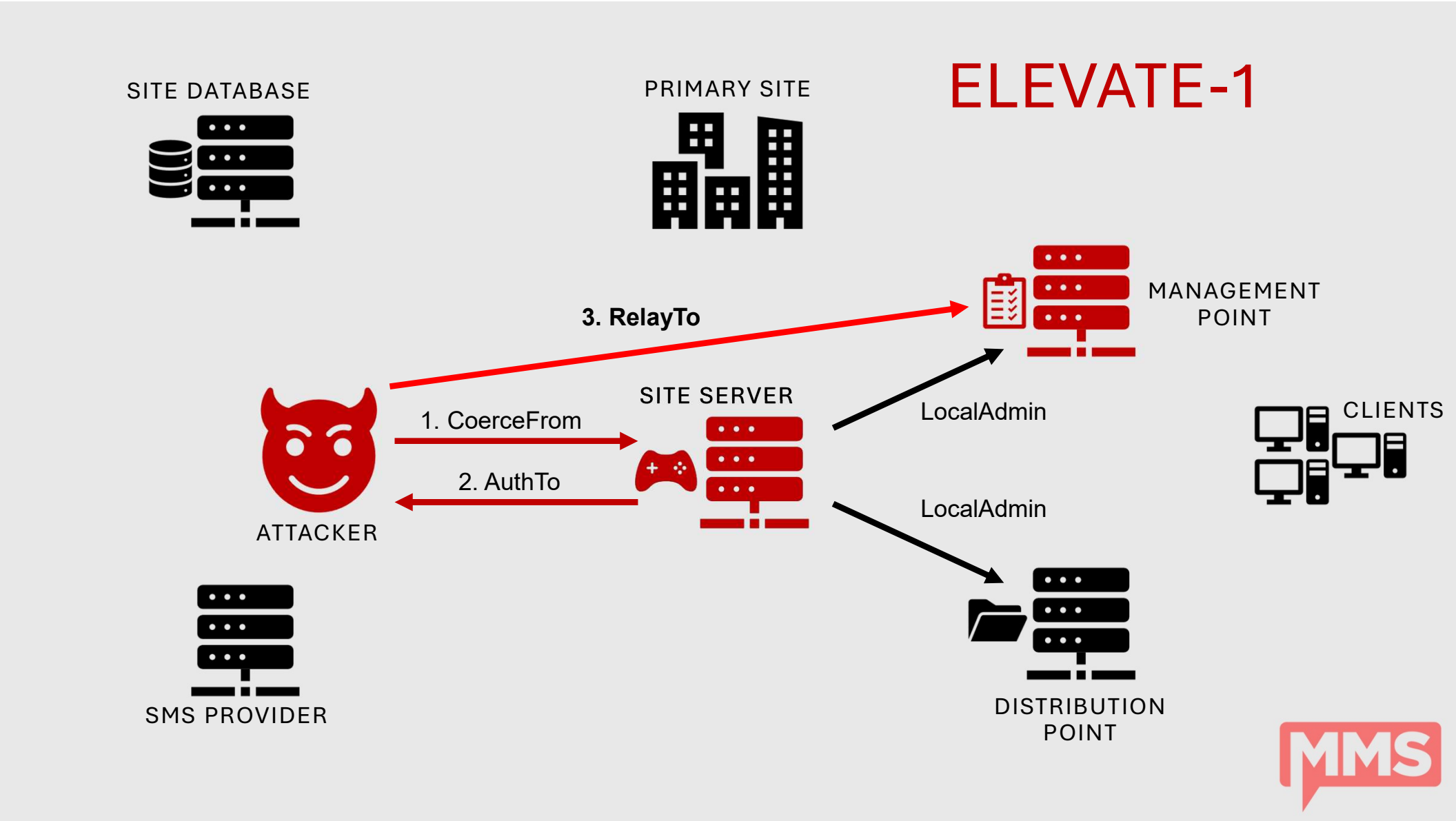
MANAGEMENT
POINT

CLIENTS

ATTACKER

SMS PROVIDER

DISTRIBUTION
POINT



ELEVATE-1

SITE DATABASE



PRIMARY SITE

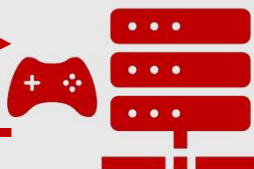


ATTACKER

1. CoerceFrom

2. AuthTo

SITE SERVER



LocalAdmin

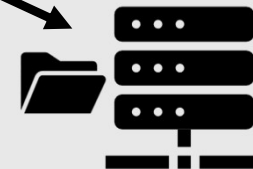
LocalAdmin



MANAGEMENT
POINT



CLIENTS



DISTRIBUTION
POINT



SMS PROVIDER



ELEVATE-1

SITE DATABASE



PRIMARY SITE



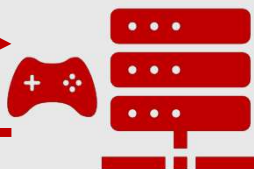
ATTACKER

1. CoerceFrom

2. AuthTo

3. RelayTo

SITE SERVER



LocalAdmin

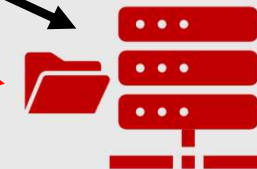
LocalAdmin



MANAGEMENT POINT



CLIENTS



DISTRIBUTION POINT



SMS PROVIDER



TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Require SMB signing on site systems

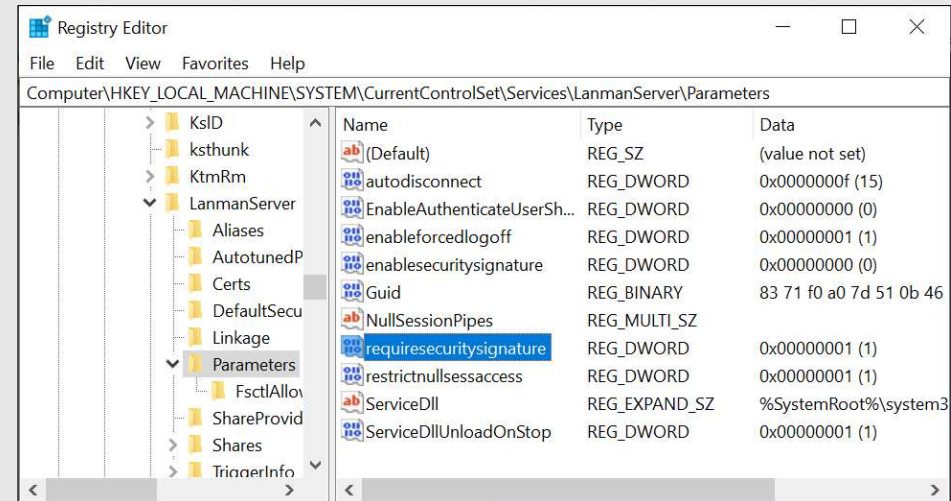
PREVENT-12

On **every** site system role and client:

1. Open regedit
2. Navigate to
HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\
3. Set “RequireSecuritySignature” to 1

Equivalent GPO: “Microsoft network client: Digitally sign communications (always)”

Configuring this setting “if client agrees” or “if server agrees” does not offer relay protection



SCCM Attack Paths



ELEVATE-2/3

NTLM coercion via automatic
client push installation

Client Push Installation

Overview

- Deploys the client software remotely from the site server
- Copies files to the ADMIN\$ share and executes the installer
- Uses configured credentials and the **site server's domain computer account**, which must be a **local admin** to install the client software
- Can be initiated manually or automatically when new devices are discovered (e.g., in a certain domain/subnet)

Automatic Site-wide Client Push Installation Abuse

ELEVATE-2

- Attackers can register a fake device record in SCCM by sending requests to a management point
- This will **cause the site server to authenticate to an arbitrary IP address specified for the fake device**
- Incoming NTLM authentication can be **cracked or relayed** to other workstations or SCCM servers (where the site server has admin privileges by default)

DEMO

ELEVATE-2



TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

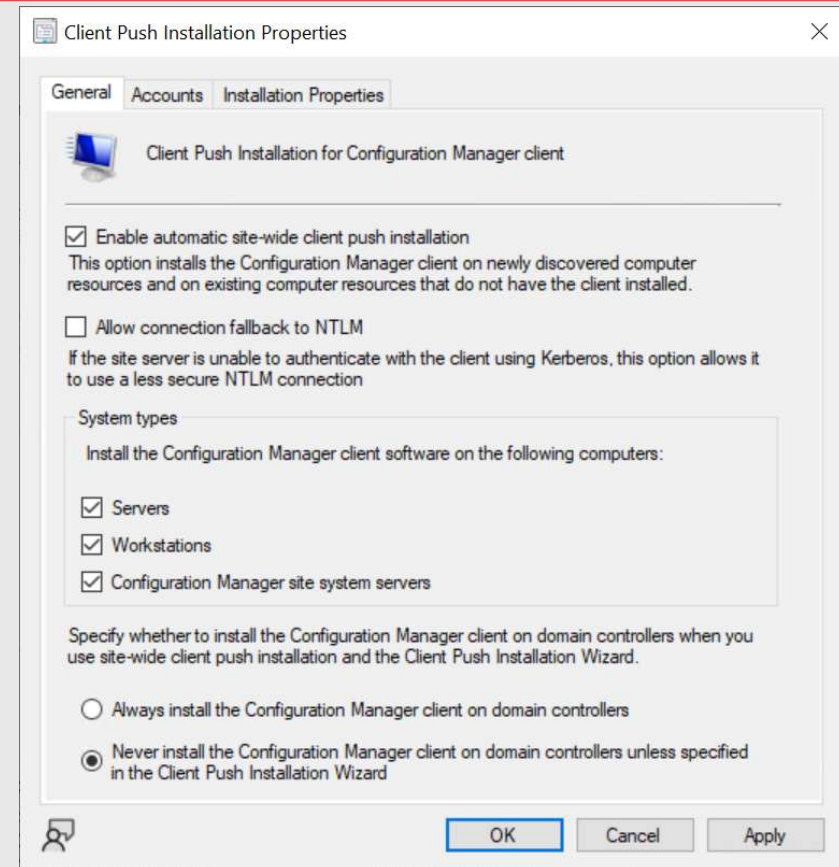
IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Disable NTLM fallback for client push installation

PREVENT-2

1. Open ConfigMgr Console
2. Navigate to “Administration”, “Overview”, “Site Configuration”, “Sites”
3. Right click the primary site, then click “Client Installation Settings”, “Client Push Installation”
4. Uncheck “Allow connection fallback to NTLM”, then click “Apply”, then “OK”

Patch KB15599094 **must** be installed for this change to take effect (**PREVENT-1**).

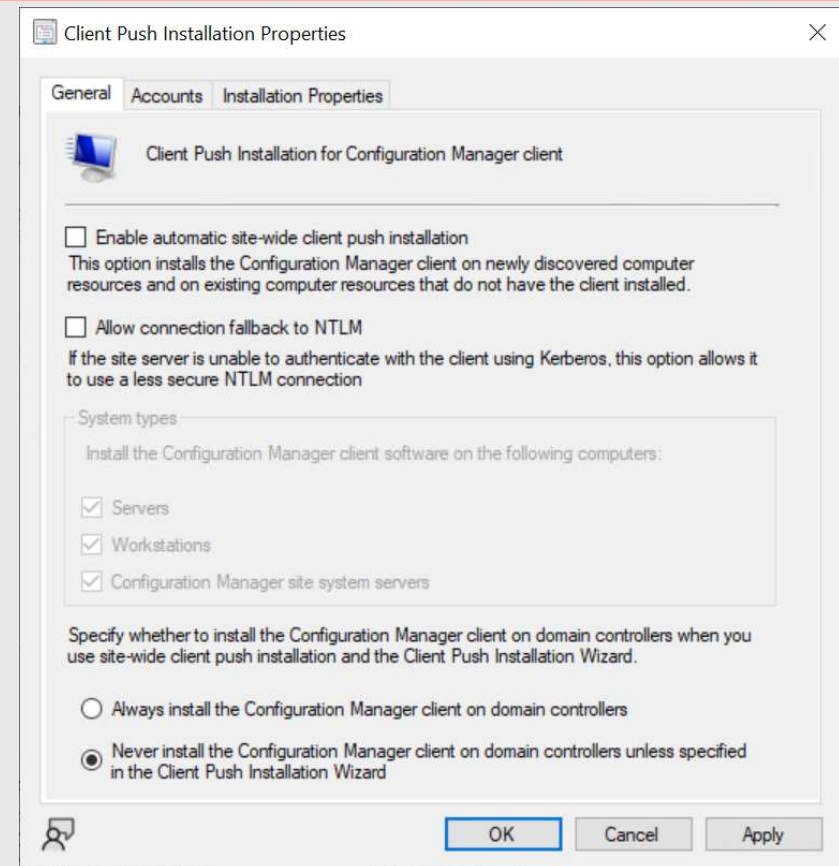


Disable automatic site-wide client push installation

PREVENT-5

1. Open ConfigMgr Console
2. Navigate to “Administration”, “Overview”, “Site Configuration”, “Sites”
3. Right click the primary site, then click “Client Installation Settings”, “Client Push Installation”
4. Uncheck “Enable automatic site-wide client push installation”, then click “Apply”, then “OK”

Does not prevent Kerberos relay if an SCCM admin initiates a manual client push installation.



SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to
MSSQL on remote site database



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database



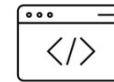
TAKEOVER-3

NTLM coercion and relay
to HTTP on ADCS



TAKEOVER-4

NTLM coercion and relay from
CAS to origin primary site server



TAKEOVER-5

NTLM coercion and relay to
AdminService on remote SMS Provider



TAKEOVER-6

NTLM coercion and relay
to SMB on remote
SMS Provider



TAKEOVER-7

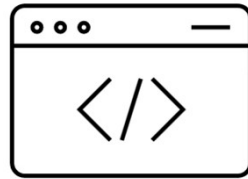
NTLM coercion and relay
to SMB between primary
and passive site servers



TAKEOVER-8

NTLM coercion and relay
HTTP to LDAP
on domain controller

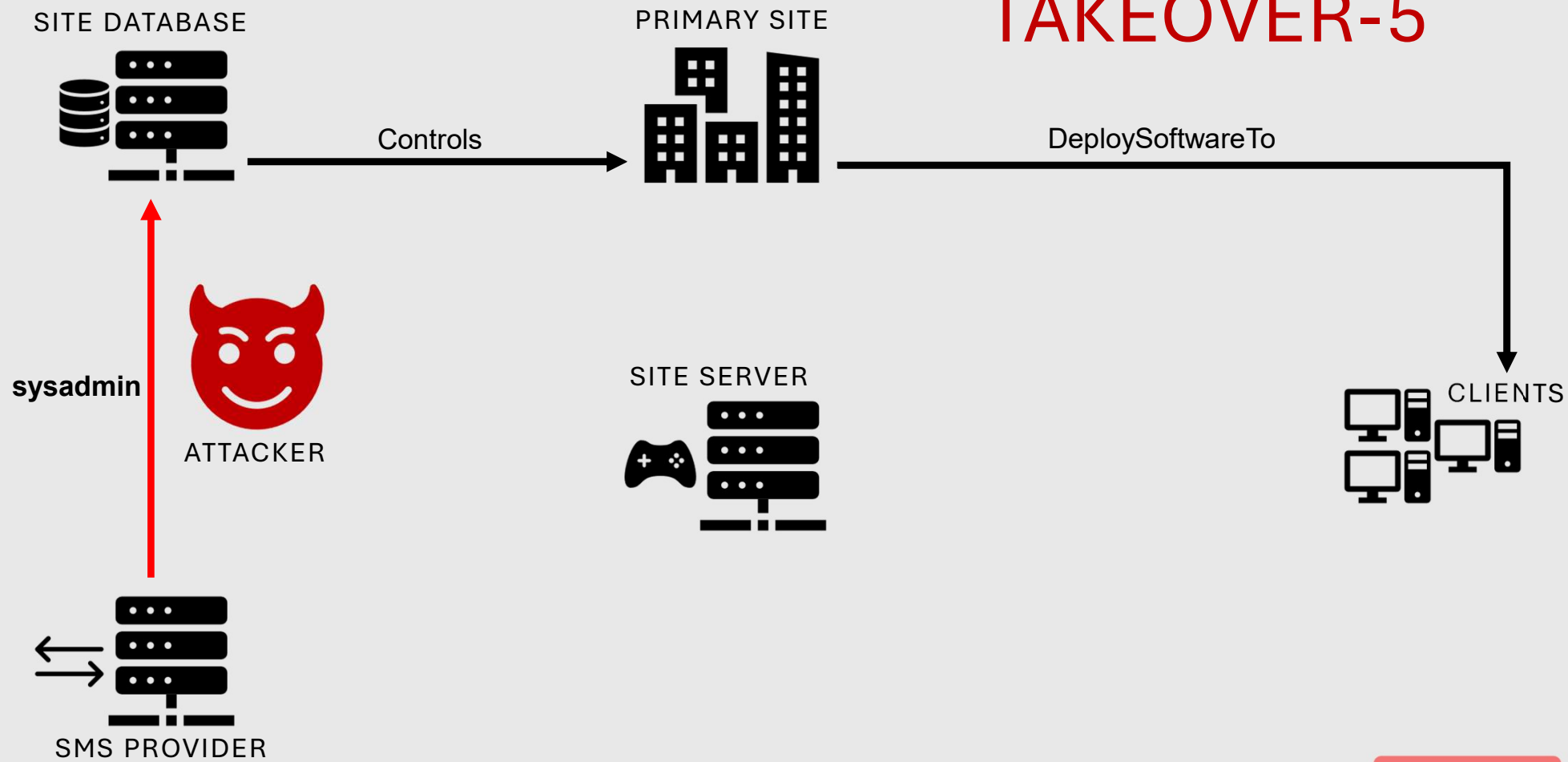
SCCM Hierarchy Takeover Attack Paths



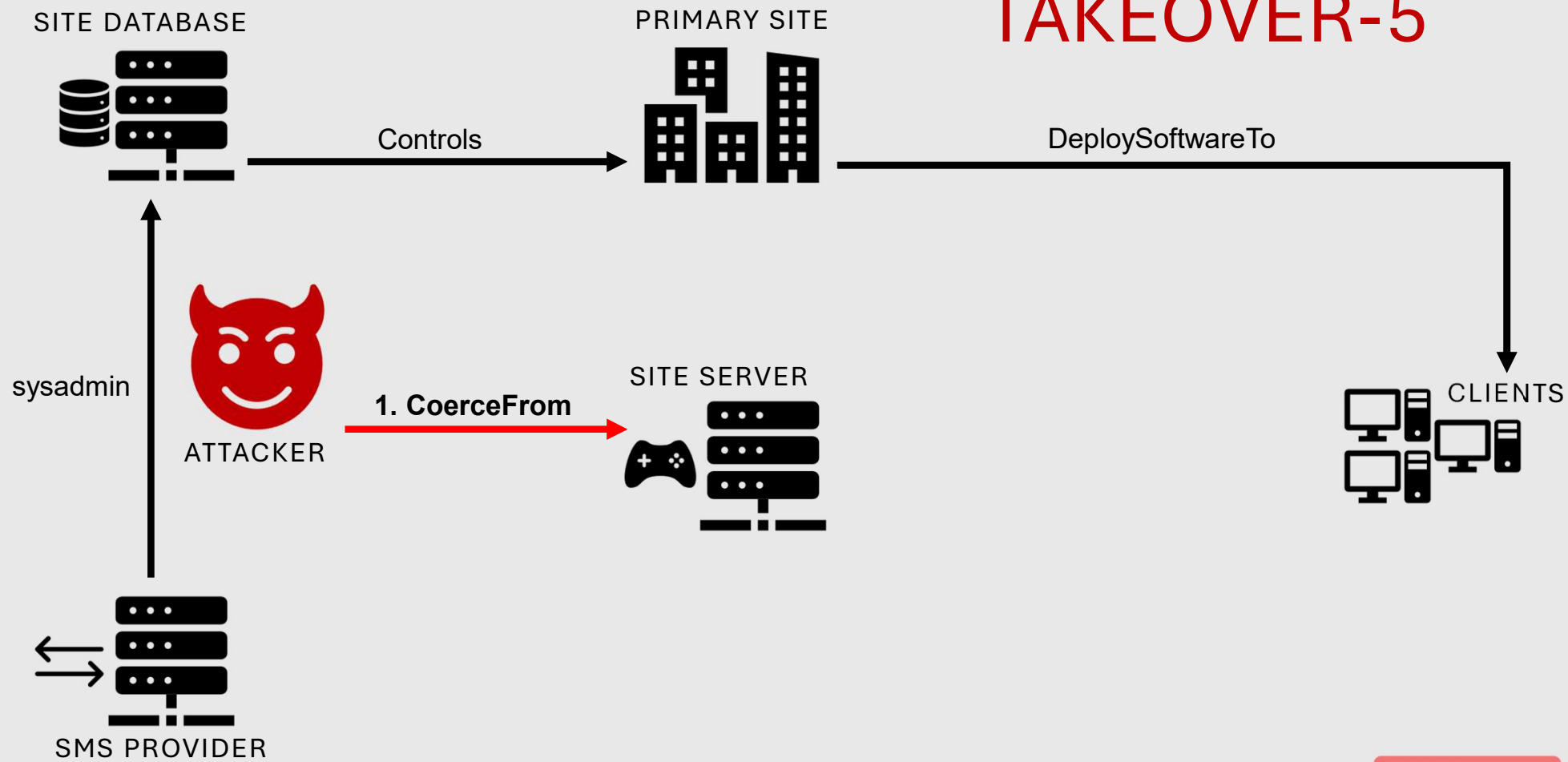
TAKEOVER-5

NTLM coercion and relay to
AdminService on remote SMS Provider

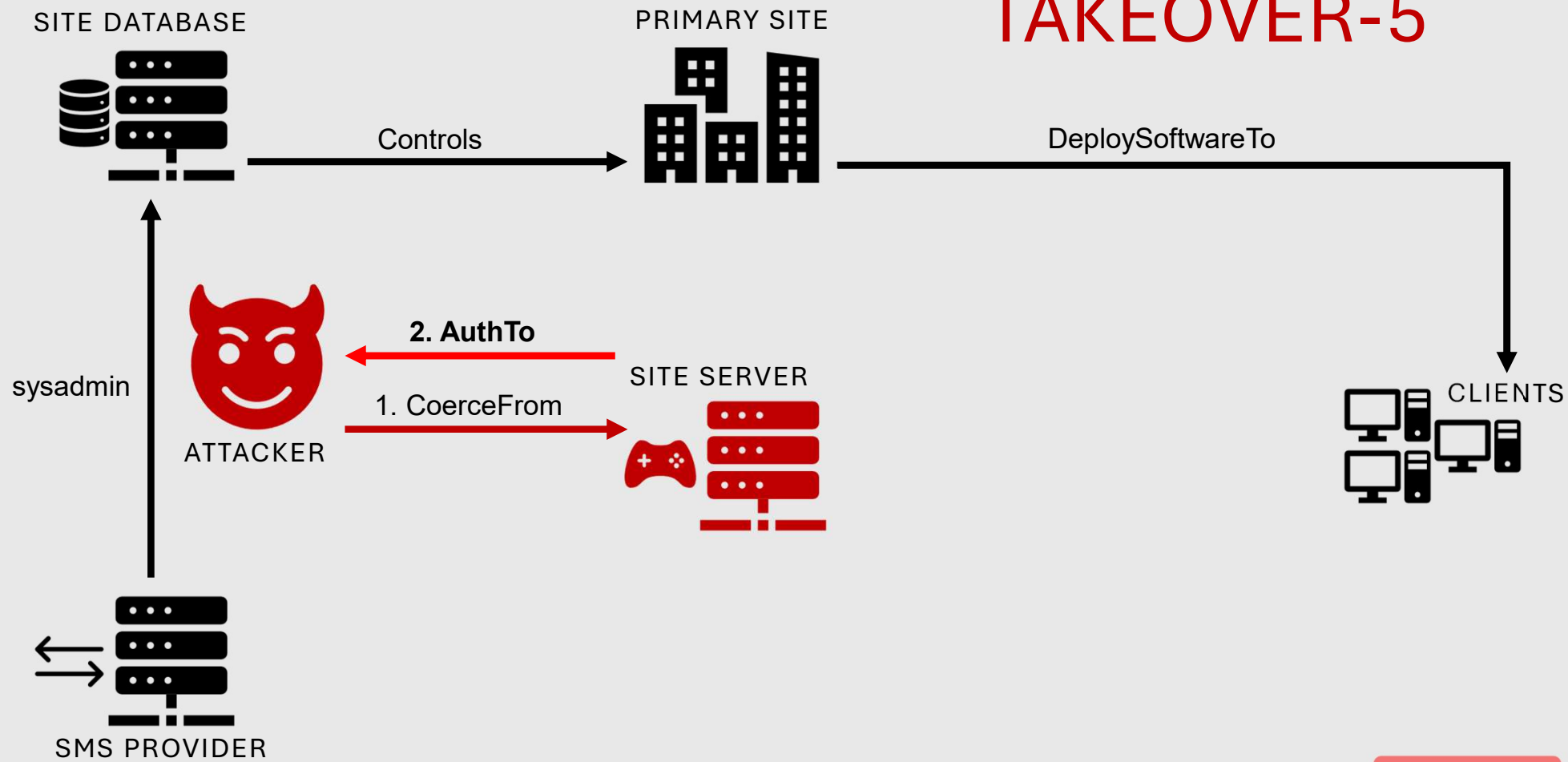
TAKEOVER-5



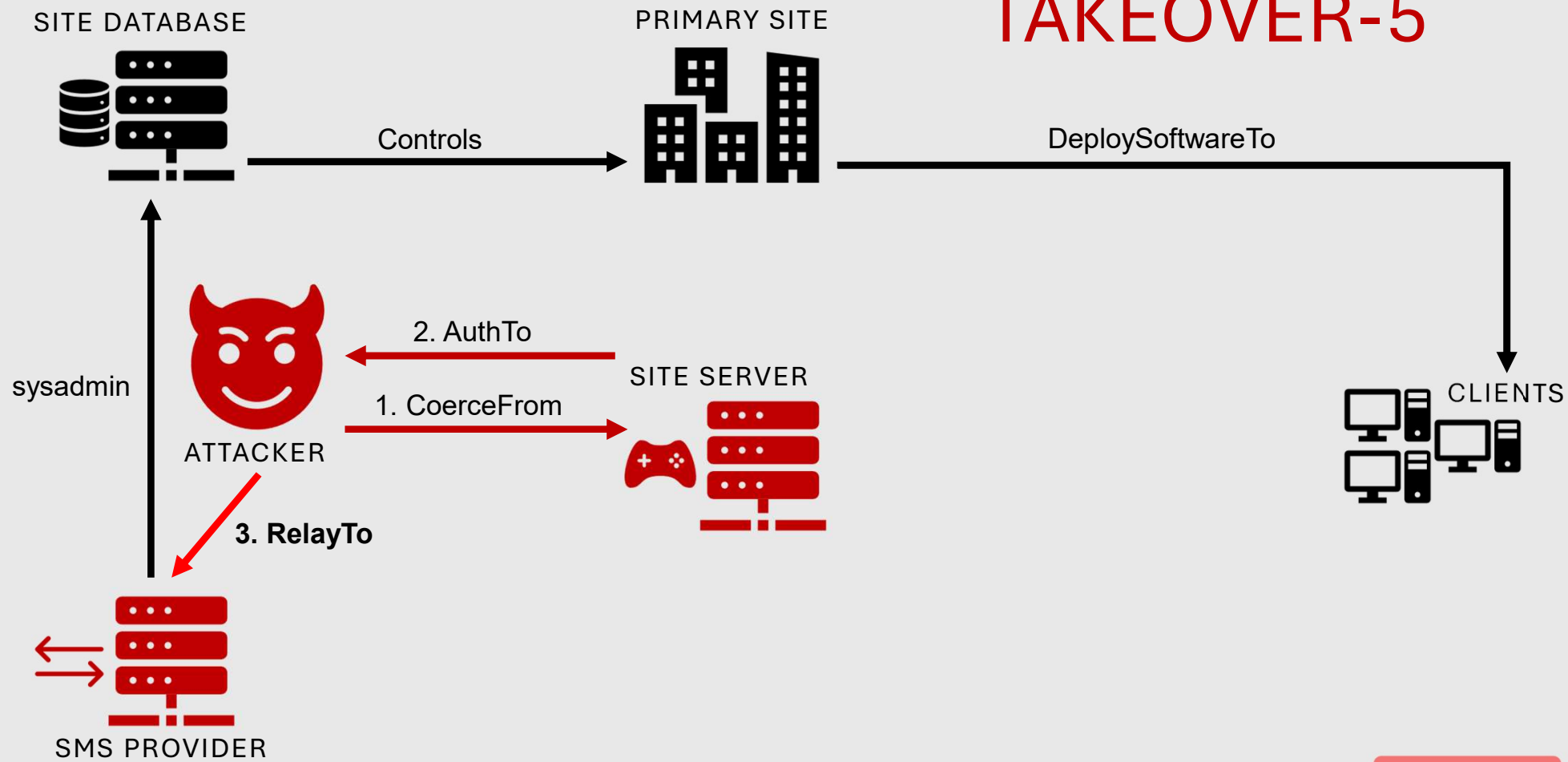
TAKEOVER-5



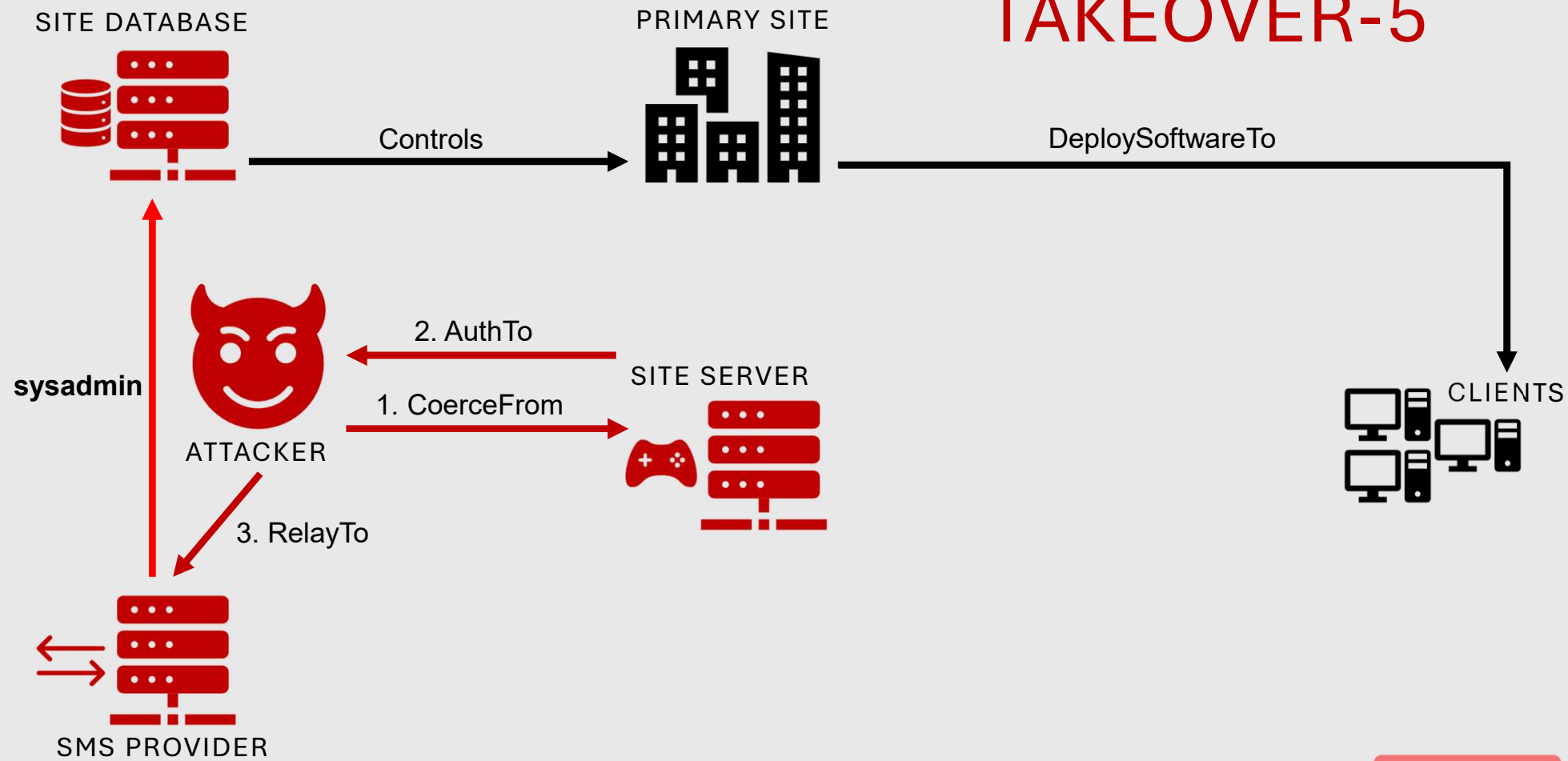
TAKEOVER-5



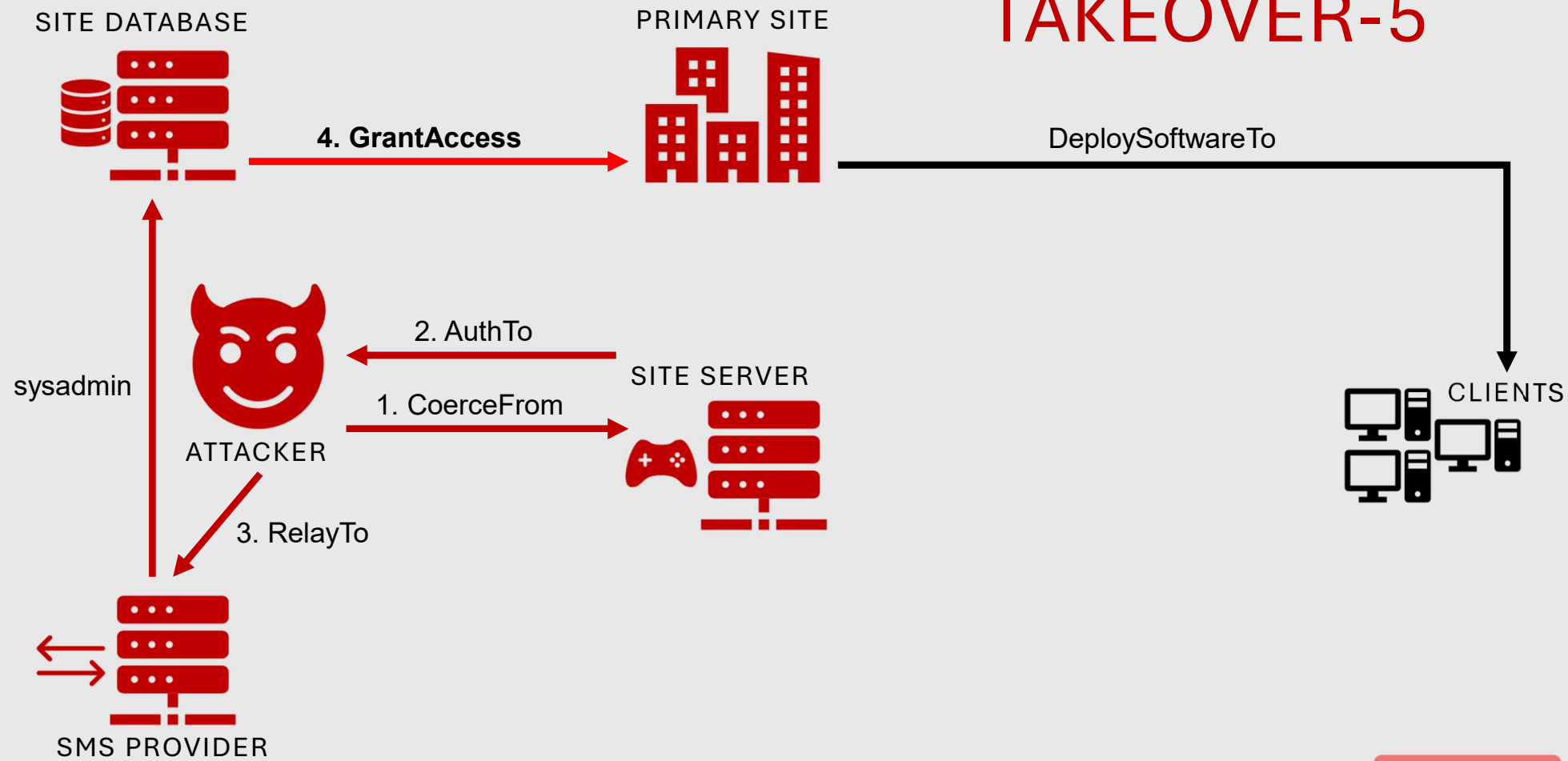
TAKEOVER-5



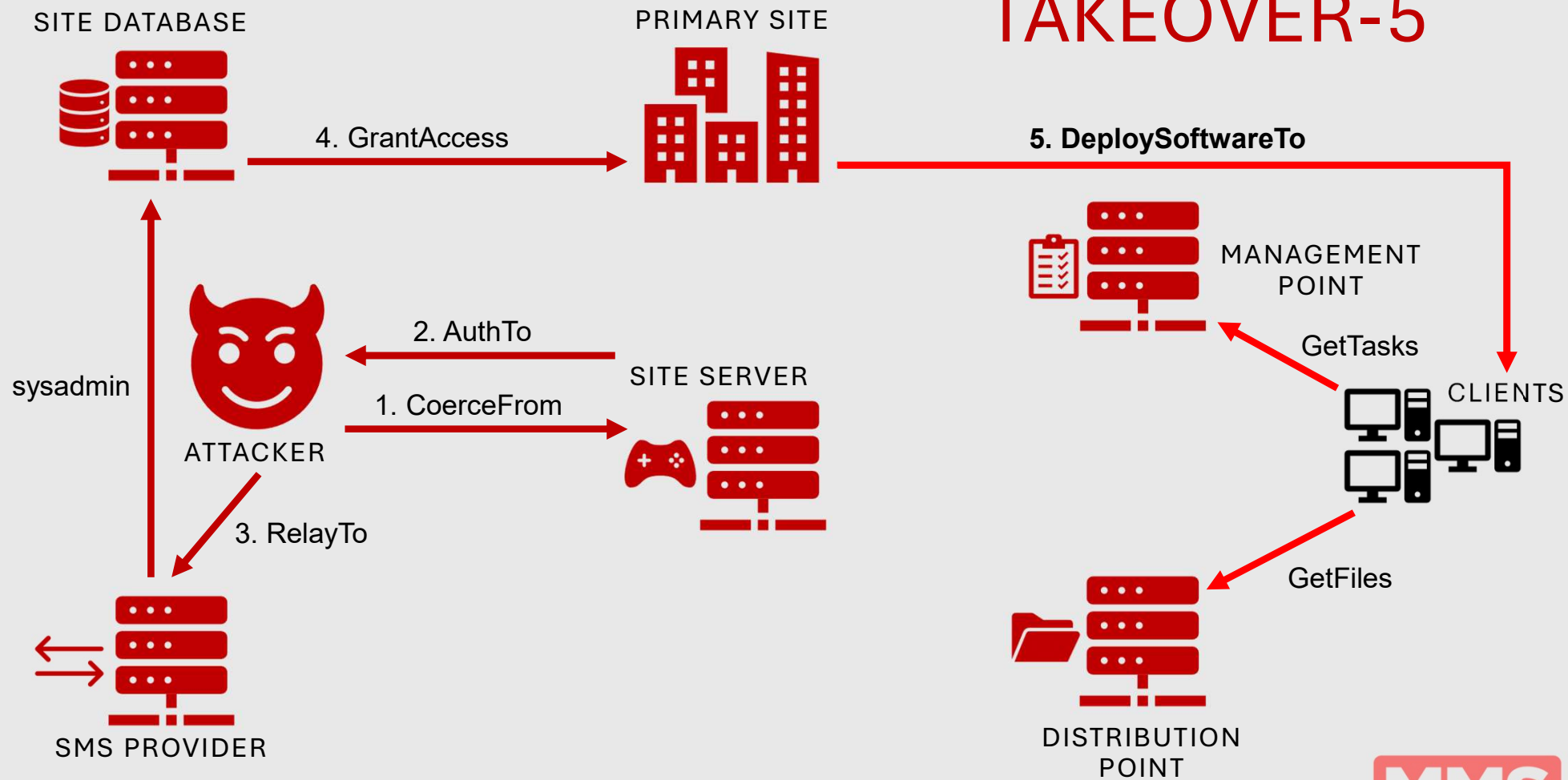
TAKEOVER-5



TAKEOVER-5



TAKEOVER-5



TAKEOVER-5



DEMO

Hierarchy TAKEOVER-5



TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

TAKEOVER-5 REMEDIATION

- **Upgrade to Configuration Manager v2509**, which denies NTLM authentication to the SMS Provider AdminService by default

OR

- Only host the SMS Provider role on a standalone primary site server
 - Won't work in hierarchies with multiple primary site servers (e.g., passive, CAS) because one can be coerced and relayed to the SMS Provider on the other



SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to
MSSQL on remote site database



TAKEOVER-2

NTLM coercion and relay to
SMB on remote site database



TAKEOVER-3

NTLM coercion and relay
to HTTP on ADCS



TAKEOVER-4

NTLM coercion and relay from
CAS to origin primary site server



TAKEOVER-5

NTLM coercion and relay to
AdminService on remote SMS Provider



TAKEOVER-6

NTLM coercion and relay
to SMB on remote
SMS Provider



TAKEOVER-7

NTLM coercion and relay
to SMB between primary
and passive site servers



TAKEOVER-8

NTLM coercion and relay
HTTP to LDAP
on domain controller

SCCM Hierarchy Takeover Attack Paths



TAKEOVER-3

NTLM coercion and relay
to HTTP on ADCS

TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

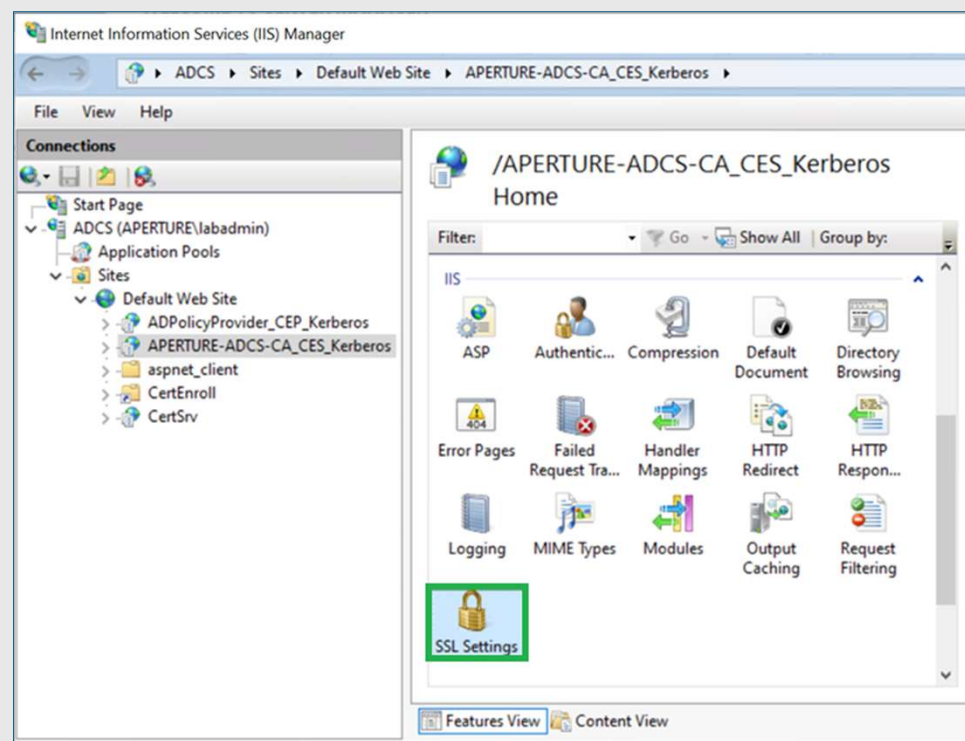
IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Require EPA on AD CS

PREVENT-14

On AD CS servers:

1. Open IIS Manager
2. Expand the connection, “Sites”, and “Default Web Site”
3. Click on “CertSrv” to configure the Certificate Authority Enrollment Service
4. Double-click “SSL Settings”



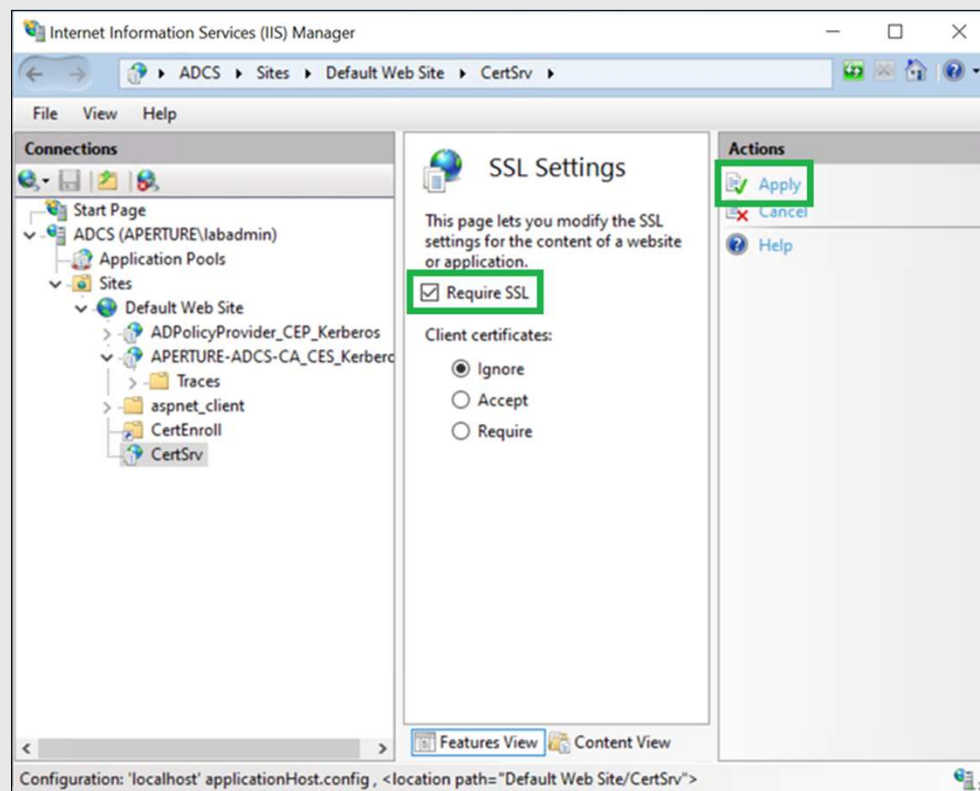
<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Require EPA on AD CS

PREVENT-14

5. Check the box next to “Require SSL”
6. Click “Apply”

If this setting is not applied,
relaying to HTTP instead of HTTPS
will bypass EPA

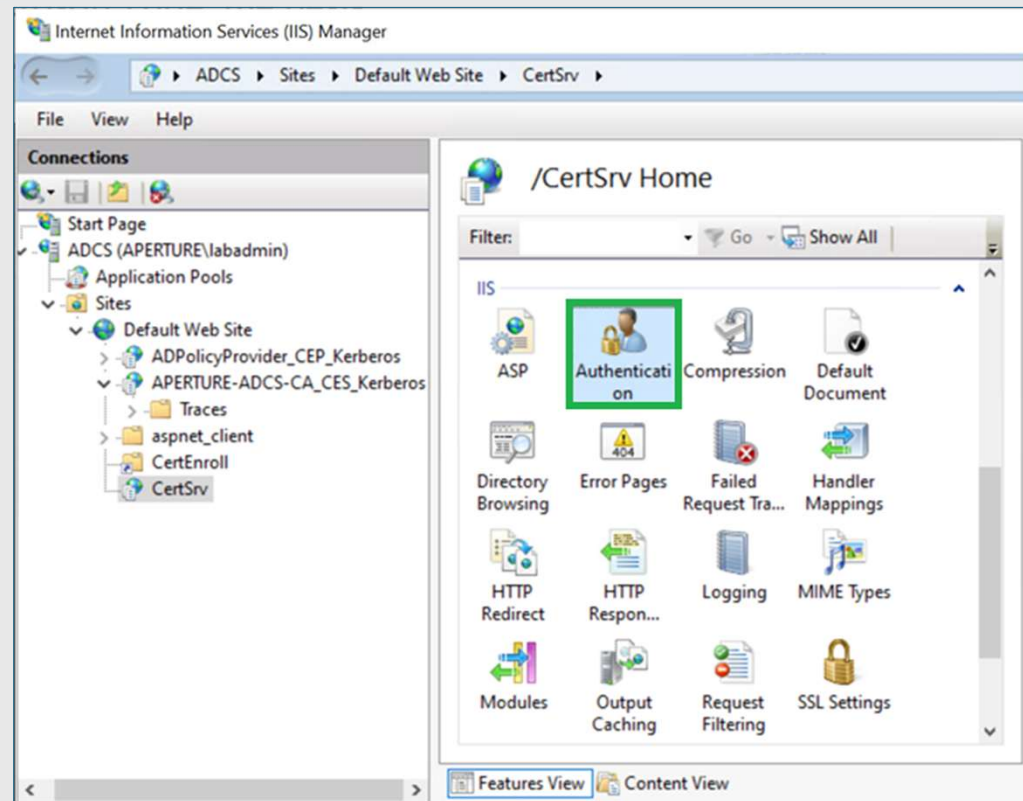


<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Require EPA on AD CS

PREVENT-14

7. Click on the “CertSrv” site again
8. Double-click “Authentication”



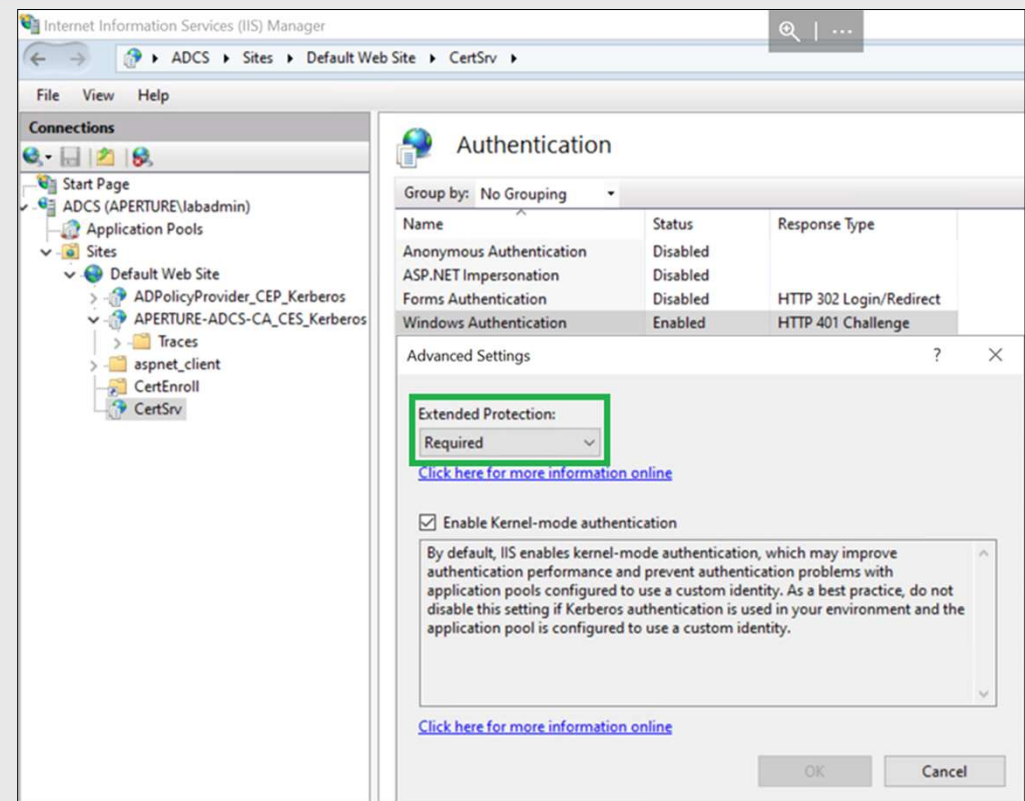
<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Require EPA on AD CS

PREVENT-14

9. Right click “Windows Authentication”
10. Click “Advanced Settings”
11. Set “Extended Protection” to “Required”
12. Click “OK”

Setting to “Accept” will not prevent NTLM relay attacks if the coerced client doesn’t support channel binding

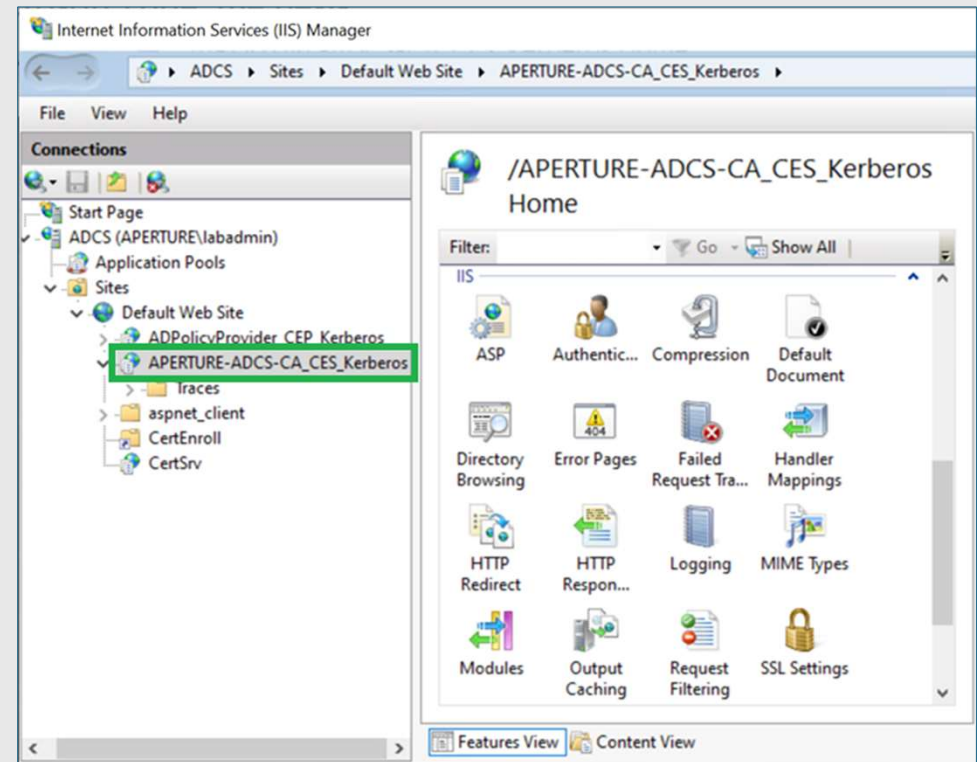


<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Require EPA on AD CS

PREVENT-14

13. Repeat steps 3-12 for the Certificate Enrollment Web Service (“APERTURE-ADCS-CA_CES_Kerberos” in the example)



<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Require EPA on AD CS

PREVENT-14

14. Append “<%windir%>\systemdata\CES\<CA>_CES_Kerberos\web.config”:

```
<binding name="TransportWithHeaderClientAuth">
  <security mode="Transport">
    <transport clientCredentialType="Windows">
      <extendedProtectionPolicy policyEnforcement="Always" />
    </transport>
    <message clientCredentialType="None" establishSecurityContext="false" negotiateServiceCredential="false" />
  </security>
  <readerQuotas maxStringLength="131072" />
</binding>
```

15. Restart the IIS service by issuing the “iisreset /restart” command

<https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

SCCM Hierarchy Takeover Attack Paths



TAKEOVER-1

NTLM coercion and relay to MSSQL on remote site database



TAKEOVER-2

NTLM coercion and relay to SMB on remote site database



TAKEOVER-3

NTLM coercion and relay to HTTP on ADCS



TAKEOVER-4

NTLM coercion and relay from CAS to origin primary site server



TAKEOVER-5

NTLM coercion and relay to AdminService on remote SMS Provider



TAKEOVER-6

NTLM coercion and relay to SMB on remote SMS Provider



TAKEOVER-7

NTLM coercion and relay to SMB between primary and passive site servers



TAKEOVER-8

NTLM coercion and relay HTTP to LDAP on domain controller

SCCM Hierarchy Takeover Attack Paths



TAKEOVER-8

NTLM coercion and relay
HTTP to LDAP
on domain controller

TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

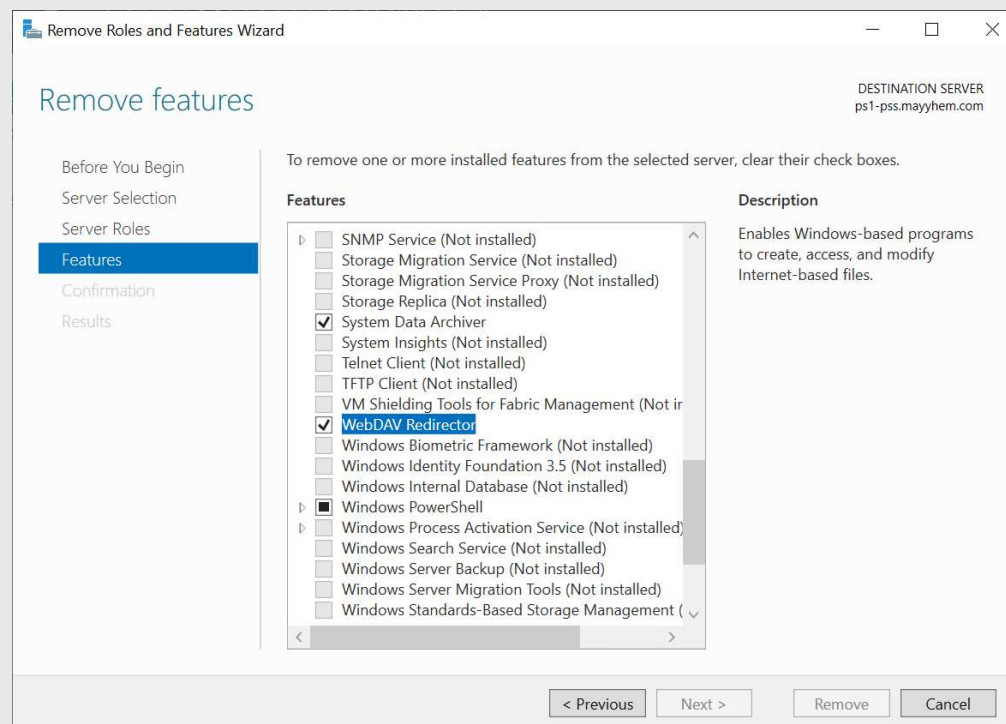
IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Disable and uninstall WebClient on site servers

PREVENT-11

On each primary site server, central administration site server, and passive site server:

1. Open Server Manager
2. Click “Add Roles and Features”
3. Click “Start the Remove Roles and Features Wizard”
4. Click “Next” until reaching “Remove features”
5. Uncheck “WebDAV Redirector”, then click “Next”
6. Check “Restart the destination server automatically if required” (or restart manually later), then click “Remove”



<https://www.redfoxsec.com/blog/an-in-depth-exploration-into-webclient-abuse>

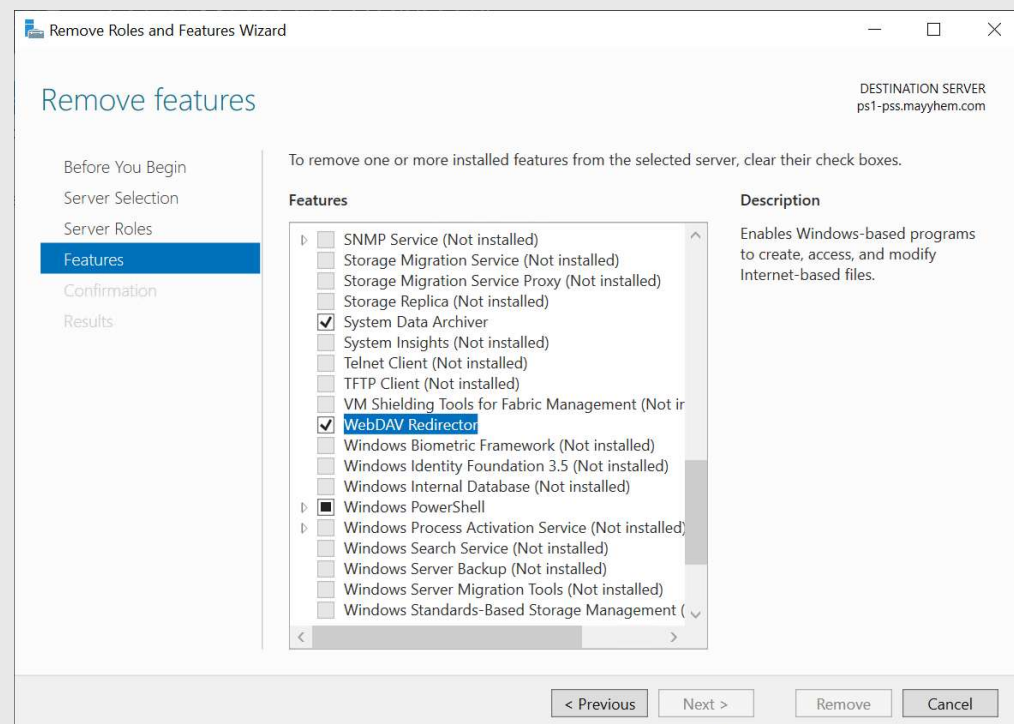
Disable and uninstall WebClient on site servers

PREVENT-11

Equivalent GPO: Computer Configuration > Windows Settings > Security Settings > System Services > WebClient > Startup Type: Disabled

PS> Uninstall-WindowsFeature -Name WebDAV-Redirector

If WebClient is installed but not running, it can potentially be triggered to start and be abused



<https://www.redfoxsec.com/blog/an-in-depth-exploration-into-webclient-abuse>

Require LDAP channel binding and signing

PREVENT-13

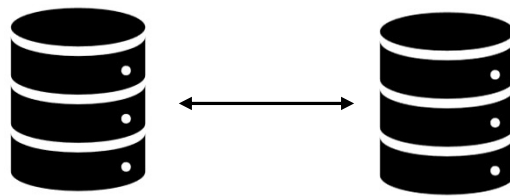
1. Configure Windows clients and domain controllers to negotiate channel binding **and** signing via GPO **when supported**
2. **Monitor events** to identify clients that may not comply with signing or channel binding requirements
3. **After handling outliers**, require LDAP channel binding **and** signing

If only channel binding is required, relay to LDAP with StartTLS is possible because TLS is established after NTLM authentication is complete

If only signing is required, relay to LDAPS is possible (pre-Windows Server 2025) because TLS traffic is signed

<https://www.hub.trimarcsecurity.com/post/ldap-channel-binding-and-signing>

SCCM Hierarchy Takeover Attack Paths



TAKEOVER-9

Ride MSSQL links configured
with DBA privileges

TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Remove unnecessary links to site databases

PREVENT-19

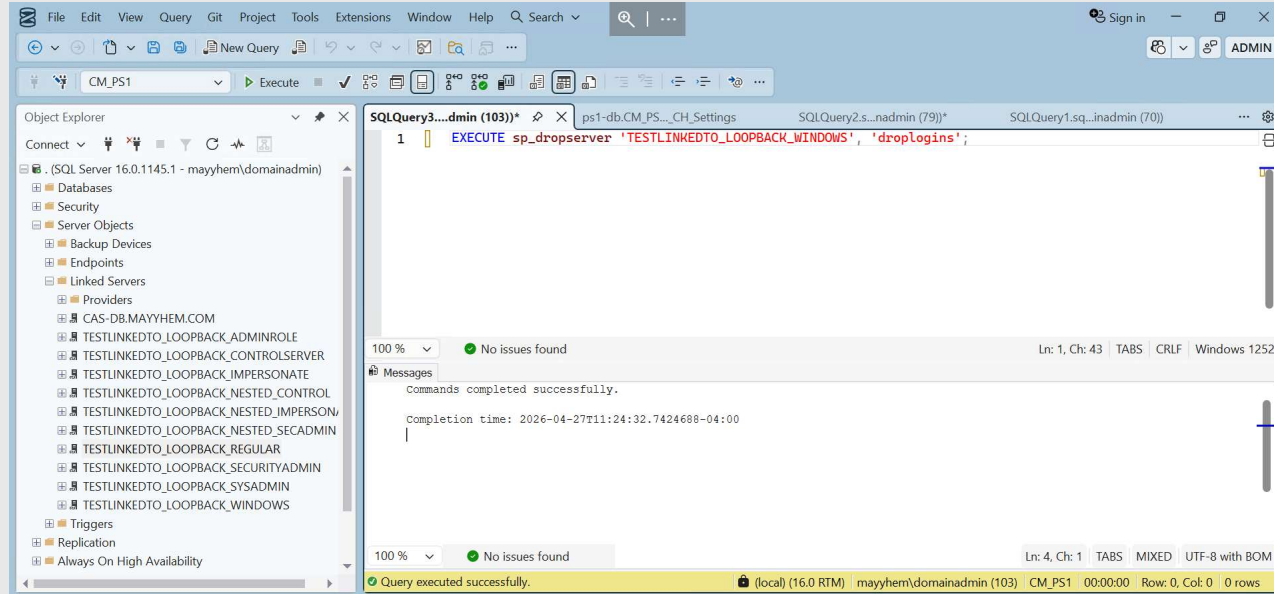
- Unfortunately, this is much easier said than done
- You can't see what servers are linked TO a site database server with SQL queries run on the site database server
- You can **monitor login events and client connections**, but these still may return false negatives for linked servers that rarely connect to the site database
- Another option is to **collect links from ALL other SQL servers**, which we'll cover in a few slides

<https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-dropserver-transact-sql?view=sql-server-ver17>

Remove unnecessary links to site databases

PREVENT-19

1. Open SQL Server Management Studio
2. Connect to databases with connectivity to the site database
3. View any configured links in “Server Objects” > “Linked Servers”
4. Click “New Query”
5. Run “EXECUTE sp_dropserver ‘<name>’, ‘droplogins’”



<https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-dropserver-transact-sql?view=sql-server-ver17>

Kerberoasting

- By design, **attackers can request Kerberos service tickets** for accounts with Service Principal Names (SPNs)
 - e.g., site database service account
- If configured **with a weak password**, these service tickets can be **cracked** (via password guessing until a match is found) to obtain the cleartext password for the domain service account
- The password for this account can be used to get service tickets for any user of any service running as that account
 - e.g., **impersonate the site server** or another DBA to the site database

TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

TAKEOVER/ELEVATE Prevention

Technique	Codename
Require EPA on site databases	PREVENT-14
Require SMB signing on site systems	PREVENT-12
Patch site server with KB15599094	PREVENT-1
Disable NTLM fallback for client push installation	PREVENT-2
Disable automatic site-wide client push installation	PREVENT-5
Upgrade to v2509 to prevent relay to AdminService	Noted in TAKEOVER-5
Require EPA on AD CS servers	PREVENT-14
Disable and uninstall WebClient on site servers	PREVENT-11
Require LDAP channel binding and signing	PREVENT-13
Remove unnecessary links to site databases	PREVENT-19
Set a strong MSSQL service account password	Prevents Kerberoasting
Block unnecessary connections to site systems	PREVENT-20

IMPORTANT: Implementing these settings may impact connectivity and/or performance, so it is crucial to first audit and test these changes in your environment before implementing in production.

Block unnecessary connections to site systems

PREVENT-20

Site servers (including primary site, central administration site, and passive site servers):

- TCP/445 (SMB) - inbound **and outbound**

Site database servers:

- TCP/445 (SMB) - inbound
- TCP/1433 (MSSQL) - inbound

<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/ports>

Block unnecessary connections to site systems

PREVENT-20

There is no support for relay protection on the SMS Provider AdminService!

Pre-v2509, it is imperative to restrict the following ports on remote SMS Providers:

- TCP/443 (HTTPS) - inbound
- TCP/445 (SMB/WMI) – inbound

Not applicable to standalone primary site servers with the **only** SMS Provider

If necessary, move SMS Providers to a system without client-facing roles

Restricting connections to TCP/443 and TCP/445 isn't feasible when the server also hosts client-facing roles (e.g., management point, distribution point), so these ports are often open

<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/ports>

CRED Attacks



Machine Policy Secrets

Downloaded from Management Points

- Network Access Accounts (NAA)
 - Domain accounts used by systems that are not joined to AD to download content from software distribution points
- Task Sequences
 - Step-by-step instructions executed by clients, often for operating system deployment or complicated software installations/setup
- Collection Variables
 - Environment variables defined for a device collection to access

<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts>



Machine Policy Secrets

Downloaded from Management Points

- May contain obfuscated **domain join** credentials, **local admin** credentials, **RunAs credentials**
 - Can be **requested from a management point** and deobfuscated by **approved** devices
 - Attackers can create a domain computer account as any domain user, use it to registering a fake device with a self-signed cert, and SCCM will auto-approve it, after which the attacker can request policy for it
- OR
- Attackers can reuse an existing client device's certificate to request policy (requires admin)

<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts>



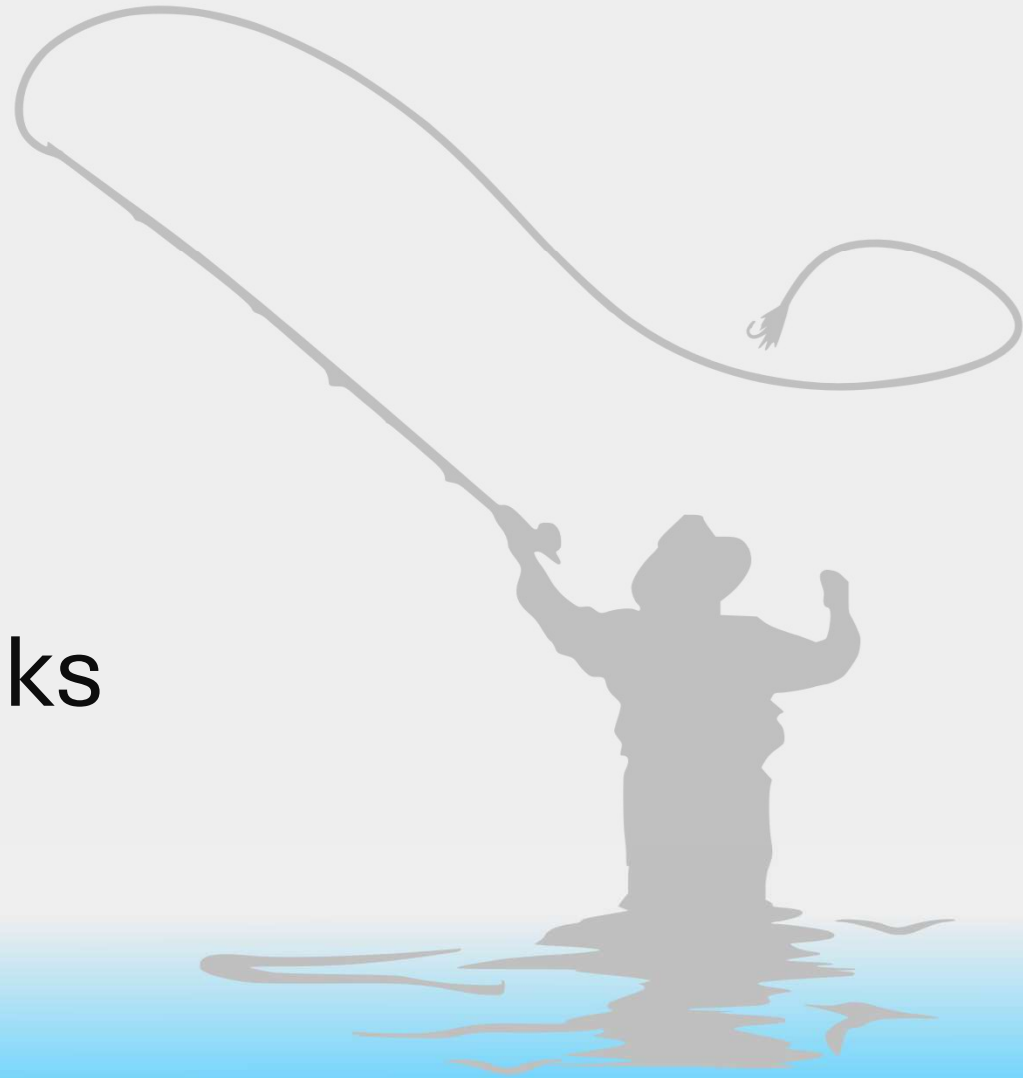
Machine Policy Secrets

On Client Devices

- Credentials are stored on clients as DPAPI blobs protected by the system's masterkey
- Retrievable via WMI as a privileged user
- Remain in CIM repository after client is uninstalled or account rotation
 - C:\Windows\System32\Wbem\Repository\OBJECTS.DATA

DEMO

CRED Attacks

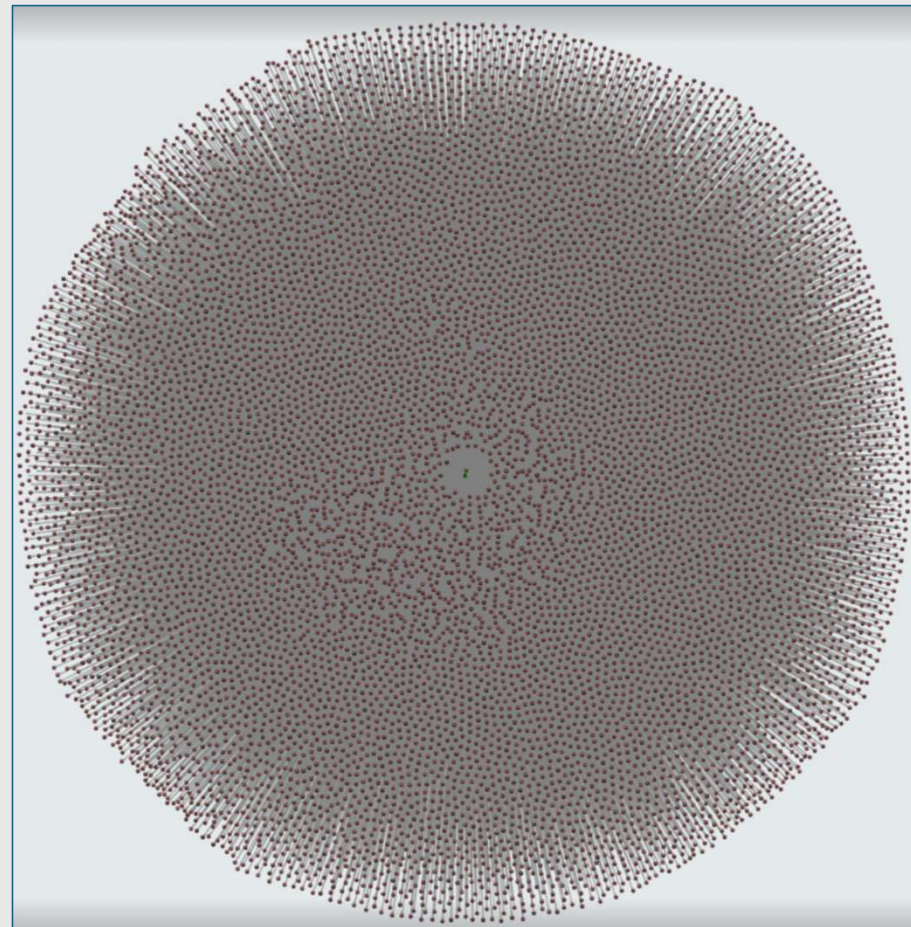


Real World Examples

Overprivileged Policy Secrets

- Domain join account in PXE boot task sequence Owns all computers in the domain
- Remember to change ownership and remove rights assignments from accounts that do not require them
 - dsHeuristics 29th bit blocks implicit owner rights for computer objects

Creds in PXE boot task sequences can be retrieved remotely if there is no PXE password or a weak one



CRED Prevention

Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 + PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

*Configuring PKI certificates for client authentication (PREVENT-8) would be ideal but involves a lot of overhead compared to EHTTP

**If you must have an NAA, disable interactive logon and restrict to read-only access to distribution point network shares

CRED Prevention

Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 + PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

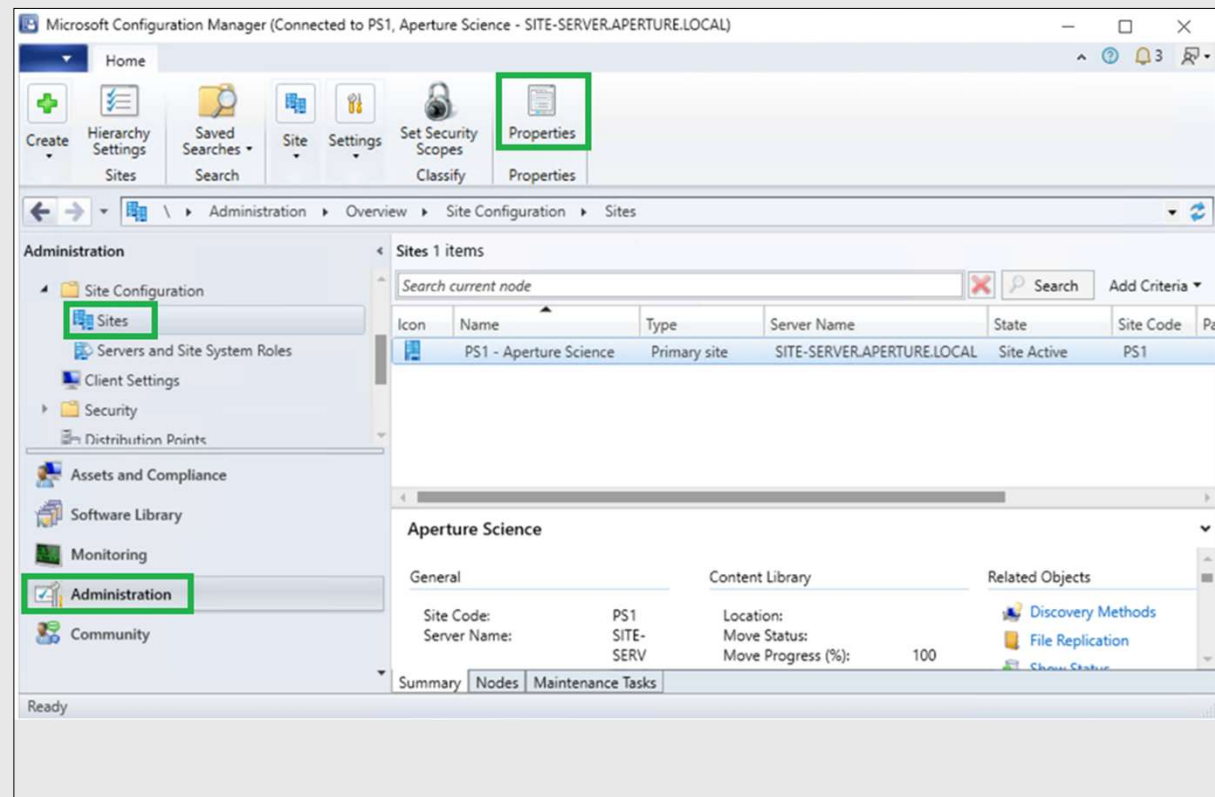
***Configuring PKI certificates for client authentication (PREVENT-8)
would be ideal but involves a lot of overhead compared to EHTTP**

****If you must have an NAA, disable interactive logon and restrict to
read-only access to distribution point network shares**

Configure Enhanced HTTP

PREVENT-4

1. Open the Configuration Manager Console
2. Navigate to Administration > Site Configuration > Sites, then click the site
3. Click “Properties”



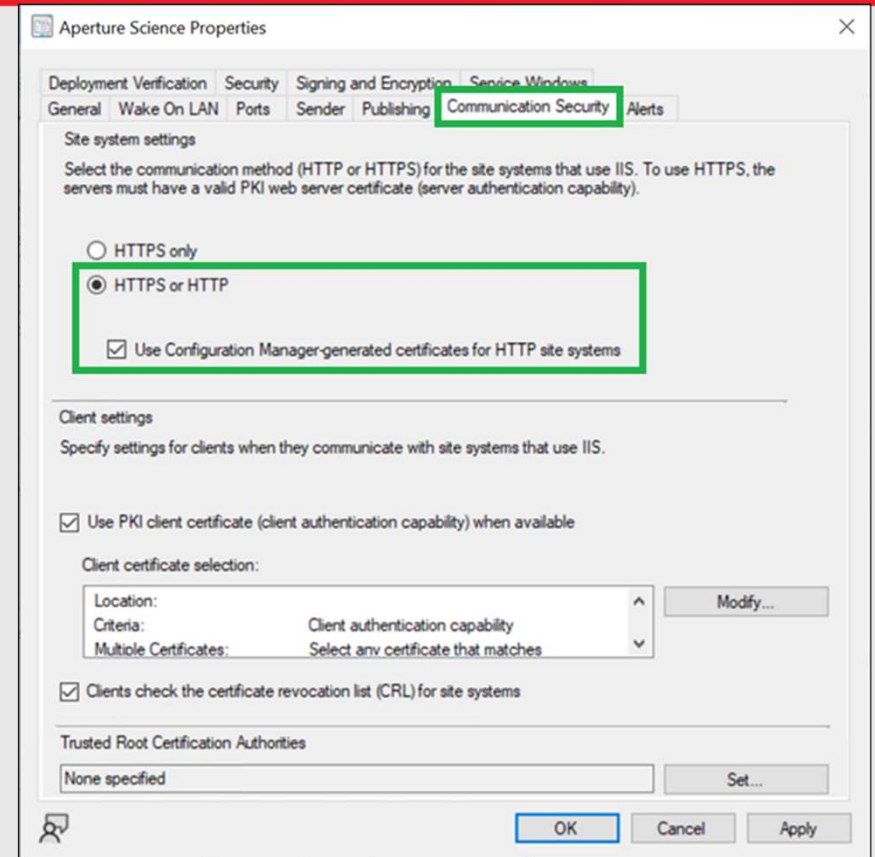
<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/enhanced-http>

Configure Enhanced HTTP

PREVENT-4

4. Click the “Communication Security” tab
5. Select “HTTPS or (E)HTTP”
6. Check the box next to “Use Configuration Manager-generated certificates for HTTP site systems”
7. Click “Apply”, then “OK”

Enhanced HTTP does not prevent registration of fake device records to download machine policy secrets or coerce automatic client push



<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/enhanced-http>

CRED Prevention

Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 + PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

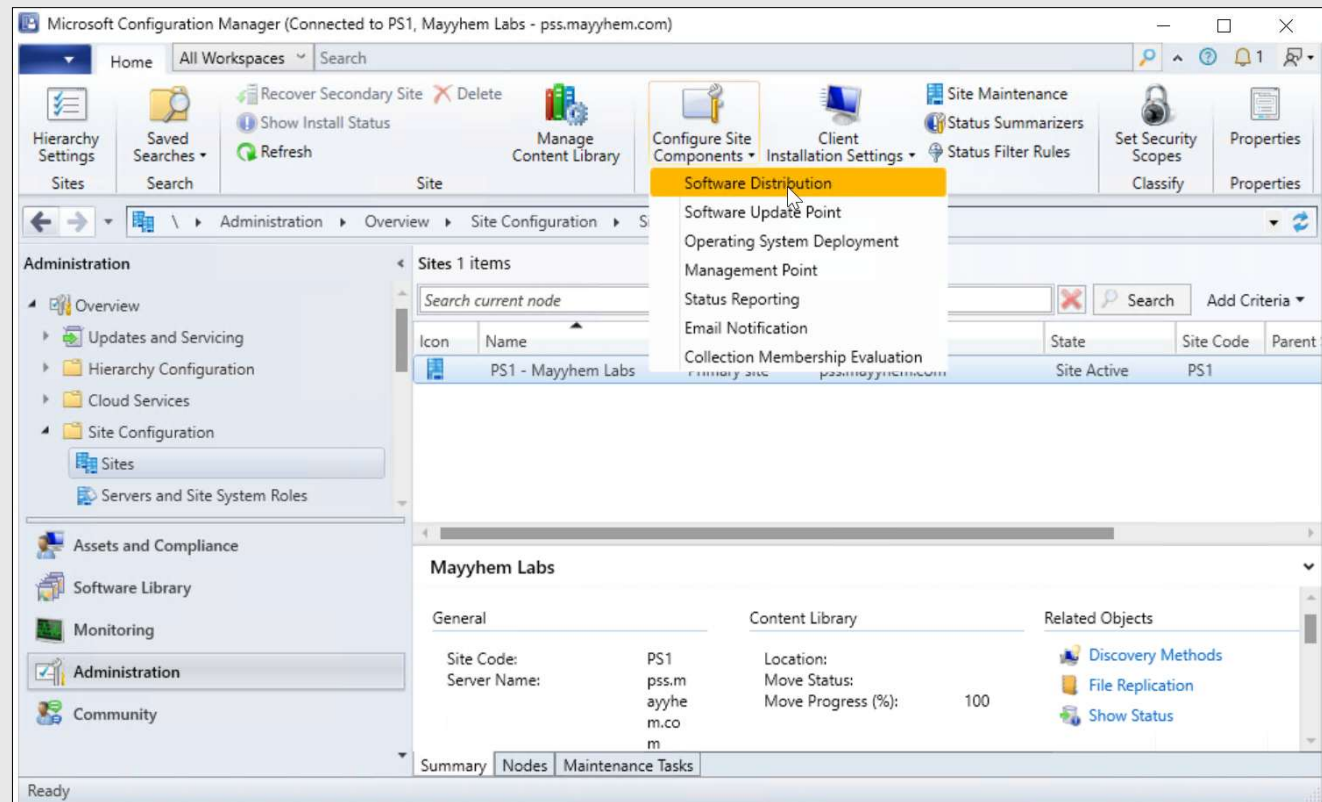
*Configuring PKI certificates for client authentication (PREVENT-8) would be ideal but involves a lot of overhead compared to EHTTP

**If you must have an NAA, disable interactive logon and restrict to read-only access to distribution point network shares

Disable Network Access Accounts

PREVENT-3

1. Open the Configuration Manager Console
2. Navigate to Administration > Site Configuration > Sites, then click the site
3. Click “Configure Site Components”, then “Software Distribution”

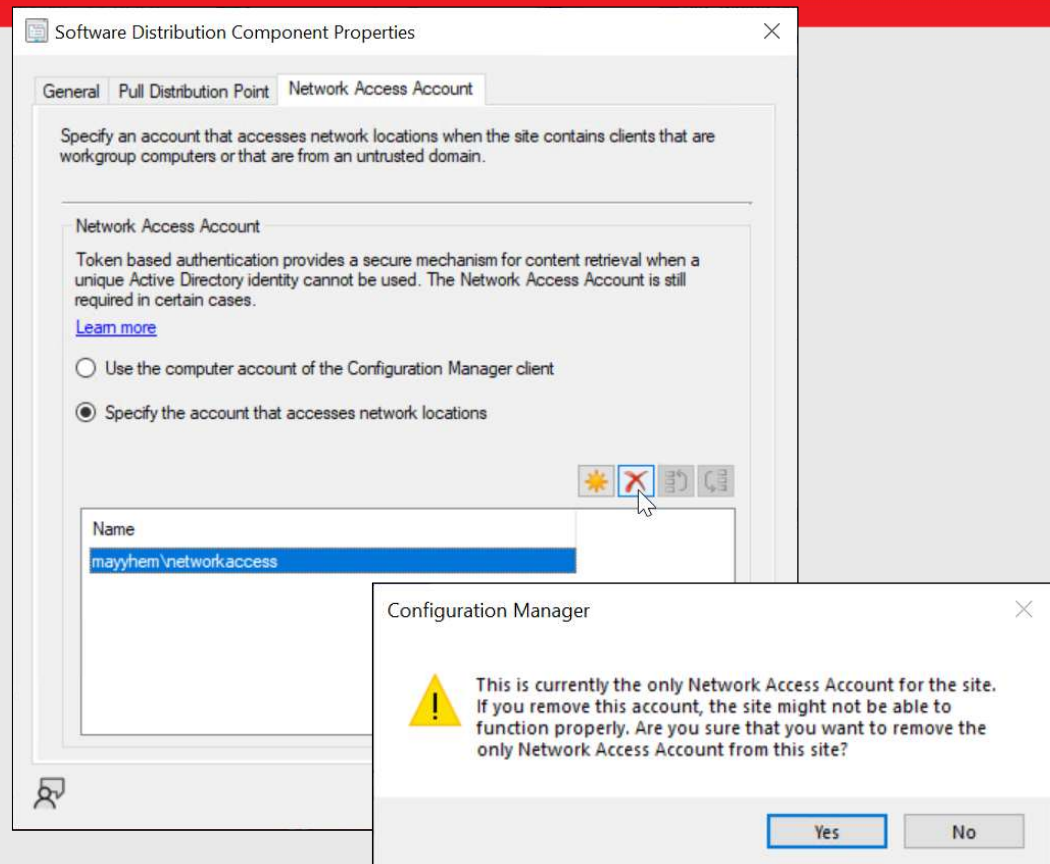


<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>

Disable Network Access Accounts

PREVENT-3

4. Click the “Network Access Account” tab
5. Select each account and click the big red X
6. When prompted to delete the only NAA, say “Yes”
7. Click “Apply”, then “OK”

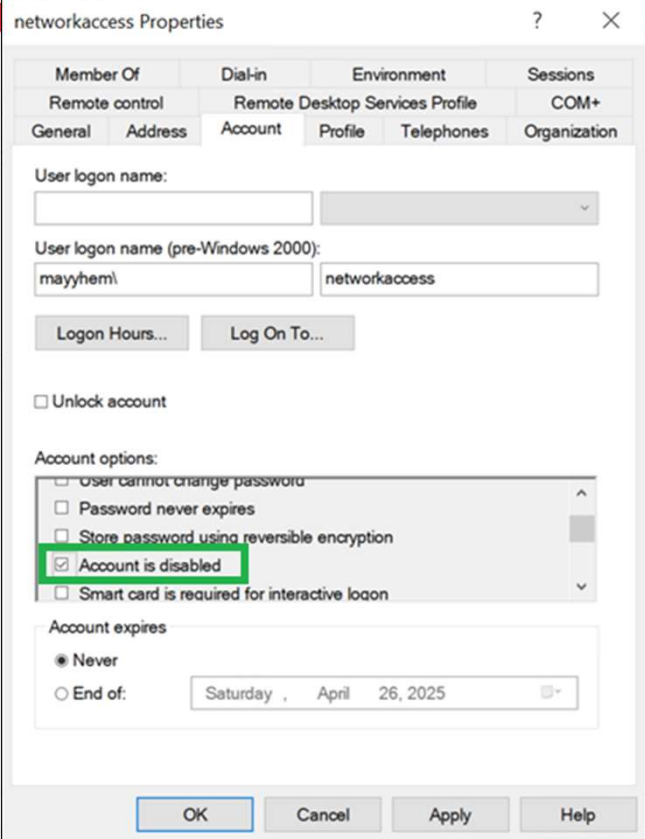


<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>

Disable Network Access Accounts

PREVENT-15

8. Open Active Directory Users and Computers
9. Open the “Properties” window for each NAA
10. Click the “Account” tab, check the box next to “Account is disabled”
11. Click “Apply”, then “OK”
12. Rejoice

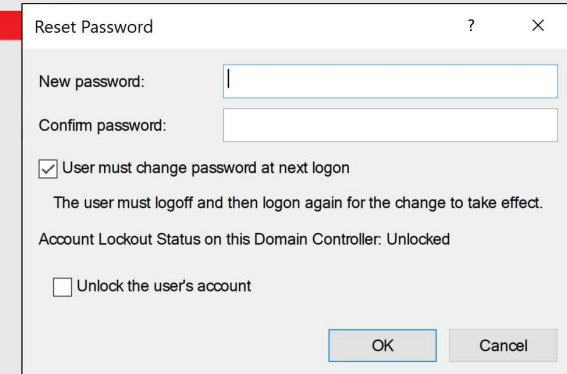


The screenshot shows the 'networkaccess Properties' dialog box with the 'Account' tab selected. The 'User login name' field is empty, and the 'User login name (pre-Windows 2000)' field contains 'mayyhem\'. The 'Logon Hours...' and 'Log On To...' buttons are visible. The 'Unlock account' checkbox is unchecked. Under 'Account options', the 'Account is disabled' checkbox is checked and highlighted with a green box. Other options include 'User cannot change password', 'Password never expires', 'Store password using reversible encryption', and 'Smart card is required for interactive logon'. The 'Account expires' section shows 'Never' selected. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Disable Network Access Accounts

PREVENT-15

- Alternatively, rotate the password after removing the NAA from SCCM by selecting “Reset Password” in ADUC **and revoke any issued certificates in Certification Authority.**
- If the NAA is removed from SCCM but not disabled or the password rotated, the WMI repository on client devices will still contain valid credentials.
- If those credentials were at any point used to request a certificate that is still valid, that certificate can still be used for authentication and to get the account’s TGT and NT hash **even after the password has been rotated.**



Reset Password

New password:

Confirm password:

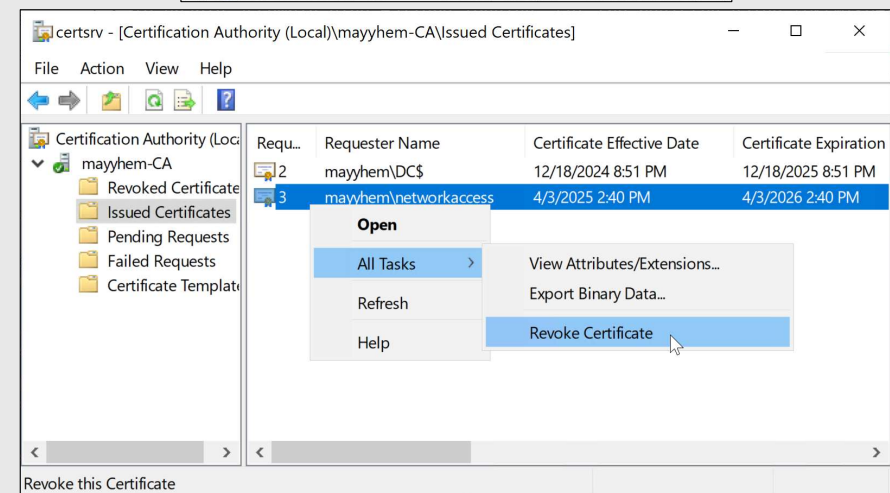
☒ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

☐ Unlock the user's account

OK Cancel



CRED Prevention

Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 + PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

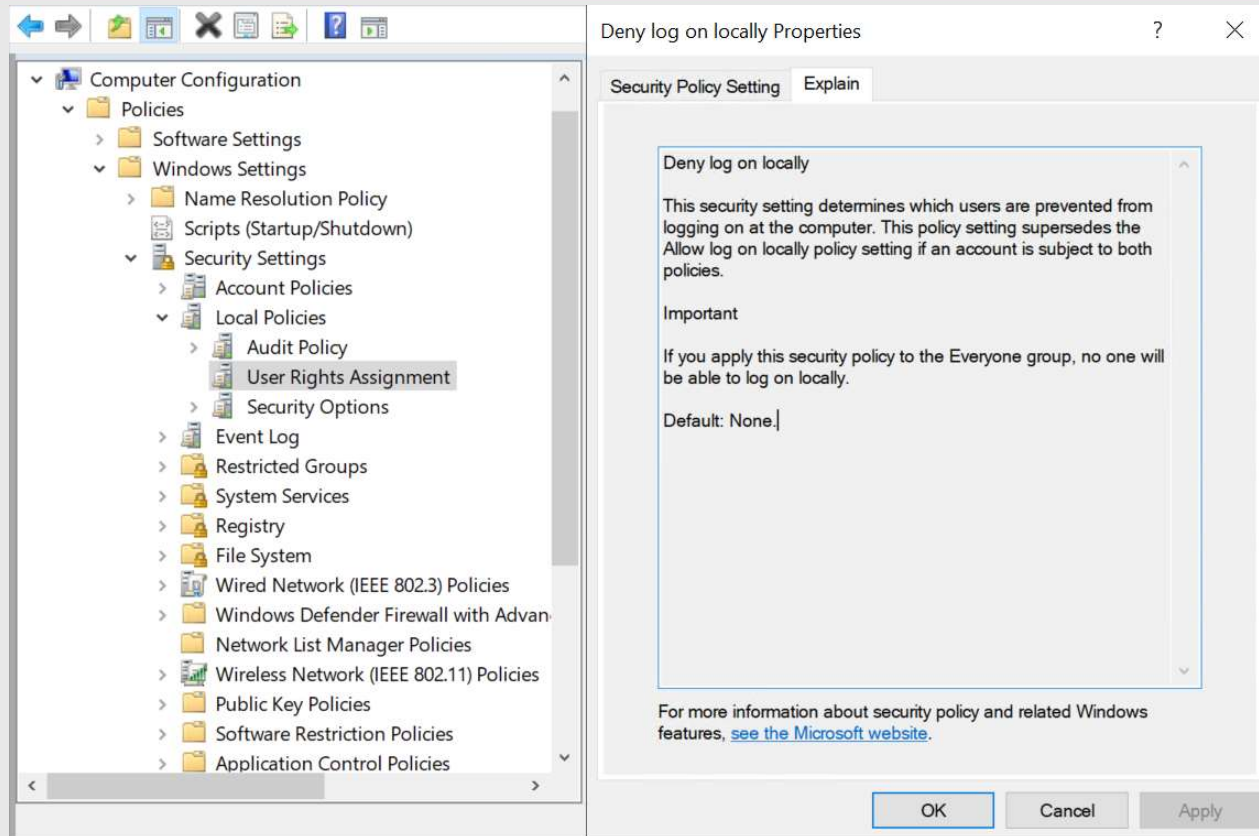
*Configuring PKI certificates for client authentication (PREVENT-8) would be ideal but involves a lot of overhead compared to EHTTP

****If you must have an NAA, disable interactive logon and restrict to read-only access to distribution point network shares**

Enforce the principle of least privilege for accounts

PREVENT-10

- GPOs:
 - Deny log on locally
 - Deny log on through Remote Desktop Services



<https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/accounts#actions-that-require-the-network-access-account>

CRED Prevention

Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 + PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

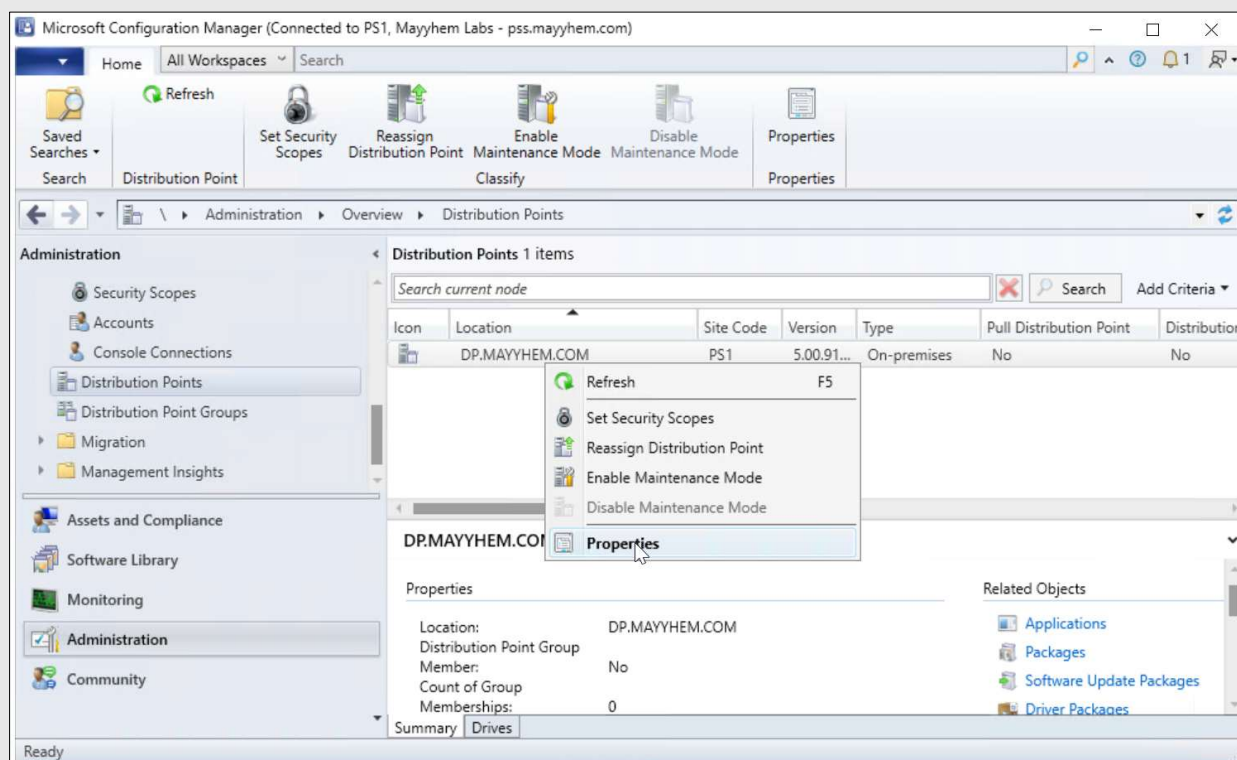
*Configuring PKI certificates for client authentication (PREVENT-8) would be ideal but involves a lot of overhead compared to EHTTP

**If you must have an NAA, disable interactive logon and restrict to read-only access to distribution point network shares

Configure a strong PXE boot password

PREVENT-6

1. Open the Configuration Manager Console
2. Navigate to Administration > Distribution Points
3. Right click on each distribution point and select “Properties”



https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences

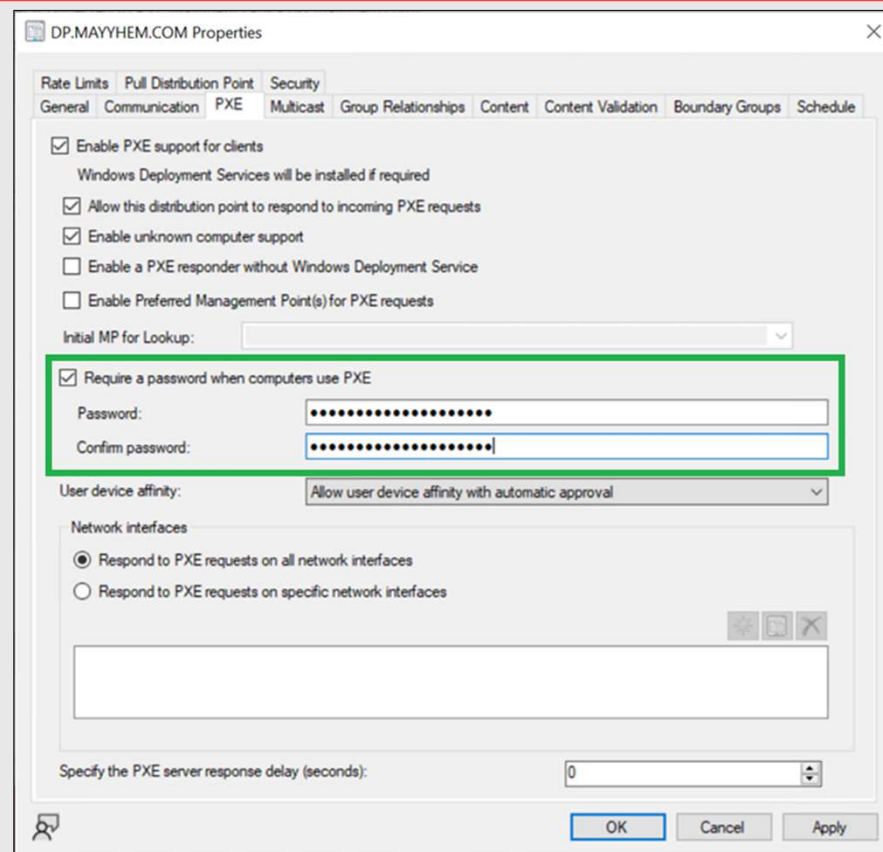
Configure a strong PXE boot password

PREVENT-6

4. Click on the “PXE” tab
5. Check the box next to “Require a password when computers use PXE”
6. Enter a strong passphrase
7. Click “Apply”, then “OK”

If an **uncrackable** password is not set, task sequences that may contain creds (and the distribution point's cert, if using PKI) can still be dumped remotely

Restrict PXE to specific VLANs if possible!



The screenshot shows the 'DP.MAYYHEM.COM Properties' dialog box with the 'PXE' tab selected. The 'Require a password when computers use PXE' checkbox is checked and highlighted with a green box. Below it, the 'Password' and 'Confirm password' fields are filled with masked characters. The 'Initial MP for Lookup' dropdown is set to 'Allow user device affinity with automatic approval'. The 'Network interfaces' section shows 'Respond to PXE requests on all network interfaces' selected. The 'Specify the PXE server response delay (seconds)' field is set to 0. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

DP.MAYYHEM.COM Properties

Rate Limits | Pull Distribution Point | Security | General | Communication | PXE | Multicast | Group Relationships | Content | Content Validation | Boundary Groups | Schedule

☒ Enable PXE support for clients
Windows Deployment Services will be installed if required

☒ Allow this distribution point to respond to incoming PXE requests

☒ Enable unknown computer support

☐ Enable a PXE responder without Windows Deployment Service

☐ Enable Preferred Management Point(s) for PXE requests

Initial MP for Lookup: [Dropdown]

☒ Require a password when computers use PXE

Password: [Masked]

Confirm password: [Masked]

User device affinity: [Dropdown: Allow user device affinity with automatic approval]

Network interfaces

☒ Respond to PXE requests on all network interfaces

☐ Respond to PXE requests on specific network interfaces

[List of network interfaces]

Specify the PXE server response delay (seconds): [0]

OK Cancel Apply

CRED Prevention

Protect Secrets Stored in Machine Policies

Technique	Codename
*Configure Enhanced HTTP	PREVENT-4
Disable network access accounts	PREVENT-3 + PREVENT-15
**Enforce the principle of least privilege for accounts	PREVENT-10
Configure a strong PXE boot password	PREVENT-6
Restrict permissions to join machines to AD	PREVENT-16

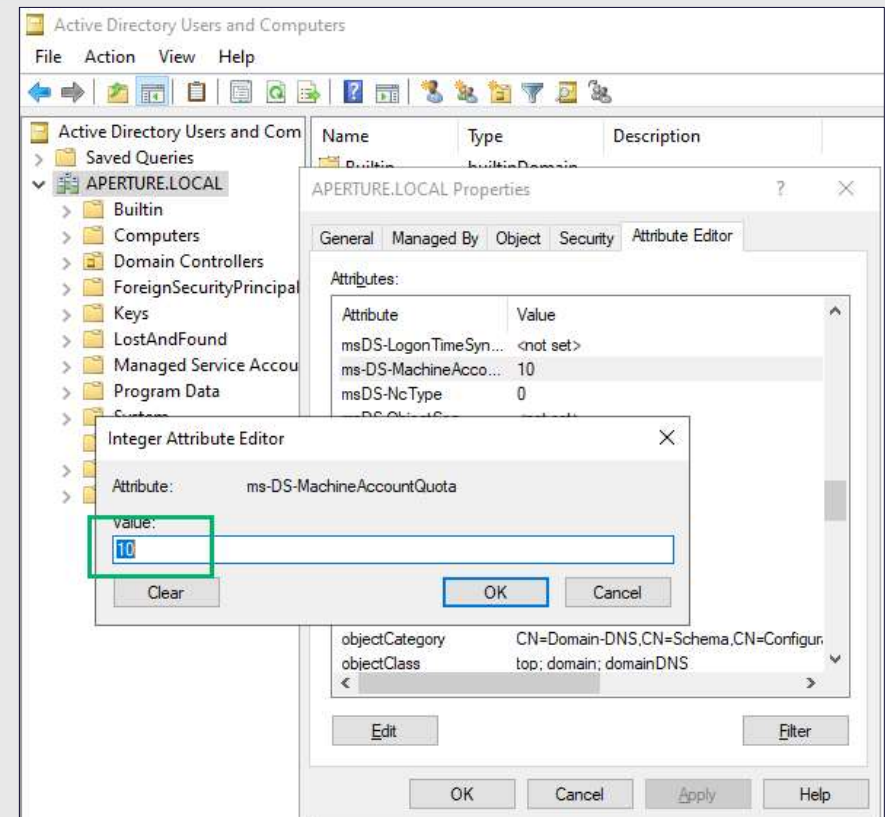
*Configuring PKI certificates for client authentication (PREVENT-8) would be ideal but involves a lot of overhead compared to EHTTP

**If you must have an NAA, disable interactive logon and restrict to read-only access to distribution point network shares

Restrict permission to join machines to AD

PREVENT-16

1. Open ADUC on a DC
2. Right click the domain object and select "Properties"
3. Select the "Attribute Editor" tab
4. Find the "ms-DS-MachineAccountQuota" attribute
5. Set the attribute to 0



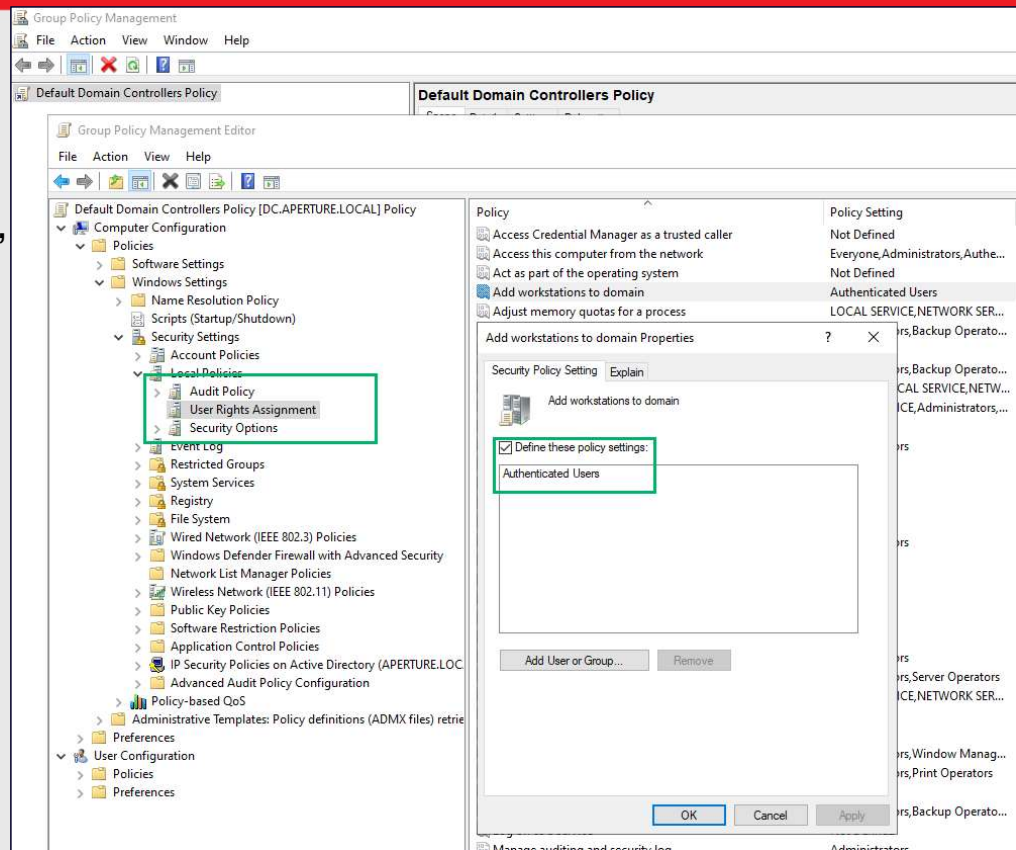
<https://learn.microsoft.com/en-us/windows/win32/adschema/a-ms-ds-machineaccountquota>

Restrict permission to join machines to AD

PREVENT-16

1. Open Group Policy Management
2. Right click "Default Domain Controllers Policy" and select "Edit"
3. Navigate to "User Rights Assignment"
4. Right click "Add workstations to domain" and select "Edit"
5. Remove "Authenticated Users", then click "Apply" and "OK"

Attackers can still impersonate a client device to fetch secret policies from a management point with local admin on any domain-joined computer



<https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/add-workstations-to-domain>

CANARY Techniques

Tripwires for attackers to stumble over

- NAA
- task sequence
- collection variable
- WIM file on DP
- Script on DP

Automating issue discovery



BloodHound



BloodHound

- Attack path management for:
 - Active Directory
 - Entra ID

Free and open-source!

<https://bloodhound.specterops.io>



BloodHound

- Depicts control relationships (**edges**) between identities (**nodes**)
- Identifies long-forgotten, unintended chains of **permissions** and **abuses** that allow control of critical infrastructure

<https://bloodhound.specterops.io>



Best

42 hr

3 days

1,015 hr

11 days

San Diego, California

Manhattan, New York, NY

Add destination

Options

Send directions to your phone

Copy link

via US-54 W

1,015 hr

This route includes a ferry.

2,787 miles

This route crosses through Mexico.

This route has restricted usage or private roads.

Your destination is in a different time zone.

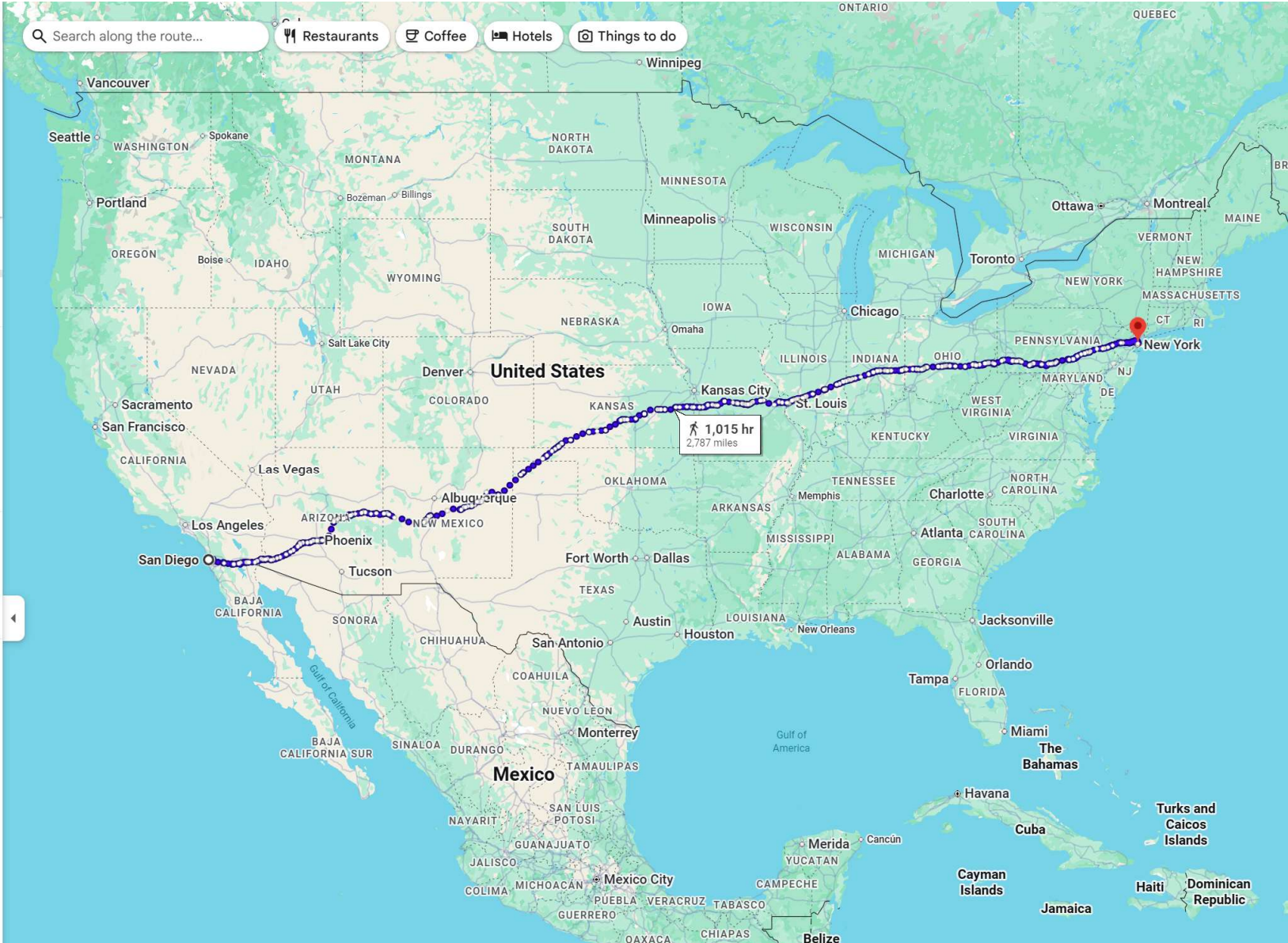
Details

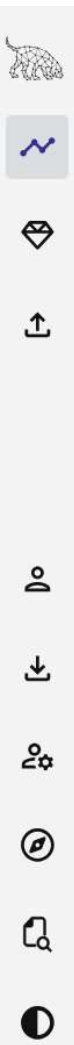
Preview

↑ 70,121 ft · ↓ 70,089 ft

8,153 ft

-3 ft





— 🔍 SEARCH [PATHFINDING](#) </> CYPHER

●

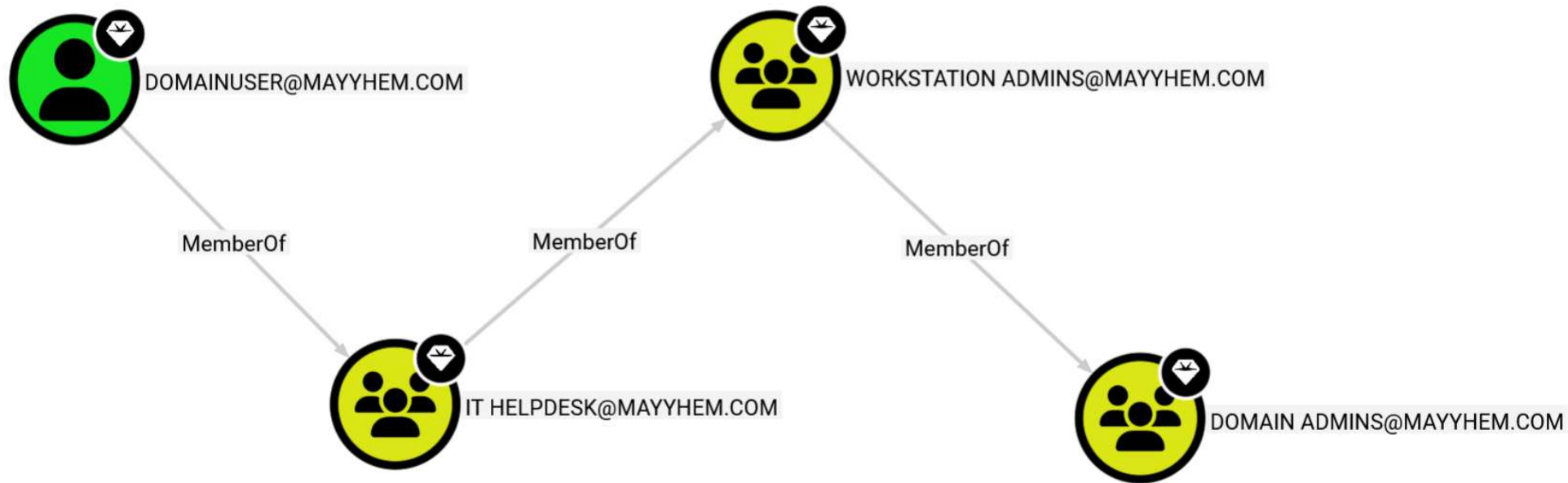
DOMAINUSER@MAYYHEM.COM

⦿

DOMAIN ADMINS@MAYYHEM.COM

↕

⏏



None Selected



Select a node to view the associated information

Hide Labels Layout Export Search



BloodHound OpenGraph

- Allows anyone to extend the graph to additional technologies
- Add your own identities (**nodes**) and relationships (**edges**)

<https://bloodhound.specterops.io/opengraph/library>



BloodHound OpenGraph

- Attack path management for:
 - Active Directory
 - Entra ID
 - **All the things!**

Free and open-source!

<https://bloodhound.specterops.io>



OpenGraph Library

▼  1Password

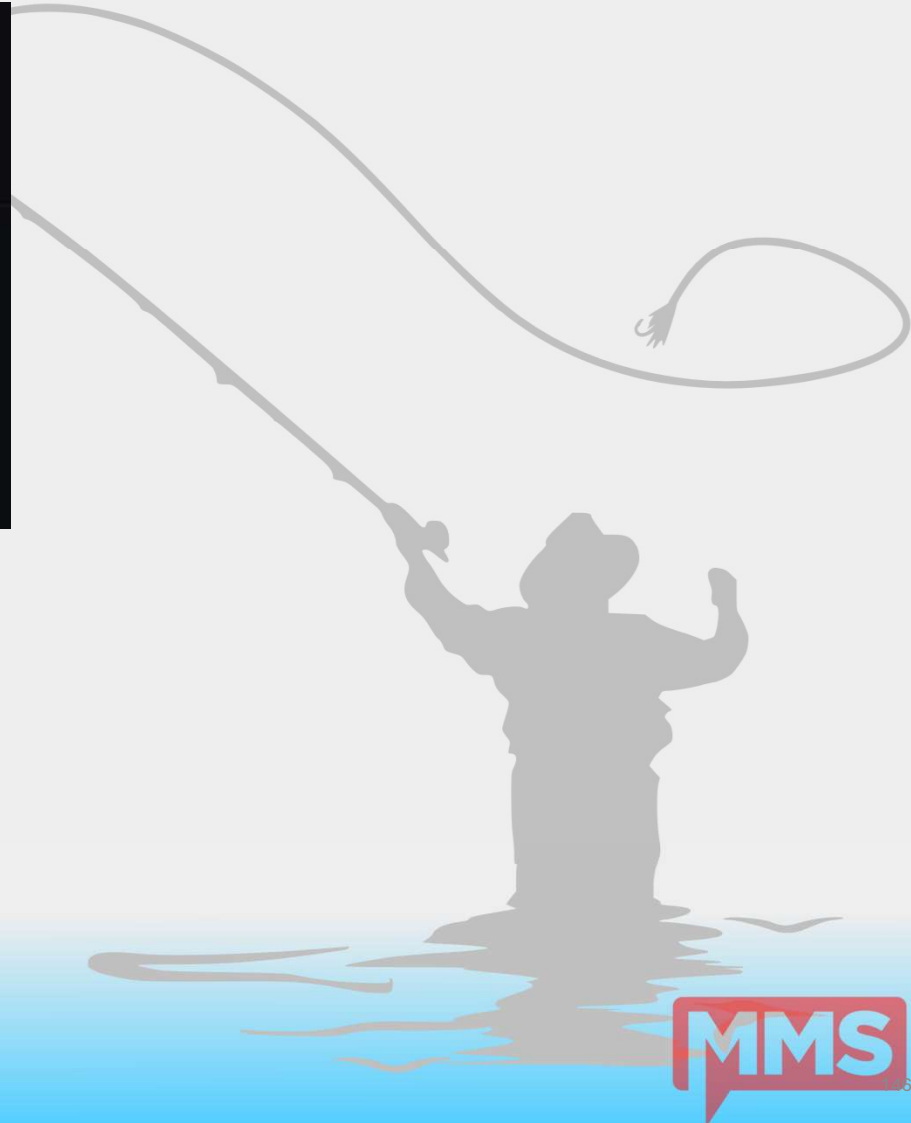
 **1PassHound**

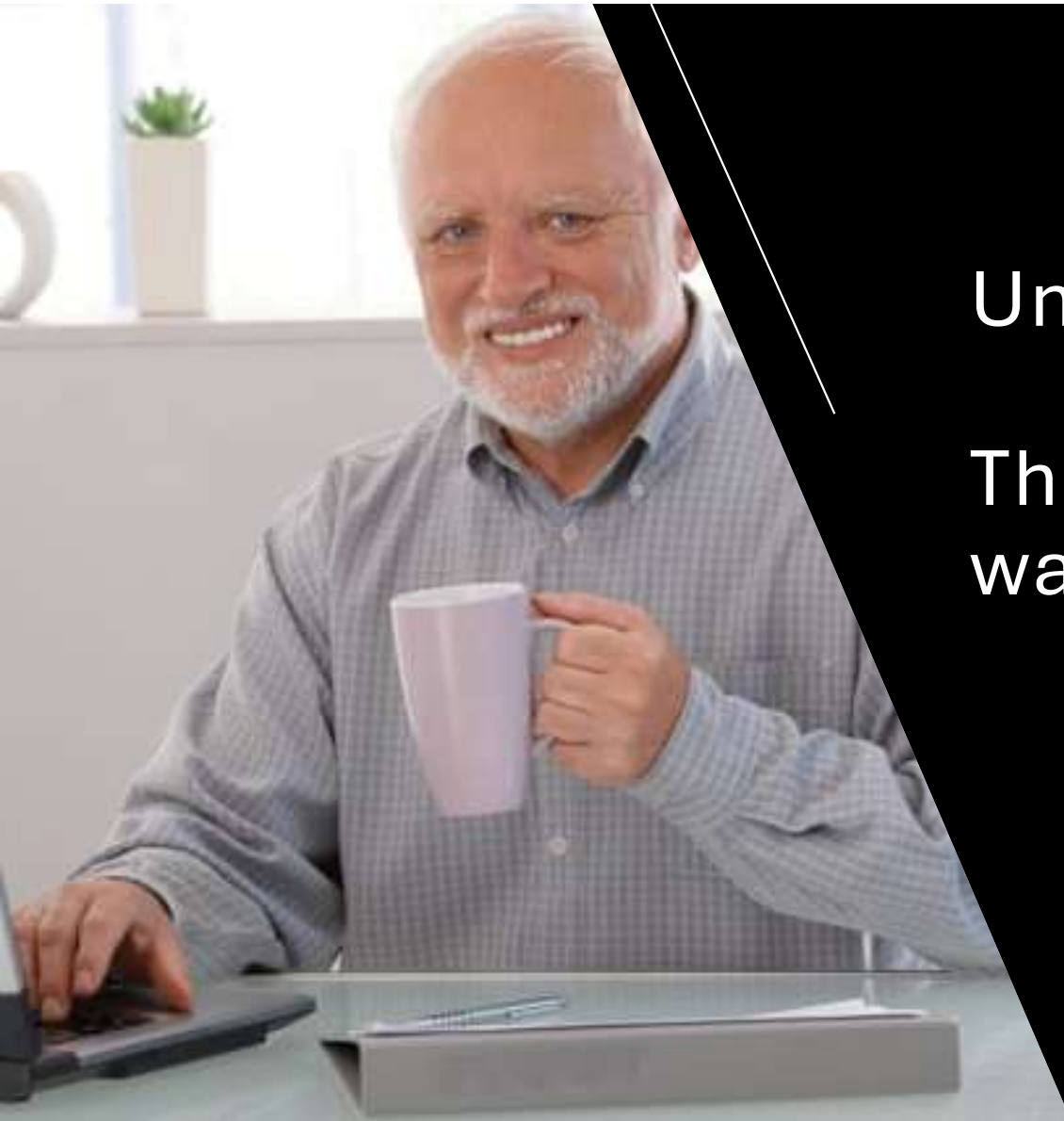
▼  Ansible

 **AnsibleHound**

▼  Active Directory (AD)

 **ADAttributeHound**





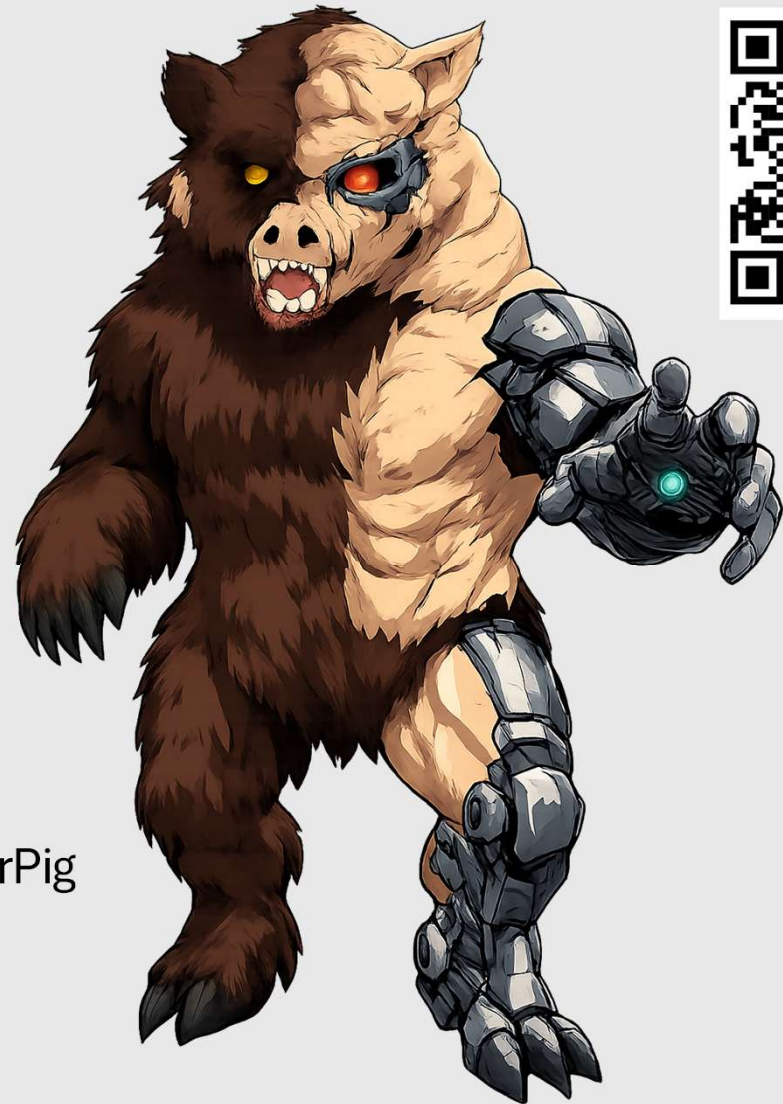
Unfortunately...

The name SCCMHound
was already taken

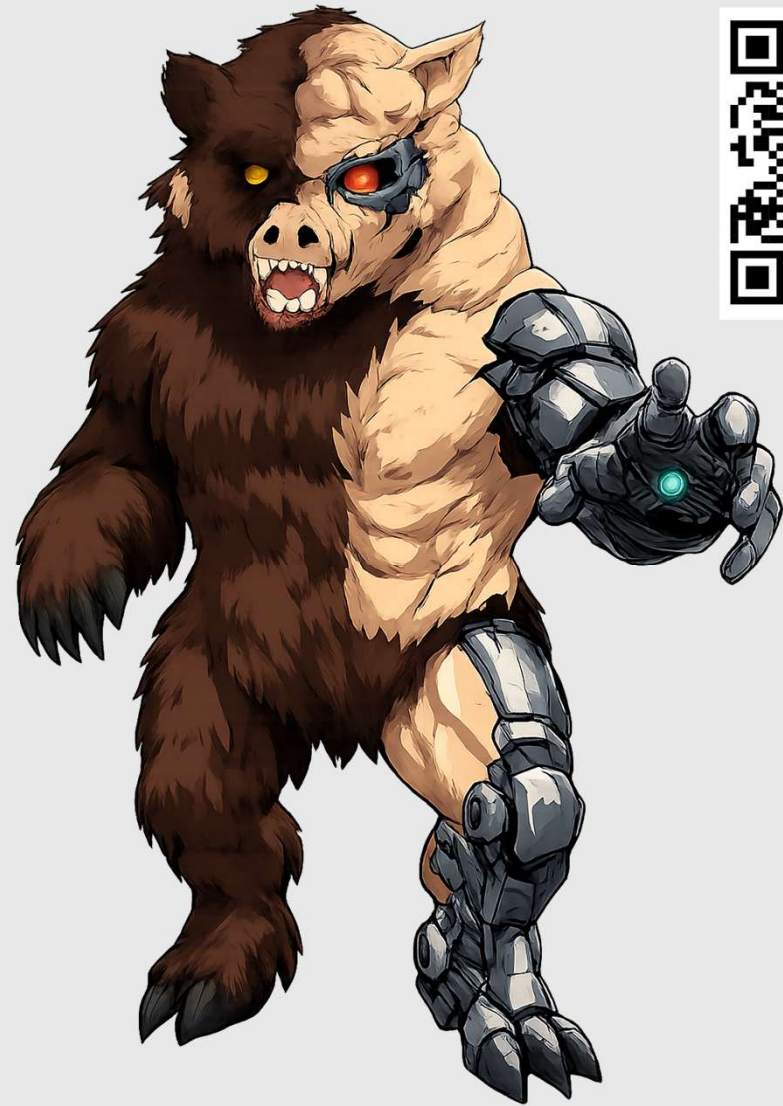
ConfigManBearPig

- A PowerShell (Python coming soon) OpenGraph collector for SCCM
- 5 new nodes
- 20 new edges
- 13 existing edges
- Does NOT require privileged access, just a domain user

<https://github.com/Mayyhem/ConfigManBearPig>



RECON: 6/7
CRED: 3/8
COERCE: 0/2
ELEVATE: 1/5
TAKEOVER: 8/9
EXEC: 2/2

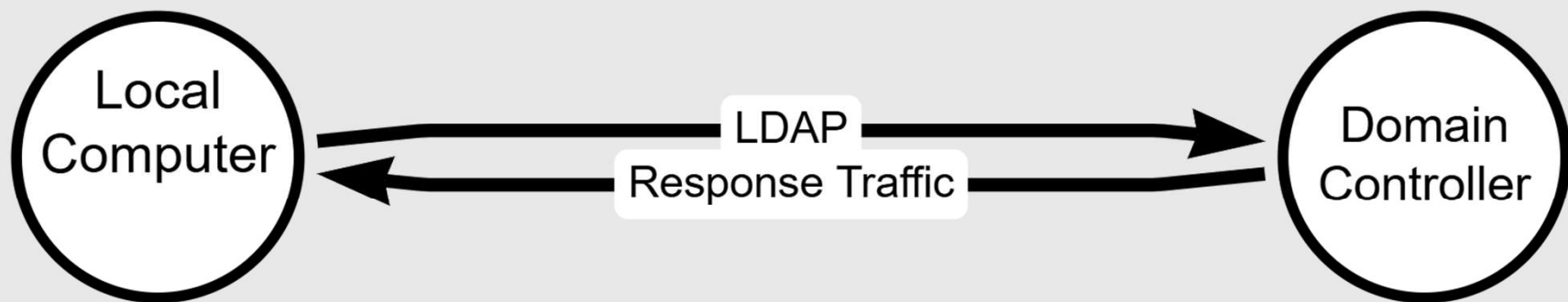


Collection

RUN ONCE PHASES

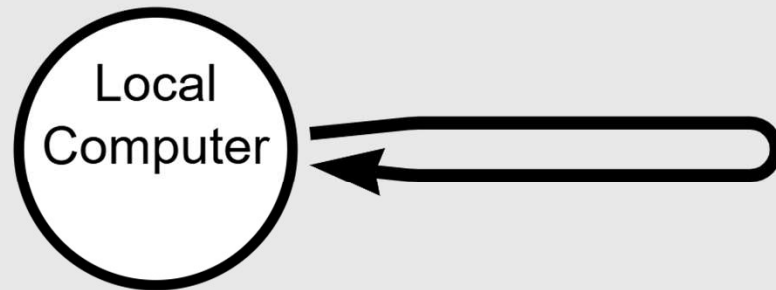


LDAP



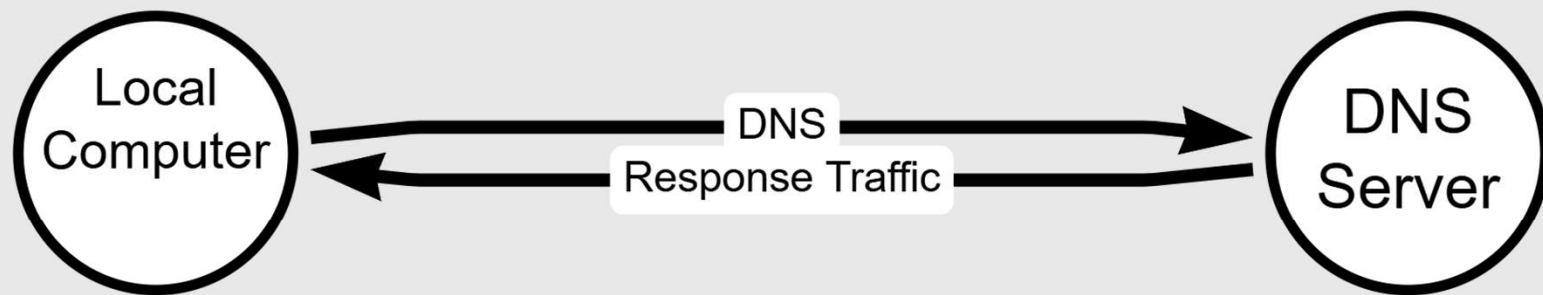
- Reads from **System Management** container in Active Directory
- Discovers:
 - sites, site servers, management points

Local



- Reads **client device logs** on disk
- Discovers:
 - management points, distribution points

DNS



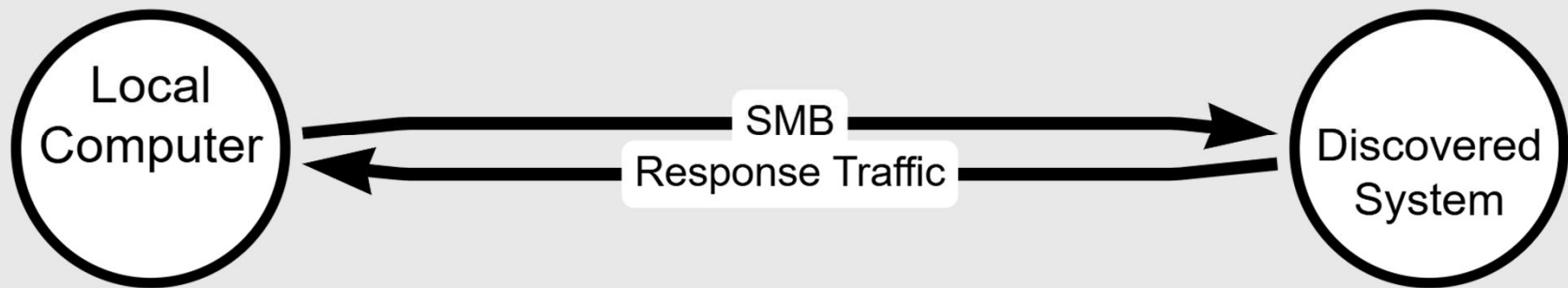
- Uses known site codes to query **SRV records**
- Discovers:
 - management points

Collection

PER HOST PHASES

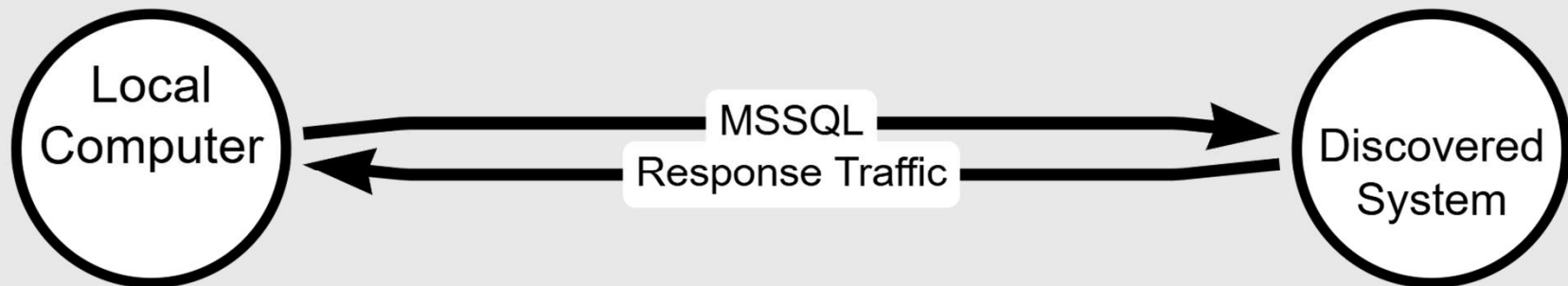


Remote Registry



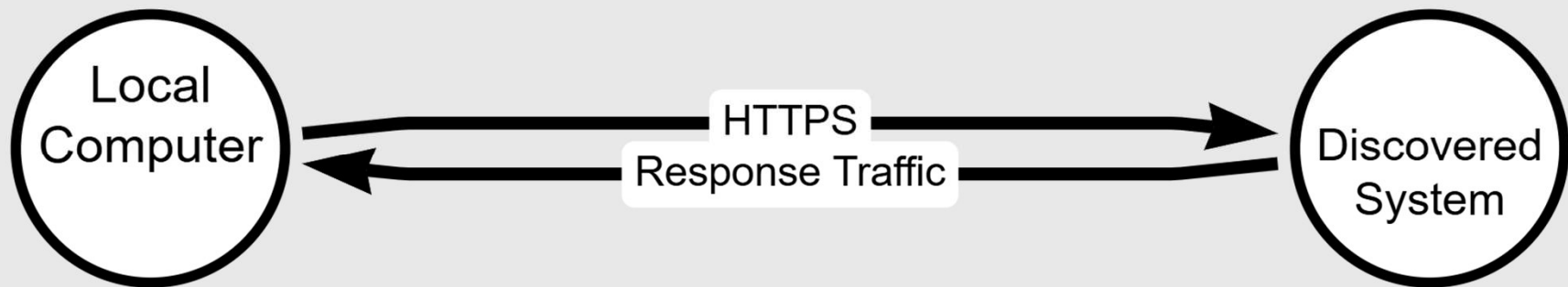
- Queries **subkeys accessible to authenticated users**
- Discovers:
 - site servers, site database servers, current user

MSSQL



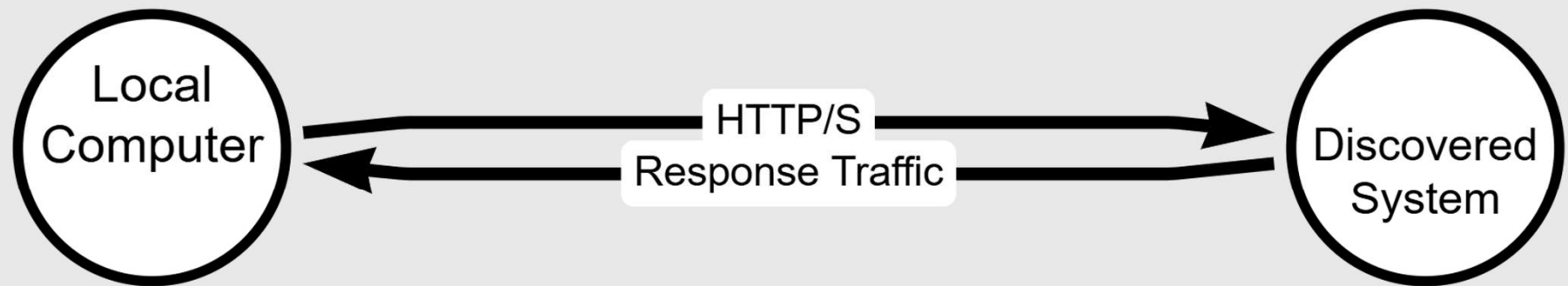
- Identifies **extended protection for authentication** settings
- Discovers:
 - site database servers, server and database principals

AdminService



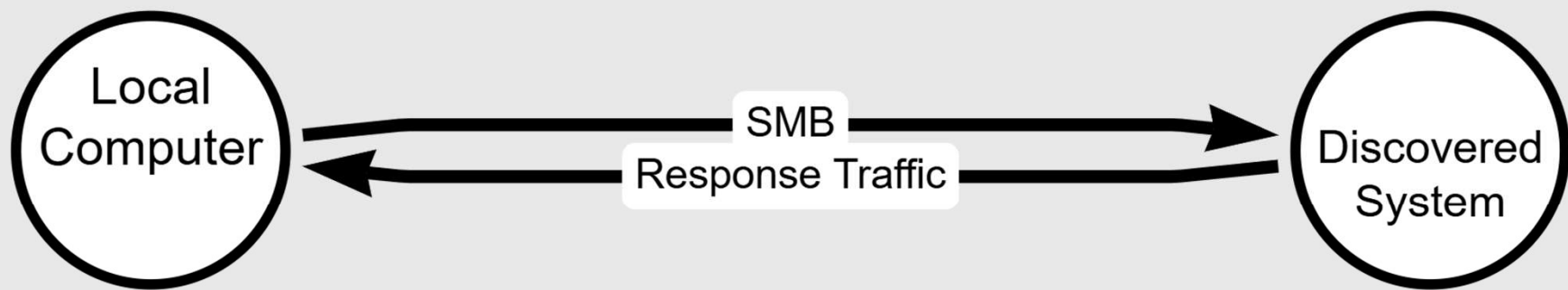
- Queries **AdminService** REST API on SMS Providers
- Discovers:
 - site systems, admin users/roles, client devices, logged in users

HTTP



- Requests **known HTTP endpoints** and evaluates response codes
- Discovers:
 - management points, distribution points, SMS Providers

SMB



- Identifies **SMB signing** requirements
- Reads SMB **share names and descriptions**
- Discovers:
 - site servers, distribution points

Processing

- Sites
- Admin users and roles
- Site system roles
- Relay to MSSQL
- Relay to AdminService
- Relay to SMB

Interesting Edges

- CoerceAndRelayToAdminService
- SameHostAs
- SCCM_AdminsReplicatedTo
- SCCM_AllPermissions
- SCCM_AssignAllPermissions
- SCCM_HasCurrentUser/HasADLastLogon/HasPrimaryUser
- SCCM_HasNetworkAccessAccount
- SCCM_HasStoredAccount
- SCCM_IsMappedTo

ConfigManBearPig To Do

- ~~Port to Python~~
- Abuse Info
- ~~DHCP/WM/CMPivot~~ collection
- Add more existing/new attack techniques
- ~~Optimize run duration~~ and Cypher queries
- Enable support for BloodHound Enterprise

MSSQL Attack Paths



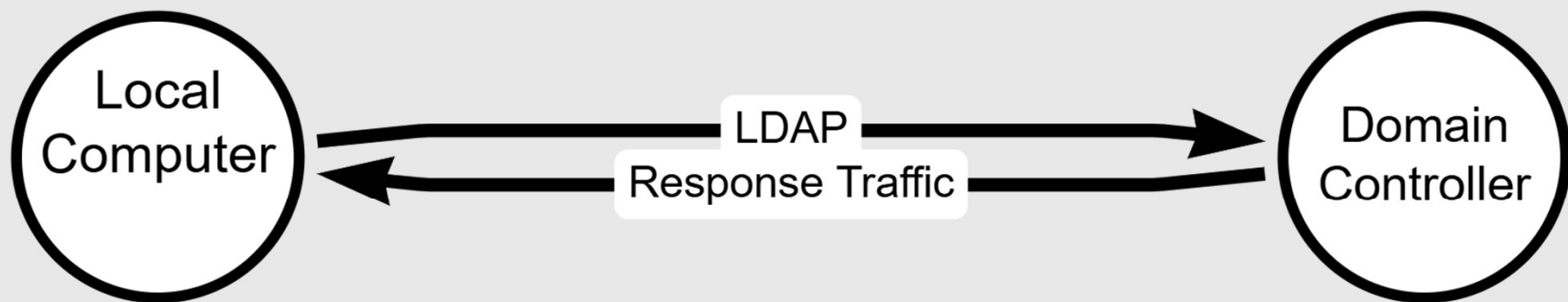
MSSQLHound

- A PowerShell Go OpenGraph collector for MSSQL
- 7 new nodes
- 37 new edges
- Requires an MSSQL server login

<https://github.com/SpecterOps/MSSQLHOUND>

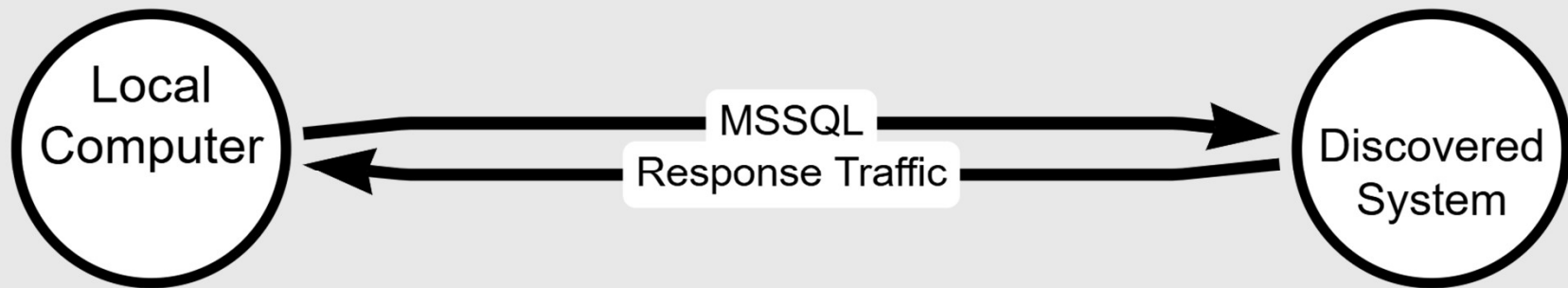


LDAP



- Searches for computers with MSSQLSvc **service principal names**
- Discovers:
 - MSSQL hostnames, ports, and instance names

MSSQL



- Identifies extended protection for authentication settings
- Discovers:
 - server and database principals, role members, linked servers, stored credentials, and much more

Processing

- Server logins and roles
- Database users and roles
- Members
- Permissions
- Ownership
- Trustworthiness
- Linked servers
- Stored credentials

Interesting Edges

- CoerceAndRelayToMSSQL
- MSSQL_ChangePassword
- MSSQL_ExecuteAs
- MSSQL_ExecuteAsOwner
- MSSQL_ExecuteOnHost
- MSSQL_Get[Admin]TGS
- MSSQL_GrantAny[DB]Permission
- MSSQL_Has*Cred
- MSSQL_HostFor
- **MSSQL_LinkedAsAdmin**

Go Port

- PR'd and co-authored by 2026 SpecterOps Top Dog Javier Azofra
- **Concurrent** targeting, reducing run duration from 17 minutes to 17 seconds in SCCM Ludus lab environment
- **SOCKS** proxy support
- Cross-platform
- Authenticate with **NT hash** or Kerberos **ticket**
- Direct **upload to BloodHound**
- TDS 8.0 and additional EPA configurations

SCCM Lab



- A domain controller
- A central administration site (CAS) with the following site system roles installed on separate systems:
 - primary site server
 - site database
 - service connection point
- A child primary site (PS1) under CAS with the following site system roles installed on separate systems:
 - primary site server
 - site database
 - SMS Provider
 - management point
 - distribution point
 - content library
 - passive site server
 - development workstation / client device
- A child secondary site (SEC) under PS1 with a secondary site server (PS1-SEC) hosting the management point and distribution point site system roles

https://github.com/Mayyhem/ludus_sccm



DEMO

Visualizing Attack Paths



Wrapping It Up

What should I look at next?



Offensive/defensive walkthroughs:
misconfigurationmanager.com



#sccm Slack Tradedcraft Community:
<https://slack.specterops.io/>



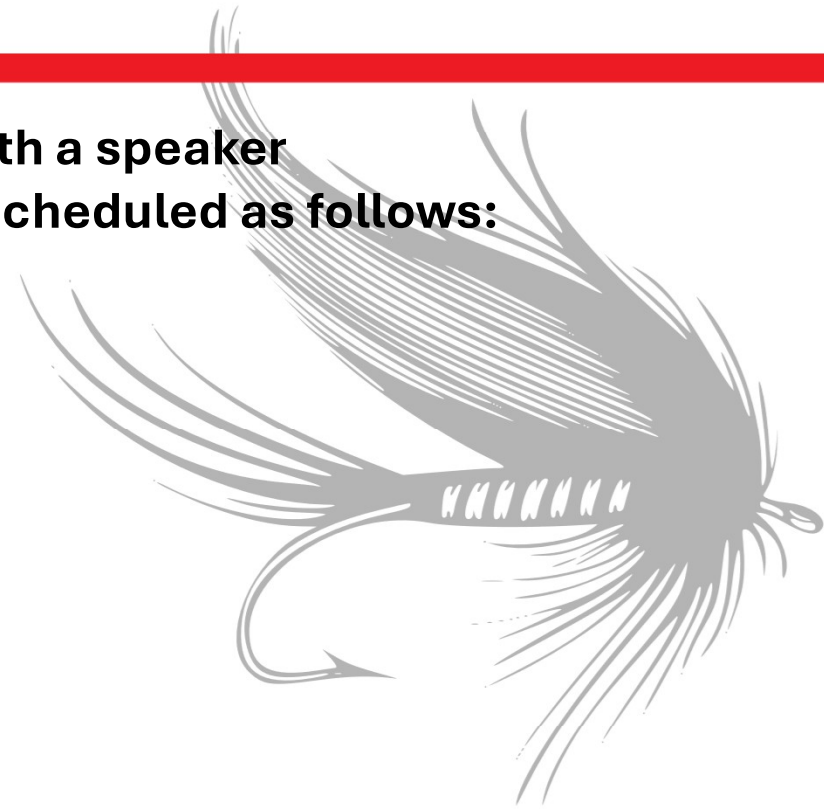
ConfigManBearPig Tool:
<https://github.com/Mayyhem/ConfigManBearPig>



Practice lab:
https://github.com/Mayyhem/ludus_sccm

Fishing Sessions

**Be sure to find Wally and sign up for 1:1 time with a speaker
If you'd like to "catch" us for a session, we are scheduled as follows:**



Don't forget to leave feedback for your speakers!

SAVE THE DATES

Oct 25-28, 2026



May 2-6, 2027



Oct 10-13, 2027



Extended Q&A



Recast



ninjaOne®



numecent®

