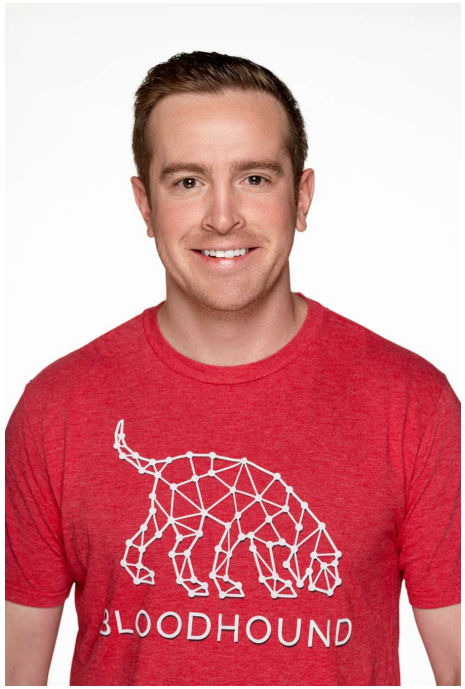
Exposing SCCM and MSSQL Attack Paths in Hardened Environments with OpenGraph



CHRIS THOMPSON

X: @_MAYYHEM

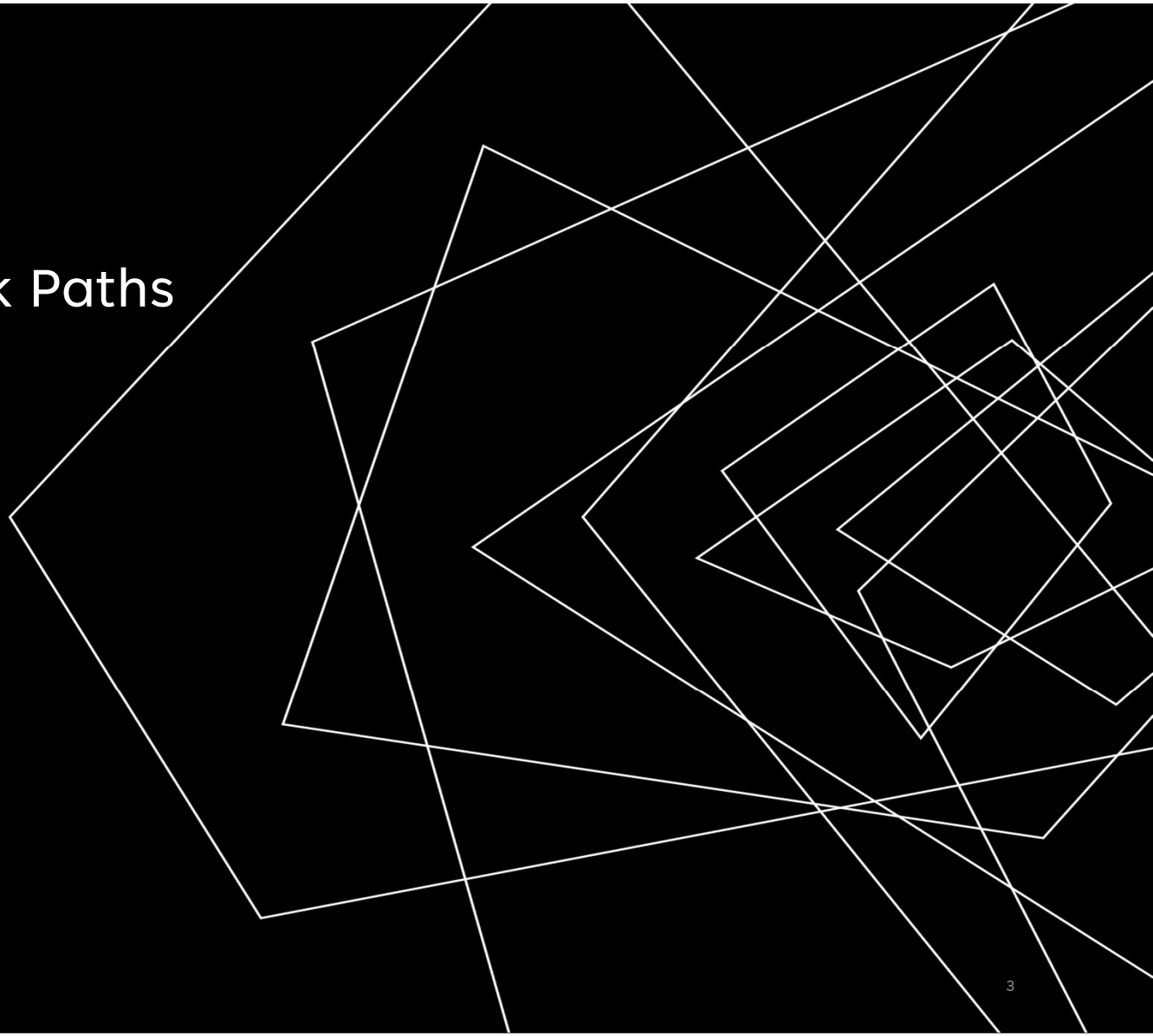
SLACK: @MAYYHEM

SPECTEROPS.SLACK.COM

AGENDA

SCCM/MSSQL Attack Paths

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



WHAT IS SCCM?

System Center Configuration Manager

- Deploys software at scale to fleets of workstations and servers

WHAT IS SCCM?

System Center Configuration Manager

- Deploys software at scale to fleets of workstations and servers
- **Command and control server**

SCCM HIERARCHY

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

PRIMARY SITE

PRIMARY SITES

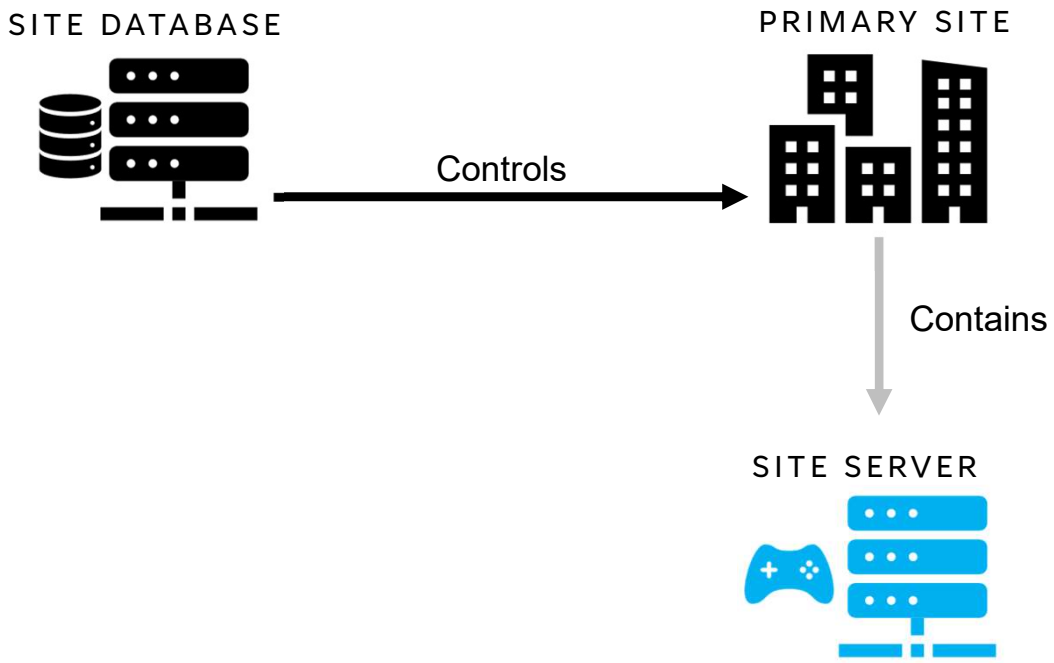
- Serve software to SCCM client devices
- Manage “site system roles”, servers that host various services for SCCM
- ID is 3-character site code (e.g., PS1)

SITE DATABASES

- Hierarchy system of record

SITE DATABASES

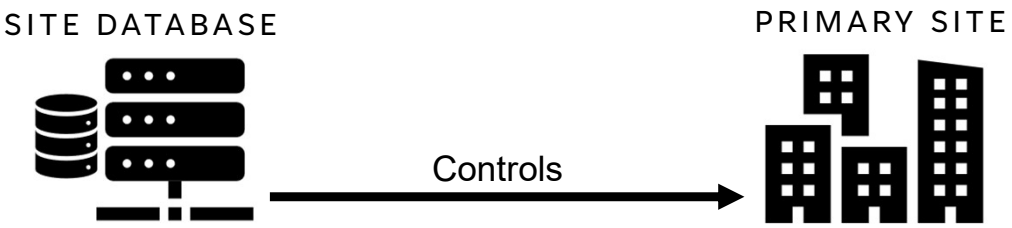
- Hierarchy system of record
- Define admin users and roles



SITE SERVERS

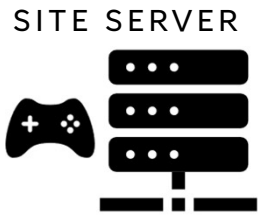
Orchestrate all actions for:

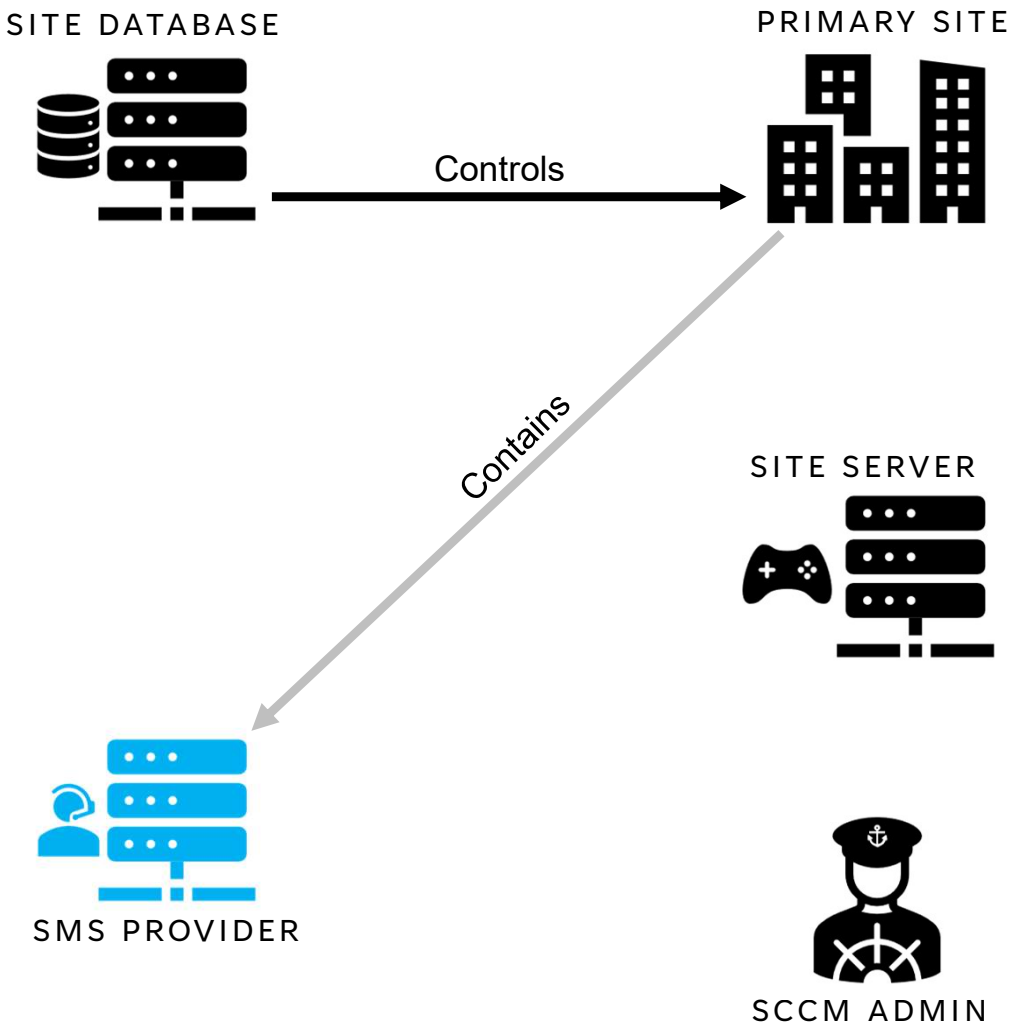
- site
- client devices
- site system roles



SCCM ADMINS

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

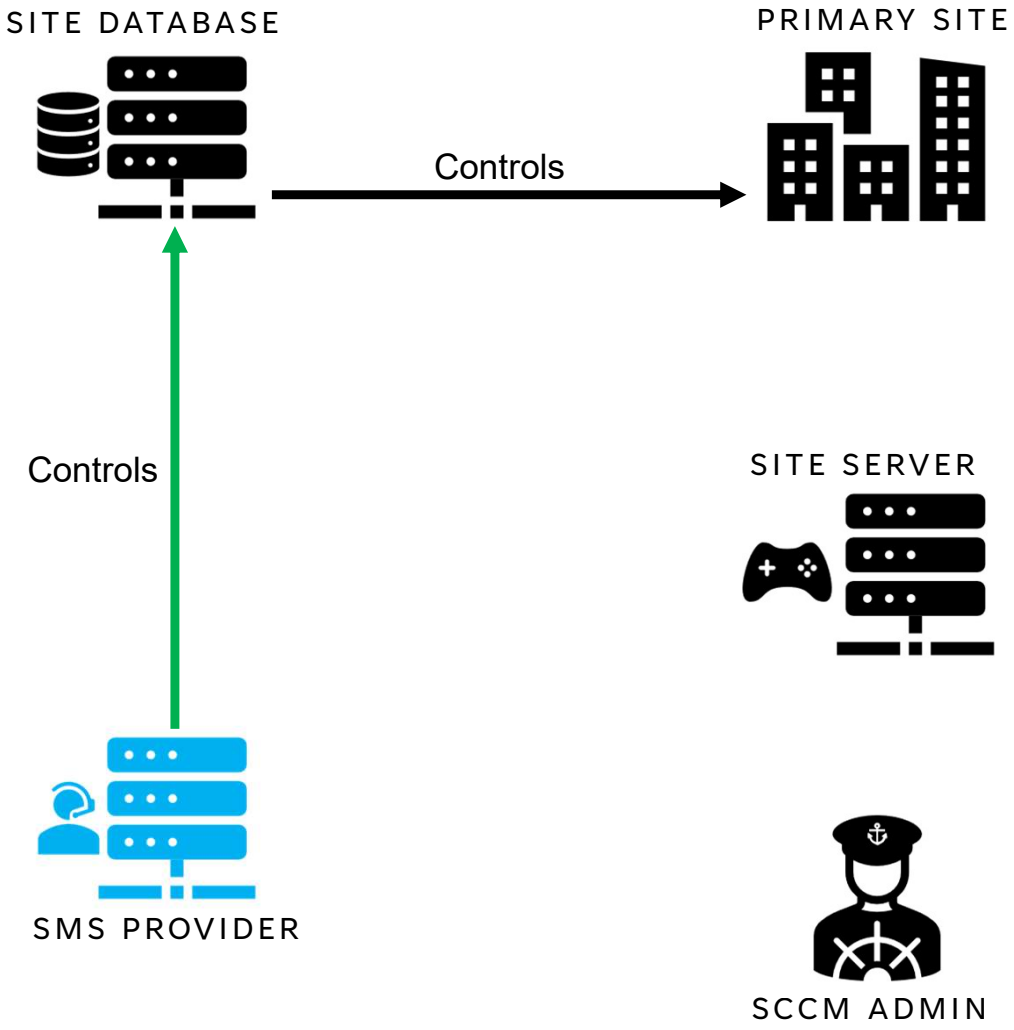




SMS PROVIDERS

Host two APIs for SCCM admins to manage site database:

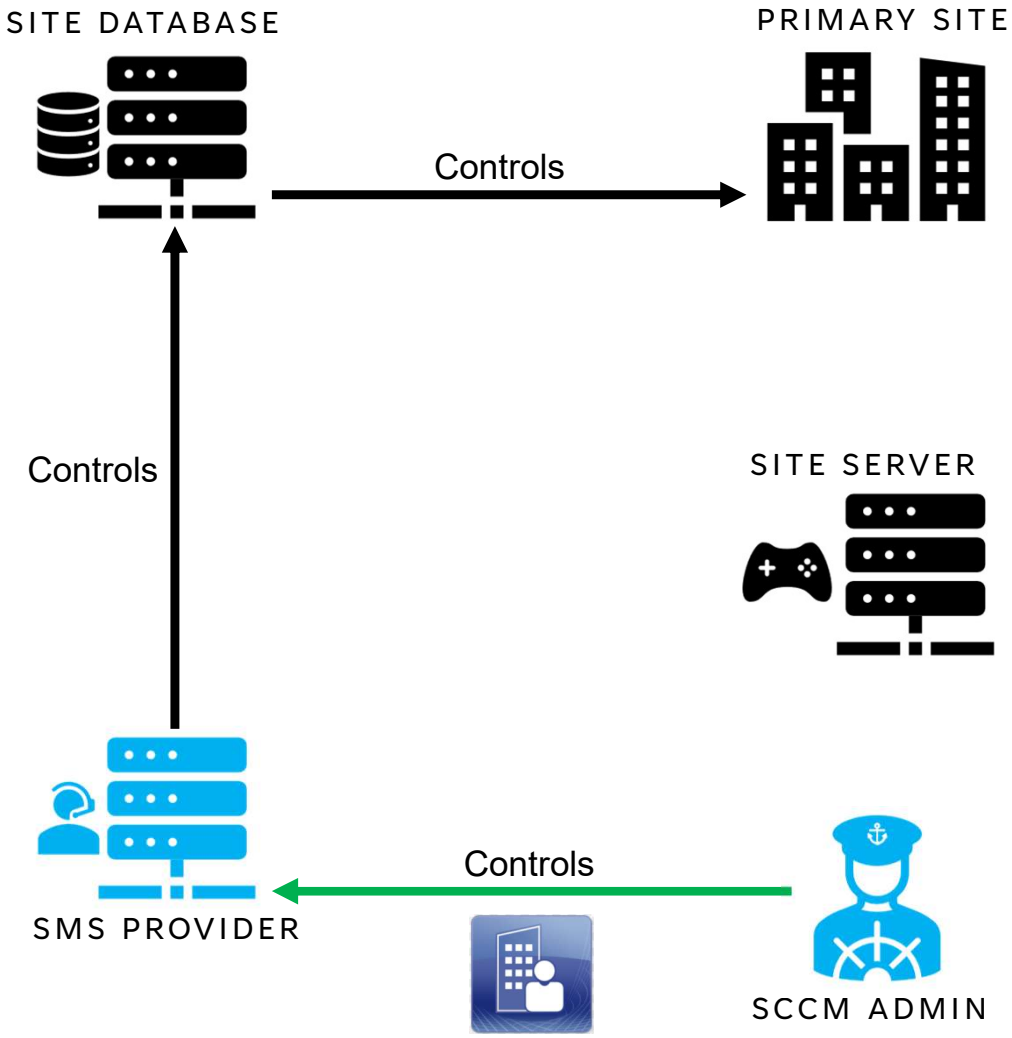
- AdminService
- WMI



SMS PROVIDERS

Host two APIs for SCCM admins to manage site database:

- AdminService
- WMI



SCCM ADMINS

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

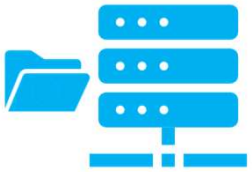
SITE DATABASE

PRIMARY SITE

Contains

SITE SERVER

SMS PROVIDER



DISTRIBUTION POINT

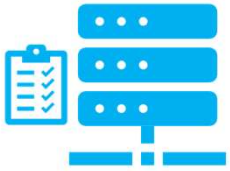
DISTRIBUTION POINTS

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

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

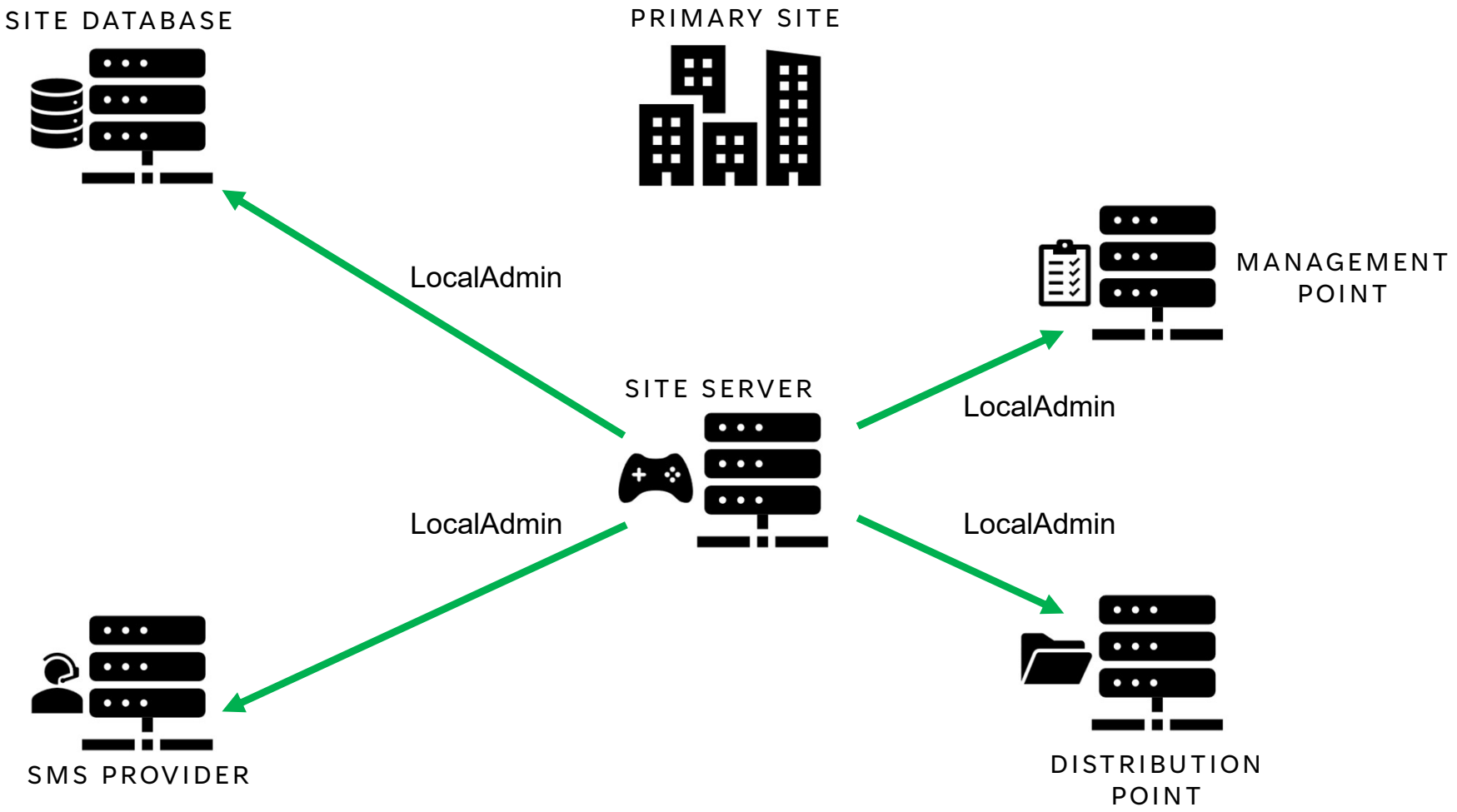
PRIMARY SITE

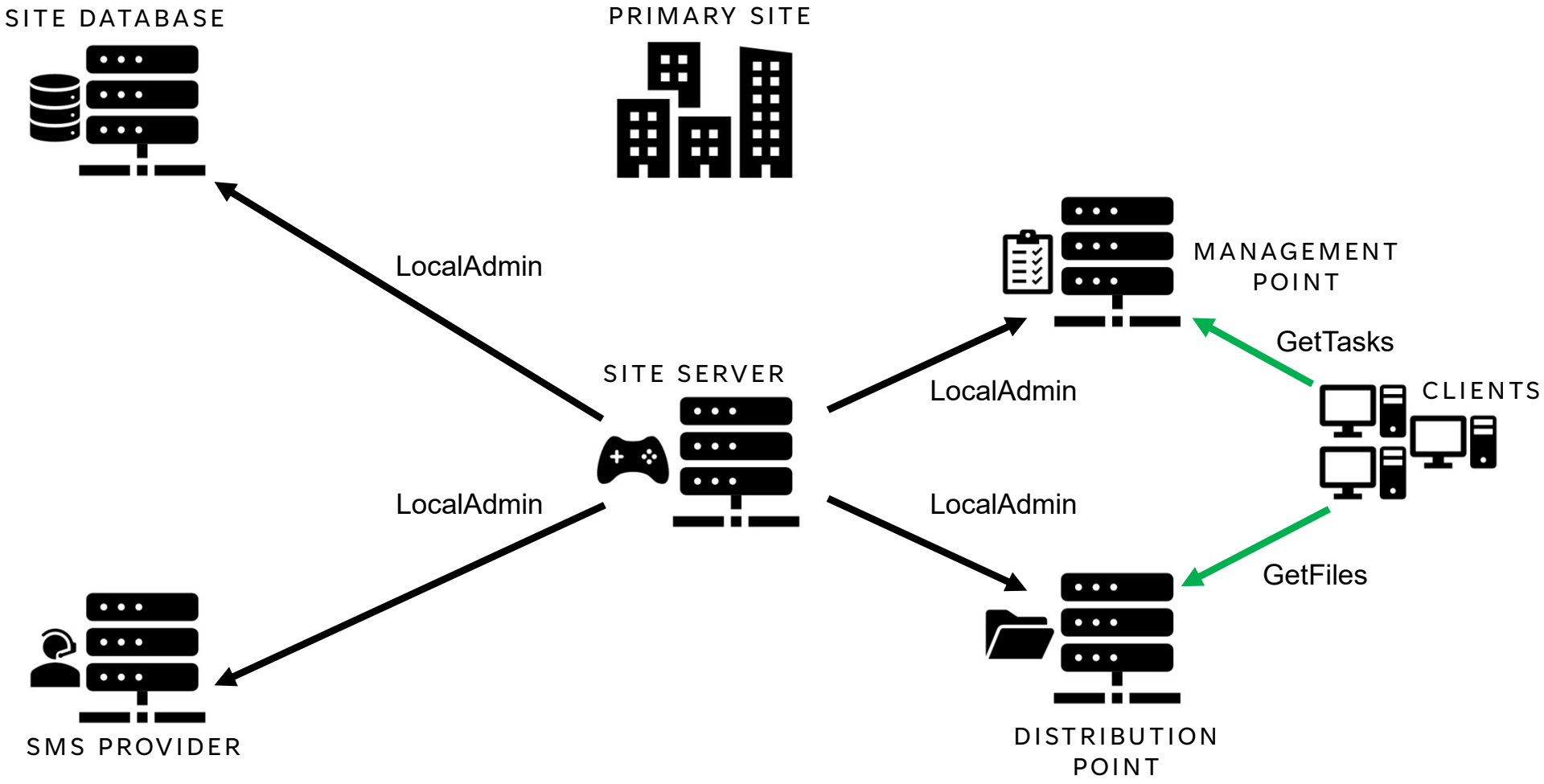
MANAGEMENT POINT

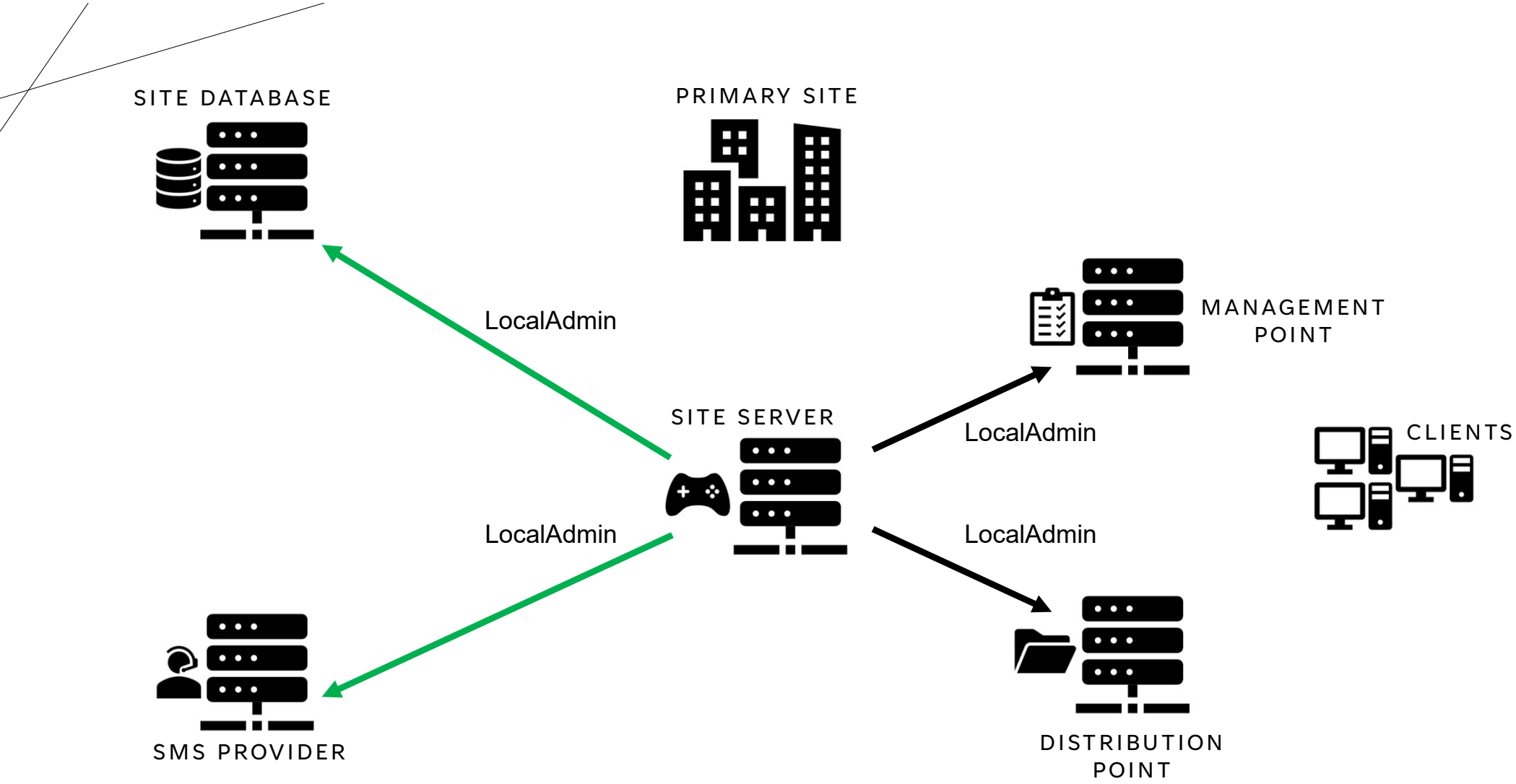
SITE SERVER

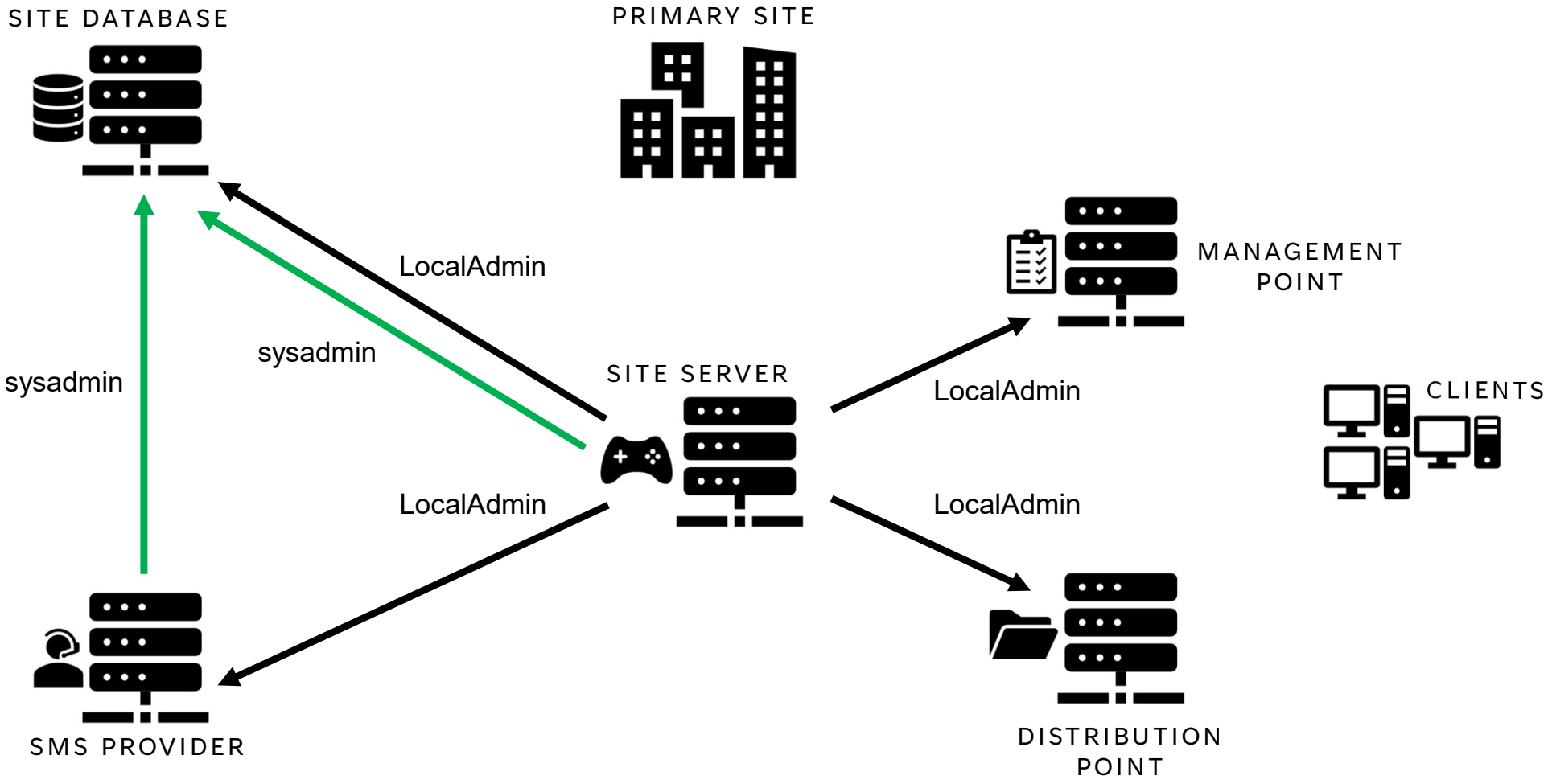
SMS PROVIDER

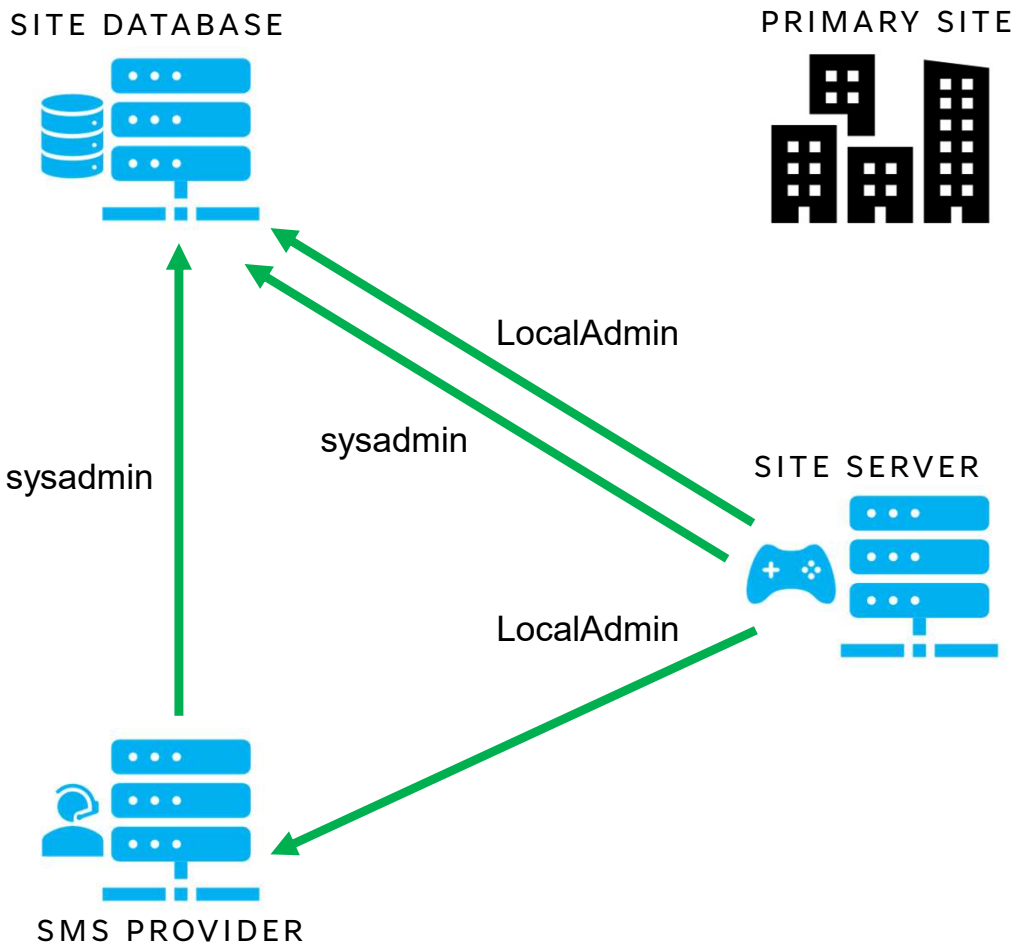
DISTRIBUTION POINT


SITE DATABASE
PRIMARY SITE
LocalAdmin
MANAGEMENT POINT
SITE SERVER
LocalAdmin
LocalAdmin
LocalAdmin
SMS PROVIDER
DISTRIBUTION POINT


SITE DATABASE
PRIMARY SITE
LocalAdmin
MANAGEMENT POINT
GetTasks
SITE SERVER
LocalAdmin
CLIENTS
LocalAdmin
LocalAdmin
GetFiles
SMS PROVIDER
DISTRIBUTION POINT


SITE DATABASE
PRIMARY SITE
LocalAdmin
MANAGEMENT POINT
SITE SERVER
LocalAdmin
CLIENTS
LocalAdmin
LocalAdmin
SMS PROVIDER
DISTRIBUTION POINT

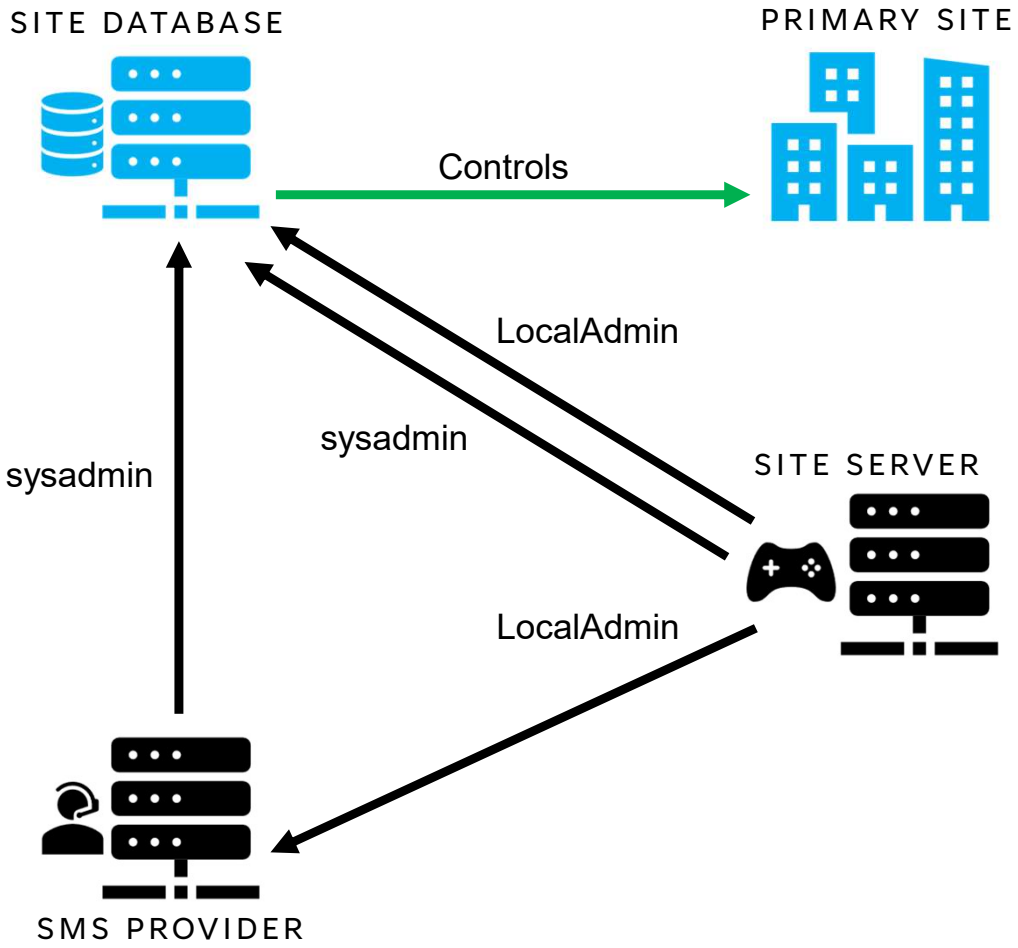

SITE DATABASE
PRIMARY SITE
LocalAdmin
sysadmin
sysadmin
SITE SERVER
MANAGEMENT POINT
LocalAdmin
CLIENTS
LocalAdmin
LocalAdmin
SMS PROVIDER
DISTRIBUTION POINT



MANAGEMENT POINT

CLIENTS

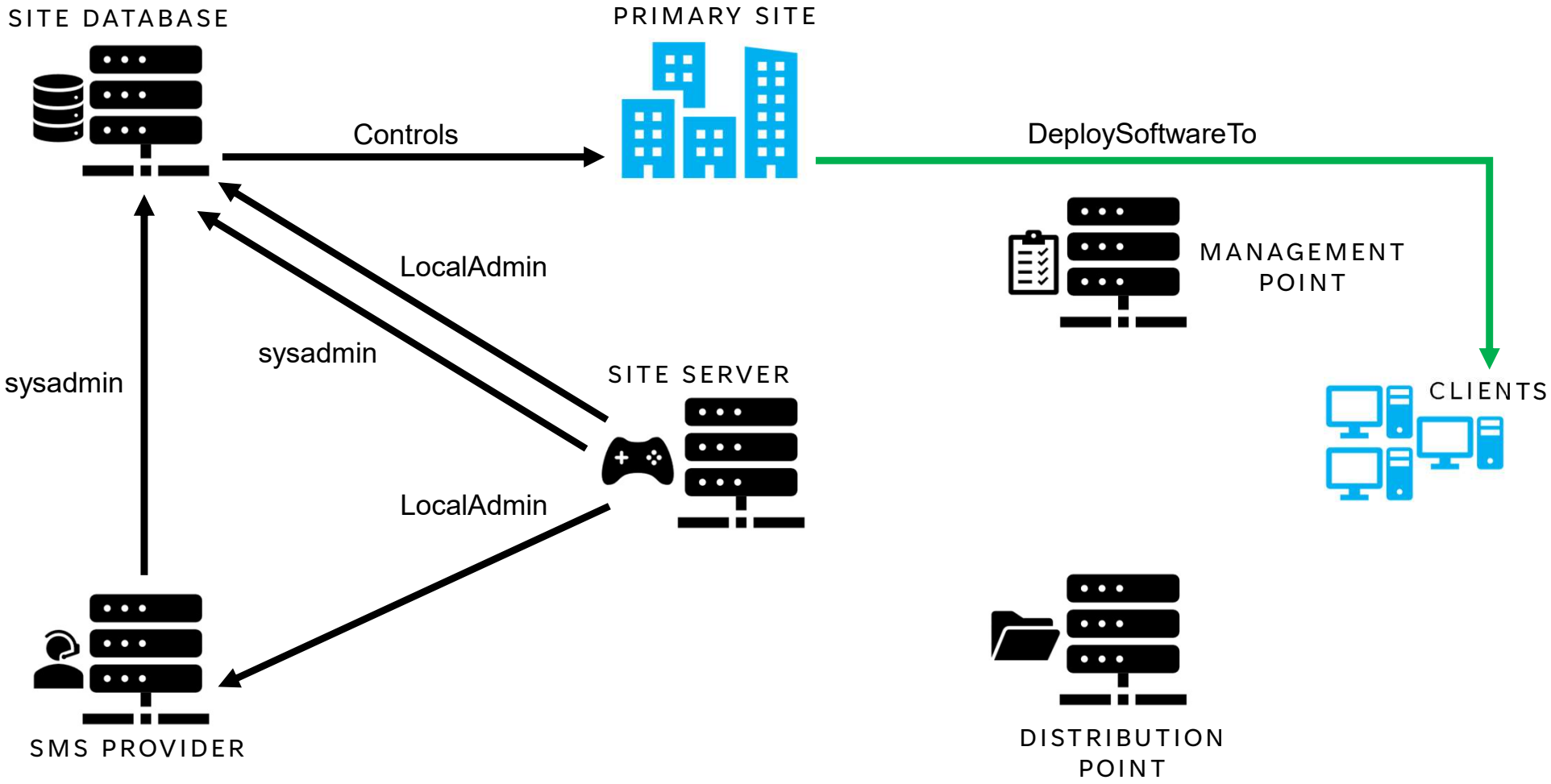
DISTRIBUTION POINT



MANAGEMENT POINT

CLIENTS

DISTRIBUTION POINT


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
MANAGEMENT POINT
LocalAdmin
sysadmin
sysadmin
SITE SERVER
CLIENTS
LocalAdmin
SMS PROVIDER
DISTRIBUTION POINT

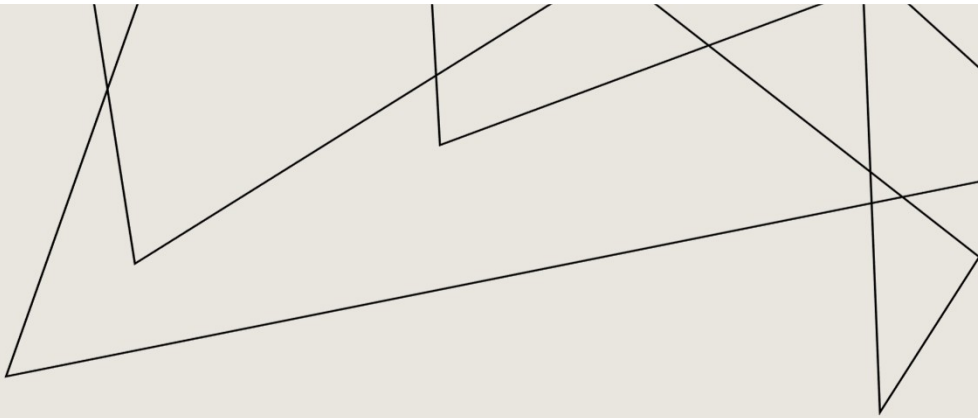
SCCM ATTACK PATHS

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 (à la Certified Pre-Owned)
- Based on MITRE ATT&CK
- PowerShell script to identify TAKEOVER and ELEVATE issues
- 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 can use to authenticate themselves over the network

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

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

site servers

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

- e.g., Printerbug, PetitPotam

NTLM RELAY

Attackers can **coerce site servers** into authenticating to their machine and **use** the creds on **other SCCM servers** 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


PRIMARY SITE
GrantAccess
DeploySoftwareTo
CLIENTS
ATTACKER

SITE DATABASE

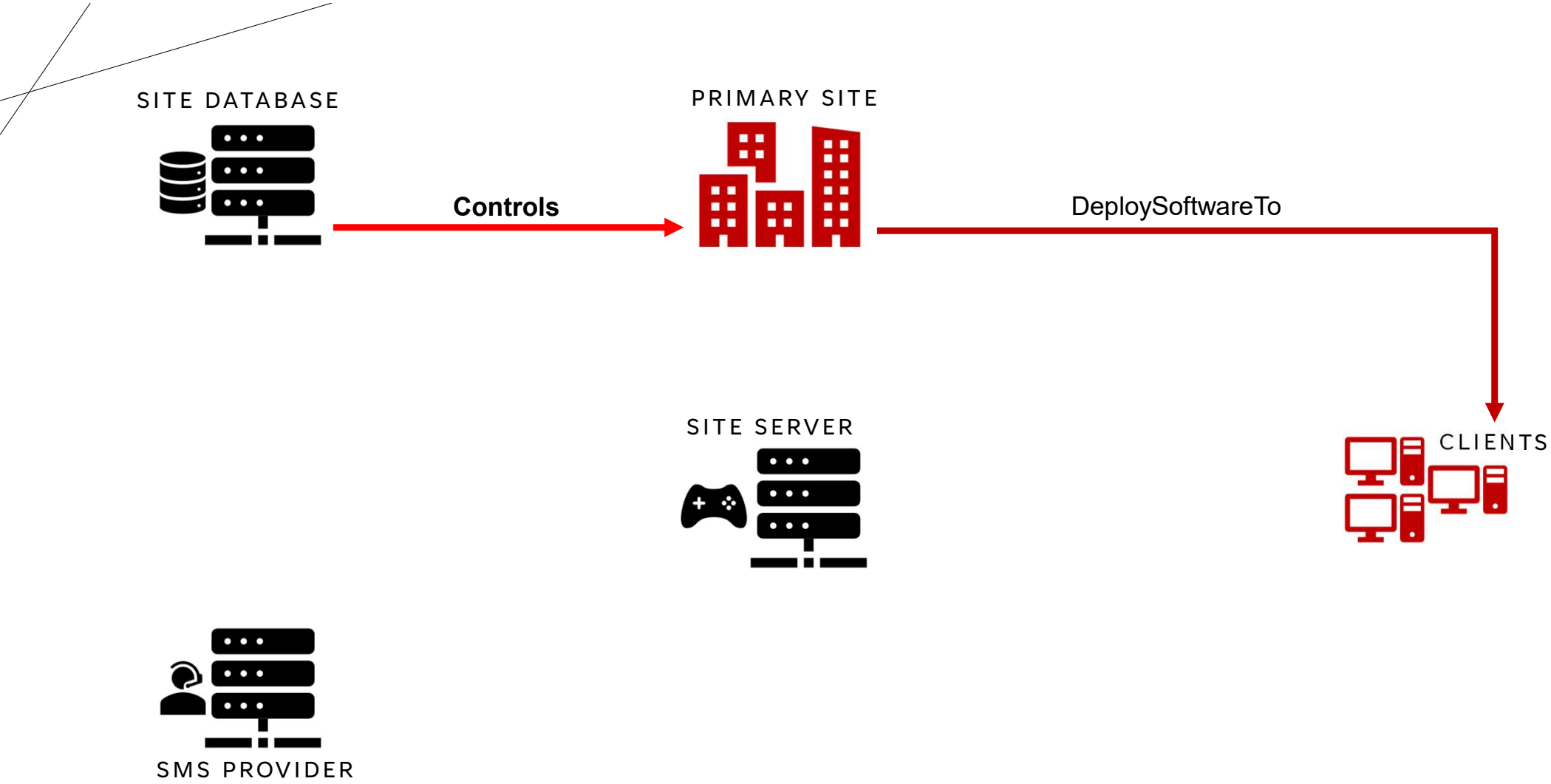
PRIMARY SITE

DeploySoftwareTo

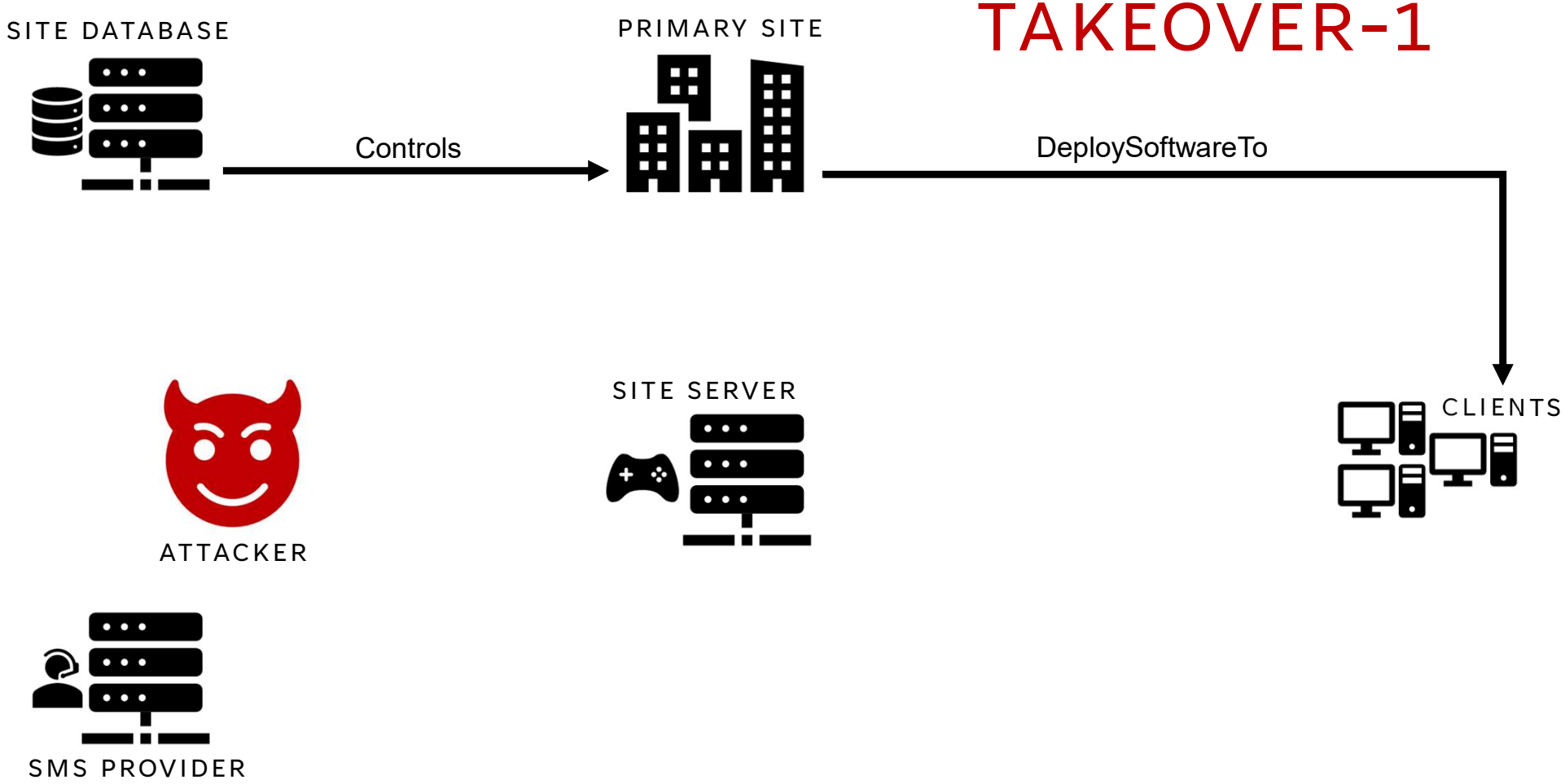
SITE SERVER

CLIENTS

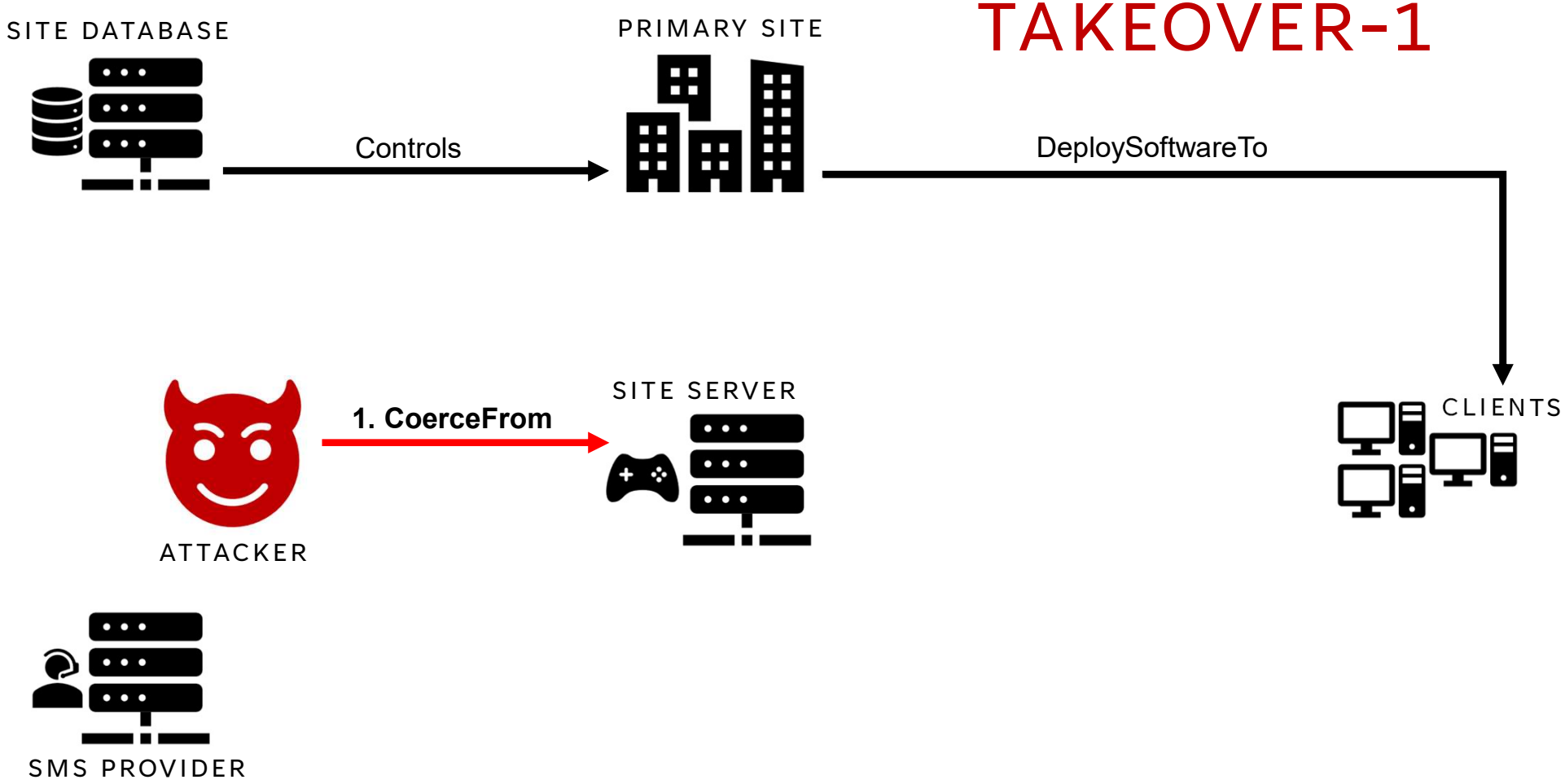
SMS PROVIDER


SITE DATABASE
Controls
PRIMARY SITE
DeploySoftwareTo
SITE SERVER
CLIENTS
SMS PROVIDER

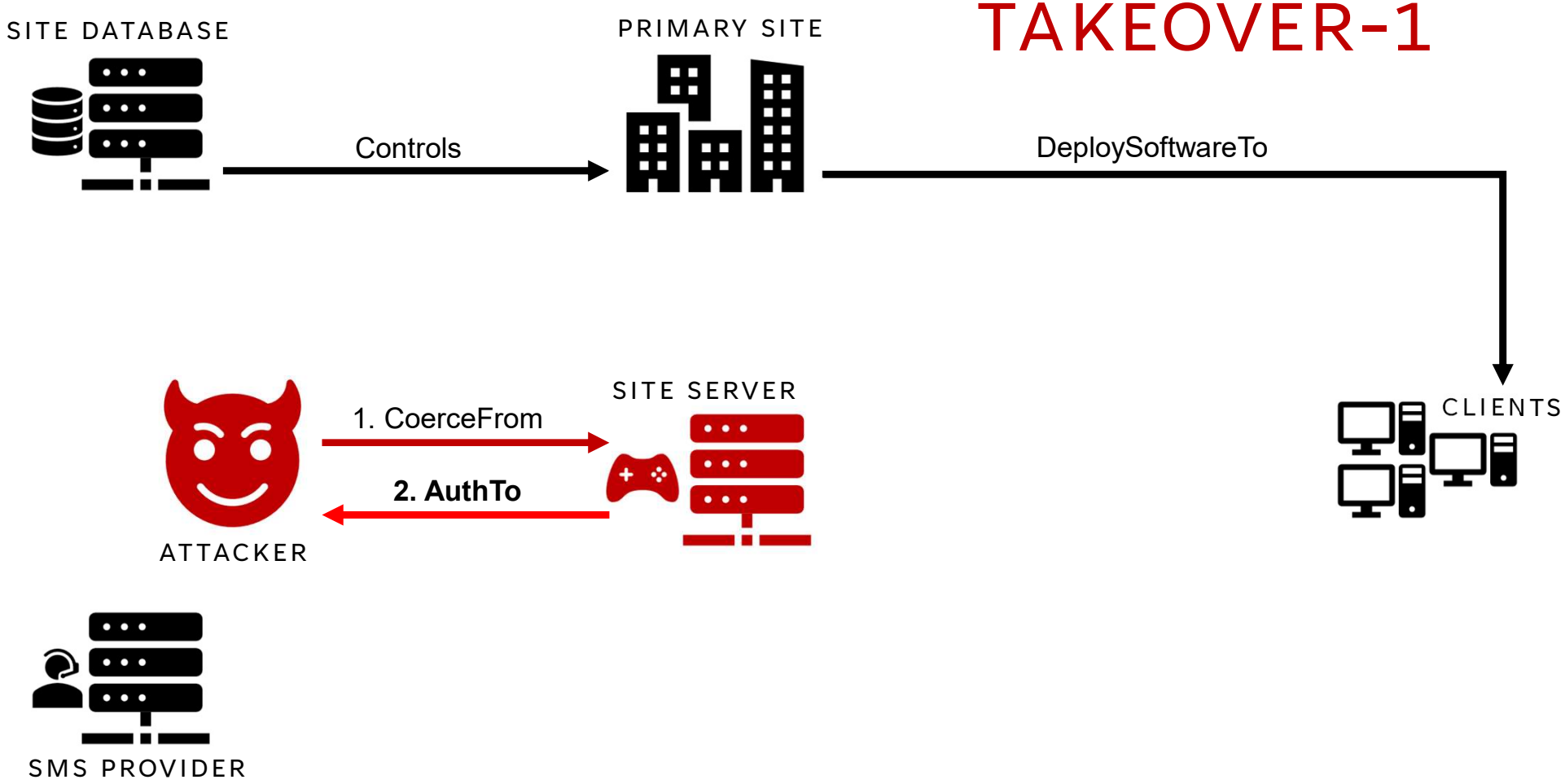
TAKEOVER-1


SITE DATABASE
Controls
PRIMARY SITE
DeploySoftwareTo
CLIENTS
ATTACKER
SITE SERVER
SMS PROVIDER

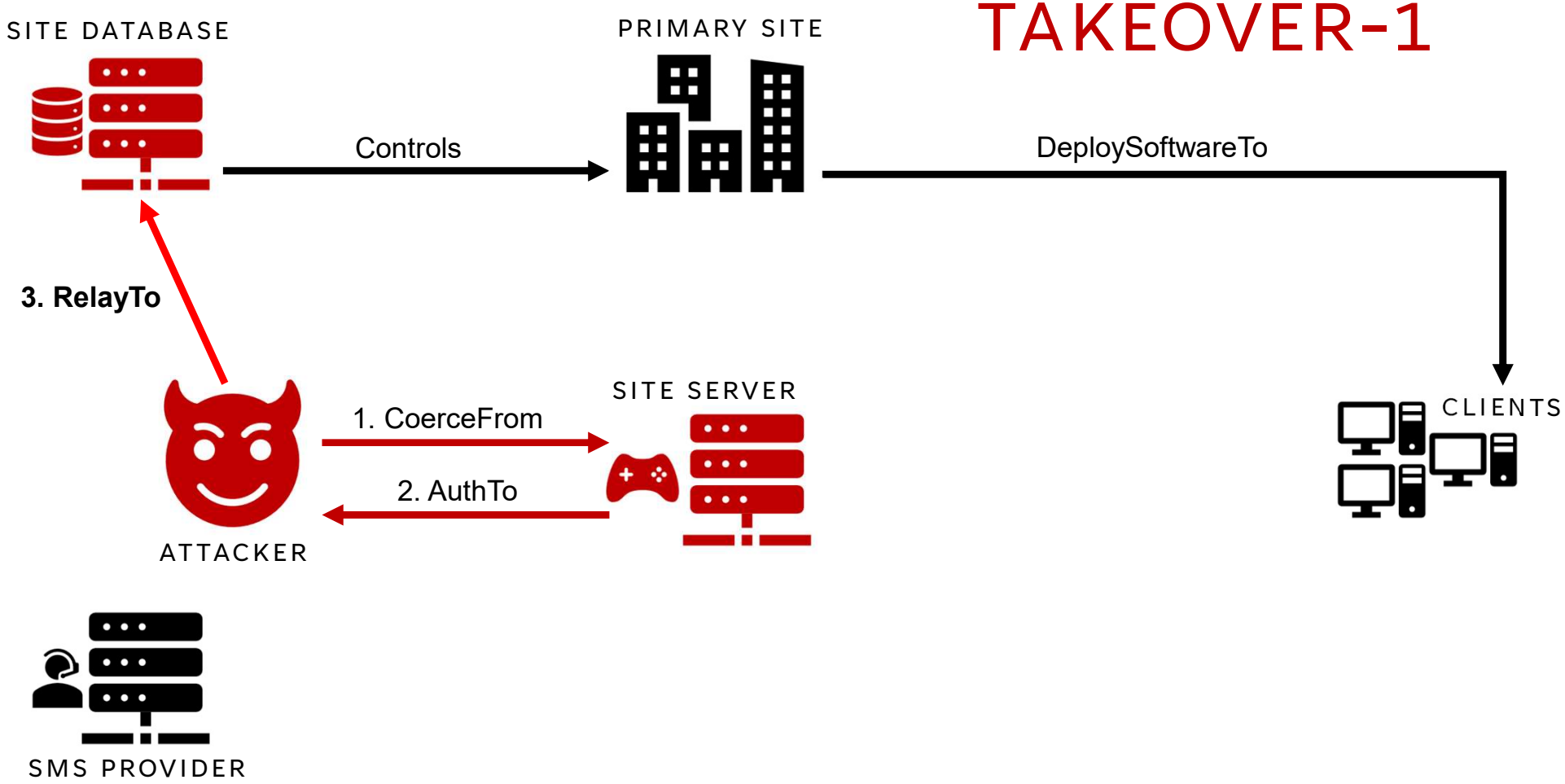
TAKEOVER-1


SITE DATABASE
Controls
PRIMARY SITE
DeploySoftwareTo
CLIENTS
1. CoerceFrom
SITE SERVER
ATTACKER
SMS PROVIDER

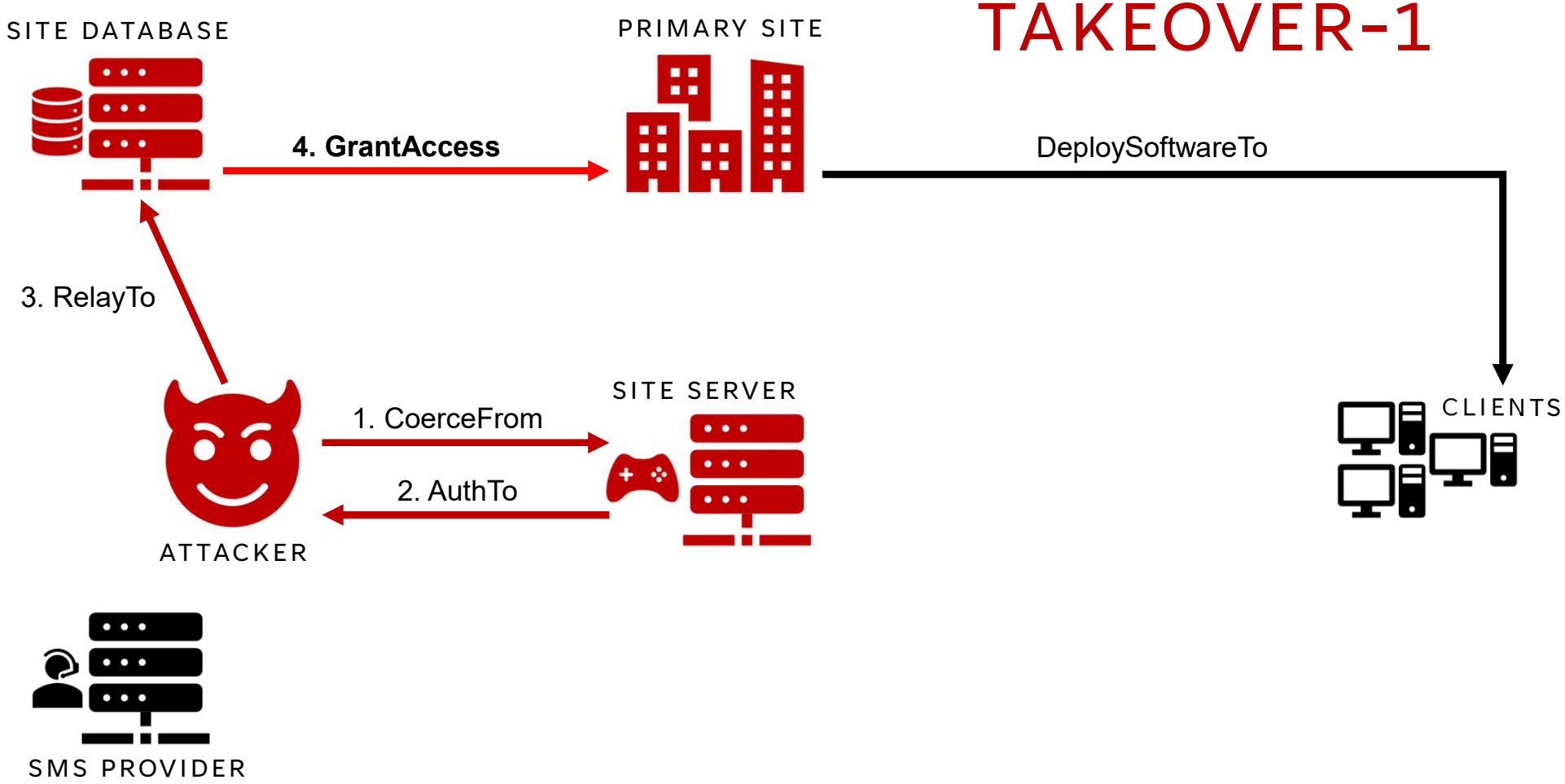
TAKEOVER-1


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
CLIENTS
SITE SERVER
1. CoerceFrom
2. AuthTo
ATTACKER
SMS PROVIDER

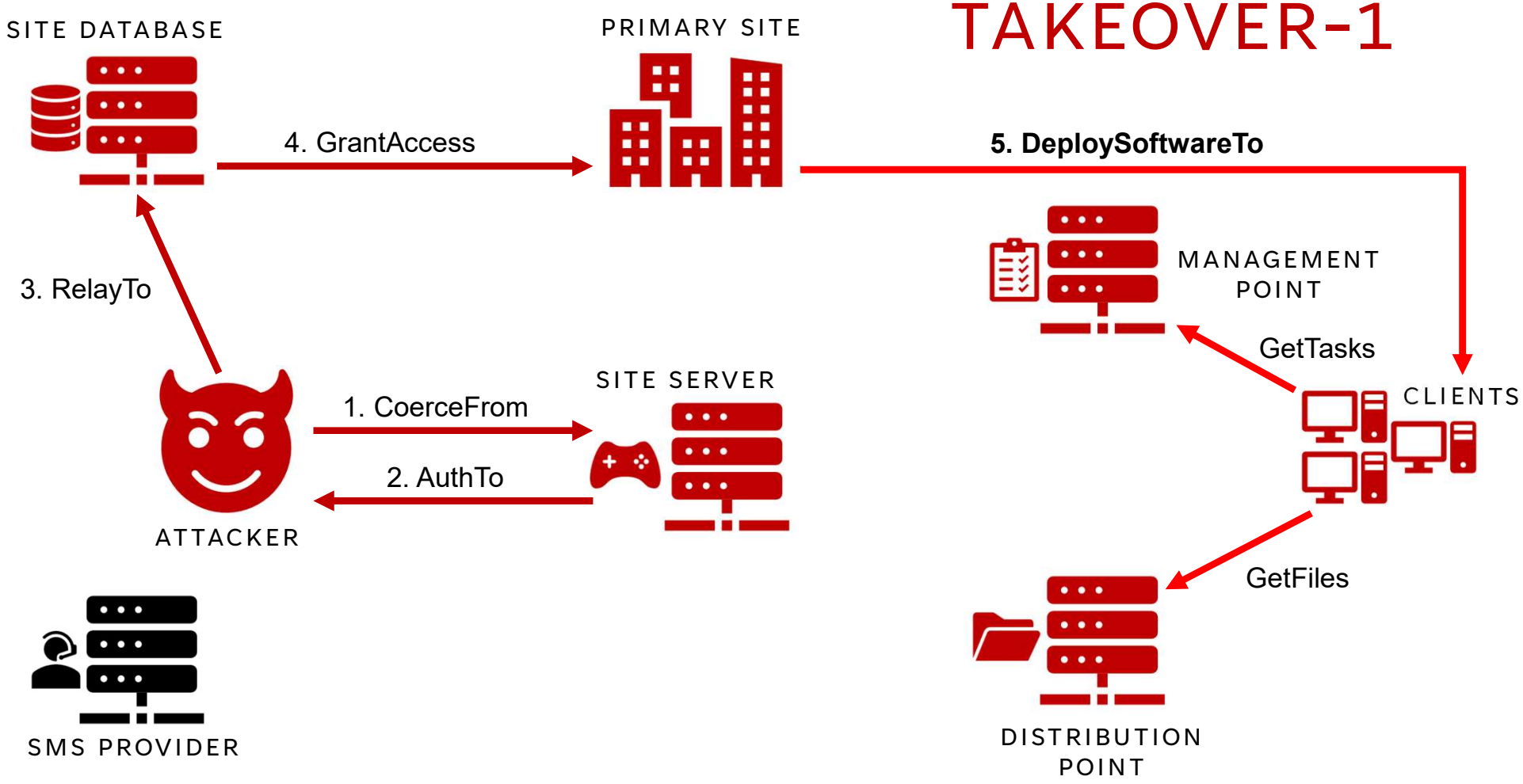
TAKEOVER-1


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
3. RelayTo
SITE SERVER
1. CoerceFrom
2. AuthTo
CLIENTS
ATTACKER
SMS PROVIDER

TAKEOVER-1

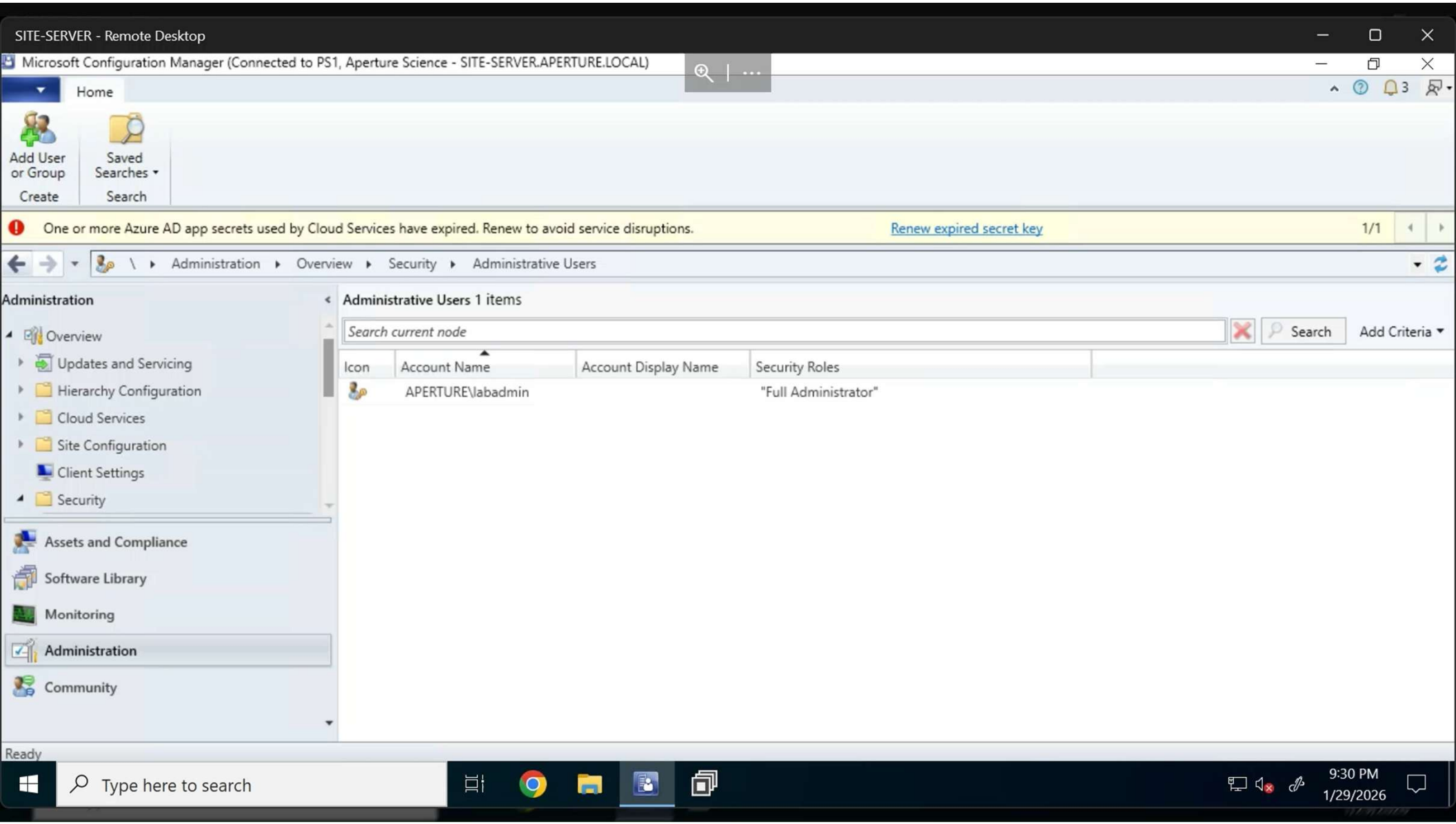

SITE DATABASE
PRIMARY SITE
4. GrantAccess
DeploySoftwareTo
3. RelayTo
SITE SERVER
1. CoerceFrom
2. AuthTo
CLIENTS
ATTACKER
SMS PROVIDER

TAKEOVER-1


SITE DATABASE
PRIMARY SITE
4. GrantAccess
5. DeploySoftwareTo
MANAGEMENT POINT
3. RelayTo
GetTasks
CLIENTS
SITE SERVER
1. CoerceFrom
2. AuthTo
ATTACKER
GetFiles
SMS PROVIDER
DISTRIBUTION POINT

TAKEOVER-1


PRIMARY SITE
GrantAccess
DeploySoftwareTo
CLIENTS
ATTACKER


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 ▸ Security ▸ Administrative Users
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
Search
Add Criteria
Icon
Account Name
Account Display Name
Security Roles
APERTURE\labadmin
"Full Administrator"
Ready
Type here to search
9:30 PM
1/29/2026

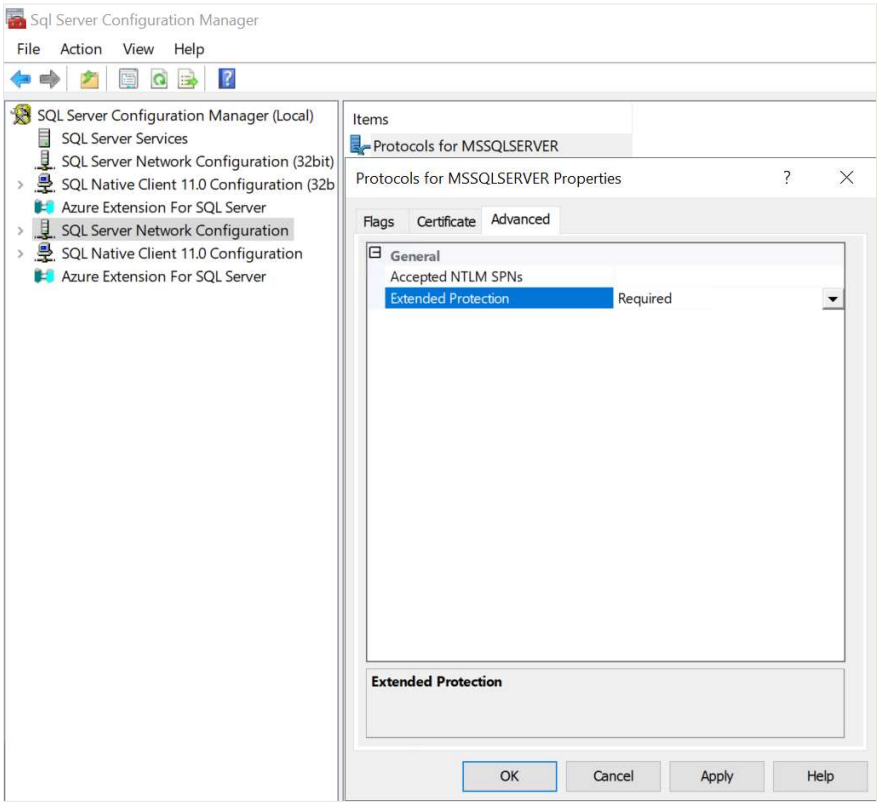
TAKEOVER-1 REMEDIATION

Require Extended Protection On Remote Site Databases

On 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

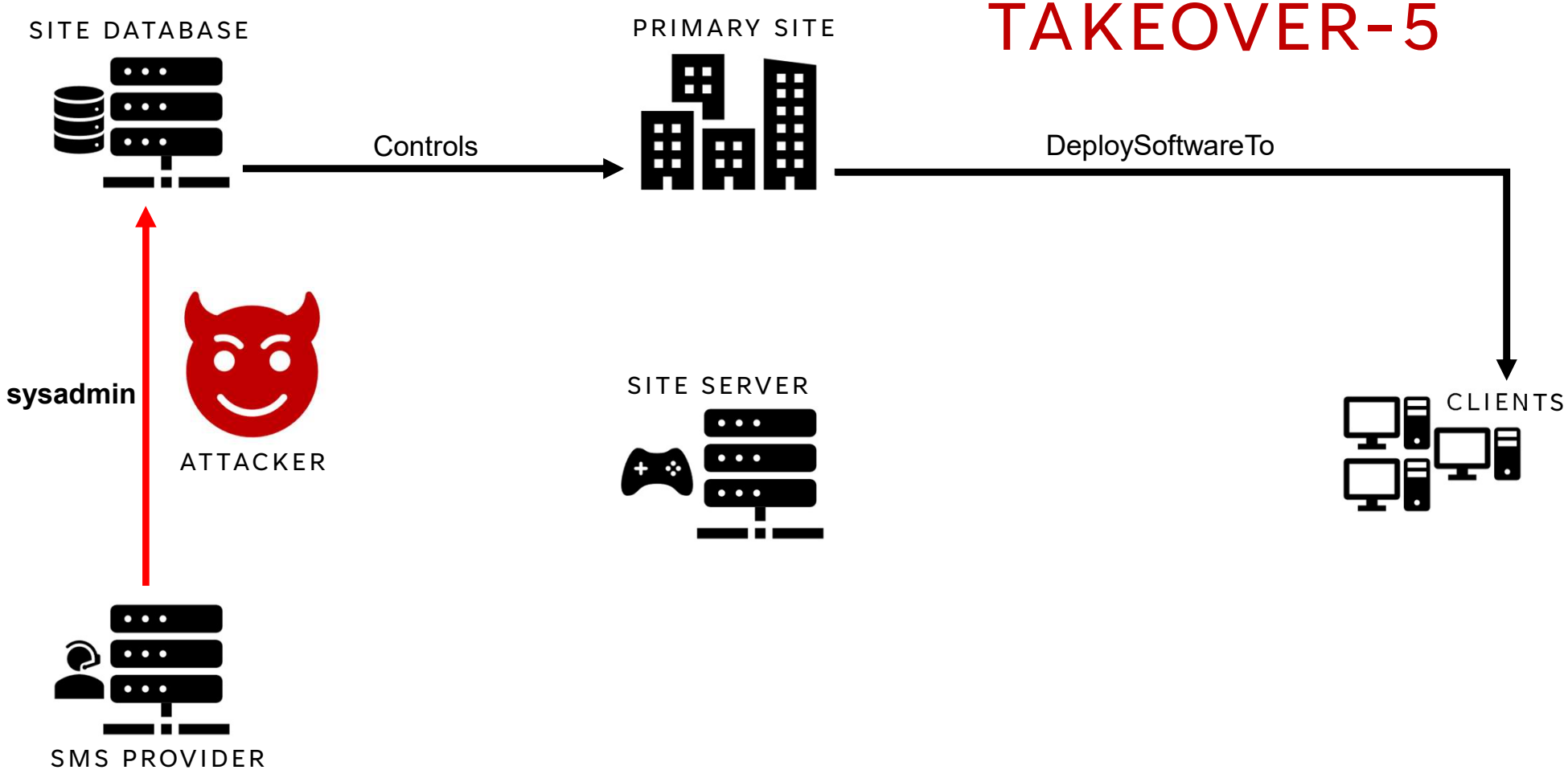
Setting to “Allowed” will not prevent NTLM relay attacks if the coerced client doesn’t support channel binding



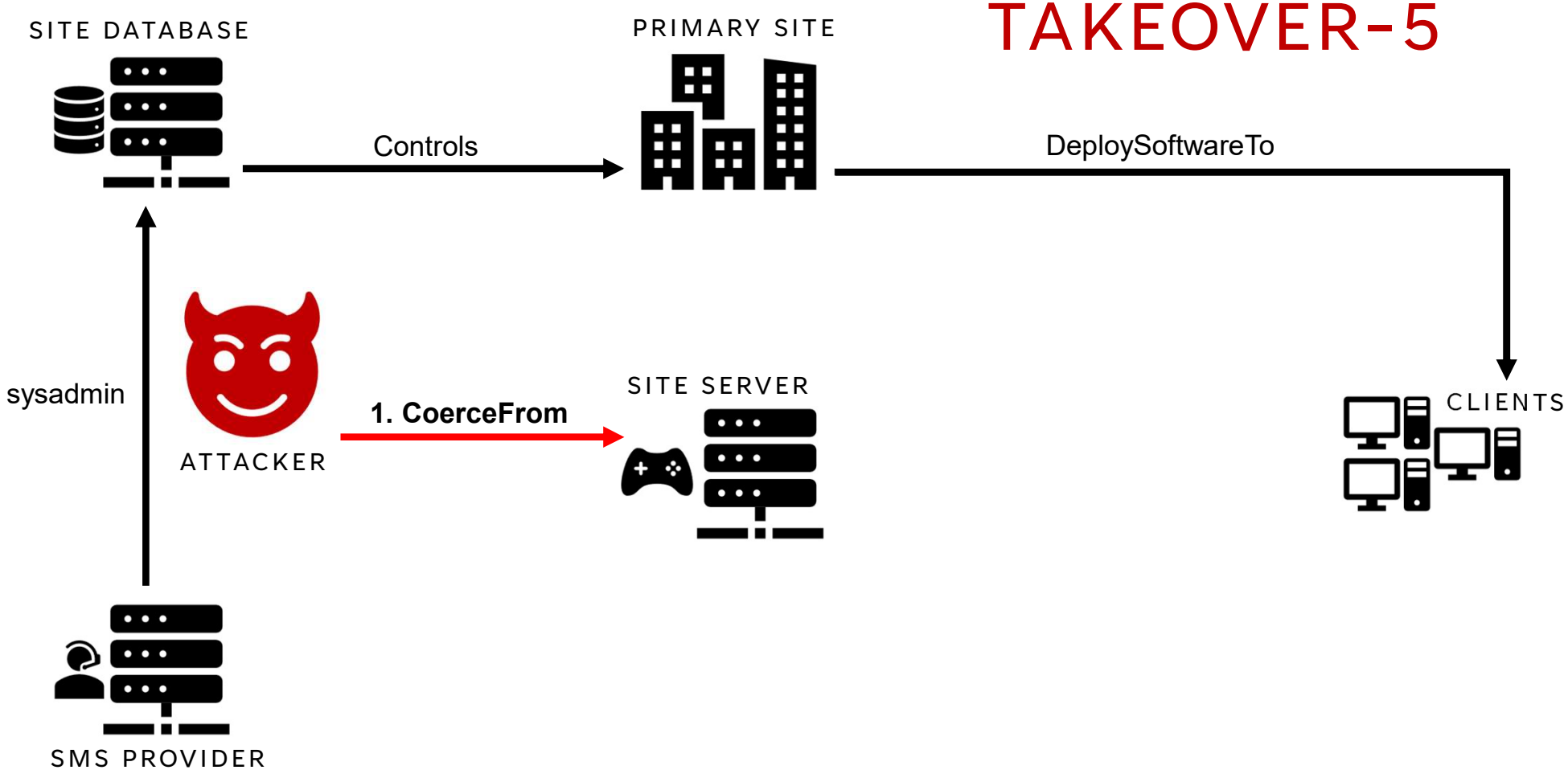
TAKEOVER-5


PRIMARY SITE
GrantAccess
DeploySoftwareTo
CLIENTS
ATTACKER

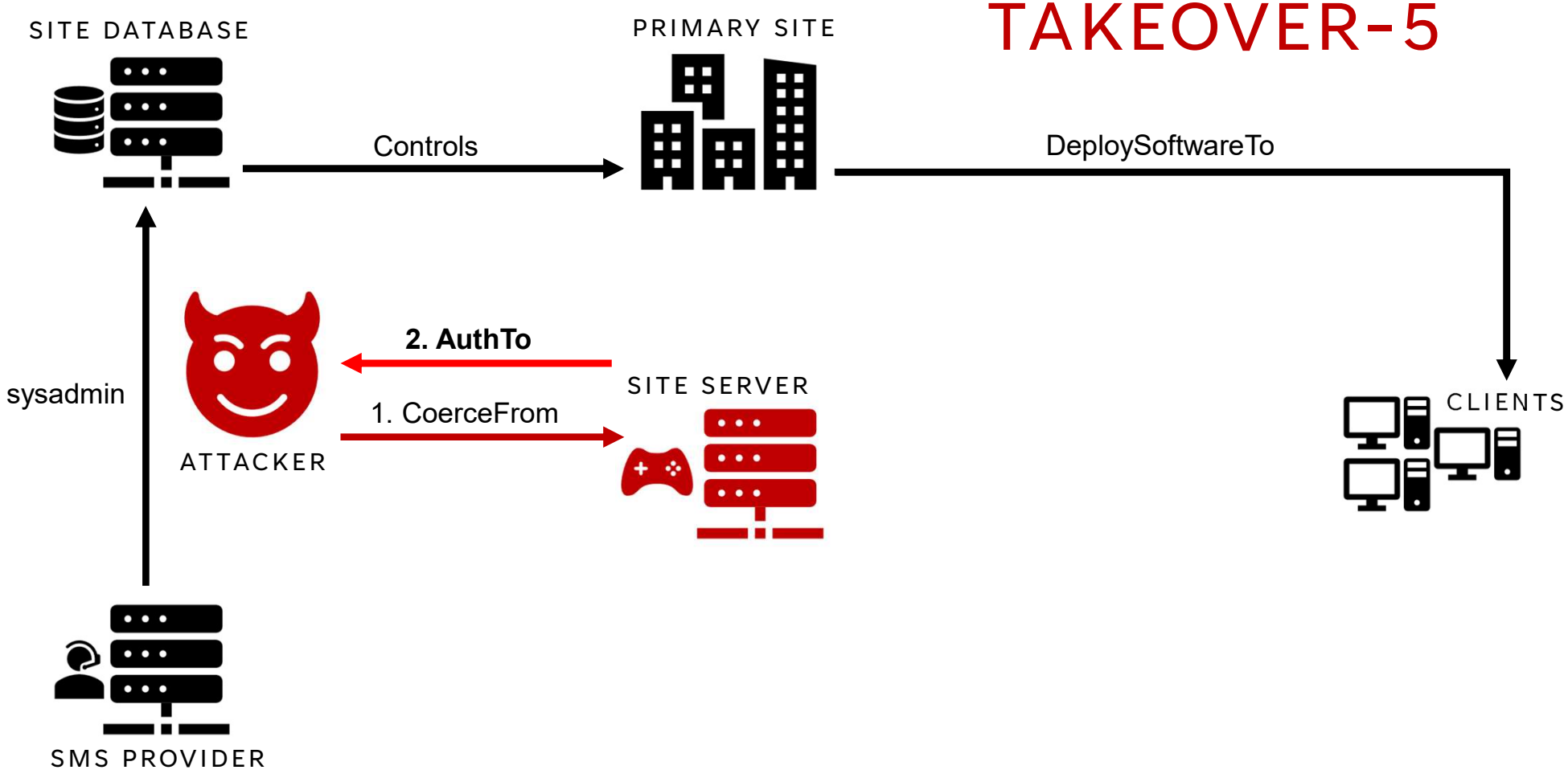
TAKEOVER-5


SITE DATABASE
Controls
PRIMARY SITE
DeploySoftwareTo
sysadmin
ATTACKER
SITE SERVER
CLIENTS
SMS PROVIDER

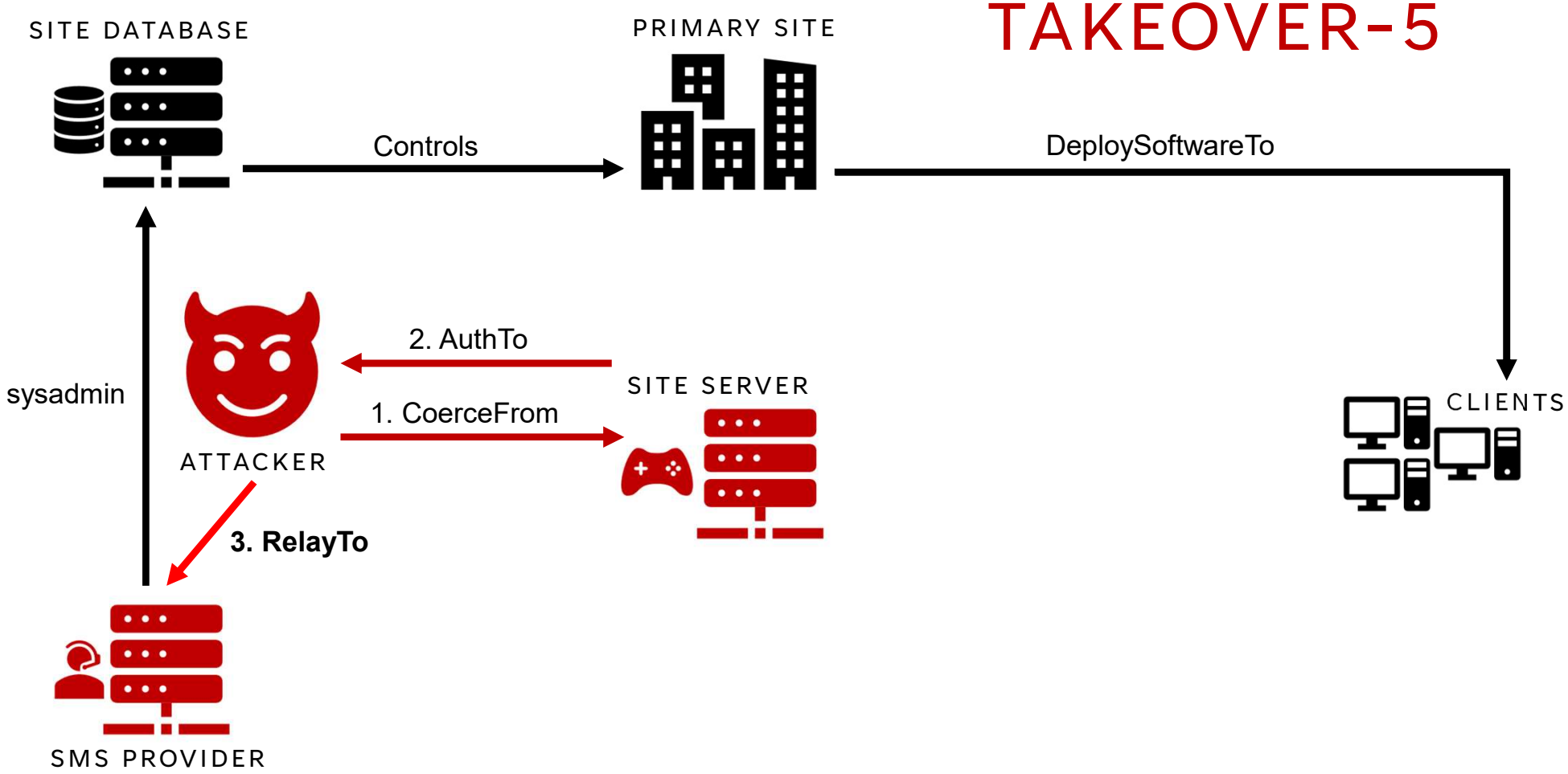
TAKEOVER-5


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
sysadmin
ATTACKER
1. CoerceFrom
SITE SERVER
CLIENTS
SMS PROVIDER

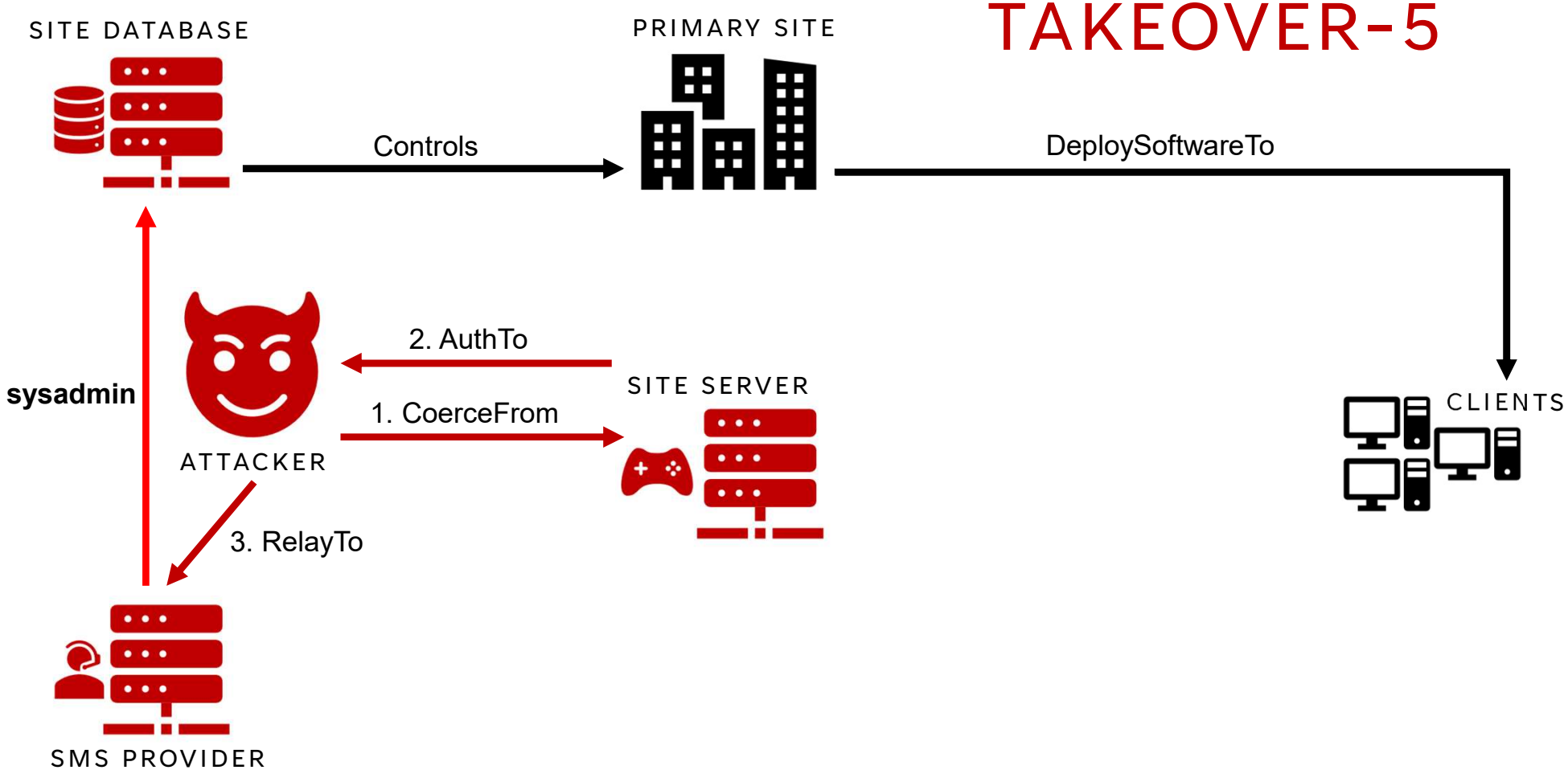
TAKEOVER-5


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
sysadmin
2. AuthTo
1. CoerceFrom
SITE SERVER
CLIENTS
ATTACKER
SMS PROVIDER

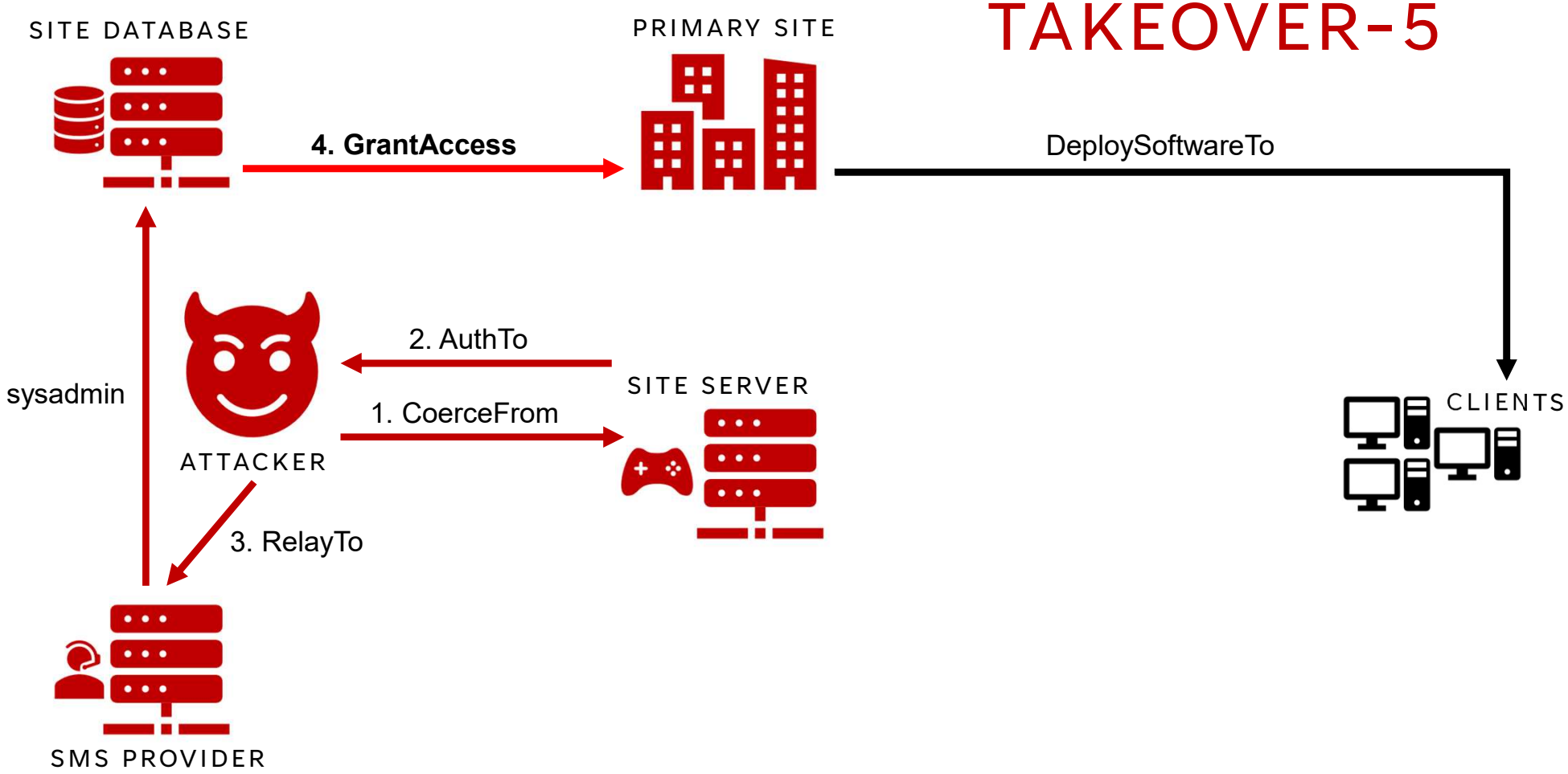
TAKEOVER-5


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
sysadmin
ATTACKER
2. AuthTo
1. CoerceFrom
SITE SERVER
CLIENTS
3. RelayTo
SMS PROVIDER

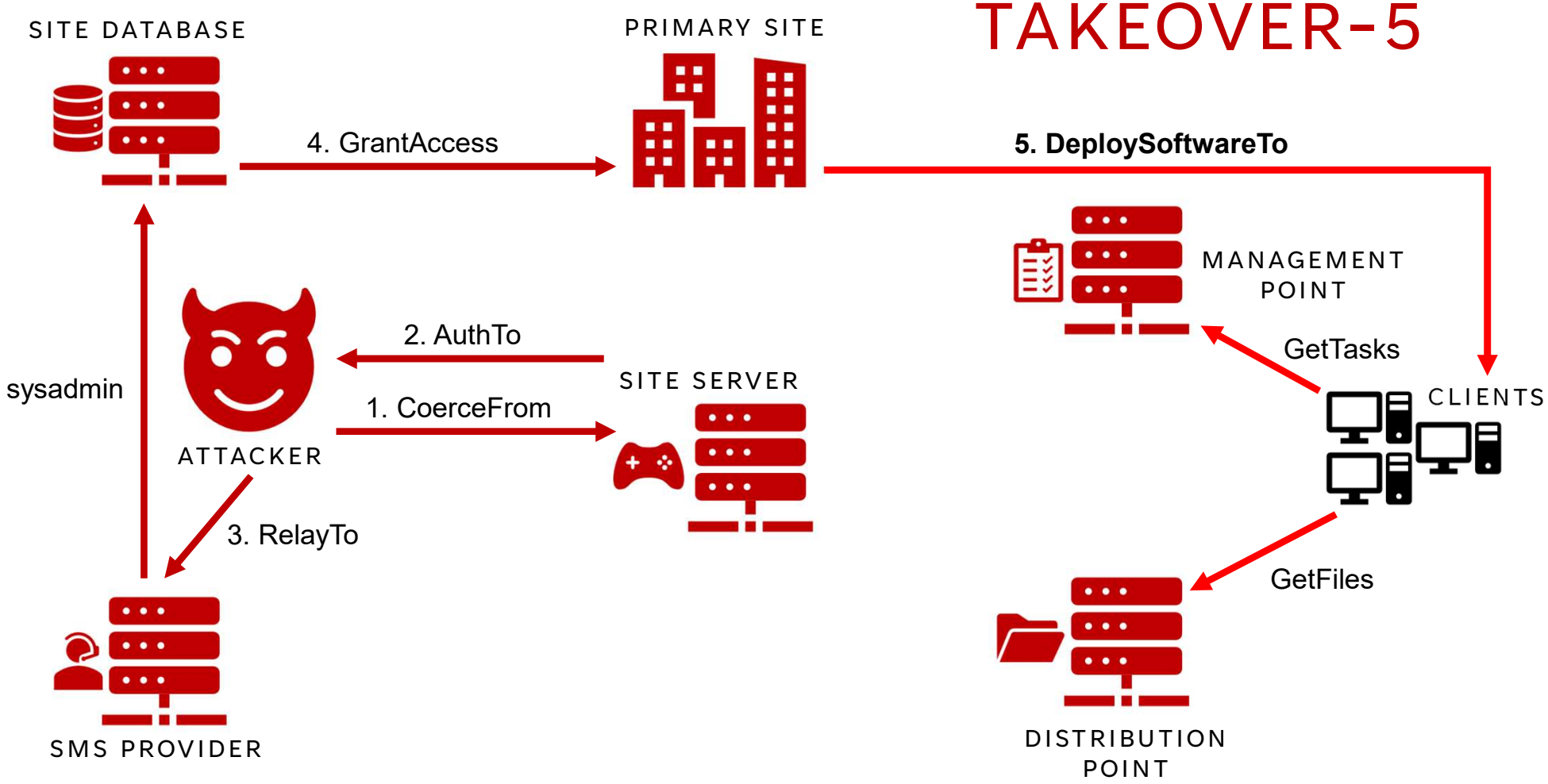
TAKEOVER-5


SITE DATABASE
PRIMARY SITE
Controls
DeploySoftwareTo
CLIENTS
sysadmin
ATTACKER
2. AuthTo
1. CoerceFrom
SITE SERVER
3. RelayTo
SMS PROVIDER

TAKEOVER-5

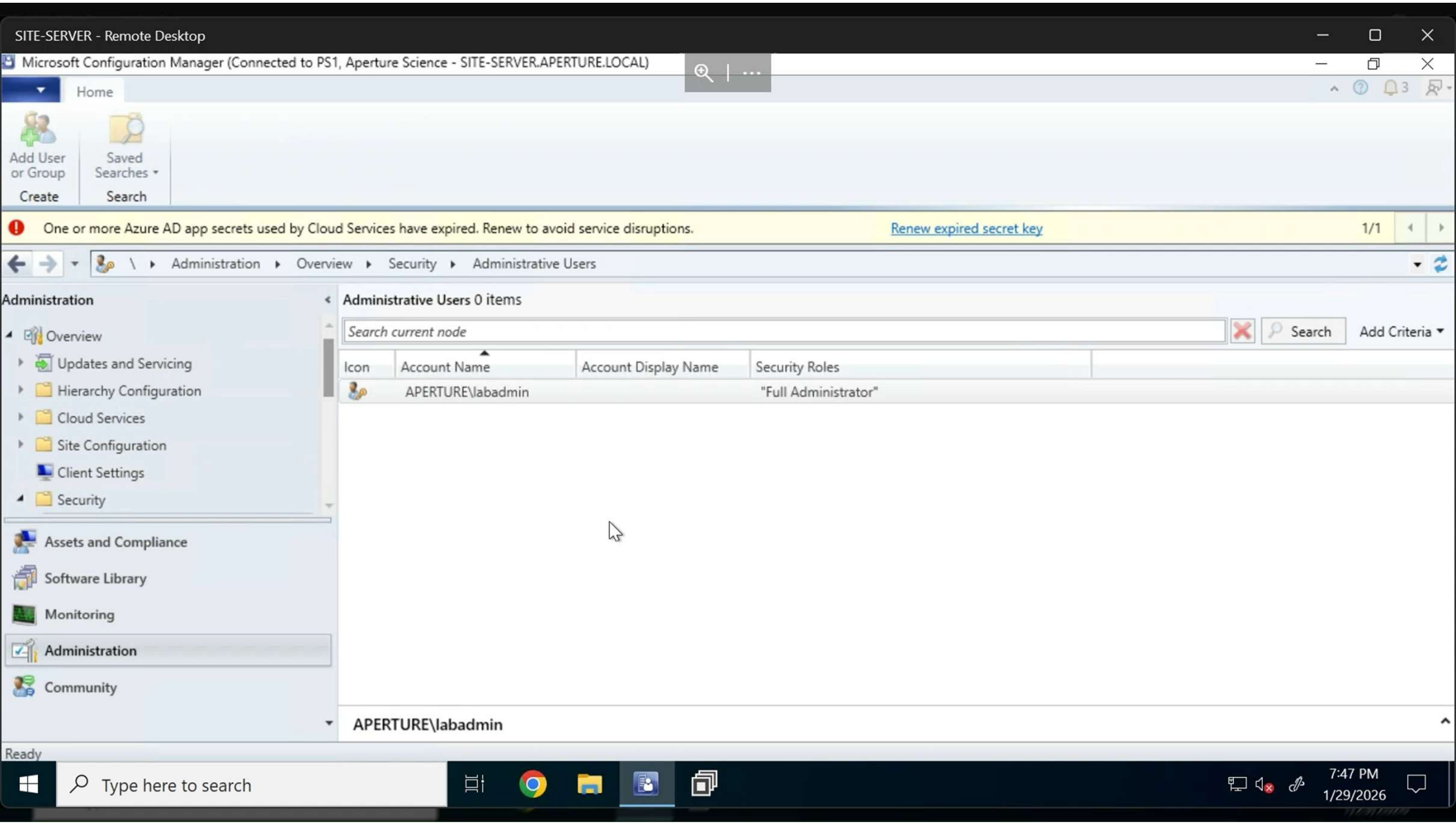

SITE DATABASE
PRIMARY SITE
4. GrantAccess
DeploySoftwareTo
sysadmin
2. AuthTo
SITE SERVER
1. CoerceFrom
CLIENTS
ATTACKER
3. RelayTo
SMS PROVIDER

TAKEOVER-5


SITE DATABASE
PRIMARY SITE
4. GrantAccess
5. DeploySoftwareTo
MANAGEMENT POINT
GetTasks
CLIENTS
2. AuthTo
SITE SERVER
sysadmin
1. CoerceFrom
ATTACKER
3. RelayTo
GetFiles
SMS PROVIDER
DISTRIBUTION POINT

TAKEOVER-5


PRIMARY SITE
GrantAccess
DeploySoftwareTo
CLIENTS
ATTACKER


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 ▸ Overview ▸ Security ▸ Administrative Users
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Client Settings
Security
Assets and Compliance
Software Library
Monitoring
Administration
Community
Administrative Users 0 items
Search current node
Search
Add Criteria
Icon
Account Name
Account Display Name
Security Roles
APERTURE\labadmin
"Full Administrator"
APERTURE\labadmin
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

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/

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.

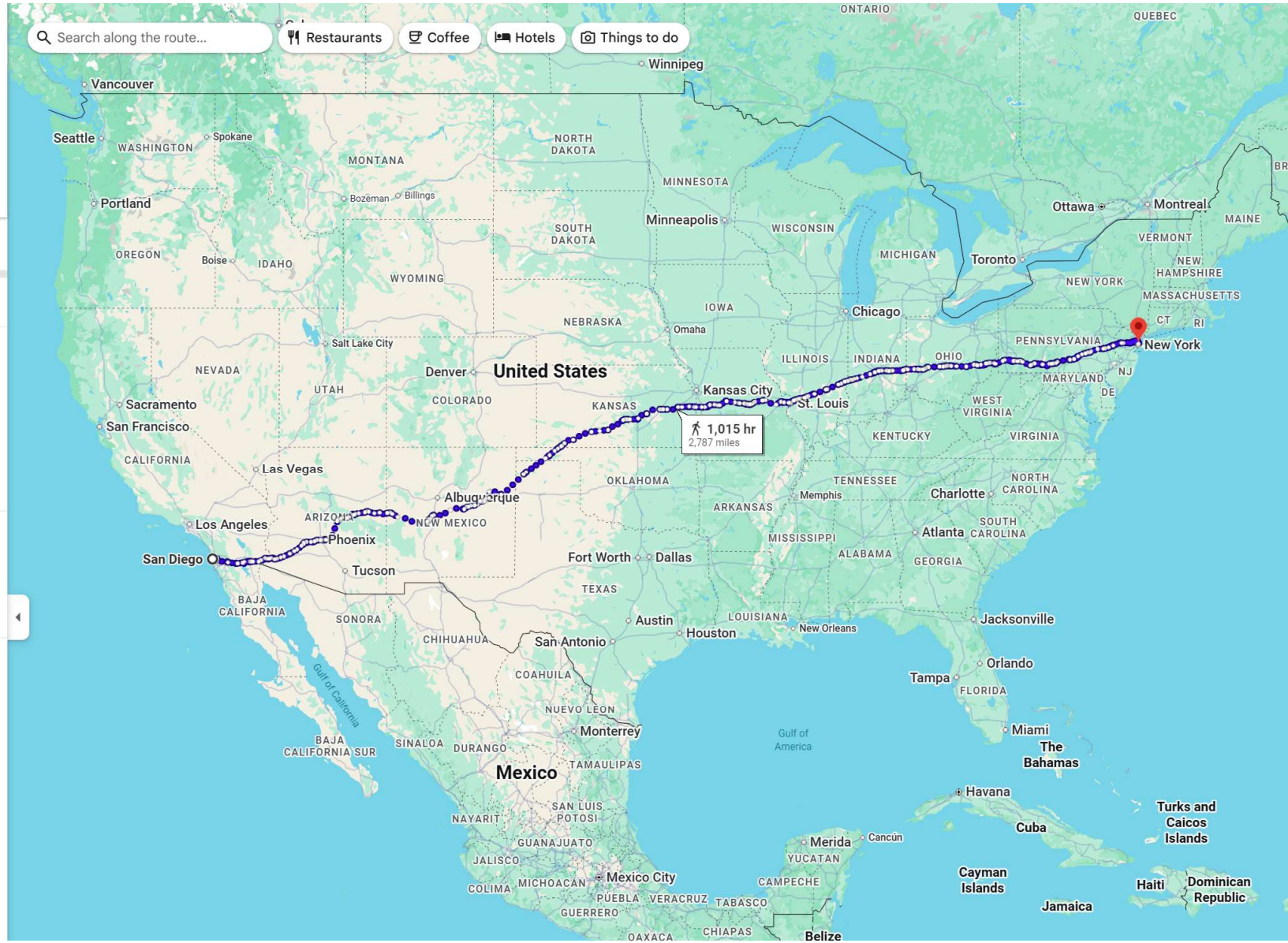
⚠ Your destination is in a different time zone.

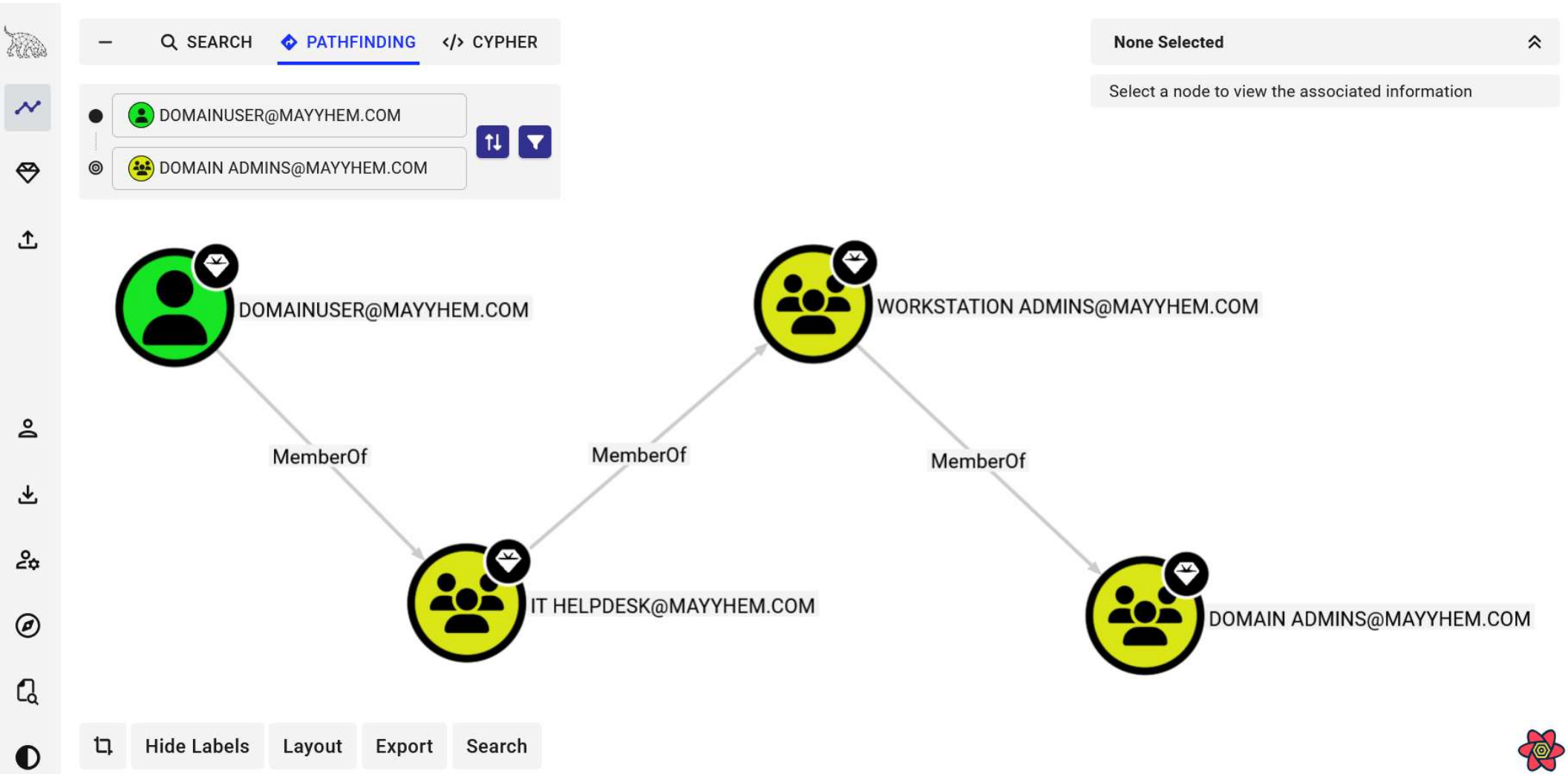
Details Preview

↑ 70,121 ft · ↓ 70,089 ft

8,153 ft

-3 ft




SEARCH
PATHFINDING
CYPHER
None Selected
Select a node to view the associated information
DOMAINUSER@MAYYHEM.COM
DOMAIN ADMINS@MAYYHEM.COM
DOMAINUSER@MAYYHEM.COM
WORKSTATION ADMINS@MAYYHEM.COM
MemberOf
MemberOf
MemberOf
IT HELPDESK@MAYYHEM.COM
DOMAIN ADMINS@MAYYHEM.COM
Hide Labels
Layout
Export
Search

OPENGRAPH

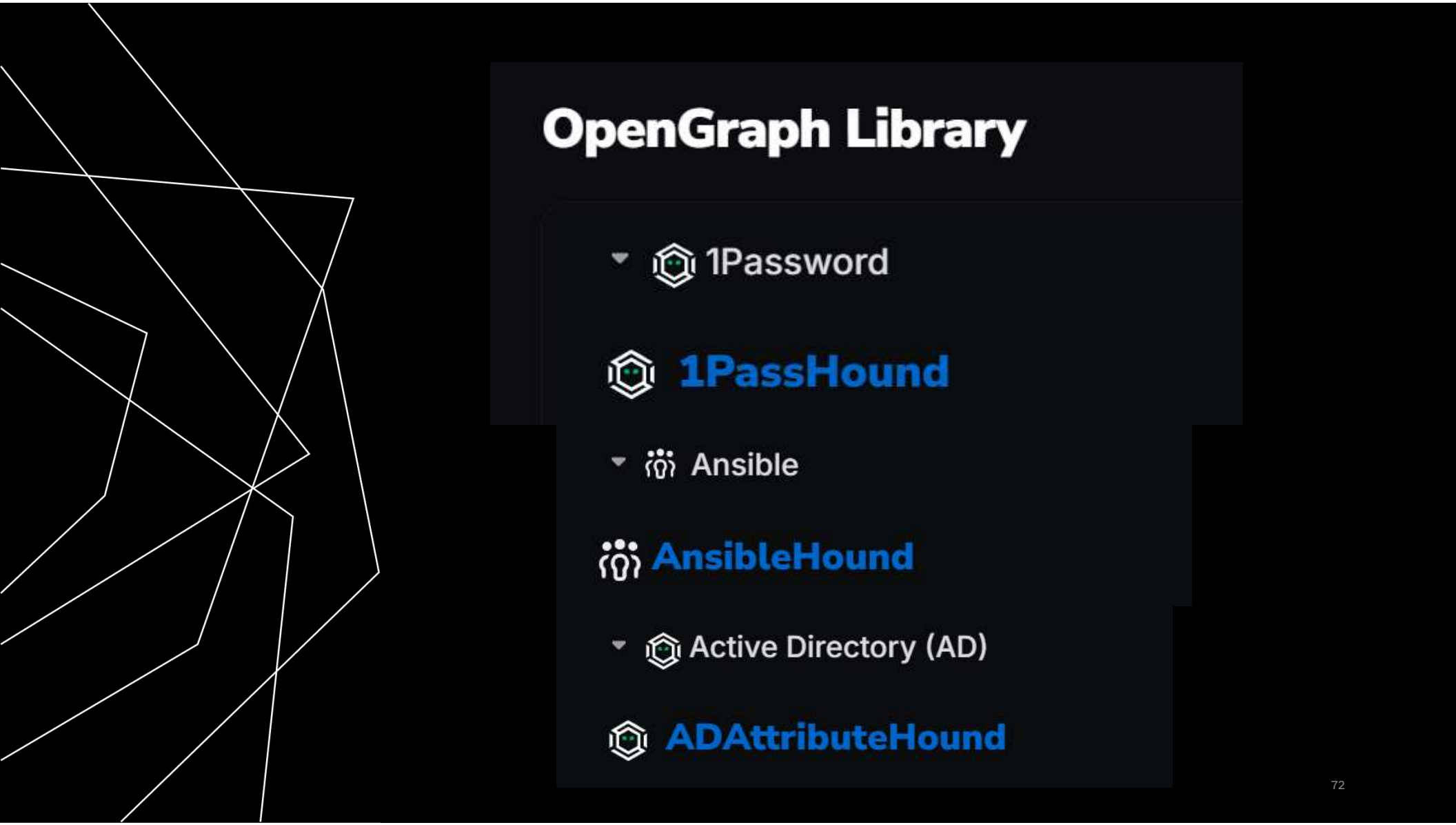
https://bloodhound.specterops.io/opengraph/library

BLOODHOUND

Attack path management for:

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

https://bloodhound.specterops.io/

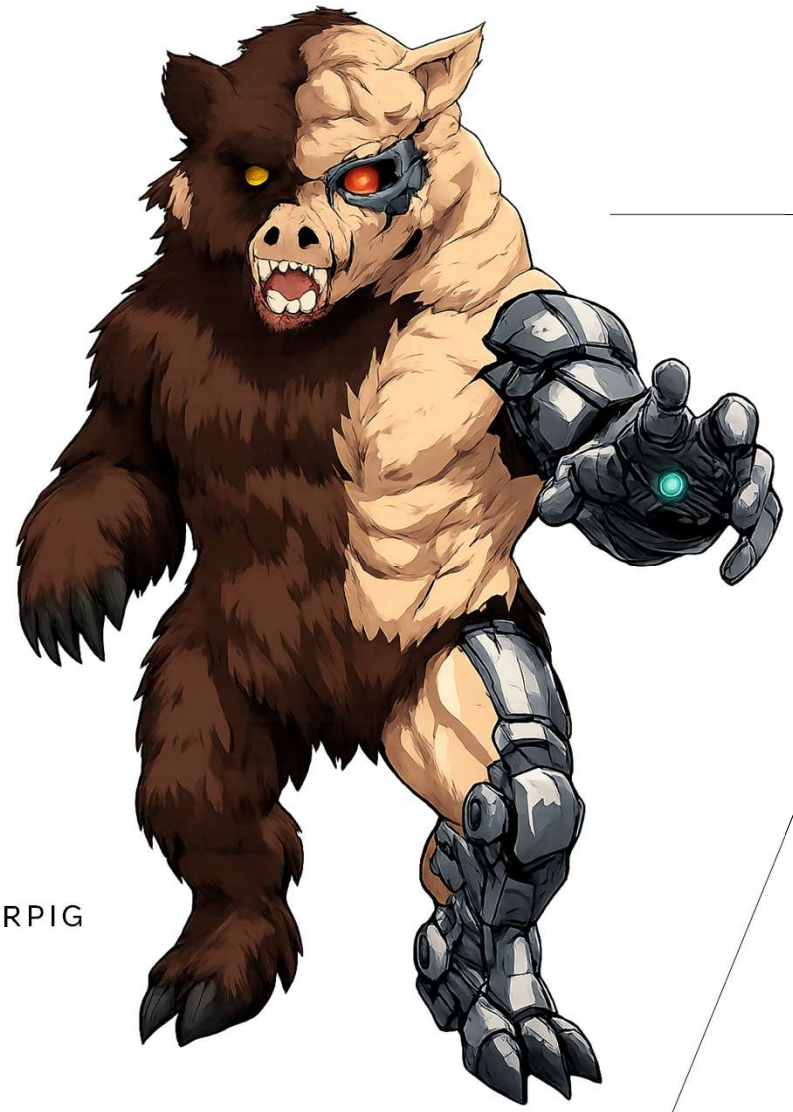

OpenGraph Library
1Password
1PassHound
Ansible
AnsibleHound
Active Directory (AD)
ADAttributeHound

Unfortunately...

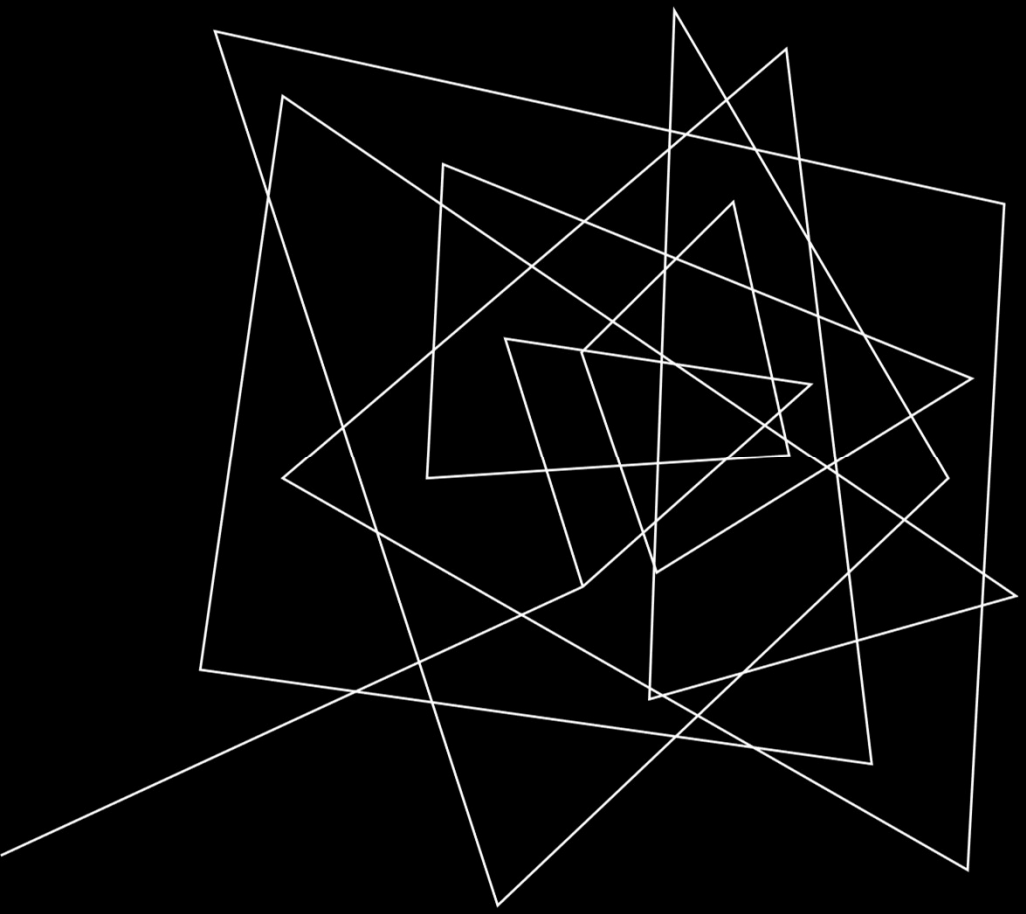
The name **SCCMHOUND** was already taken

ConfigManBearPig

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



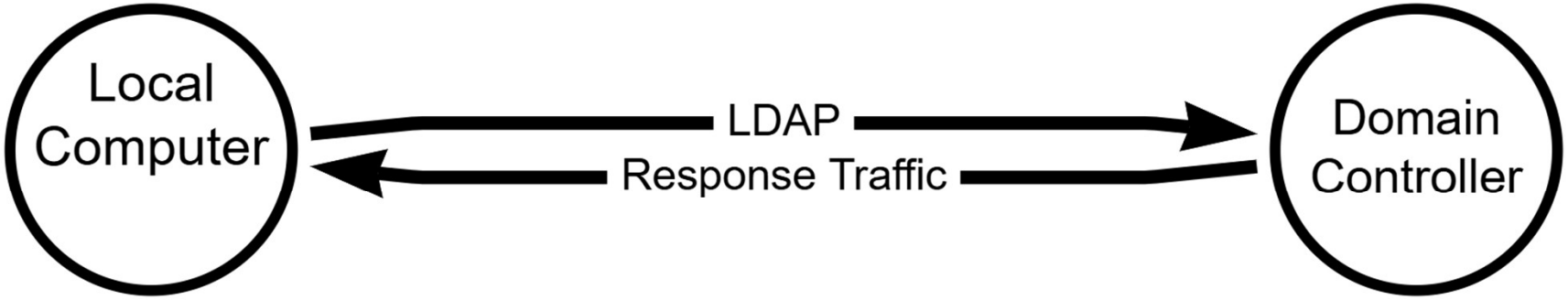
HTTPS://GITHUB.COM/MAYYHEM/CONFIGMANBEARPIG



COLLECTION

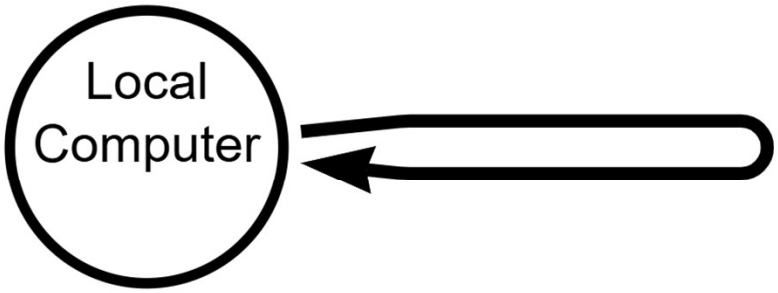
RUN ONCE PHASES

LDAP



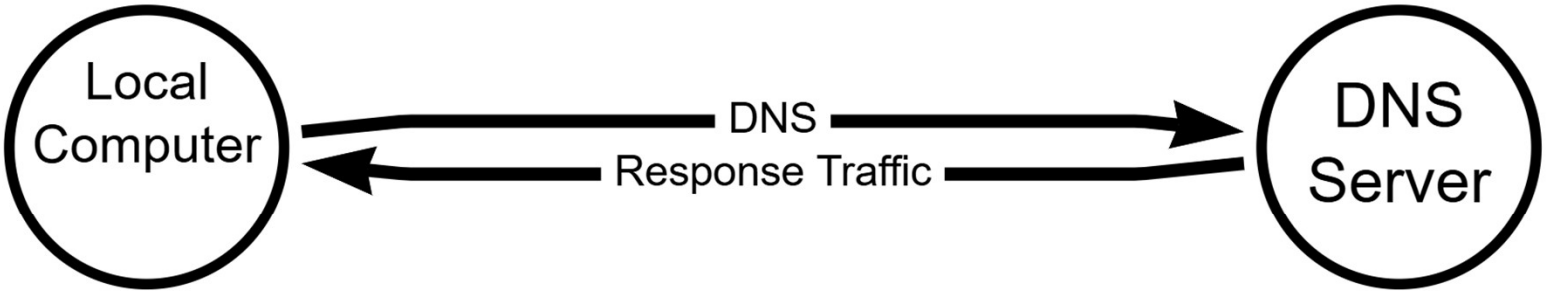
- Reads from System Management container in Active Directory
- Discovers:
  - sites, site servers, fallback status points, management points

LOCAL

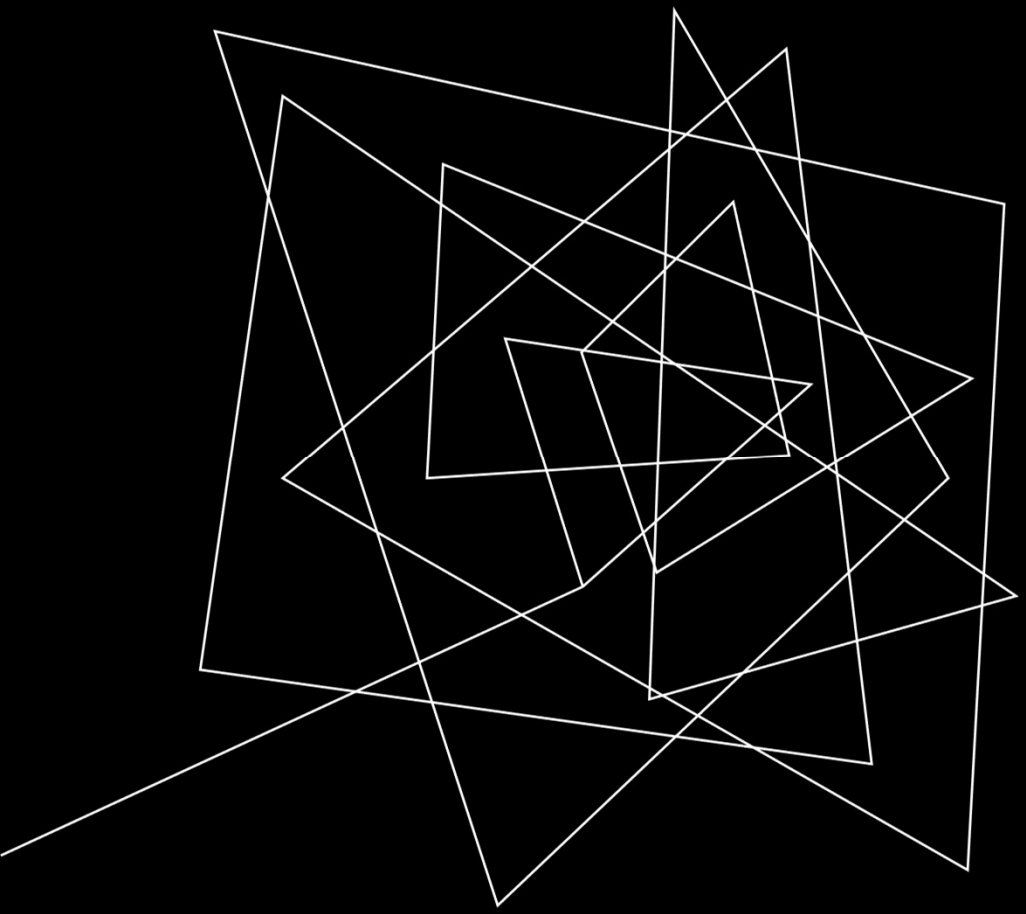


- Reads logs on disk
- Discovers:
  - management points, distribution points
- DPAPI-decrypts network access accounts if you risk detection

DNS



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



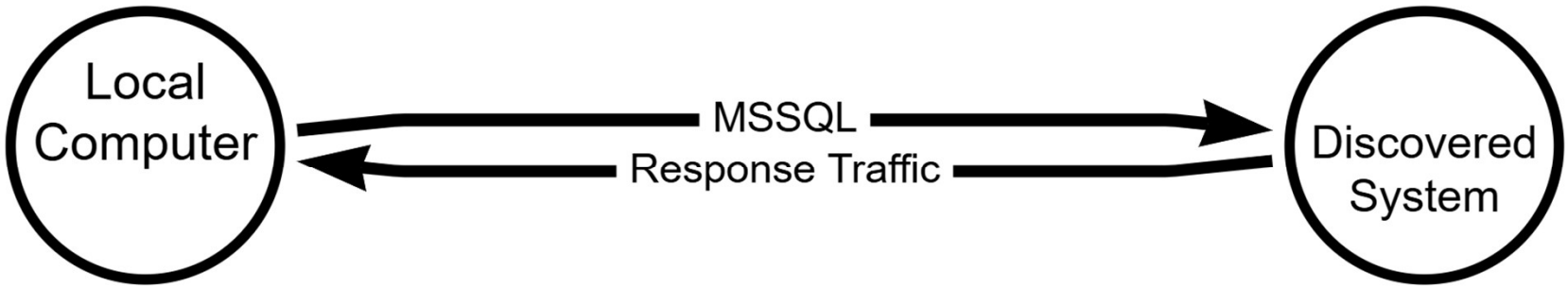
COLLECTION

PER HOST PHASES

REMOTE REGISTRY

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

MSSQL

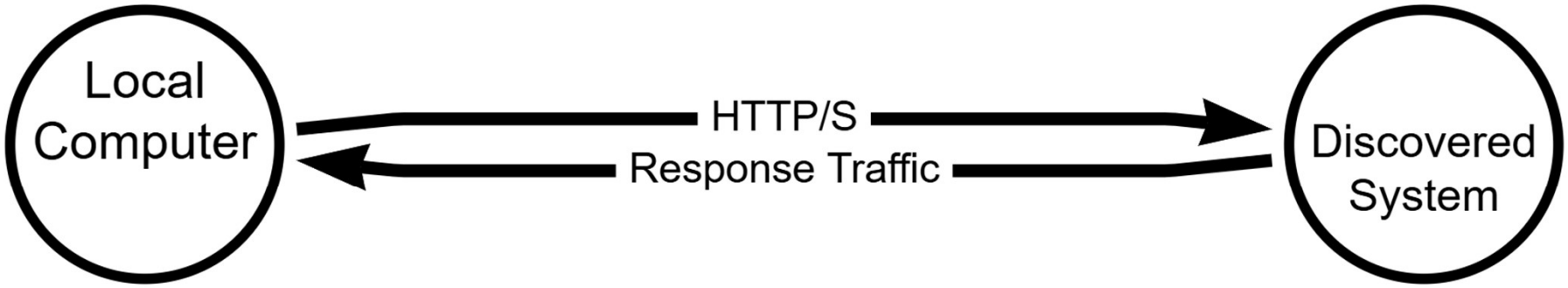


- Identifies extended protection for authentication settings
- Discovers:
  - site database servers, server and database principals

ADMINSERVICE

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

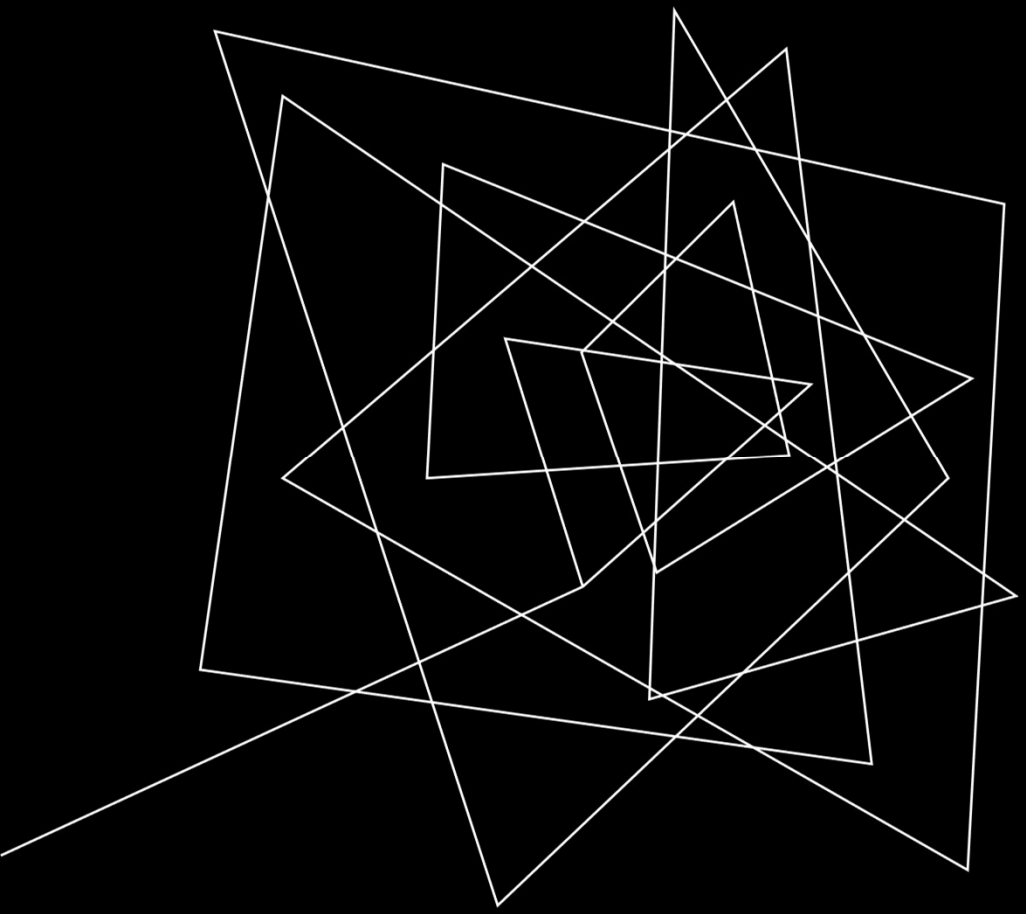
HTTP



- 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

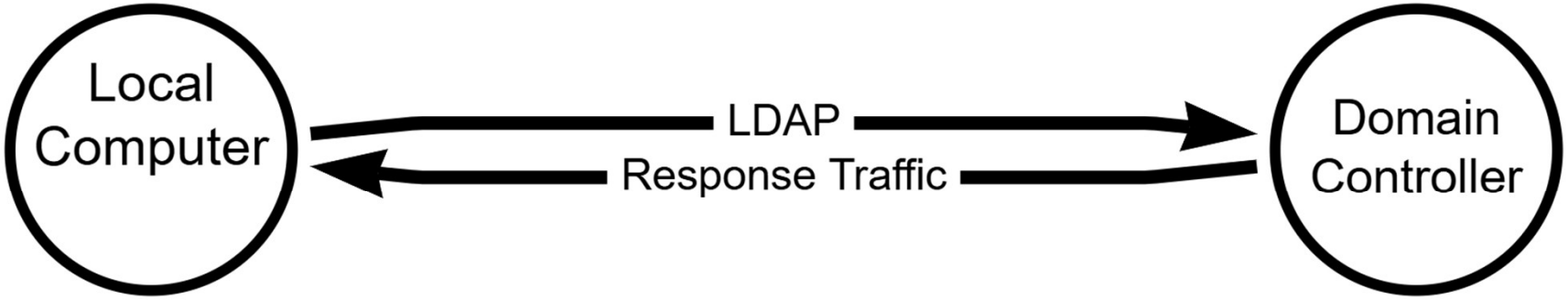
ALLOW ACCESS TO DATABASES... AND MORE

MSSQLHound

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

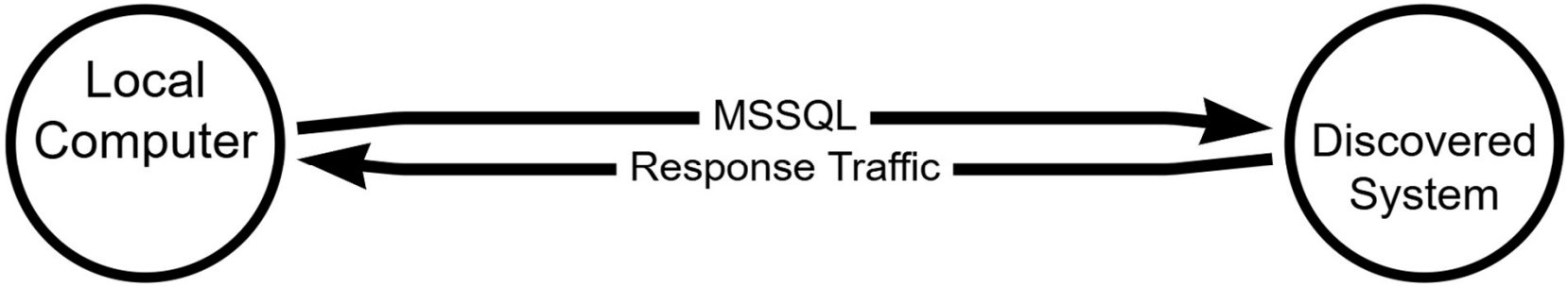
HTTPS://GITHUB.COM/SPECTEROPS/MSSQLHOUND

LDAP

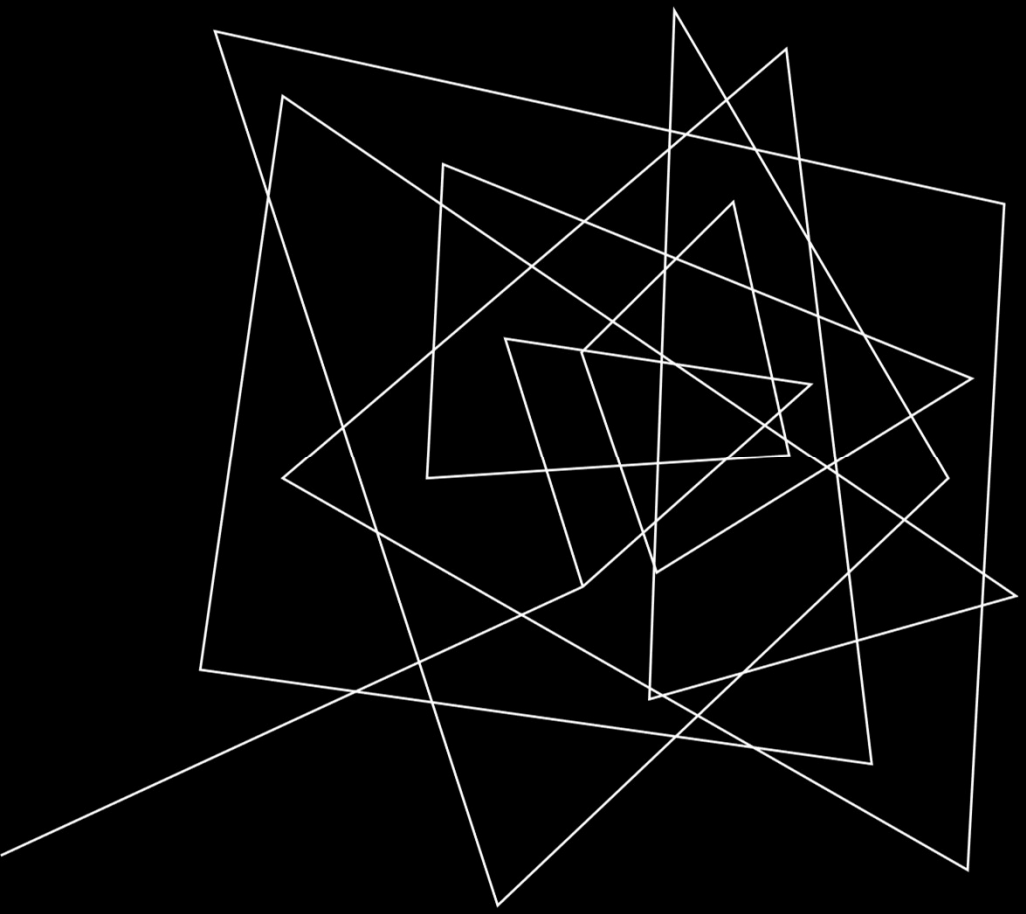


- Searches for computers with MSSQLSvc service principal names
- Discovers:
  - MSSQL hostnames, ports, and instance names

MSSQL



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



POST-PROCESSING

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

GRAPHING ATTACK PATHS DEMO

THANK YOU!

Chris Thompson

X: @_Mayyhem

Slack: @Mayyhem

GitHub: Mayyhem