



DECEMBER 7-8, 2022

BRIEFINGS

Writing Your Own Ticket to the Cloud like APT

A Deep-dive to AD FS Attacks, Detections, and Mitigations

Dr. Nestori Syynimaa & Roberto Rodriguez

whoarewe



Secureworks[®]

Dr. Nestori Syynimaa

Senior Principal Security Researcher



 Microsoft

Roberto Rodriguez

Principal Threat Researcher

*Defenders think in lists.
Attackers think in graphs.
As long as this is true, attackers win.*

John Lambert (2015)

<https://github.com/JohnLaTwC/Shared/blob/master/Defenders%20think%20in%20lists.%20Attackers%20think%20in%20graphs.%20As%20long%20as%20this%20is%20true%2C%20attackers%20win.md>

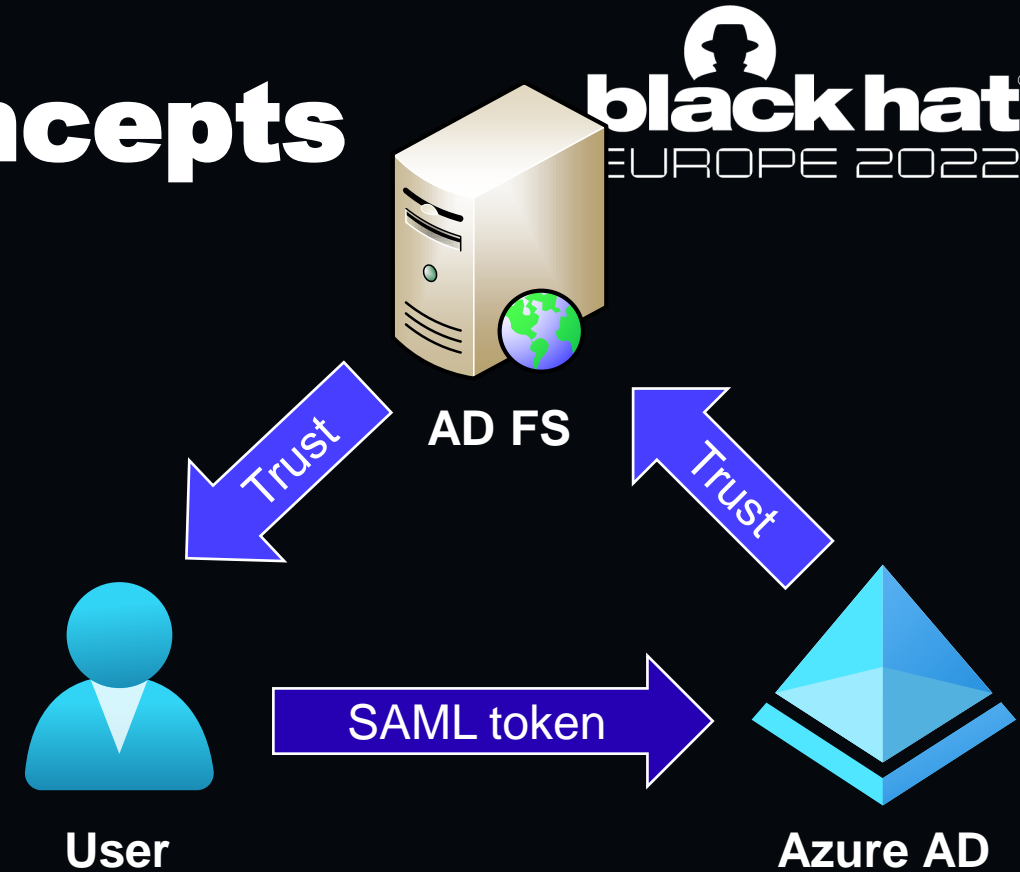
Contents



- Introduction
- AD FS attack & defend graphs
- Protecting against GoldenSAML attacks

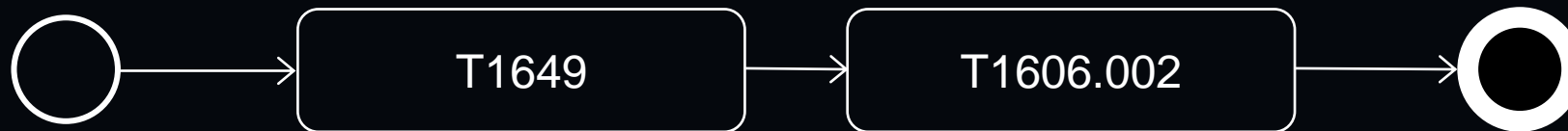
Identity federation concepts

- Service Provider (SP)
 - Azure AD
- Identity Provider (IdP)
 - On-prem AD FS
- Security Token (ST)
 - Security Assertion Markup Language (SAML)
 - Signed by *IdP*, trusted by *SP*



Golden SAML Attack

- Mitre ATT&CK® Techniques:
 - T1649 "Steal or Forge Authentication Certificates"
 - T1606.002 "Forge Web Credentials: SAML Tokens"



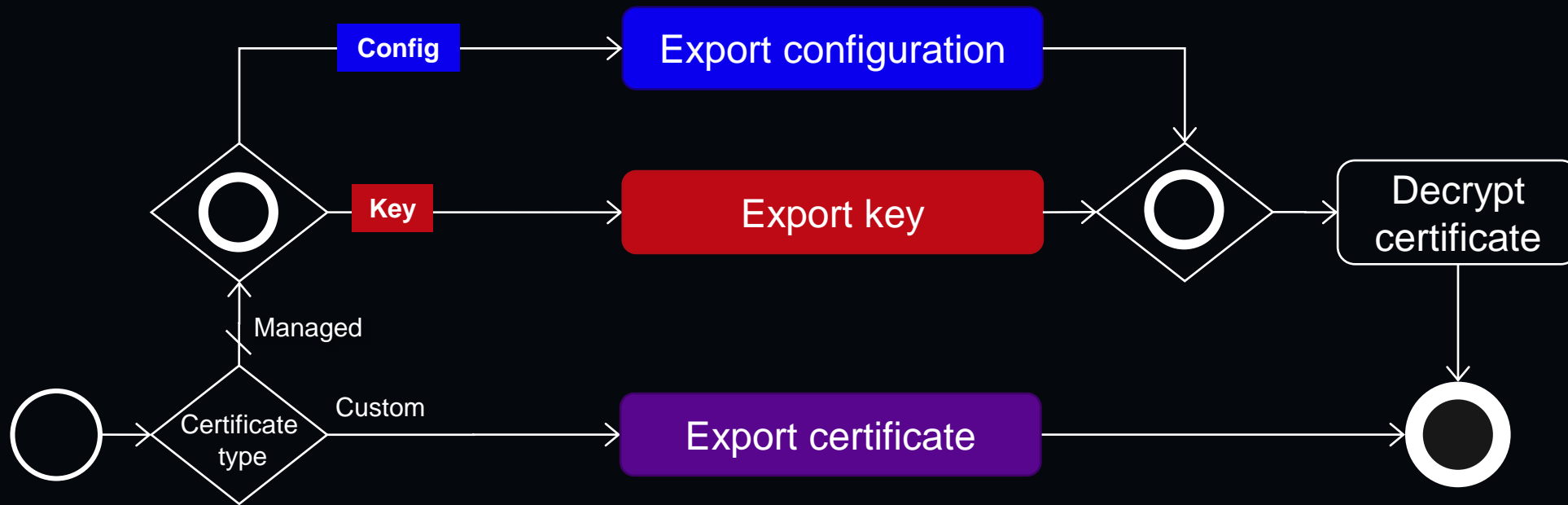
AD FS Attack List



AD FS Certificate Options

- Managed – *default*
 - Stored in *configuration database*, encrypted with DKM key (stored in AD)
- Custom
 - Stored in *certificate store* of each AD FS server (or HSM)

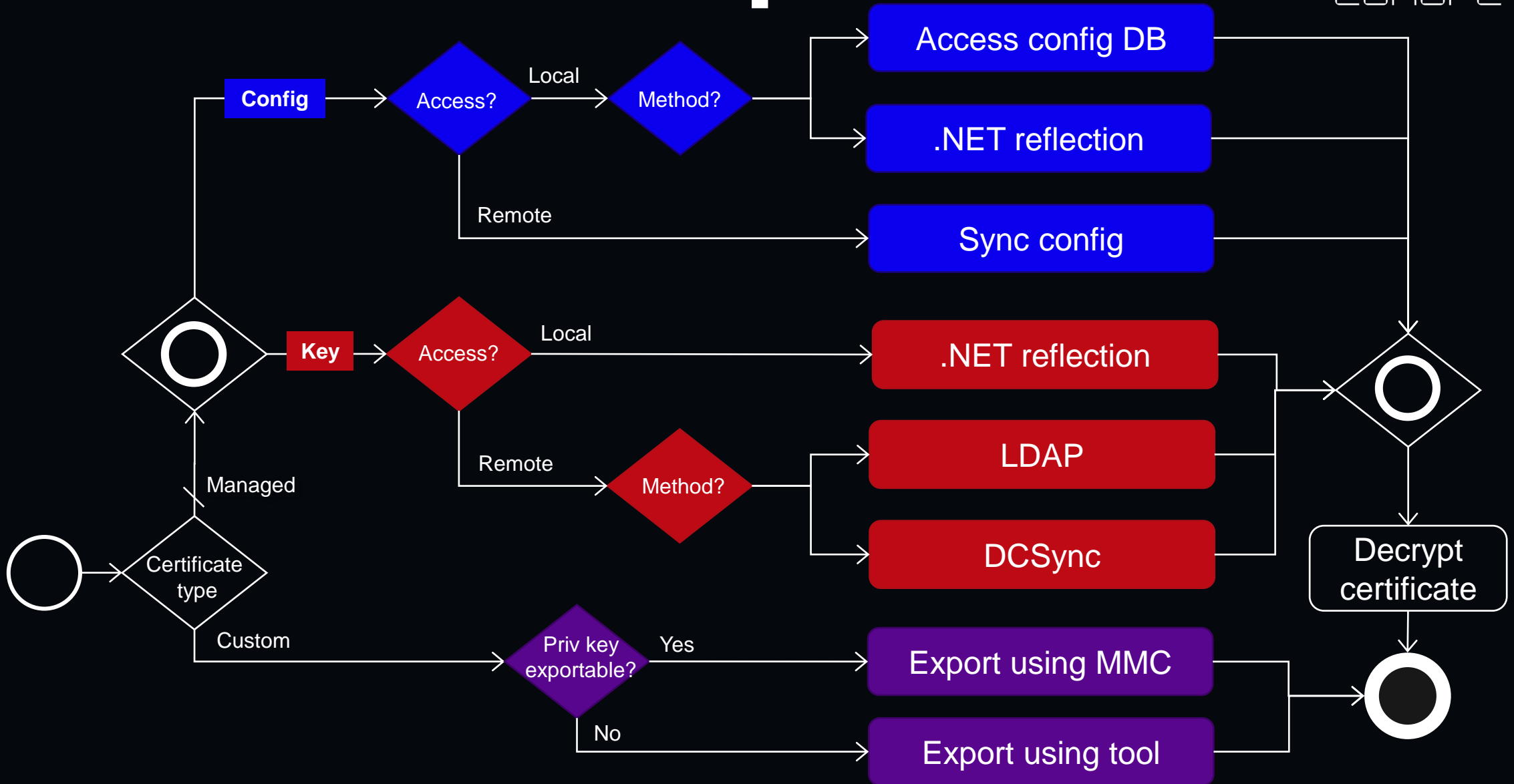
AD FS Attack Graph



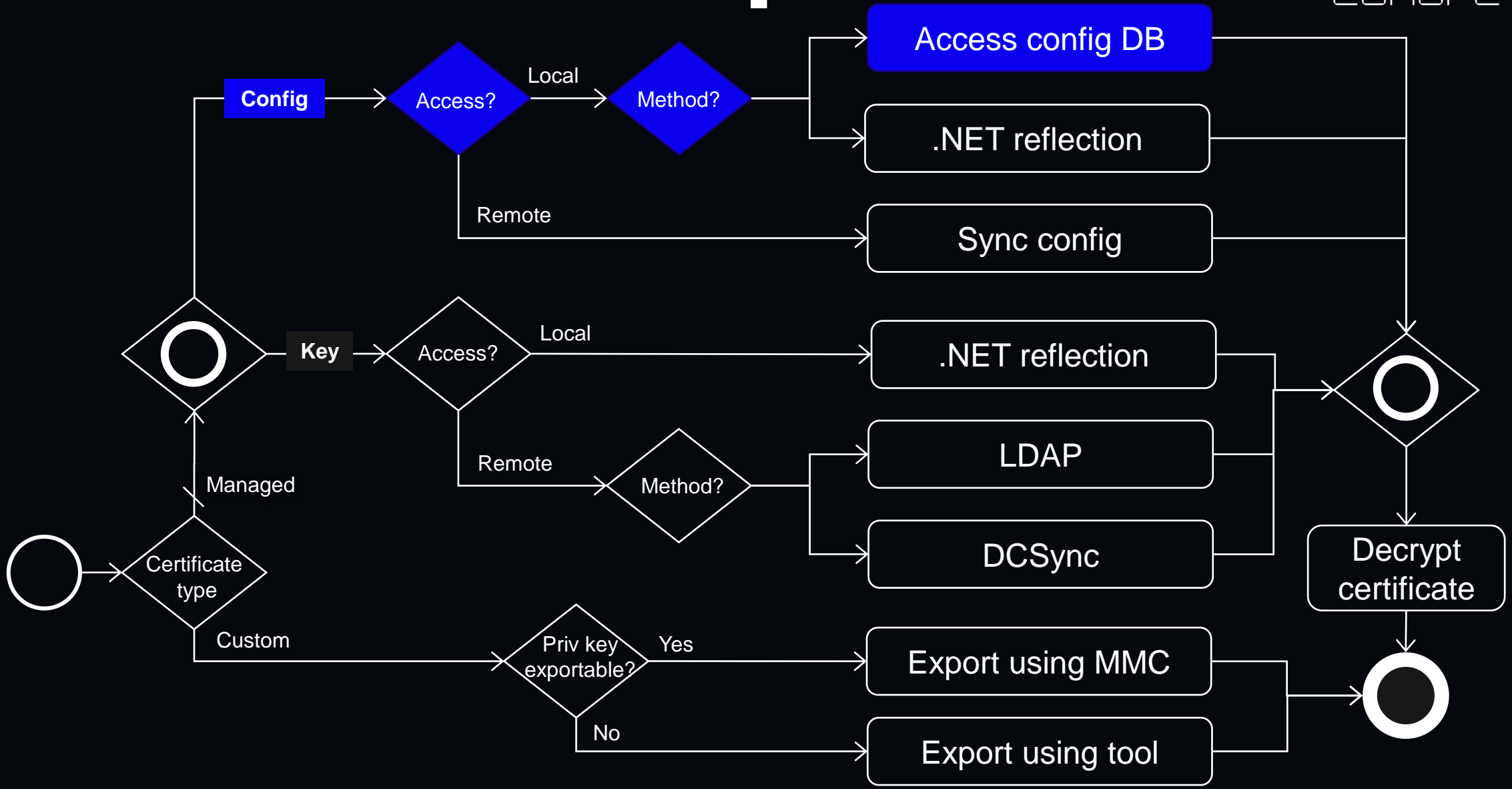
AD FS Configuration Storage Options

- Windows Internal Database (WID) – *default*
- Microsoft SQL server

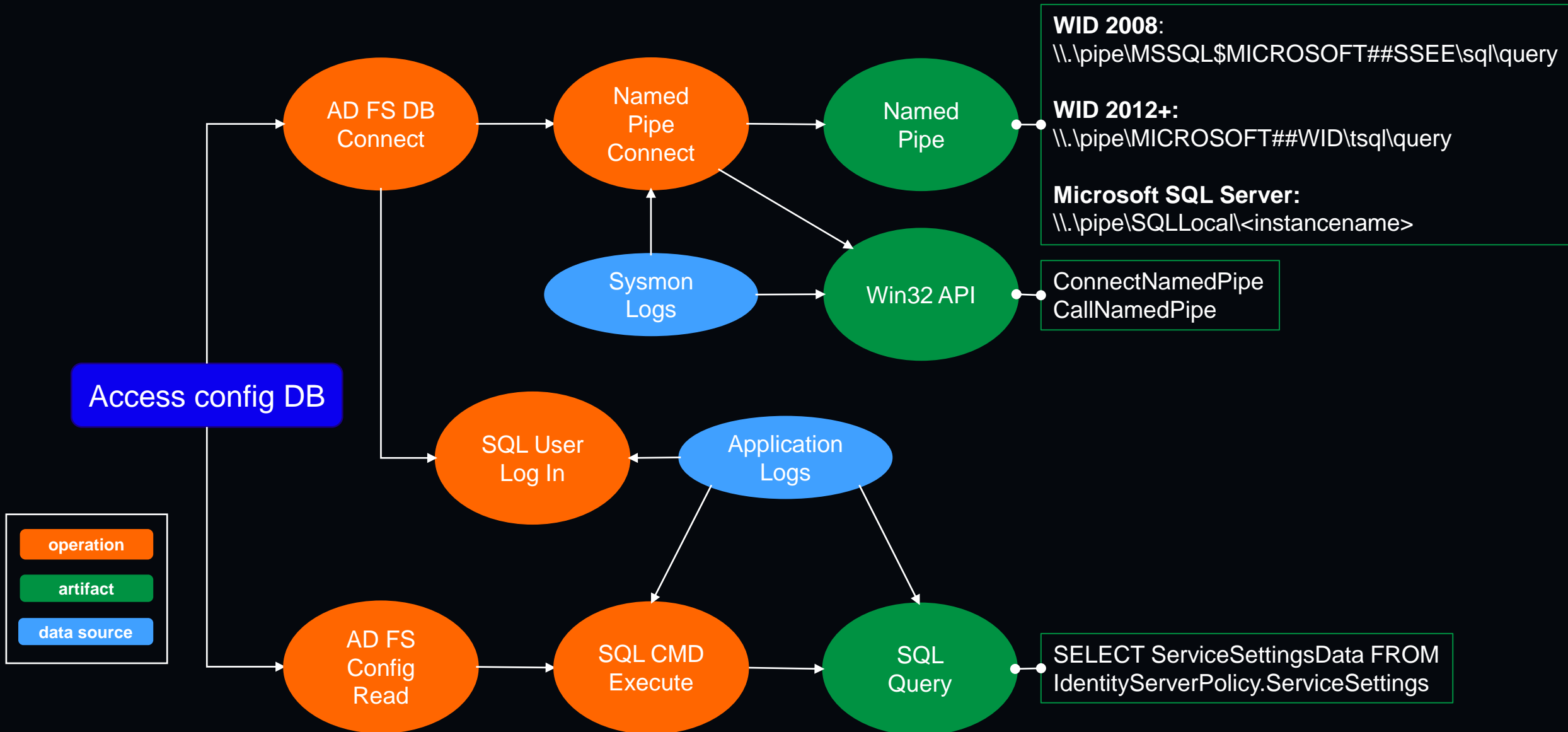
AD FS Attack Graph



AD FS Attack Graph

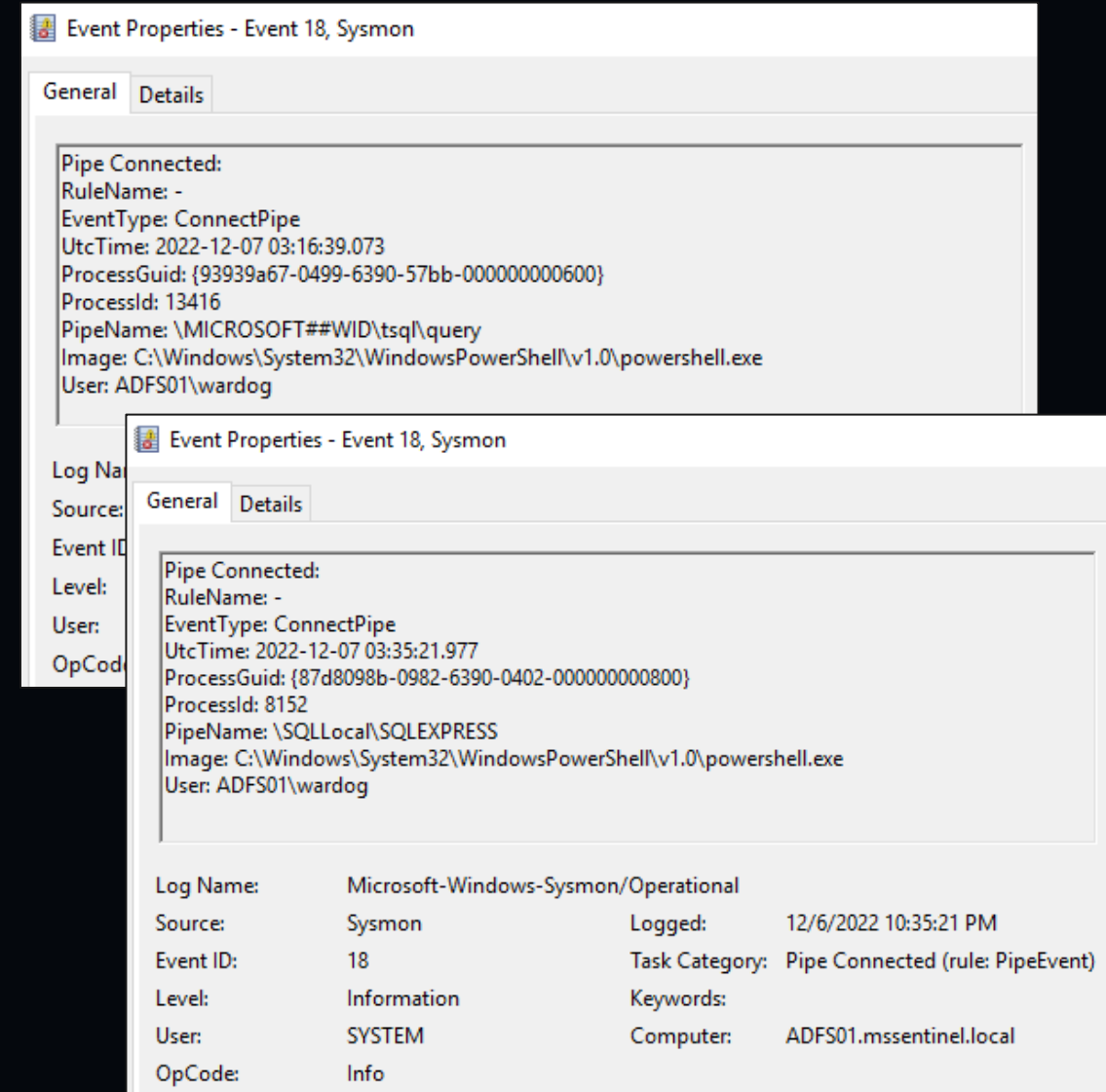


AD FS Defence Graph



AD FS Pipe Connection

- **Log Name:** Microsoft-Windows-Sysmon/Operational
- **Event:** 18 (Pipe Connected)
- **Entities:** User, Host, Pipe, Process
- **Notes:**
 - \Microsoft##WID\tsql\query
 - \SQLLocal\<InstanceName>
 - C:\Windows\ADFS\Microsoft.IdentityServer.ServiceHost.exe



Event Properties - Event 18, Sysmon

General Details

Pipe Connected:
RuleName: -
EventType: ConnectPipe
UtcTime: 2022-12-07 03:16:39.073
ProcessGuid: {93939a67-0499-6390-57bb-000000000600}
ProcessId: 13416
PipeName: \MICROSOFT##WID\tsql\query
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: ADFS01\wardog

Event Properties - Event 18, Sysmon

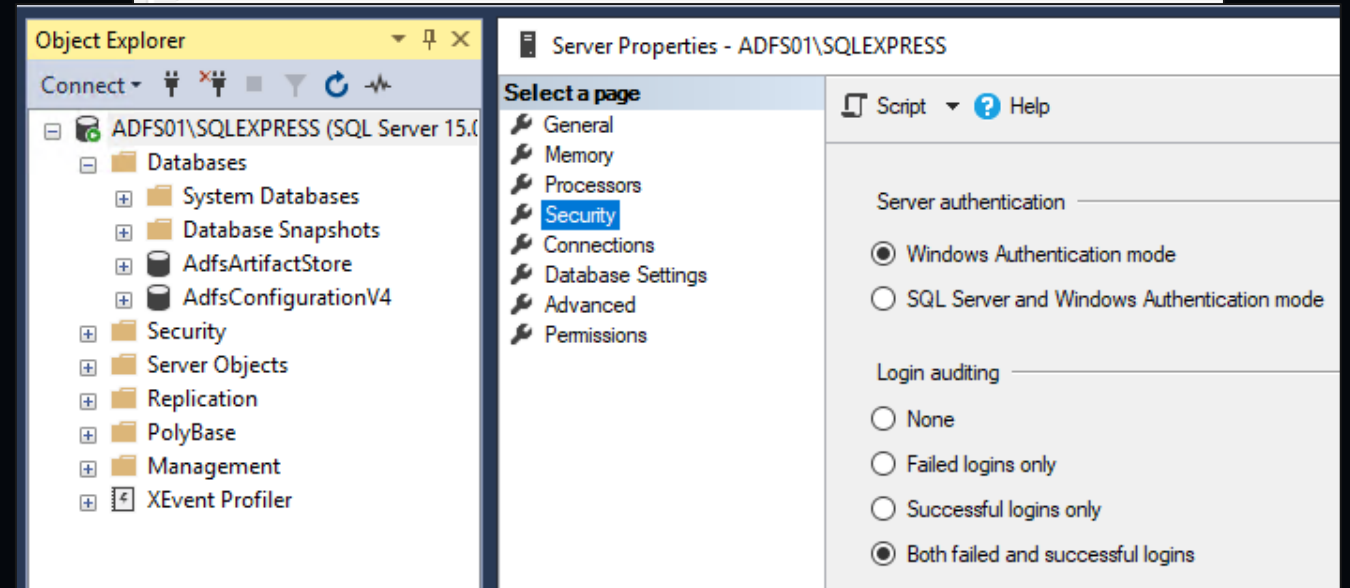
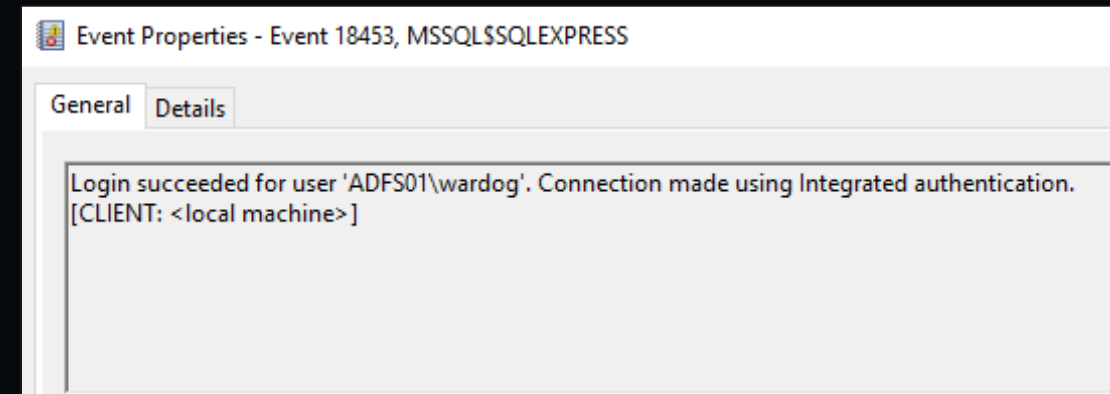
General Details

Pipe Connected:
RuleName: -
EventType: ConnectPipe
UtcTime: 2022-12-07 03:35:21.977
ProcessGuid: {87d8098b-0982-6390-0402-000000000800}
ProcessId: 8152
PipeName: \SQLLocal\SQLEXPRESS
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: ADFS01\wardog

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	12/6/2022 10:35:21 PM
Event ID:	18	Task Category:	Pipe Connected (rule: PipeEvent)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	ADFS01.mssentinel.local
OpCode:	Info		

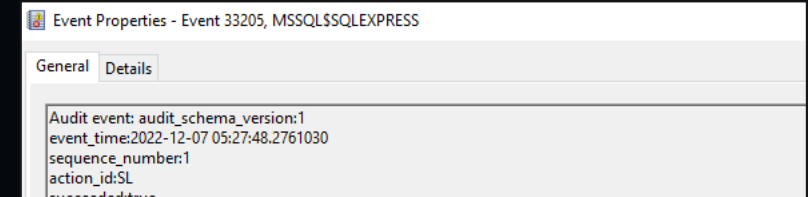
AD FS SQL DB Login Auditing

- **Log Name:** Application
- **Event:** 18453
- **Entities:** User, Host
- **Notes:**
 - Integrated authentication
 - Client information
 - AD FS service account



AD FS SQL DB Query Auditing

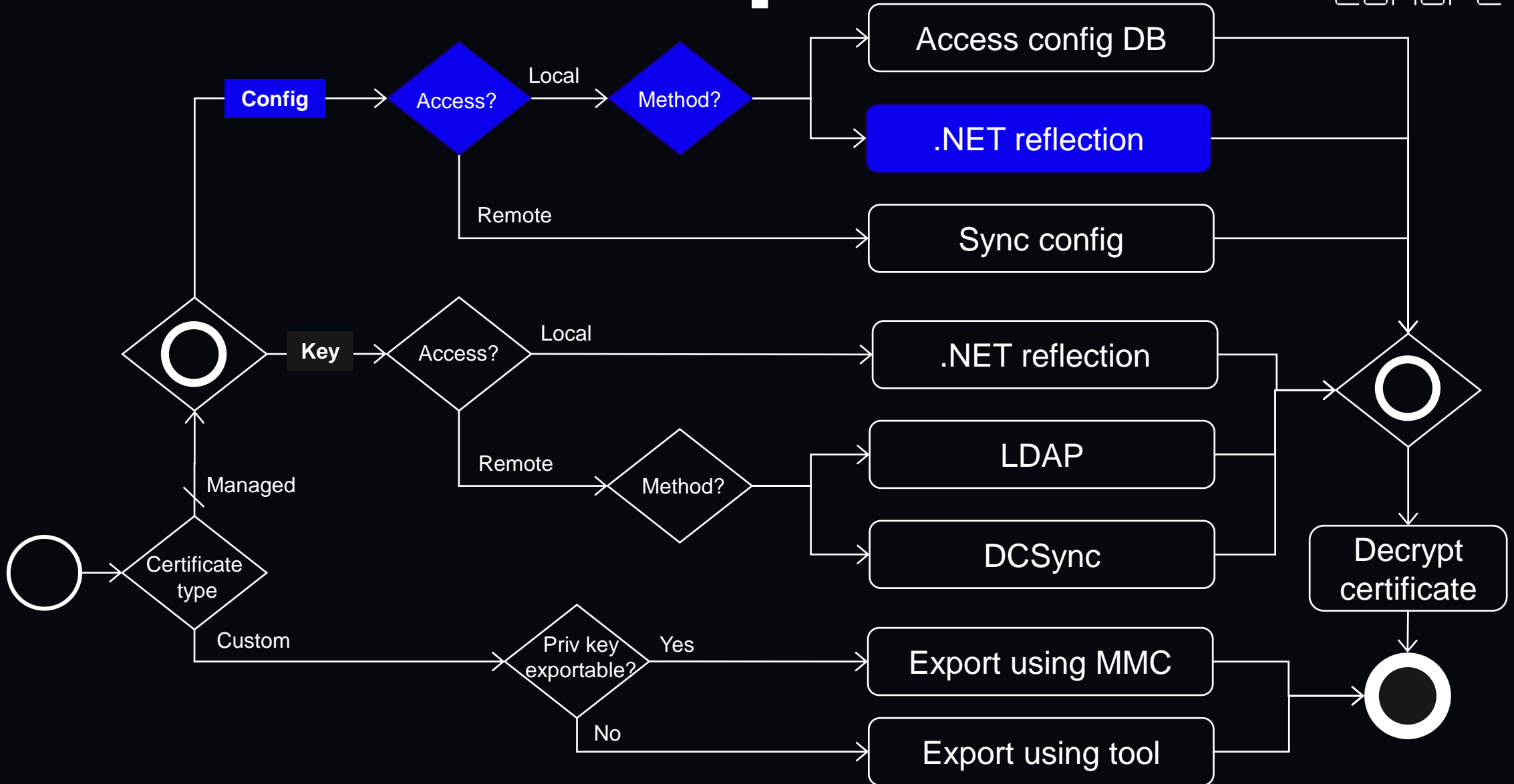
- **Log Name:** Application
- **Event:** 33205
- **Entities:** User, Host, SQL Query
- **Notes:**
 - Create a server audit and database audit specification
 - Correlate user on other events
 - Stack count SQL statements



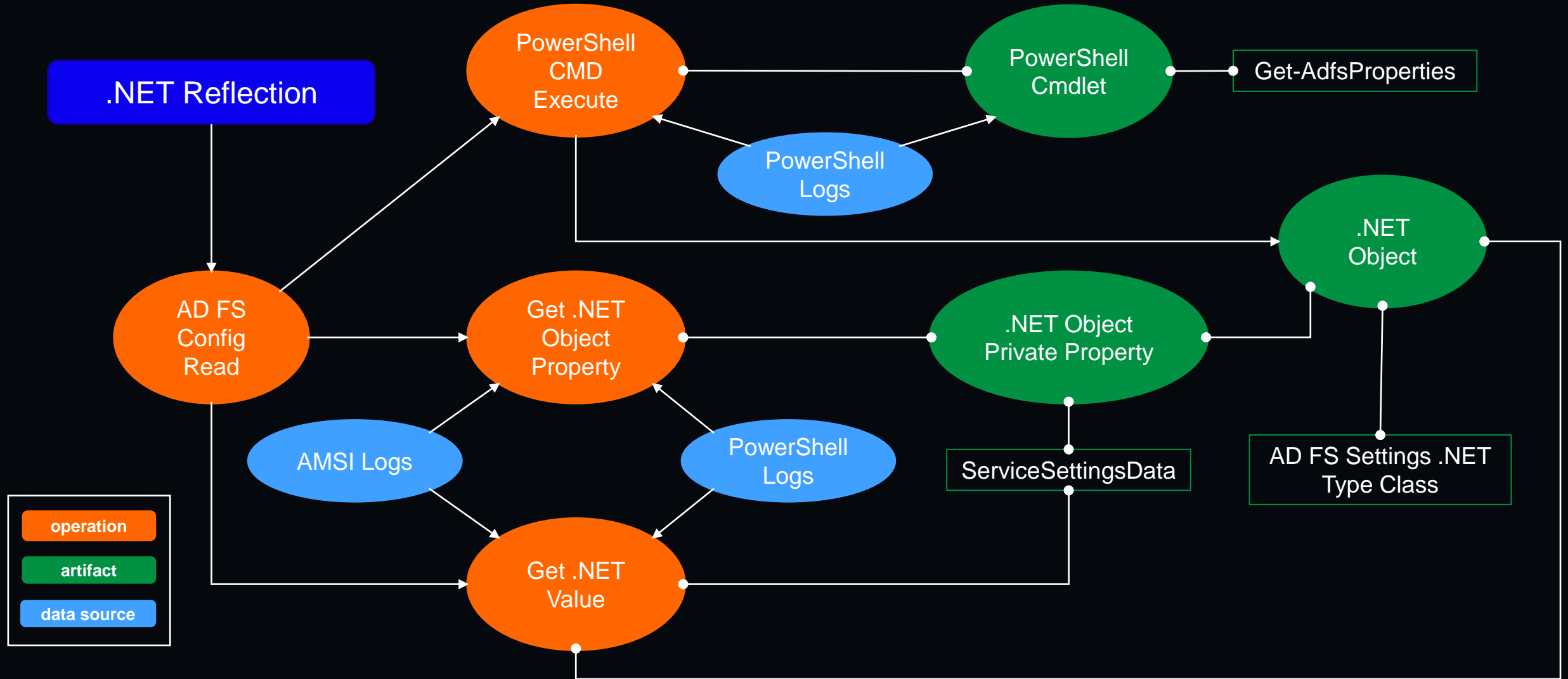
```
session_server_principal_name:ADFS01\wardog  
server_principal_name:ADFS01\wardog  
server_principal_sid:010500000000000515000000875897ac4a8c59e1191c7e26f4010000  
database_principal_name:dbo  
target_server_principal_name:  
target_server_principal_sid:  
target_database_principal_name:  
server_instance_name:ADFS01\SQLEXPRESS  
database_name:AdfsConfigurationV4  
schema_name:IdentityServerPolicy  
object_name:ServiceSettings  
statement:SELECT ServiceSettingsData from IdentityServerPolicy.ServiceSettings  
additional_information:  
user_defined_information:  
application_name:.Net SqlClient Data Provider  
connection_id:E3EAF0C0-EDBC-4729-8EF9-9EF98FDC1403  
data_sensitivity_information:  
host_name:ADFS01
```

Log Name:	Application	Logged:	12/7/2022 12:27:48 AM
Source:	MSSQL\$SQLEXPRESS	Task Category:	None
Event ID:	33205	Keywords:	Classic,Audit Success
Level:	Information	User:	N/A
User:	N/A	Computer:	ADFS01.mssentinel.local
OpCode:			

AD FS Attack Graph

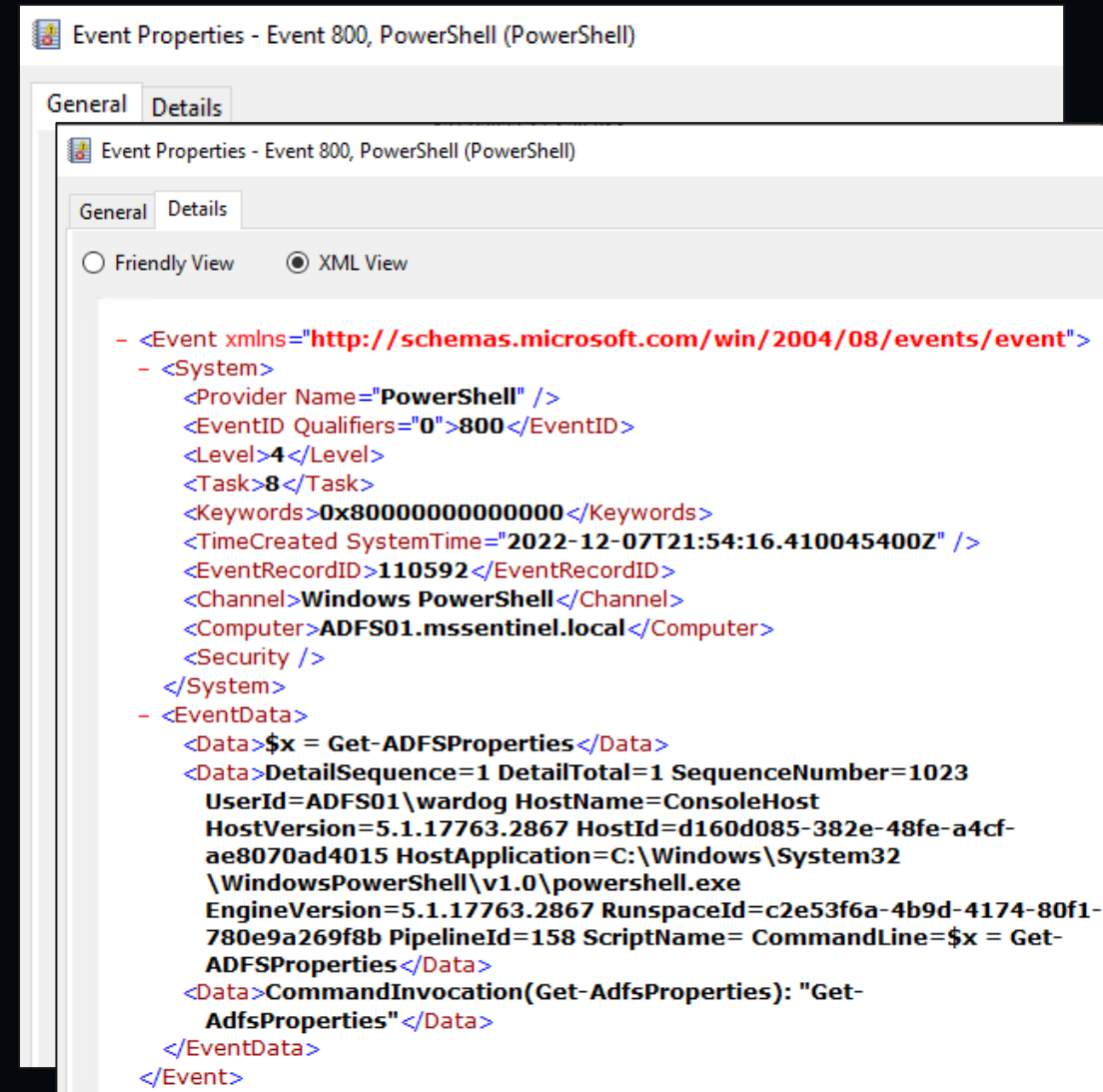


AD FS Defence Graph



AD FS PowerShell Cmdlet

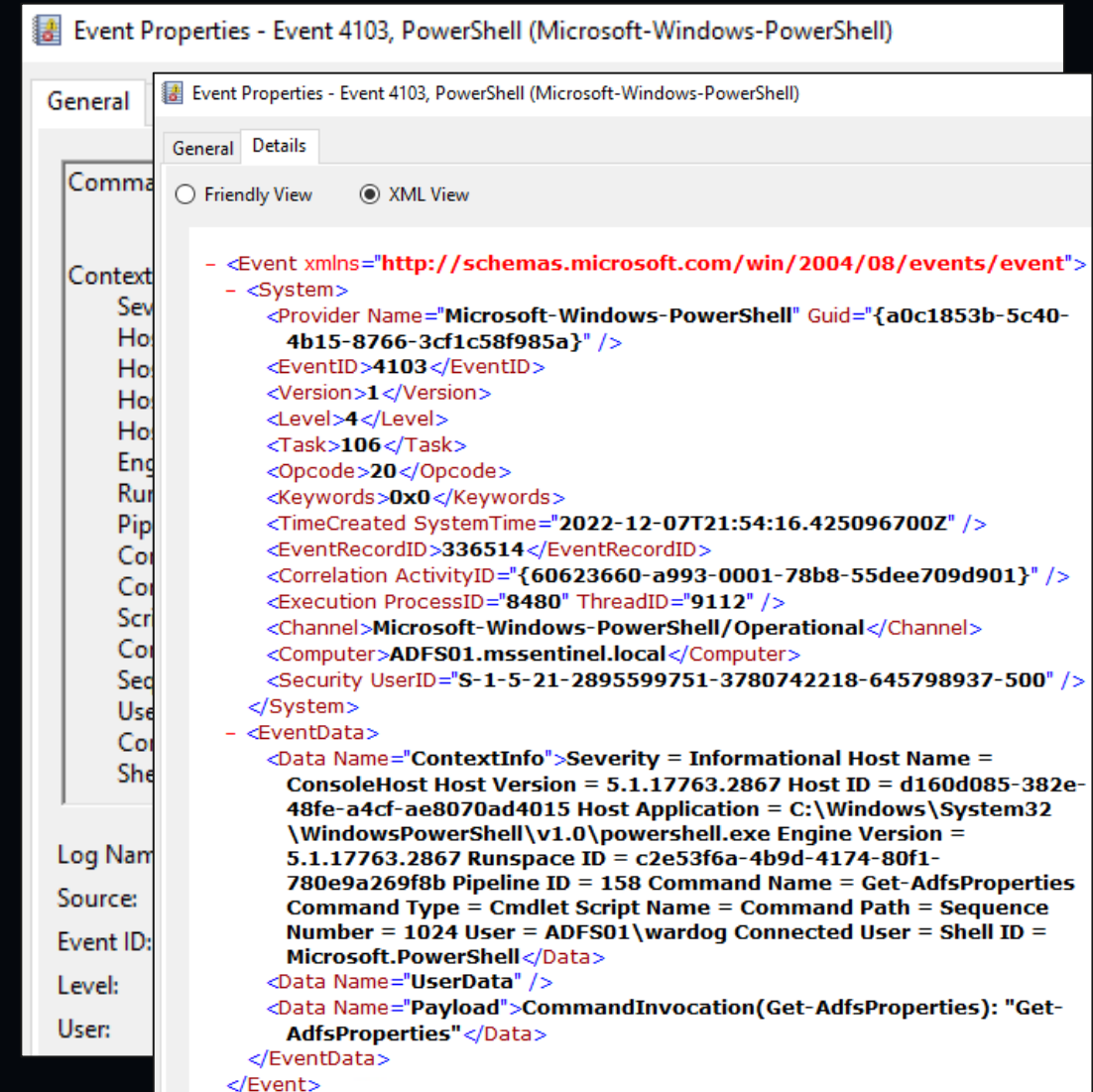
- **Log Name:** Windows PowerShell
- **Event:** 800 (Pipeline Execution)
- **Entities:** Host, Command
- **Notes:**
 - PowerShell v3+
 - Command line context
 - No user context
 - No process context (PID)



```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="PowerShell" />
  <EventID Qualifiers="0">800</EventID>
  <Level>4</Level>
  <Task>8</Task>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2022-12-07T21:54:16.410045400Z" />
  <EventRecordID>110592</EventRecordID>
  <Channel>Windows PowerShell</Channel>
  <Computer>ADFS01.mssentinel.local</Computer>
  <Security />
</System>
- <EventData>
  <Data>$x = Get-ADFSProperties</Data>
  <Data>DetailSequence=1 DetailTotal=1 SequenceNumber=1023
  UserId=ADFS01\wardog HostName=ConsoleHost
  HostVersion=5.1.17763.2867 HostId=d160d085-382e-48fe-a4cf-
  ae8070ad4015 HostApplication=C:\Windows\System32
  \WindowsPowerShell\v1.0\powershell.exe
  EngineVersion=5.1.17763.2867 RunspaceId=c2e53f6a-4b9d-4174-80f1-
  780e9a269f8b PipelineId=158 ScriptName= CommandLine=$x = Get-
  ADFSProperties</Data>
  <Data>CommandInvocation(Get-AdfsProperties): "Get-
  ADFSProperties"</Data>
</EventData>
</Event>
```

AD FS PowerShell Cmdlet

- **Log Name:** Microsoft-Windows-PowerShell/Operational
- **Event:** 4103 (Pipeline Execution)
- **Entities:** Host, Process, Command, User
- **Notes:**
 - PowerShell v5+
 - User and Process (PID) context
 - User and Process context can be correlated with other events



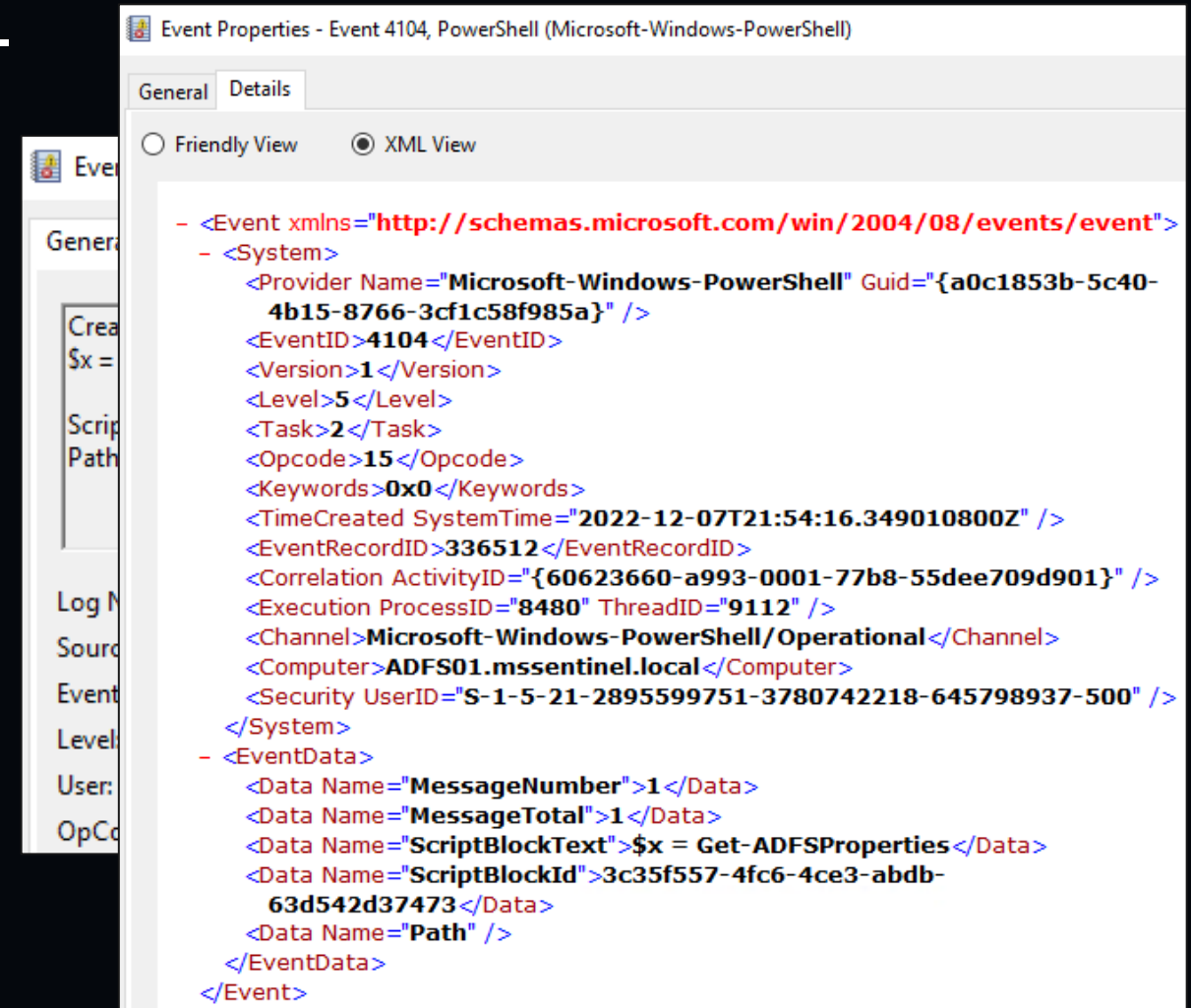
```
Event Properties - Event 4103, PowerShell (Microsoft-Windows-PowerShell)

General Details
Friendly View XML View

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-PowerShell" Guid="{a0c1853b-5c40-4b15-8766-3cf1c58f985a}" />
  <EventID>4103</EventID>
  <Version>1</Version>
  <Level>4</Level>
  <Task>106</Task>
  <Opcode>20</Opcode>
  <Keywords>0x0</Keywords>
  <TimeCreated SystemTime="2022-12-07T21:54:16.425096700Z" />
  <EventRecordID>336514</EventRecordID>
  <Correlation ActivityID="{60623660-a993-0001-78b8-55dee709d901}" />
  <Execution ProcessID="8480" ThreadID="9112" />
  <Channel>Microsoft-Windows-PowerShell/Operational</Channel>
  <Computer>ADFS01.mssentinel.local</Computer>
  <Security UserID="S-1-5-21-2895599751-3780742218-645798937-500" />
</System>
- <EventData>
  <Data Name="ContextInfo">Severity = Informational Host Name =
  ConsoleHost Host Version = 5.1.17763.2867 Host ID = d160d085-382e-48fe-a4cf-ae8070ad4015 Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Engine Version = 5.1.17763.2867 Runspace ID = c2e53f6a-4b9d-4174-80f1-780e9a269f8b Pipeline ID = 158 Command Name = Get-AdfsProperties Command Type = Cmdlet Script Name = Command Path = Sequence Number = 1024 User = ADFS01\wardog Connected User = Shell ID = Microsoft.PowerShell</Data>
  <Data Name="UserData" />
  <Data Name="Payload">CommandInvocation(Get-AdfsProperties): "Get-AdfsProperties"</Data>
</EventData>
</Event>
```

AD FS PowerShell Cmdlet

- **Log Name:** Microsoft-Windows-PowerShell/Operational
- **Event:** 4104 (Scriptblock)
- **Entities:** Host, Command, Process
- **Notes:**
 - PowerShell v5+
 - Interactive session vs full script
 - Global PowerShell Scriptblock logging



```
Event Properties - Event 4104, PowerShell (Microsoft-Windows-PowerShell)
General Details
Friendly View XML View
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-PowerShell" Guid="{a0c1853b-5c40-4b15-8766-3cf1c58f985a}" />
  <EventID>4104</EventID>
  <Version>1</Version>
  <Level>5</Level>
  <Task>2</Task>
  <Opcode>15</Opcode>
  <Keywords>0x0</Keywords>
  <TimeCreated SystemTime="2022-12-07T21:54:16.349010800Z" />
  <EventRecordID>336512</EventRecordID>
  <Correlation ActivityID="{60623660-a993-0001-77b8-55dee709d901}" />
  <Execution ProcessID="8480" ThreadID="9112" />
  <Channel>Microsoft-Windows-PowerShell/Operational</Channel>
  <Computer>ADFS01.mssentinel.local</Computer>
  <Security UserID="S-1-5-21-2895599751-3780742218-645798937-500" />
</System>
- <EventData>
  <Data Name="MessageNumber">1</Data>
  <Data Name="MessageTotal">1</Data>
  <Data Name="ScriptBlockText">$x = Get-ADFSProperties</Data>
  <Data Name="ScriptBlockId">3c35f557-4fc6-4ce3-abdb-63d542d37473</Data>
  <Data Name="Path" />
</EventData>
</Event>
```

Antimalware Scan Interface



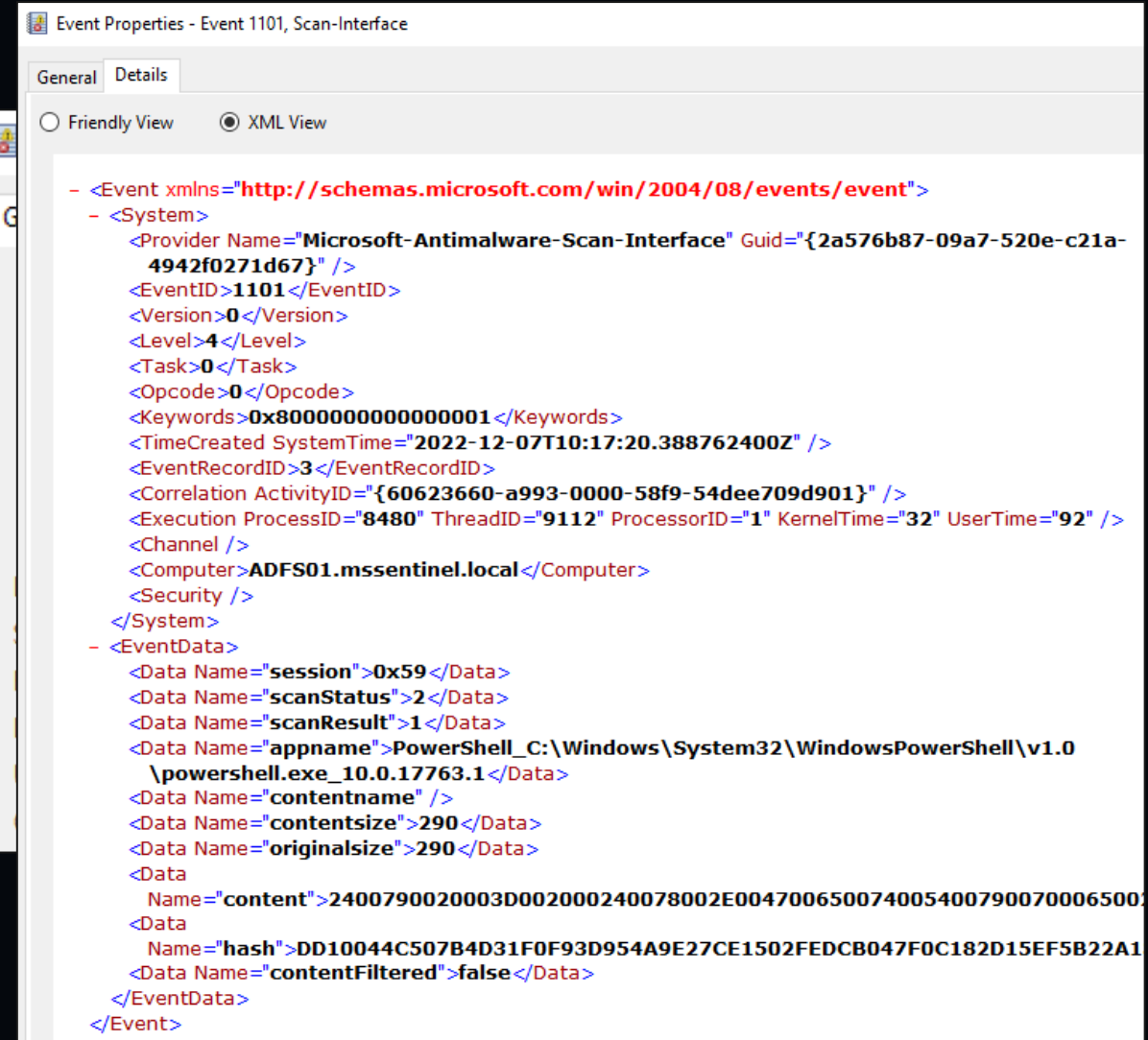
AMSI is an application programming interface (API) developed by Microsoft that enables developers to opt in to sending content to vendor endpoint security agents, regardless of the content's origination, on disk or in memory.

Apps Designed to Send Content to AMSI

- **PowerShell**: instrumented in System.Management.Automation.dll
- **VBScript**: instrumented in vbscript.dll
- **JScript**: instrumented in jscript.dll, jscript9.dll, and jscriptlegacy.dll
- **VBA macros in Office documents**: instrumented in VBE7.dll
- **Excel 4.0 macros**: instrumented in excel.exe and excelcnv.exe
- **Exchange Server 2016**: instrumented in Microsoft.Exchange.HttpRequestFiltering.dll
- **WMI**: instrumented in fastprox.dll
- **.NET in-memory assembly loads**: instrumented in .NET 4.8+ in clr.dll and coreclr.dll
- **Volume shadow copy operations**: instrumented in VSSVC.exe and swprv.dll
- **User Account Control (UAC) elevations**: instrumented in consent.exe

Capturing AMSI Events

- **Provider:** Microsoft-Antimalware-Scan-Interface
- **Steps to capture events:**
 - logman start AMSITrace -p Microsoft-Antimalware-Scan-Interface Event1 -o AMSITrace.etl -ets
 - logman stop AMSITrace -ets



```
Event Properties - Event 1101, Scan-Interface
General Details
Friendly View XML View
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Antimalware-Scan-Interface" Guid="{2a576b87-09a7-520e-c21a-4942f0271d67}" />
  <EventID>1101</EventID>
  <Version>0</Version>
  <Level>4</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000001</Keywords>
  <TimeCreated SystemTime="2022-12-07T10:17:20.388762400Z" />
  <EventRecordID>3</EventRecordID>
  <Correlation ActivityID="{60623660-a993-0000-58f9-54dee709d901}" />
  <Execution ProcessID="8480" ThreadID="9112" ProcessorID="1" KernelTime="32" UserTime="92" />
  <Channel />
  <Computer>ADFS01.mssentinel.local</Computer>
  <Security />
</System>
- <EventData>
  <Data Name="session">0x59</Data>
  <Data Name="scanStatus">2</Data>
  <Data Name="scanResult">1</Data>
  <Data Name="appname">PowerShell_C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe_10.0.17763.1</Data>
  <Data Name="contentname" />
  <Data Name="contentsize">290</Data>
  <Data Name="originalsize">290</Data>
  <Data
    Name="content">2400790020003D002000240078002E004700650074005400790070006500
  </Data>
  <Data
    Name="hash">DD10044C507B4D31F0F93D954A9E27CE1502FEDCB047F0C182D15EF5B22A1
  </Data>
  <Data Name="contentFiltered">>false</Data>
</EventData>
</Event>
```


Interpreting AMSI Content

```
Administrator: Windows PowerShell
PS C:\programdata> Get-AmsiEvent -Path AMSITrace.etl | Where-Object {$_.Content -ne 'prompt'}

ProcessId      : 8480
ThreadId       : 9112
TimeCreated    : 12/7/2022 5:17:20 AM
```

```
Select Administrator: Windows PowerShell
PS C:\programdata> Get-AmsiEvent -Path AMSITrace.etl | Where-Object {$_.Content -ne 'prompt'} | Select Content

Content
-----
$X = Get-ADFSPProperties
$Y = $X.GetType().GetProperty("ServiceSettingsData", [System.Reflection.BindingFlags]::Instance)
$Z = $Y.GetValue($X, $null)

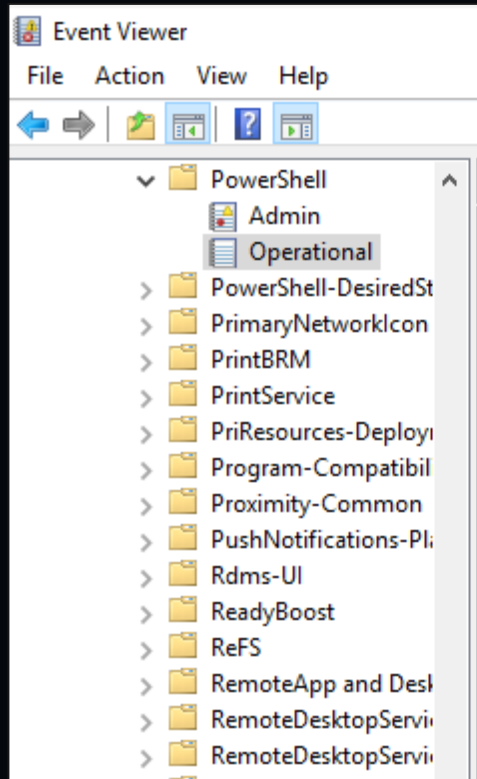
PS C:\programdata>

[System.Reflection.BindingFlags]::NonPublic
Hash      : DD10044C507B4D31F0F93D954A9E27CE1502FEDCB047F0C182D15EF5B22A139A
ContentFiltered : False
```

<https://gist.github.com/mgraeber-rc/1eb42d3ec9c2f677e70bb14c3b7b5c9c>

PowerShell Scriptblock Logging

- **Log Name:** Microsoft-Windows-PowerShell/Operational
- **Event:** 4104



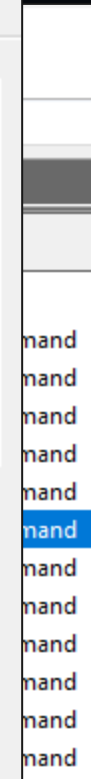
Event Properties - Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):
`Sy = $x.GetType().GetProperty("ServiceSettingsData", [System.Reflection.BindingFlags]::Instance -bor [System.Reflection.BindingFlags]::NonPublic)`

ScriptBlock ID: de799f62-5379-40e1-bd48-b95baaa2de87
Path:

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	12/7/2022 5:49:47 AM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Warning	Keywords:	None
User:	ADFS01\wardog	Computer:	ADFS01.mssentinel.local
OpCode:	On create calls		



PowerShell Strings -> Warning



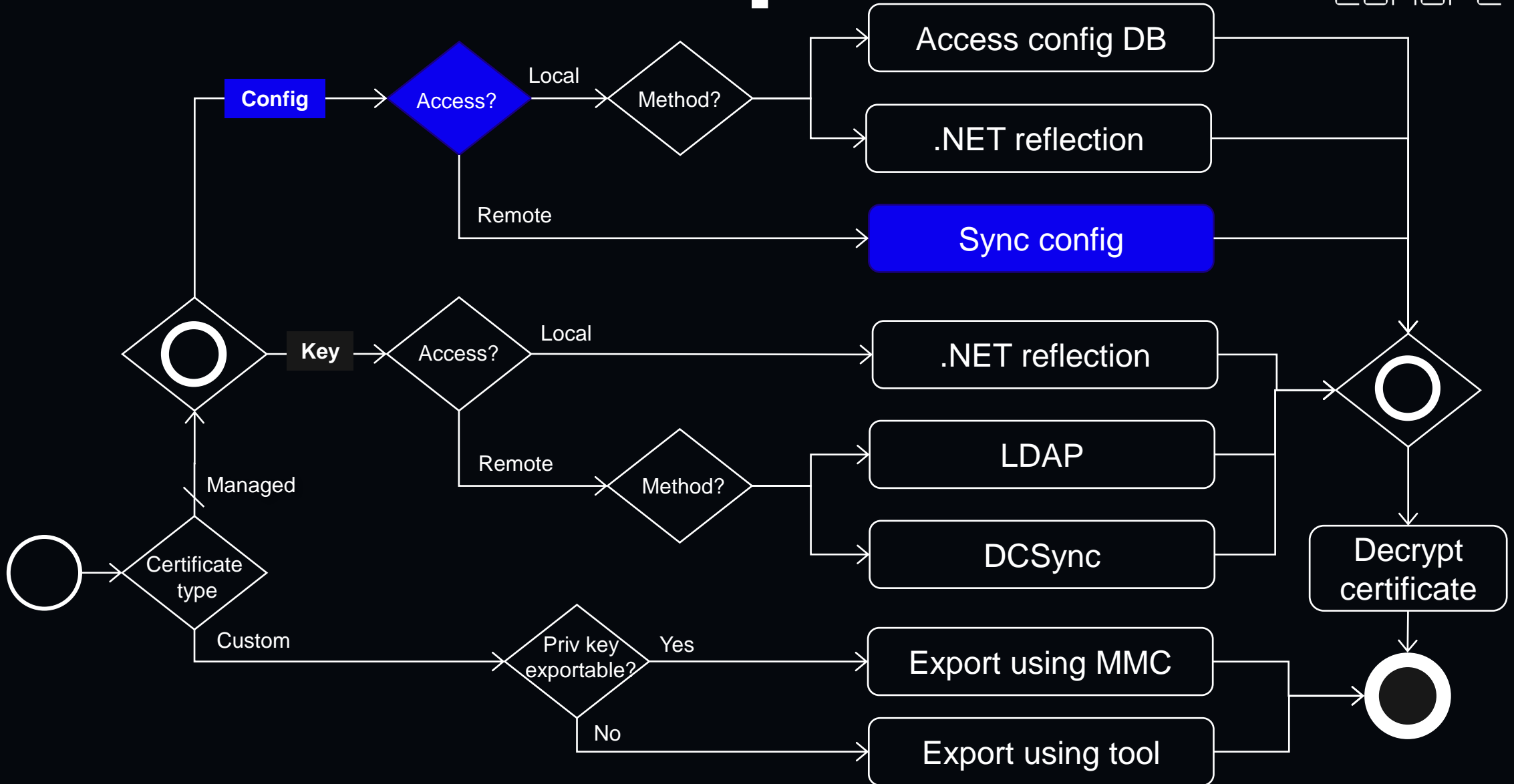
Add-Type, DllImport, DefineDynamicAssembly, DefineDynamicModule, DefineType, DefineConstructor, CreateType, DefineLiteral, DefineEnum, DefineField, ILGenerator, Emit, UnverifiableCodeAttribute, DefinePInvokeMethod, GetTypes, GetAssemblies, Methods, Properties, GetConstructor, GetConstructors, GetDefaultMembers, GetEvent, GetEvents, GetField, GetFields, GetInterface, GetInterfaceMap, GetInterfaces, GetMember, GetMembers, GetMethod, GetMethods,

GetNestedType, GetNestedTypes, GetProperties, **GetProperty**, InvokeMember, MakeArrayType, MakeByRefType, MakeGenericType, MakePointerType, DeclaringMethod, DeclaringType, ReflectedType, TypeHandle, TypeInitializer, UnderlyingSystemType, InteropServices, Marshal, AllocHGlobal, PtrToStructure, StructureToPtr, FreeHGlobal, IntPtr, MemoryStream, DeflateStream, FromBase64String, EncodedCommand, Bypass, ToBase64String, ExpandString, GetPowerShell, OpenProcess, VirtualAlloc, VirtualFree, WriteProcessMemory, CreateUserThread, CloseHandle, GetDelegateForFunctionPointer, kernel32, CreateThread, memcpy, LoadLibrary, GetModuleHandle, GetProcAddress, VirtualProtect, FreeLibrary, ReadProcessMemory, CreateRemoteThread, AdjustTokenPrivileges, WriteByte, WriteInt32, OpenThreadToken, PtrToString, ZeroFreeGlobalAllocUnicode, OpenProcessToken, GetTokenInformation, SetThreadToken, ImpersonateLoggedOnUser, RevertToSelf, GetLogonSessionData, CreateProcessWithToken, DuplicateTokenEx, OpenWindowStation, OpenDesktop, MiniDumpWriteDump, AddSecurityPackage, EnumerateSecurityPackages, GetProcessHandle, DangerousGetHandle, CryptoServiceProvider, Cryptography, RijndaelManaged, SHA1Managed, CryptoStream, CreateEncryptor, CreateDecryptor, TransformFinalBlock, DeviceIoControl, SetInformationProcess, PasswordDeriveBytes, GetAsyncKeyState, GetKeyboardState, GetForegroundWindow, **BindingFlags**,

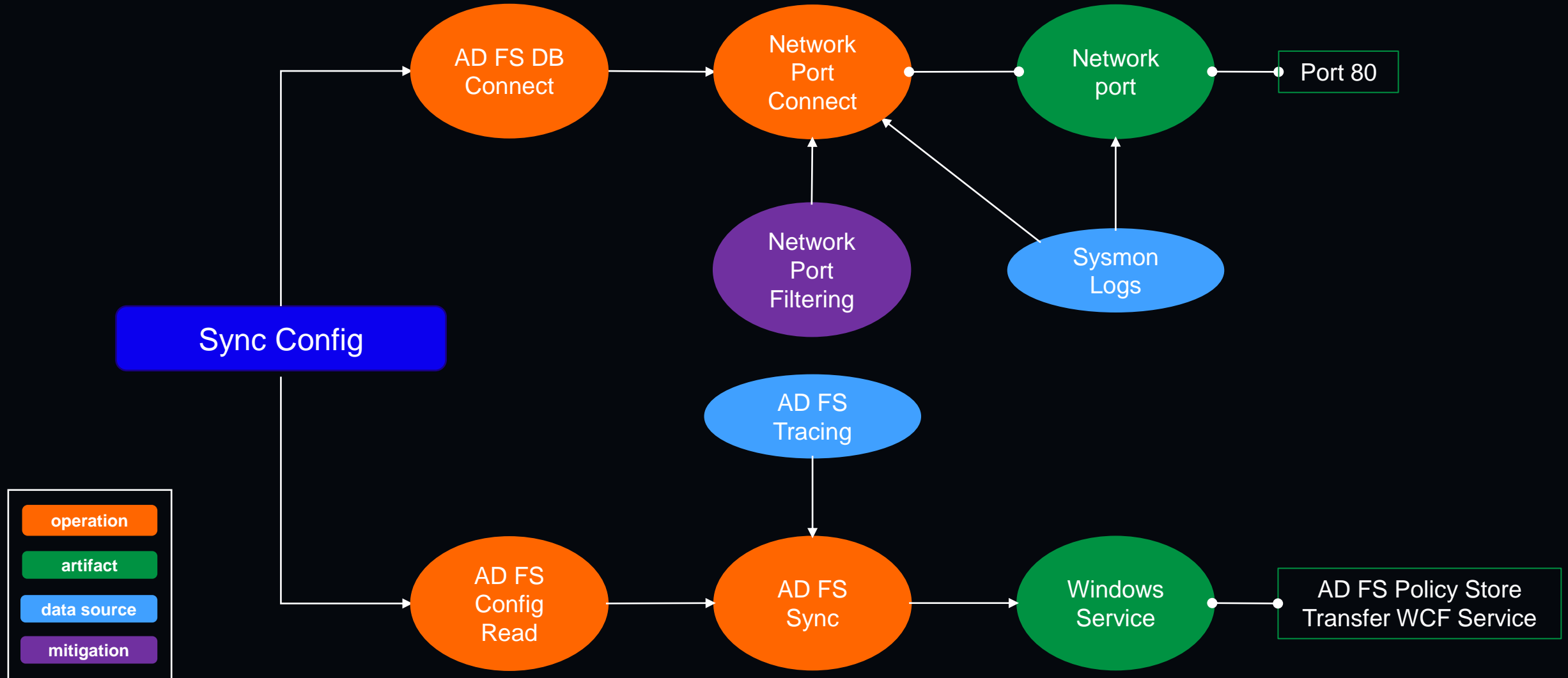
NonPublic, ScriptBlockLogging, LogPipelineExecutionDetails, ProtectedEventLogging

<https://redcanary.com/blog/amsi/>

AD FS Attack Graph

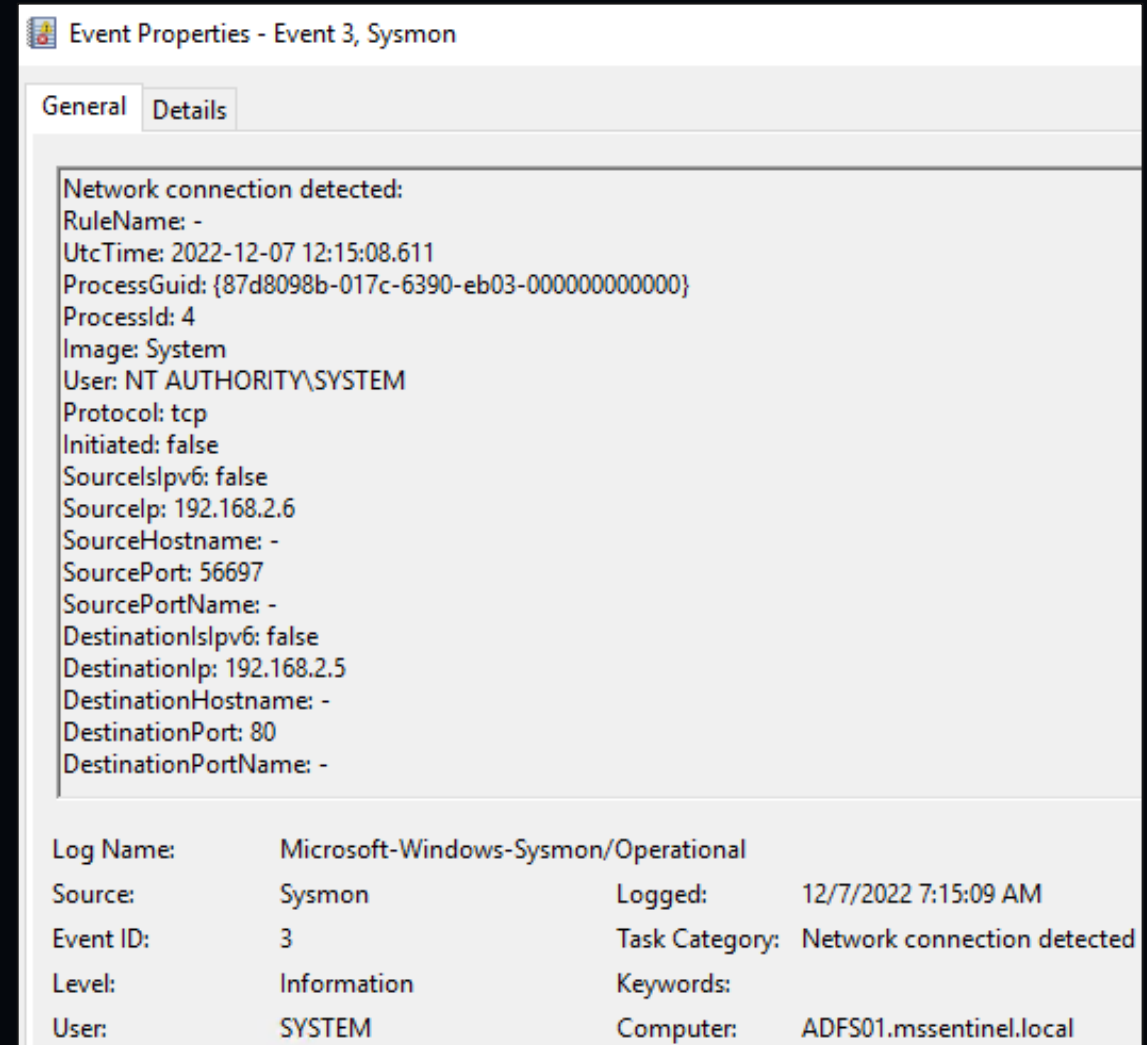


AD FS Defence Graph



AD FS Sync – Network Port

- **Log Name:** Microsoft-Windows-Sysmon/Operational
- **Event:** 3 (Network Connection)
- **Entities:** Host, IP, Port
- **Notes:**
 - Http traffic is only used by load balancers to probe whether the AD FS service is up or not.



Event Properties - Event 3, Sysmon

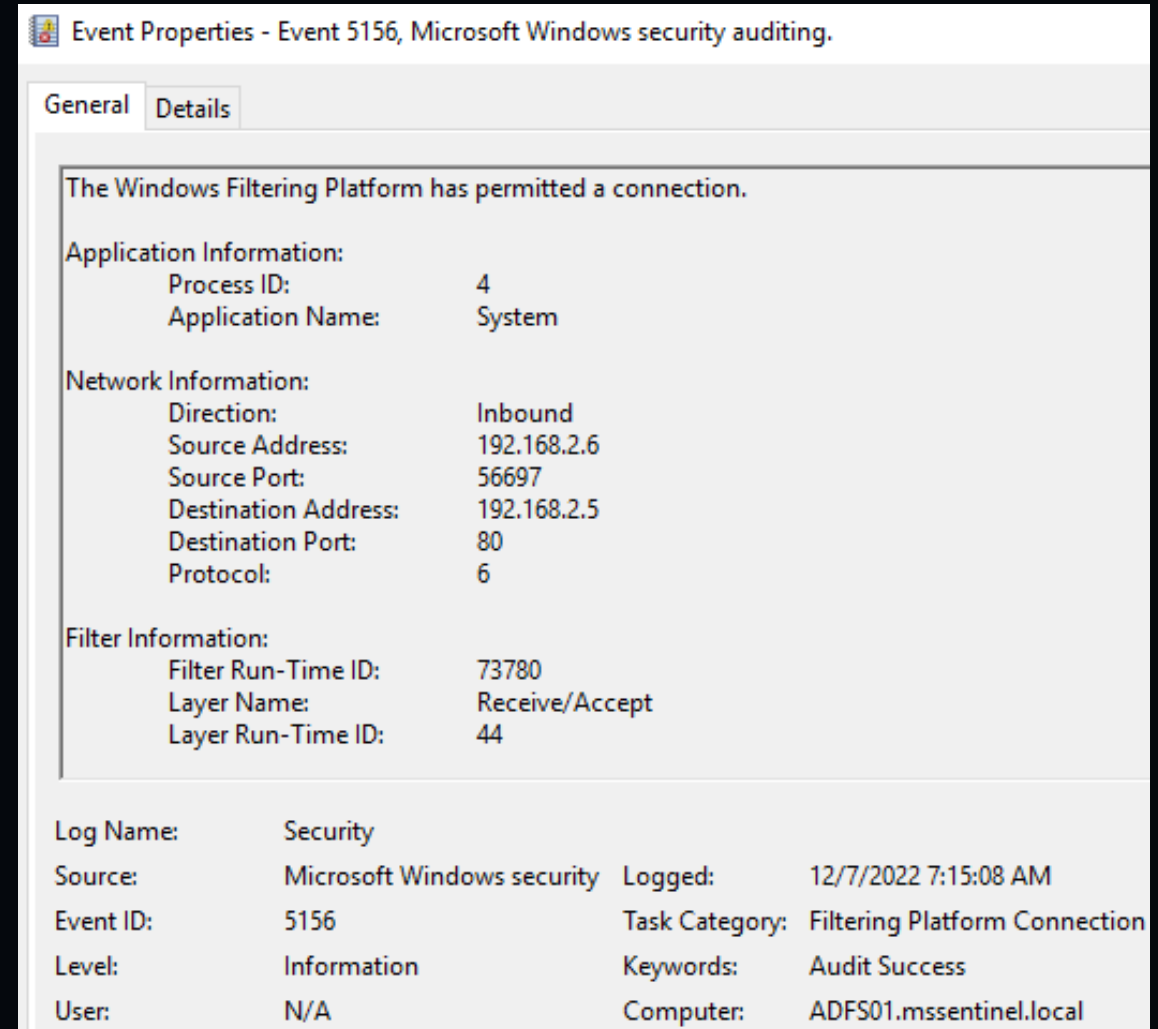
General Details

Network connection detected:
RuleName: -
UtcTime: 2022-12-07 12:15:08.611
ProcessGuid: {87d8098b-017c-6390-eb03-000000000000}
ProcessId: 4
Image: System
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: false
SourceIspv6: false
SourceIp: 192.168.2.6
SourceHostname: -
SourcePort: 56697
SourcePortName: -
DestinationIspv6: false
DestinationIp: 192.168.2.5
DestinationHostname: -
DestinationPort: 80
DestinationPortName: -

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	12/7/2022 7:15:09 AM
Event ID:	3	Task Category:	Network connection detected
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	ADFS01.mssentinel.local

AD FS Sync – Network Port

- **Log Name:** Security
- **Event:** 5156
- **Entities:** Host, IP, Port
- **Notes:**
 - Http traffic is only used by load balancers to probe whether the AD FS service is up or not.
 - Not user context, but not needed.



Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID:	4
Application Name:	System

Network Information:

Direction:	Inbound
Source Address:	192.168.2.6
Source Port:	56697
Destination Address:	192.168.2.5
Destination Port:	80
Protocol:	6

Filter Information:

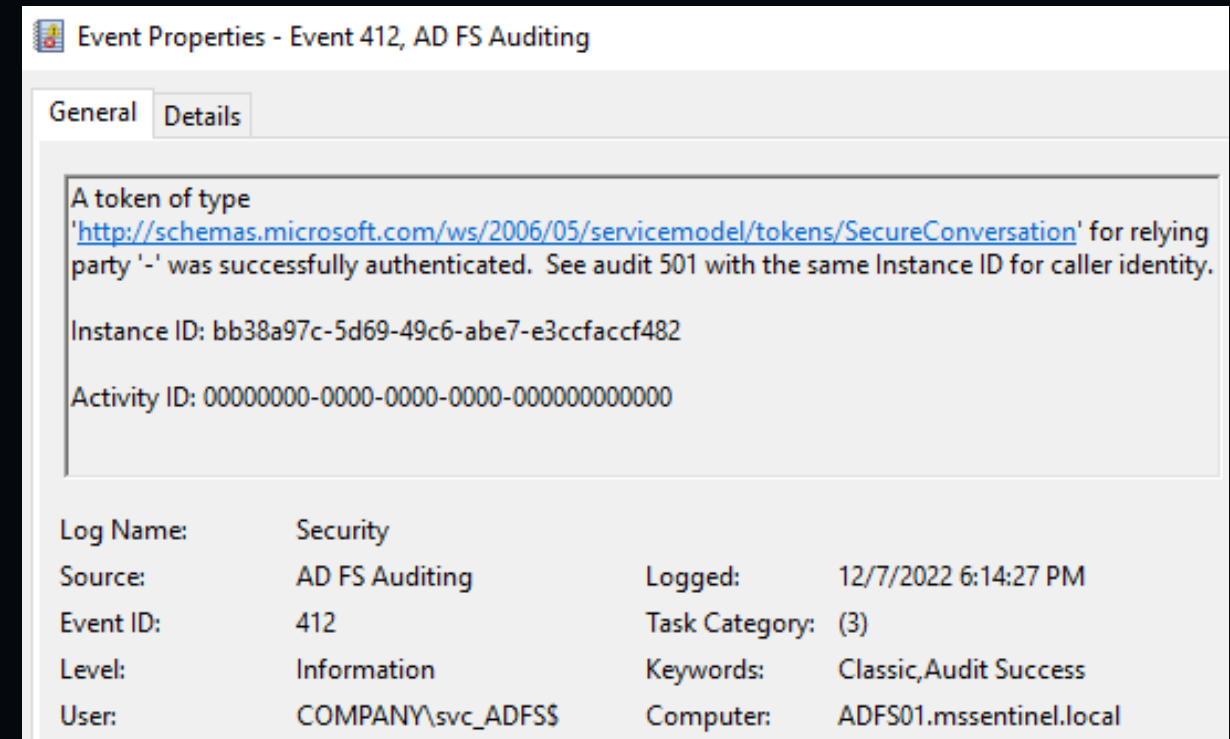
Filter Run-Time ID:	73780
Layer Name:	Receive/Accept
Layer Run-Time ID:	44

Log Name: Security

Source:	Microsoft Windows security	Logged:	12/7/2022 7:15:08 AM
Event ID:	5156	Task Category:	Filtering Platform Connection
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	ADFS01.mssentinel.local

AD FS Sync – Authentication

- **Log Name:** Security
- **Event:** 412
- **Entities:** Host, Service
- **Notes:**
 - Join event 412 and 501 from AD FS auditing on Instance ID
 - Service Model (WCF tracing)



Event Properties - Event 412, AD FS Auditing

General Details

A token of type ['http://schemas.microsoft.com/ws/2006/05/servicemodel/tokens/SecureConversation'](http://schemas.microsoft.com/ws/2006/05/servicemodel/tokens/SecureConversation) for relying party '-' was successfully authenticated. See audit 501 with the same Instance ID for caller identity.

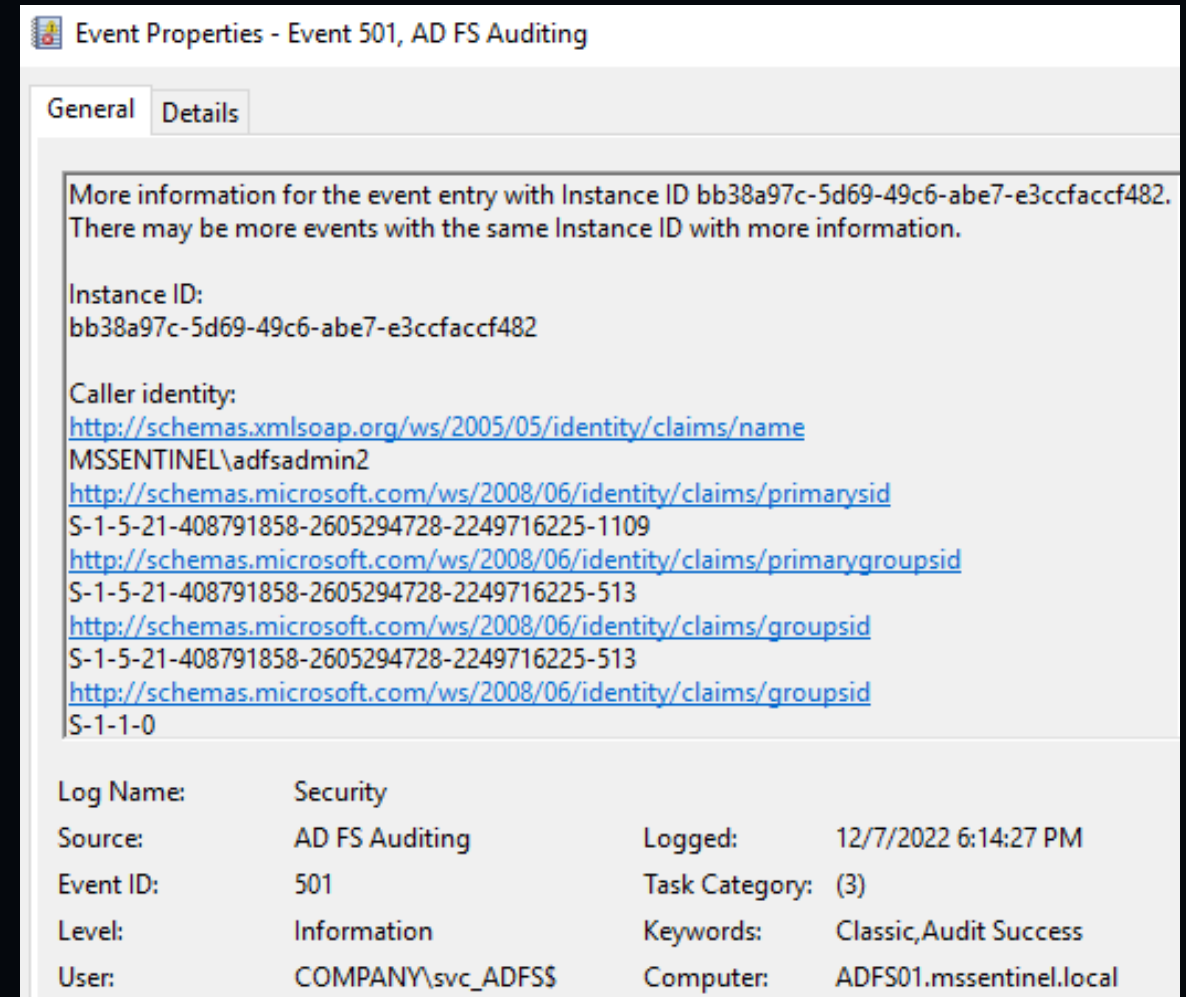
Instance ID: bb38a97c-5d69-49c6-abe7-e3ccfaccf482

Activity ID: 00000000-0000-0000-0000-000000000000

Log Name:	Security	Logged:	12/7/2022 6:14:27 PM
Source:	AD FS Auditing	Task Category:	(3)
Event ID:	412	Keywords:	Classic,Audit Success
Level:	Information	Computer:	ADFS01.mssentinel.local
User:	COMPANY\svc_ADFSS		

AD FS Sync – Authentication

- **Log Name:** Security
- **Event:** 501
- **Entities:** Host, User
- **Notes:**
 - Join event 412 and 501 from AD FS auditing on Instance ID
 - Caller Identity -> AD FS Service account



Event Properties - Event 501, AD FS Auditing

General Details

More information for the event entry with Instance ID bb38a97c-5d69-49c6-abe7-e3ccfaccf482. There may be more events with the same Instance ID with more information.

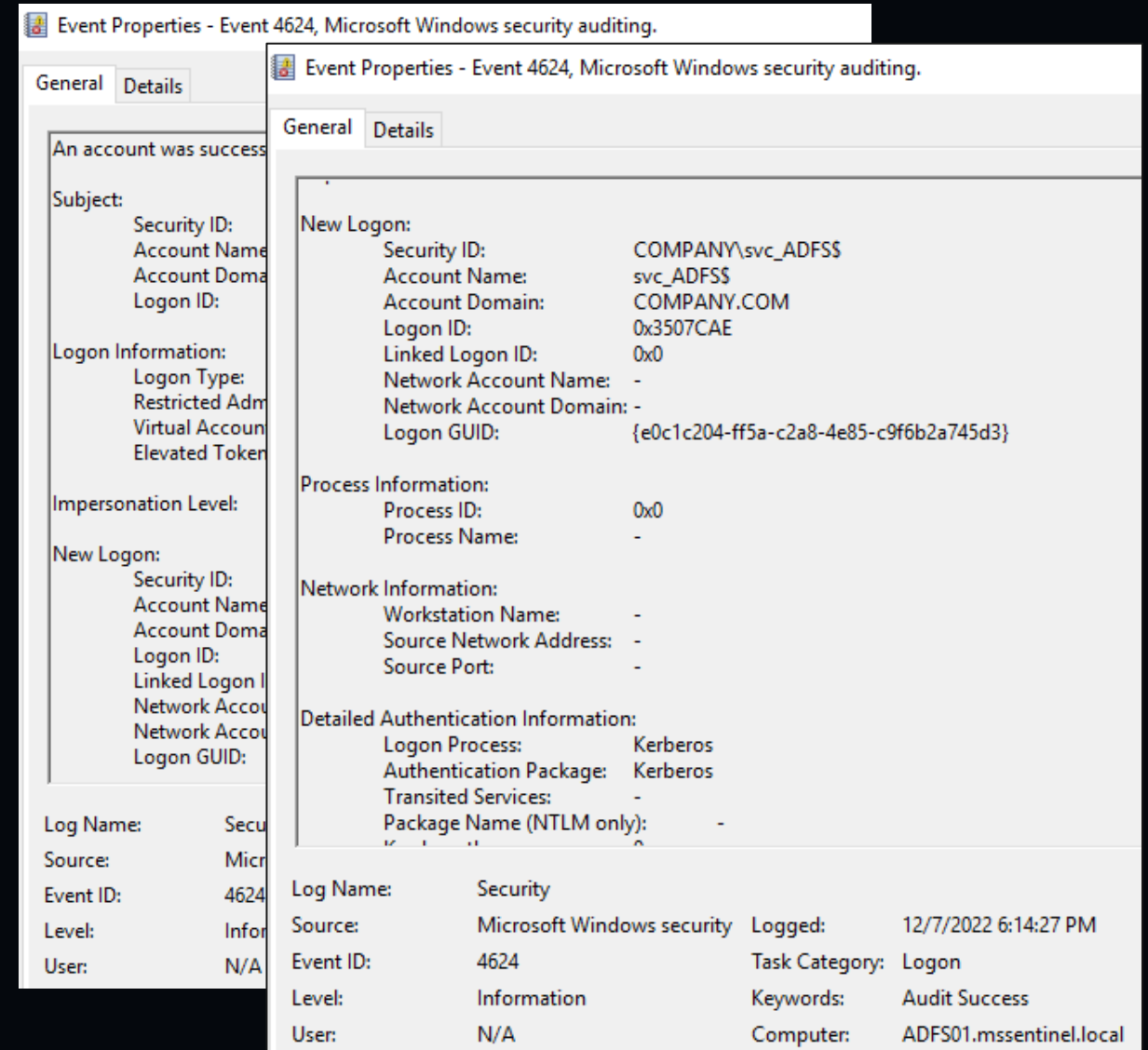
Instance ID:
bb38a97c-5d69-49c6-abe7-e3ccfaccf482

Caller identity:
<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>
MSENTINEL\adfsadmin2
<http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid>
S-1-5-21-408791858-2605294728-2249716225-1109
<http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupsid>
S-1-5-21-408791858-2605294728-2249716225-513
<http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid>
S-1-5-21-408791858-2605294728-2249716225-513
<http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid>
S-1-1-0

Log Name:	Security	Logged:	12/7/2022 6:14:27 PM
Source:	AD FS Auditing	Task Category:	(3)
Event ID:	501	Keywords:	Classic,Audit Success
Level:	Information	User:	COMPANY\svc_ADFSS
User:	COMPANY\svc_ADFSS	Computer:	ADFS01.mssentinel.local

AD FS Sync – Authentication

- **Log Name:** Security
- **Event:** 4624
- **Entities:** Host, User
- **Notes:**
 - COMPANY\svc_ADFS\$?
 - AADInternals signature



Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID:
- Account Name:
- Account Domain:
- Logon ID:

Logon Information:

- Logon Type:
- Restricted Administrator:
- Virtual Account:
- Elevated Token:

Impersonation Level:

New Logon:

- Security ID:
- Account Name:
- Account Domain:
- Logon ID:
- Linked Logon ID:
- Network Account Name:
- Network Account Domain:
- Logon GUID:

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

- Security ID: COMPANY\svc_ADFS\$
- Account Name: svc_ADFS\$
- Account Domain: COMPANY.COM
- Logon ID: 0x3507CAE
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {e0c1c204-ff5a-c2a8-4e85-c9f6b2a745d3}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: -
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:

- Logon Process: Kerberos
- Authentication Package: Kerberos
- Transited Services: -
- Package Name (NTLM only): -

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

Logged: 12/7/2022 6:14:27 PM

Task Category: Logon

Keywords: Audit Success

Computer: ADFS01.msssentinel.local

AD FS Sync – Authentication



```
https://github.com/Gerenios/AADInternals/blob/master/ADFS.ps1#L335-L351  
335 Write-Verbose "*" Start dumping AD FS configuration from  
336  
337 # Generate required stuff  
338 $sessionKey = (New-Guid).ToByteArray()  
339 $params=@{  
340     hash = $Hash  
341     SidString = $SID  
342     UserName= 'svc_ADFS$'  
343     UserDisplayName= ""  
344     UserPrincipalName= 'svc_ADFS$@company.com'  
345     ServerName= "DC"  
346     DomainName= "COMPANY"  
347     Realm= "COMPANY.COM"  
348     ServiceTarget = "host/sts.company.com"  
349     SessionKey = $sessionKey  
350 }  
351 $kerberosTicket = New-KerberosTicket @Params
```

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	No

Impersonation Level: Identification

New Logon:

Security ID:	COMPANY\svc_ADFS\$
Account Name:	svc_ADFS\$
Account Domain:	COMPANY.COM
Logon ID:	0x3507CAE
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{e0c1c204-ff5a-c2a8-4e85-c9f6b2a745d3}

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

Logged: 12/7/2022 6:14:27 PM

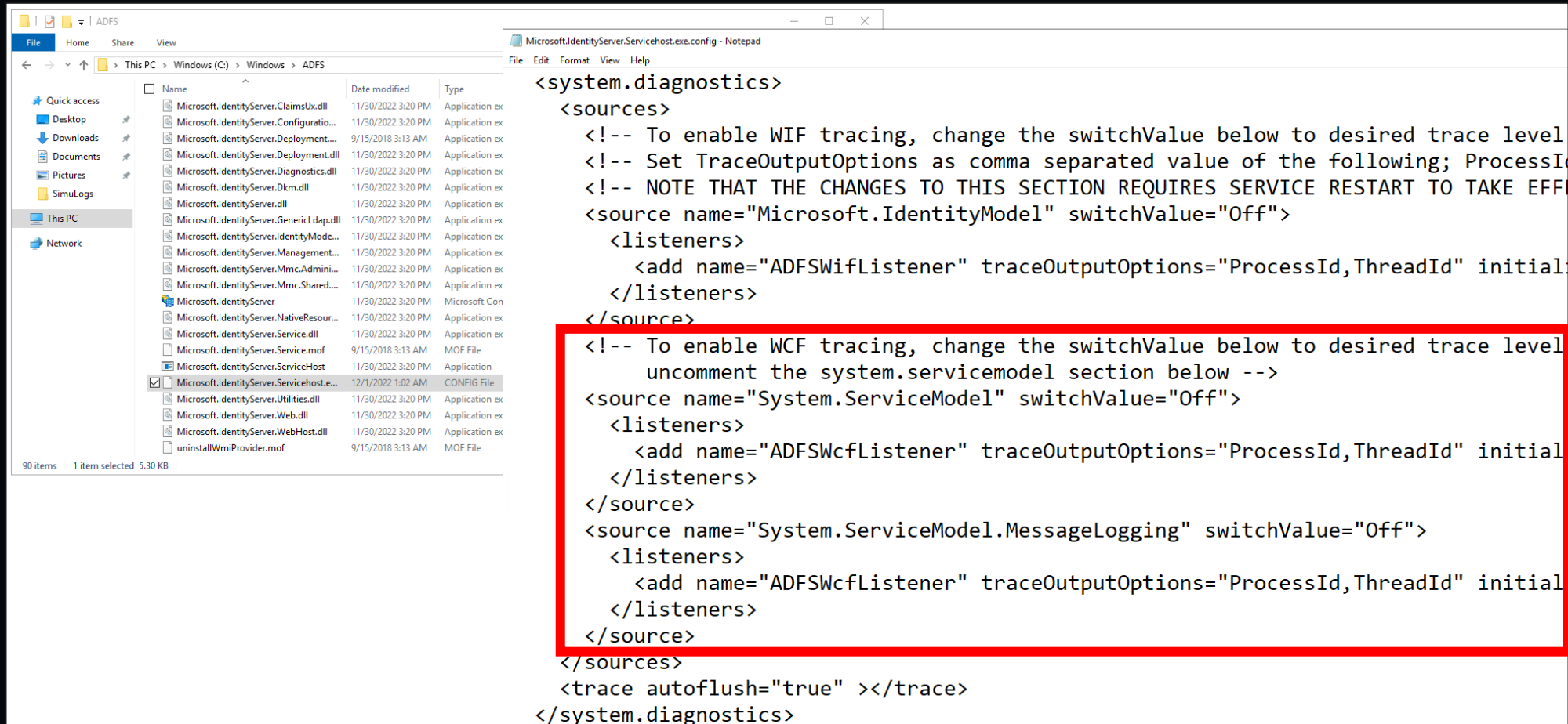
Task Category: Logon

Keywords: Audit Success

Computer: ADFS01.mssentinel.local

Additional AD FS Windows Communication Foundation (WCF) Logs - AD FS Tracing

Modify Microsoft.IdentityServer.ServiceHost.Exe.Config file






















The image shows a Windows File Explorer window displaying the contents of the AD FS directory. The file `Microsoft.IdentityServer.ServiceHost.exe.config` is selected. To the right, a Notepad window shows the XML configuration for this file. A red box highlights the following section of the XML:

```
<!-- To enable WCF tracing, change the switchValue below to desired trace level
uncomment the system.servicemodel section below -->
<source name="System.ServiceModel" switchValue="Off">
  <listeners>
    <add name="ADFSWcfListener" traceOutputOptions="ProcessId,ThreadId" initial
  </listeners>
</source>
<source name="System.ServiceModel.MessageLogging" switchValue="Off">
  <listeners>
    <add name="ADFSWcfListener" traceOutputOptions="ProcessId,ThreadId" initial
  </listeners>
</source>
```

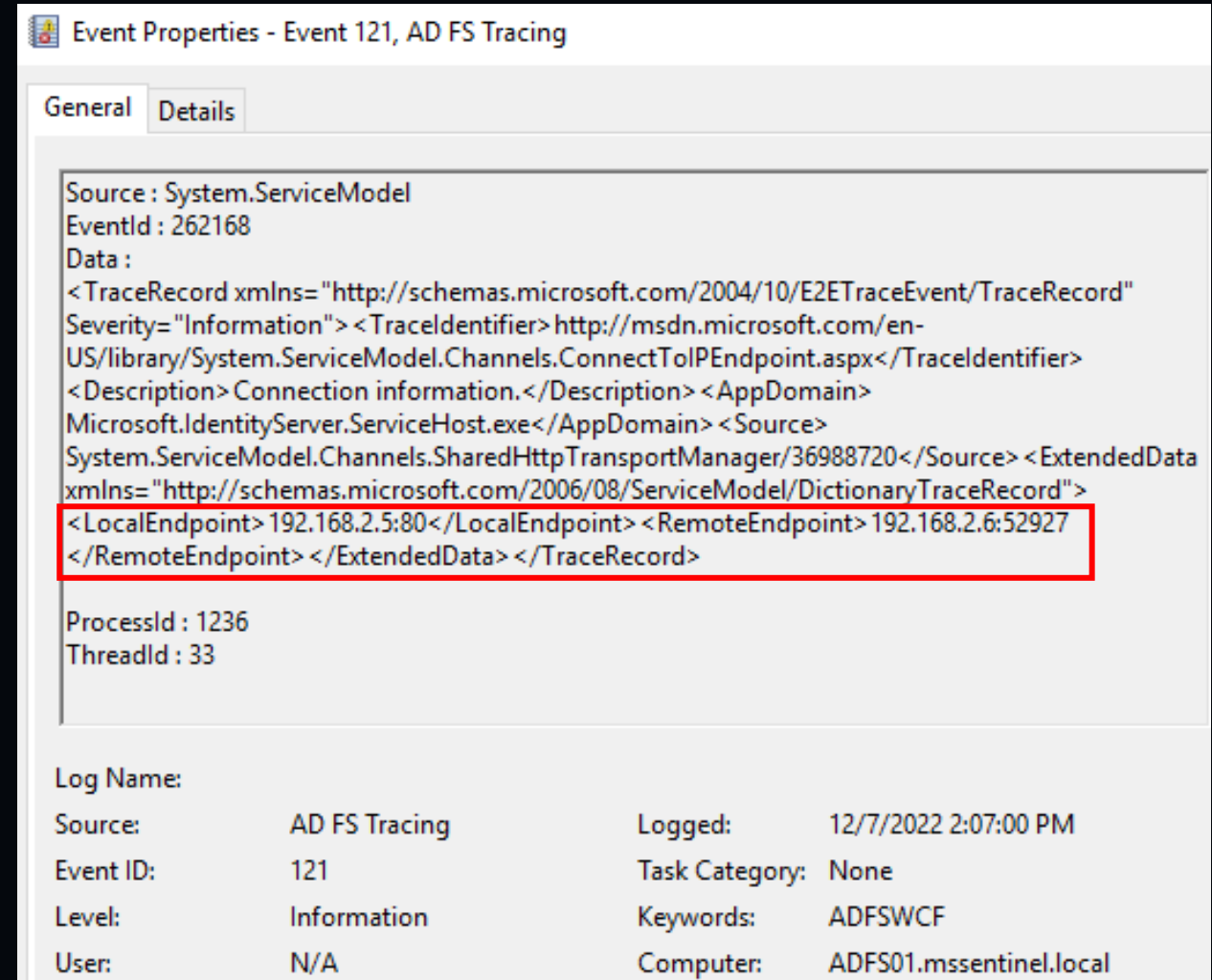
Capture AD FS WCF Events

- **Provider:** AD FS Tracing
- **Steps to capture events:**
 - logman start ADFSWCFTTrace -p "AD FS Tracing" -o ADFSTraceWCF.etl -ets
 - logman stop ADFSWCFTTrace -ets

Level	Date and Time	Source	Event ID	Task Category
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	998	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Verbose	12/7/2022 2:07:00 PM	AD FS Tracing	122	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	998	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	998	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	998	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	998	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	998	None
 Verbose	12/7/2022 2:07:00 PM	AD FS Tracing	122	None
 Verbose	12/7/2022 2:07:00 PM	AD FS Tracing	122	None
 Verbose	12/7/2022 2:07:00 PM	AD FS Tracing	122	None
 Verbose	12/7/2022 2:07:00 PM	AD FS Tracing	122	None
 Information	12/7/2022 2:07:00 PM	AD FS Tracing	121	None
 Information	12/7/2022 2:06:55 PM		0	None

AD FS Tracing – WCF Events

- **Provider:** AD FS Tracing
- **Event:** 121 (Connection information)
- **Entities:** Host, IP, Port
- **Notes:**
 - Extract “Remote Endpoint” values to identify suspicious connections (No AD FS related)



Event Properties - Event 121, AD FS Tracing

General Details

Source : System.ServiceModel
EventId : 262168
Data :
<TraceRecord xmlns="http://schemas.microsoft.com/2004/10/E2ETraceEvent/TraceRecord" Severity="Information"> <TraceIdentifier> http://msdn.microsoft.com/en-US/library/System.ServiceModel.Channels.ConnectToIPEndpoint.aspx</TraceIdentifier> <Description> Connection information.</Description> <AppDomain> Microsoft.IdentityServer.ServiceHost.exe</AppDomain> <Source> System.ServiceModel.Channels.SharedHttpTransportManager/36988720</Source> <ExtendedData xmlns="http://schemas.microsoft.com/2006/08/ServiceModel/DictionaryTraceRecord"> <LocalEndpoint>192.168.2.5:80</LocalEndpoint> <RemoteEndpoint>192.168.2.6:52927</RemoteEndpoint> </ExtendedData> </TraceRecord>

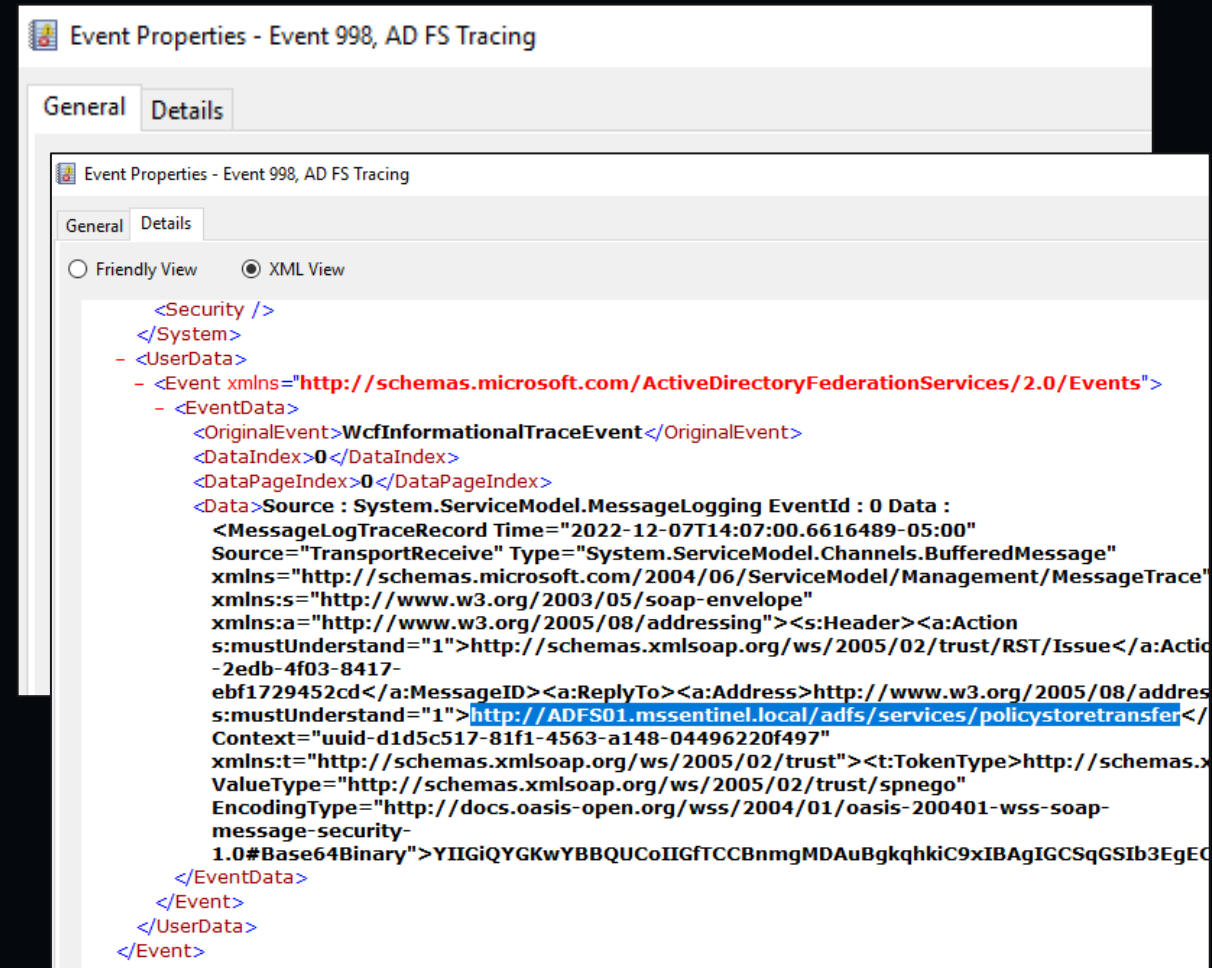
ProcessId : 1236
ThreadId : 33

Log Name:

Source:	AD FS Tracing	Logged:	12/7/2022 2:07:00 PM
Event ID:	121	Task Category:	None
Level:	Information	Keywords:	ADFS WCF
User:	N/A	Computer:	ADFS01.mssentinel.local

AD FS Tracing – WCF Events

- **Provider:** AD FS Tracing
- **Event:** 998
- **Notes:**
 - Client connects to the URL `http://<adfs server name>:80/adfs/services/policystoretransfer`.
 - The actual data being exchanged is encrypted during transit.



```
<Security />
</System>
- <UserData>
- <Event xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events">
- <EventData>
<OriginalEvent>WcfInformationalTraceEvent</OriginalEvent>
<DataIndex>0</DataIndex>
<DataPageIndex>0</DataPageIndex>
<Data>Source : System.ServiceModel.MessageLogging EventId : 0 Data :
<MessageLogTraceRecord Time="2022-12-07T14:07:00.6616489-05:00"
Source="TransportReceive" Type="System.ServiceModel.Channels.BufferedMessage"
xmlns="http://schemas.microsoft.com/2004/06/ServiceModel/Management/MessageTrace"
xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing"><s:Header><a:Action
s:mustUnderstand="1">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action
-2edb-4f03-8417-
ebf1729452cd</a:MessageID><a:ReplyTo><a:Address>http://www.w3.org/2005/08/address
s:mustUnderstand="1">http://ADFS01.mssentinel.local/adfs/services/policystoretransfer</
Context="uuid-d1d5c517-81f1-4563-a148-04496220f497"
xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust"><t:TokenType>http://schemas.x
ValueType="http://schemas.xmlsoap.org/ws/2005/02/trust/spnego"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-
1.0#Base64Binary">YIIGiQYGKwYBBQUCoIIGfTCCBnmgMDAuBgkqhkiC9xIBAgIGCSqGSIB3EgEC
</EventData>
</Event>
</UserData>
</Event>
```

AD FS Tracing – WCF Events

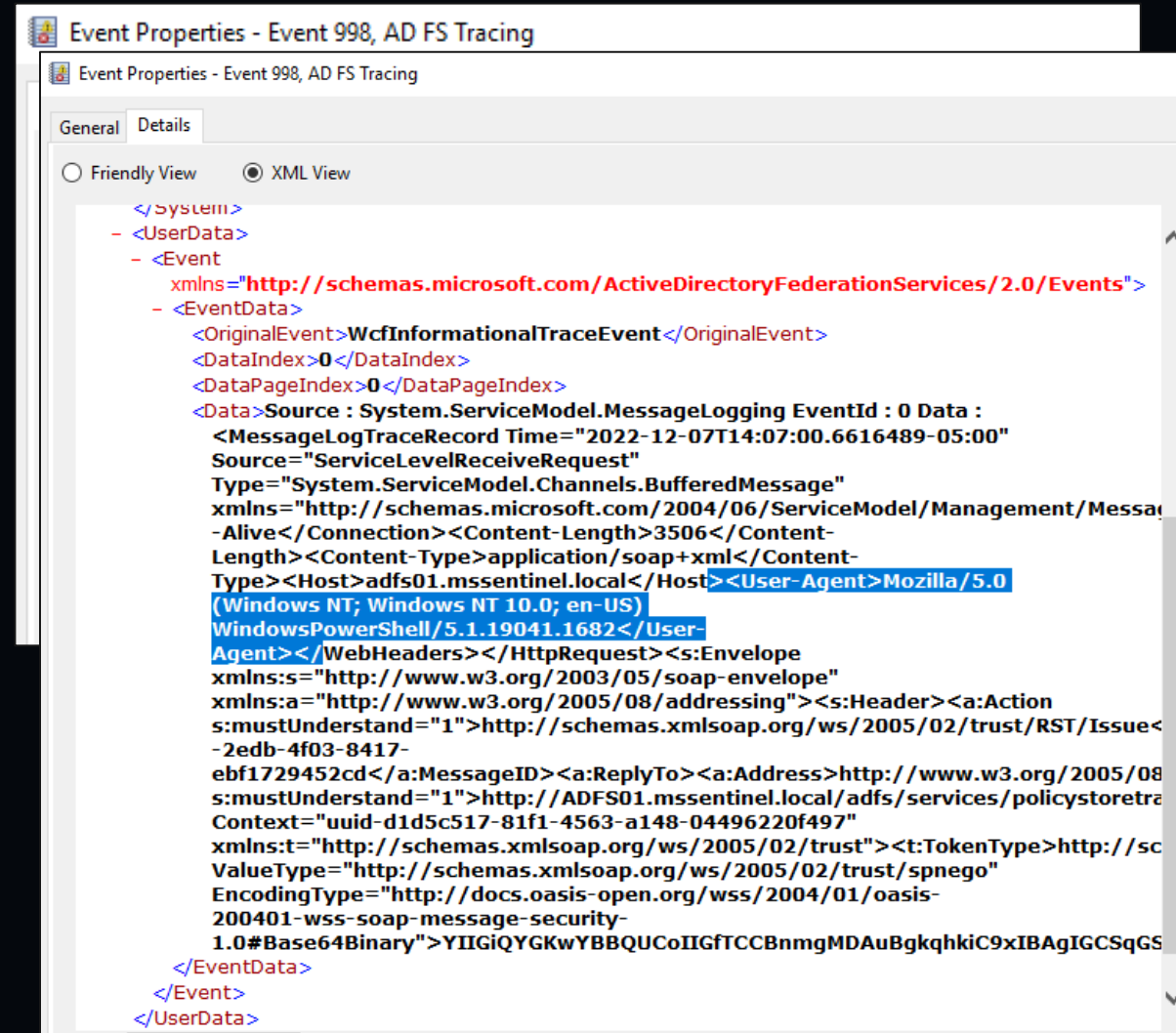


- **Provider:** AD FS Tracing
- **Event:** 121 (Received a message over a channel)
- **Notes:**
 - Client connects to the URL `http://<adfs server name>:80/adfs/services/policystoretransfer`.

A screenshot of the Windows Event Viewer showing the details of Event 121, AD FS Tracing. The window title is "Event Properties - Event 121, AD FS Tracing". The "Details" tab is selected, showing the following information:
Source: System.ServiceModel
EventId: 262163
Data:
<TraceRecord xmlns="http://schemas.microsoft.com/2004/10/E2ETraceEvent/TraceRecord" Severity="Information">
<TraceIdentifier> http://msdn.microsoft.com/en-US/library/System.ServiceModel.Channels.MessageReceived.aspx
</TraceIdentifier> <Description> Received a message over a channel.</Description> <AppDomain>
Microsoft.IdentityServer.ServiceHost.exe</AppDomain> <Source>
System.ServiceModel.Channels.HttpRequestContext+ListenerHttpContext+ListenerContextHttpInput/23214600</Source>
<ExtendedData xmlns="http://schemas.microsoft.com/2006/08/ServiceModel/MessageTransmitTraceRecord">
<MessageProperties> <Encoder> application/soap+xml; charset=utf-8</Encoder> <AllowOutputBatching> False
</AllowOutputBatching> <Via> http://adfs01.mssentinel.local/adfs/services/policystoretransfer</Via> </MessageProperties>
<MessageHeaders> <a:Action s:mustUnderstand="1" xmlns:s="http://www.w3.org/2003/05/soap-envelope"
xmlns:a="http://www.w3.org/2005/08/addressing"> http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</a:Action>
<a:MessageID xmlns:a="http://www.w3.org/2005/08/addressing"> urn:uuid:e1fccf1c-2edb-4f03-8417-ebf1729452cd
</a:MessageID> <a:ReplyTo xmlns:a="http://www.w3.org/2005/08/addressing"> <a:Address>
http://www.w3.org/2005/08/addressing/anonymous</a:Address> </a:ReplyTo> <a:To s:mustUnderstand="1"
xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
<http://ADFS01.mssentinel.local/adfs/services/policystoretransfer></a:To> </MessageHeaders> </ExtendedData>
</TraceRecord>
ProcessId: 1236
ThreadId: 33
Log Name:
Source: AD FS Tracing Logged: 12/7/2022 2:07:00 PM
Event ID: 121 Task Category: None
Level: Information Keywords: ADFS WCF
User: N/A Computer: ADFS01.mssentinel.local

AD FS Tracing – WCF Events

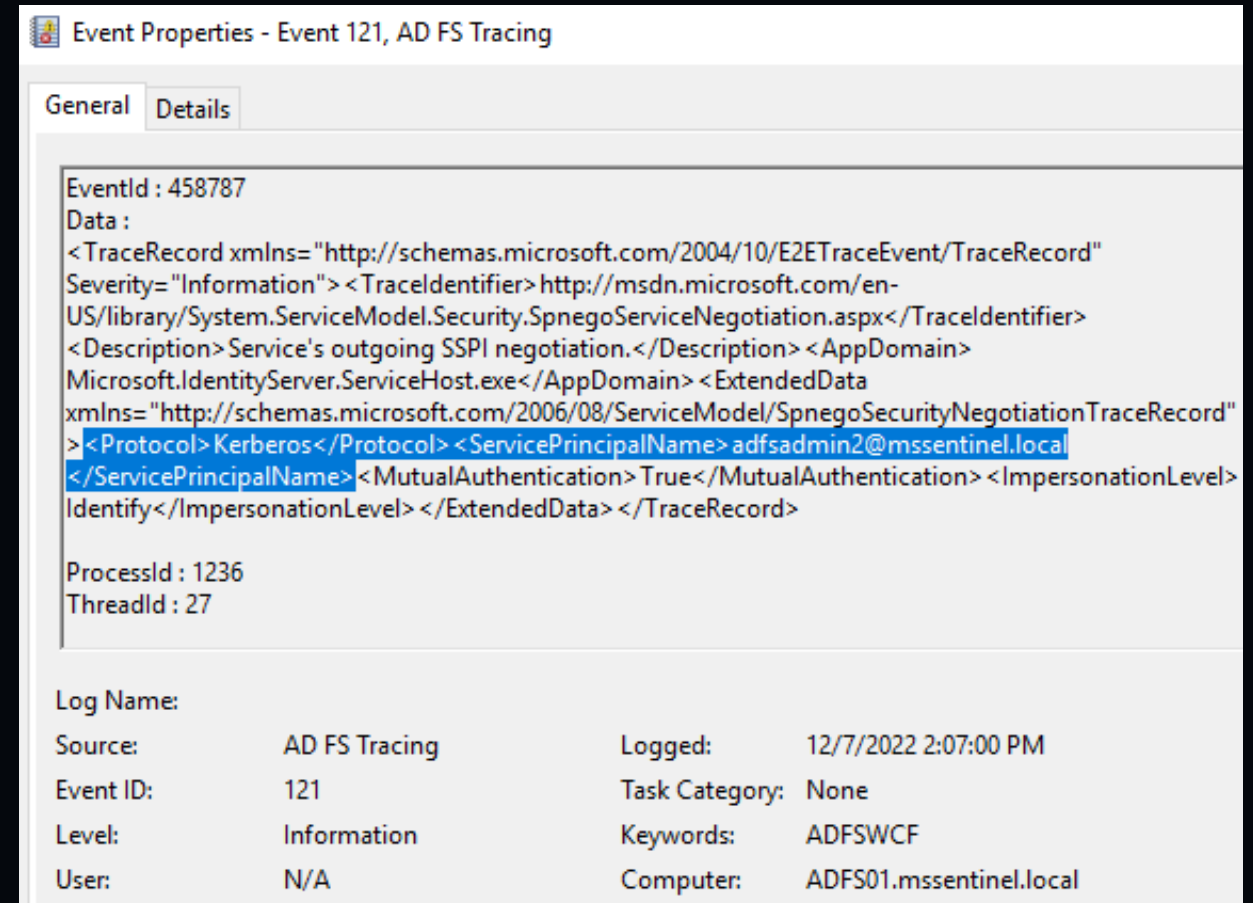
- **Provider:** AD FS Tracing
- **Event:** 998
- **Notes:**
 - Soap Envelope
 - Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1682



```
</System>
- <UserData>
- <Event
  xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events">
- <EventData>
  <OriginalEvent>WcfInformationalTraceEvent</OriginalEvent>
  <DataIndex>0</DataIndex>
  <DataPageIndex>0</DataPageIndex>
  <Data>Source : System.ServiceModel.MessageLogging EventId : 0 Data :
  <MessageLogTraceRecord Time="2022-12-07T14:07:00.6616489-05:00"
  Source="ServiceLevelReceiveRequest"
  Type="System.ServiceModel.Channels.BufferedMessage"
  xmlns="http://schemas.microsoft.com/2004/06/ServiceModel/Management/Messa
  -Alive</Connection><Content-Length>3506</Content-
  Length><Content-Type>application/soap+xml</Content-
  Type><Host>adfs01.msssentinel.local</Host><User-Agent>Mozilla/5.0
  (Windows NT; Windows NT 10.0; en-US)
  WindowsPowerShell/5.1.19041.1682</User-
  Agent></WebHeaders></HttpRequest><s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing"><s:Header><a:Action
  s:mustUnderstand="1">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue<
  -2edb-4f03-8417-
  ebf1729452cd</a:MessageID><a:ReplyTo><a:Address>http://www.w3.org/2005/08
  s:mustUnderstand="1">http://ADFS01.msssentinel.local/adfs/services/policystoretra
  Context="uuid-d1d5c517-81f1-4563-a148-04496220f497"
  xmlns:t="http://schemas.xmlsoap.org/ws/2005/02/trust"><t:TokenType>http://sc
  ValueType="http://schemas.xmlsoap.org/ws/2005/02/trust/spnego"
  EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
  200401-wss-soap-message-security-
  1.0#Base64Binary">YIIgiQYGKwYBBQUCoIIGfTCCBnmgMDAuBgkqhkiC9xIBAgIGCSqGS
  </EventData>
</Event>
</UserData>
```

AD FS Tracing – WCF Events

- **Provider:** AD FS Tracing
- **Event:** 121 (Services's Outgoing SSIP Negotiation)
- **Notes:**
 - Kerberos protocol
 - SPN: AD FS Service account



Event Properties - Event 121, AD FS Tracing

General Details

EventId : 458787
Data :
<TraceRecord xmlns="http://schemas.microsoft.com/2004/10/E2ETraceEvent/TraceRecord" Severity="Information"><TracelIdentifier>http://msdn.microsoft.com/en-US/library/System.ServiceModel.Security.SpnegoServiceNegotiation.aspx</TracelIdentifier><Description>Service's outgoing SSPI negotiation.</Description><AppDomain>Microsoft.IdentityServer.ServiceHost.exe</AppDomain><ExtendedData xmlns="http://schemas.microsoft.com/2006/08/ServiceModel/SpnegoSecurityNegotiationTraceRecord"><Protocol>Kerberos</Protocol><ServicePrincipalName>adfsadmin2@mssentinel.local</ServicePrincipalName><MutualAuthentication>True</MutualAuthentication><ImpersonationLevel>Identify</ImpersonationLevel></ExtendedData></TraceRecord>

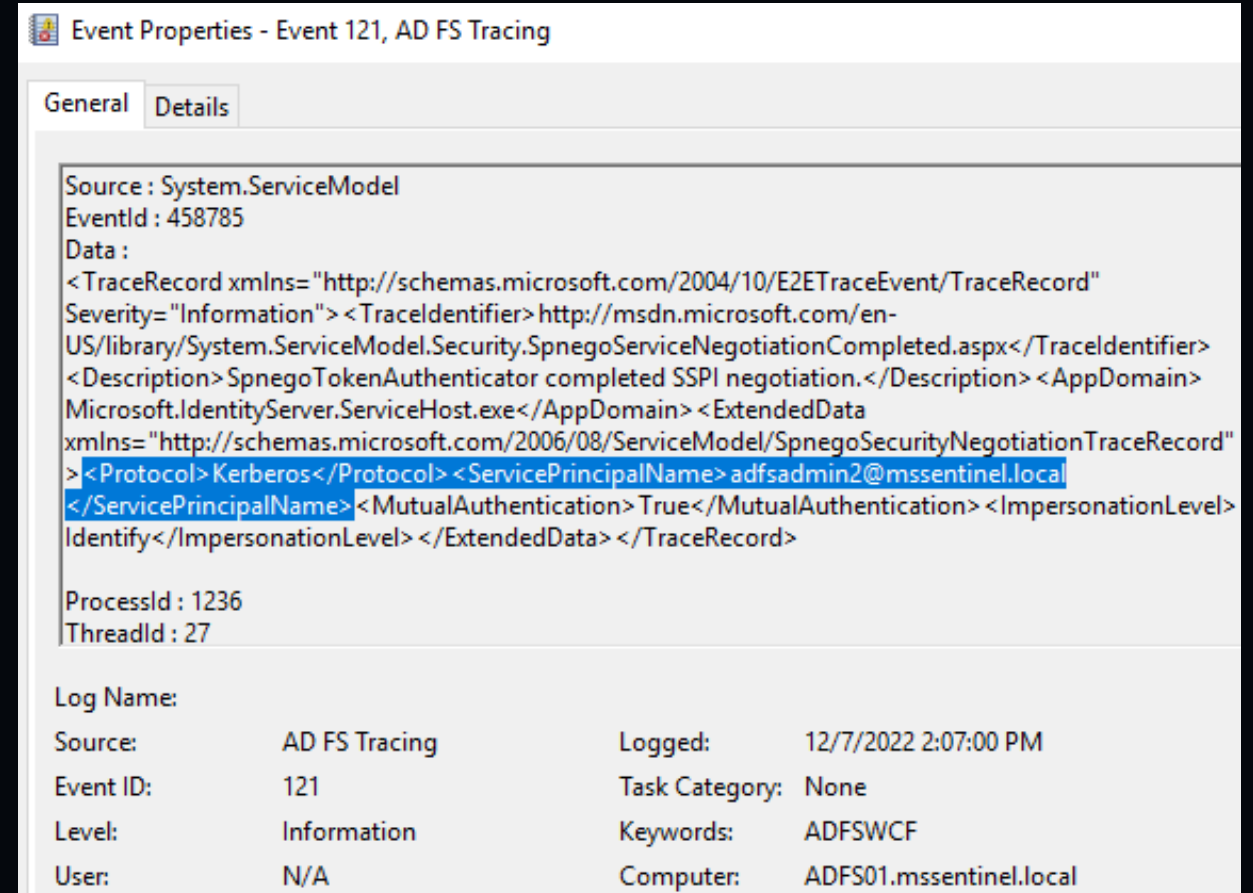
ProcessId : 1236
ThreadId : 27

Log Name:

Source:	AD FS Tracing	Logged:	12/7/2022 2:07:00 PM
Event ID:	121	Task Category:	None
Level:	Information	Keywords:	ADFS WCF
User:	N/A	Computer:	ADFS01.mssentinel.local

AD FS Tracing – WCF Events

- **Provider:** AD FS Tracing
- **Event:** 121 (SPNEGO SSPI negotiation completed)
- **Notes:**
 - Kerberos protocol
 - SPN: AD FS Service account



Event Properties - Event 121, AD FS Tracing

General Details

Source : System.ServiceModel
EventId : 458785
Data :
<TraceRecord xmlns="http://schemas.microsoft.com/2004/10/E2ETraceEvent/TraceRecord" Severity="Information"><TracIdentifier> http://msdn.microsoft.com/en-US/library/System.ServiceModel.Security.SpnegoServiceNegotiationCompleted.aspx</TracIdentifier><Description> SpnegoTokenAuthenticator completed SSPI negotiation.</Description> <AppDomain> Microsoft.IdentityServer.ServiceHost.exe</AppDomain> <ExtendedData xmlns="http://schemas.microsoft.com/2006/08/ServiceModel/SpnegoSecurityNegotiationTraceRecord"><Protocol> Kerberos</Protocol> <ServicePrincipalName> adfsadmin2@mssentinel.local</ServicePrincipalName> <MutualAuthentication> True</MutualAuthentication> <ImpersonationLevel> Identify</ImpersonationLevel> </ExtendedData> </TraceRecord>

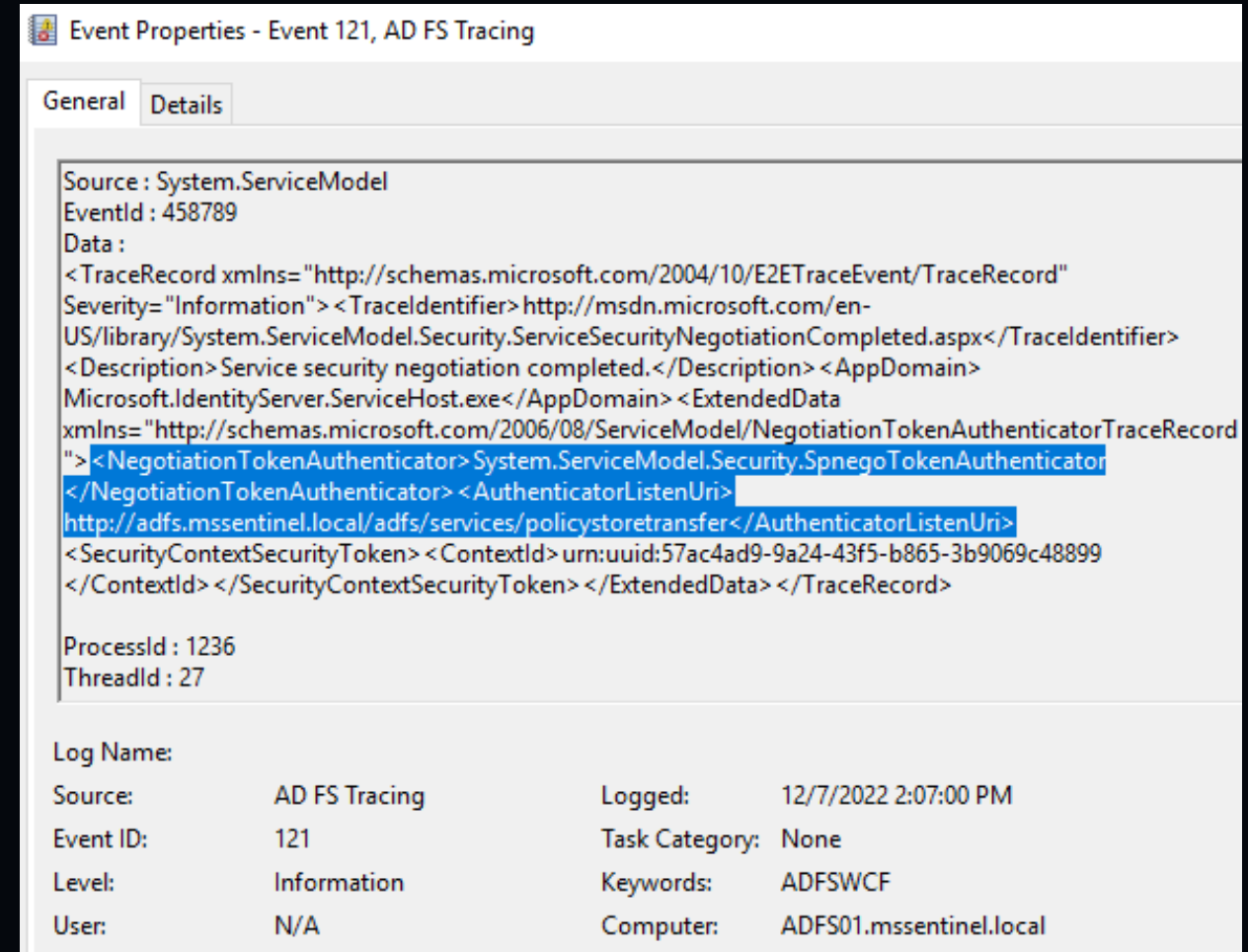
ProcessId : 1236
ThreadId : 27

Log Name:

Source:	AD FS Tracing	Logged:	12/7/2022 2:07:00 PM
Event ID:	121	Task Category:	None
Level:	Information	Keywords:	ADFSWCF
User:	N/A	Computer:	ADFS01.mssentinel.local

AD FS Tracing – WCF Events

- **Provider:** AD FS Tracing
- **Event:** 121 (Service security negotiation completed)
- **Notes:**
 - **http://<adfs server name>:80/adfs/services/policy storetransfer**



Event Properties - Event 121, AD FS Tracing

General Details

Source : System.ServiceModel
EventId : 458789
Data :
<TraceRecord xmlns="http://schemas.microsoft.com/2004/10/E2ETraceEvent/TraceRecord" Severity="Information"> <TraceIdentifier>http://msdn.microsoft.com/en-US/library/System.ServiceModel.Security.ServiceSecurityNegotiationCompleted.aspx</TraceIdentifier> <Description>Service security negotiation completed.</Description> <AppDomain>Microsoft.IdentityServer.ServiceHost.exe</AppDomain> <ExtendedData xmlns="http://schemas.microsoft.com/2006/08/ServiceModel/NegotiationTokenAuthenticatorTraceRecord"> <NegotiationTokenAuthenticator> System.ServiceModel.Security.SpnegoTokenAuthenticator </NegotiationTokenAuthenticator> <AuthenticatorListenUri> http://adfs.mssentinel.local/adfs/services/policystoretransfer</AuthenticatorListenUri> <SecurityContextSecurityToken> <ContextId>urn:uuid:57ac4ad9-9a24-43f5-b865-3b9069c48899 </ContextId> </SecurityContextSecurityToken> </ExtendedData> </TraceRecord>

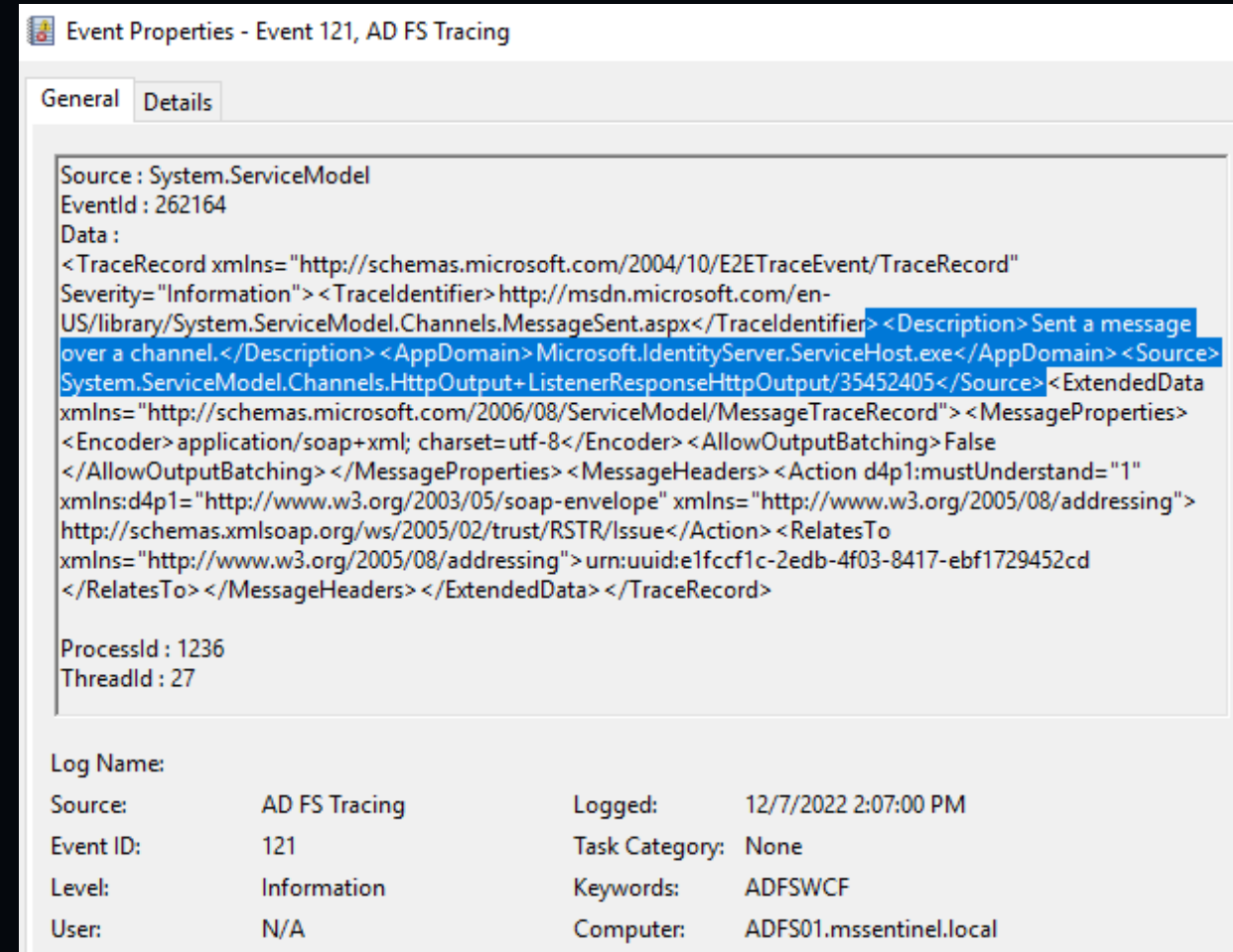
ProcessId : 1236
ThreadId : 27

Log Name:

Source:	AD FS Tracing	Logged:	12/7/2022 2:07:00 PM
Event ID:	121	Task Category:	None
Level:	Information	Keywords:	ADFSWCF
User:	N/A	Computer:	ADFS01.mssentinel.local

AD FS Tracing – WCF Events

- **Provider:** AD FS Tracing
- **Event:** 121 (Sent a message over a channel)



Event Properties - Event 121, AD FS Tracing

General Details

Source : System.ServiceModel
EventId : 262164
Data :
<TraceRecord xmlns="http://schemas.microsoft.com/2004/10/E2ETraceEvent/TraceRecord"
Severity="Information"><TraceIdentifier>http://msdn.microsoft.com/en-
US/library/System.ServiceModel.Channels.MessageSent.aspx</TraceIdentifier><Description> Sent a message
over a channel.</Description><AppDomain> Microsoft.IdentityServer.ServiceHost.exe</AppDomain><Source>
System.ServiceModel.Channels.HttpOutput+ListenerResponseHttpOutput/35452405</Source><ExtendedData
xmlns="http://schemas.microsoft.com/2006/08/ServiceModel/MessageTraceRecord"><MessageProperties>
<Encoder> application/soap+xml; charset=utf-8</Encoder><AllowOutputBatching> False
</AllowOutputBatching></MessageProperties><MessageHeaders><Action d4p1:mustUnderstand="1"
xmlns:d4p1="http://www.w3.org/2003/05/soap-envelope" xmlns="http://www.w3.org/2005/08/addressing">
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue</Action><RelatesTo
xmlns="http://www.w3.org/2005/08/addressing"> urn:uuid:e1fccf1c-2edb-4f03-8417-ebf1729452cd
</RelatesTo></MessageHeaders></ExtendedData></TraceRecord>

ProcessId : 1236
ThreadId : 27

Log Name:

Source:	AD FS Tracing	Logged:	12/7/2022 2:07:00 PM
Event ID:	121	Task Category:	None
Level:	Information	Keywords:	ADFS WCF
User:	N/A	Computer:	ADFS01.mssentinel.local

Mitigation - Windows Firewall



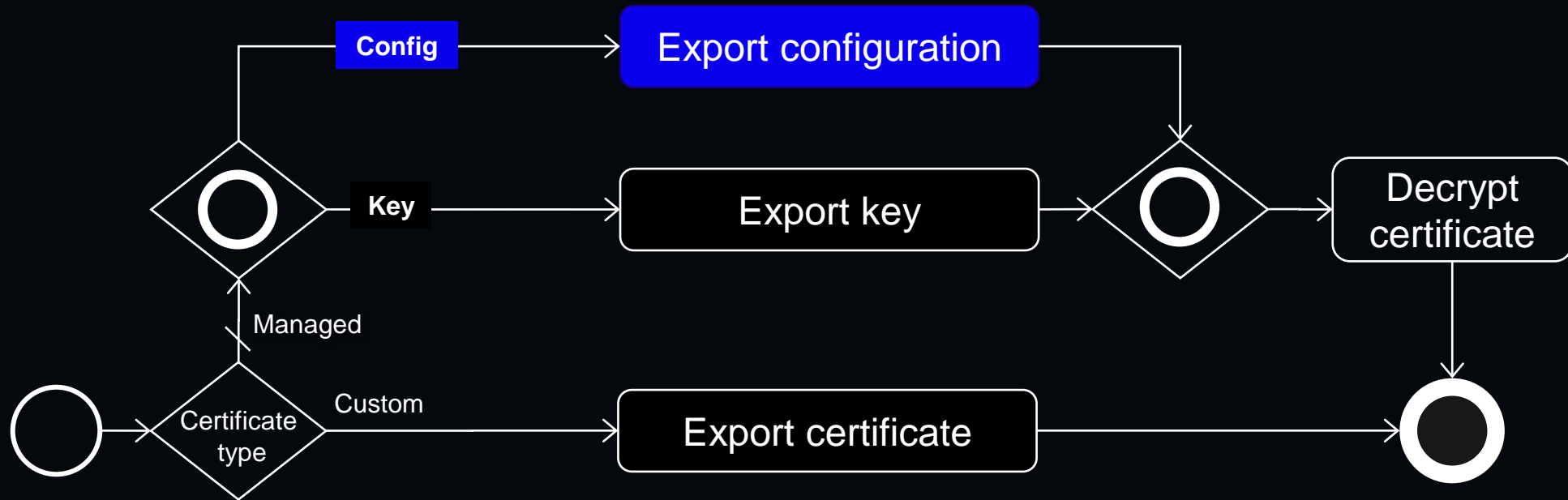
Modify existing inbound rule

```
Set-NetFirewallRule -DisplayName "AD FS HTTP Services (TCP-In)" -RemoteAddress <ADFS1 IP address>,<ADFS2 IP Address>
```

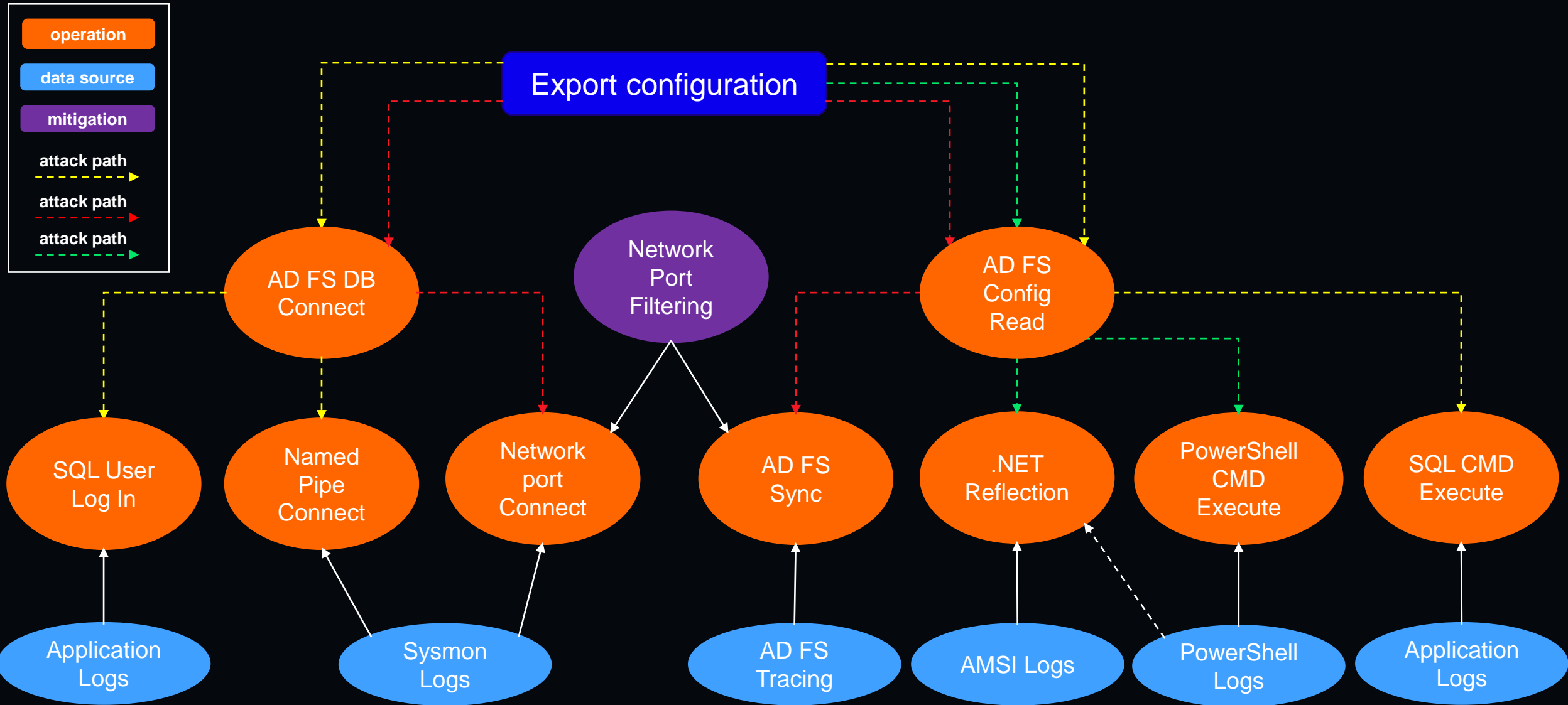
Create new inbound rule

```
New-NetFirewallRule -DisplayName "Allow ADFS Servers TCP 80" -  
Direction Inbound -Action Allow -Protocol TCP -LocalPort 80 -  
RemoteAddress <ADFS1 IP address>,<ADFS2 IP Address>
```

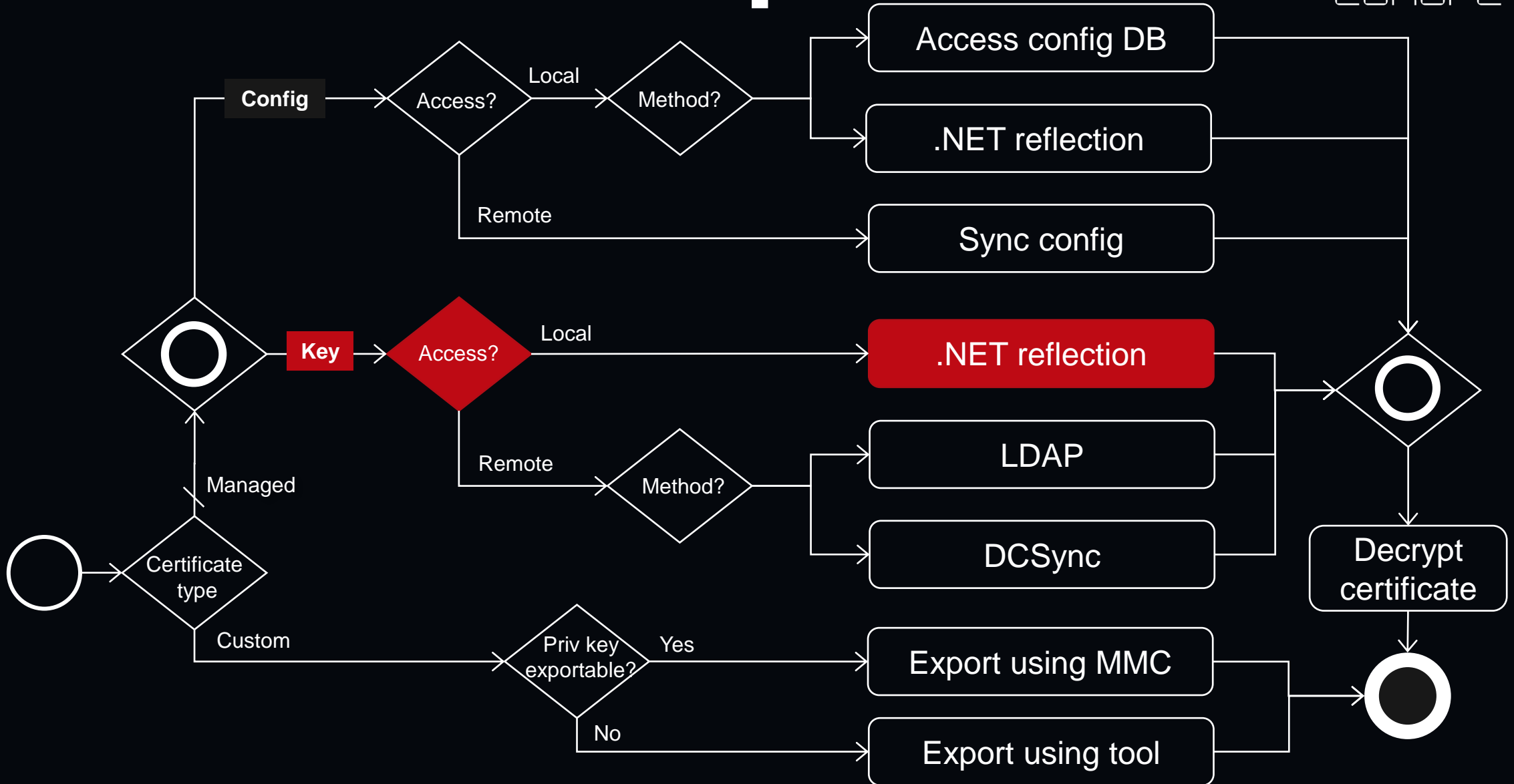
AD FS Attack Graph



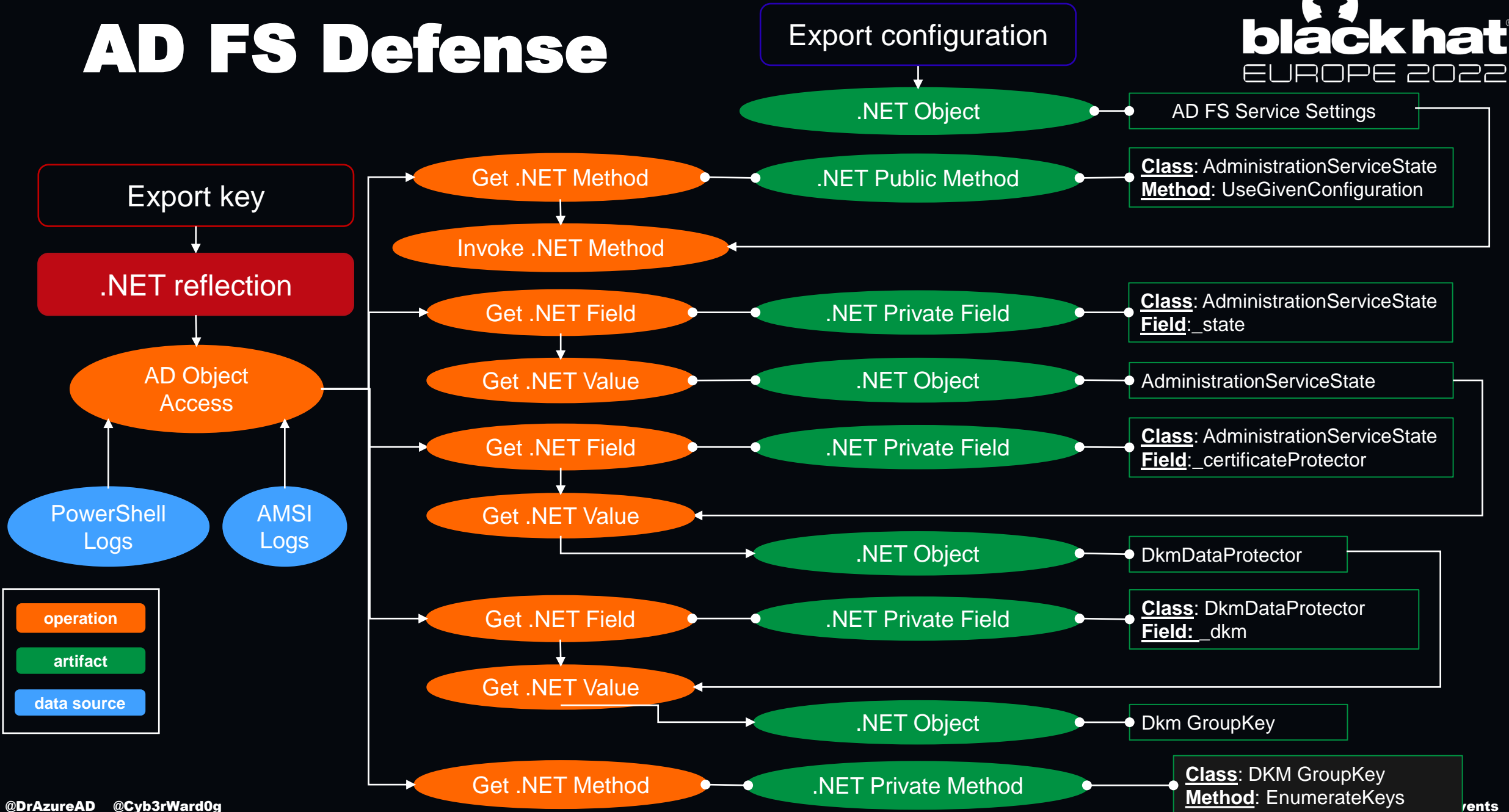
AD FS Attack - Defence Graph



AD FS Attack Graph

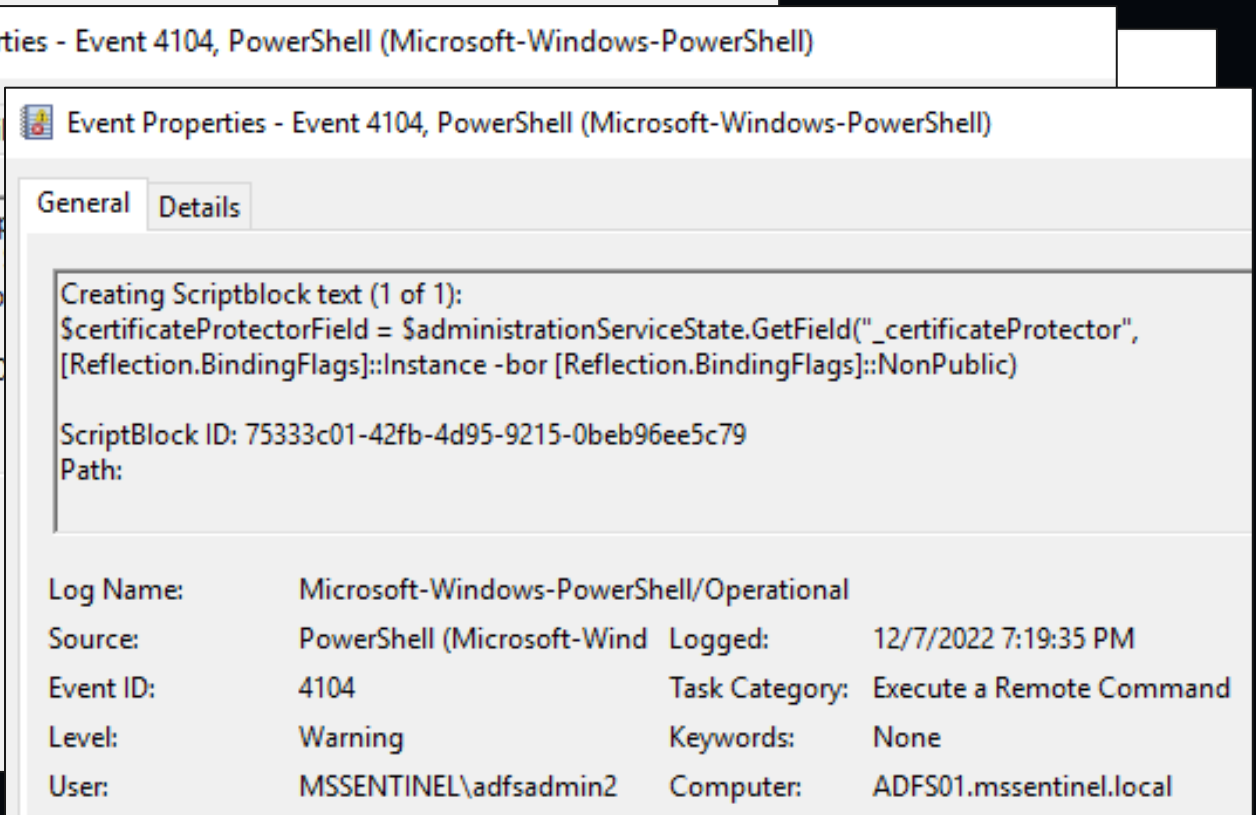
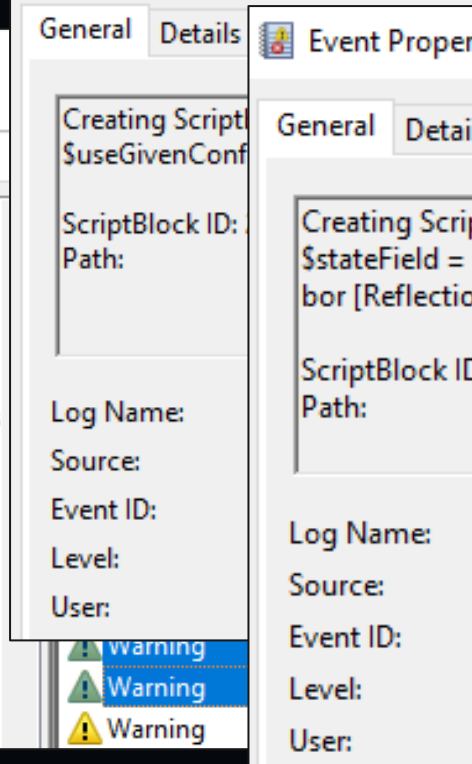
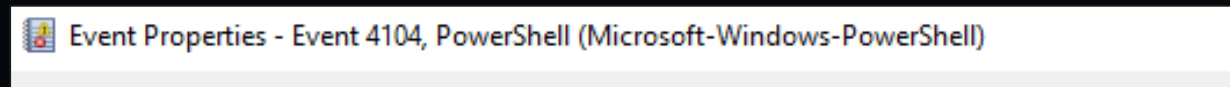
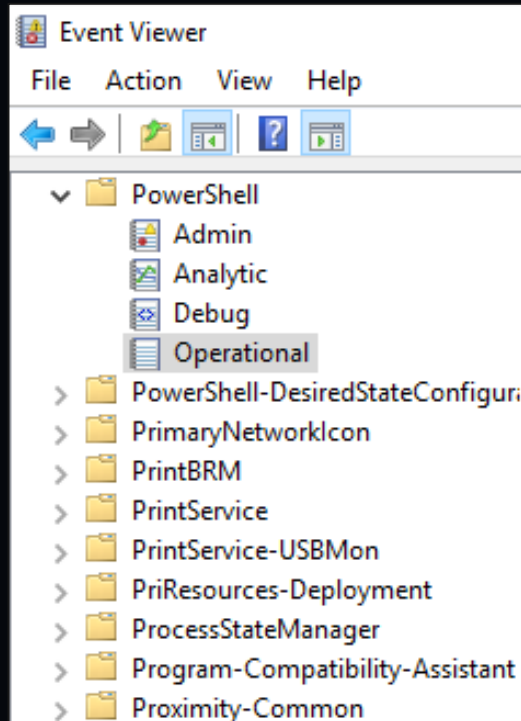


AD FS Defense



PowerShell Scriptblock Logging

- **Log Name:** Microsoft-Windows-PowerShell/Operational
- **Event:** 4104



Interpreting AMSI Content



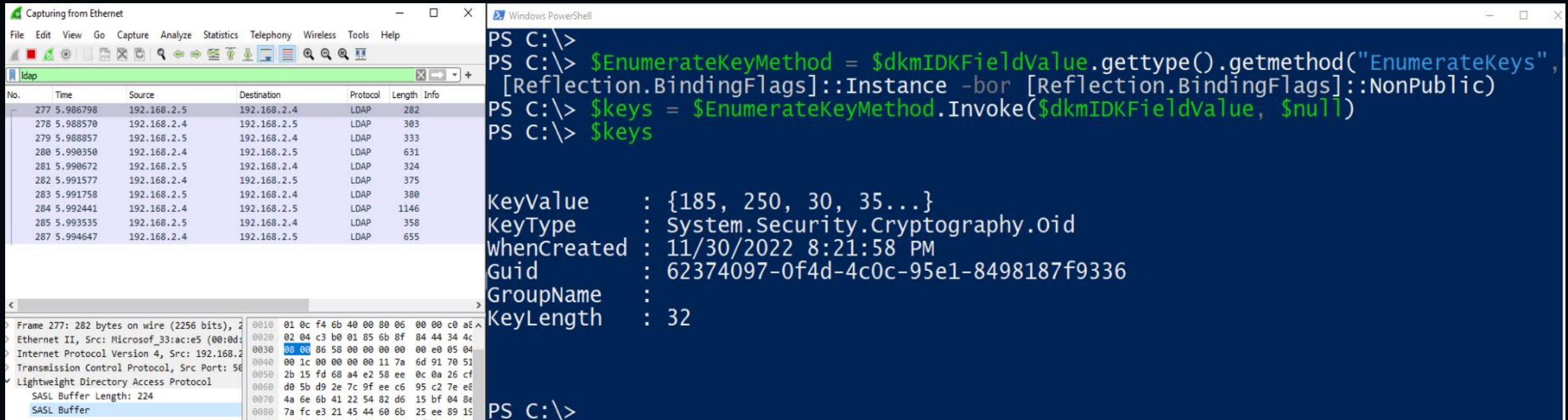
Administrator: Windows PowerShell

```
PS C:\programdata> Get-AmsiEvent -Path .\AMSITraceADFSDKMKey.etl | Where-Object {$_.Content -ne 'prompt'} | Select Content

Content
-----
$ServiceProperties = Get-ADFSProperties
...
$ServiceSettingsDataProperty = $ServiceProperties.GetType().GetProperty("ServiceSettingsData", [System.Reflection.BindingFlags]::NonPublic)
$ServiceSettingsDataPropertyValue = $ServiceSettingsDataProperty.GetValue($ServiceProperties, $null)
$adfsService = get-wmiobject -query 'select * from win32_service where name="adfssrv"'
@{...
$adfsDirectory = (get-item $adfsService.PathName).Directory.FullName
$msIdentityServerServiceDLLPath = Join-Path -Path $adfsDirectory -ChildPath 'Microsoft.IdentityServer.Service.dll'
[Environment]::OSVersion.Version
$global:?
$peBytes = [IO.File]::ReadAllBytes($msIdentityServerServiceDLLPath)
$msIdentityServerServiceAssembly = [Reflection.Assembly]::Load($PEBytes)
$administrationServiceState = $msIdentityServerServiceAssembly.GetType('Microsoft.IdentityServer.Service.Configuration.AdminServiceState')
[Environment]::OSVersion.Version
$global:?
$useGivenConfig = $administrationServiceState.GetMethod('UseGivenConfiguration')
$useGivenConfig.invoke($null, $ServiceSettingsDataPropertyValue)
```

<https://gist.github.com/mgraeber-rc/1eb42d3ec9c2f677e70bb14c3b7b5c9c>

LDAP Traffic?



The screenshot displays two windows side-by-side. On the left is Wireshark, showing a capture of LDAP traffic between 192.168.2.5 and 192.168.2.4. The selected frame (277) is expanded to show the following protocol layers:

- Frame 277: 282 bytes on wire (2256 bits), 2000 bytes captured (15360 bits) on interface 0
- Ethernet II, Src: Microsoft...:ac:e5 (00:0d:5c:ac:e5:00), Dst: 08:00:2b:15:fd:68
- Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.4
- Transmission Control Protocol, Src Port: 5688, Dst Port: 389
- Lightweight Directory Access Protocol
- SASL Buffer Length: 224
- SASL Buffer

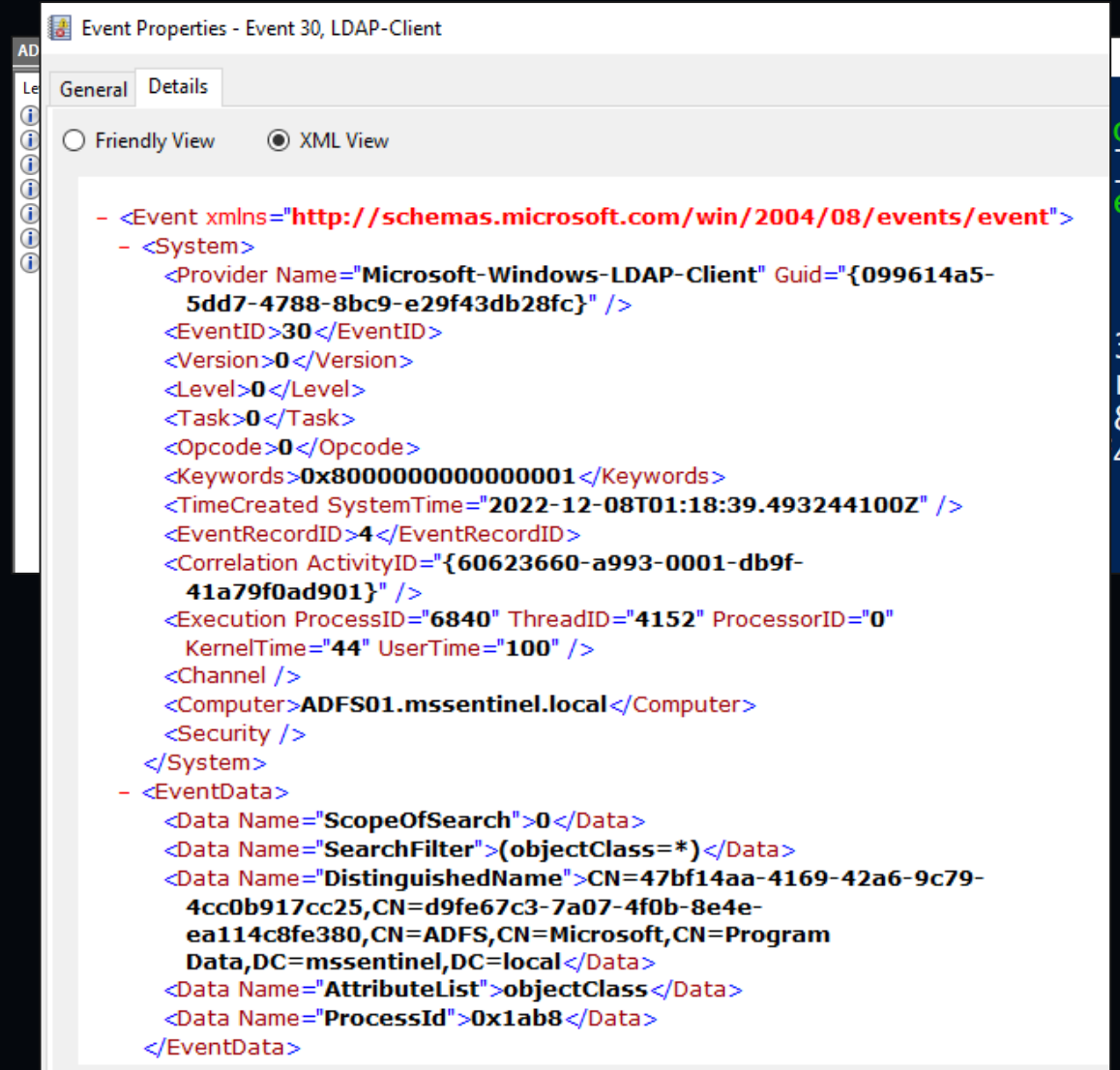
On the right is a Windows PowerShell terminal window. It shows a PowerShell script that uses reflection to enumerate keys from a specific LDAP field value. The output of the script is as follows:

```
PS C:\> $EnumerateKeyMethod = $dkmIDKFieldValue.GetType().GetMethod("EnumerateKeys", [Reflection.BindingFlags]::Instance -bor [Reflection.BindingFlags]::NonPublic)
PS C:\> $keys = $EnumerateKeyMethod.Invoke($dkmIDKFieldValue, $null)
PS C:\> $keys

KeyValue       : {185, 250, 30, 35...}
KeyType        : System.Security.Cryptography.Oid
WhenCreated    : 11/30/2022 8:21:58 PM
Guid           : 62374097-0f4d-4c0c-95e1-8498187f9336
GroupName      :
KeyLength      : 32
PS C:\>
```

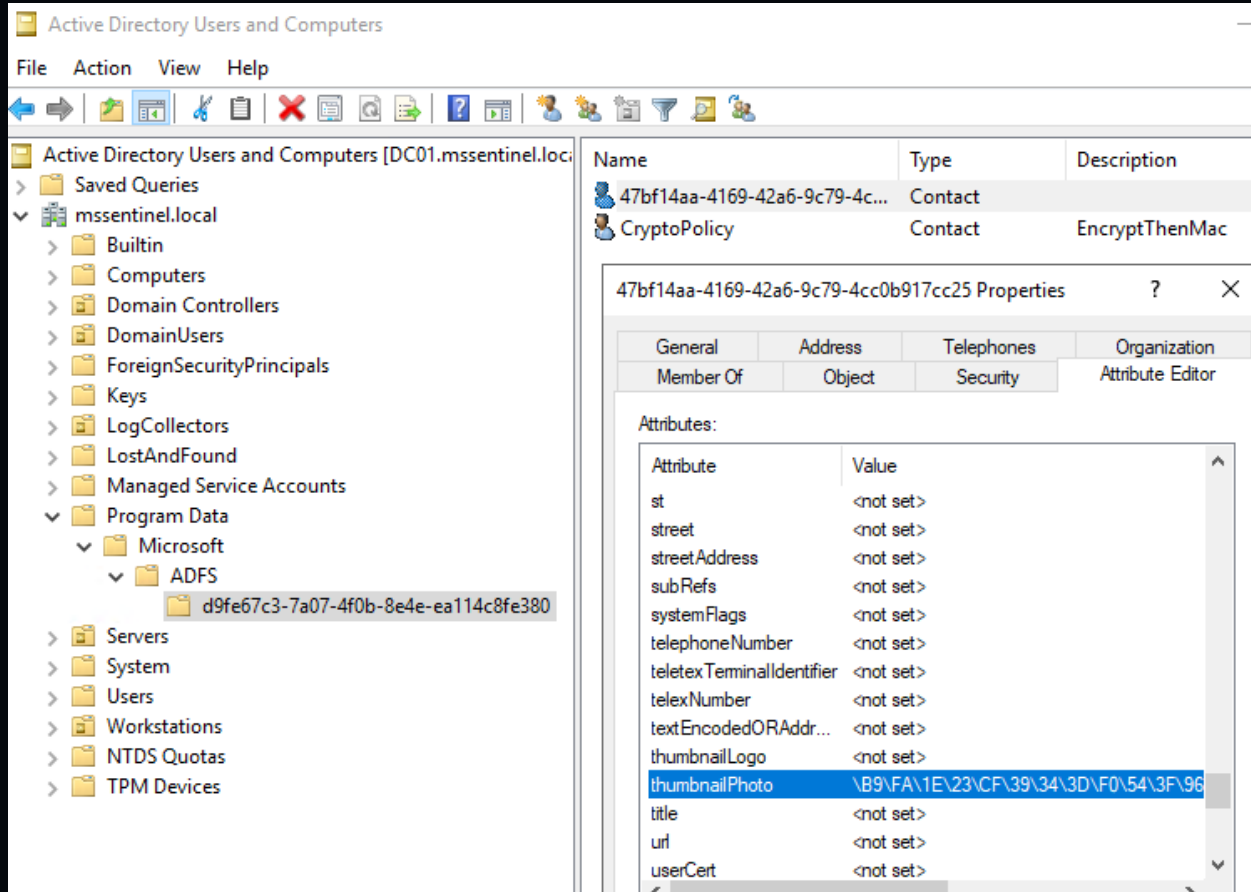
AD FS LDAP – Capture Events

- **Provider:** Microsoft-Windows-LDAP-Client
- **Steps to capture events:**
 - logman start LDAPTrace -p "Microsoft-Windows-LDAP-Client" -o LDAPTrace.etl -ets
 - logman stop LDAPTrace -ets



```
Event Properties - Event 30, LDAP-Client
General Details
Friendly View XML View
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-LDAP-Client" Guid="{099614a5-5dd7-4788-8bc9-e29f43db28fc}" />
  <EventID>30</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000001</Keywords>
  <TimeCreated SystemTime="2022-12-08T01:18:39.493244100Z" />
  <EventRecordID>4</EventRecordID>
  <Correlation ActivityID="{60623660-a993-0001-db9f-41a79f0ad901}" />
  <Execution ProcessID="6840" ThreadID="4152" ProcessorID="0" KernelTime="44" UserTime="100" />
  <Channel />
  <Computer>ADFS01.mssentinel.local</Computer>
  <Security />
</System>
- <EventData>
  <Data Name="ScopeOfSearch">0</Data>
  <Data Name="SearchFilter">(objectClass=*)</Data>
  <Data Name="DistinguishedName">CN=47bf14aa-4169-42a6-9c79-4cc0b917cc25,CN=d9fe67c3-7a07-4f0b-8e4e-ea114c8fe380,CN=ADFS,CN=Microsoft,CN=ProgramData,DC=mssentinel,DC=local</Data>
  <Data Name="AttributeList">objectClass</Data>
  <Data Name="ProcessId">0x1ab8</Data>
</EventData>
```


AD FS LDAP -> AD FS DKM Key



Active Directory Users and Computers [DC01.mssentinel.local]

File Action View Help

Active Directory Users and Computers [DC01.mssentinel.local]

- Saved Queries
- mssentinel.local
 - Builtin
 - Computers
 - Domain Controllers
 - DomainUsers
 - ForeignSecurityPrincipals
 - Keys
 - LogCollectors
 - LostAndFound
 - Managed Service Accounts
 - Program Data
 - Microsoft
 - ADFS
 - d9fe67c3-7a07-4f0b-8e4e-ea114c8fe380
 - Servers
 - System
 - Users
 - Workstations
 - NTDS Quotas
 - TPM Devices

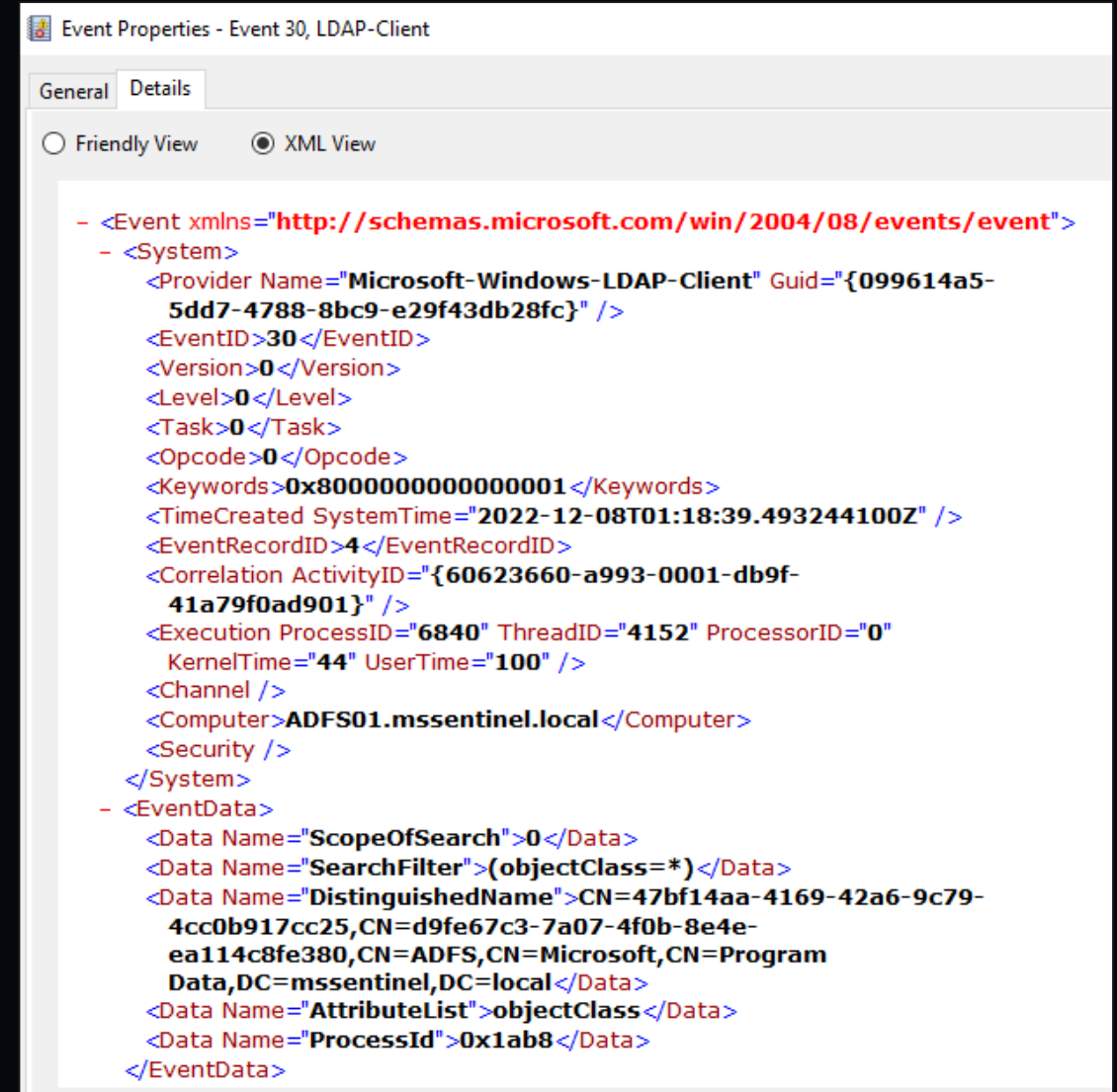
Name	Type	Description
47bf14aa-4169-42a6-9c79-4c...	Contact	
CryptoPolicy	Contact	EncryptThenMac

47bf14aa-4169-42a6-9c79-4cc0b917cc25 Properties ? X

General	Address	Telephones	Organization
Member Of	Object	Security	Attribute Editor

Attributes:

Attribute	Value
st	<not set>
street	<not set>
streetAddress	<not set>
subRefs	<not set>
systemFlags	<not set>
telephoneNumber	<not set>
teletexTerminalIdentifier	<not set>
telexNumber	<not set>
textEncodedORAddr...	<not set>
thumbnailLogo	<not set>
thumbnailPhoto	\B9\FA\1E\23\CF\39\34\3D\F0\54\3F\96
title	<not set>
url	<not set>
userCert	<not set>



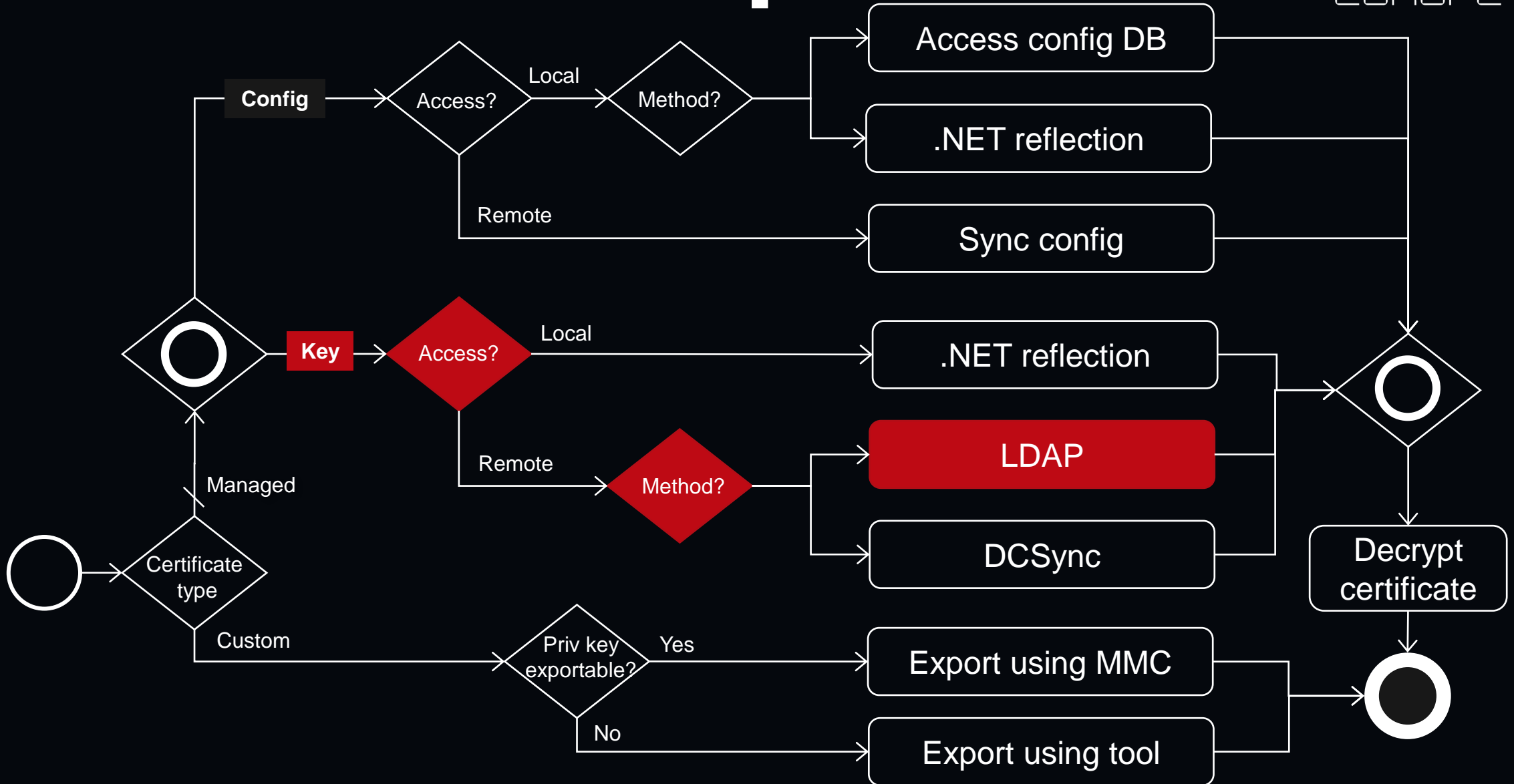
Event Properties - Event 30, LDAP-Client

General Details

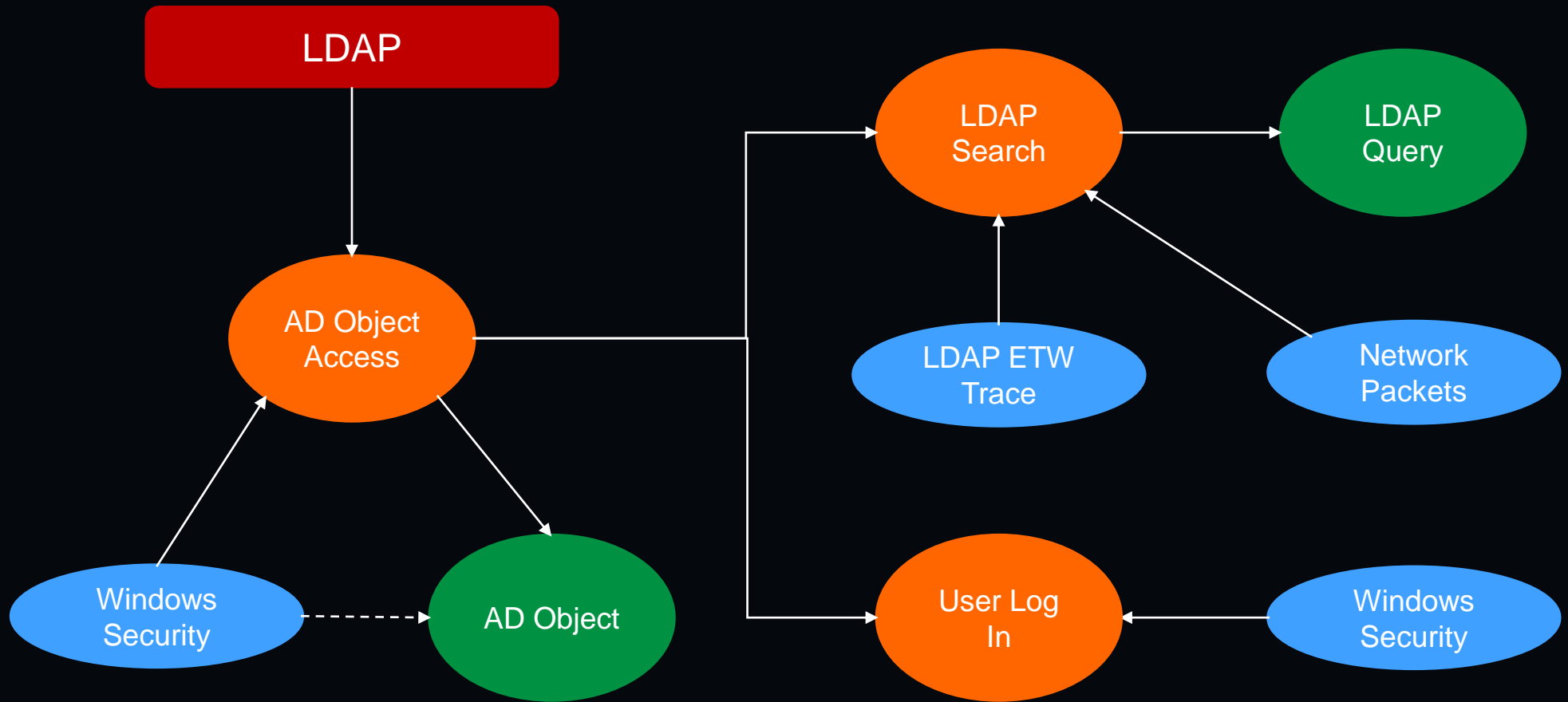
Friendly View XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-LDAP-Client" Guid="{099614a5-5dd7-4788-8bc9-e29f43db28fc}" />
  <EventID>30</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8000000000000001</Keywords>
  <TimeCreated SystemTime="2022-12-08T01:18:39.493244100Z" />
  <EventRecordID>4</EventRecordID>
  <Correlation ActivityID="{60623660-a993-0001-db9f-41a79f0ad901}" />
  <Execution ProcessID="6840" ThreadID="4152" ProcessorID="0" KernelTime="44" UserTime="100" />
  <Channel />
  <Computer>ADFS01.mssentinel.local</Computer>
  <Security />
</System>
- <EventData>
  <Data Name="ScopeOfSearch">0</Data>
  <Data Name="SearchFilter">(objectClass=*)</Data>
  <Data Name="DistinguishedName">CN=47bf14aa-4169-42a6-9c79-4cc0b917cc25,CN=d9fe67c3-7a07-4f0b-8e4e-ea114c8fe380,CN=ADFS,CN=Microsoft,CN=Program Data,DC=mssentinel,DC=local</Data>
  <Data Name="AttributeList">objectClass</Data>
  <Data Name="ProcessId">0x1ab8</Data>
</EventData>
```

AD FS Attack Graph



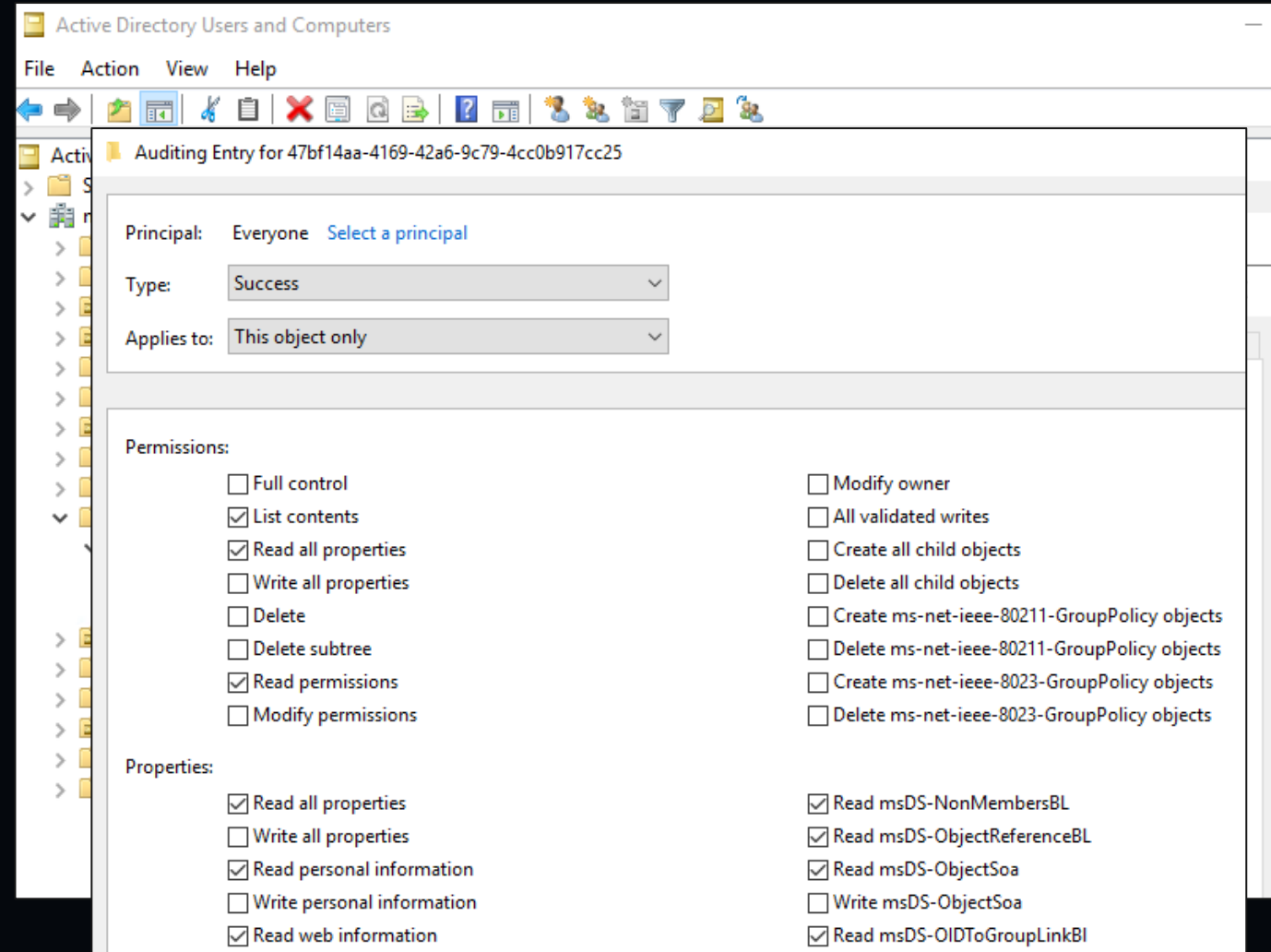
AD FS Defence Graph



AD FS Distributed Key Manager (DKM) container in AD DC

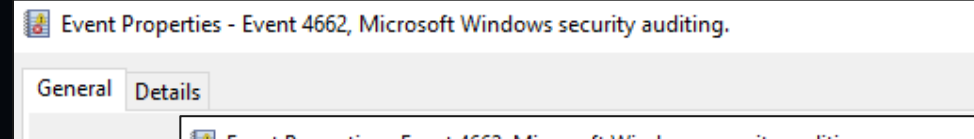
- **Notes:**

- Add an entry on the system access control list (SACL) of the AD object.
- Audit attempts to access the securable object
- AD FS service account use blends in with normal activity.



AD DC – AD FS DKM Key Access

- **Log Name:** Security
- **Event:** 4662
- **Entities:** User, Host, AD Object
- **Notes:**
 - XML representation shows a GUID for the AD Object
 - Property accessed: **8d3bca50-1d7e-11d0-a081-00aa006c33ed**
 - Join 4662 and 4624 on Logon ID



2.364 Attribute thumbnailPhoto

Article • 02/14/2019 • 2 minutes to read

Picture

```
cn: Picture
ldapDisplayName: thumbnailPhoto
attributeId: 2.16.840.1.113730.3.1.35
attributeSyntax: 2.5.5.10
omSyntax: 4
isSingleValued: TRUE
schemaIdGuid: 8d3bca50-1d7e-11d0-a081-00aa006c33ed
systemOnly: FALSE
searchFlags: 0
rangeLower: 0
rangeUpper: 102400
attributeSecurityGuid: 77b5b886-944a-11d1-aebd-0000f80367c1
```

```
User: </EventData>
</Event>
```

Logon + AD FS DKM Key Access

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level: Impersonation

New Logon:

Security ID:	MSENTINEL\adfsadmin2
Account Name:	adfsadmin2
Account Domain:	MSENTINEL.LOCAL
Logon ID:	0x8150BA
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{bece78a7-87b1-f773-8189-f6423fc10691}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	-
Source Network Address:	192.168.2.5
Source Port:	51088

Log Name: Security
Source: Microsoft Windows security Logged: 12/7/2022 9:12:25 PM
Event ID: 4624 Task Category: Logon

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

Security ID:	MSENTINEL\adfsadmin2
Account Name:	adfsadmin2
Account Domain:	MSENTINEL
Logon ID:	0x8150BA

Object:

Object Server:	DS
Object Type:	contact
Object Name:	CN=47bf14aa-4169-42a6-9c79-4cc0b917cc25,CN=d9fe67c3-7a07-4f0b-8e4e-ea114c8fe380,CN=ADFS,CN=Microsoft,CN=Program Data,DC=mssentinel,DC=local
Handle ID:	0x0

Operation:

Operation Type:	Object Access
Accesses:	Read Property
Access Mask:	0x10
Properties:	Read Property {77b5b886-944a-11d1-aebd-0000f80367c1} {8d3bca50-1d7e-11d0-a081-00aa006c33ed} {5cb41ed0-0e4c-11d0-a286-00aa003049e2}

Log Name: Security
Source: Microsoft Windows security Logged: 12/7/2022 9:12:25 PM
Event ID: 4662 Task Category: Directory Service Access

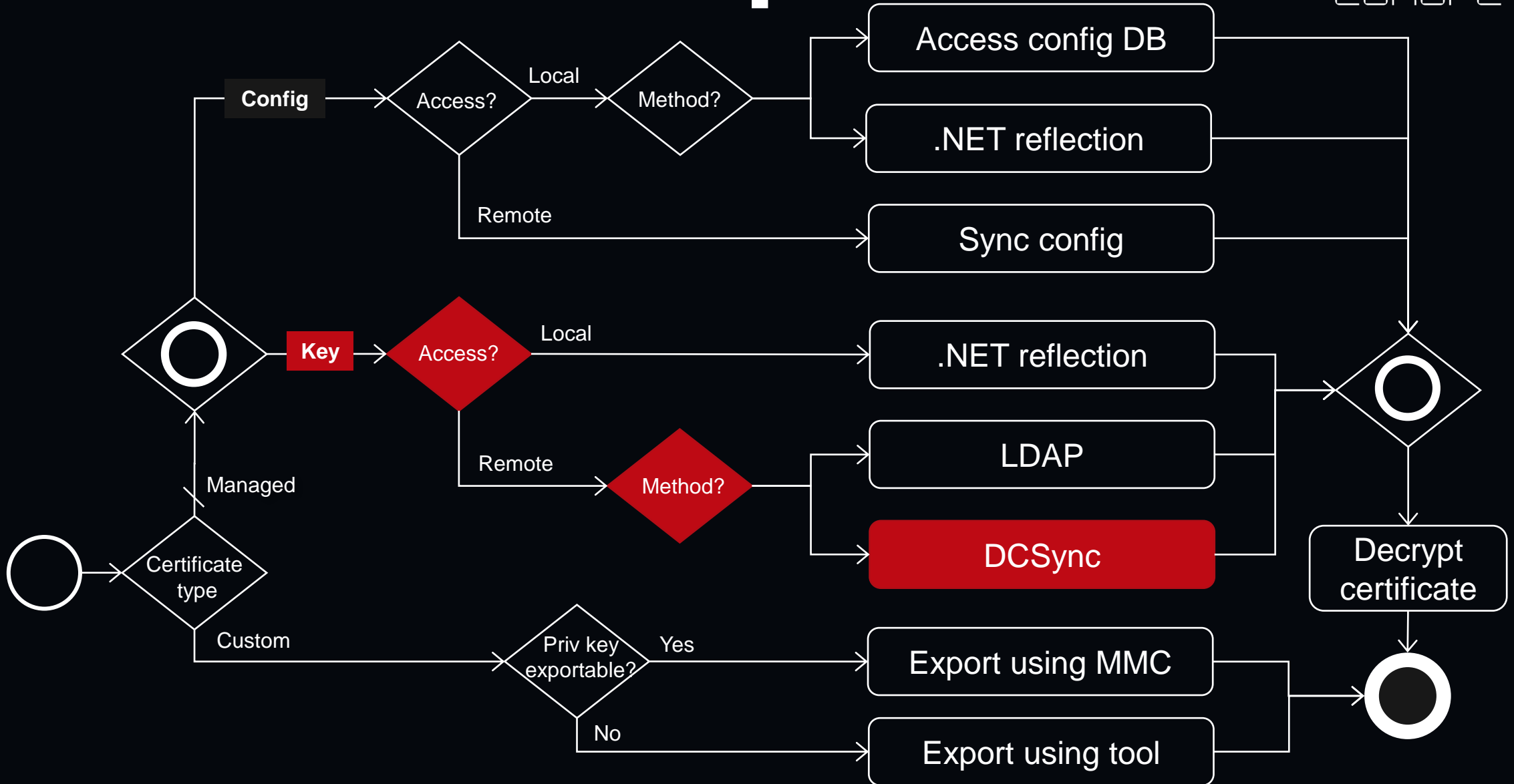
AD FS LDAP – Capture Events

- **Provider:** Microsoft-Windows-LDAP-Client
- **Steps to capture events:**
 - logman start LDAPTrace -p "Microsoft-Windows-LDAP-Client" -o LDAPTrace.etl -ets
 - logman stop LDAPTrace -ets

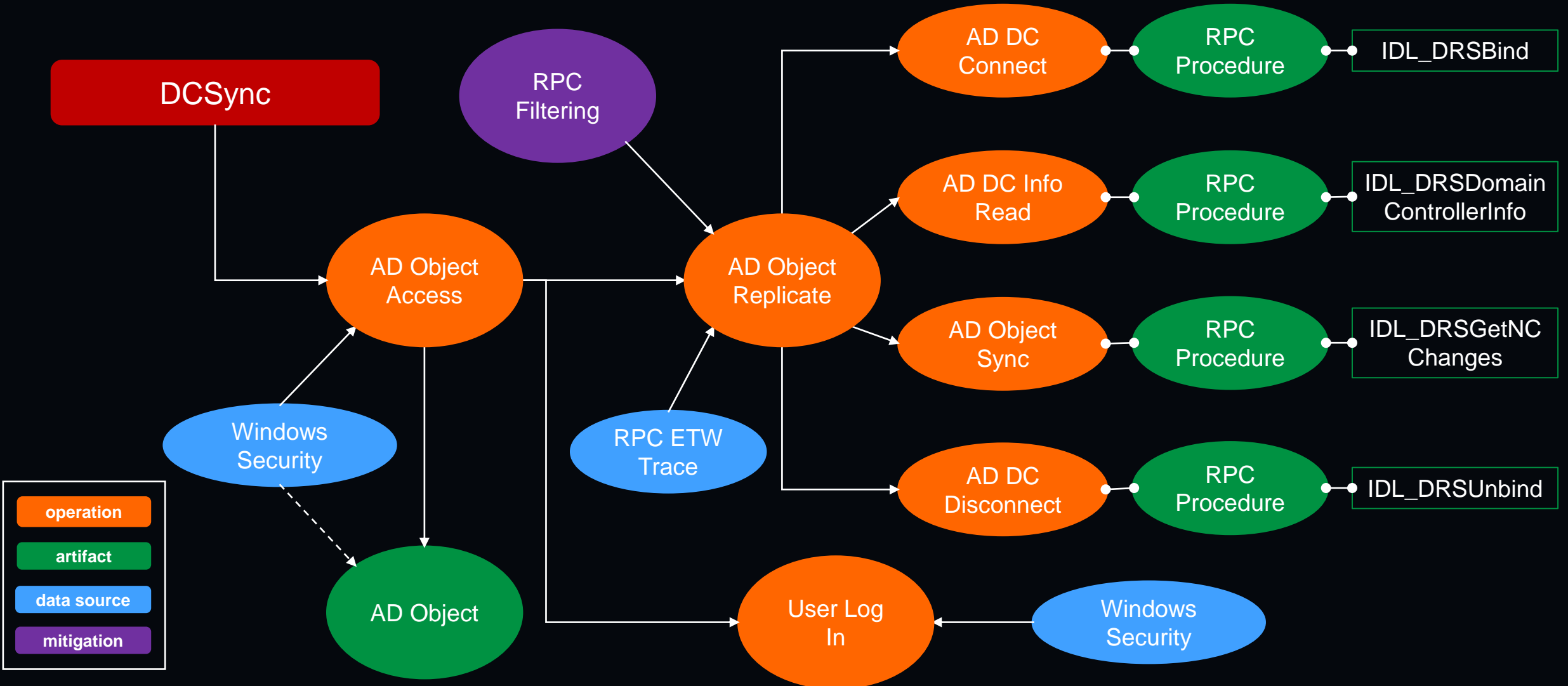
```
- <EventData>
  <Data Name="ScopeOfSearch">0</Data>
  <Data Name="SearchFilter">(objectClass=*)</Data>
  <Data Name="DistinguishedName">CN=d9fe67c3-7a07-4f0b-8e4e-
    ea114c8fe380,CN=ADFS,CN=Microsoft,CN=Program
    Data,DC=mssentinel,DC=local</Data>
  <Data Name="AttributeList">objectClass</Data>
  <Data Name="ProcessId">0x1ab8</Data>
</EventData>
</Event>
```

```
- <EventData>
  <Data Name="ScopeOfSearch">0</Data>
  <Data Name="SearchFilter">(objectClass=*)</Data>
  <Data Name="DistinguishedName">CN=d9fe67c3-7a07-4f0b-8e4e-
    ea114c8fe380,CN=ADFS,CN=Microsoft,CN=Program
    Data,DC=mssentinel,DC=local</Data>
  <Data Name="AttributeList">objectClass</Data>
  <Data Name="ProcessId">0x1ab8</Data>
</EventData>
</Event>
```

AD FS Attack Graph

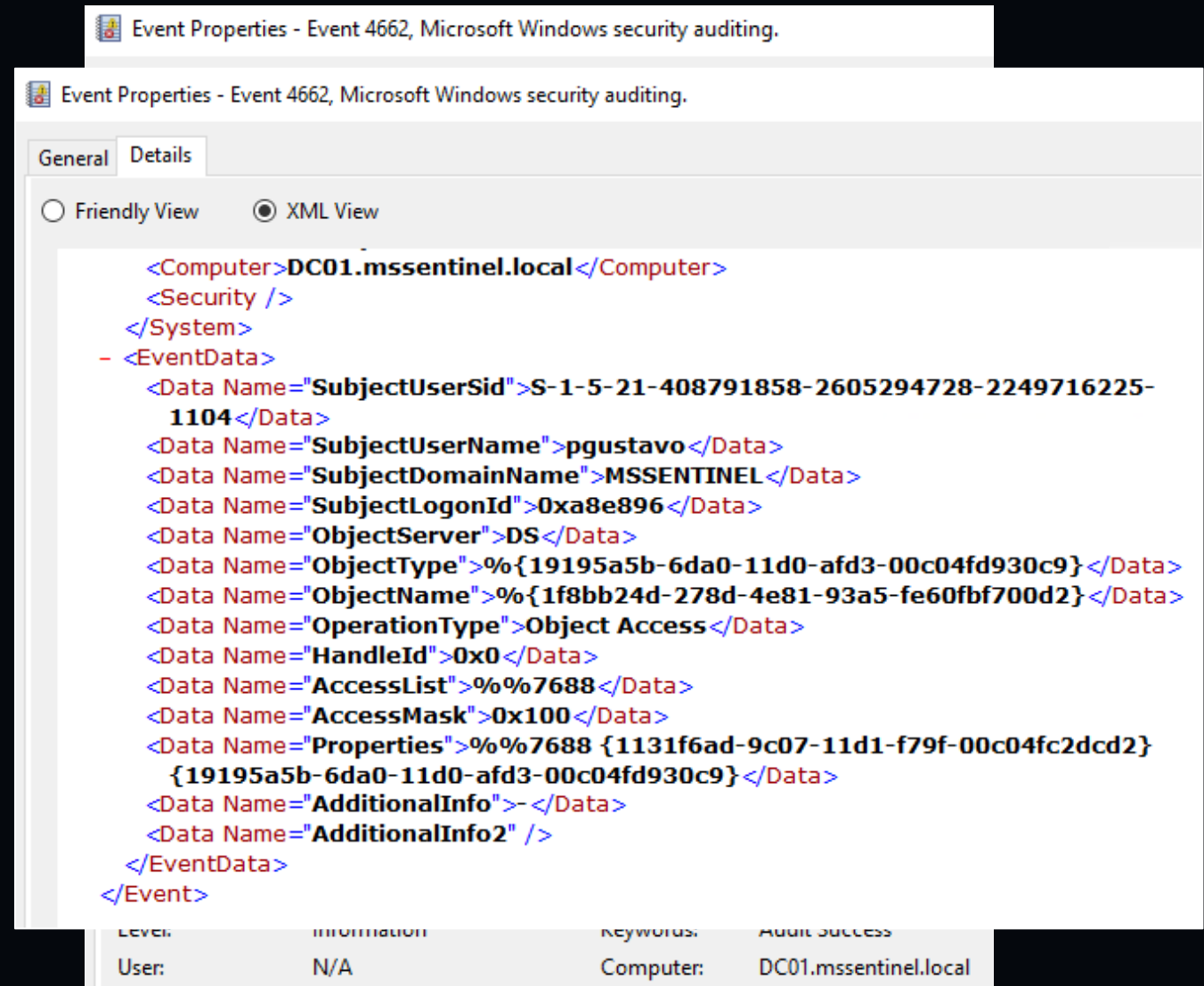


AD FS Defence Graph



AD DC Access via MS-DRSR

- **Log Name:** Security
- **Event:** 4662
- **Entities:** Host, User
- **Notes:**
 - SACL does NOT work here
 - Access to the Domain-DNS Class object
 - Extended Right: **1131f6ad-9c07-11d1-f79f-00c04fc2dcd2**



```
<Computer>DC01.mssentinel.local</Computer>
<Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-5-21-408791858-2605294728-2249716225-1104</Data>
  <Data Name="SubjectUserName">pgustavo</Data>
  <Data Name="SubjectDomainName">MSENTINEL</Data>
  <Data Name="SubjectLogonId">0xa8e896</Data>
  <Data Name="ObjectServer">DS</Data>
  <Data Name="ObjectType">%{19195a5b-6da0-11d0-afd3-00c04fd930c9}</Data>
  <Data Name="ObjectName">%{1f8bb24d-278d-4e81-93a5-fe60fbf700d2}</Data>
  <Data Name="OperationType">Object Access</Data>
  <Data Name="HandleId">0x0</Data>
  <Data Name="AccessList">%%7688</Data>
  <Data Name="AccessMask">0x100</Data>
  <Data Name="Properties">%%7688 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}{19195a5b-6da0-11d0-afd3-00c04fd930c9}</Data>
  <Data Name="AdditionalInfo">-</Data>
  <Data Name="AdditionalInfo2" />
</EventData>
</Event>
```

Level:	Information	Keywords:	Admin Success
User:	N/A	Computer:	DC01.mssentinel.local

Logon + AD DC - MS-DRSR

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level: Impersonation

New Logon:

Security ID:	MSENTINEL\pgustavo
Account Name:	pgustavo
Account Domain:	MSENTINEL.LOCAL
Logon ID:	0xA8E896

Linked Logon ID: 0x0

Network Account Name: -

Network Account Domain: -

Logon GUID: {6a49269b-8590-30ae-0ade-d45b6f09e193}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	-
Source Network Address:	192.168.2.5
Source Port:	52166

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Logged: 12/7/2022 10:18:00 PM

Task Category: Logon

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

Security ID:	MSENTINEL\pgustavo
Account Name:	pgustavo
Account Domain:	MSENTINEL
Logon ID:	0xA8E896

Object:

Object Server:	DS
Object Type:	domainDNS
Object Name:	DC=mssentinel,DC=local
Handle ID:	0x0

Operation:

Operation Type:	Object Access
Accesses:	Control Access
Access Mask:	0x100
Properties:	Control Access {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}

Log Name: Security

Source: Microsoft Windows security

Event ID: 4662

Logged: 12/7/2022 10:18:00 PM

Task Category: Directory Service Access

Level: Information

Keywords: Audit Success

User: N/A

Computer: DC01.mssentinel.local

Mitigation – RPC Filtering



Zero Networks – RPC Firewall Project

```
uuid:e3514235-4b06-11d1-ab04-00c04fc2dcd2 addr:<dc_addr1> action:allow
uuid:e3514235-4b06-11d1-ab04-00c04fc2dcd2 addr:<dc_addr2> action:allow
uuid:e3514235-4b06-11d1-ab04-00c04fc2dcd2 action:block audit:true action:allow
audit:false
```

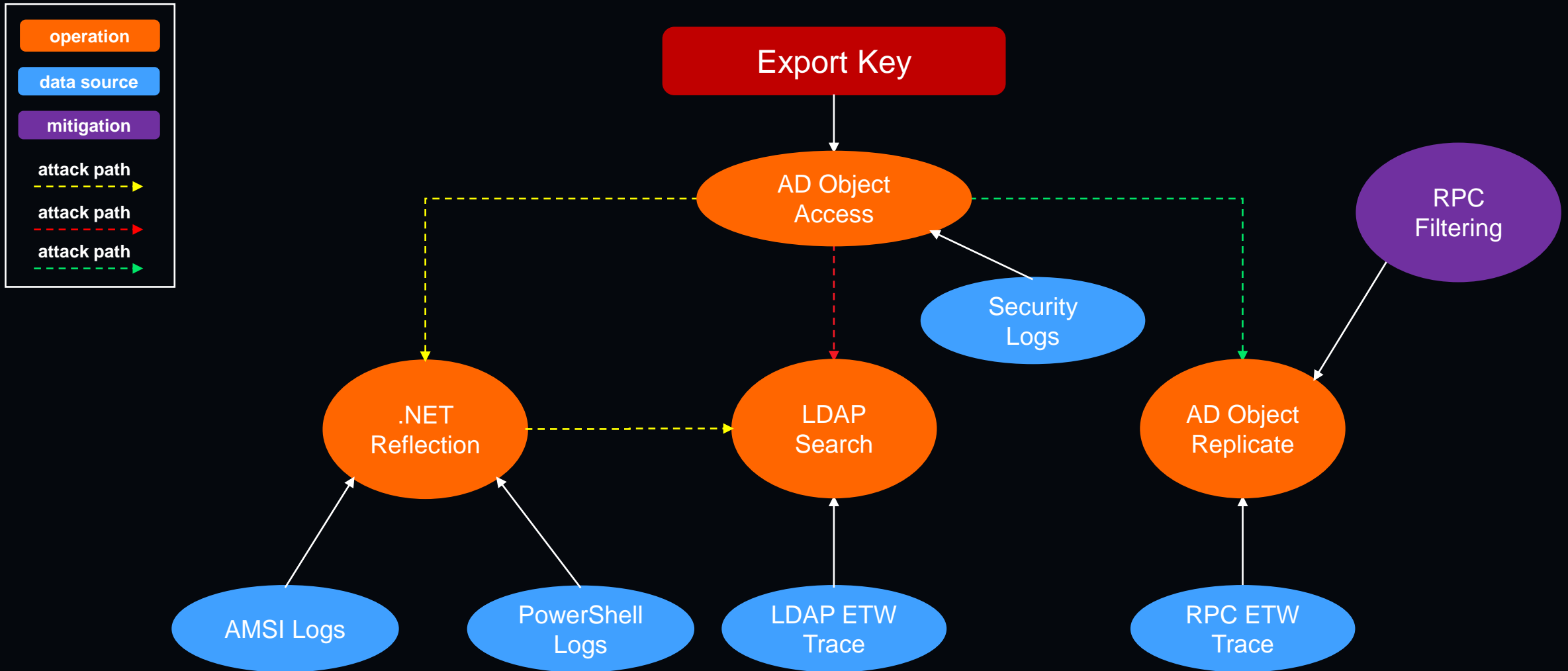
<https://zeronetworks.com/blog/stopping-lateral-movement-via-the-rpc-firewall/>

MSRPC-to-ATTACK Project (@jsecurity101) – Research Lab Only

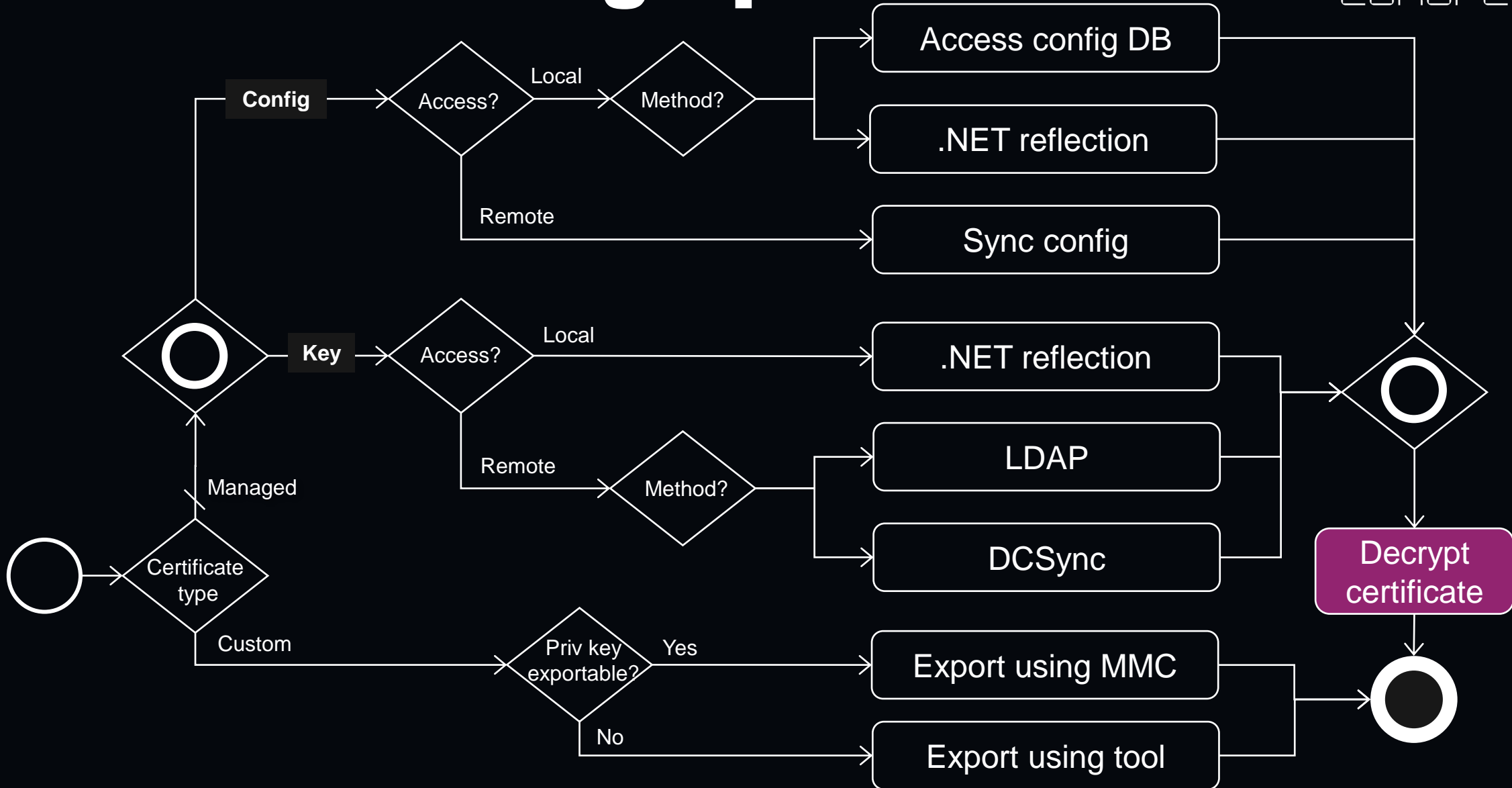
```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uid matchtype=equal data=e3514235-4b06-11d1-ab04-00c04fc2dcd2
add condition field=remote_user_token matchtype=equal data=D:(A;;CC;;;DD)
add filter
add rule layer=um actiontype=block
add condition field=if_uid matchtype=equal data=e3514235-4b06-11d1-ab04-00c04fc2dcd2
add filter
quit
```

<https://github.com/jsecurity101/MSRPC-to-ATTACK/blob/main/documents/MS-DRSR.md>

AD FS Attack - Defence Graph



AD FS attack graph

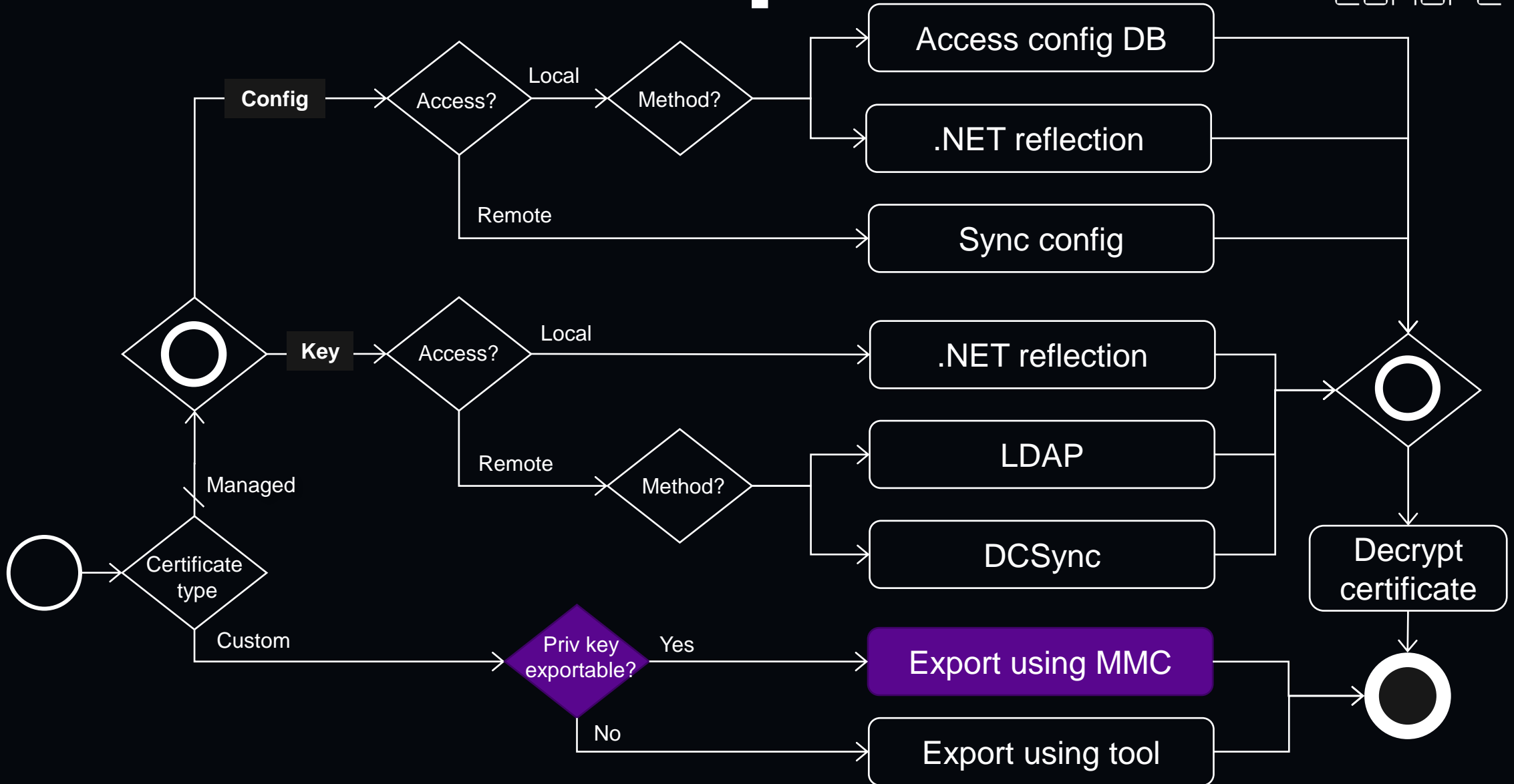


AD FS Defence Graph

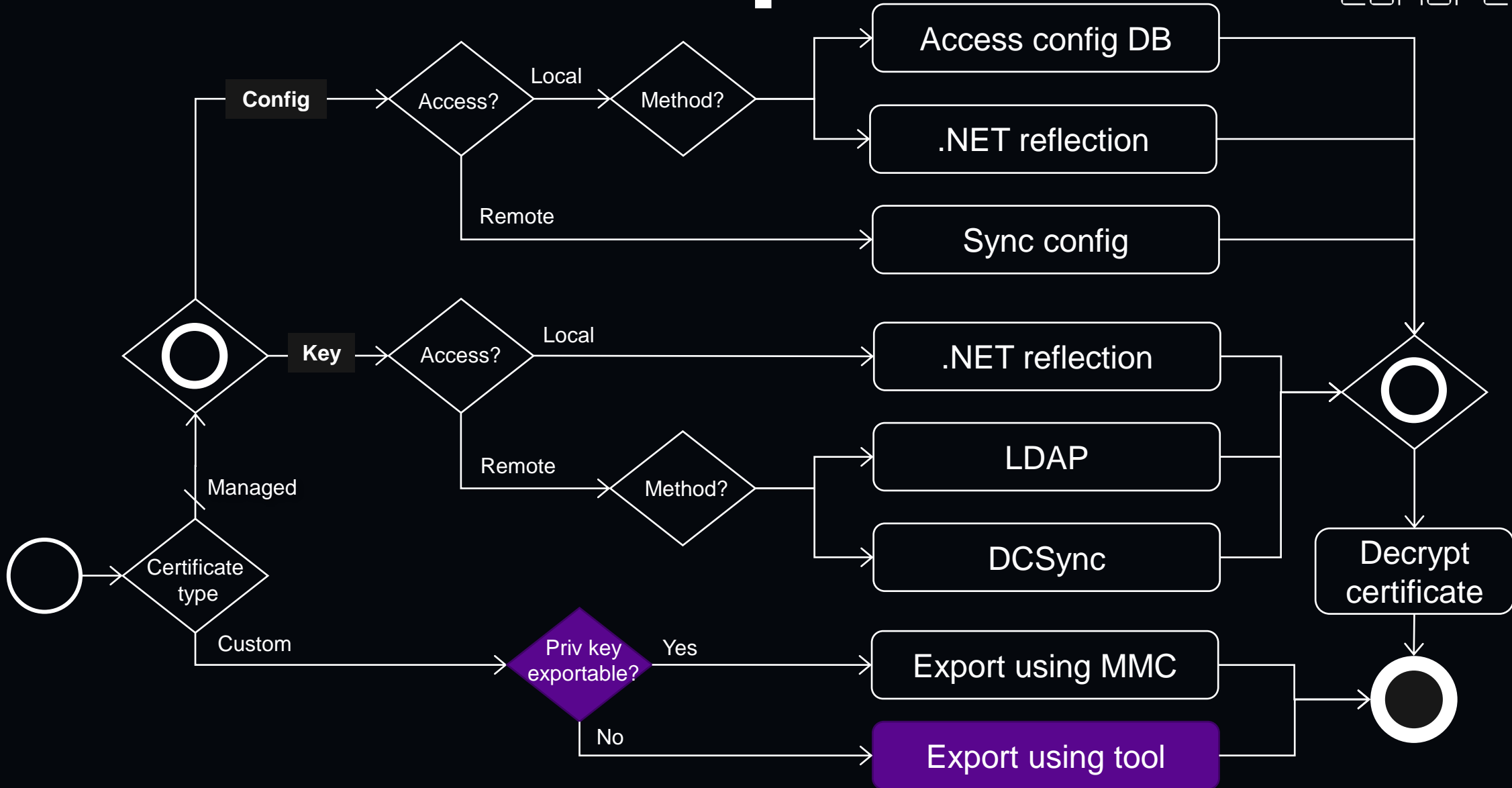


This page is intentionally left blank

AD FS Attack Graph



AD FS Attack Graph

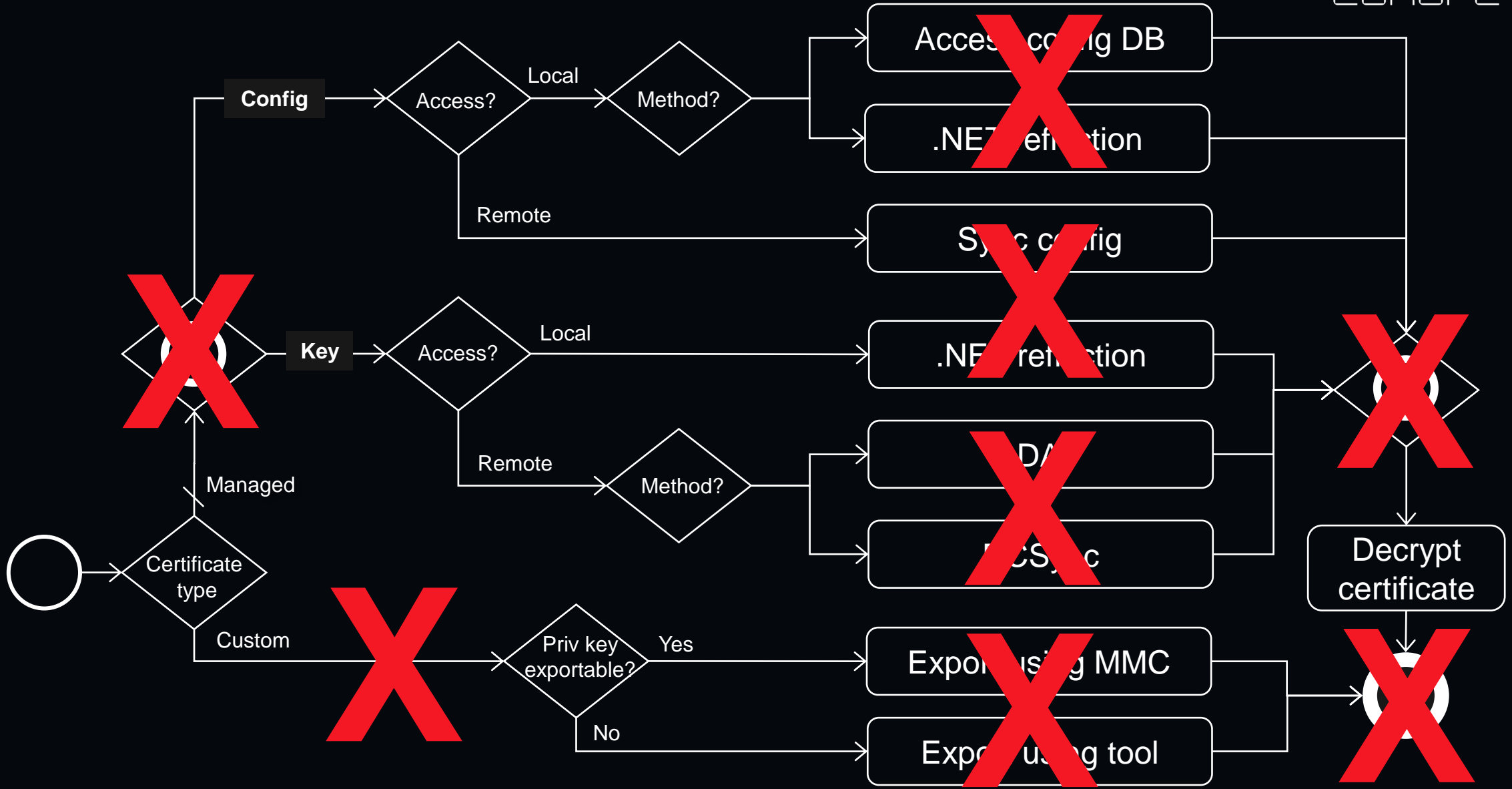


Defence Notes

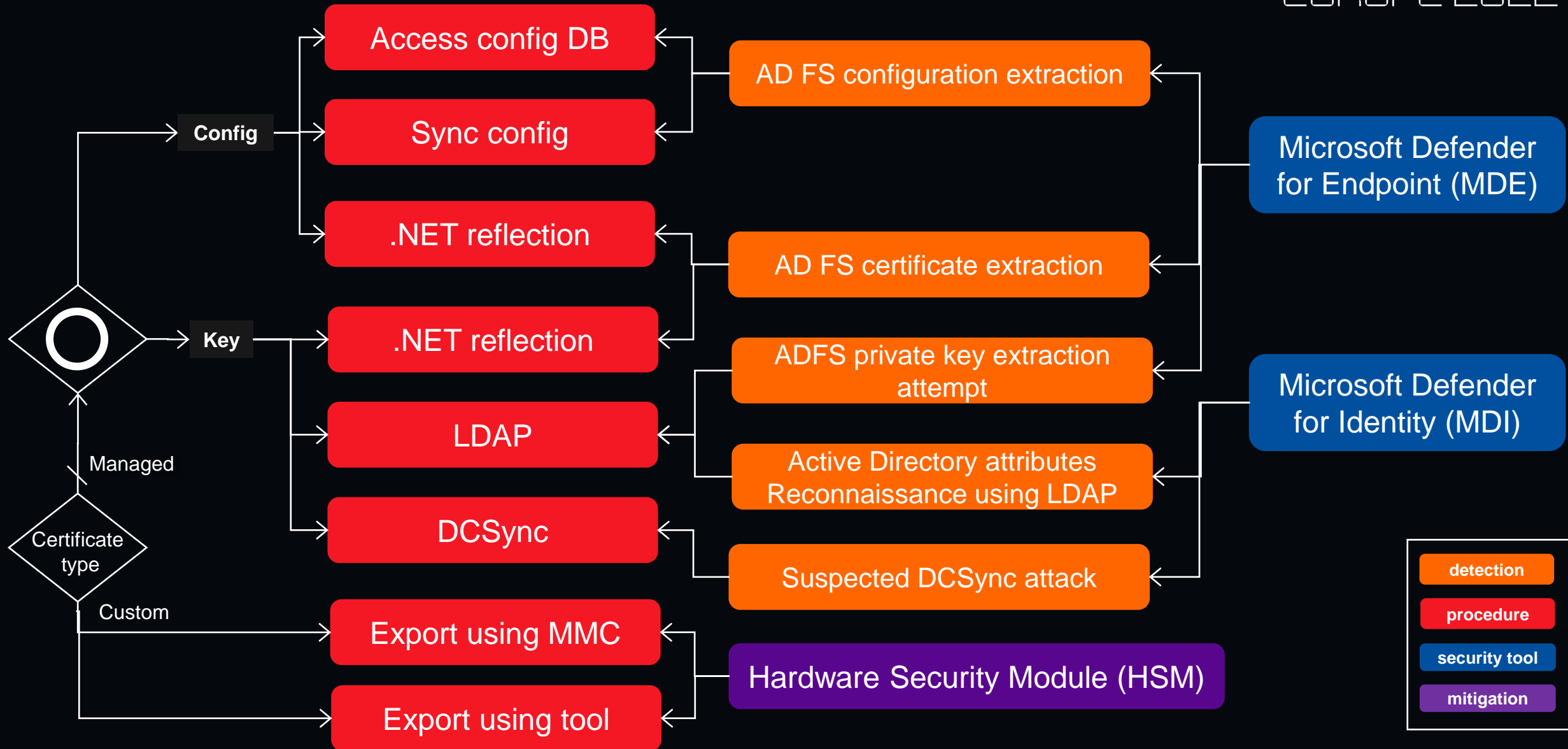
- SACL on AD FS Certificate is too noisy
- Auditing DPAPI APIs is too noisy
- Ensure the installed certificates are protected against theft (don't store these on a share on the network) and set a calendar reminder to ensure they get renewed before expiring (expired certificate breaks federation auth).
- Additionally, we recommend protecting signing keys/certificates in a **hardware security module (HSM)** attached to AD FS.

<https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs>

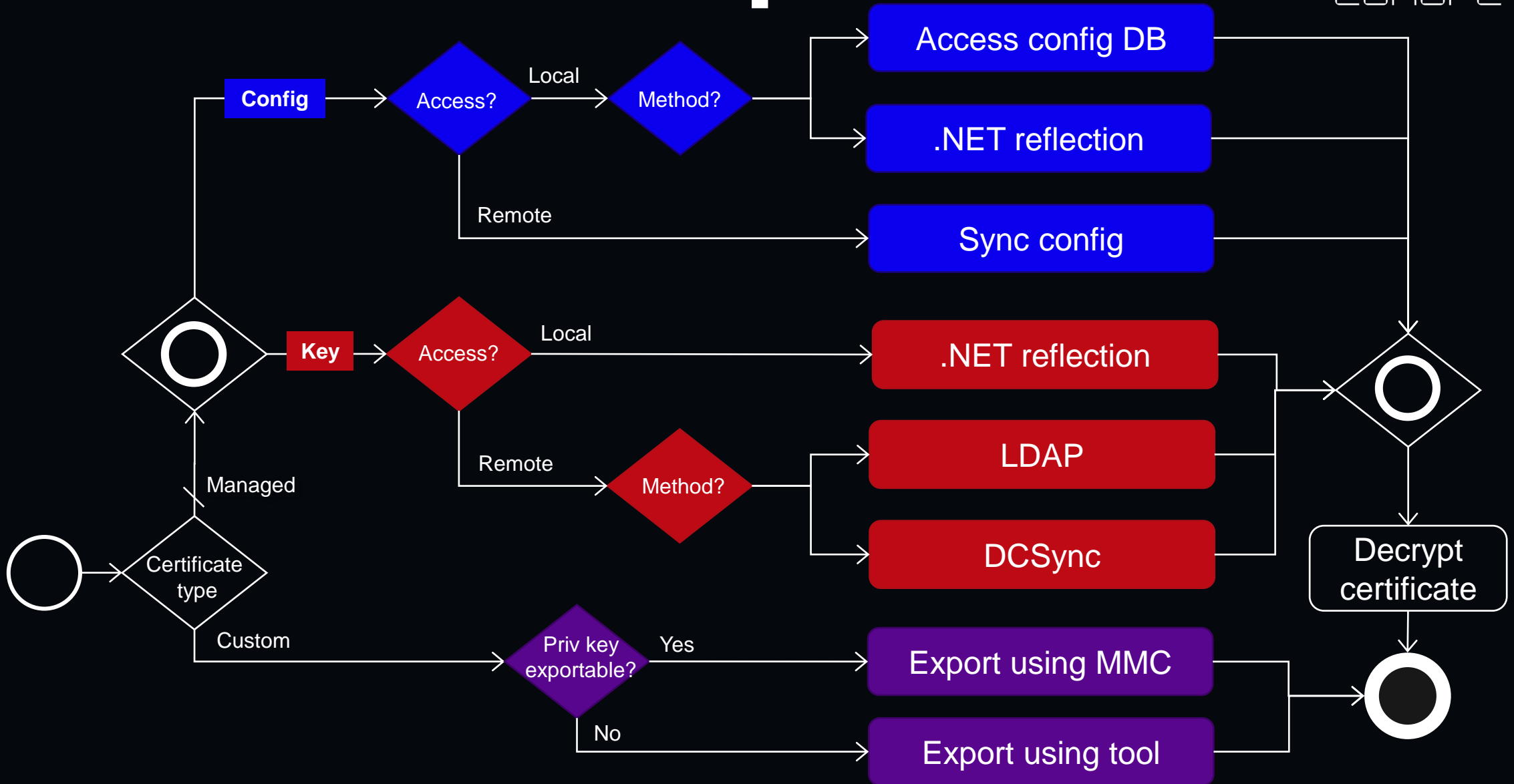
Reduce AD FS Attack Surface



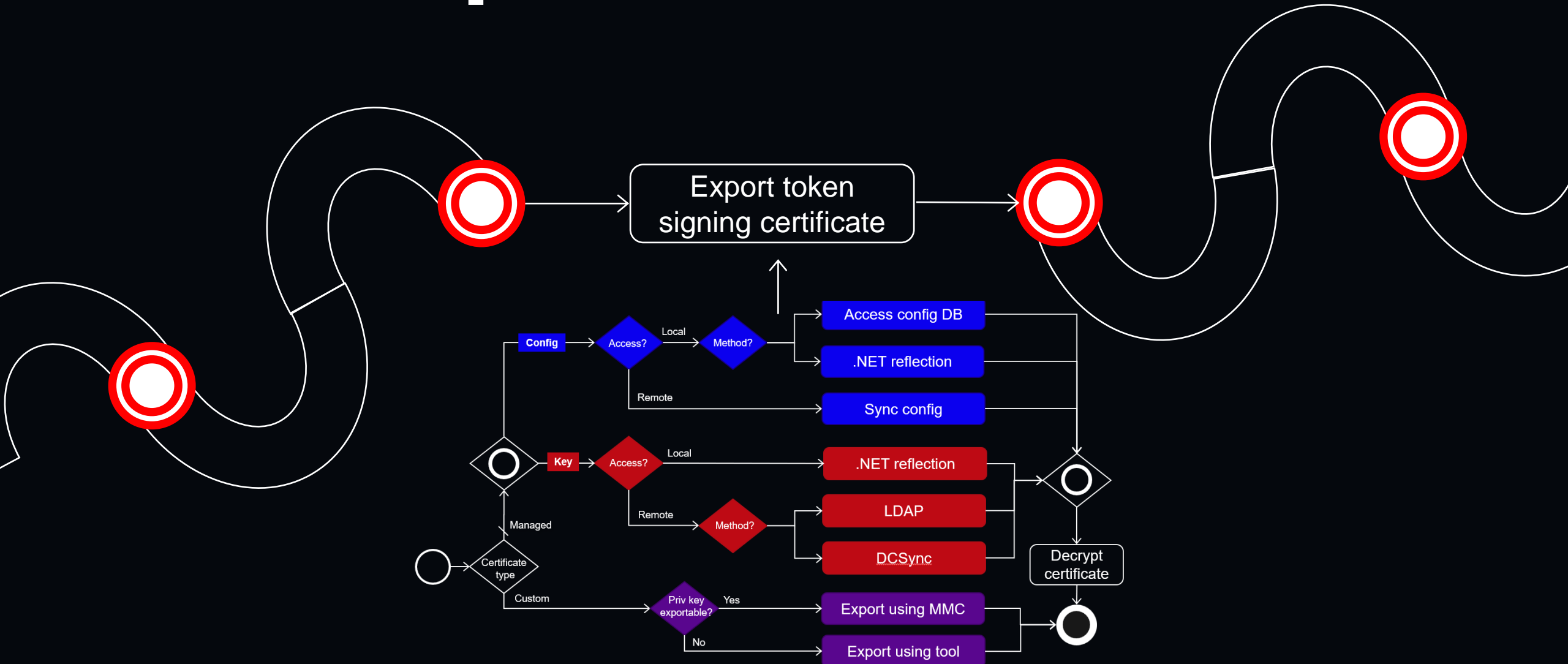
Additional Defence Notes



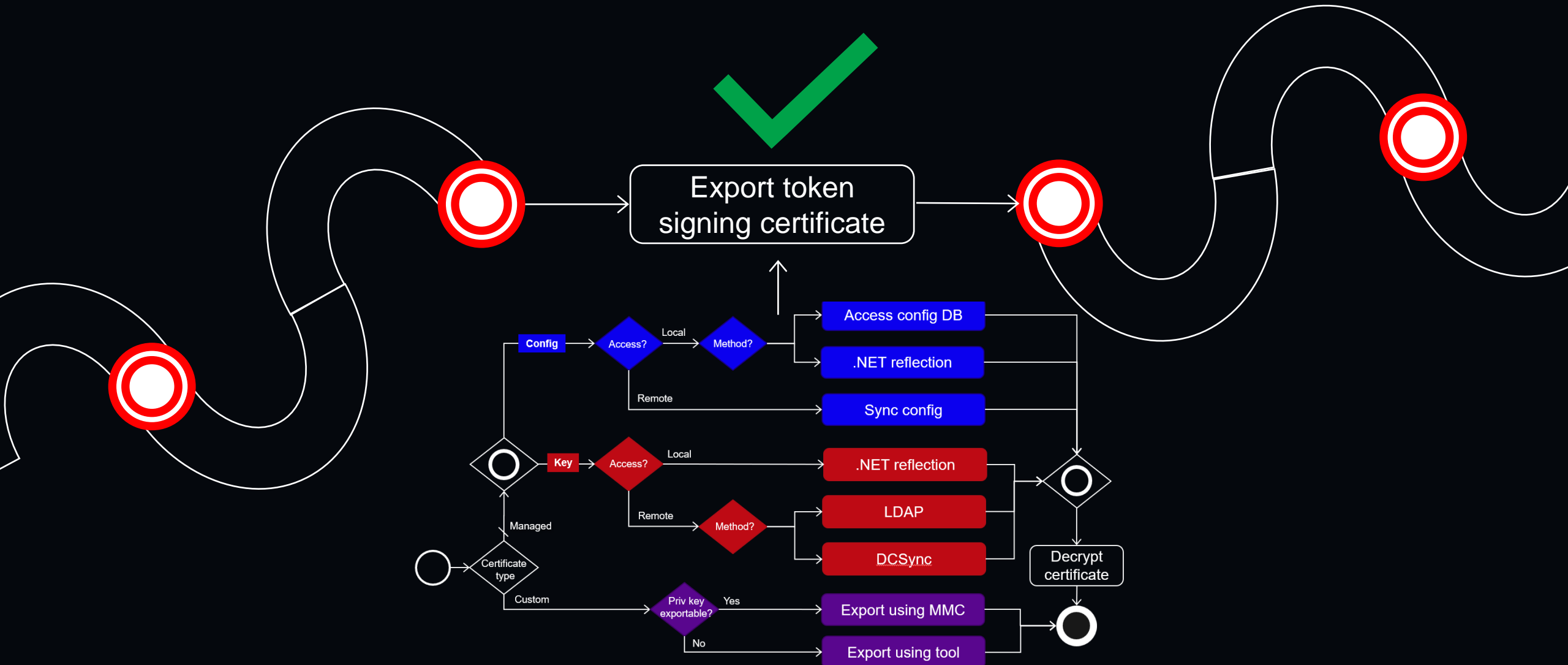
AD FS Attack Graph



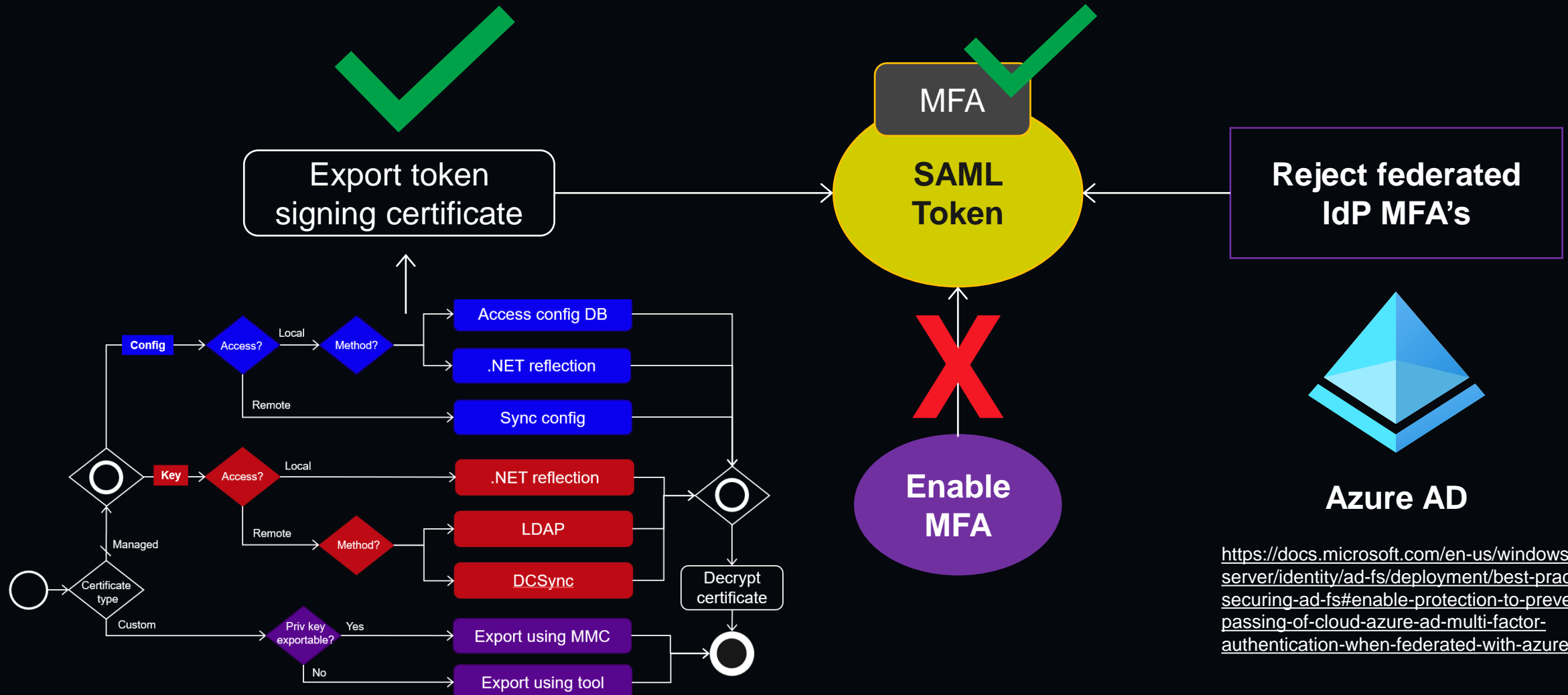
One step in the attack sequence!



Even when they succeed ...



Even when they succeed ...



<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs#enable-protection-to-prevent-by-passing-of-cloud-azure-ad-multi-factor-authentication-when-federated-with-azure-ad>

Protecting against GoldenSAML



1. Treat all AD FS servers as Tier-0!
2. Configure Azure AD to reject federated IdP MFA's¹
3. AD FS managed certificates:
 - Block port 80 (http) from all except AD FS servers & proxies
 - Treat also SQL server as Tier-0!
4. Custom certificates:
 - Block port 80 (http) from all except AD FS proxies
 - Use HSM

1. <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs#enable-protection-to-prevent-by-passing-of-cloud-azure-ad-multi-factor-authentication-when-federated-with-azure-ad>

Takeaways



- Slides and other resources
 - <https://aka.ms/BHEU2022-ADFS>
- Tools
 - [AADInternals](#)
 - [ADFSDump](#) ([ADFSpooF](#))
 - Mimikatz

Thank you!