Detecting Configuration Manager Attack Paths

SCCM Focused Detections and Evasions

Joshua Prager

SpecterOps

Joshua Prager

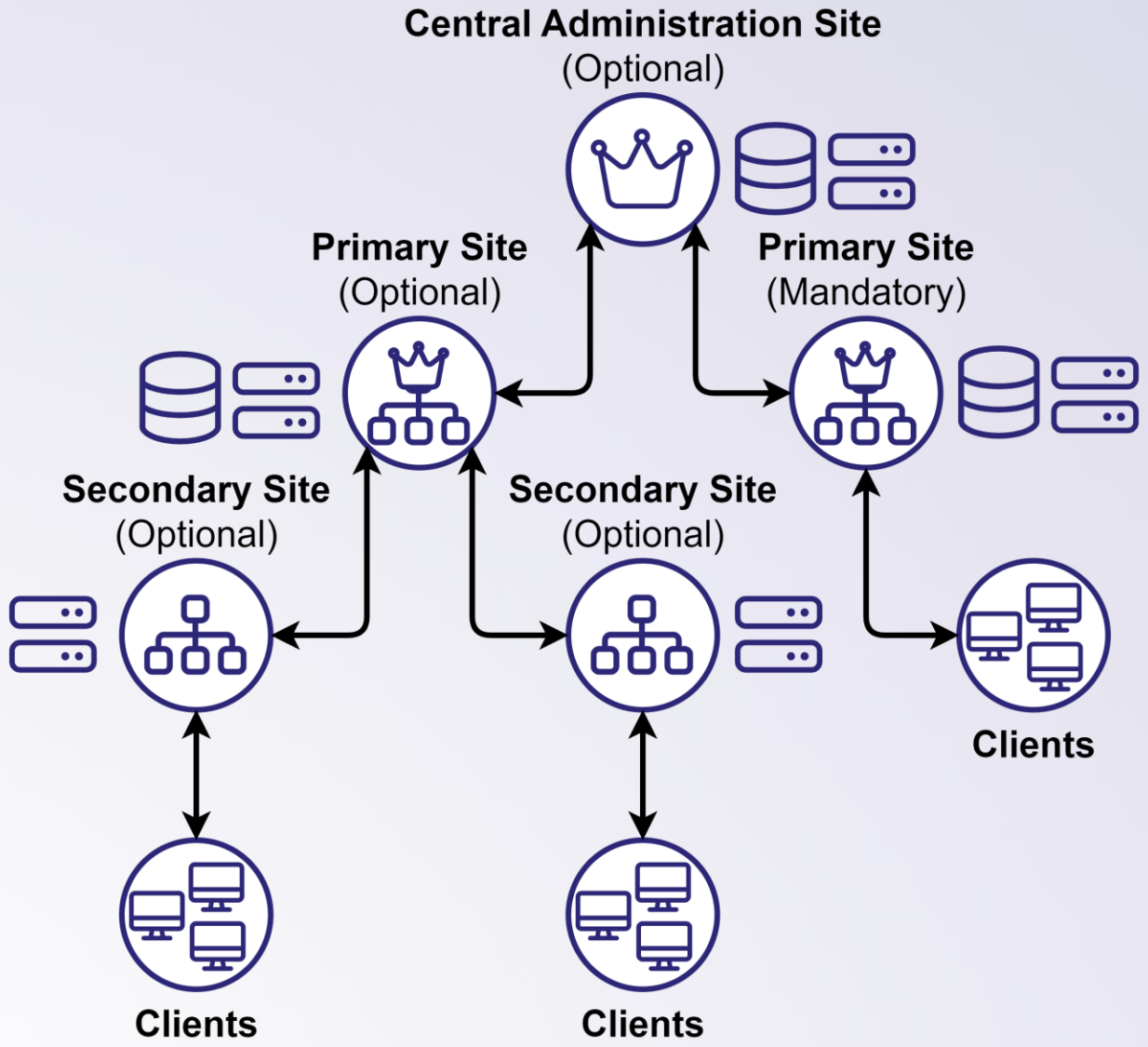
- Principal Consultant, Adversary Detection at SpecterOps
- US Enlisted Navy Veteran (‘09 – ‘17)
- NYU Cyber Fellowship Alumni ‘24
- Contributor to Misconfiguration Manager
- X: @praga_prag
- Blogs

SPECTEROPS SO-CON 2025

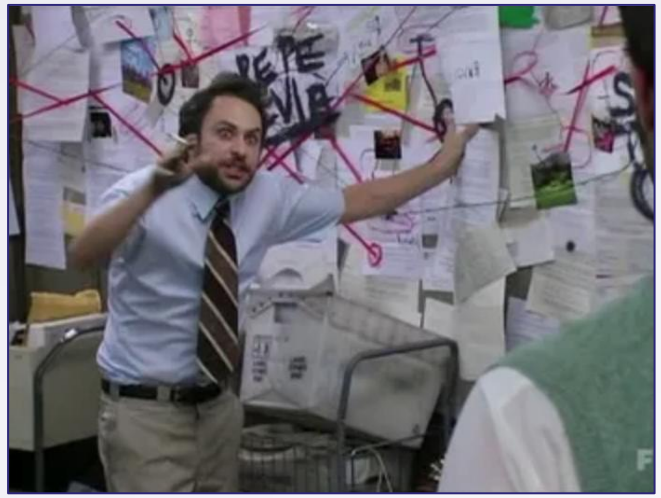
SCCM Primer

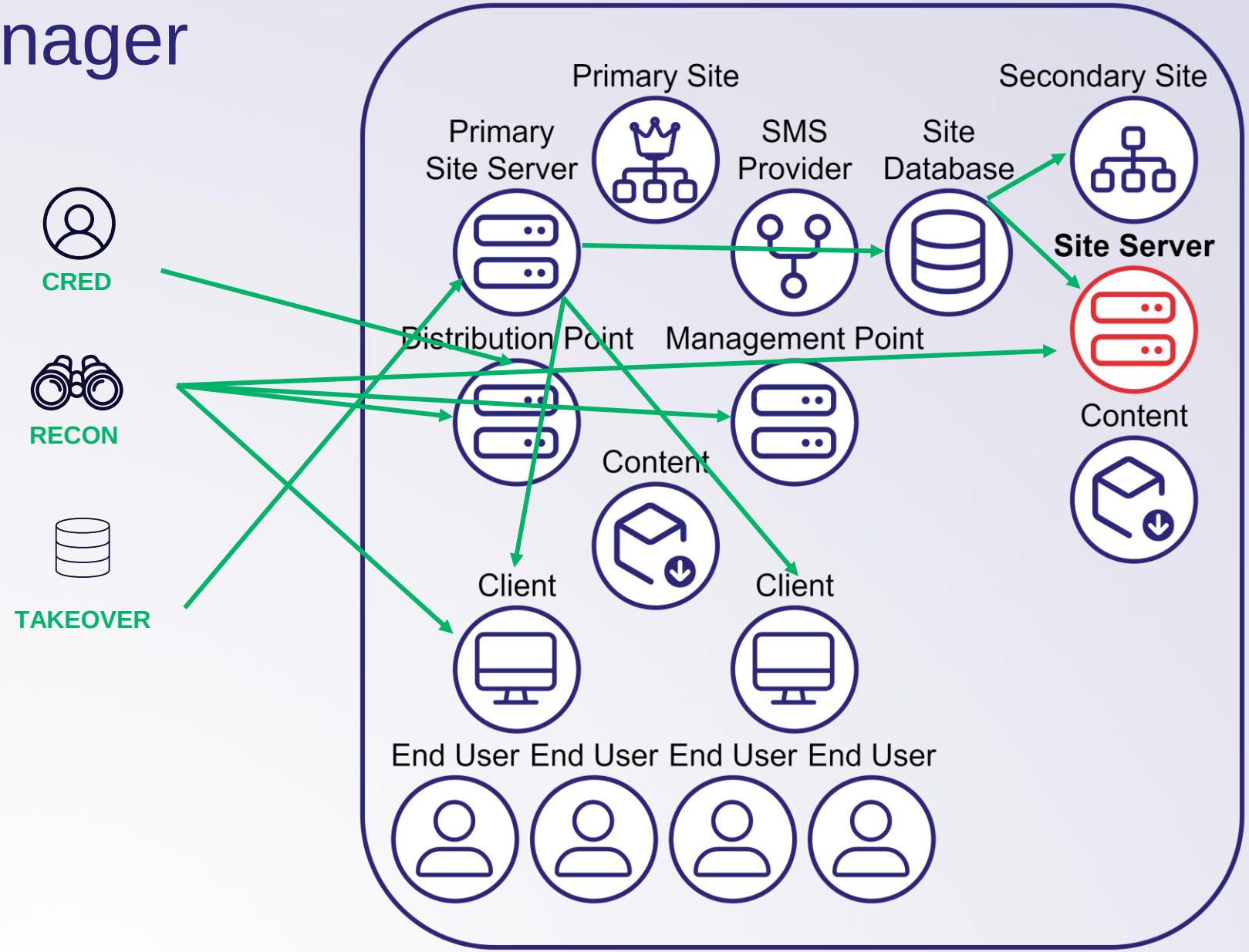
Overview

- Enables wide-scale deployment of applications, software updates, operating systems, and compliance settings
- Allows real-time management of servers, desktops, and laptops
- Intended for **on-premises endpoint management**, whereas Intune is Microsoft's solution for cloud-based endpoint management



Configuration Manager Attack Paths





Misconfiguration Manager Taxonomy

Because "Hierarchy takeover via NTLM coercion and relay to MSSQL on remote site database" does not roll off the tongue…

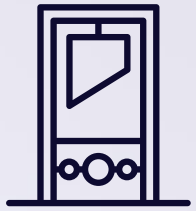
Attack Techniques

RECON

CRED

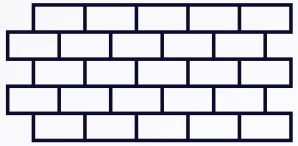
ELEVATE

TAKEOVER



EXEC

Defense Techniques



PREVENT

DETECT

CANARY

Misconfiguration Manager Introduction

Knowledge-base to manage Configuration Manager attack paths

- ***Misconfiguration Manager*** is a knowledge-base of known Configuration Manager abuse attack paths, prevention controls, and detection guidance.
- Introduced a taxonomy to simplify concepts inspired by SaaS Attacks Matrix
- Contains detailed step-by-step foundational, offensive, and defensive write-ups for most known techniques
- Authored by:
  - Duane Michael
  - Chris Thompson
  - Garrett Foster

Misconfiguration Manager

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
PXE Credentials	App Deployment	App Deployment	Relay to Site Server SMB	App Deployment	PXE Credentials	LDAP Enumeration	Relay to DB MSSQL	CMPivot		CMPivot
	Script Deployment	Script Deployment	Relay Client Push Installation	Script Deployment	Policy Request Credentials	SMB Enumeration	Relay to DB SMB	Relay Client Push Installation		
		ADCS Relay	Relay to DB MSSQL		DPAPI Credentials	HTTP Enumeration	Relay to Site Server SMB			
		LDAP Relay	Relay to LDAP		Legacy Credentials	CMPivot	App Deployment			
			Relay to DB SMB		Site Database Credentials	SMS Provider Enumeration	Script Deployment			
			Relay to ADCS		Client Push Installation Account	Site Server Enumeration	Relay to Site System SMB			
			Relay CAS to Child		Distribution Point Looting	Local File Enumeration	Relay CAS to Child			
			Relay to AdminService				Relay to SMS Provider SMB			
			Relay to SMS Provider SMB				SQL Linked as DBA			
			Relay between HA							
			SQL Linked as DBA							
			Relay to Site DB							

Configuration Manager Attack Paths

SCCM Abuse Impact

- Configuration Manager attack paths can lead to domain compromise
  - In most cases, organizations use SCCM to manage critical assets (tier 0 endpoints)
  - SCCM client control is powerful (application pushes, script execution, reconfigurations, etc)
  - Frequent misconfigurations in SCCM environments provides multiple attack vectors to site takeover

Configuration Manager Attack Paths

SCCM Abuse Impact

- Site Takeover enables an attacker full control of all systems in the hierarchy
  - Site databases are replicated to all sites in the hierarchy
    - E.g., Adding an admin to the site databases replicates that admin to the CAS and other primary sites
  - If an attacker successfully takes over any one primary site – they takeover the entire hierarchy

Configuration Manager Site Takeover

SCCM Abuse Impact

- Takeover attack paths leverage NTLM Coercion and Relay
  - Primary Site Server server's domain computer account must be:
    - Local admin on the site database server
    - Sysadmin in the Site Database
    - Local admin on every other site system role
  - By default, the Primary Site Server’s account is DBA on the site database server and a local admin on every site system role

Detection Focus

Detections Introduced:

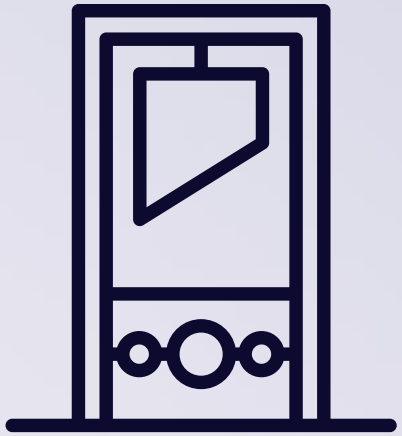
- Monitor Application Deployment
- Monitor Group Membership Changes (SMS Admins)
- Monitor Group Membership Changes (RBAC_Admins table)
- Read Access to SMSTemp
- Monitor Winreg Named Pipe Connections
- Monitor Local SCCM File Access

Presentation does NOT cover:

- Walkthroughs of *all* offensive techniques in Misconfiguration Manager
- Specific preventative controls walkthroughs
- Comprehensive treatment of topics discussed

Monitor Application Deployment

Misconfiguration Manager DETECT- 4



SCCM allows administrators to deploy applications to client devices from a specified UNC path, running them as SYSTEM, the currently logged-in user, or a specific user. This functionality can be exploited to execute malicious applications on remote systems.

Attackers can abuse this feature to deploy applications, execute malicious binaries, or relay NTLM authentication to gain lateral movement. Applications can be hidden from the SCCM console, making detection difficult.

The typical operational flow:

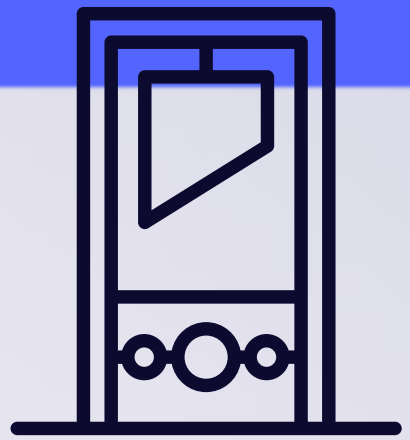
- Create a Collection of devices
- Create an Application and Scope
- Create a Deployment
- Initiate Deployment

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-4/detect-4_description.md

Red vs. Blue

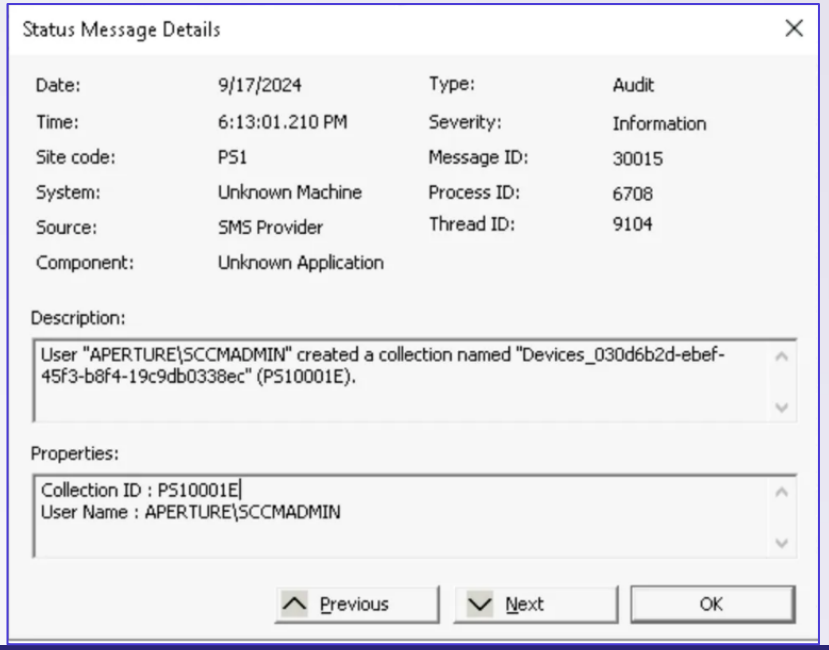
Monitor Application Deployment

Misconfiguration Manager DETECT- 4



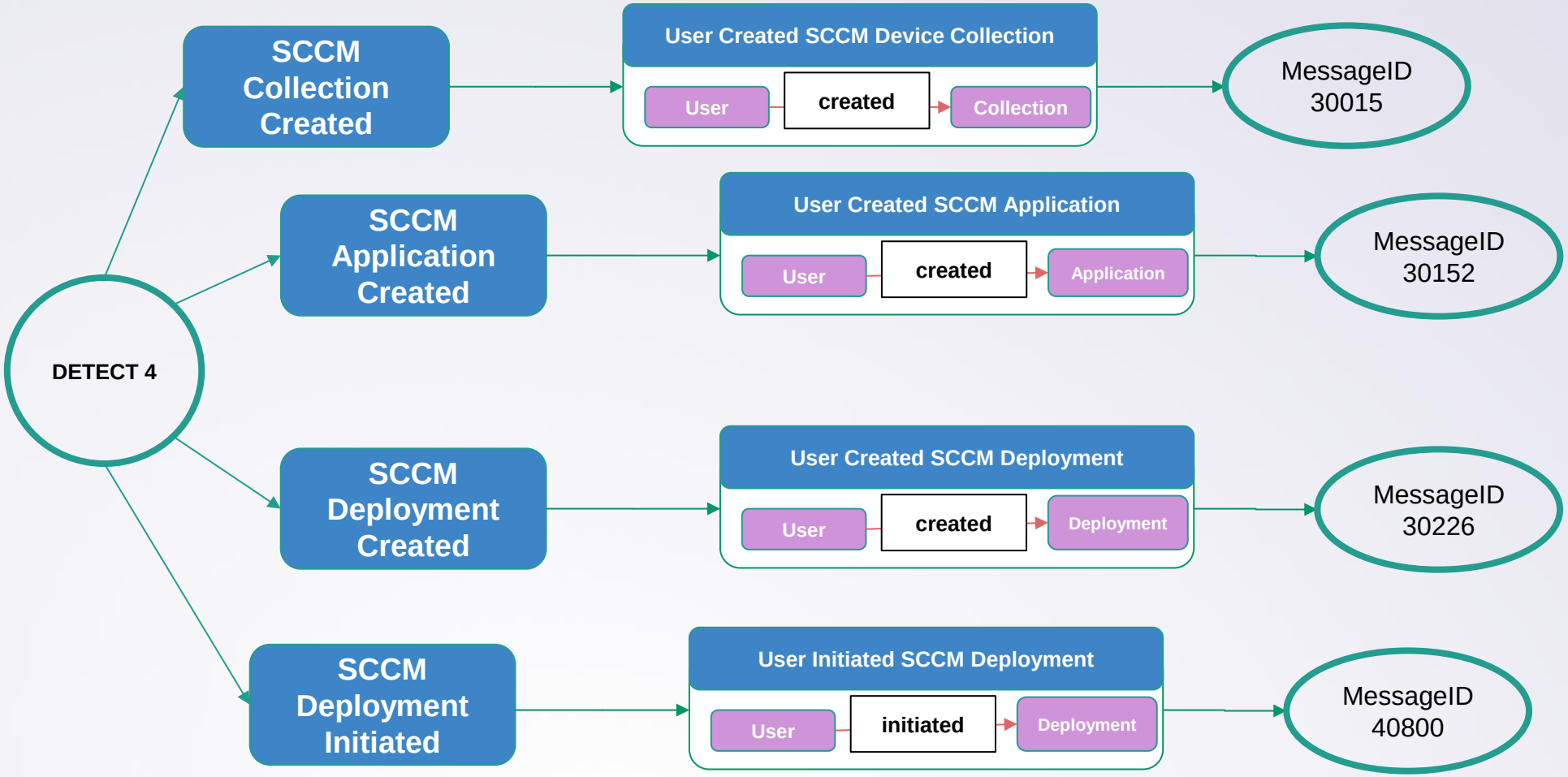
The Configuration Manager Status Message Queue contains Message IDs corresponding to the operational flow previously mentioned.

- The Status Message Queue logs is generated from the ***smsprov.log*** on the CM Site Server and the properties of the log are filled in by querying the MSSQL backend server for CM.



https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-4/detect-4_description.md

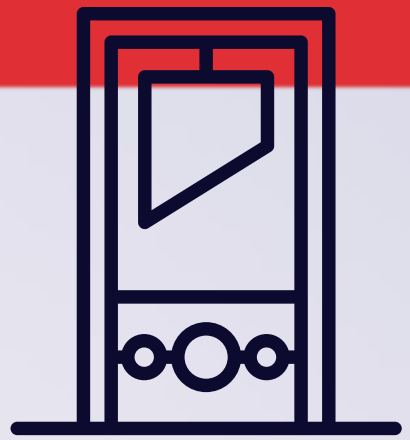
DETECT - 4



https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-4/detect-4_description.md

Script Deployment

Evasion for Misconfiguration Manager DETECT- 4



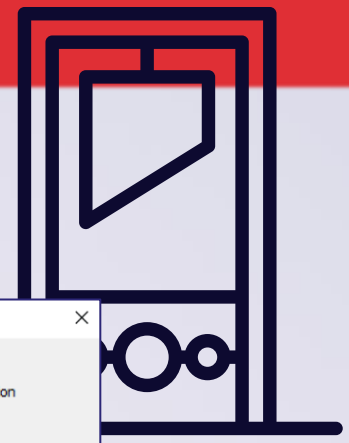
Instead of deploying an application or payload, consider using a PowerShell script deployment instead.

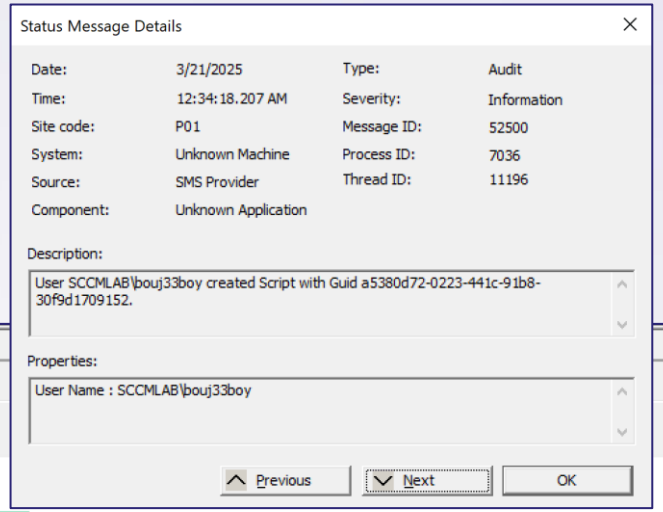
- Executes in System context
- Target Artifacts:
  - CcmExec.exe -> powershell.exe
- The Status Message Queue logs will still generate telemetry. However, there are less events related to script execution:
  - Message ID: 52500 – Script Created
  - Message ID: 52501 – Script Executed

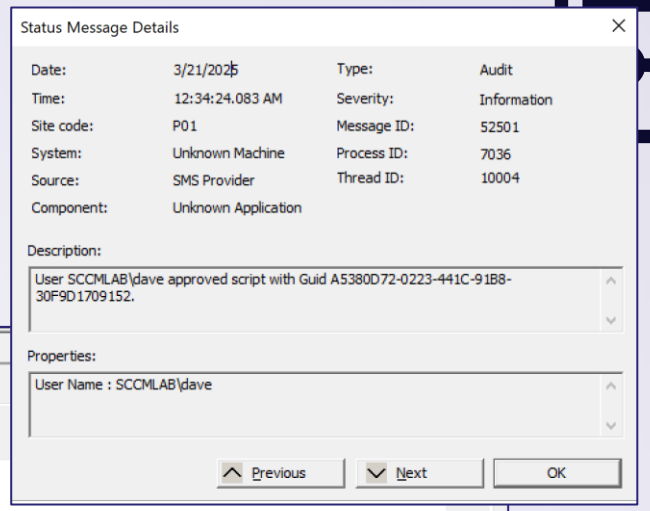
https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-4/detect-4_description.md

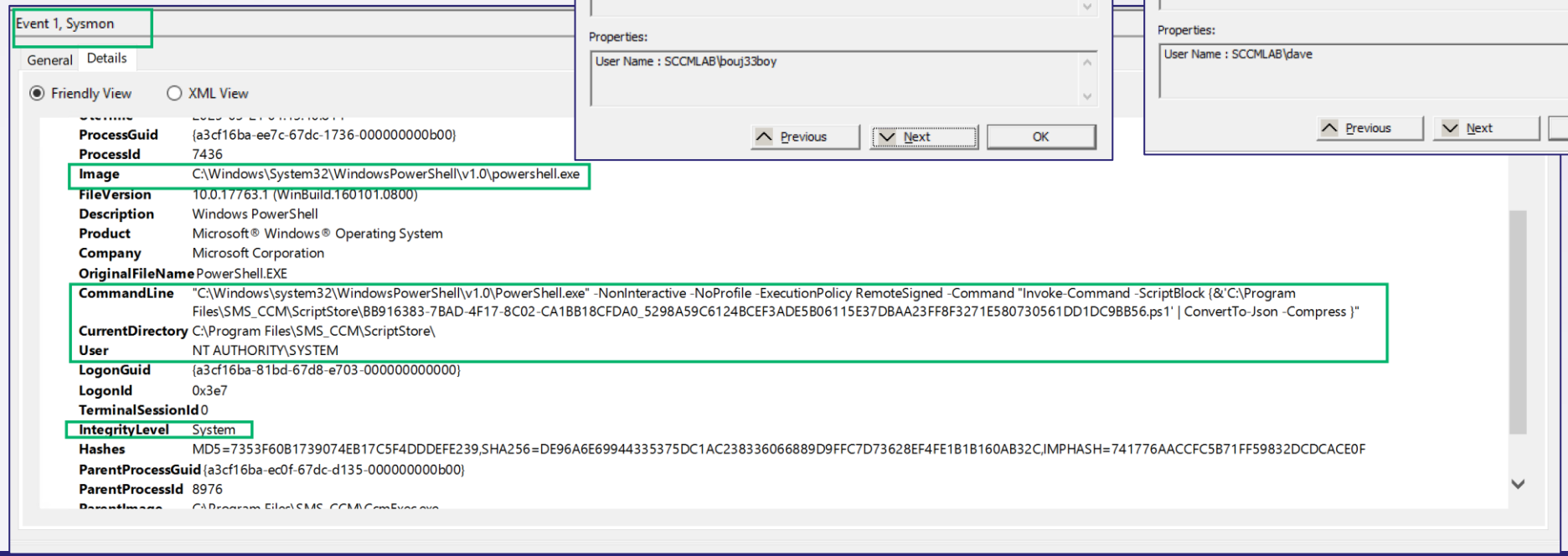
Script Deployment

Evasion for Misconfiguration Manager DETECT- 4





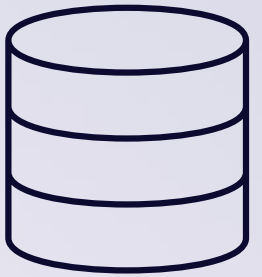




https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-4/detect-4_description.md

Monitor Group Membership Changes

Misconfiguration Manager DETECT- 5 & 6



The ***SMS Admins*** security group and the ***RBAC_Admins*** table represent the local security group with direct write access to a WMI provider, SMS Provider, for Configuration Manager.

When attackers add a Full Administrator to the ***RBAC_Admins*** and ***RBAC_ExtendedPermissions*** tables in the site database, the account is then added to the ***SMS Admins*** group on the endpoints hosting the SMS Provider role.

- The site database is replicated to all sites…
- If the attacker adds a full administrator to these tables in one primary site database – **they are full admin on the entire SCCM hierarchy**

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-5/detect-5_description.md

Red vs. Blue

Monitor Group Membership Changes

Misconfiguration Manager DETECT- 5 & 6

SMS Admins is a security group. Defenders can leverage object access auditing to determine changes (e.g., **Event ID: 4732**, new member added) to detect changes to the security group.

Auditing ***RBAC_Admins*** and ***RBAC_ExtendedPermissions*** tables in the site database require a custom solution to detect changes.

- Custom SQL Audit in the site database can be aimed at the tables
- This will generate an **Event ID: 33025** in the Application log

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-6/detect-6_description.md

Monitor Group Membership Changes

Misconfiguration Manager DETECT- 5 & 6

User Inserted Into RBAC_Admins Table

Audit event: audit_schema_version:1

event_time:2024-10-23 03:11:01.1300947

sequence_number:1

action_id:IN
…SNIP…

database_name:CM_PS1

schema_name:dbo

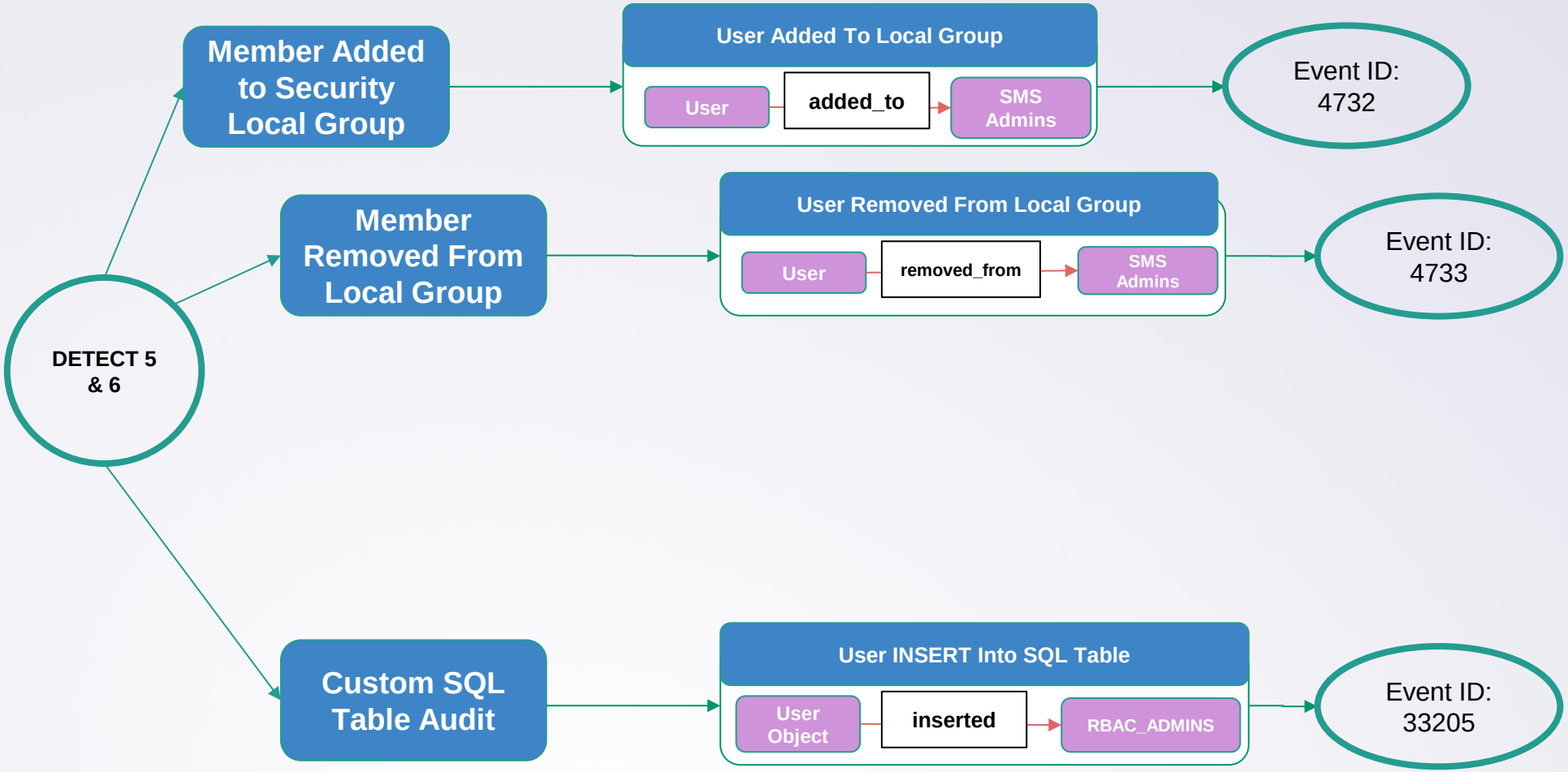
object_name:**RBAC_Admins**

statement:**INSERT INTO RBAC_Admins** (AdminSID, LogonName, IsGroup, IsDeleted, CreatedBy, CreatedDate, ModifiedBy, ModifiedDate, SourceSite) SELECT 0x0105000000000005150000007D2E52AA5AD54377C5FC12F357040000, '**APERTURE\testsubject1**', 0, 0, '', '', '', '', 'ps1' WHERE NOT EXISTS (SELECT 1 FROM RBAC_Admins WHERE LogonName = 'APERTURE\testsubject1')

…SNIP…

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-6/detect-6_description.md

DETECT – 5 & 6



https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-6/detect-6_description.md

Nested Group Membership Changes

Evasion Misconfiguration Manager DETECT- 5 & 6

SMS Admins is a *local* security group. Typically, individual users will not be added to the local security group, but instead an AD group will be added (e.g., SCCM-Admins)

- *Trading one event ID for another*
- EID: 4728: Adding a member to security enabled AD group

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-6/detect-6_description.md

Monitor Read Access to SMSTemp

Misconfiguration Manager DETECT - 7

SCCM contains a preboot execution environment (PXE) feature which allows systems to load a specific operating system image on boot.

Attackers can recover domain credentials from PXE media if weak passwords are used, potentially transitioning from an unauthenticated network context to a domain-authenticated one, allowing for privilege escalation and lateral movement.

The typical operational flow:

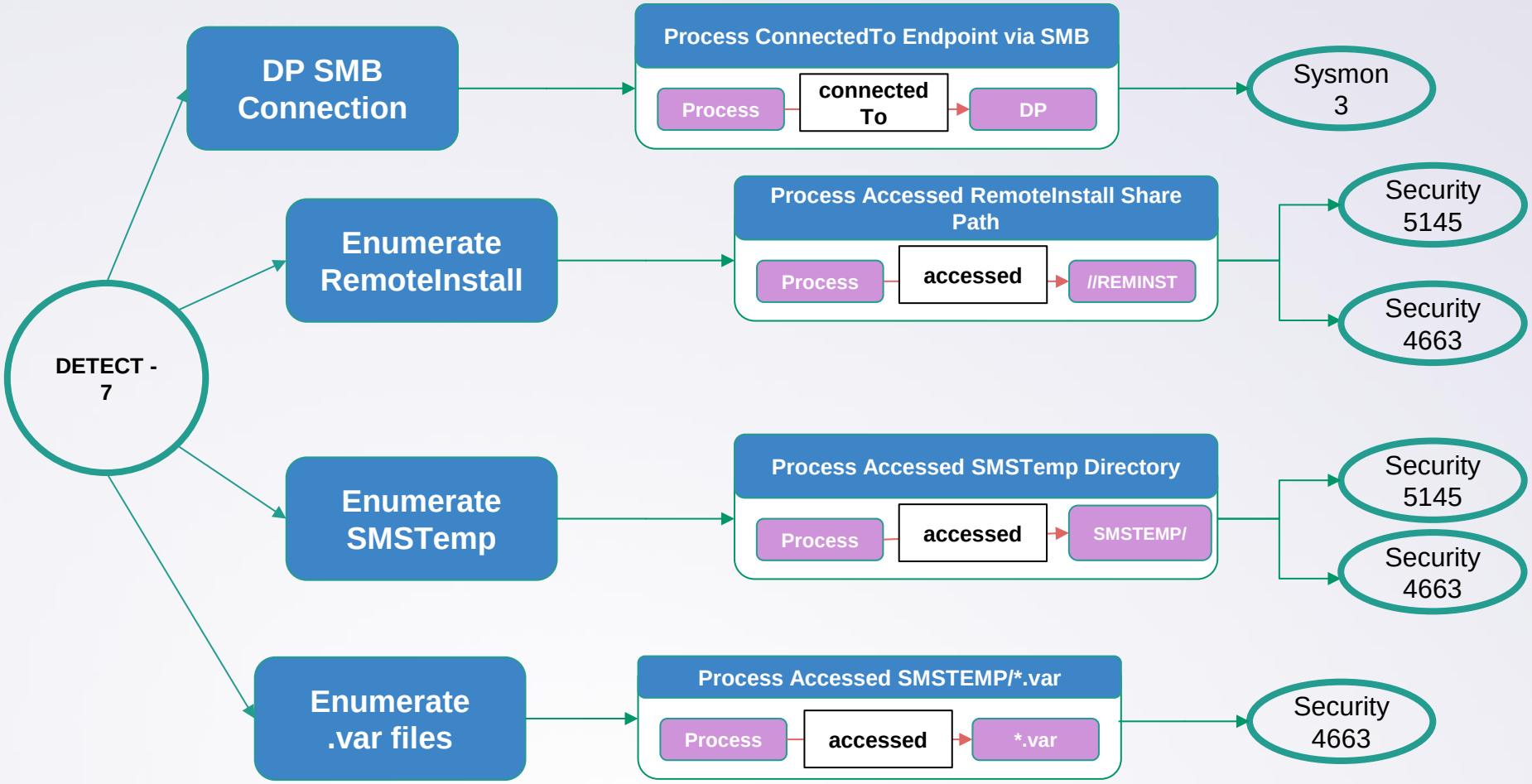
- Connect to Distribution Point via SMB
- Enumerate “REMINST” (Remote Install) share (Windows Deployment Services (WDS) and often contains PXE boot files)
- Enumerate SMSTemp directory

Spider .var extension, which likely contain PXE boot configuration variables

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-7/detect-7_description.md

Red vs. Blue

DETECT - 7



https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-7/detect-7_description.md

Avoid Brute Forcing \\REMINST

Evasion Misconfiguration Manager DETECT - 7

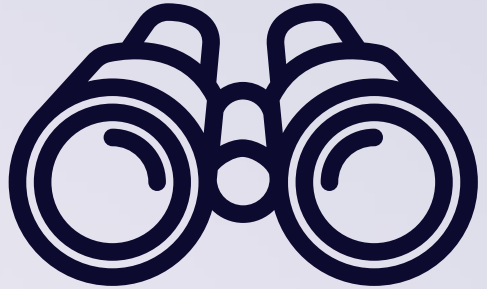
Detections for PXE enum are typically focused on:

- **LDAP Searches for DPs with RemoteInstall child objects**
  - Example: `-LDAPFilter "(objectClass=remoteInstall)"`
  - This would standout if PXE isn't used in the environment
- **Alternatives:**
  - Port Scan DP: UDP 67,68,69,4011,547
  - Remotely Query DP Registry: `Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\SMS\DP" | Select-Object IsPXE, PXEResponderEnabled, PXEInstalled`
  - Query DP SMSPXE Log: `Test-Path C:\Program Files\Microsoft Configuration Manager\Logs\SMSPXE.log`

https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/hierarchy/ports#BKMK_PortsClient-DP3

Remote and Local Enumeration

Misconfiguration Manager DETECT - 8 & 9



Authenticated domain accounts can leverage LDAP, SMB/SMB named pipes, HTTP to *remotely* identify primary (including CAS), secondary site servers, MPs, and DPs.

In an SCCM environment domain controllers contain a container called “System Management” which references the SCCM infrastructure. Some offensive tooling will connect and enumerate the referenced machine accounts in this container.

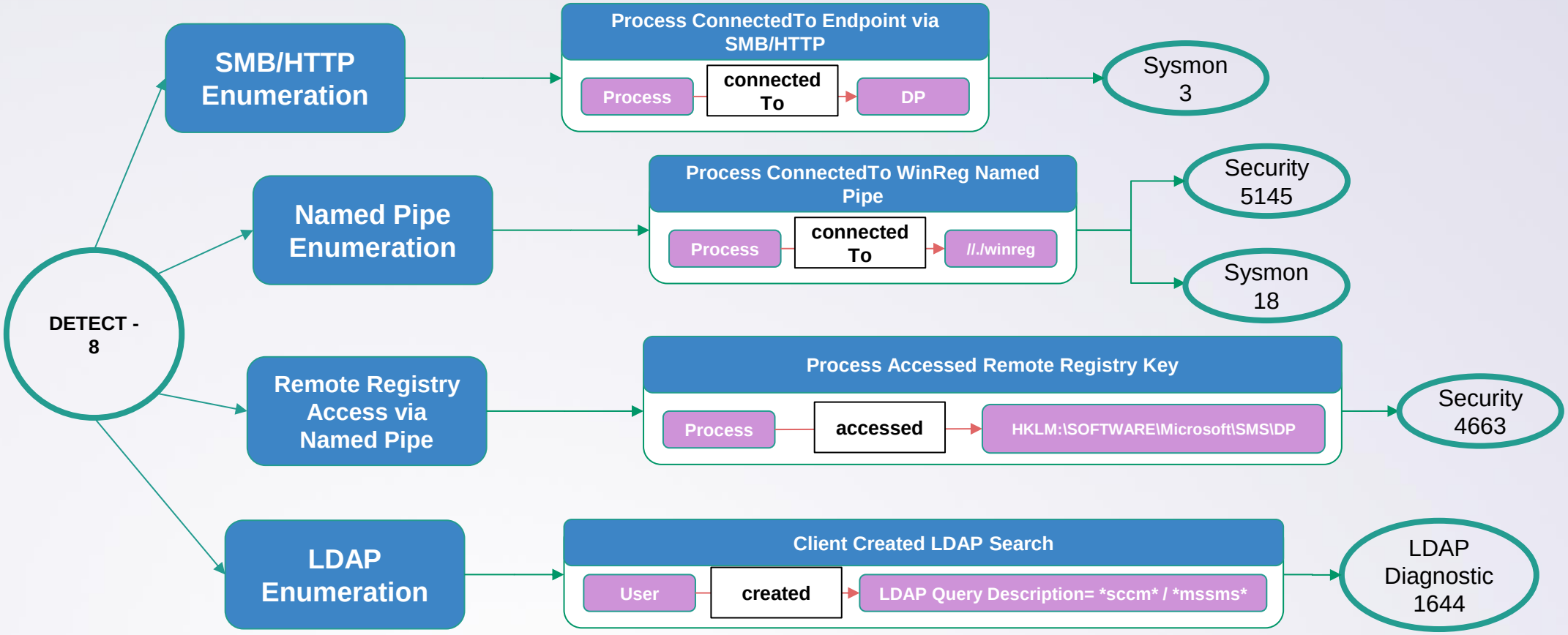
Additionally, local enumeration on SCCM clients works just as well by enumerating key files such as:

- C:\Windows\CCM\Logs\smsts.log
- C:\Windows\ccmcache
- C:\Windows\ccmsetup

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-8/detect-8_description.md

Red vs. Blue

DETECT - 8



https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-8/detect-8_description.md

Remote Enumeration

Evasion Misconfiguration Manager DETECT - 8 & 9

When searching for SCCM infrastructure via LDAP constrain queries to as few as possible (avoid mass enumeration if possible).

Typical detection for anomalous LDAP queries:

- **Mass LDAP queries within a timebucket from 1 user**

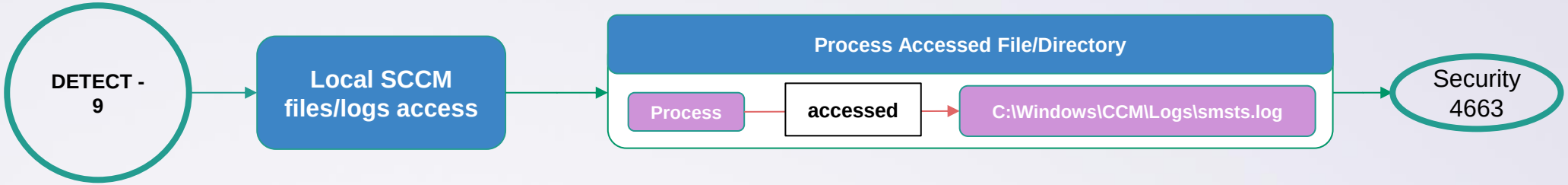
Instead, manually LDAP query Distribution Points

- Ldapsearch ldap://TARGET_IP “DC=sccm,DC=lab” “(cn=*-Remote-Installation-Services)”

OR use local: C:\Windows\SCCM

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-8/detect-8_description.md

DETECT - 9



The SACL could be set on all the following:

- C:\Windows\CCM
- C:\Windows\CCM\Logs\smsts.log
- C:\Windows\ccmcache
- C:\Windows\ccmsetup

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/DETECT/DETECT-9/detect-9_description.md

Resources

Research and Validate

- Josh Prager & Nico Shyne, Detection and Triage of Domain Persistence
- Chris Thompson, SharpSCCM
- Garrett Foster,SCCMHunter SMB Module
- Microsoft, Understanding PXE Boot
- SpecterOps, Cred1py
- Garrett Foster, SCCMHunter Find Module
- Christopher Panayi, Identifying and Retrieving Credentials From SCCM/MECM Task Sequences
- Christopher Panayi, Pulling Passwords Out of Configuration Manager
- Christopher Panayi, PXEThief
- Garrett Foster, Site Takeover via SCCM's AdminService API
- Microsoft Learn, Plan for the SMS Provider

SPECTEROPS

Thank you

Josh Prager | jprager@specterops.com