

# Exposing SCCM and MSSQL Attack Paths in Hardened Environments with BloodHound OpenGraph



Slides

**Chris Thompson**

- X: @\_Mayyhem
- Slack: @Mayyhem  
<https://slack.specterops.io>
- GitHub: Mayyhem
- LinkedIn: x24

# CHRIS THOMPSON

- Sr. Security Researcher @ SpecterOps
- Red Teamer / Pentester
- Open-source Tool Developer
  - SharpSCCM
  - Misconfiguration Manager
  - Maestro
  - MSSQLHound
- Contributor
  - BloodHound
  - SharpHound
  - AzureHound
  - SCCMHunter
  - SCKit
  - PXETHiefy
- Trainer/Speaker
  - Black Hat US/EU
  - DEF CON
  - TROOPERS
  - MMS
  - SO-CON
  - SpecterBash



X: @\_MAYYHEM

SLACK: @\_MAYYHEM  
[HTTPS://SLACK.SPECTEROPS.IO](https://slack.specterops.io)

GITHUB: MAYYHEM

LINKEDIN: X24

# AGENDA

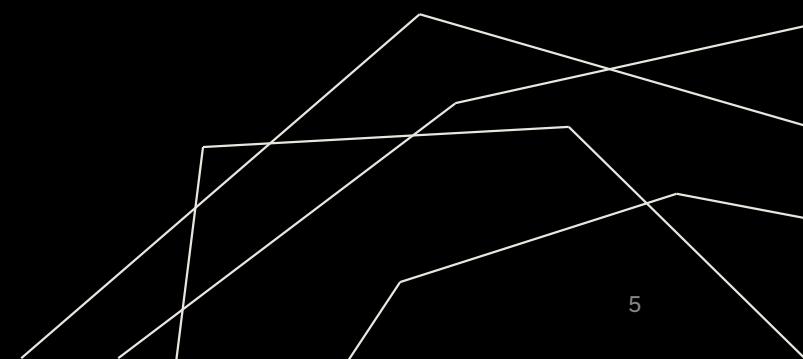
## SCCM/MSSQL Attack Paths

- Crash Course
- Attack Demos
- Data Collection
- Exploring the Graph

# WHO IS THIS TALK FOR?

- Pentesters
- Red teamers
- Defenders
- IT admins
- IT auditors
- IT leadership
- IT curious

# WHAT IS SCCM?



# WHAT IS SCCM?

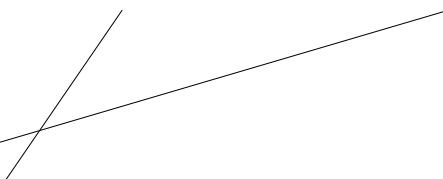
- Allows IT admins to **deploy software** and updates to computers

# WHAT IS SCCM?

- Released in **1994**
- Currently Microsoft Configuration Manager  
(ConfigMgr, ConfigMan, MCM)
- Formerly (and still sometimes referred to as):
  - Microsoft Endpoint Configuration Manager (MECM)
  - Microsoft Endpoint Manager Configuration Manager (MEMCM)
  - **System Center Configuration Manager (SCCM)**
  - Systems Management Server (SMS)

# WHAT IS SCCM?

- Allows IT admins to **deploy software** and updates to computers
- **Command and control server**



# SCCM HIERARCHY

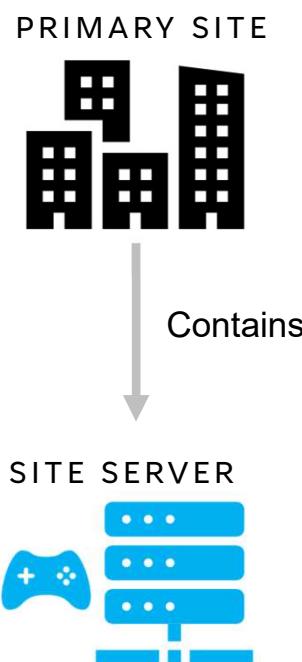
- One installation of SCCM
- Contains one or more sites
- This is the **security boundary**

PRIMARY SITE



## PRIMARY SITES

- ID'd by a 3-character **site code** (e.g., PS1)
- Serve software to managed **client devices**



# SITE SERVERS

Orchestrate all actions for:

- the site
- client devices
- site system roles

PRIMARY SITE



## SITE SYSTEM ROLES

- **Servers** that host one or more services for a primary site
- May be hosted remotely from the site server **or on the site server**



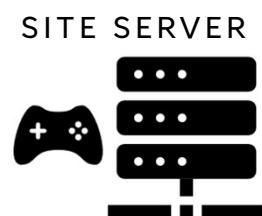
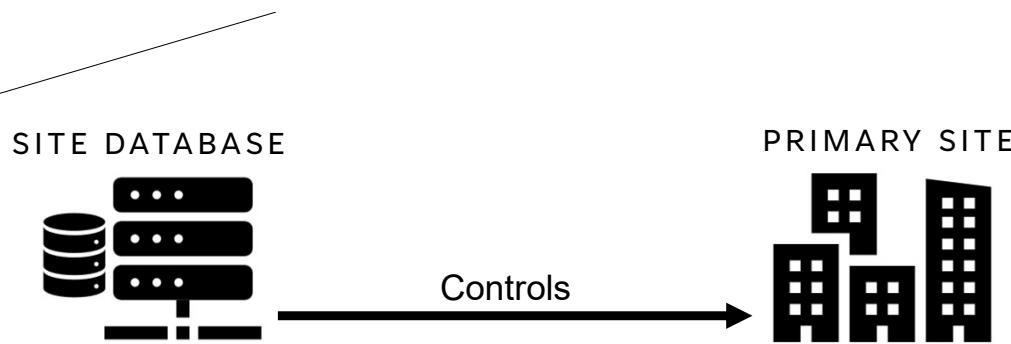
## SITE DATABASES

- Each site's system of record
- Global configs are **replicated** to all other sites in the hierarchy



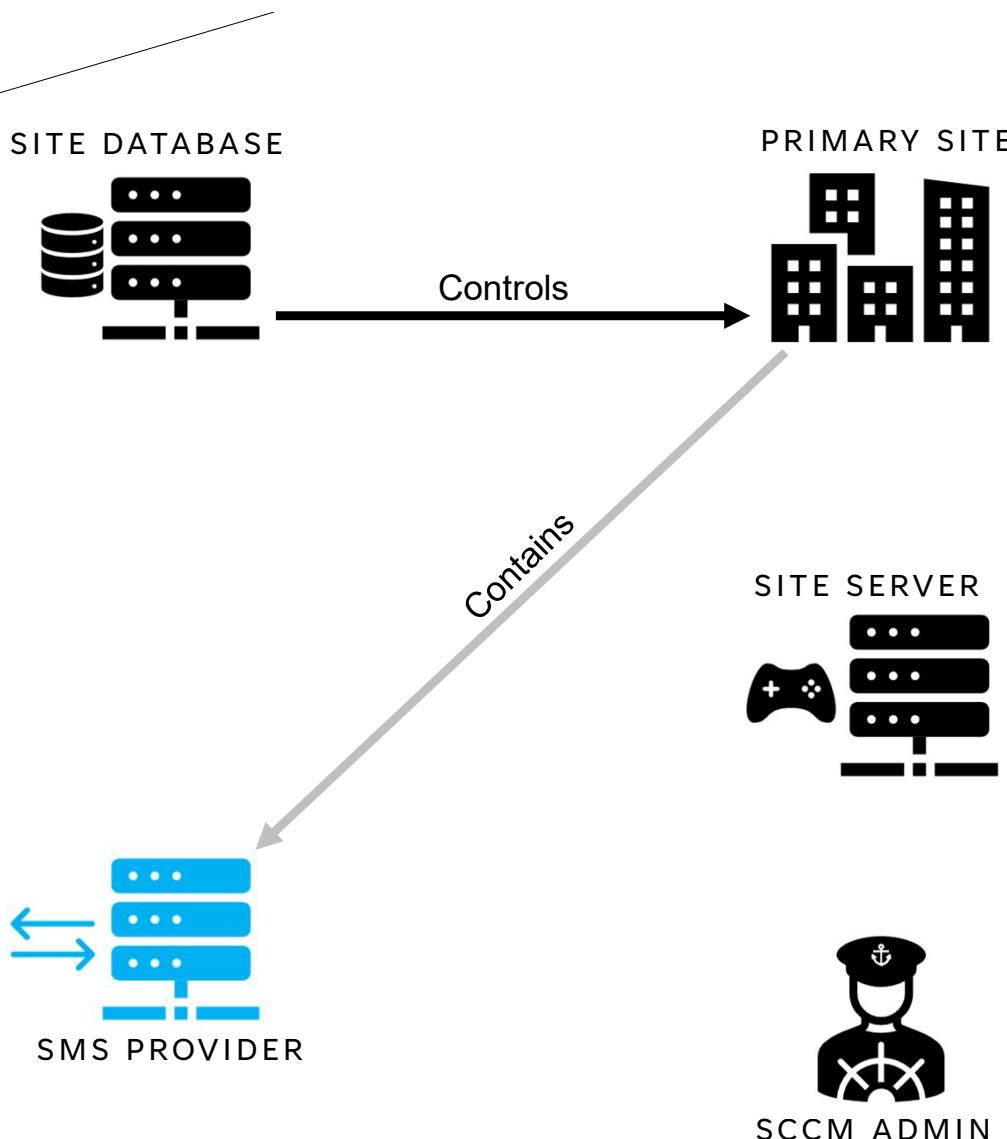
## SITE DATABASES

- Each site's system of record
- Global configs are **replicated** to all other sites in the hierarchy
- **Define admin users and roles**



## SCCM ADMINS

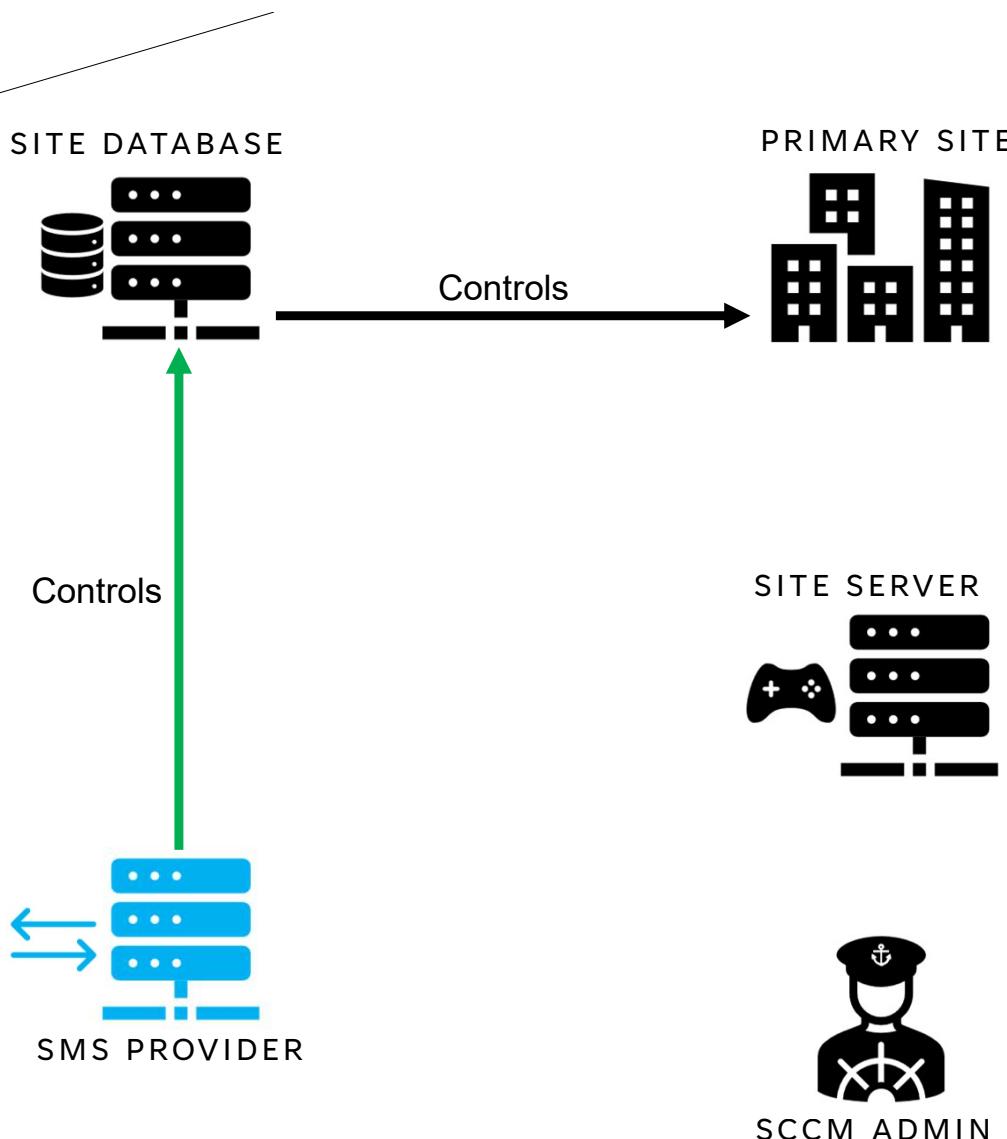
Interact with site database to manage the site... how?



## SMS PROVIDERS

Host two APIs for SCCM admins to manage site database:

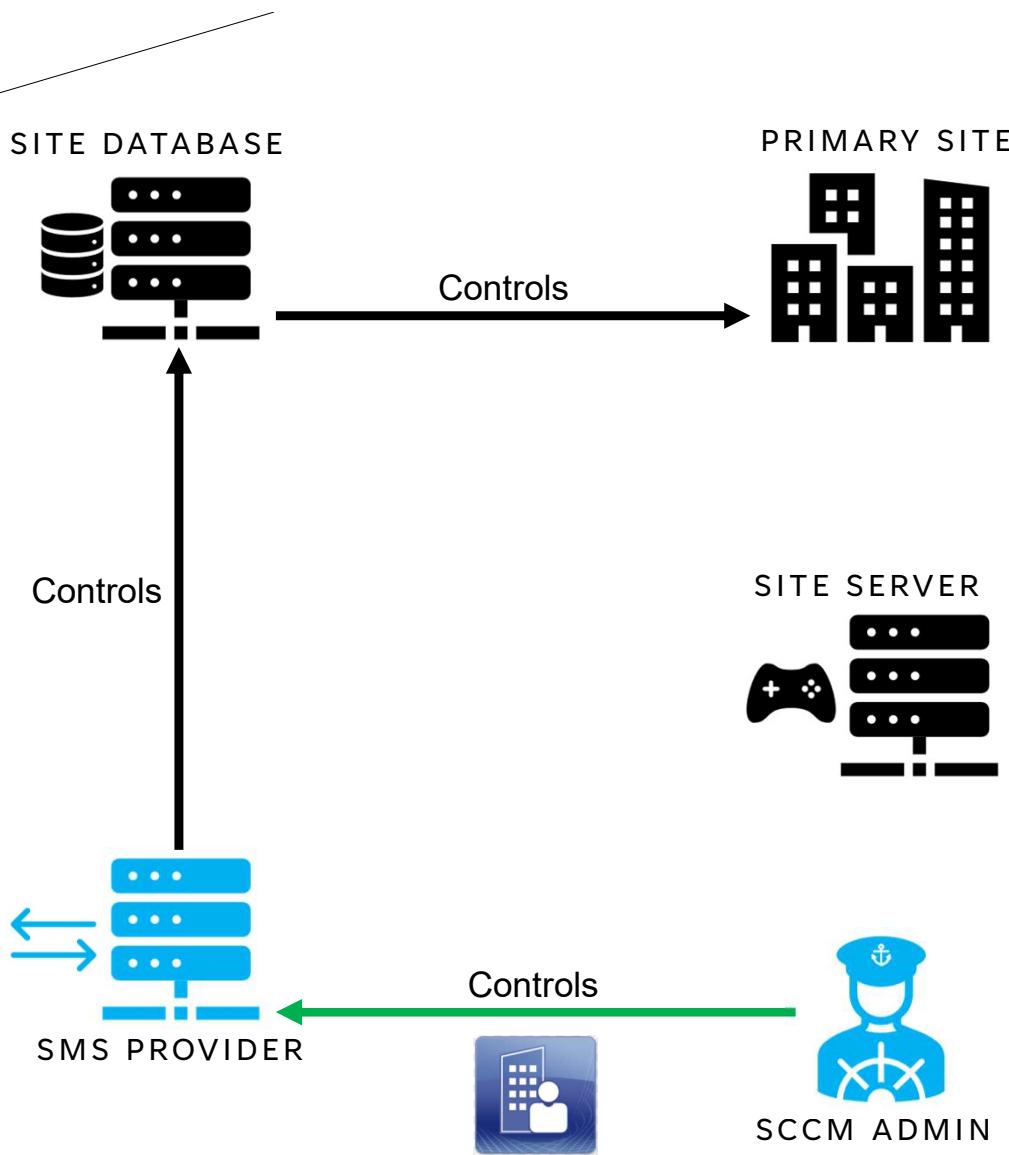
- **AdminService**
  - REST API (HTTPS)
- **WMI**
  - Windows Management Instrumentation



## SMS PROVIDERS

Host two APIs for SCCM admins to manage site database:

- **AdminService**
  - REST API (HTTPS)
- **WMI**
  - Windows Management Instrumentation



## SCCM ADMINS

Use Configuration Manager **Console** software to control SCCM via SMS Provider APIs

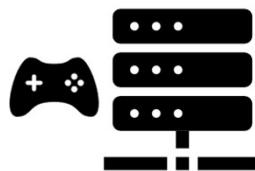
SITE DATABASE



PRIMARY SITE



SITE SERVER

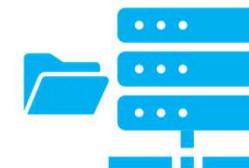


SMS PROVIDER

Contains

## DISTRIBUTION POINTS

**Host software files** for client devices to download and install via HTTP(S) and SMB



DISTRIBUTION  
POINT

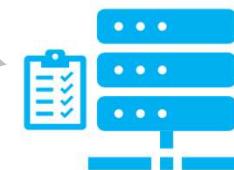
SITE DATABASE



PRIMARY SITE

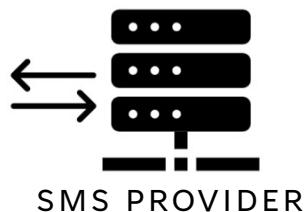


Contains



MANAGEMENT POINT

SITE SERVER



SMS PROVIDER

## MANAGEMENT POINTS

Define tasks for client devices to fetch via HTTP(S) and execute

- download/install software from X distribution point

SITE DATABASE



PRIMARY SITE



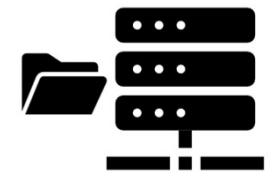
MANAGEMENT POINT



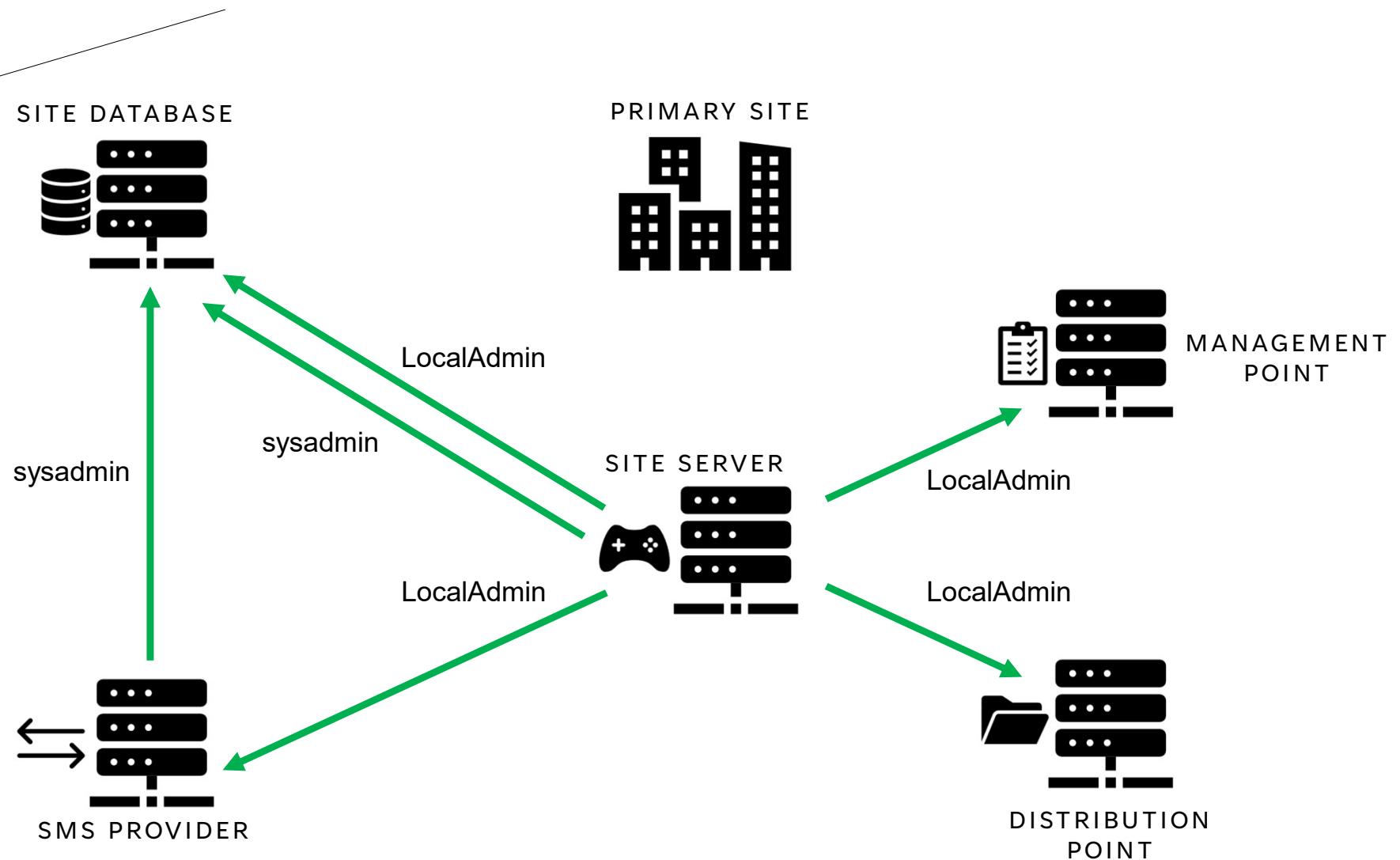
SITE SERVER

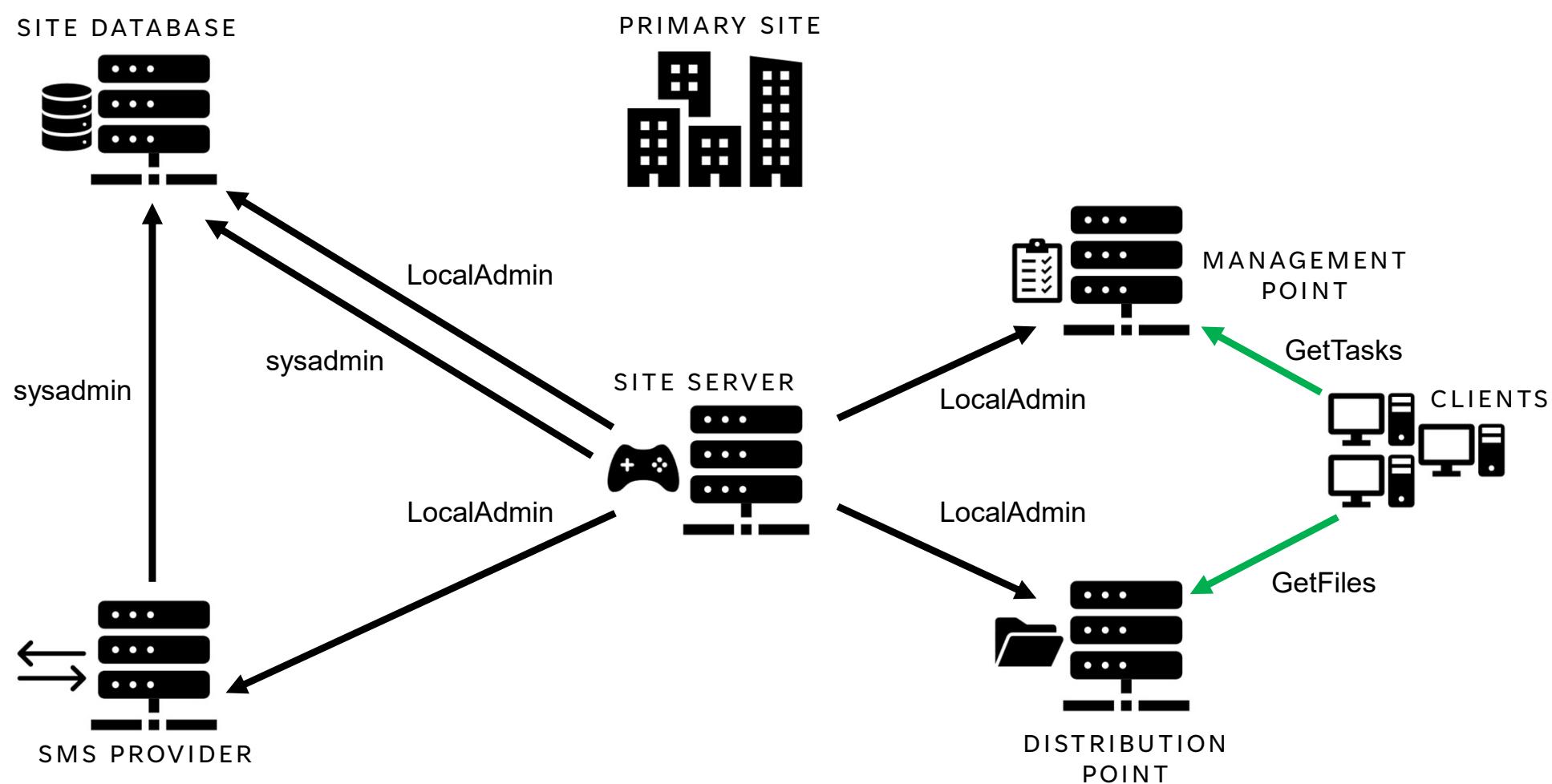


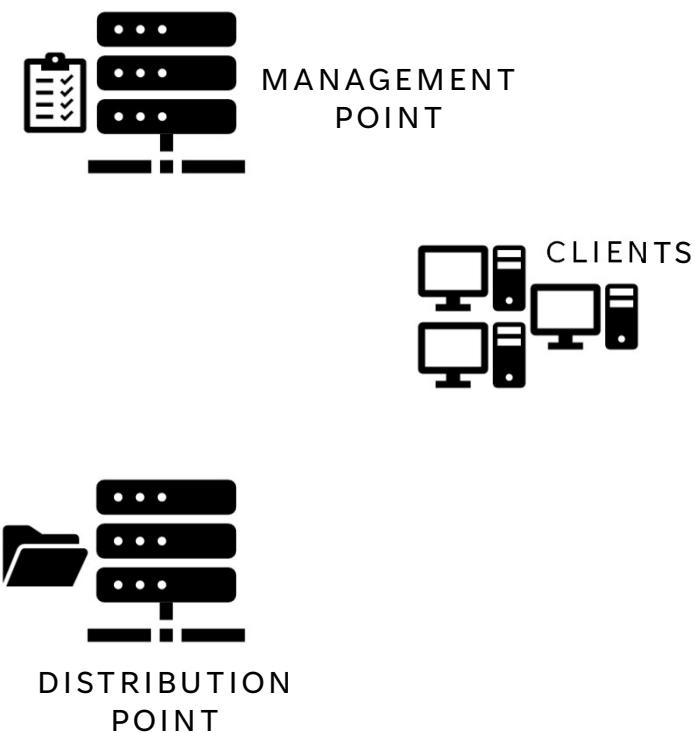
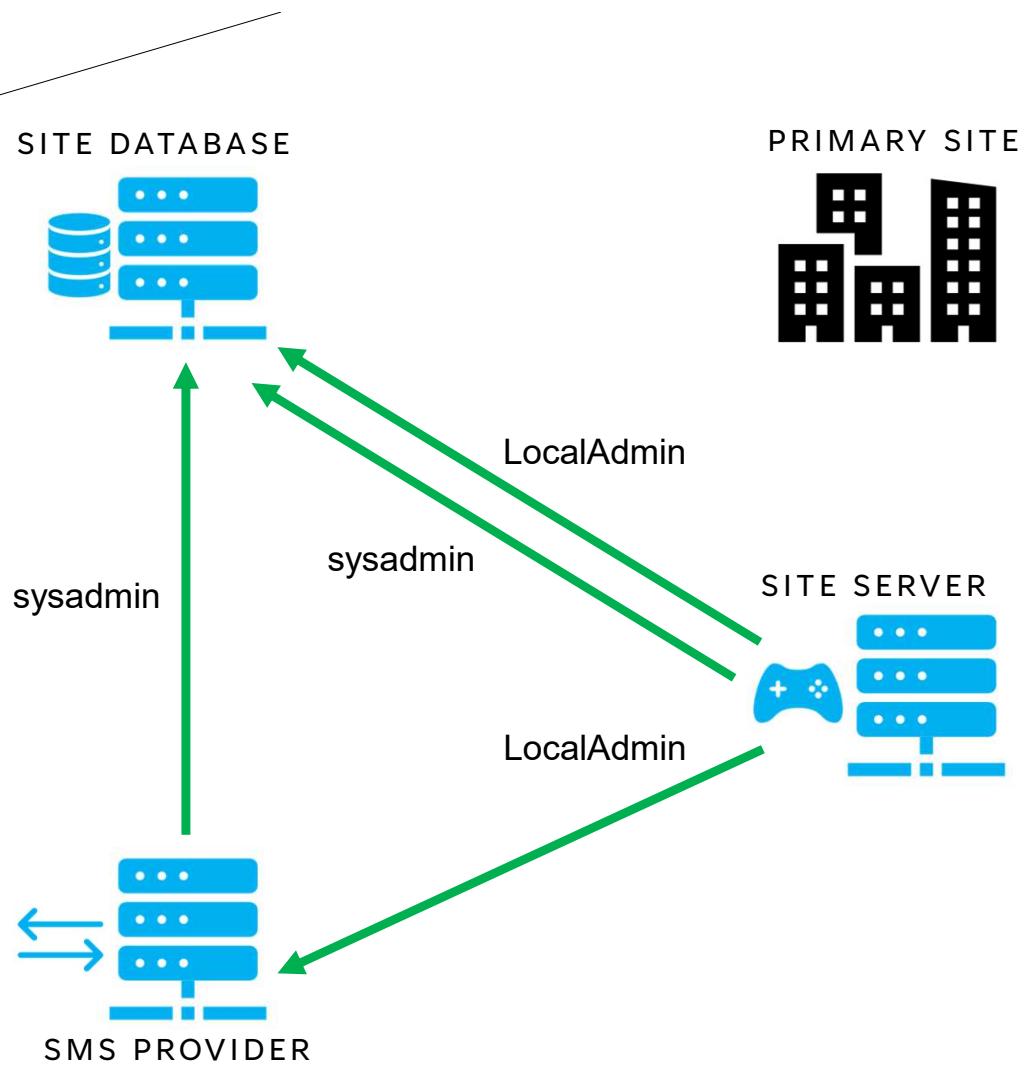
SMS PROVIDER

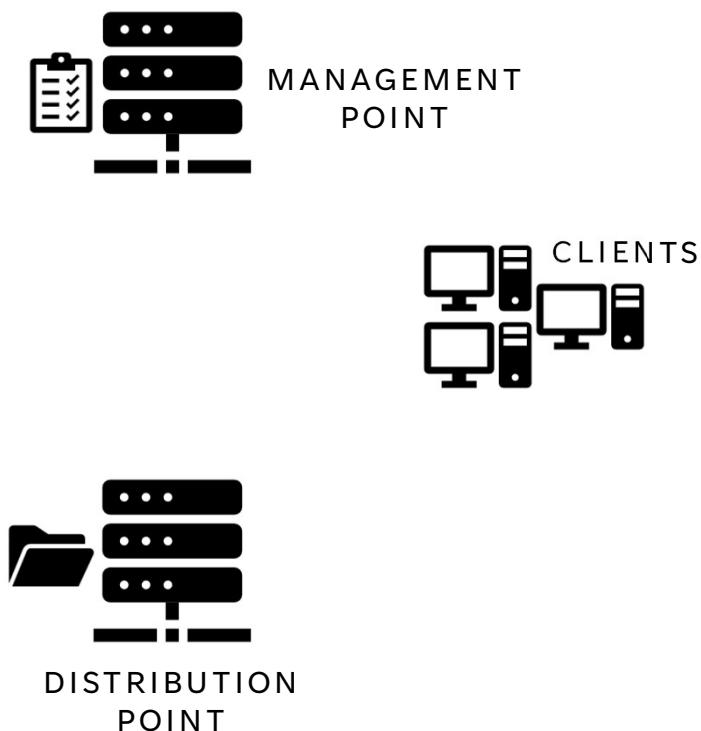
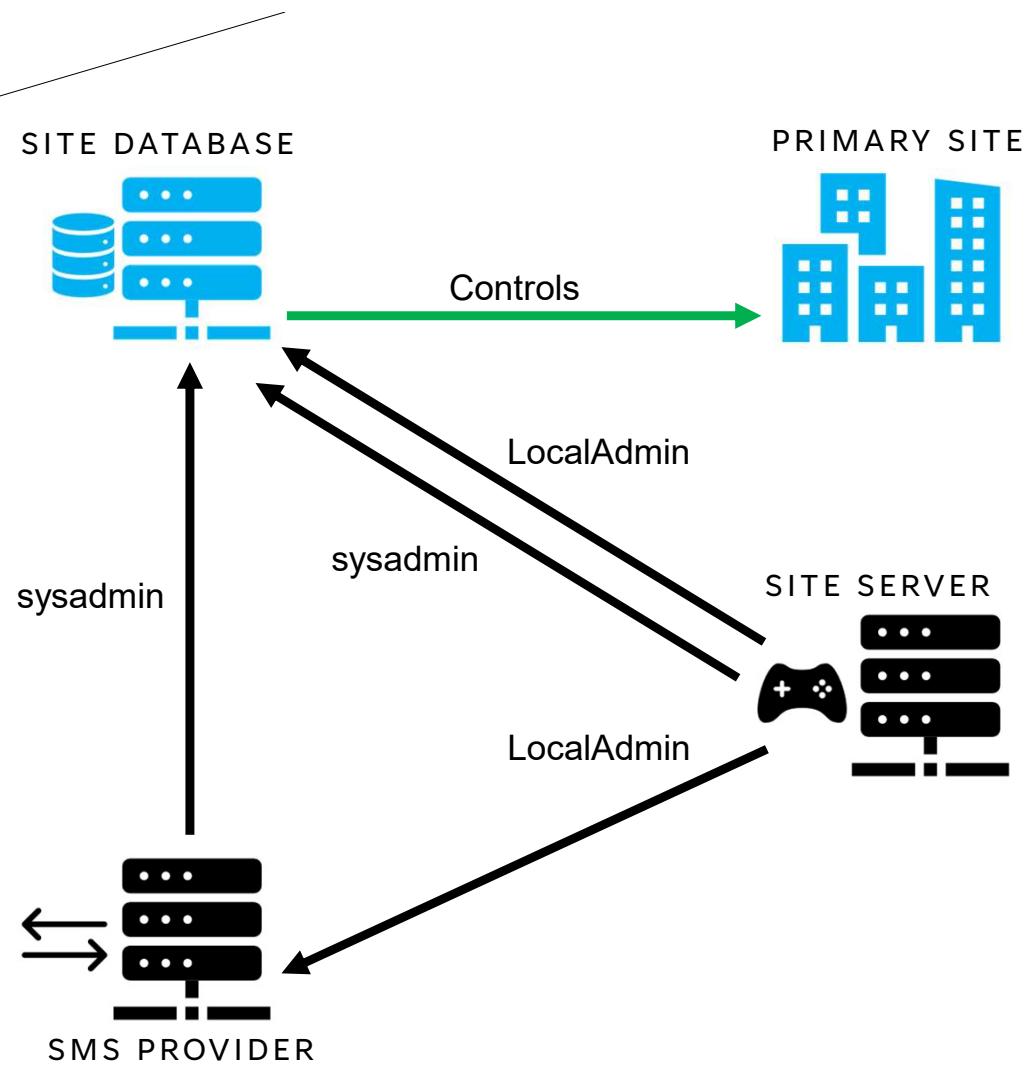


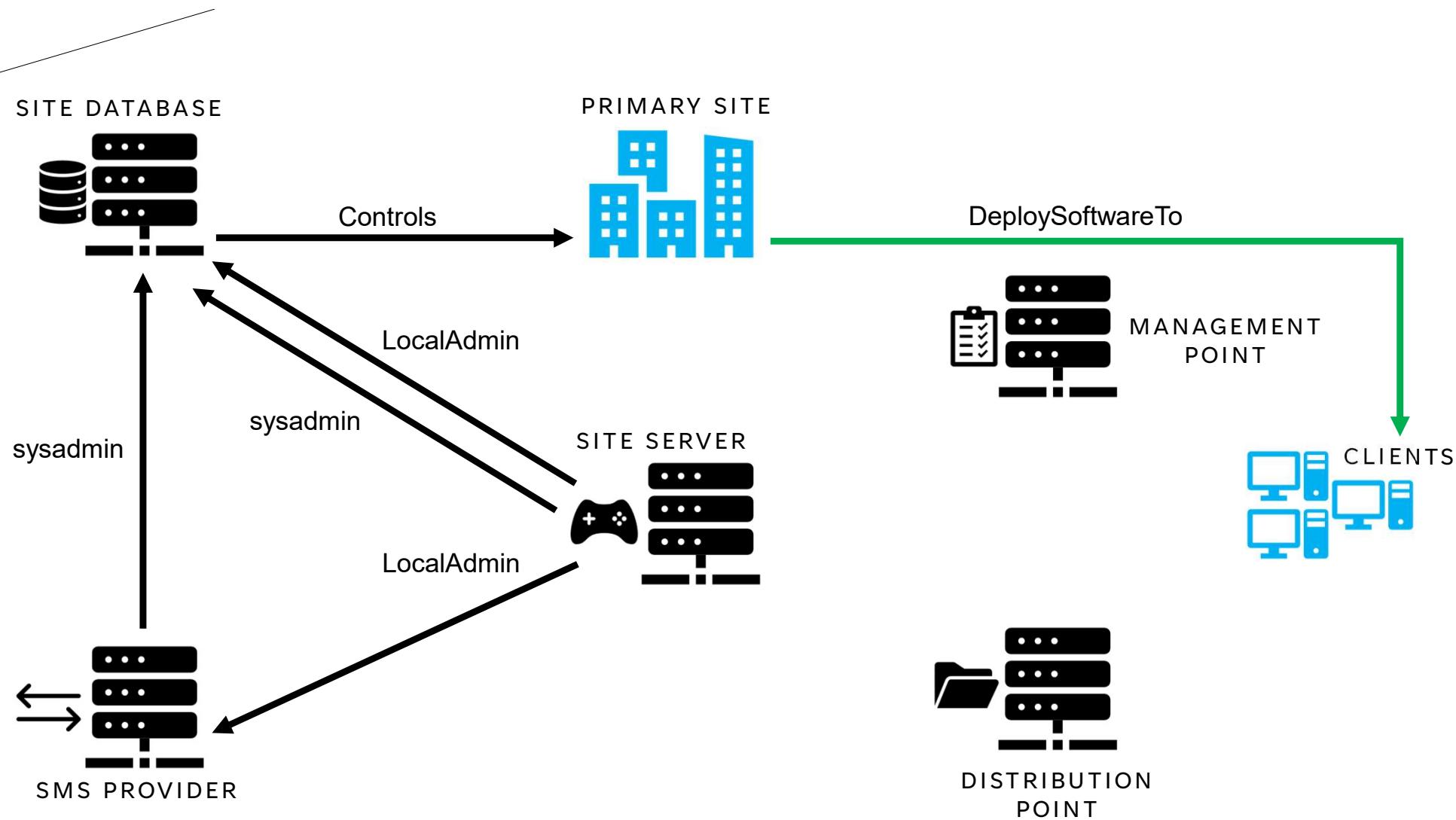
DISTRIBUTION POINT







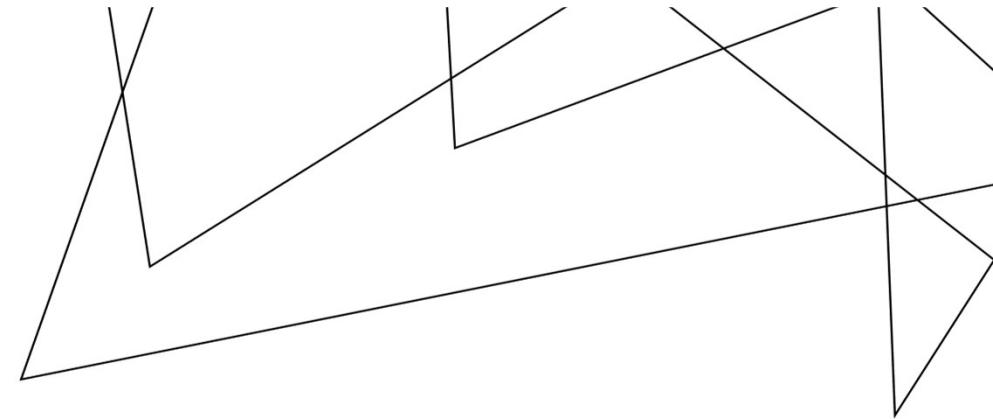






# **SCCM ATTACK PATHS**

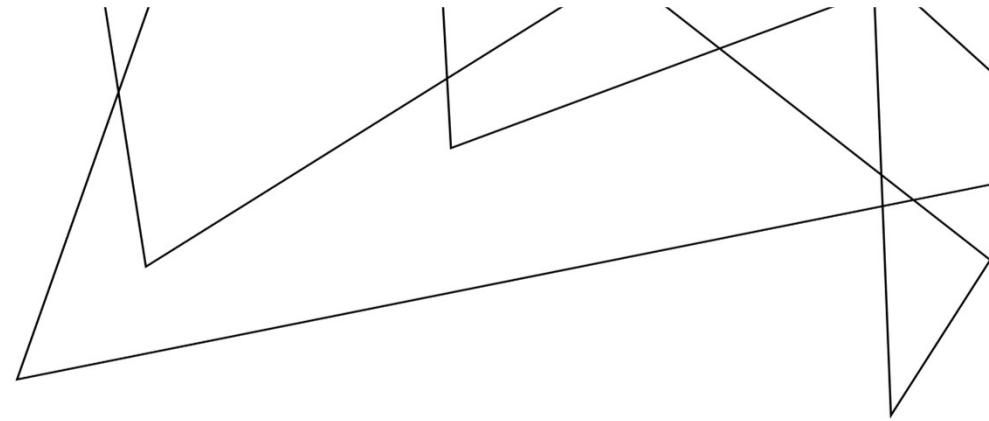
ALLOW CONTROL OF MANAGED DEVICES



**33+ ATTACK TECHNIQUES**  
**DISCOVERED SINCE 2022**

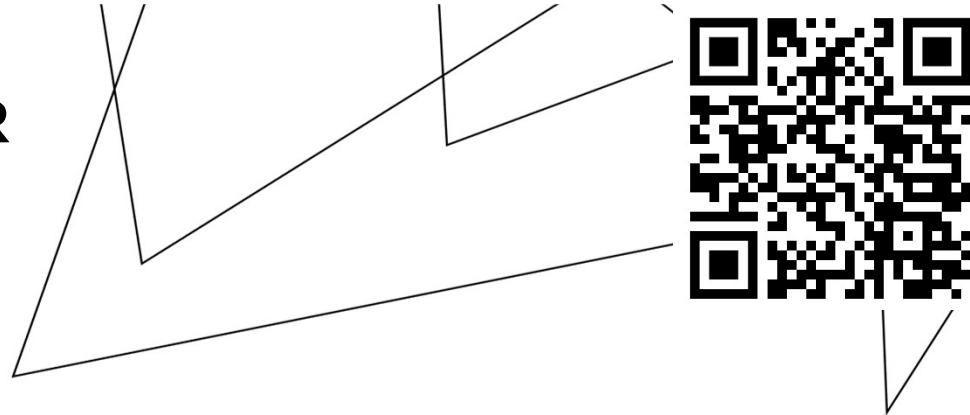
## SHOUTOUTS / PRIOR WORK

- 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)

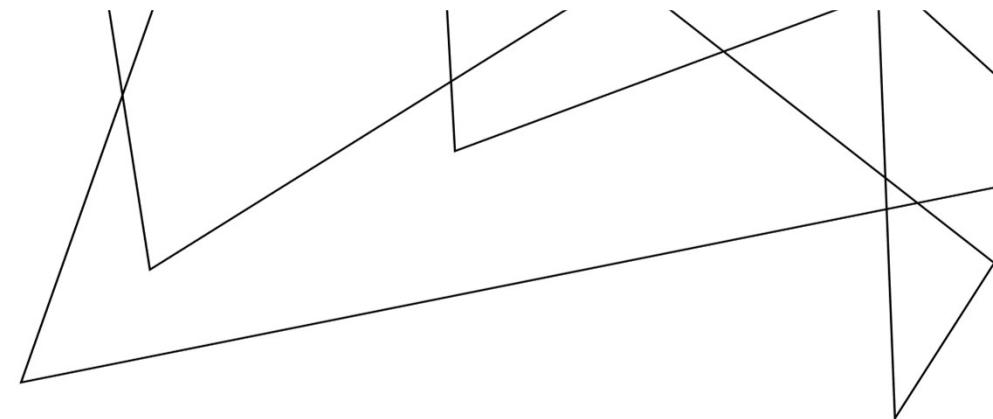


# MISCONFIGURATION MANAGER

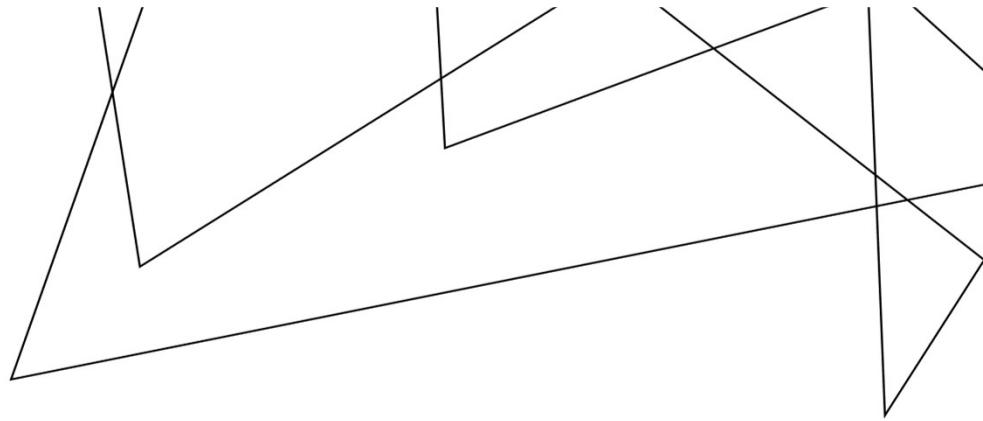
- Step-by-step offensive and defensive **write-ups** for attack techniques
- A **taxonomy** to simplify and demystify concepts
- Based on MITRE ATT&CK
- Co-authored with Duane Michael (@subat0mik) and Garrett Foster (@unsigned\_sh0rt)



RECON 



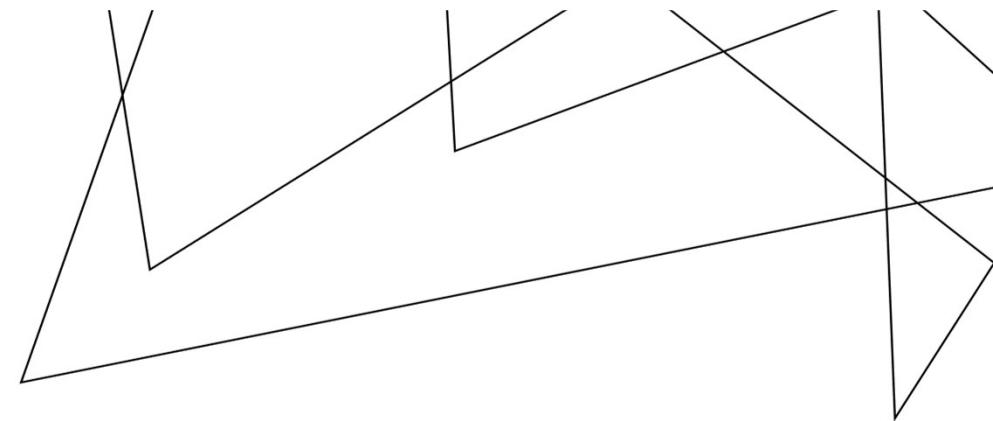
**RECON**  
**CRED** 



RECON

CRED

COERCE

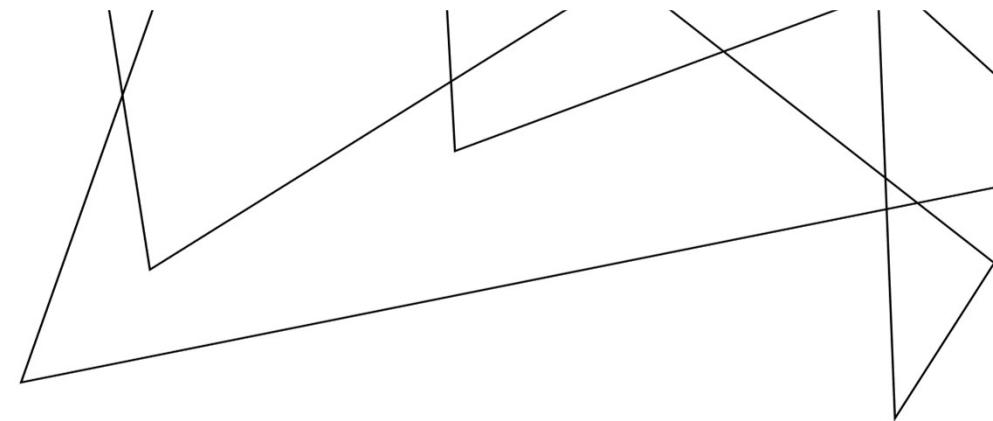


RECON

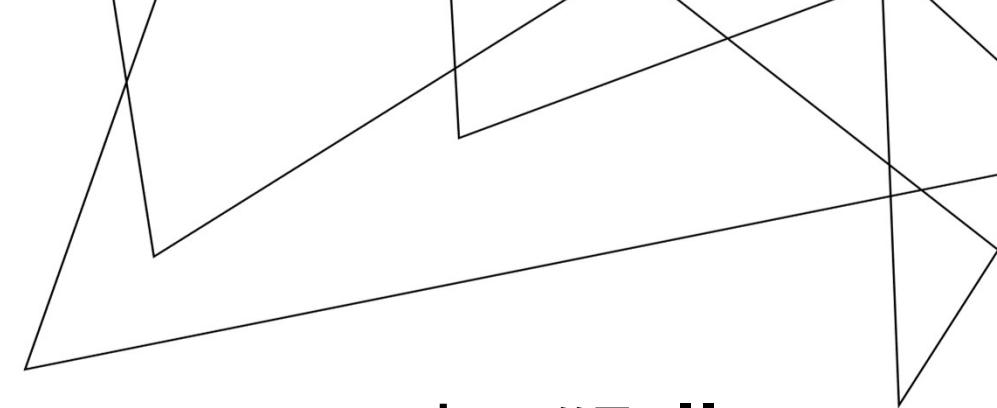
CRED

COERCE

ELEVATE



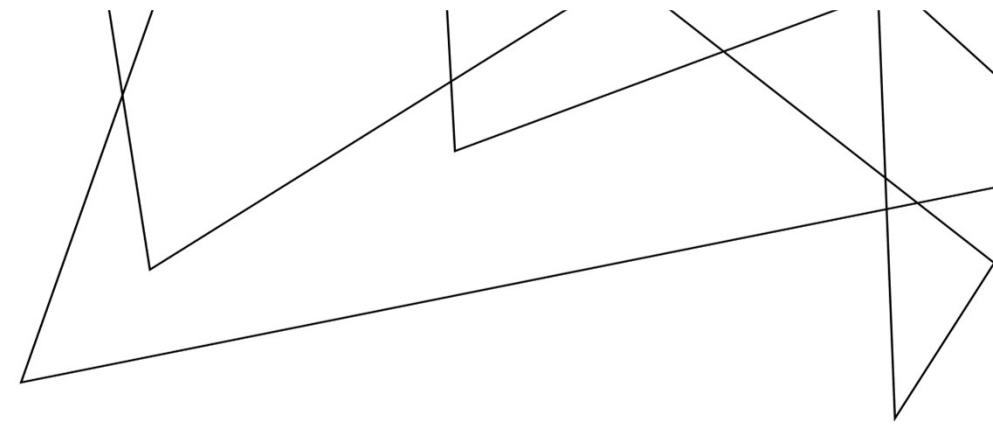
RECON  
CRED  
COERCE  
ELEVATE  
TAKEOVER



Grant a user the “**Full Administrator**” role by modifying SCCM via access to:

- site database
- SMS Provider APIs

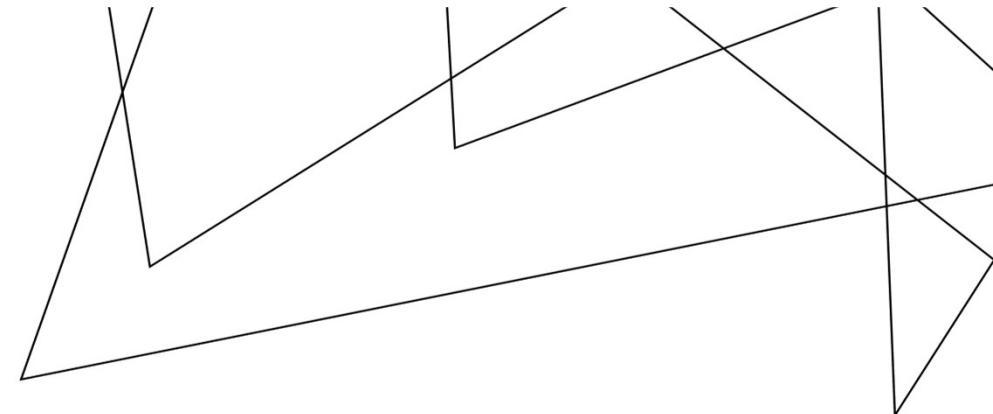
RECON  
CRED  
COERCE  
ELEVATE  
TAKEOVER  
EXEC 



ELEVATE

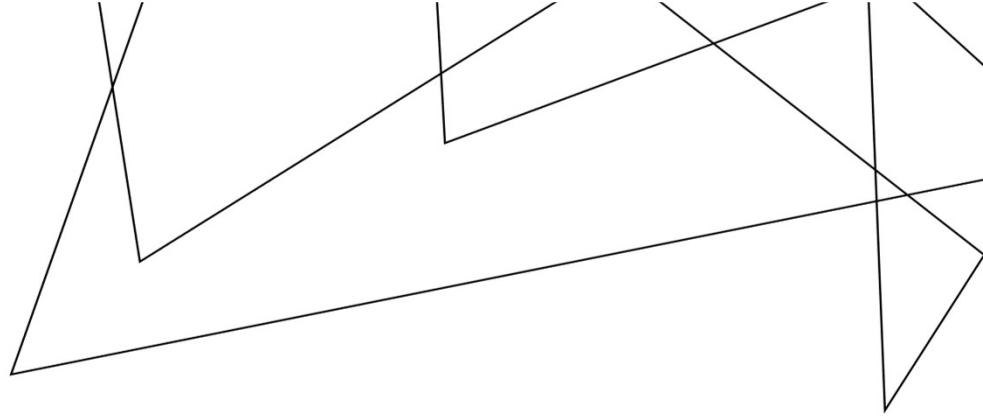


TAKEOVER



The site server's domain computer account **MUST** be:

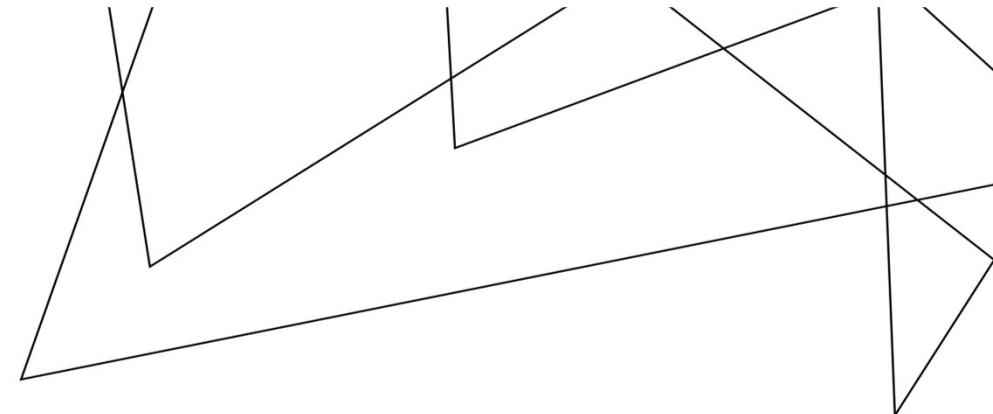
- a **local Administrator** of every other SCCM server
- a **sysadmin** in the site database



# NTLM

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

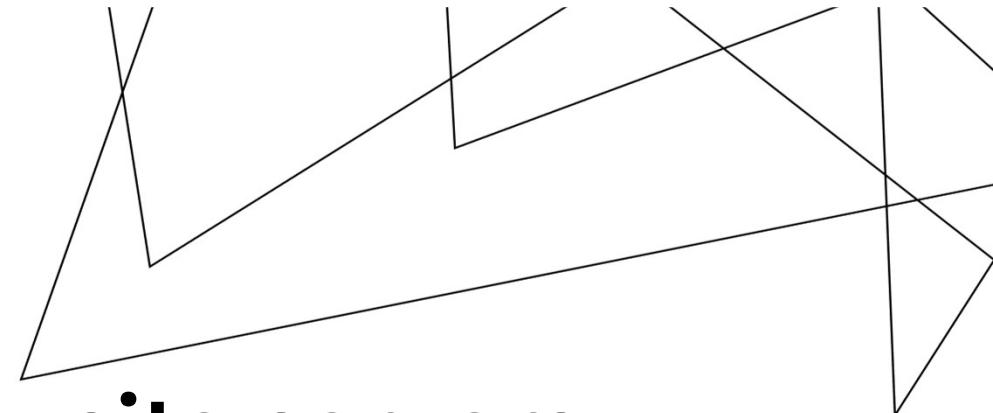
# NTLM RELAY



Attackers can **coerce** computers into authenticating to their machine and **use** the creds on another machine where that computer has privileges

- e.g., Printerbug, PetitPotam

# NTLM RELAY

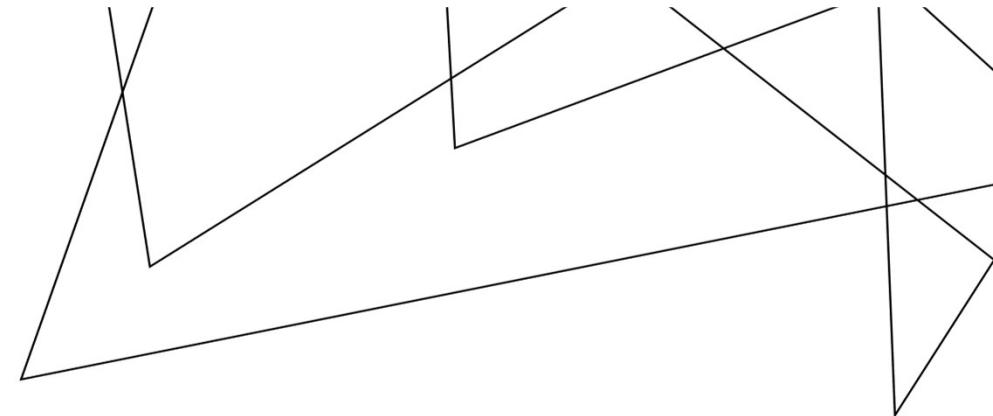


**site servers**

Attackers can **coerce** computers into authenticating to their machine and **use** the creds on another machine where that computer has privileges

- e.g., Printerbug, PetitPotam

# NTLM RELAY



Susceptible when hosted **remotely** from  
the site server:

- site database
- SMS Provider APIs
- other site system roles

# TAKEOVER



SITE DATABASE



PRIMARY SITE

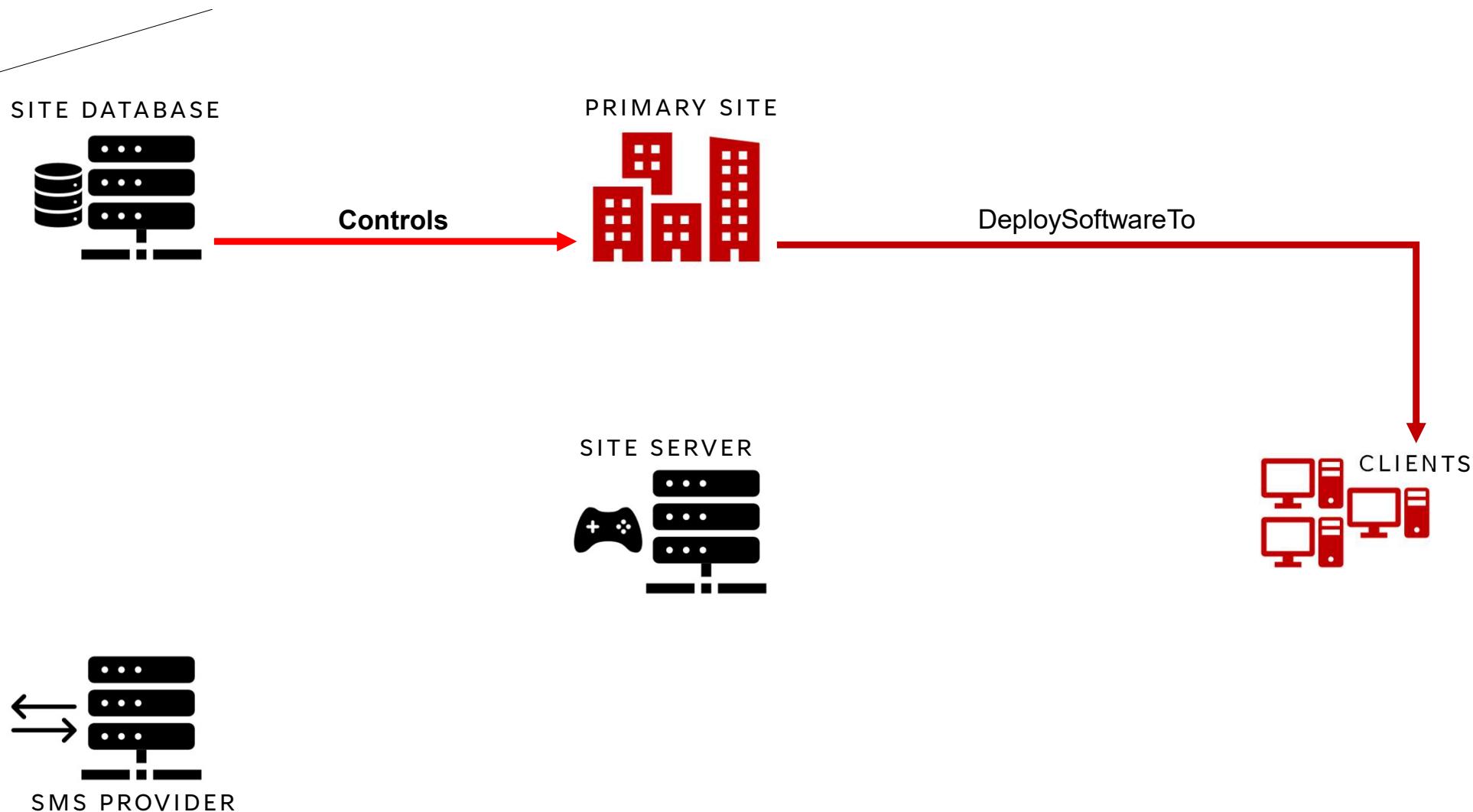


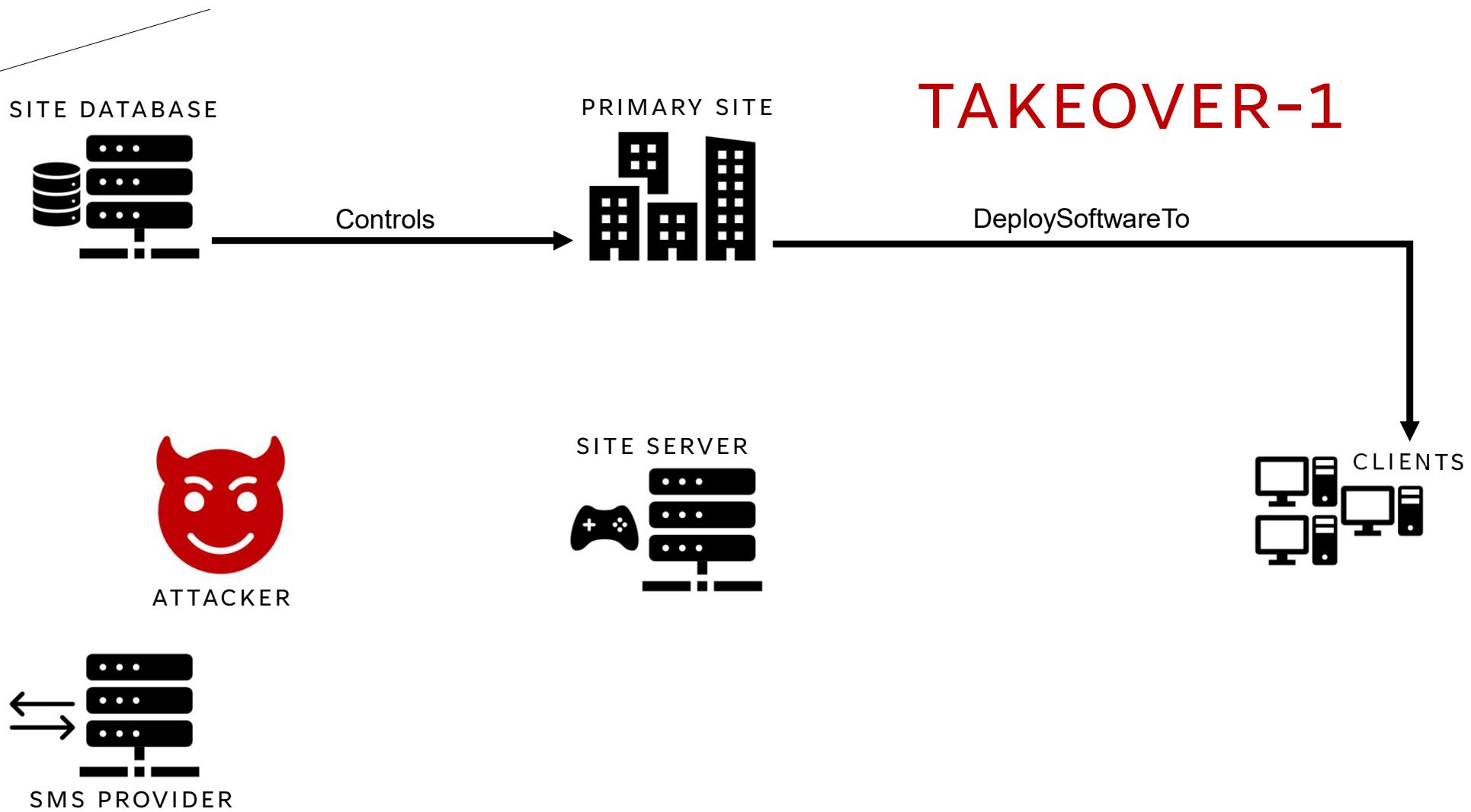
**DeploySoftwareTo**

SITE SERVER



SMS PROVIDER





SITE DATABASE



PRIMARY SITE



## TAKEOVER-1

Controls

DeploySoftwareTo



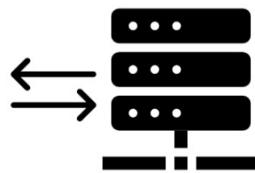
ATTACKER

1. CoerceFrom

SITE SERVER



CLIENTS



SMS PROVIDER

SITE DATABASE



PRIMARY SITE



## TAKEOVER-1

Controls

DeploySoftwareTo

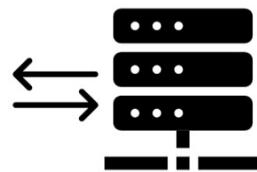


SITE SERVER



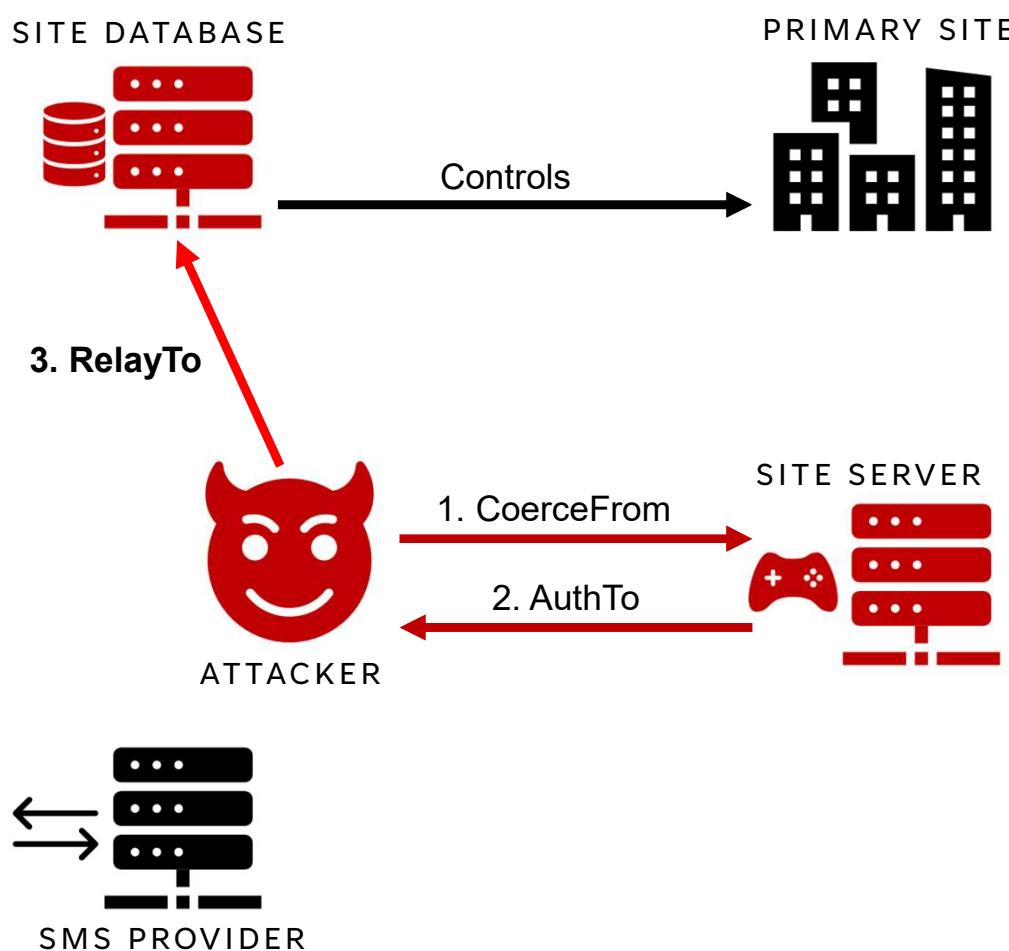
1. CoerceFrom

2. AuthTo

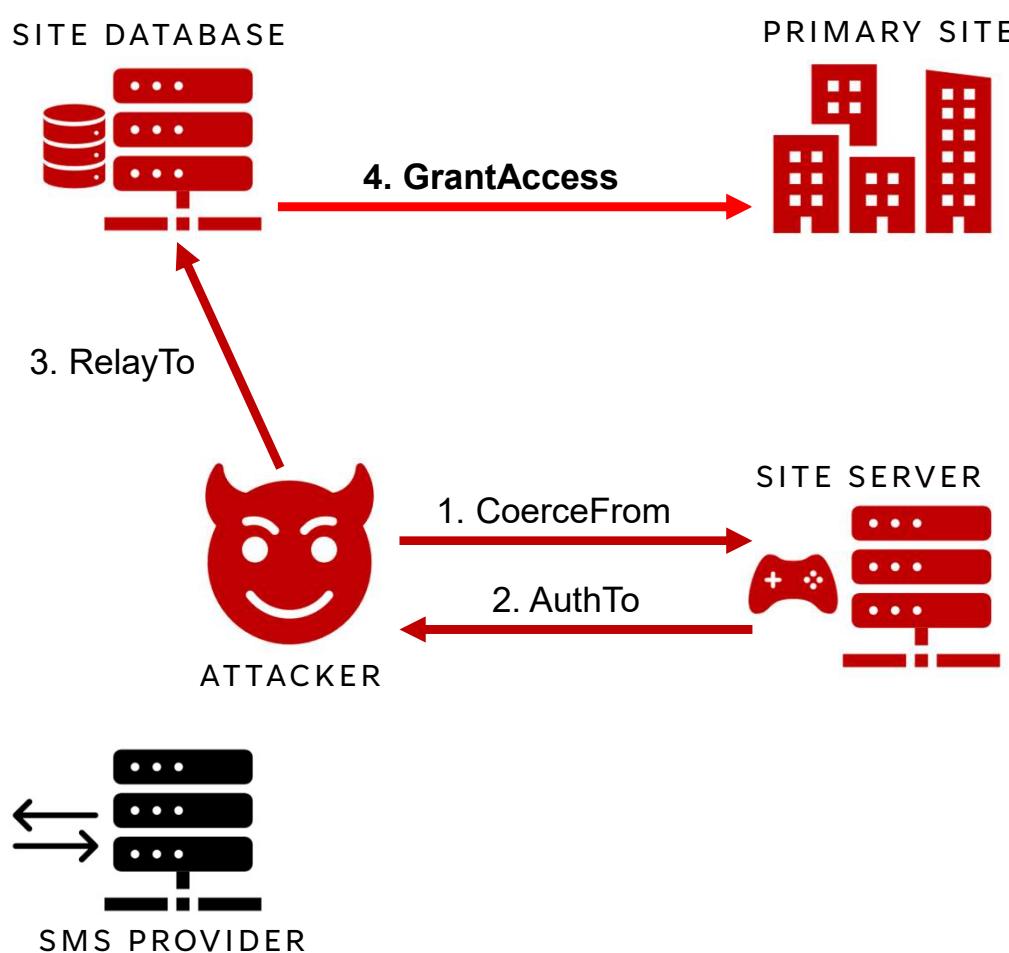


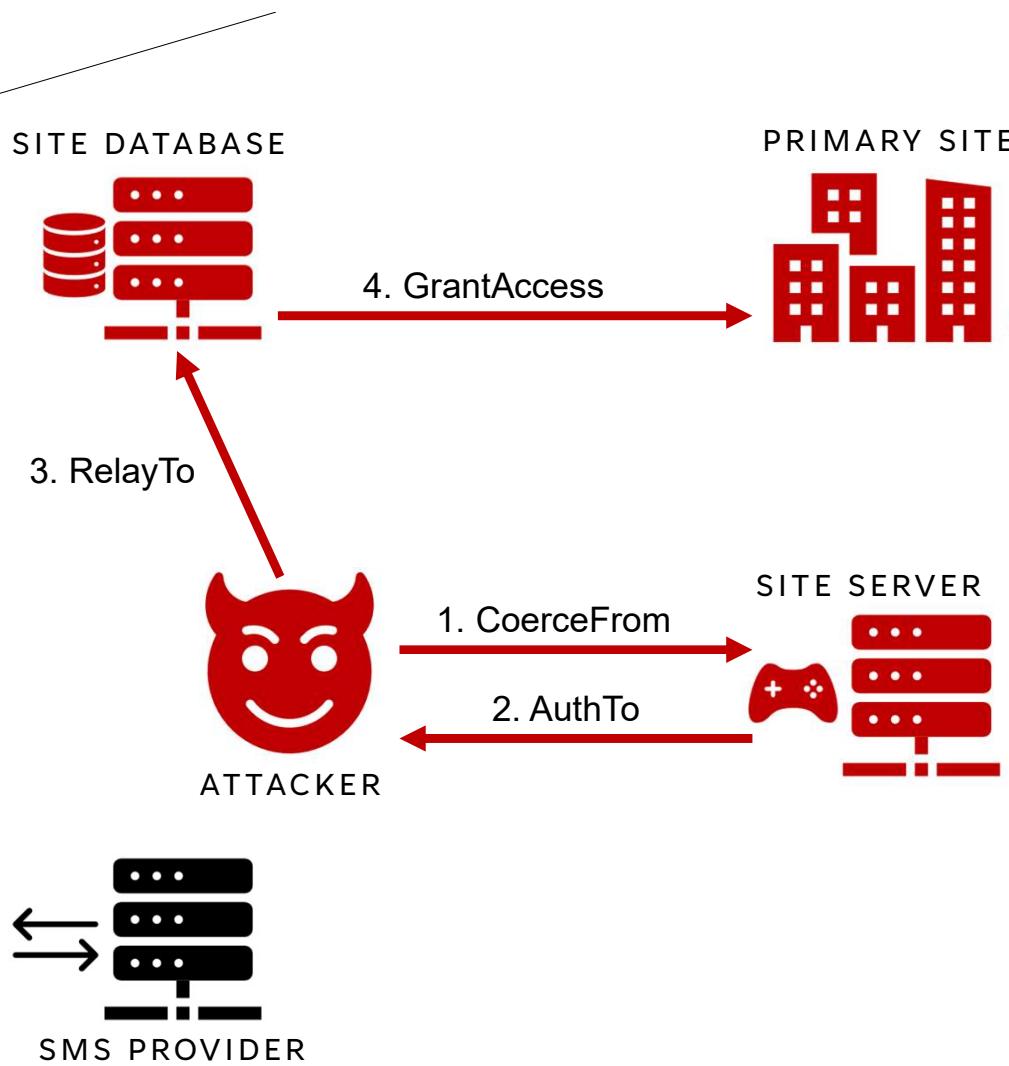
SMS PROVIDER

# TAKEOVER-1

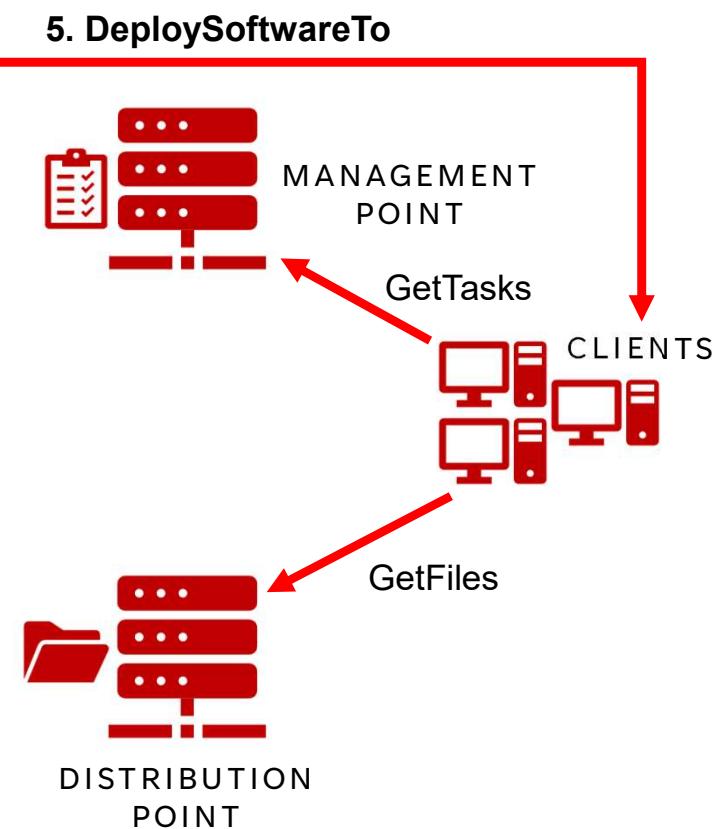


## TAKEOVER-1





## TAKEOVER-1



# TAKEOVER-1



SITE-SERVER - Remote Desktop

Microsoft Configuration Manager (Connected to PS1, Aperture Science - SITE-SERVER.APERTURE.LOCAL)

Home

Add User or Group Create Saved Searches Search

! One or more Azure AD app secrets used by Cloud Services have expired. Renew to avoid service disruptions. [Renew expired secret key](#)

1/1

Administration Overview Updates and Servicing Hierarchy Configuration Cloud Services Site Configuration Client Settings Security Assets and Compliance Software Library Monitoring Administration Community

Administrative Users 1 items

Search current node

Icon	Account Name	Account Display Name	Security Roles
User icon	APTURE\labadmin		"Full Administrator"

Ready

Type here to search

9:30 PM 1/29/2026

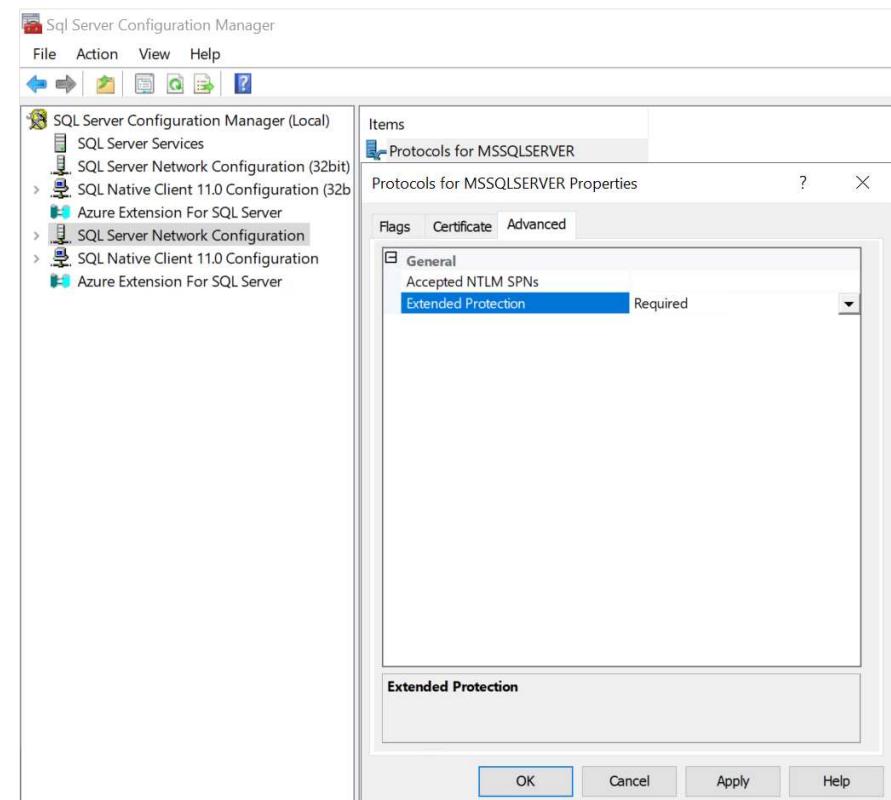
# TAKEOVER-1 REMEDIATION

## Require Extended Protection On Remote Site Databases

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

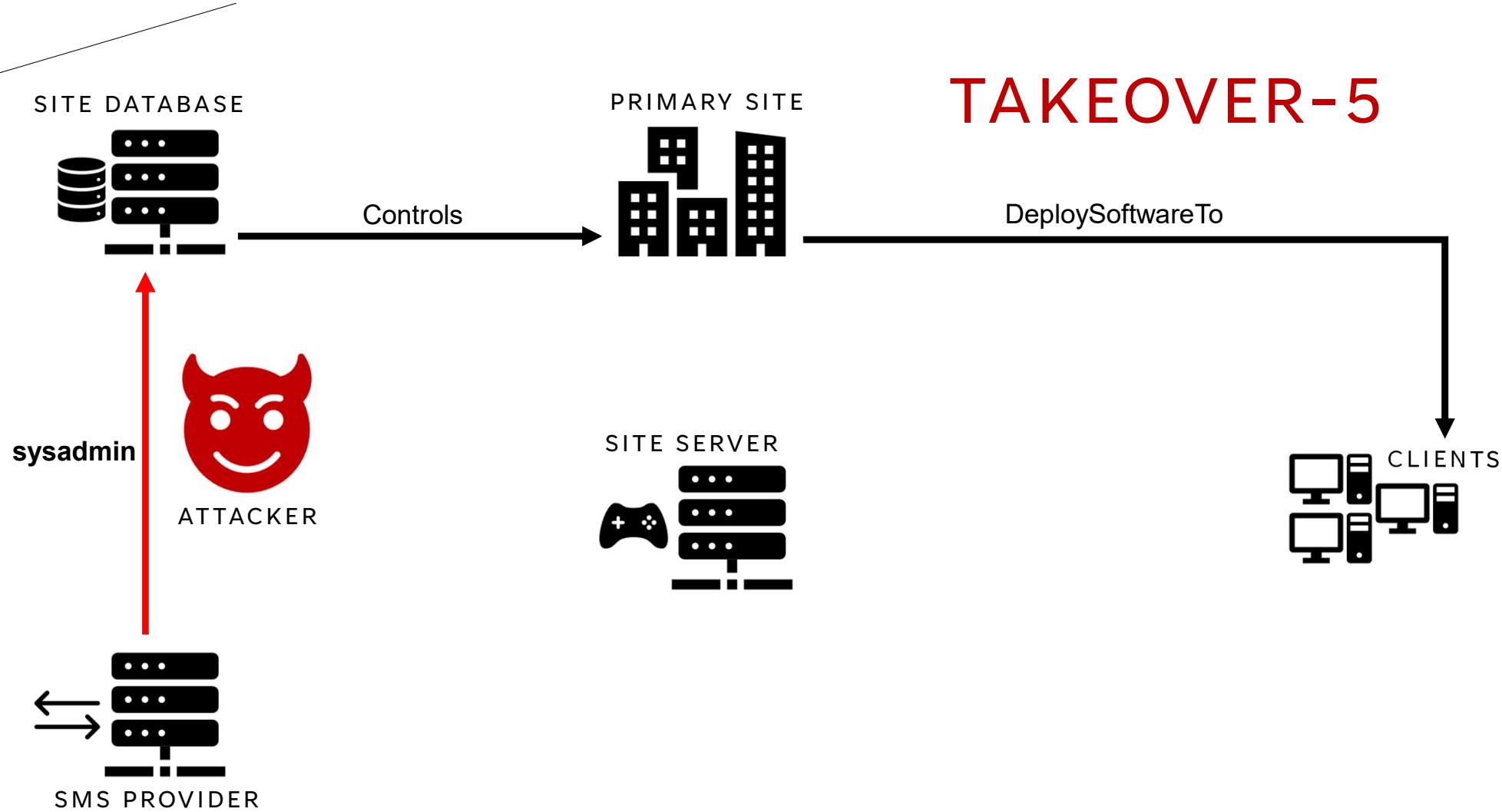
**Setting to “Allowed” will not prevent NTLM relay attacks if the coerced client doesn’t support channel binding**



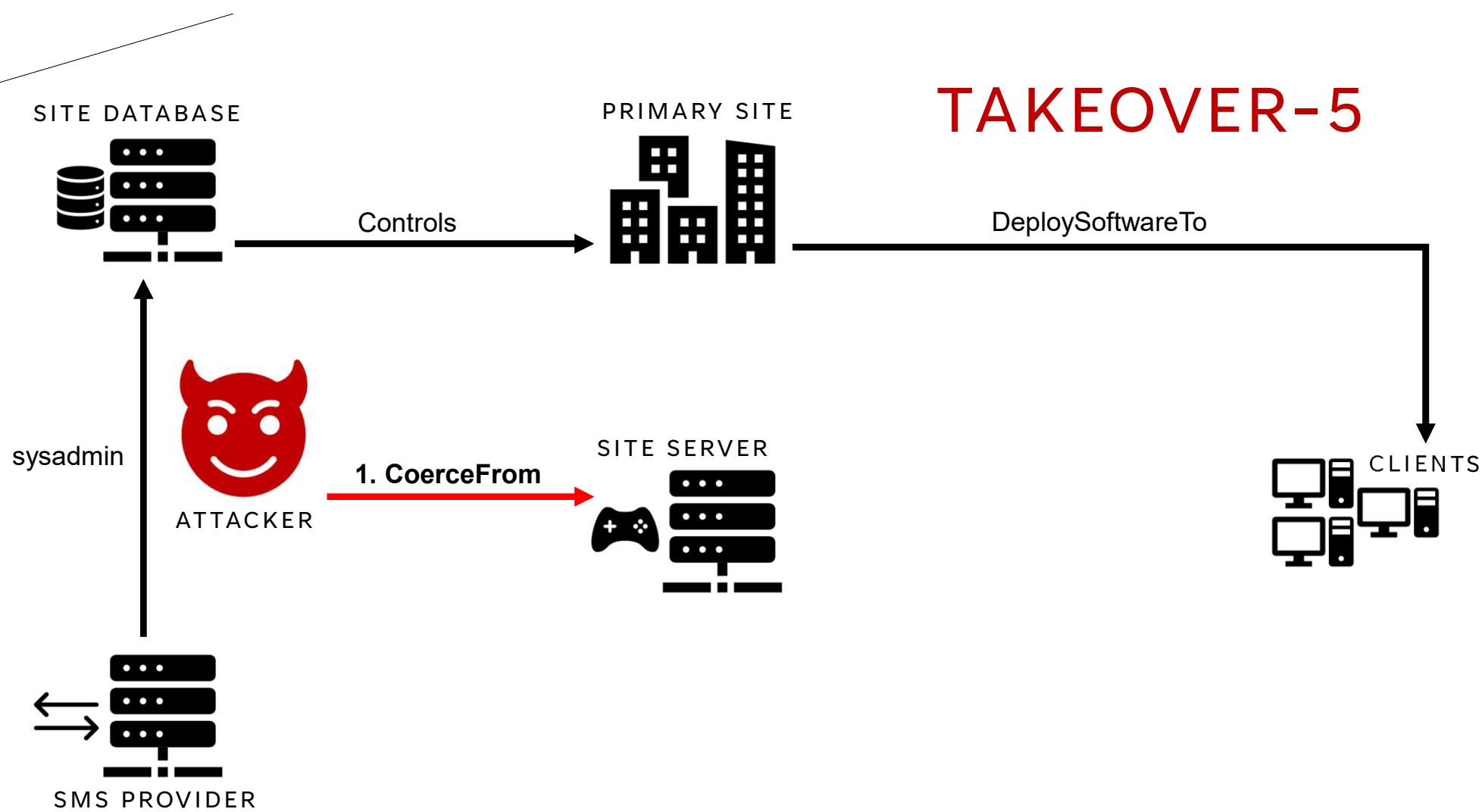
# TAKEOVER-5



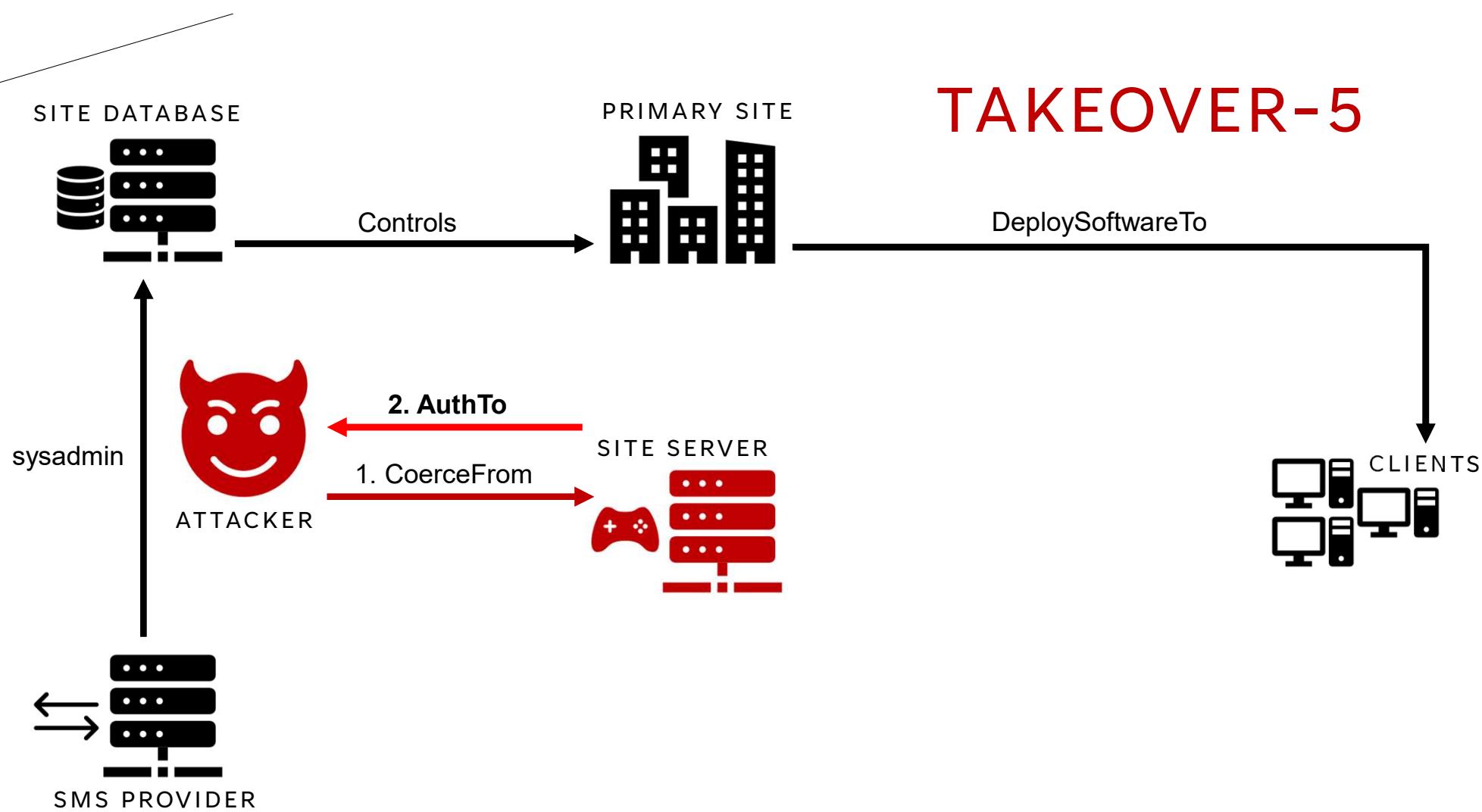
## TAKEOVER-5



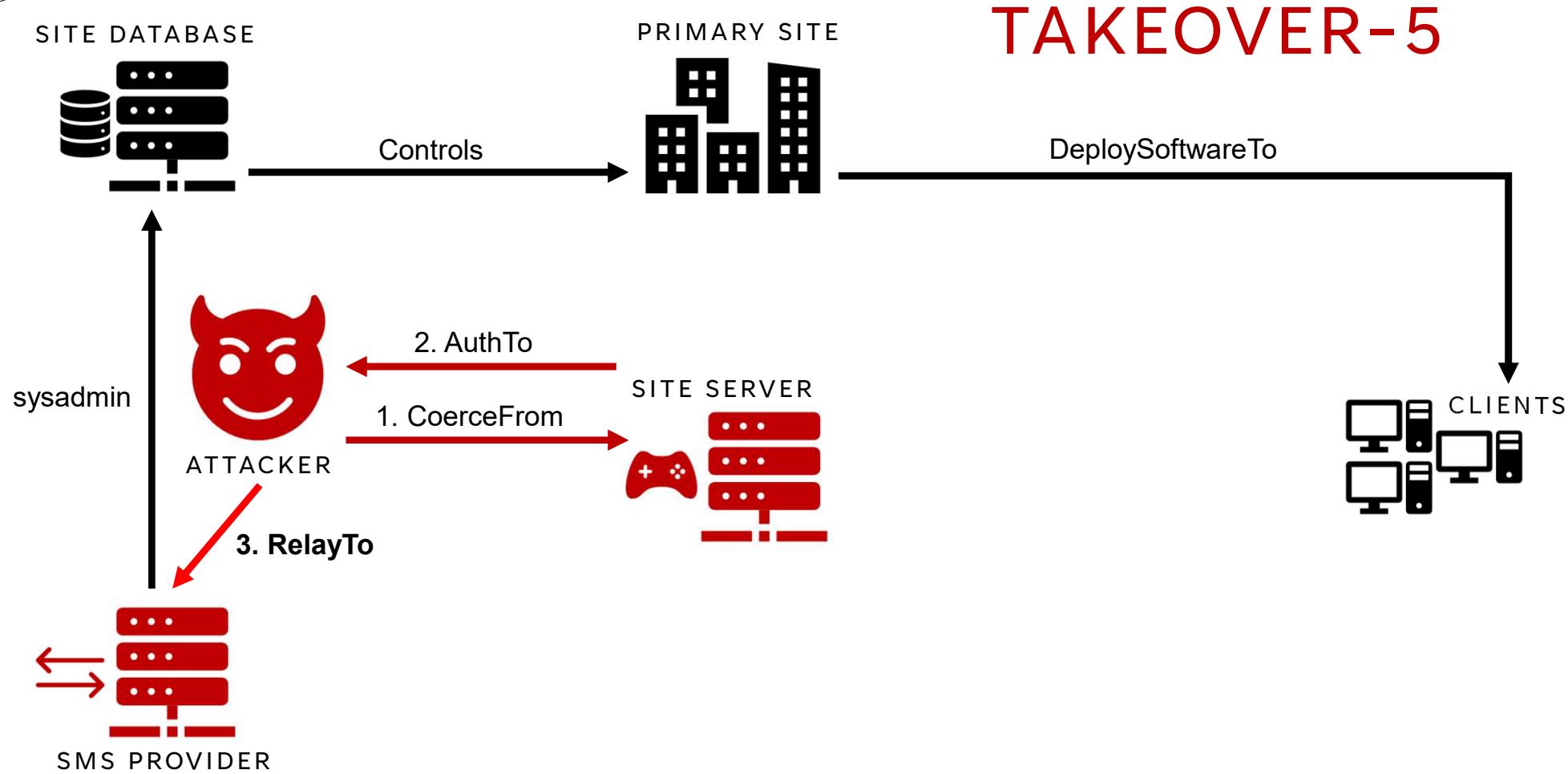
## TAKEOVER-5



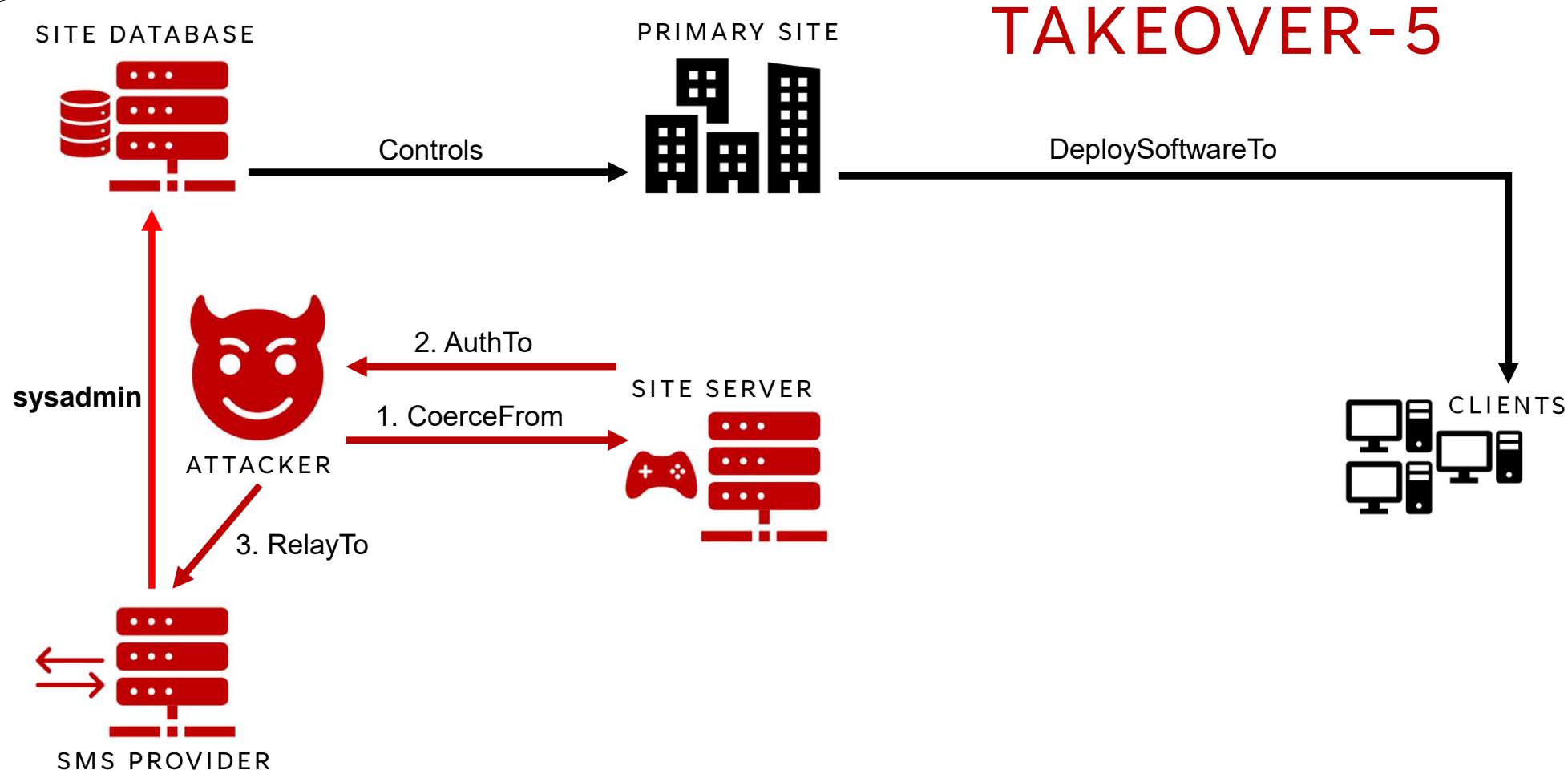
## TAKEOVER-5



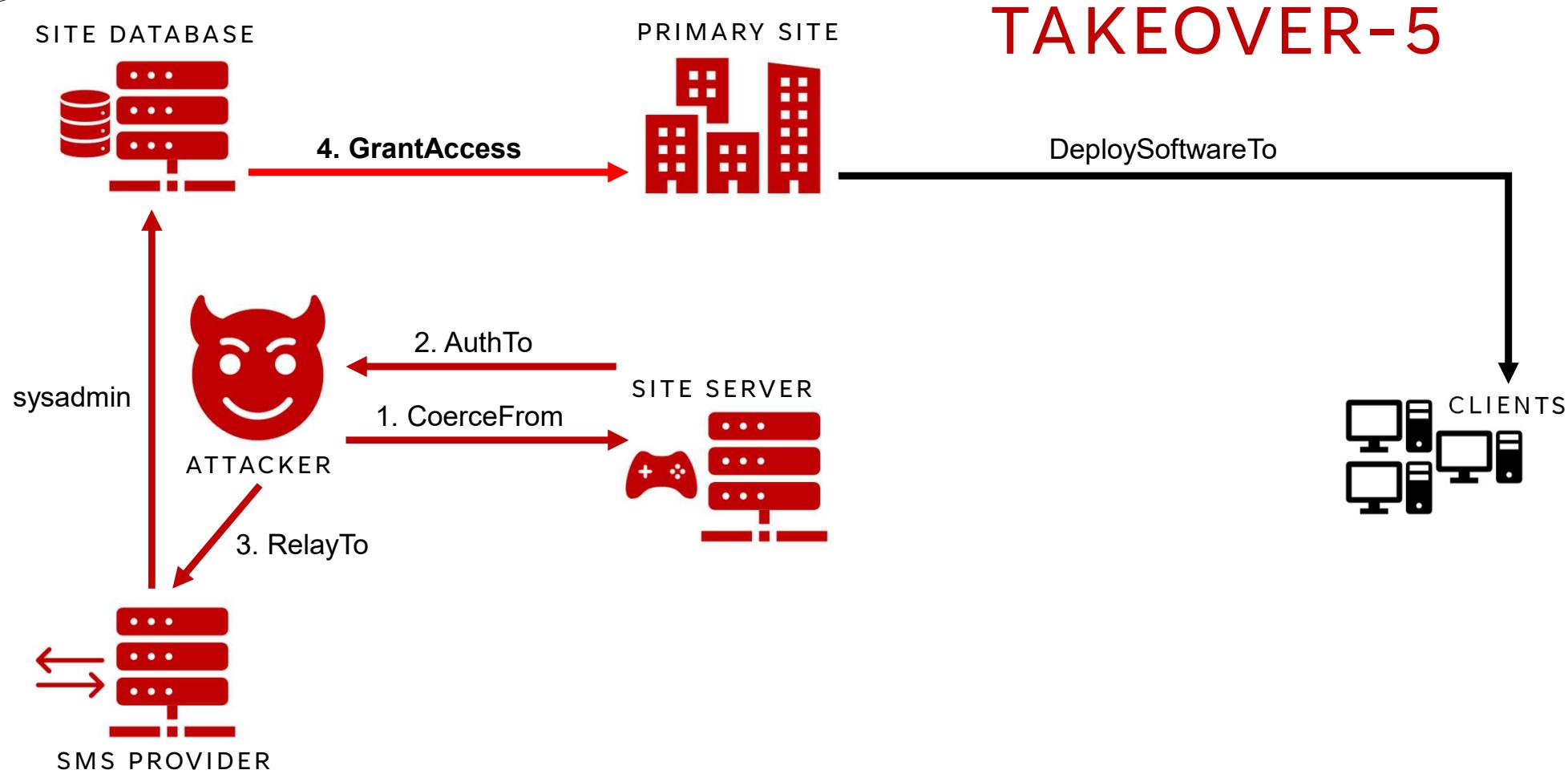
## TAKEOVER-5



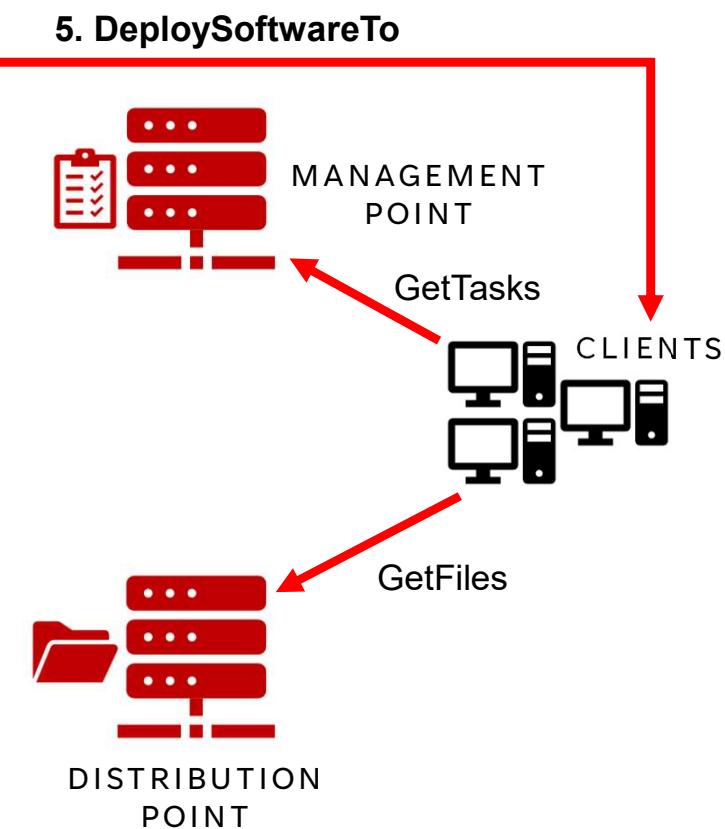
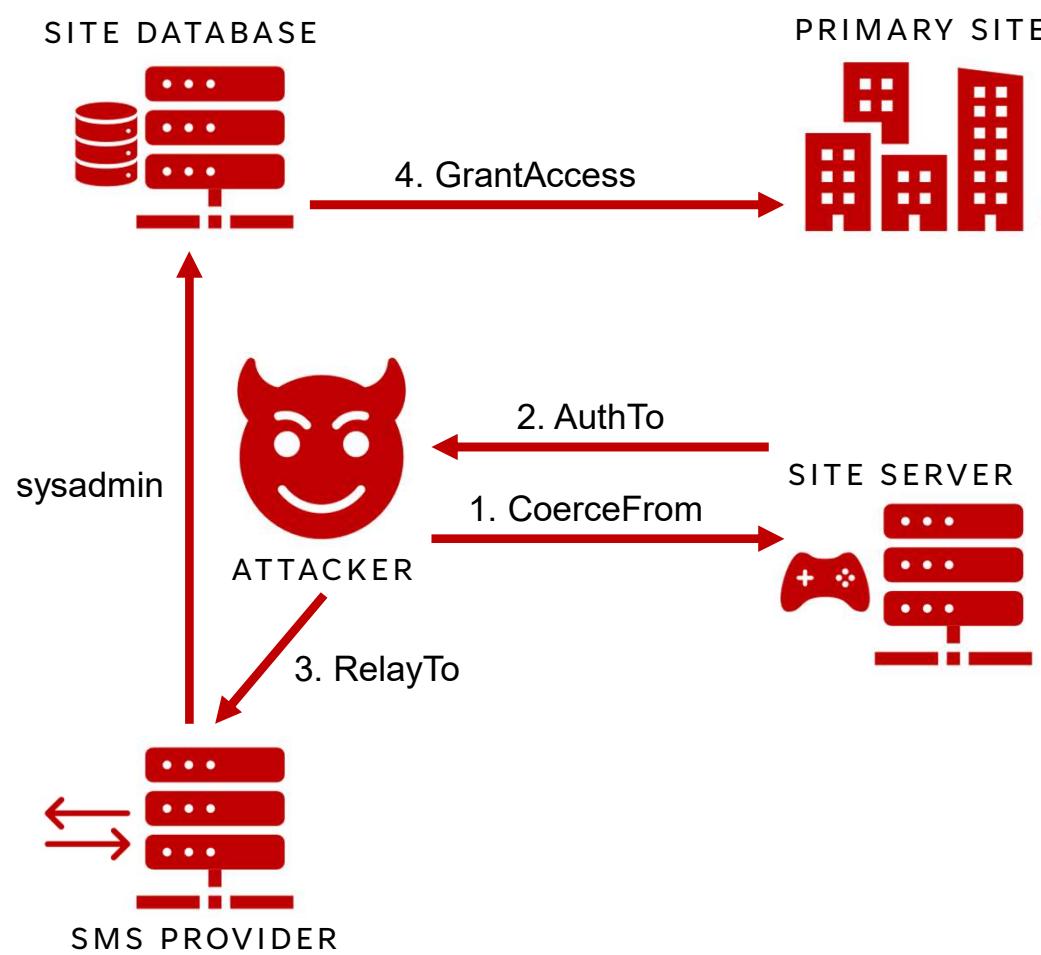
## TAKEOVER-5



## TAKEOVER-5



## TAKEOVER-5



# TAKEOVER-5



SITE-SERVER - Remote Desktop

Microsoft Configuration Manager (Connected to PS1, Aperture Science - SITE-SERVER.APERTURE.LOCAL)

Home

Add User or Group    Saved Searches

Create    Search

! One or more Azure AD app secrets used by Cloud Services have expired. Renew to avoid service disruptions. [Renew expired secret key](#)

1/1

Administration    \ Administration > Overview > Security > Administrative Users

Administrative Users 0 items

Search current node

Icon	Account Name	Account Display Name	Security Roles
User icon	APTURE\labadmin		"Full Administrator"

Icon   Account Name   Account Display Name   Security Roles

APTURE\labadmin   "Full Administrator"

Administration

- Overview
- Updates and Servicing
- Hierarchy Configuration
- Cloud Services
- Site Configuration
- Client Settings
- Security

Assets and Compliance

Software Library

Monitoring

Community

Ready

Type here to search

7:47 PM  
1/29/2026

# TAKEOVER-5 REMEDIATION

- Only host the SMS Provider role on the site server

OR

- **Upgrade** to Configuration Manager **v2509**, which denies NTLM authentication by default



# BLOODHOUND

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



# BLOODHOUND

Attack path management for:

- Active Directory
- Azure AD / Entra ID

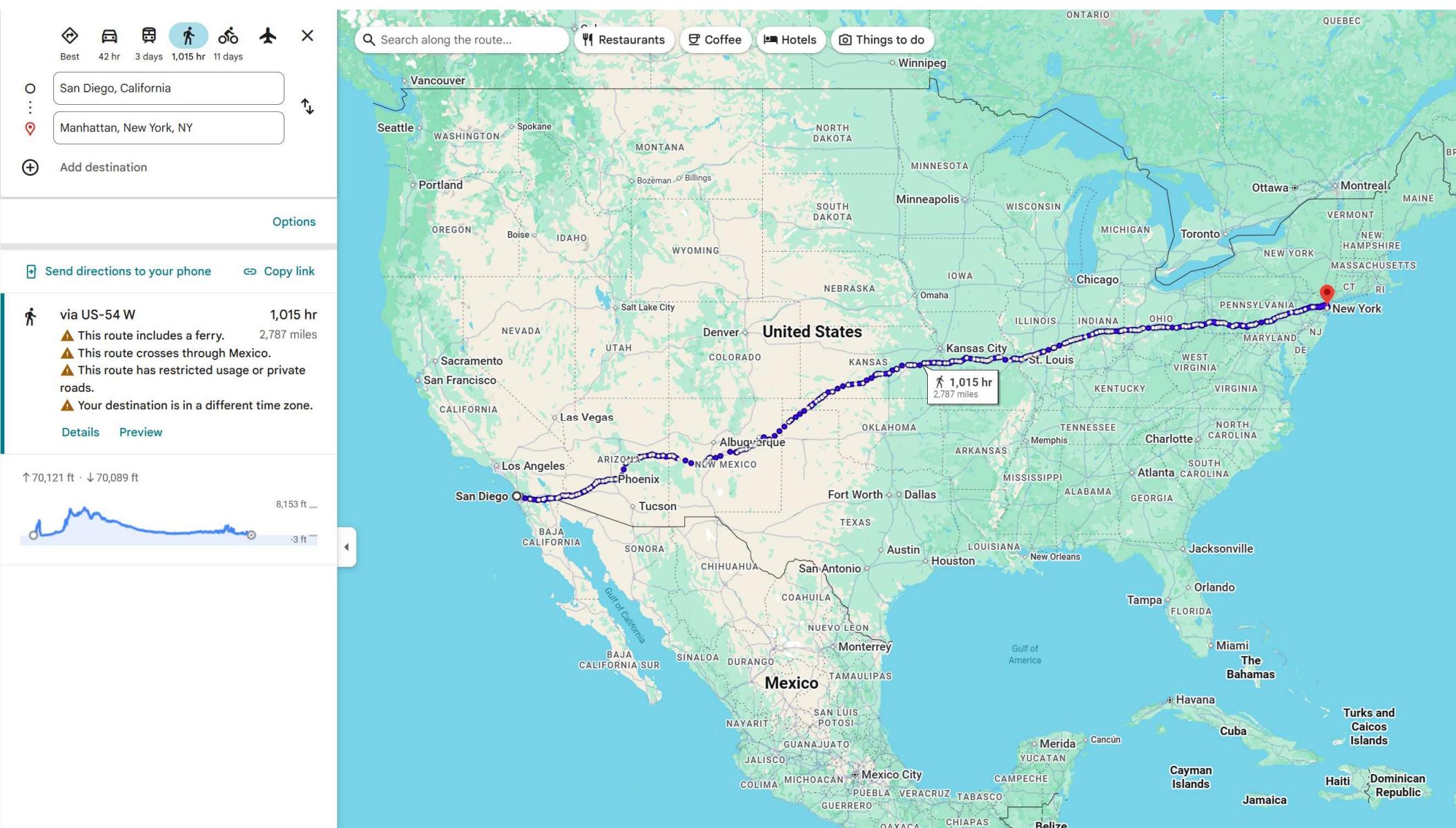
<https://bloodhound.specterops.io/>

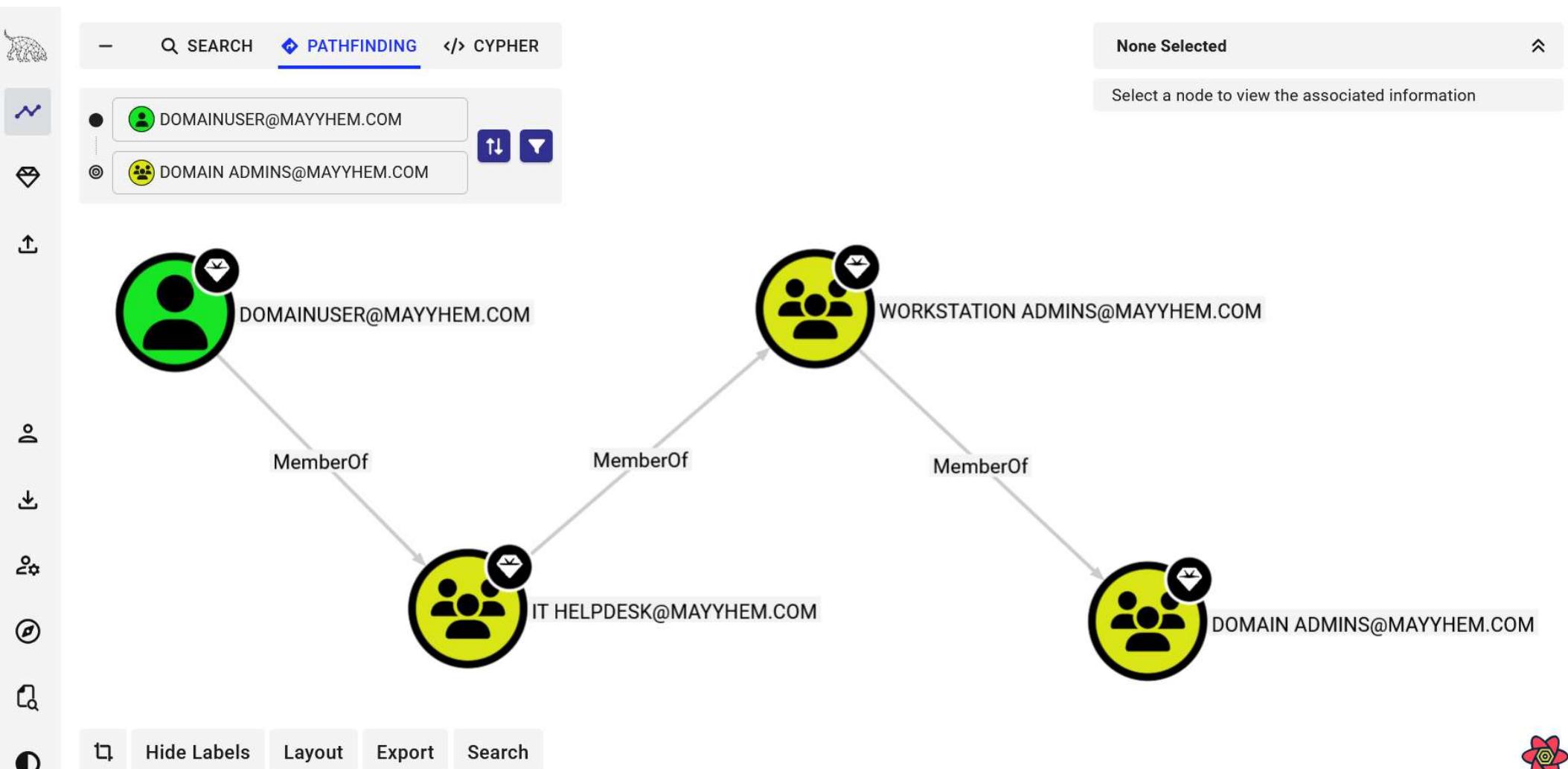


# BLOODHOUND

- 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/>







# OPENGRAPH

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



# BLOODHOUND

Attack path management for:

- Active Directory
- Azure AD / Entra ID
- All the things!

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

# OpenGraph Library

▼ 1Password

 **1PassHound**

▼ Ansible

 **AnsibleHound**

▼ Active Directory (AD)

 **ADAttributeHound**

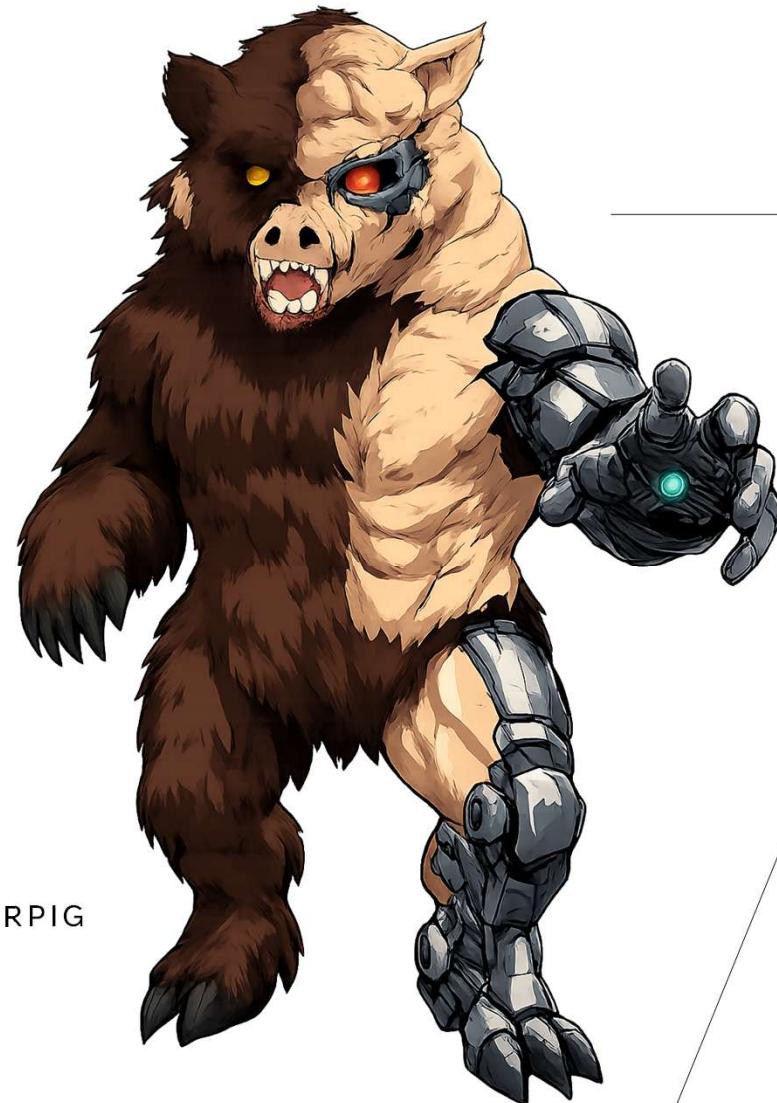


Unfortunately...  
The name  
**SCCMHOUND** was  
already taken

# ConfigManBearPig

- A PowerShell 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](https://github.com/mayyhem/ConfigManBearPig)



**RECON: 6/7**

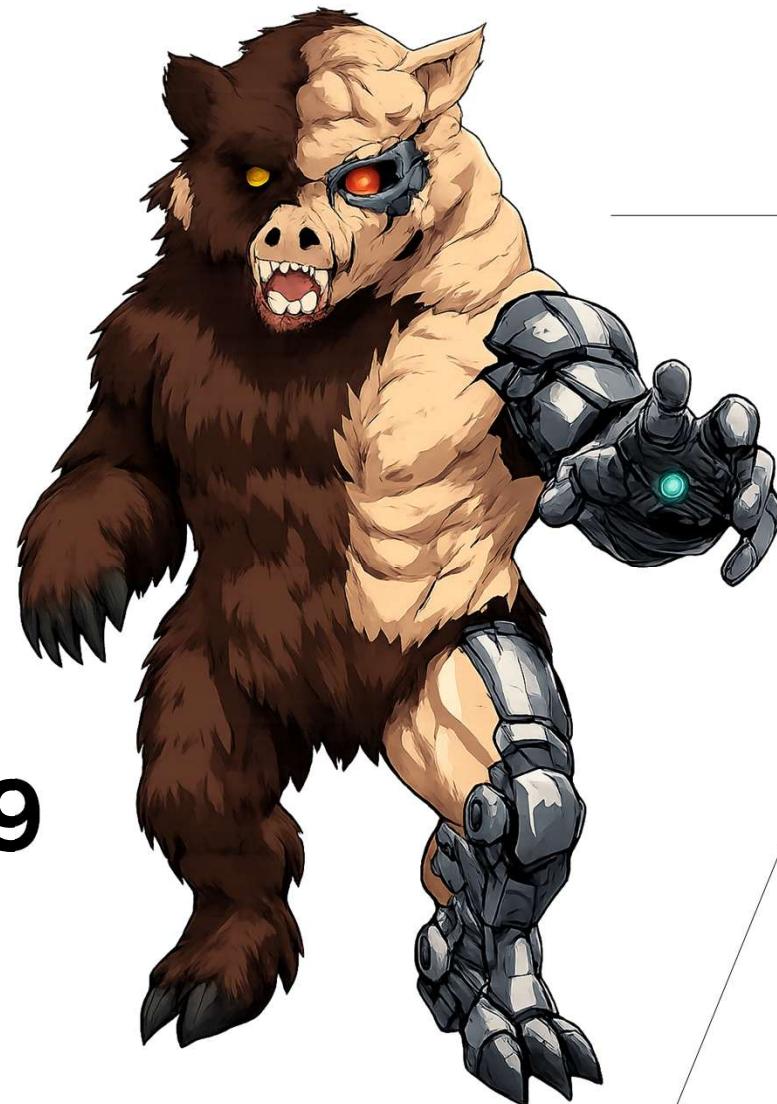
**CRED: 3/8**

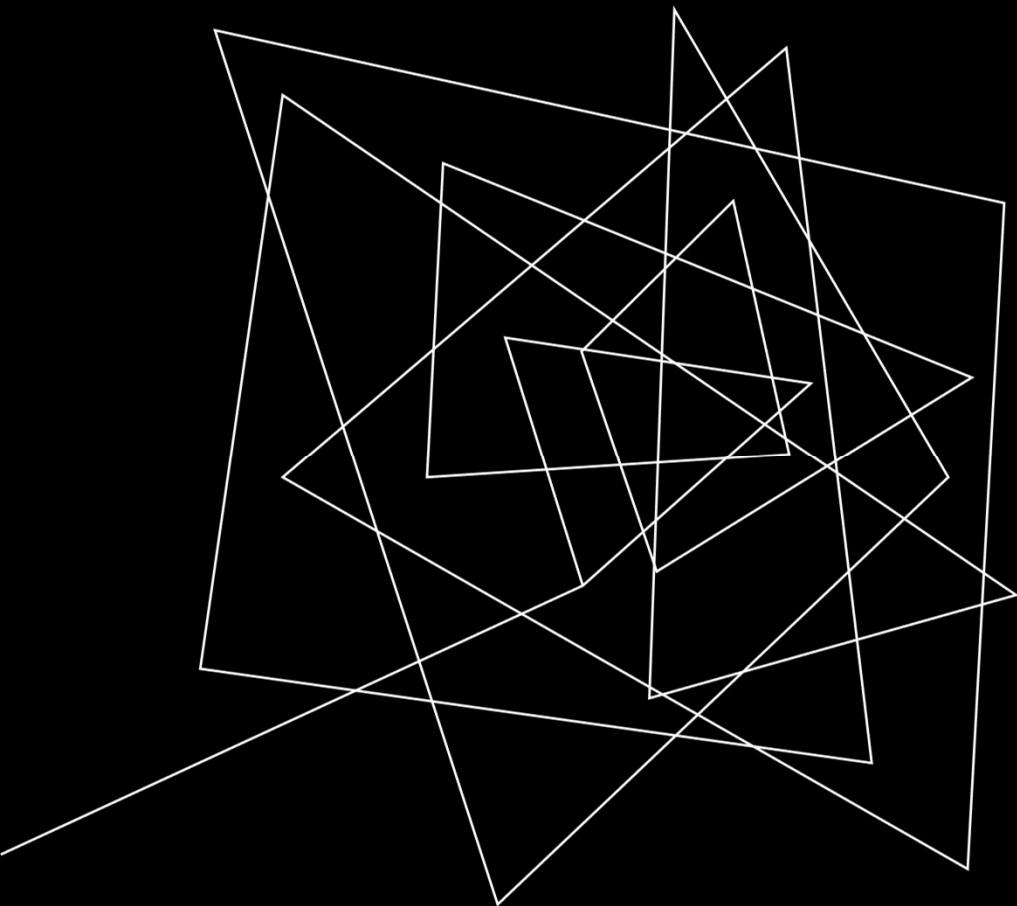
**COERCE: 0/2**

**ELEVATE: 1/5**

**TAKEOVER: 9/9**

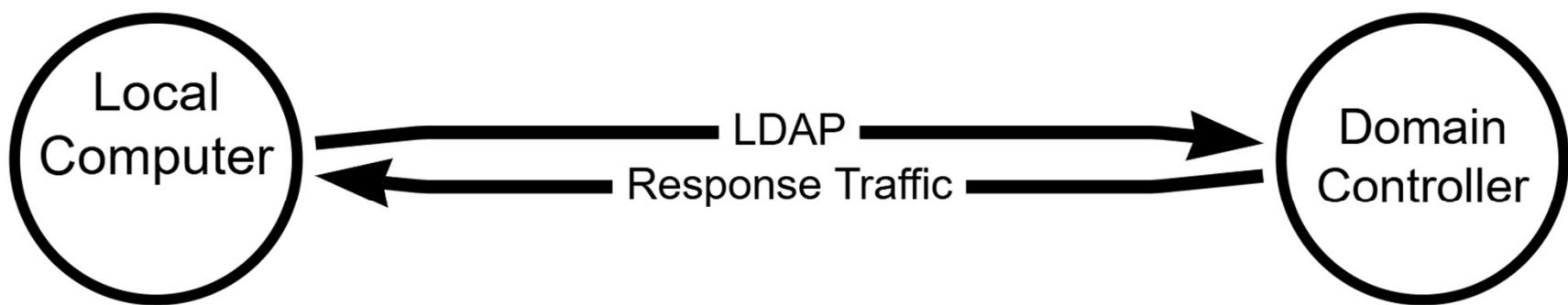
**EXEC: 2/2**





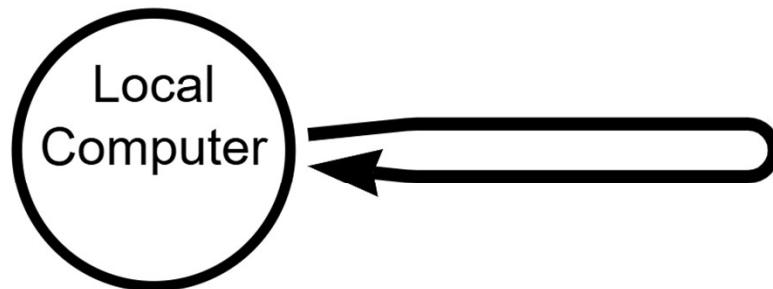
# COLLECTION RUN ONCE PHASES

# LDAP



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

# LOCAL

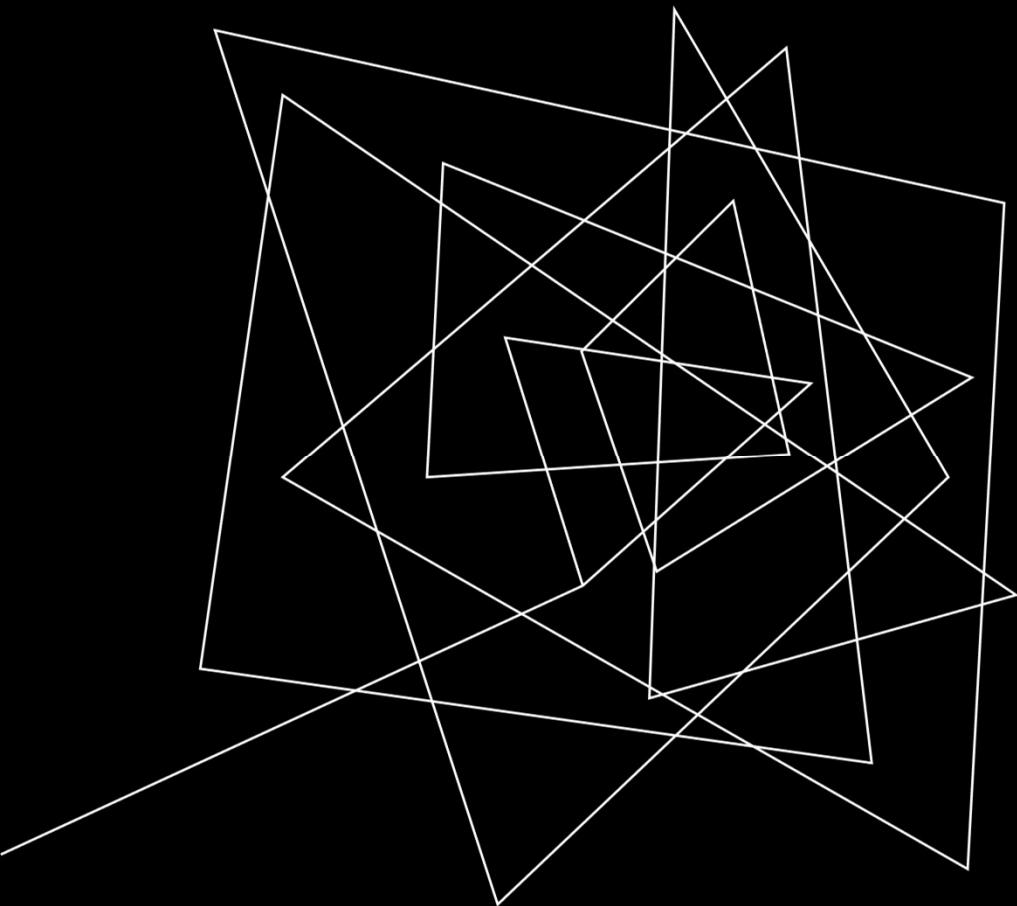


- Reads **client device logs** on disk
- Discovers:
  - management points, distribution points

# 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



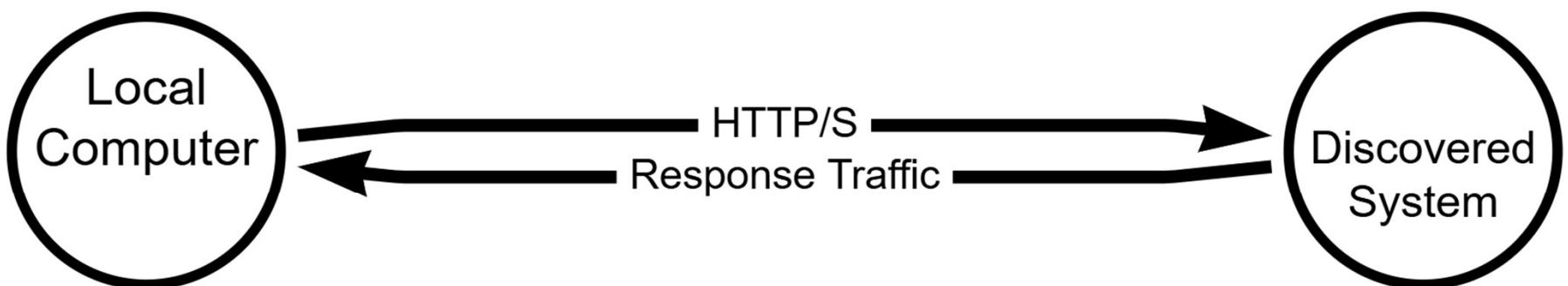
- Identifies **extended protection for authentication settings**
- Discovers:
  - site database servers, server and database principals

# ADMINSERVICE



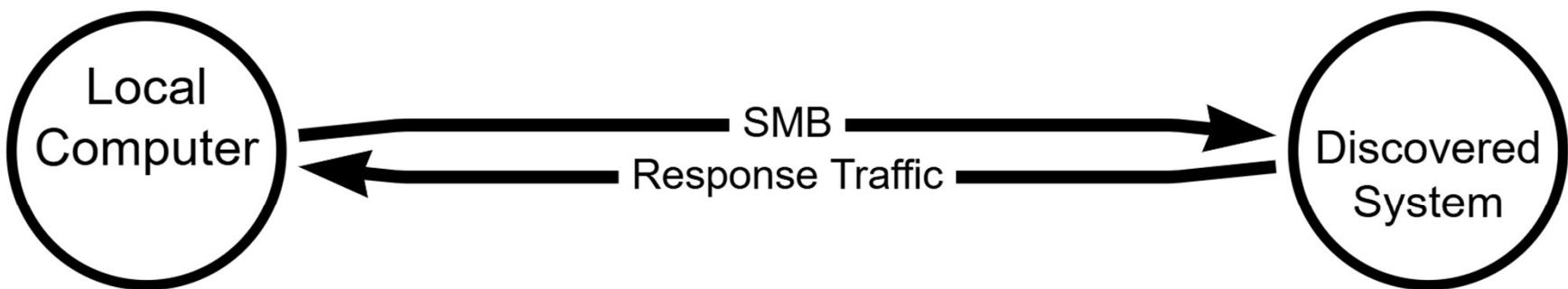
- Queries **AdminService** REST API on SMS Providers
- Discovers:
  - site systems, admin users/roles, client devices, logged in users

# HTTP

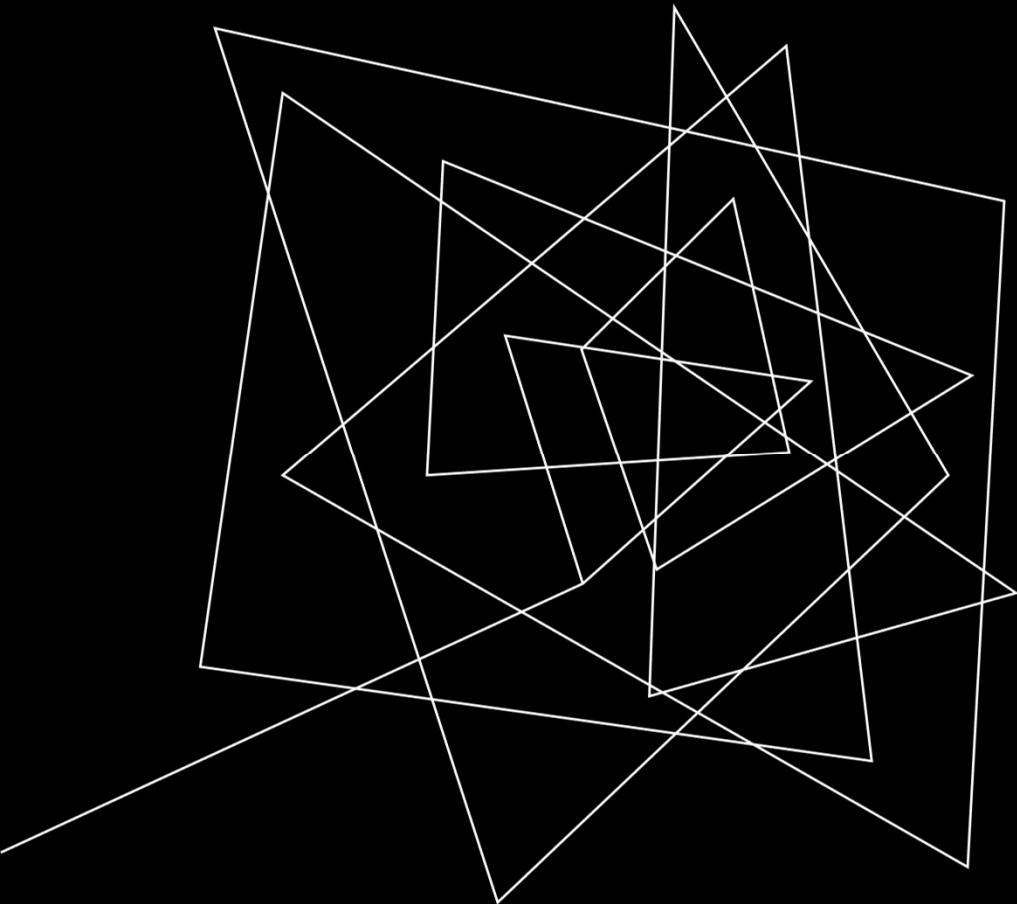


- Requests **known HTTP endpoints** and evaluates response codes
- Discovers:
  - management points, distribution points, SMS Providers

# SMB

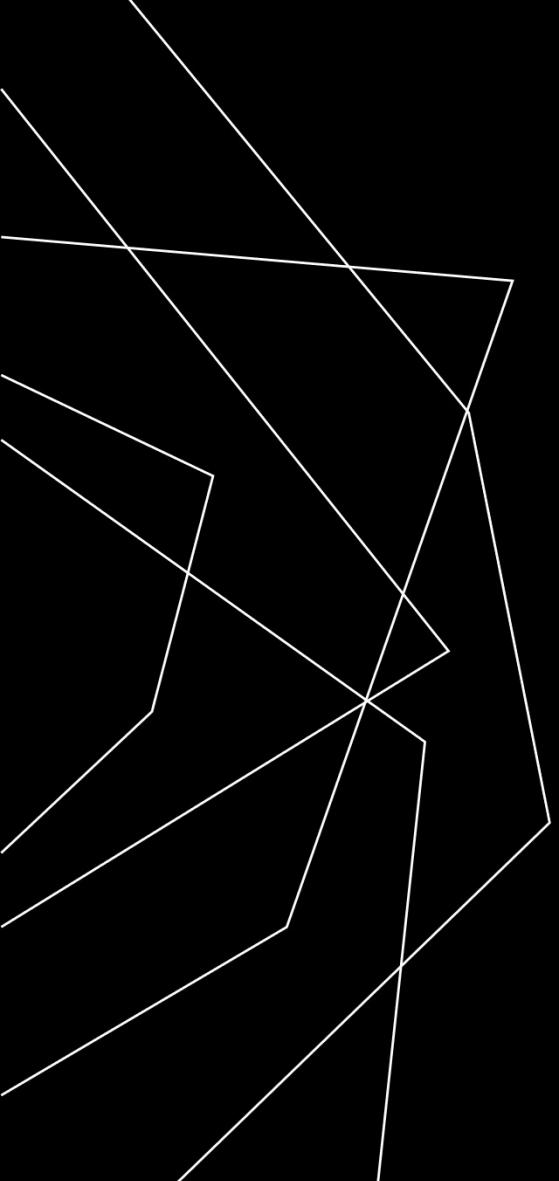


- Identifies **SMB signing** requirements
- Reads SMB **share names and descriptions**
- Discovers:
  - site servers, distribution points



## POST-PROCESSING

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



# WHAT IS MSSQL?

Microsoft SQL Server

# MSSQL ATTACK PATHS

ALLOW ACCESS TO DATABASES... AND MORE

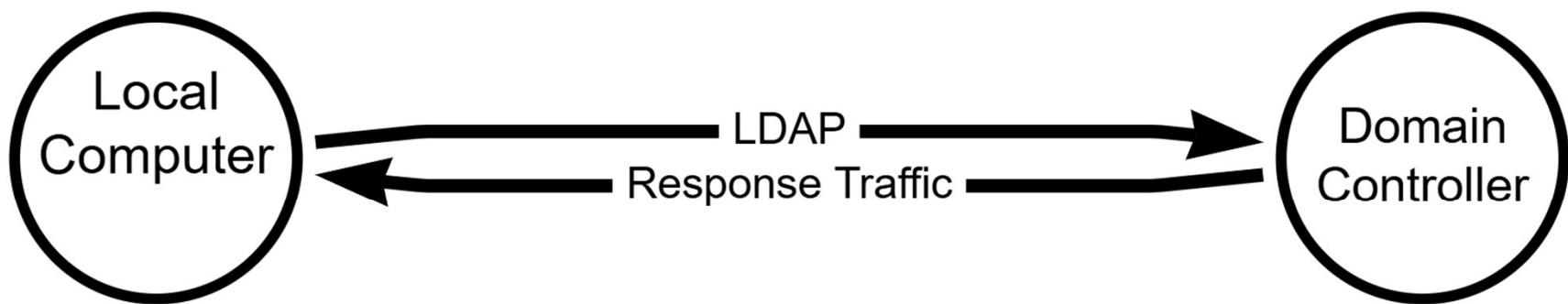
# MSSQLHound

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



[HTTPS://GITHUB.COM/SPECTEROPS/MSSQLHOUND](https://github.com/SPECTEROPS/MSSQLHOUND)

# LDAP

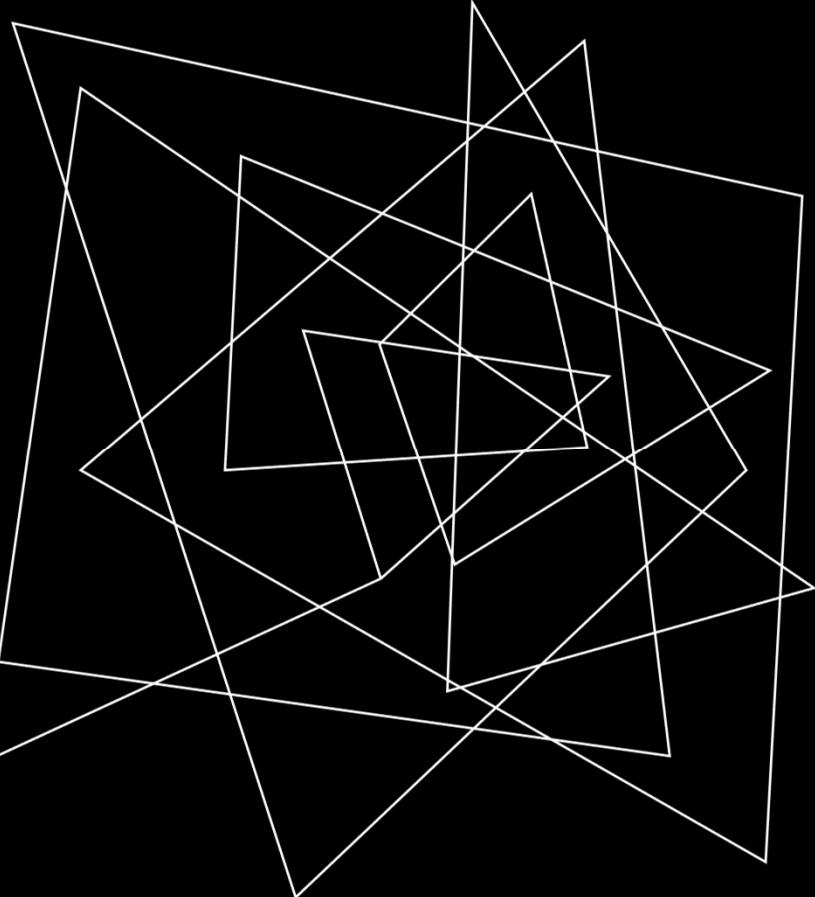


- Searches for computers with MSSQLSvc **service principal names**
- Discovers:
  - MSSQL hostnames, ports, and instance names

# MSSQL



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



## POST-PROCESSING

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



# GRAPHING ATTACK PATHS DEMO

# TO DO

---

- Optimize run duration and Cypher queries
- ConfigManBearPig
  - Port to Python (next week)
  - Abuse Info
  - DHCP/WMI/CMPivot collection
  - Add more existing/new attack techniques
- MSSQLHound
  - Port to Golang (in progress)
  - Recursive collection from linked databases
  - Database object collection (e.g., stored procedures/tables)



# THANK YOU!



**Chris Thompson**

X: @\_Mayyhem

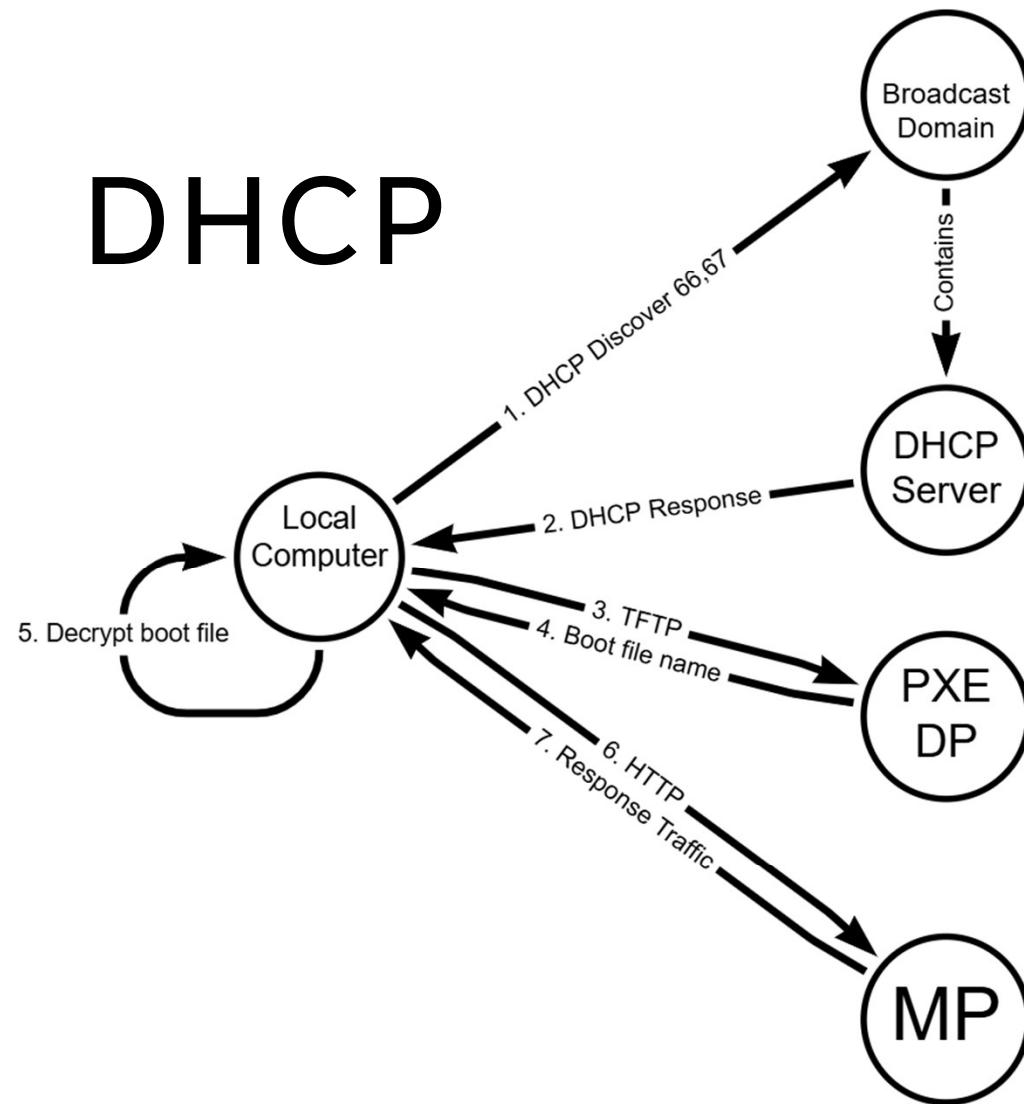
Slack: @Mayyhem

GitHub: Mayyhem

LinkedIn: x24

# DHCP

- Broadcast DHCP requests for TFTP server and PXE boot file name
- Downloads and decrypts media with blank passwords
- Discovers:
  - distribution points, management points



# CMPIVOT

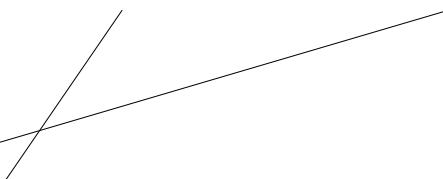


- Queries information from remote SCCM client devices
- Discovers:
  - user logon events, local Administrators group members

# WMI

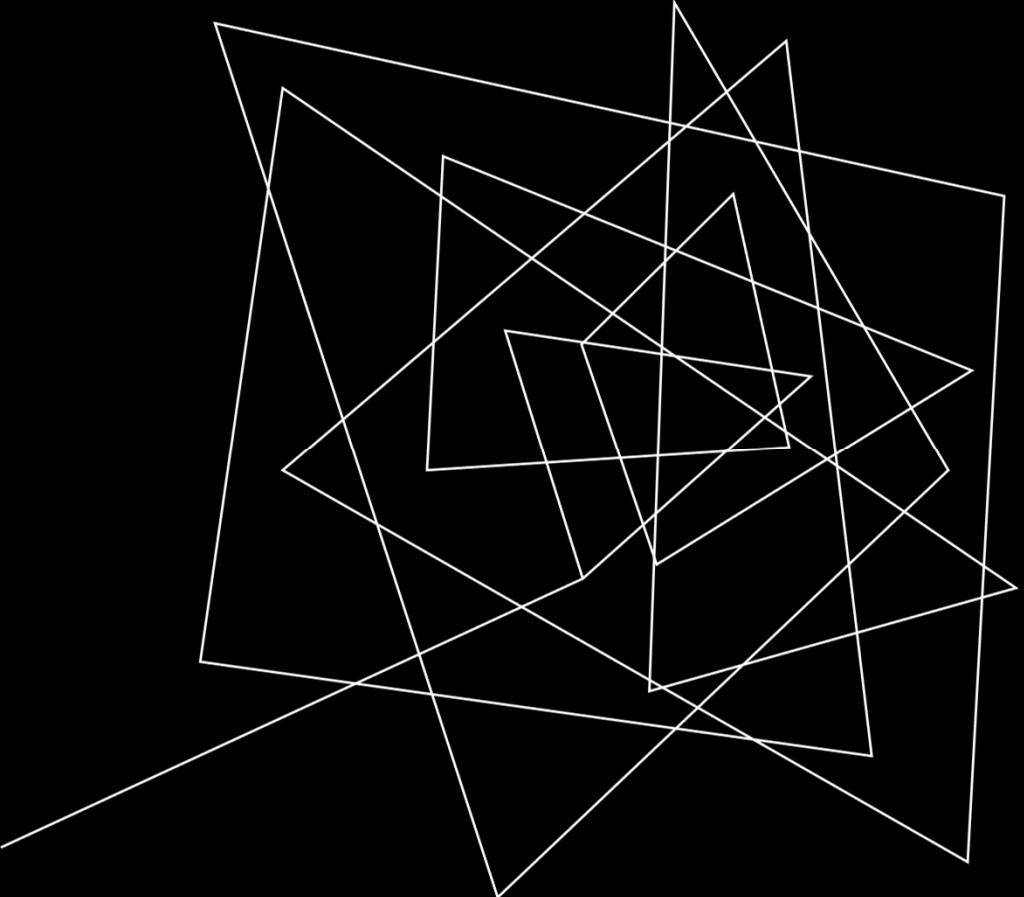


- Requires SCCM admin account
- Queries WMI classes on SMS Providers
- Discovers:
  - site systems, admin users/roles, client devices, logged in users



# USEFUL ARGUMENTS

- **EnableBadOpsec**
  - Produces `SCCM_HasNetworkAccessAccount`  
(executes CRED-3)
  
- **ShowCleartextCredentials**

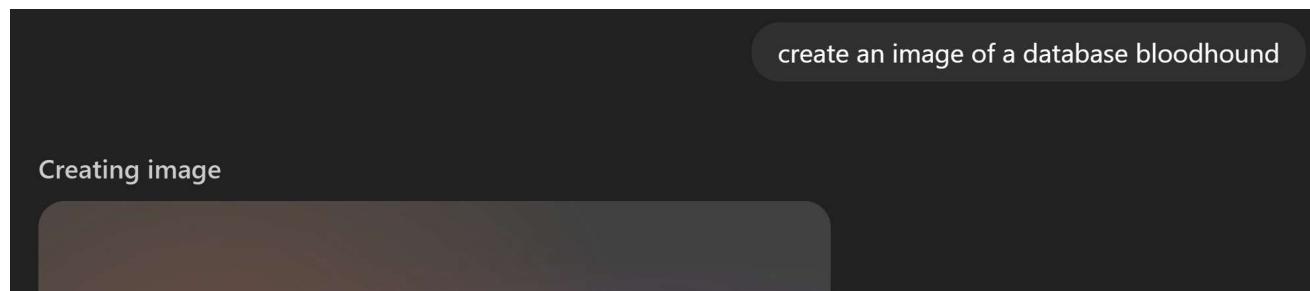


## FUTURE DEV

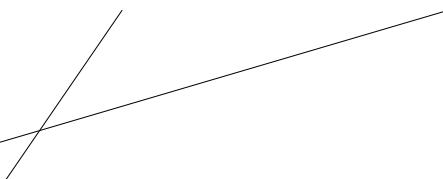
- Abuse info
- System management takeover
- Task sequences and collection variables
- Automatic client push
- MP relays
- DHCP/WMI/CMPivot

# MSSQLHound

- A PowerShell OpenGraph collector  
for MSSQL nodes and edges



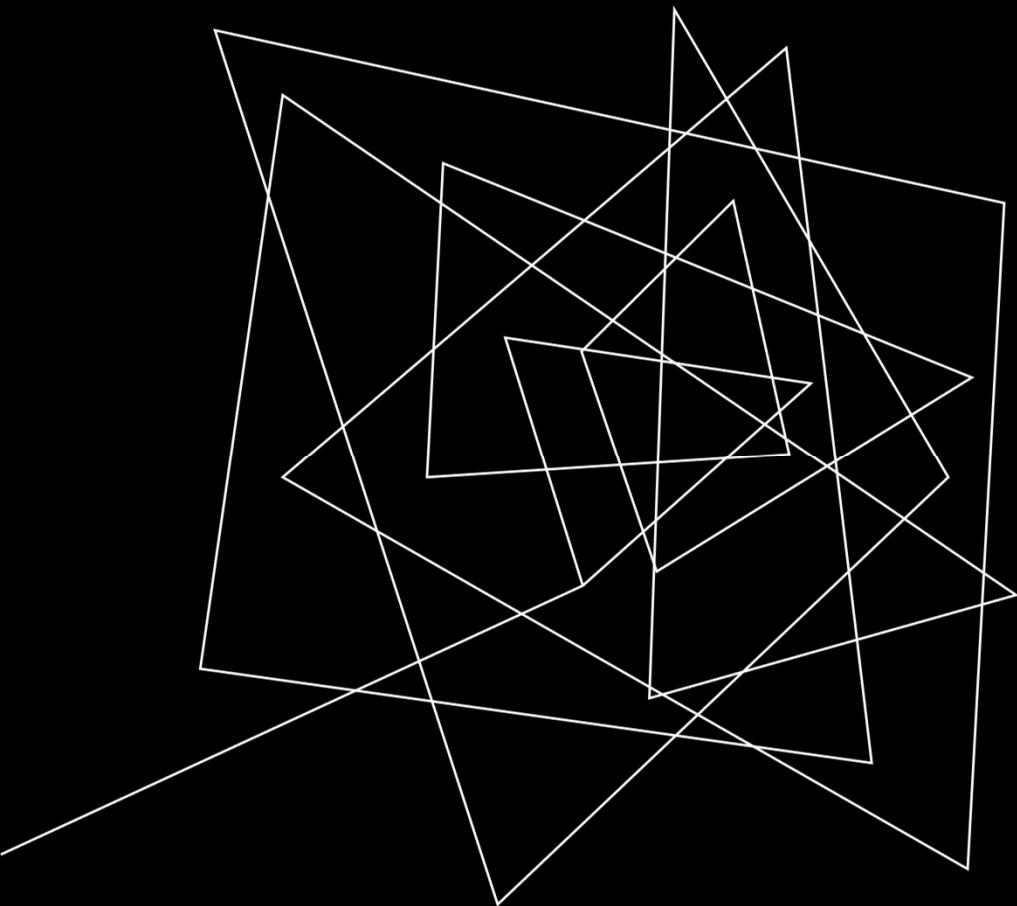
[HTTPS://GITHUB.COM/SPECTEROPS/MSSQLHOUND](https://github.com/SPECTEROPS/MSSQLHOUND)



# USEFUL ARGUMENTS

## - MakeInterestingEdgesTraversable

- MSSQL\_HasDBScopedCred
- MSSQL\_HasMappedCred
- MSSQL\_HasProxyCred
- MSSQL\_IsTrustedBy
- MSSQL\_LinkedTo
- MSSQL\_ServiceAccountFor



## FUTURE DEV

- Stored procedures
- Tables
- Collection over links  
(recursive)

- SEARCH ◆ PATHFINDING </> CYpher

DOMAINUSER



Hide Labels Layout Export Search

X DOMAINUSER

- Object Information

**Node Type:** User

**Object ID:**  
S-1-5-21-3242052782-1287495003-4091326449-1104

**ACL Inheritance Denied:** FALSE

**Admin Count:** FALSE

**AdminSDHolder Protected:** FALSE

**Allows Unconstrained Delegation:** FALSE

**Collection Source:** RemoteRegistry-CurrentUser

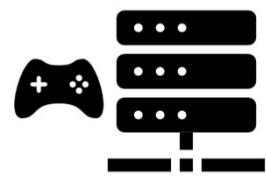
**Created:** 2025-11-25 14:43 EST (GMT-0500)

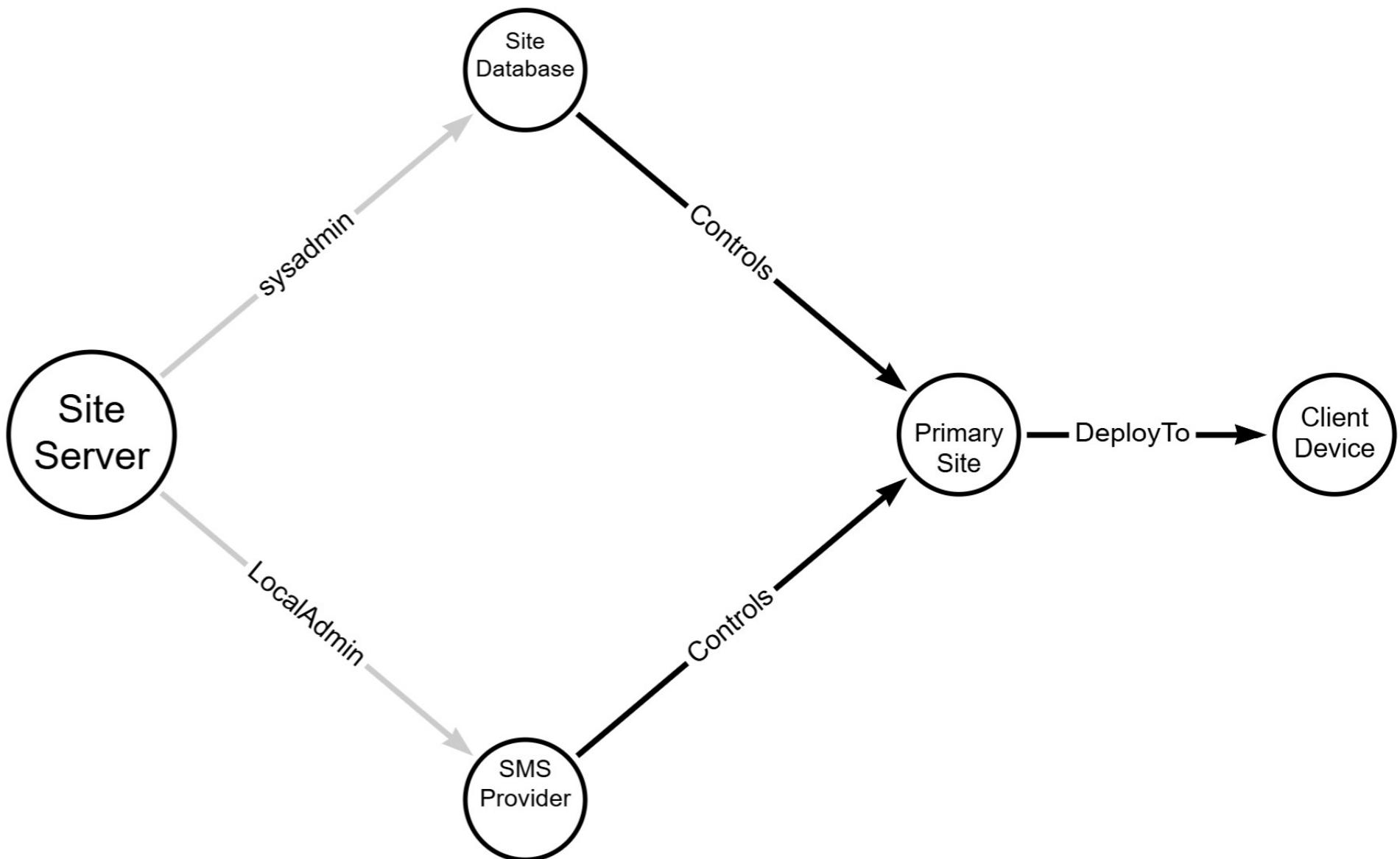
**Distinguished Name:**  
CN=domainuser,CN=Users,DC=mayhem,DC=com

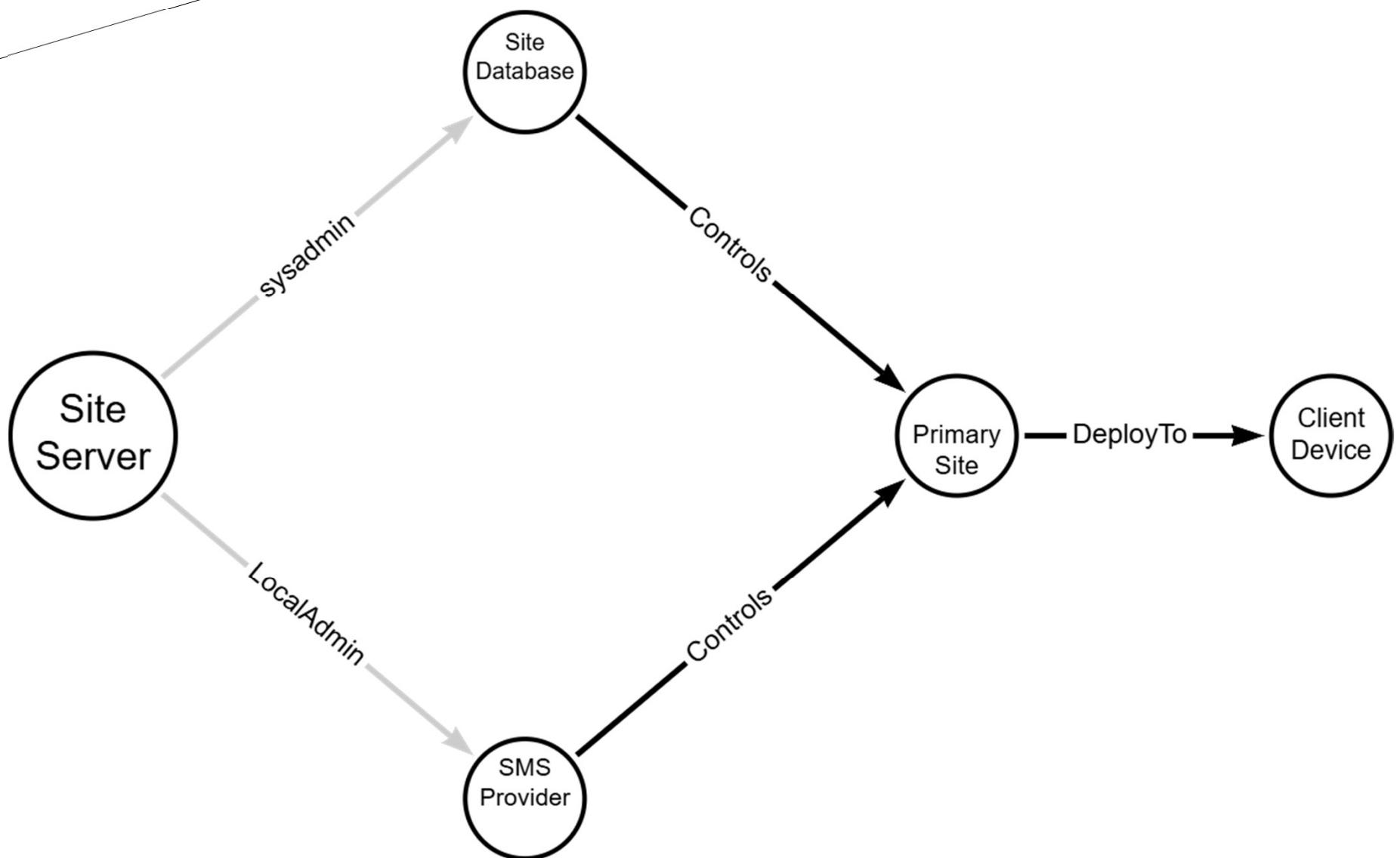
**Distinguished Name:**  
CN=DOMAINUSER,CN=USERS,DC=MAYYHEM,DC=COM

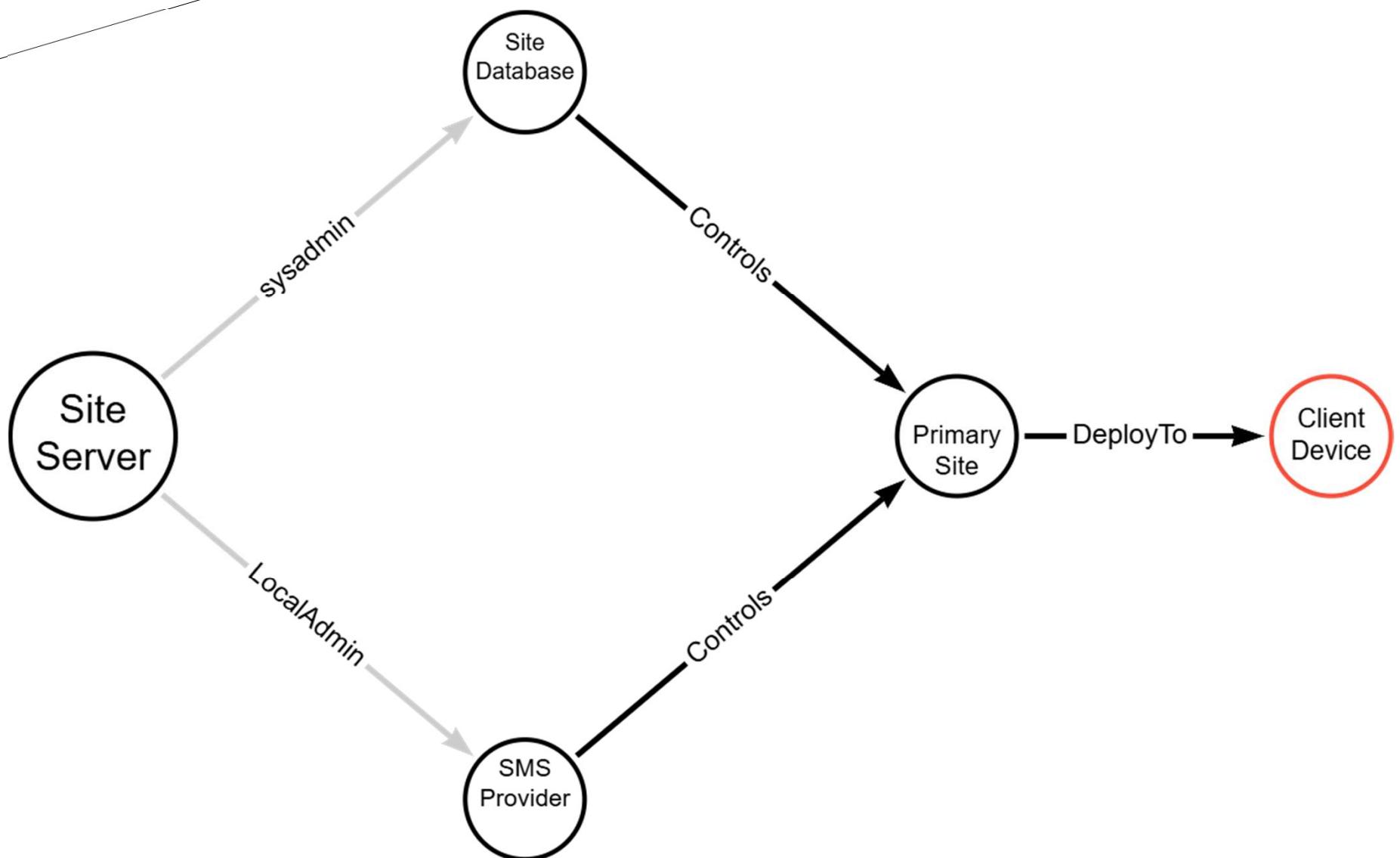
**Do Not Require Pre-Authentication:** FALSE

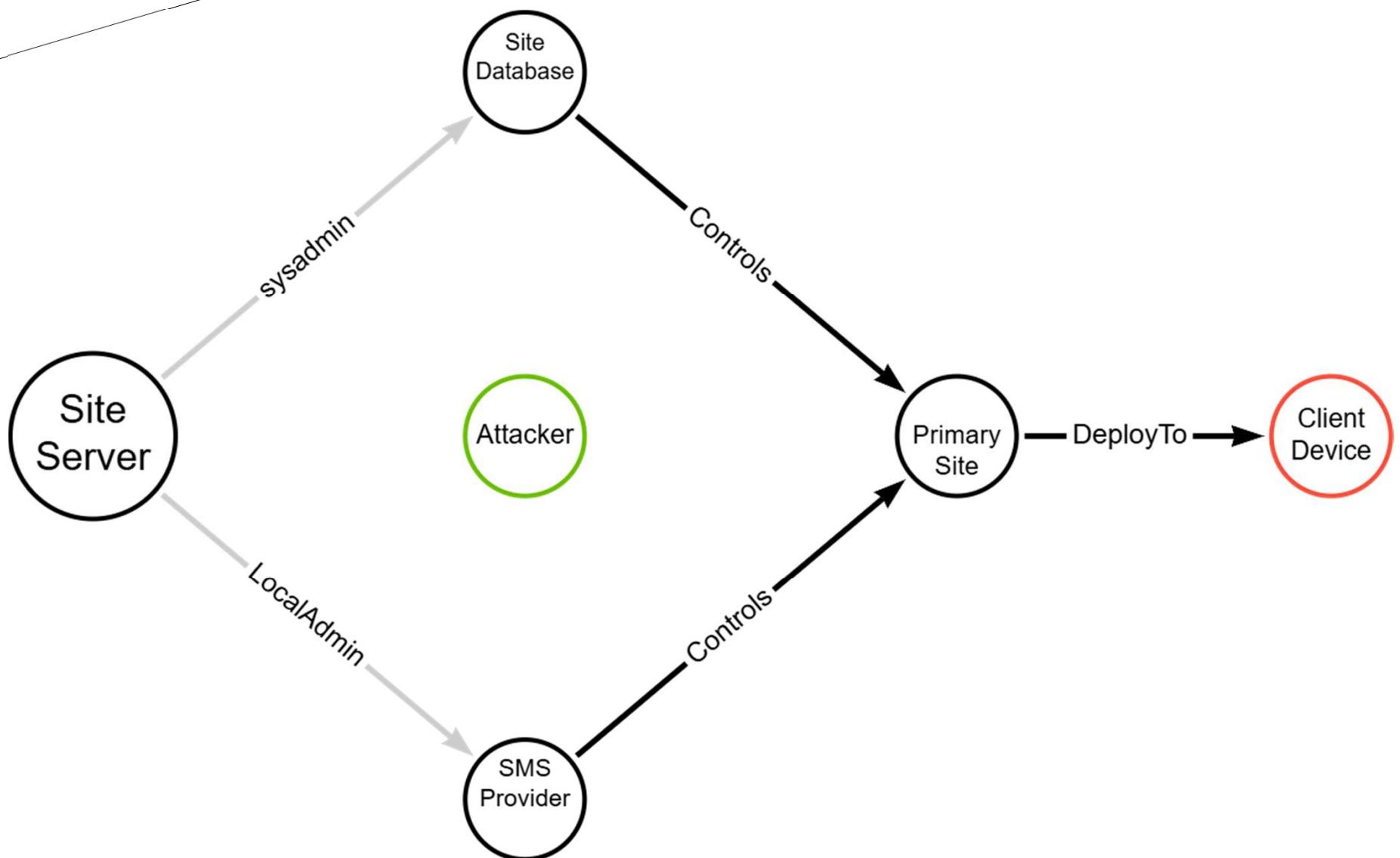


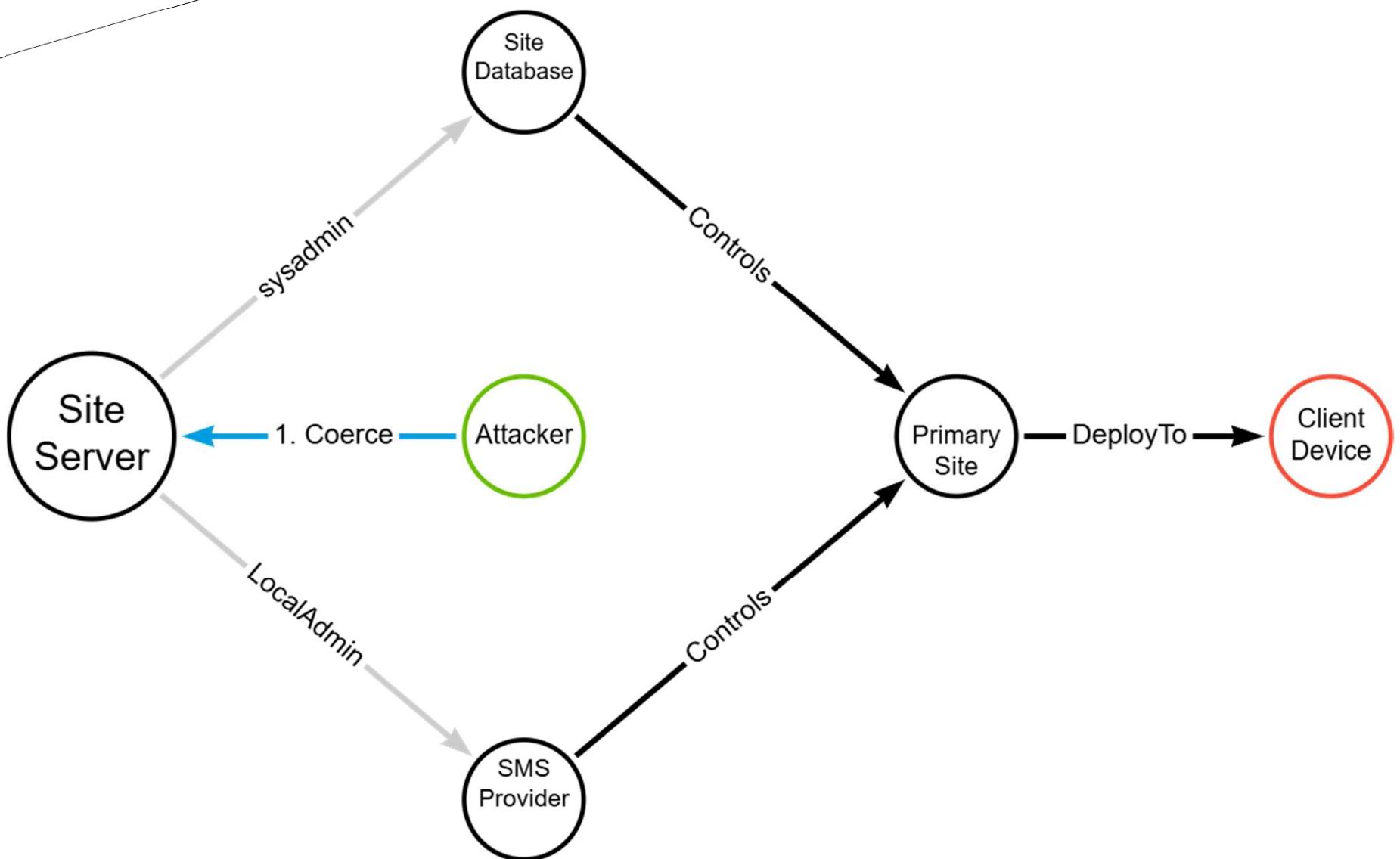


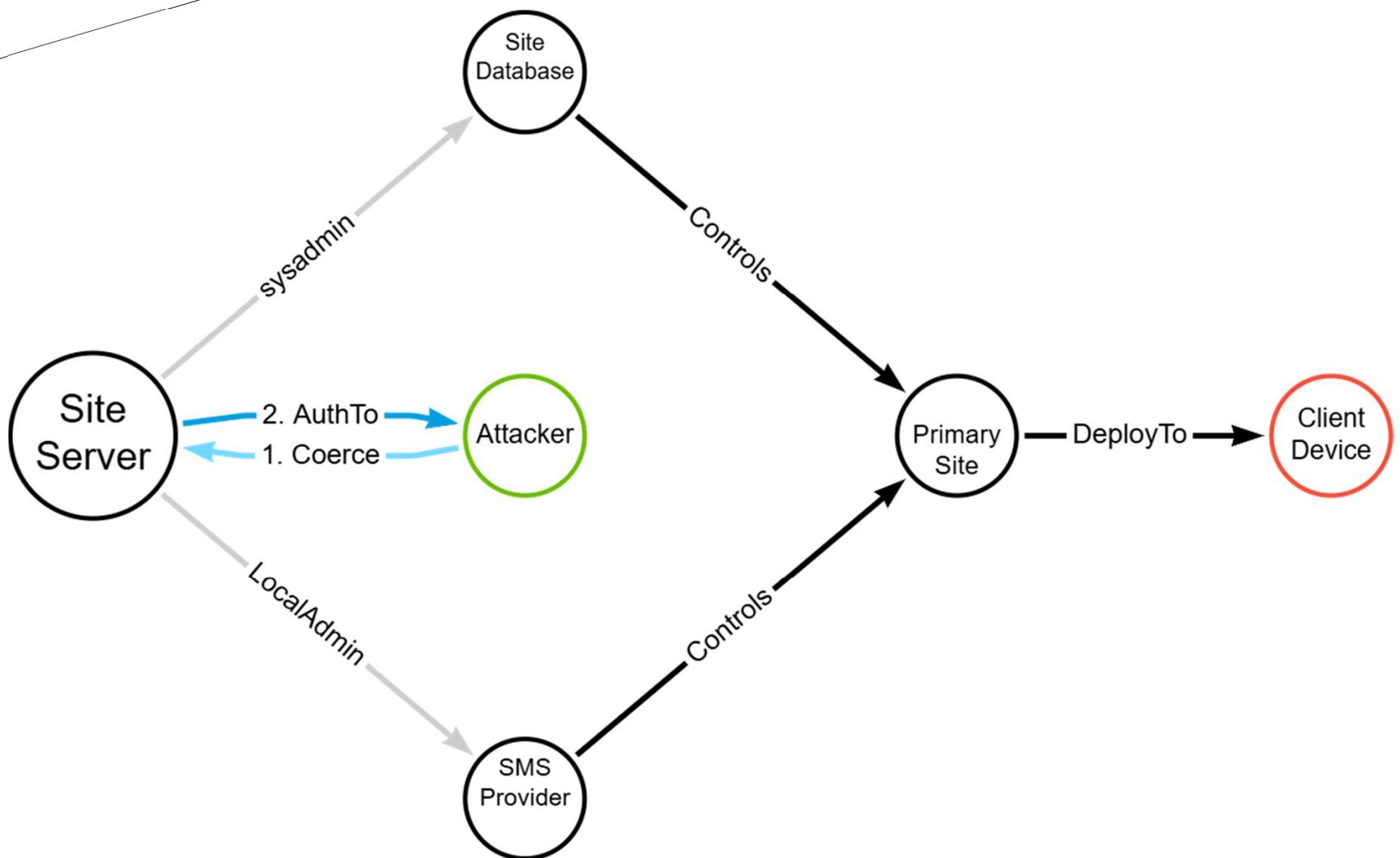


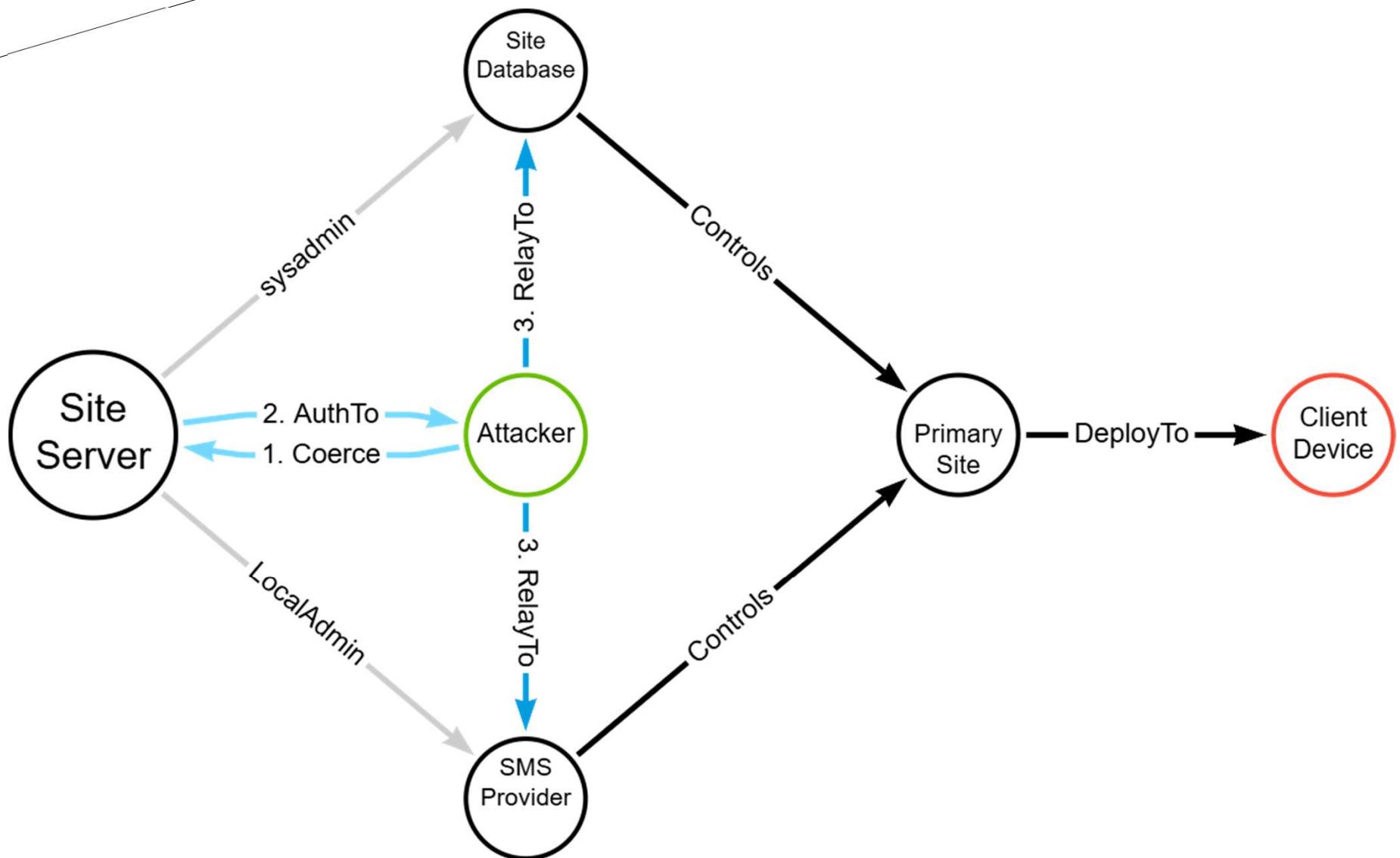


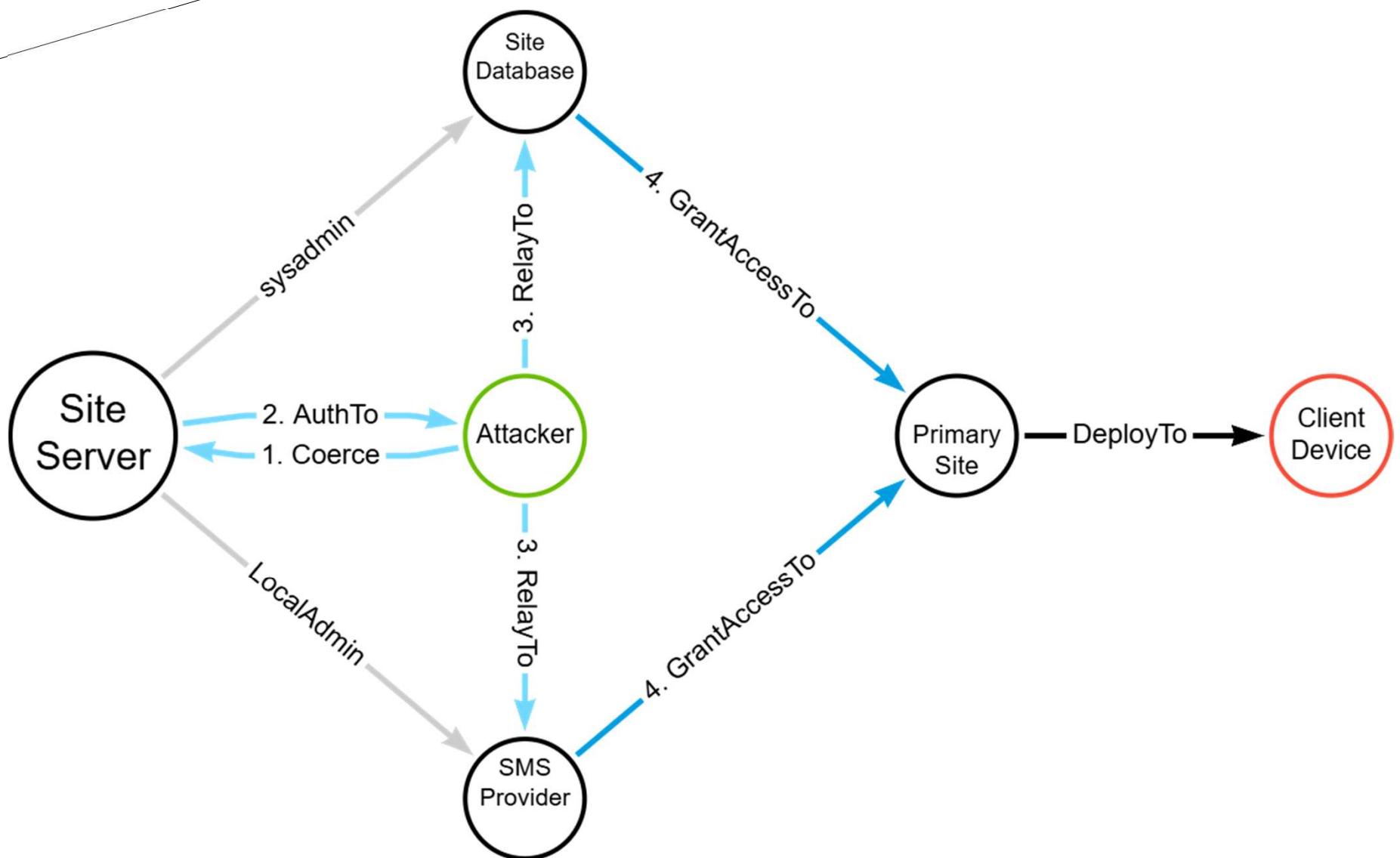


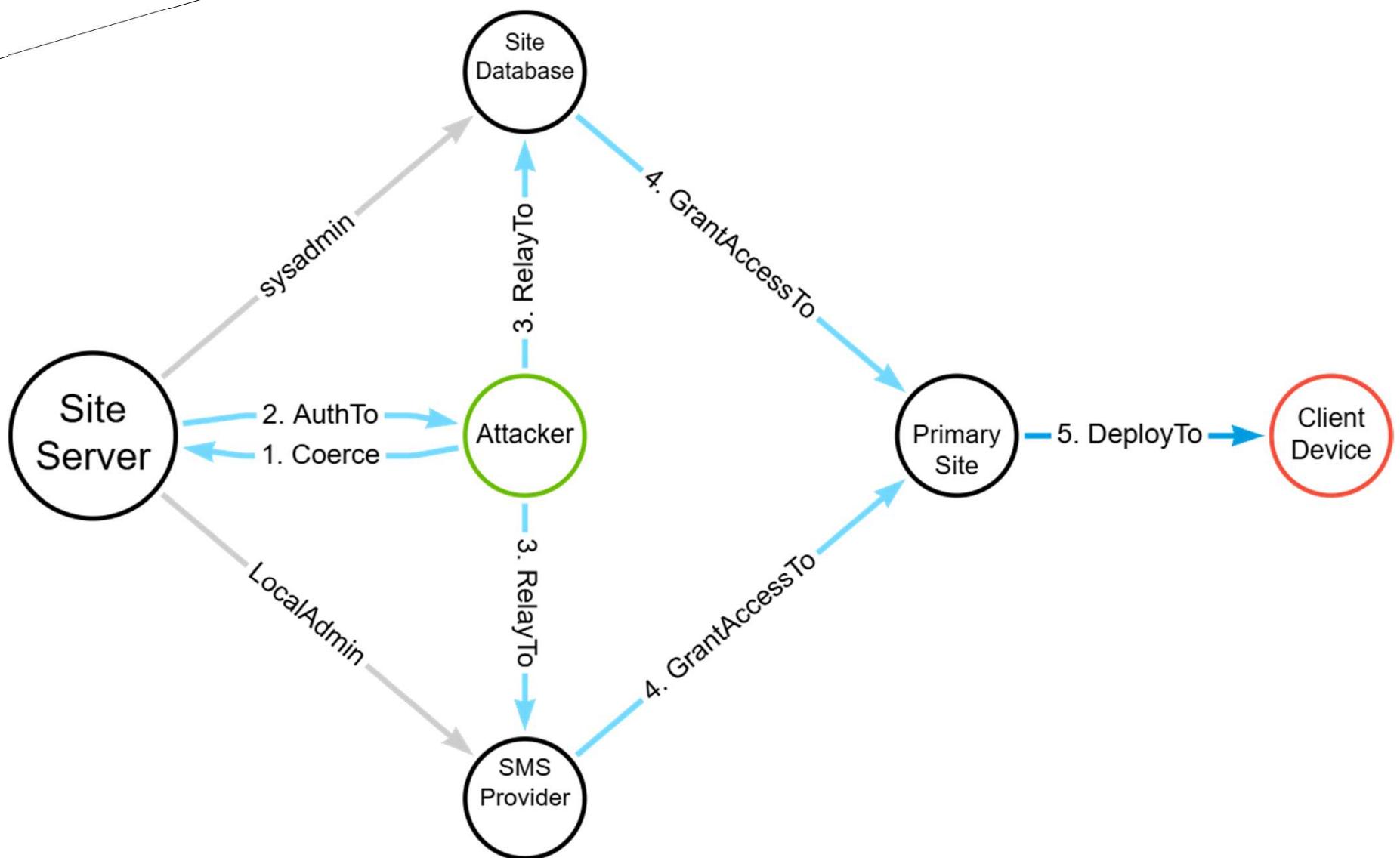












# TAKEOVER-1

