
SwissMicrosoft
SECURITY SUMMIT


scopewyse
we are what's next


Ontinue


INGRAM
MICRO


EPIC FUSION
BRING IT ALL TOGETHER


Microsoft


water
IT Security & Defense


GRABX


Swiss Post
Cybersecurity


techtask


iC CONSULT


Mediawerk

Active Directory
Under Attack

Michael Grafnetter

@MGrafnetter

www.dsinternals.com

Microsoft MVP Most Valuable Professional

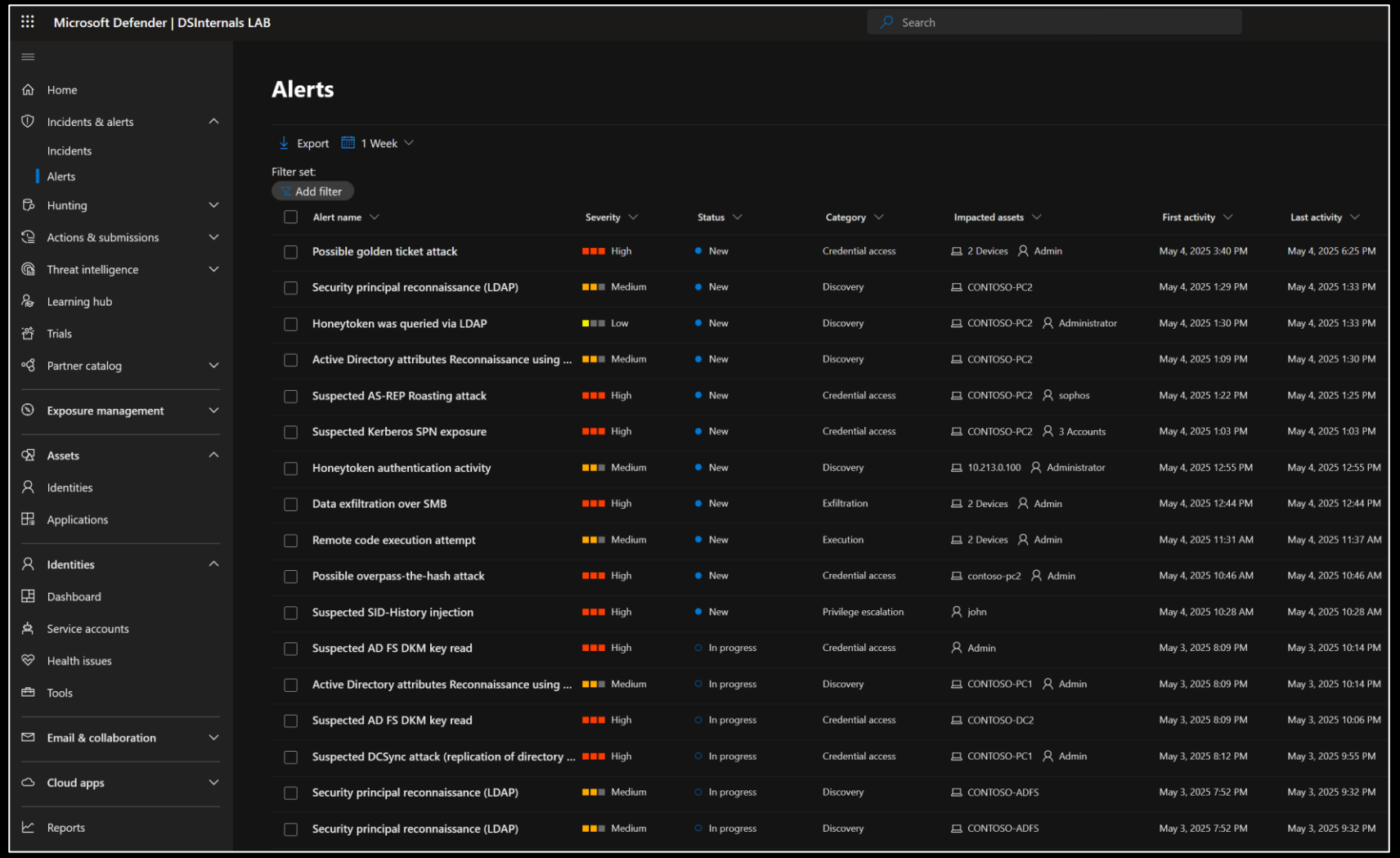
SwissMicrosoft SECURITY SUMMIT

COURE

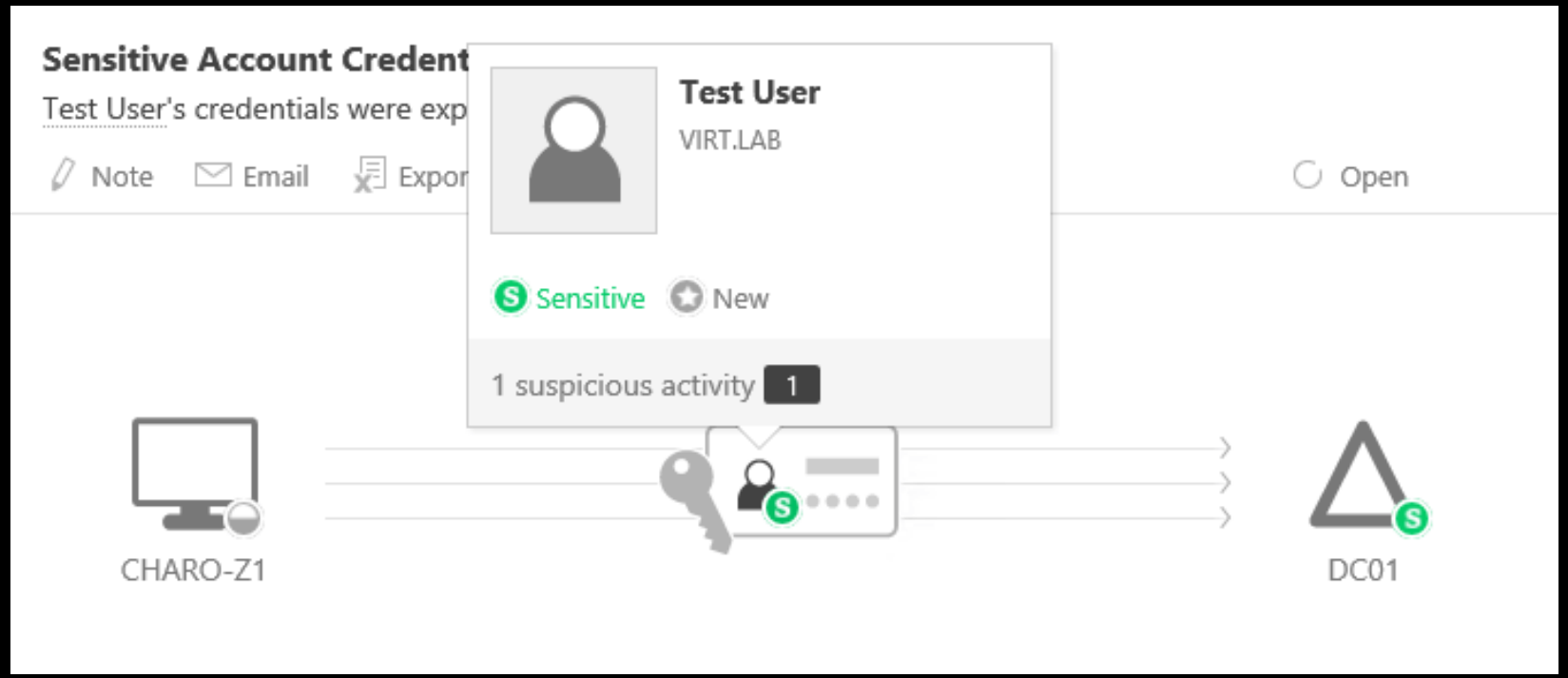
Agenda

- Intro to Microsoft Defender for Identity
- Cyber Kill Chain
  - Reconnaissance & Discovery
  - Credential Access
  - Privilege Escalation
  - Lateral Movement
  - Persistence & Data Exfiltration

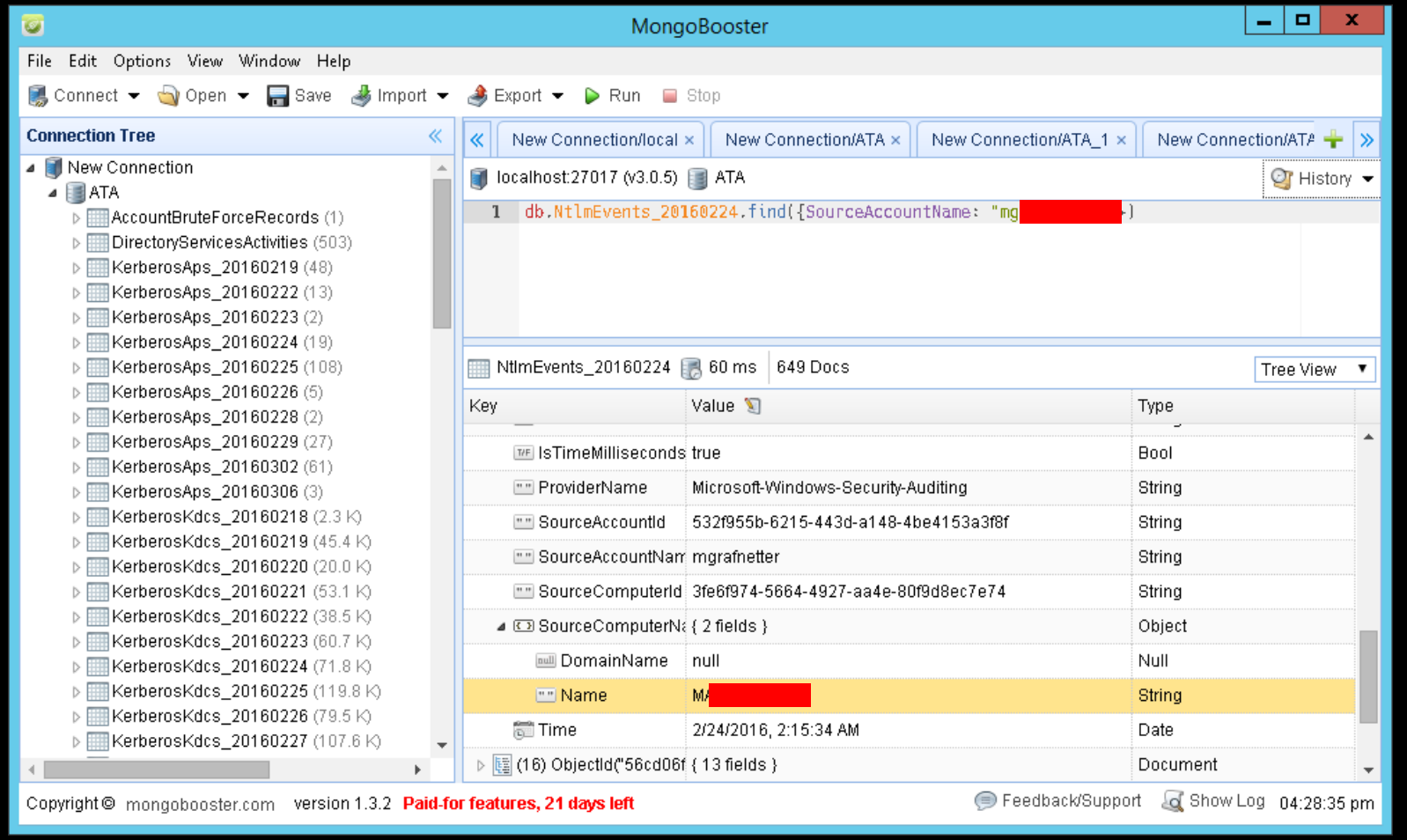
Microsoft Defender for Identity (MDI)



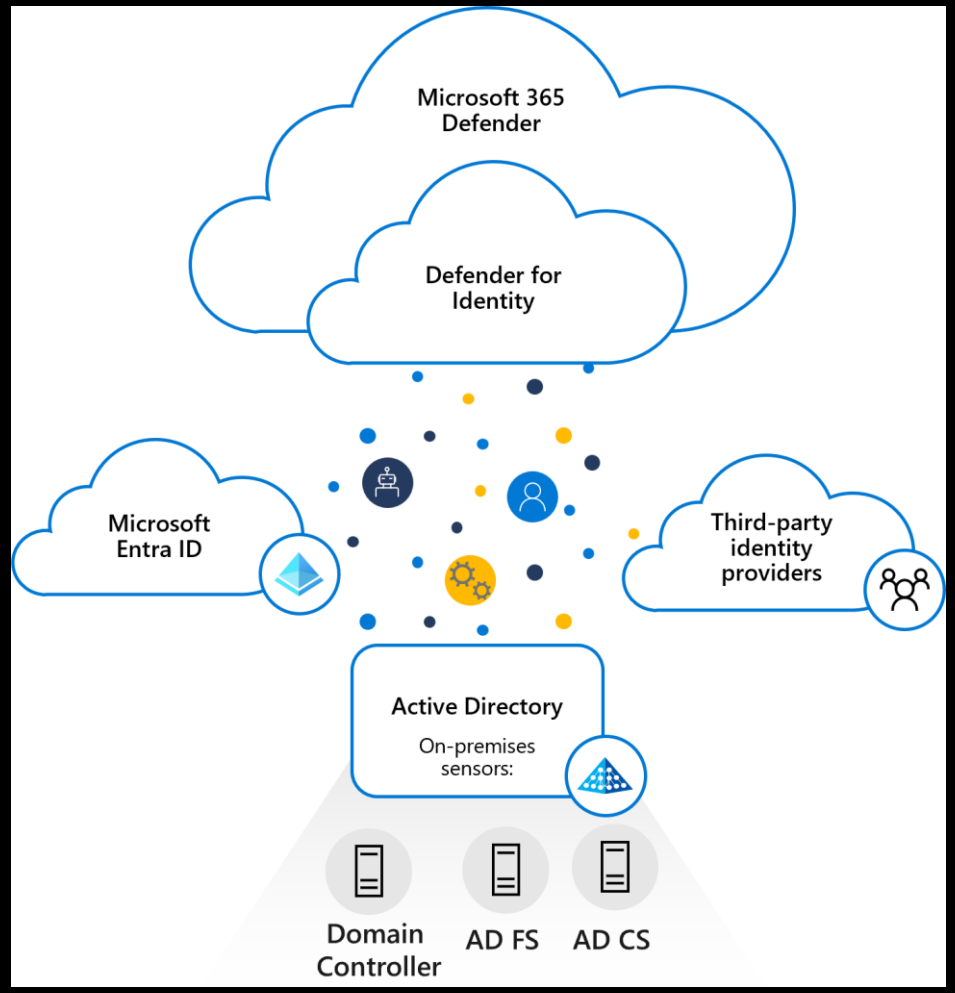
Microsoft Advanced Threat Analytics (ATA)



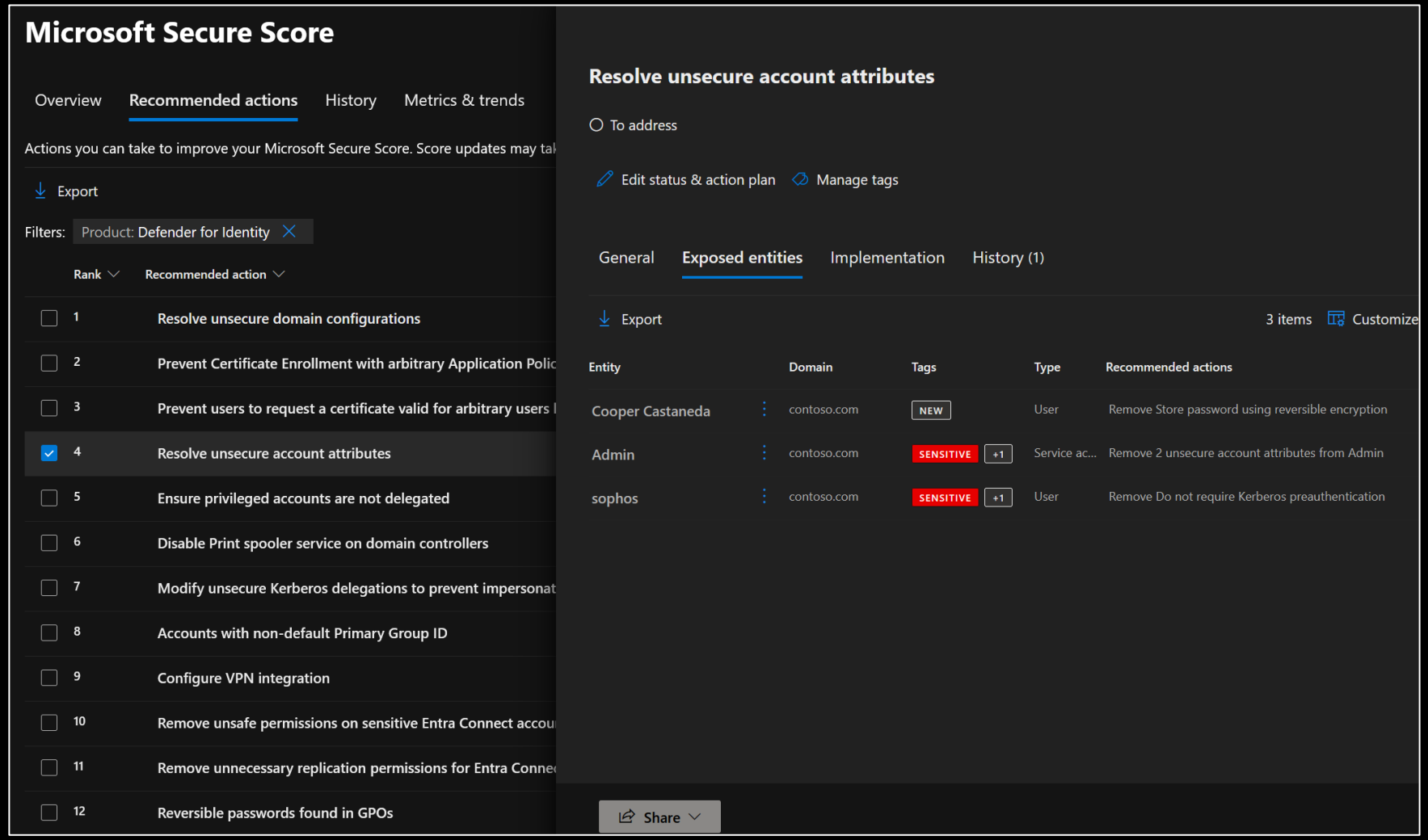
Microsoft Advanced Threat Analytics (ATA)



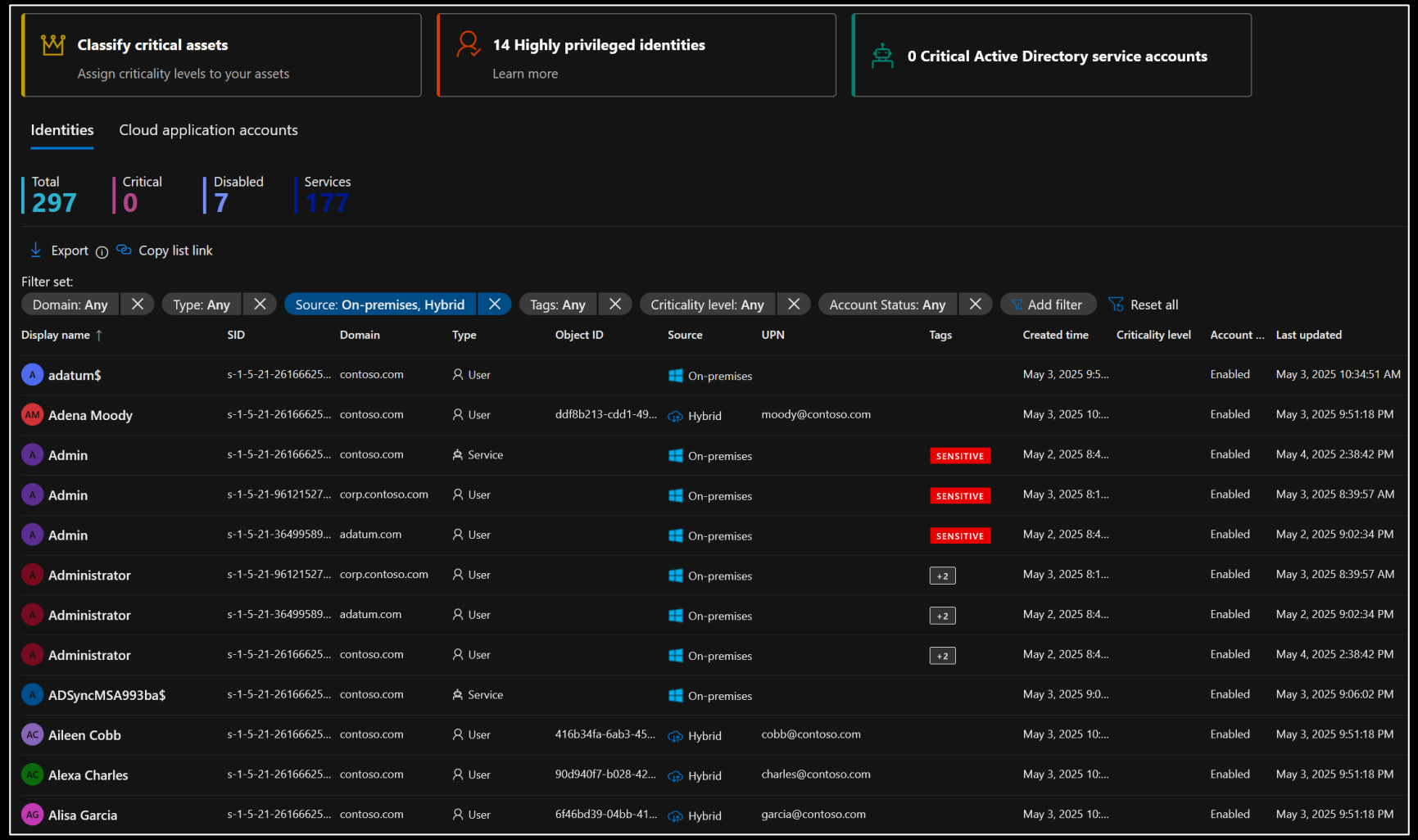
Microsoft Defender for Identity Architecture



Security Posture Recommendations



Identity Inventory



Display name	SID	Domain	Type	Object ID	Source	UPN	Tags	Created time	Criticality level	Account ...	Last updated
adatum$	s-1-5-21-26166625...	contoso.com	User		On-premises			May 3, 2025 9:5...		Enabled	May 3, 2025 10:34:51 AM
Adena Moody	s-1-5-21-26166625...	contoso.com	User	ddf8b213-cdd1-49...	Hybrid	moody@contoso.com		May 3, 2025 10:...		Enabled	May 3, 2025 9:51:18 PM
Admin	s-1-5-21-26166625...	contoso.com	Service		On-premises		SENSITIVE	May 2, 2025 8:4...		Enabled	May 4, 2025 2:38:42 PM
Admin	s-1-5-21-96121527...	corp.contoso.com	User		On-premises		SENSITIVE	May 3, 2025 8:1...		Enabled	May 3, 2025 8:39:57 AM
Admin	s-1-5-21-36499589...	adatum.com	User		On-premises		SENSITIVE	May 2, 2025 8:4...		Enabled	May 2, 2025 9:02:34 PM
Administrator	s-1-5-21-96121527...	corp.contoso.com	User		On-premises		+2	May 3, 2025 8:1...		Enabled	May 3, 2025 8:39:57 AM
Administrator	s-1-5-21-36499589...	adatum.com	User		On-premises		+2	May 2, 2025 8:4...		Enabled	May 2, 2025 9:02:34 PM
Administrator	s-1-5-21-26166625...	contoso.com	User		On-premises		+2	May 2, 2025 8:4...		Enabled	May 4, 2025 2:38:42 PM
ADSyncMSA993ba$	s-1-5-21-26166625...	contoso.com	Service		On-premises			May 3, 2025 9:0...		Enabled	May 3, 2025 9:06:02 PM
Aileen Cobb	s-1-5-21-26166625...	contoso.com	User	416b34fa-6ab3-45...	Hybrid	cobb@contoso.com		May 3, 2025 10:...		Enabled	May 3, 2025 9:51:18 PM
Alexa Charles	s-1-5-21-26166625...	contoso.com	User	90d940f7-b028-42...	Hybrid	charles@contoso.com		May 3, 2025 10:...		Enabled	May 3, 2025 9:51:18 PM
Alisa Garcia	s-1-5-21-26166625...	contoso.com	User	6f46bd39-04bb-41...	Hybrid	garcia@contoso.com		May 3, 2025 10:...		Enabled	May 3, 2025 9:51:18 PM

Service Account Discovery

Total	Service account type: Managed	Service account type: User	Critical
4	3	1	0

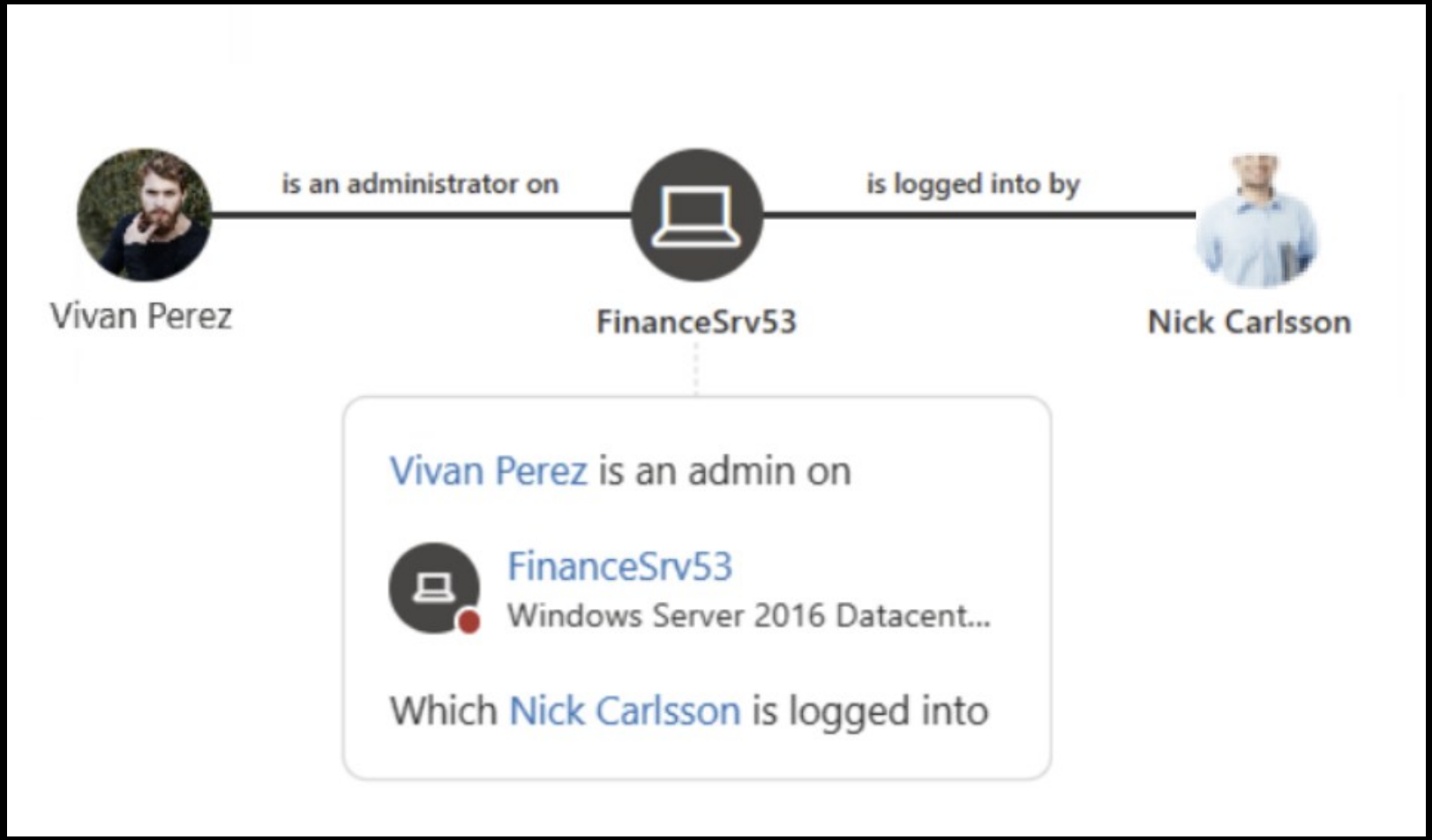
Export

Filter set:

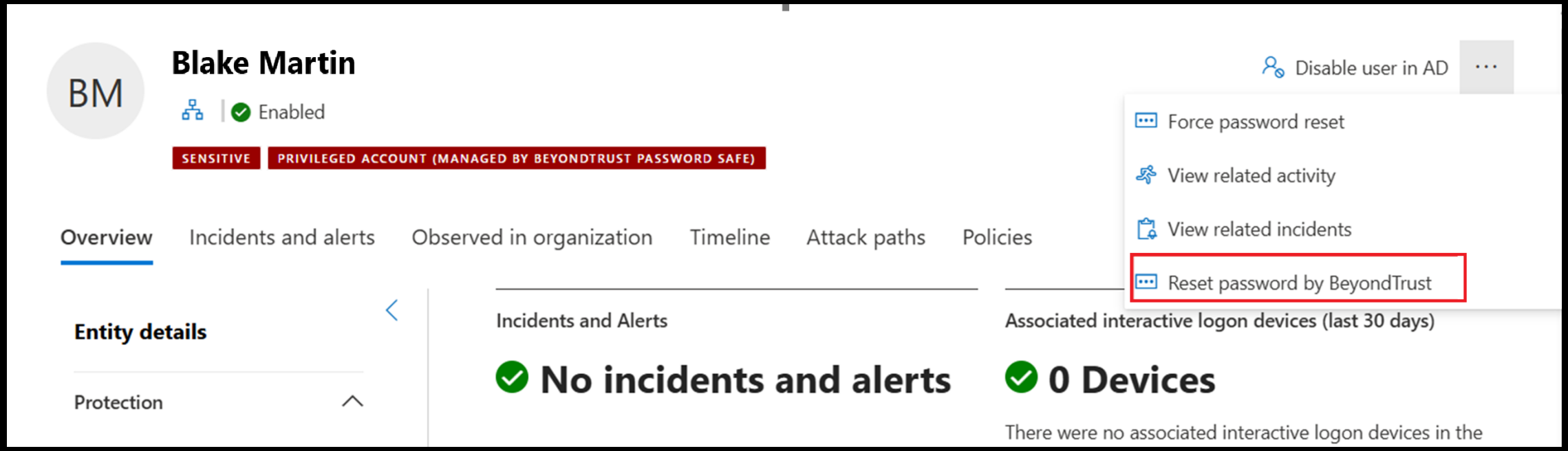
Service account type: **Any** | Auth protocol: **Any** | Criticality level: **Any** | Add filter

Display name	Domain	Type	Enabled	Tags	Last on-prem logon	Auth protocols	Service classes	Created	Last updated
Admin	contoso.com	User	Yes	SENSITIVE	May 4, 2025	Kerberos, Ntlm	LDAP	May 2, 2025 8:44:45 PM	May 4, 2025 2:38:42 PM
svc_mdi	contoso.com	gMSA	Yes		May 3, 2025	Kerberos		May 3, 2025 1:52:06 PM	May 3, 2025 1:57:48 PM
svc_adfs	contoso.com	gMSA	Yes		May 3, 2025	Kerberos		May 3, 2025 10:28:25 AM	May 3, 2025 10:30:18 AM
ADSyncMSA993ba	contoso.com	sMSA	Yes					May 3, 2025 9:05:58 PM	May 3, 2025 9:06:02 PM

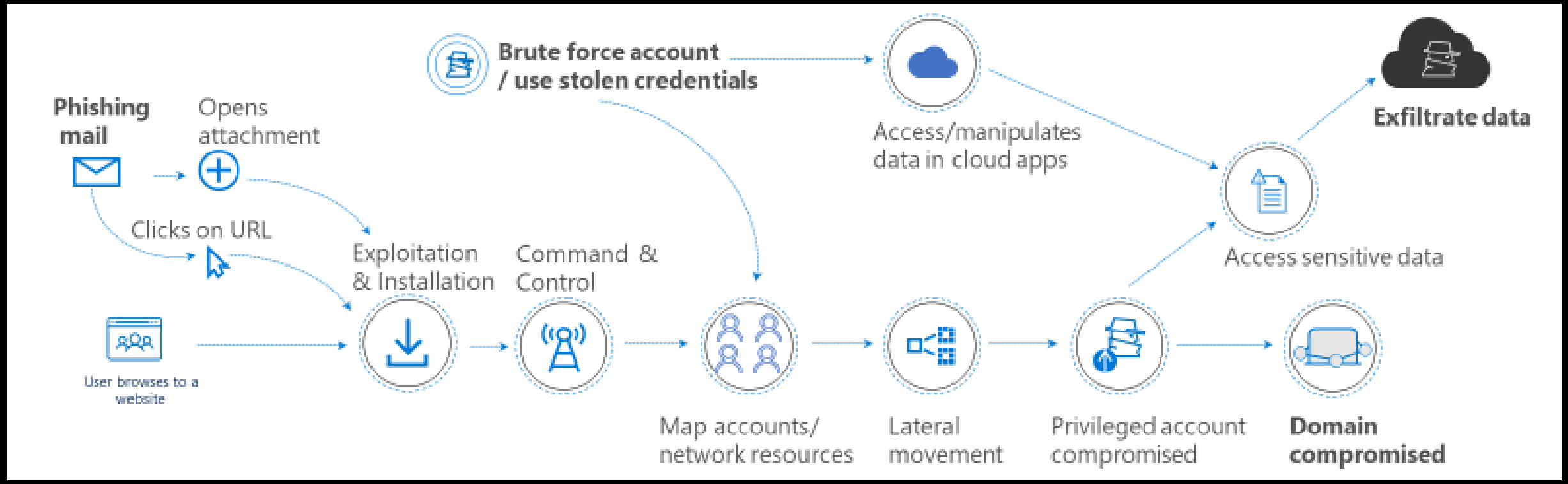
Lateral Movement Paths



Remediation Actions – PAM Integration



Enterprise Cyber Kill Chain



Active Directory
Reconnaissance & Discovery

Reconnaissance – DNS Zone Transfer

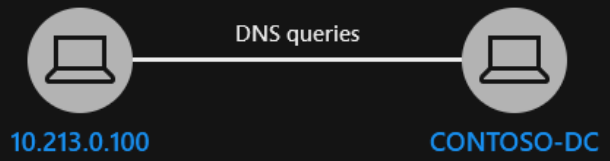
```
└─# nmap contoso-dc.contoso.com --script dns-zone-transfer --script-args "dns-zone-transfer.domain='contoso.com'" | grep ' A '
| contoso.com.                                    A    10.213.0.9
| contoso.com.                                    A    10.213.0.3
| contoso.contoso.com.                            A    10.213.0.3
| CONTOSO-ADFS.contoso.com.                       A    10.213.0.4
| contoso-dc.contoso.com.                         A    10.213.0.3
| contoso-dc2.contoso.com.                        A    10.213.0.9
| CONTOSO-PC1.contoso.com.                        A    10.213.0.6
| CONTOSO-PC2.contoso.com.                        A    10.213.0.7
| CONTOSO-SRV.contoso.com.                        A    10.213.0.5
| DomainDnsZones.contoso.com.                     A    10.213.0.9
| DomainDnsZones.contoso.com.                     A    10.213.0.3
| ForestDnsZones.contoso.com.                     A    10.213.0.9
| ForestDnsZones.contoso.com.                     A    10.213.0.3
| gateway.contoso.com.                            A    10.213.0.5
| local.contoso.com.                              A    10.213.0.1
| login.contoso.com.                              A    10.213.0.4
| certauth.login.contoso.com.                     A    10.213.0.4
```

Reconnaissance – DNS Zone Transfer

What happened

10.213.0.100 sent suspicious DNS queries to CONTOSO-DC.

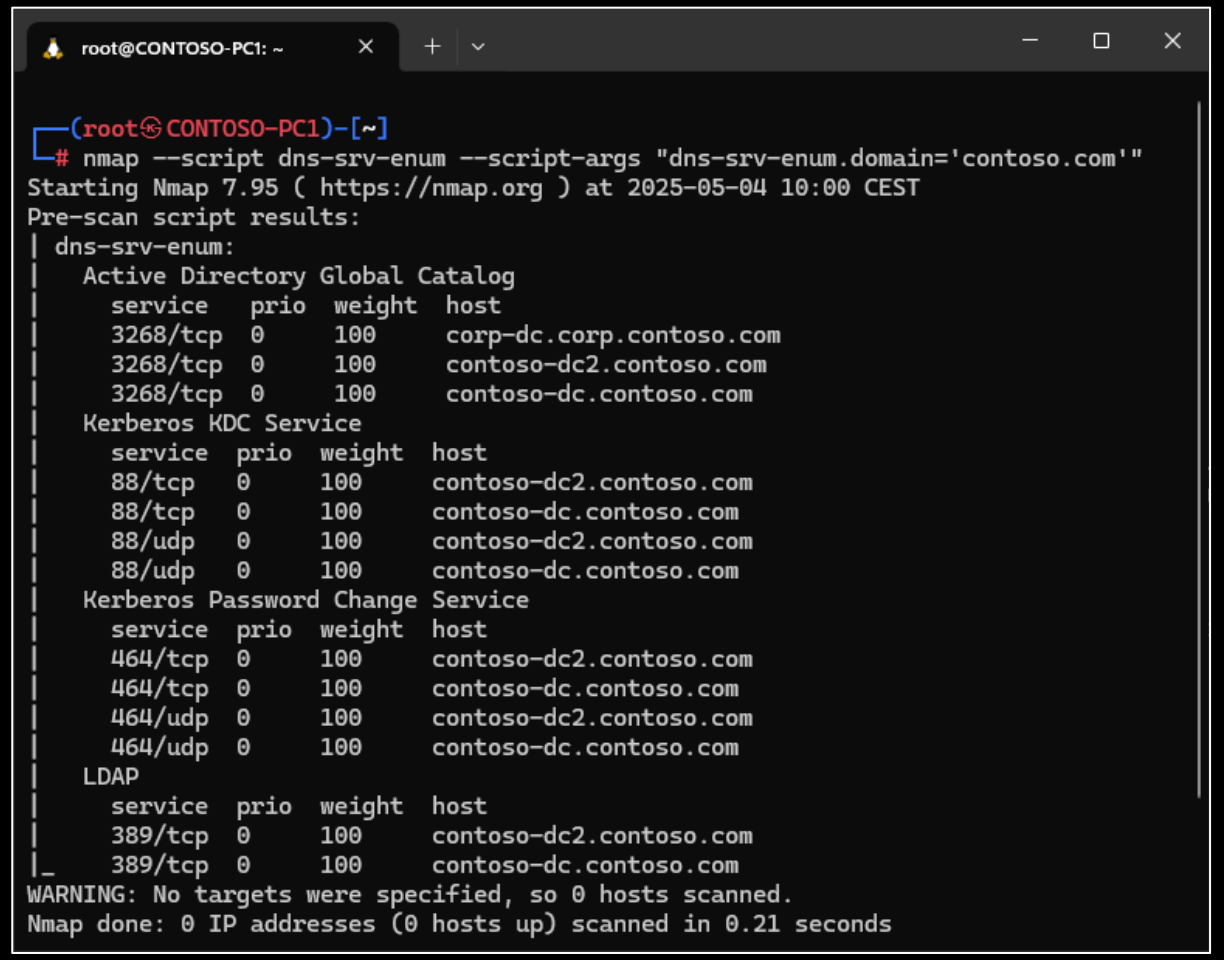
Alert graph



Important information

- 10.213.0.100 is not a DNS server.
- May 4, 2024 5:29 PM
  10.213.0.100 (10.213.0.100) requested unusually large amounts of DNS records using AXFR requests, resolving contoso.com

Reconnaissance – DNS SRV Record Enumeration



Custom Detection Rules

Run query | Last 7 days | Save | Share link

Query

```
1  IdentityQueryEvents
2  | where Protocol  == "Dns"
3  | where QueryType == "Srv"
4  | where QueryTarget in ("_xmpp-server._tcp.contoso.com","_http._tcp.kali.download")
```

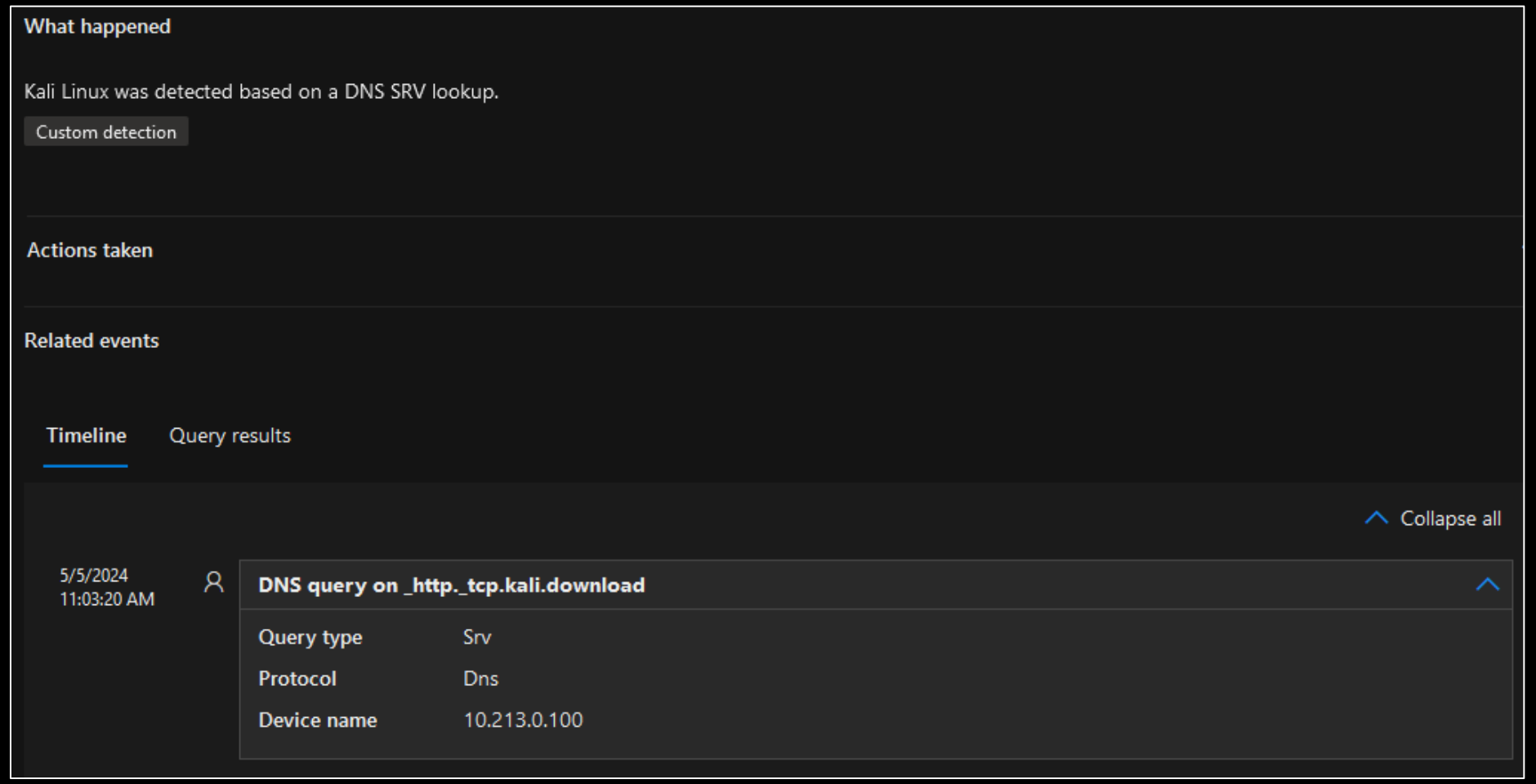
Getting started | Results | Query history

Export | Show empty columns | 6 items

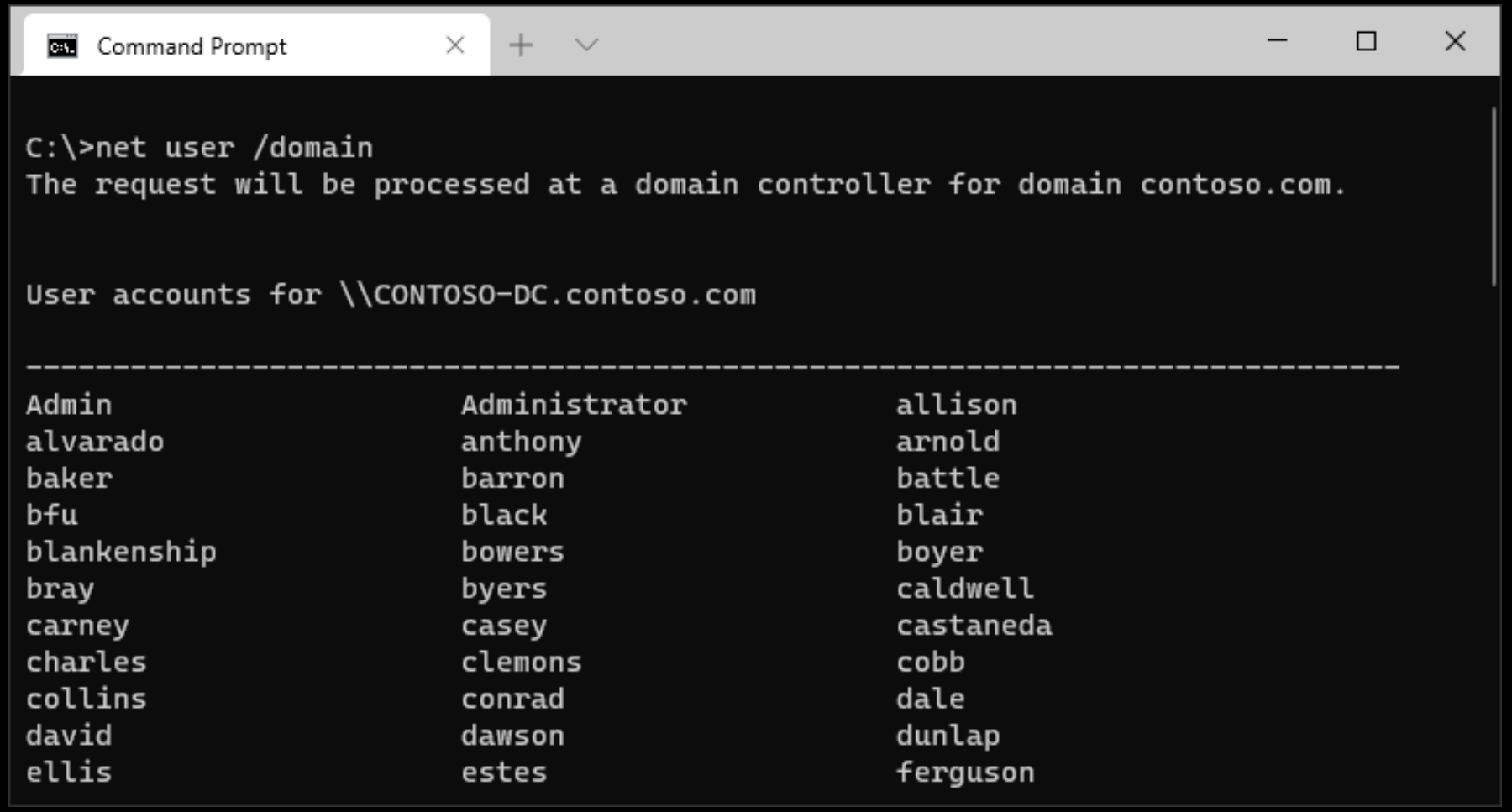
Filters: Add filter

Timestamp	ActionType	QueryType	QueryTarget	DeviceName
May 4, 2025 10:00:00 AM	DNS query	Srv	_xmpp-server._tcp.contoso.com	10.213.0.100
May 3, 2025 8:18:06 PM	DNS query	Srv	_http._tcp.kali.download	10.213.0.100
May 3, 2025 8:18:06 PM	DNS query	Srv	_http._tcp.kali.download	contoso-dc.contoso.com
May 3, 2025 8:18:06 PM	DNS query	Srv	_http._tcp.kali.download	contoso-dc.contoso.com
May 3, 2025 8:18:06 PM	DNS query	Srv	_http._tcp.kali.download	contoso-dc.contoso.com
May 3, 2025 9:59:41 PM	DNS query	Srv	_xmpp-server._tcp.contoso.com	10.213.0.100

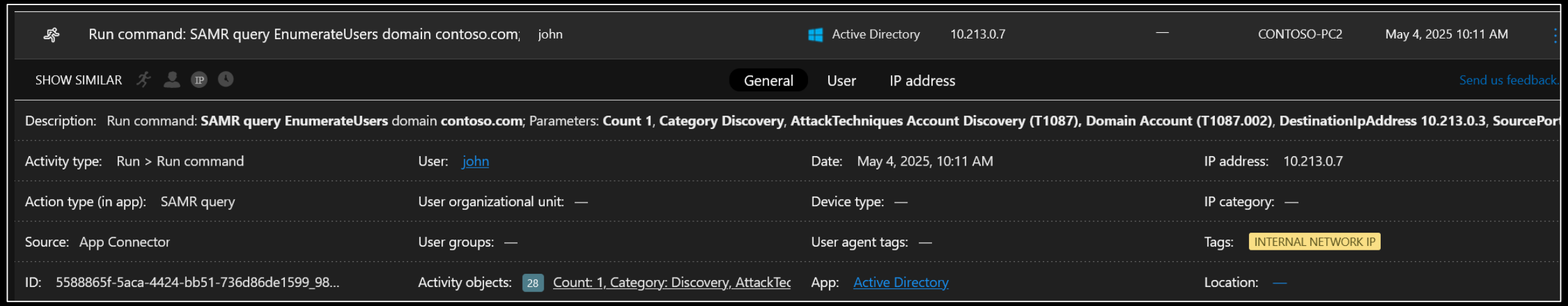
Custom Detection Rules



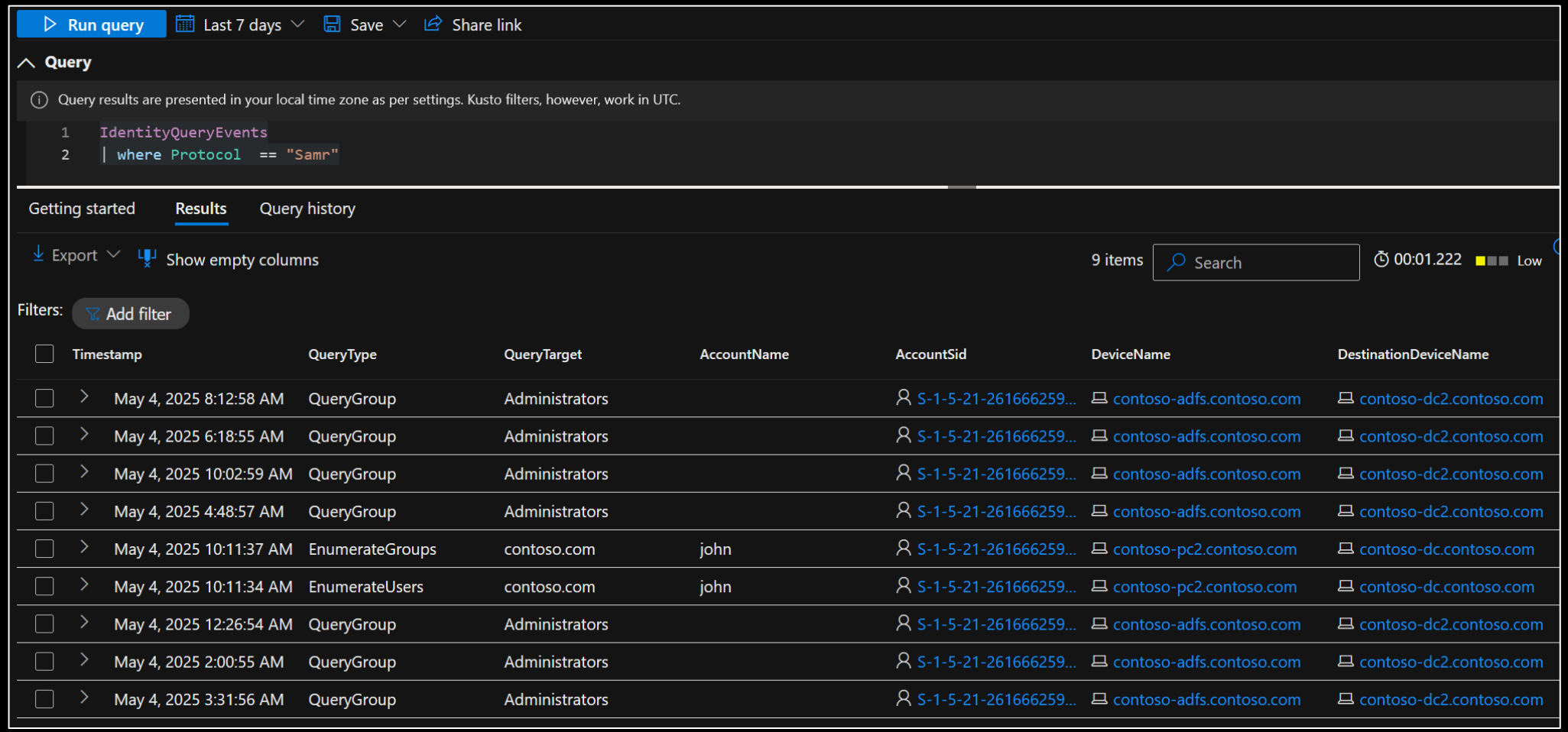
Reconnaissance – SAM-R Enumeration



SAM-R Enumeration – 1 Month Learning Period



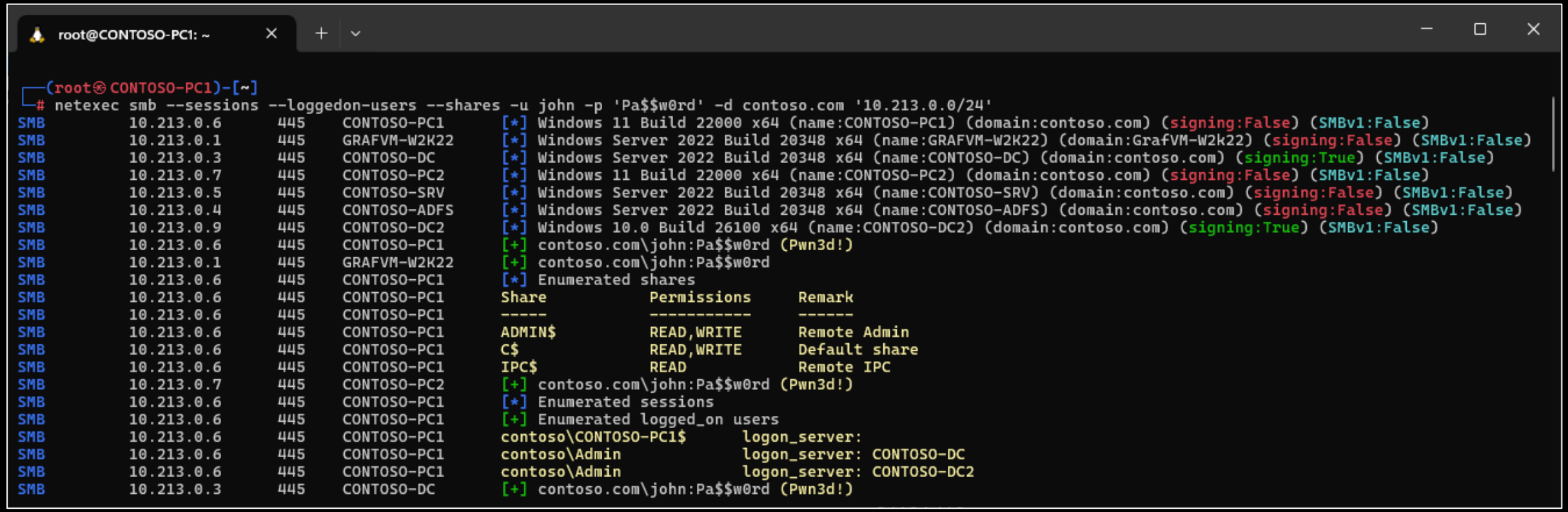
SAM-R Enumeration – Advanced Hunting



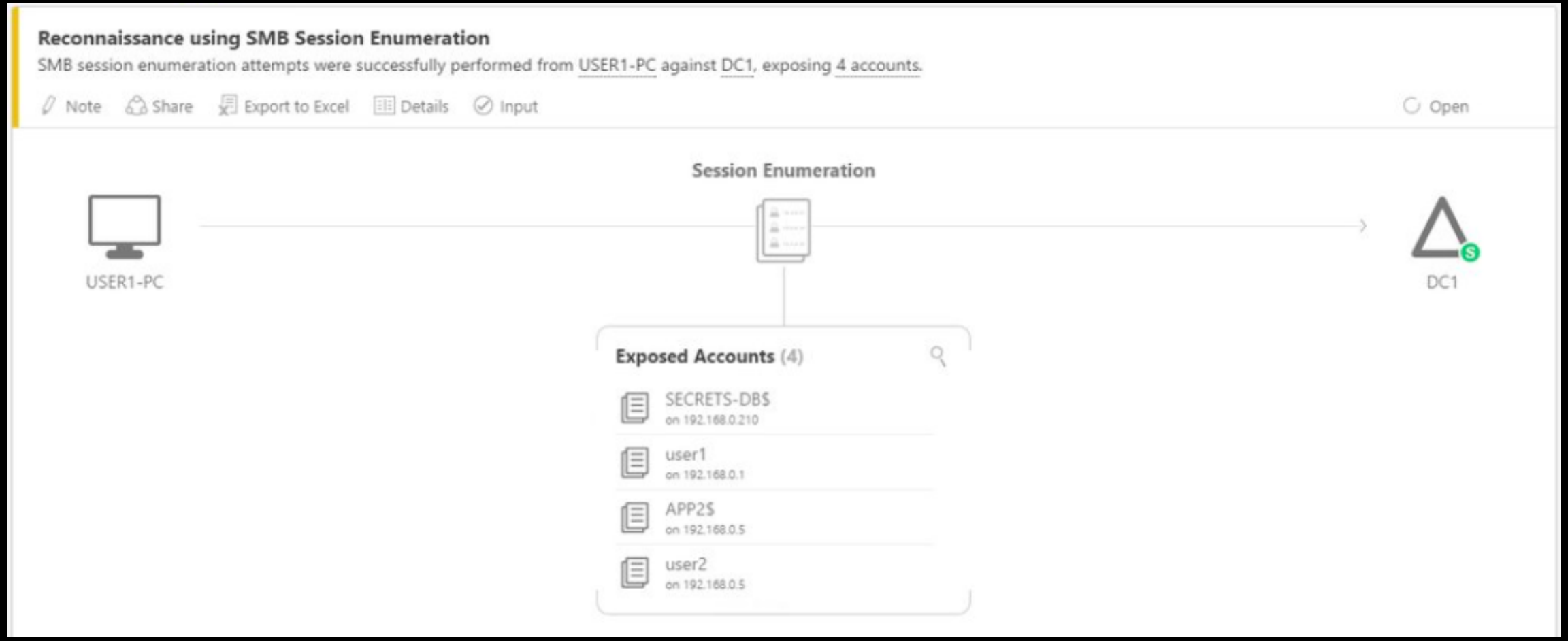
DEMO

Advanced Hunting

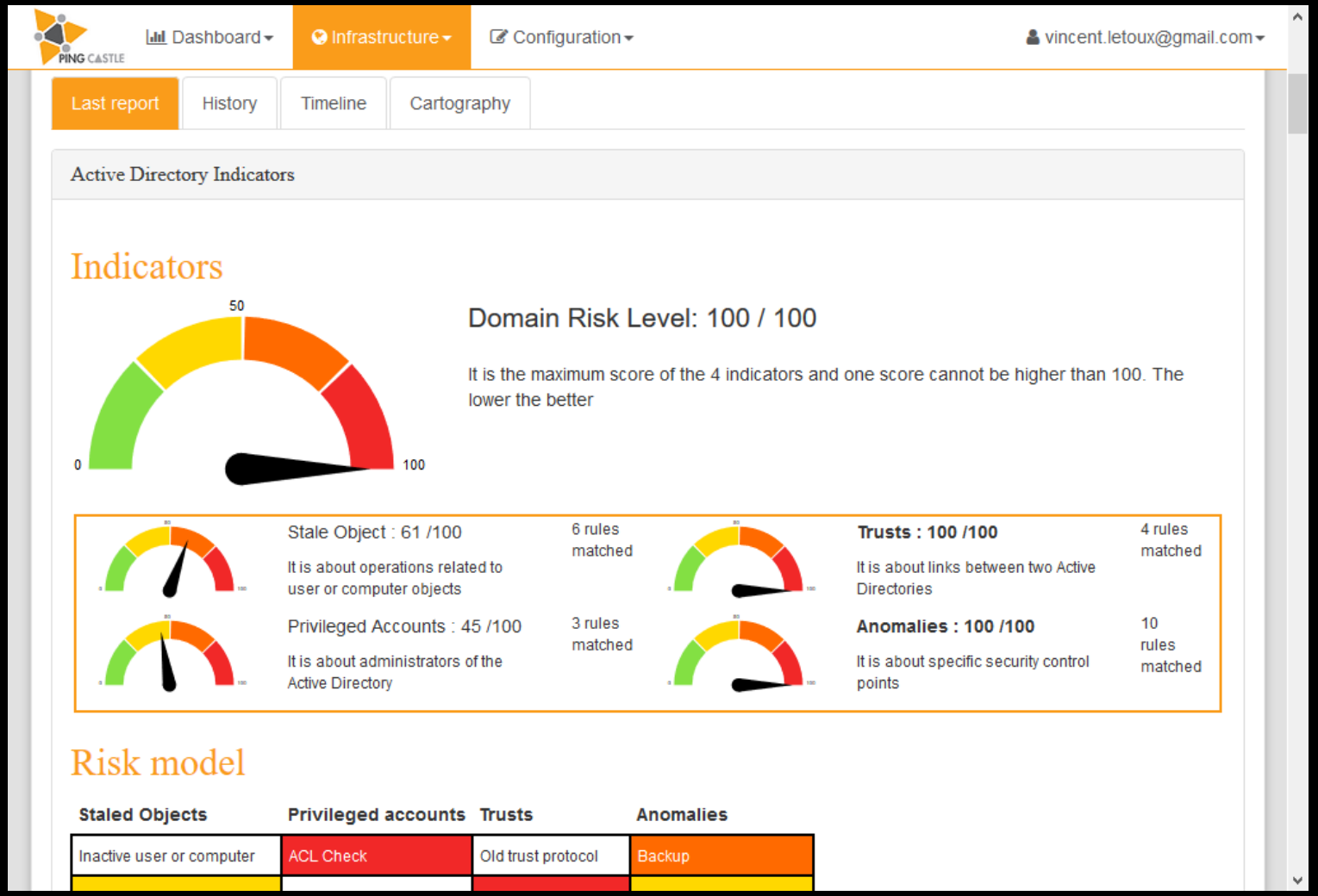
Reconnaissance – SMB Enumeration



Reconnaissance – SMB Session Enumeration



Reconnaissance – LDAP Enumeration

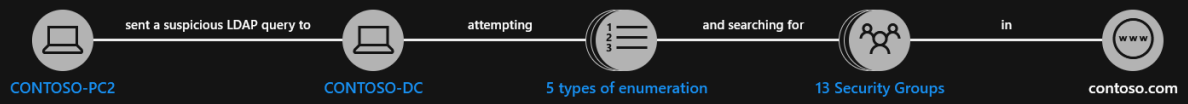


Reconnaissance – LDAP Enumeration

What happened

Actors on CONTOSO-PC2 sent suspicious LDAP queries to CONTOSO-DC, searching for 5 types of enumeration and 13 groups in contoso.com

Alert graph



Important information

Activity Details

LDAP search events

49 items Customize

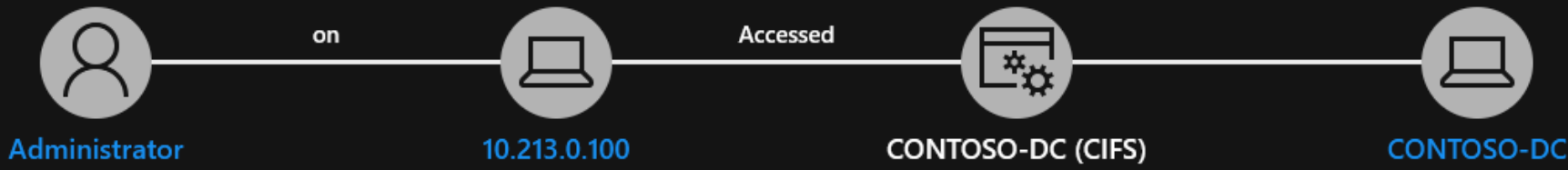
Timestamp ↓	Base object	Search scope	Search filter	Enumeration type	Queried groups
May 4, 2025 1:33 PM	CN=Administrators,CN=Builtin,DC=contoso,DC=com	BaseObject	(objectClass=*)	AllObjects	Administrators (Administrators have complete and unrestricted a
May 4, 2025 1:33 PM	CN=Backup Operators,CN=Builtin,DC=contoso,DC=com	BaseObject	(objectClass=*)	AllObjects	Backup Operators (Backup Operators can override security restri
May 4, 2025 1:33 PM	CN=Domain Controllers,CN=Users,DC=contoso,DC=com	BaseObject	(objectClass=*)	AllObjects	Domain Controllers (All domain controllers in the domain)
May 4, 2025 1:33 PM	CN=Schema Admins,CN=Users,DC=contoso,DC=com	BaseObject	(objectClass=*)	AllObjects	Schema Admins (Designated administrators of the schema)
May 4, 2025 1:33 PM	CN=Enterprise Admins,CN=Users,DC=contoso,DC=com	BaseObject	(objectClass=*)	AllObjects	Enterprise Admins (Designated administrators of the enterprise)
May 4, 2025 1:33 PM	CN=Domain Admins,CN=Users,DC=contoso,DC=com	BaseObject	(objectClass=*)	AllObjects	Domain Admins (Designated administrators of the domain)

Reconnaissance – Honeytoken Activity

What happened

Administrator performed 1 suspicious activity.

Alert graph



Important information

- Administrator attempted to authenticate from 10.213.0.100 using NTLM when accessing CONTOSO-DC (CIFS) on CONTOSO-DC.

Credential Access

Password Spraying – SMB

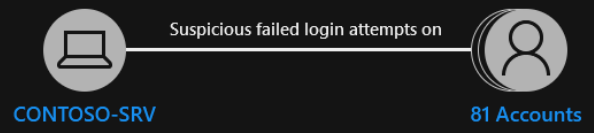
```
└─# patator smb_login host=contoso-dc port=445 user=FILE0 domain=CONTOSO password=FILE1 0=users.txt 1=passwords.txt
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  from telnetlib import Telnet
19:37:55 patator    INFO - Starting Patator 1.0 (https://github.com/lanjelot/patator) with python-3.11.8 at 2024-05-04 19:37 CEST
19:37:55 patator    INFO -
19:37:55 patator    INFO - code     size   time | candidate                          |   num | mesg
19:37:55 patator    INFO - -----------------------------------------------------------------------------
19:37:55 patator    INFO - c000006d 20    0.143 | Administrator:Contoso2024          |     1 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - 0        45    0.136 | whitaker:Password123               |    11 | contoso\CONTOSO-DC (Windows 10.0 Build 20348)
19:37:56 patator    INFO - 0        45    0.113 | Admin:Pa$$w0rd                     |     6 | contoso\CONTOSO-DC (Windows 10.0 Build 20348)
19:37:56 patator    INFO - c000006d 20    0.169 | caldwell:Contoso2024               |     7 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.422 | caldwell:Pa$$w0rd                  |     9 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.256 | Administrator:Password123          |     2 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - 0        45    0.354 | Administrator:Pa$$w0rd             |     3 | contoso\CONTOSO-DC (Windows 10.0 Build 20348)
19:37:56 patator    INFO - c000006d 20    0.489 | Admin:Password123                  |     5 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.351 | martinez:Password123               |    17 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.389 | caldwell:Password123               |     8 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.291 | dale:Contoso2024                   |    19 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.358 | whitaker:Contoso2024               |    10 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.347 | dale:Pa$$w0rd                      |    21 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.495 | Admin:Contoso2024                  |     4 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.238 | king:Pa$$w0rd                      |    15 | STATUS_LOGON_FAILURE
19:37:56 patator    INFO - c000006d 20    0.148 | leon:Pa$$w0rd                      |    27 | STATUS_LOGON_FAILURE
```

Password Spraying – SMB

What happened

An actor on CONTOSO-SRV generated a suspicious number of failed login attempts on 81 accounts. 2 accounts eventually authenticated successfully.

Alert graph



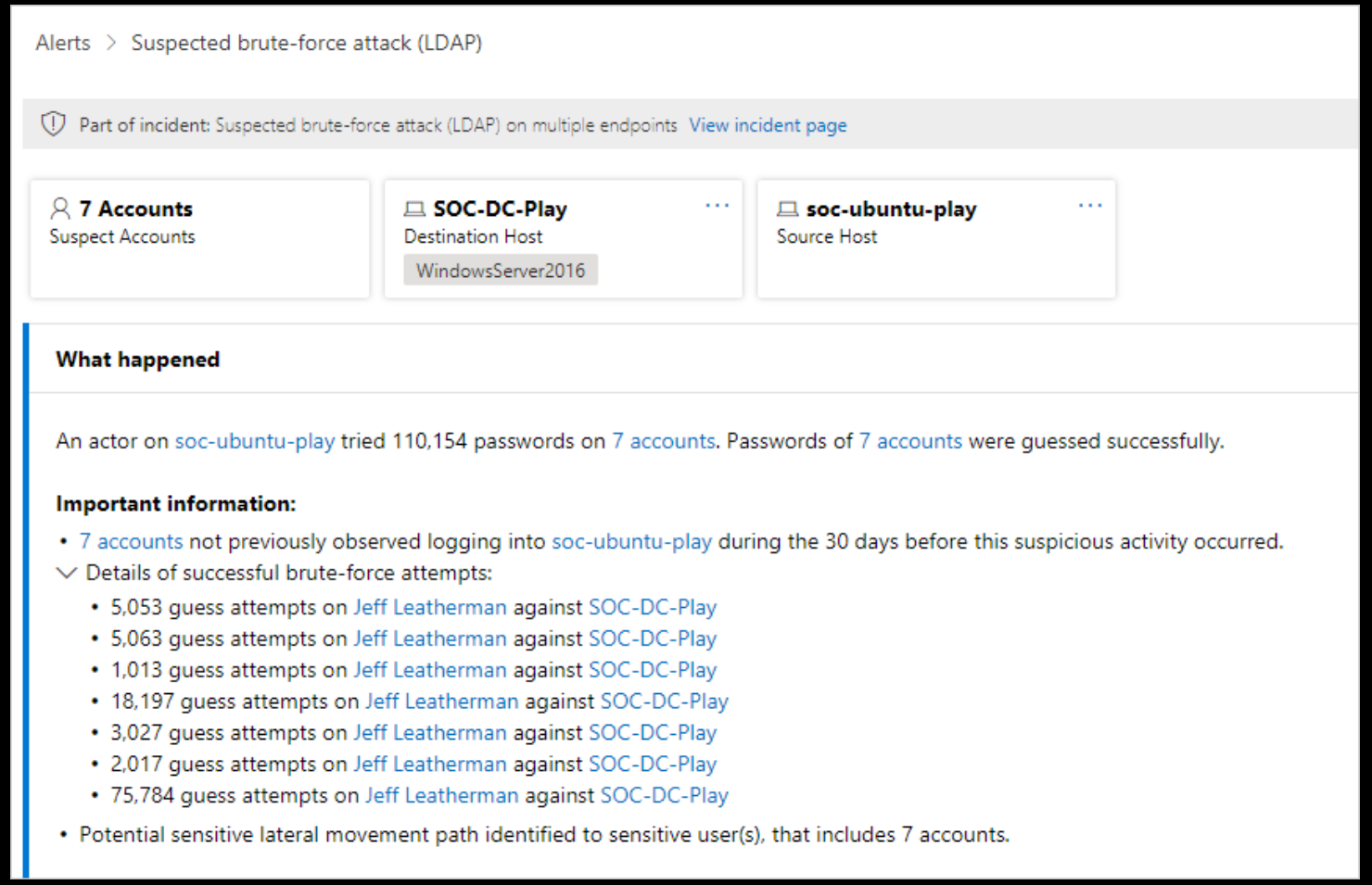
Important information

Authentication failure details by date

- On 5/4/24 43 accounts each failed to authenticate from CONTOSO-SRV 7 times, exceeding the normal failure rate for that machine.

- May 4, 2024 6:21 PM - May 4, 2024 6:30 PM
  81 accounts didn't update their password within the last 24 hours.
- None of the passwords attempted were previously used passwords.
- 81 accounts weren't recently observed logging into CONTOSO-SRV.
- May 4, 2024 6:21 PM
  2 accounts successfully logged in after multiple authentication failures.
- The suspicious authentication failures used Kerberos.

LDAP Brute-Force Attack



Credential Access - DCSync Attack

```
PS C:\> (Get-ADReplAccount -SamAccountName Admin -Server contoso-dc).SupplementalCredentials

ClearText:
NTLMStrongHash: 74b77a3232abb8a67e2b84bd05a98a17
Kerberos:
  Credentials:
    DES_CBC_MD5
      Key: 155d9baba8bfe649
  OldCredentials:
    DES_CBC_MD5
      Key: 7c1f1f73f48002dc
  Salt: CONTOSO.COMAdmin
  Flags: 0
KerberosNew:
  Credentials:
    AES256_CTS_HMAC_SHA1_96
      Key: 74aa09422b8b6e96779b2ffcddb7292bf24d23da4290af7d76c914c3f79b1d94
      Iterations: 4096
    AES128_CTS_HMAC_SHA1_96
      Key: f44c00b9a30fffab4e2c7c36a211aa10
      Iterations: 4096
    DES_CBC_MD5
      Key: 155d9baba8bfe649
      Iterations: 4096
```

Credential Access - DCSync Attack

What happened

Admin on CONTOSO-PC1 sent 2 replication requests to CONTOSO-DC.

Alert graph

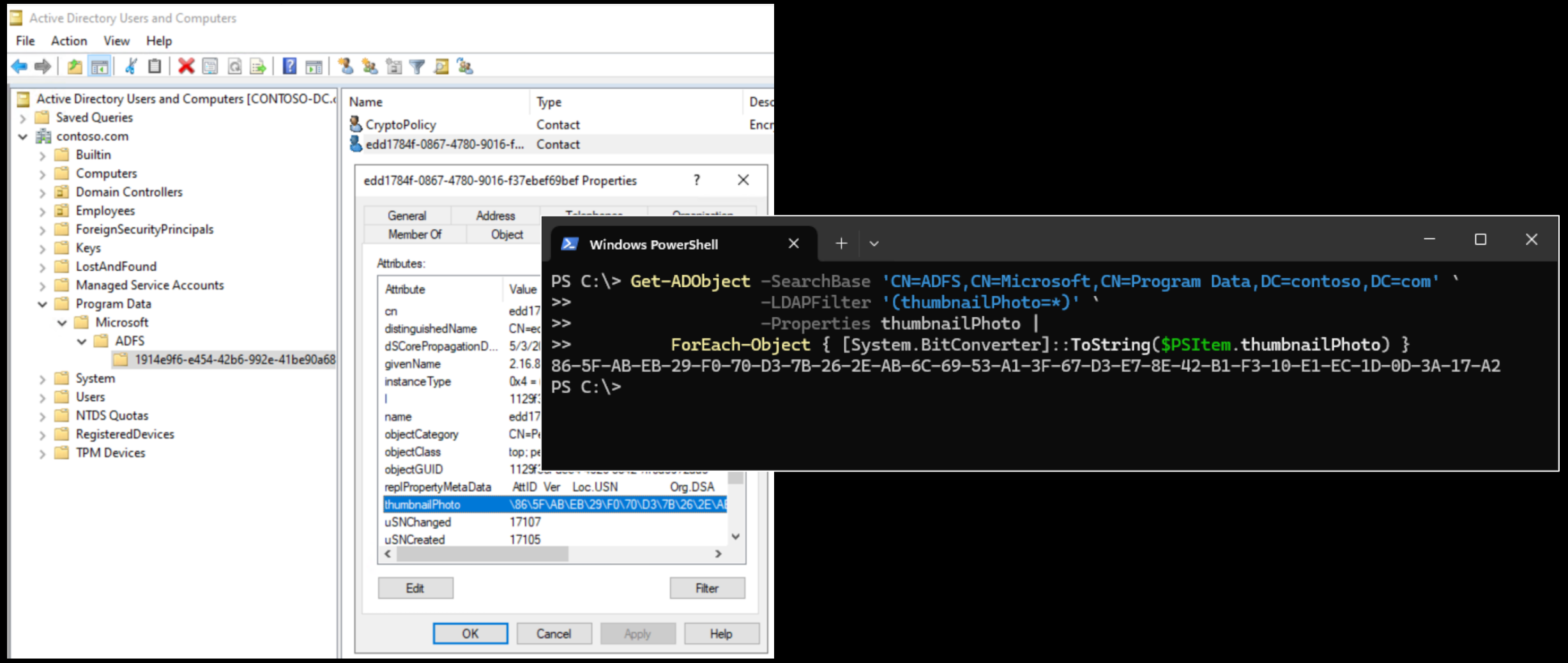
Important information

- CONTOSO-PC1 is not a recognized domain controller.
- May 4, 2024 8:07 PM
  CONTOSO-PC1 resolved from 10.213.0.6 with high certainty.

DEMO

DCSync Attack

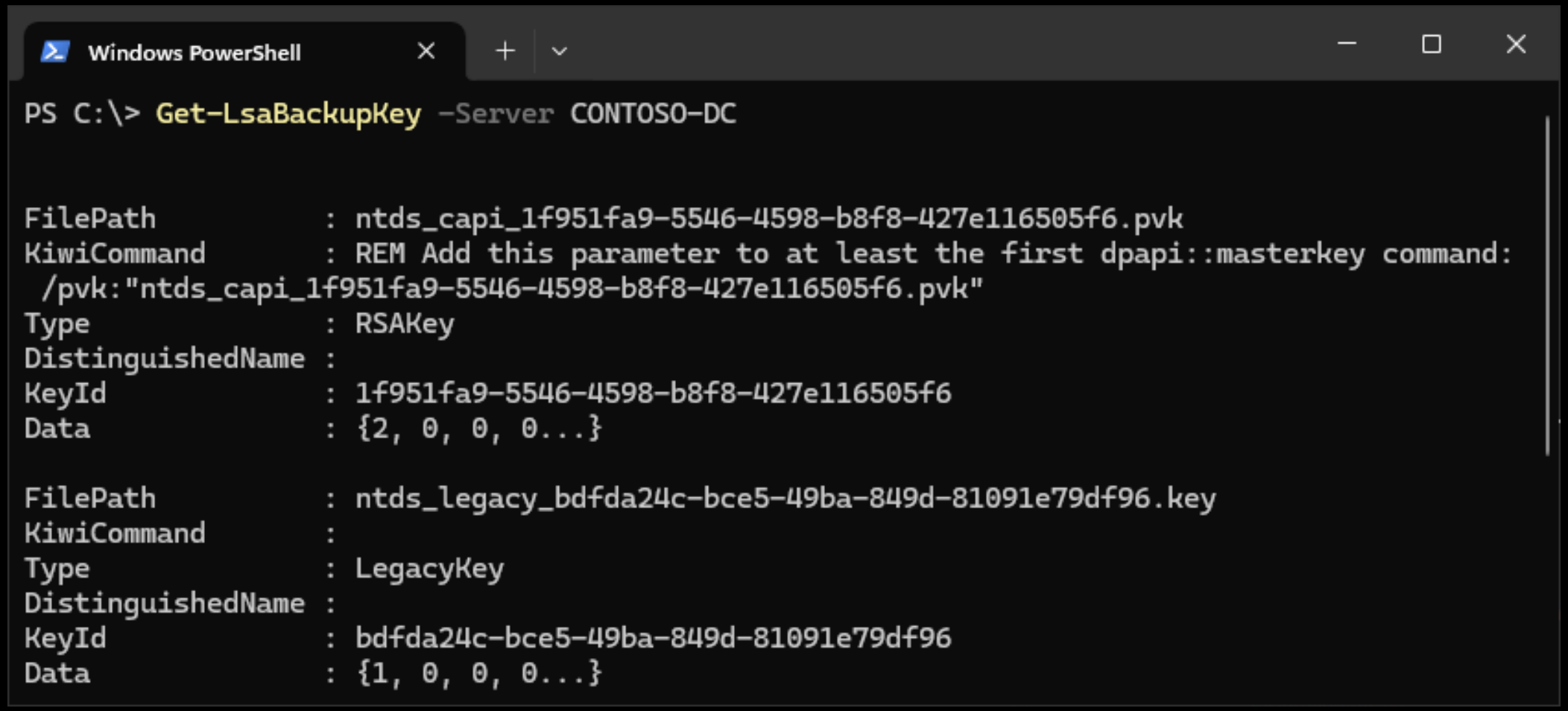
Credential Access - AD FS DKM Key Read



DEMO

AD FS DKM Key

Credential Access – DPAPI Backup Key Request

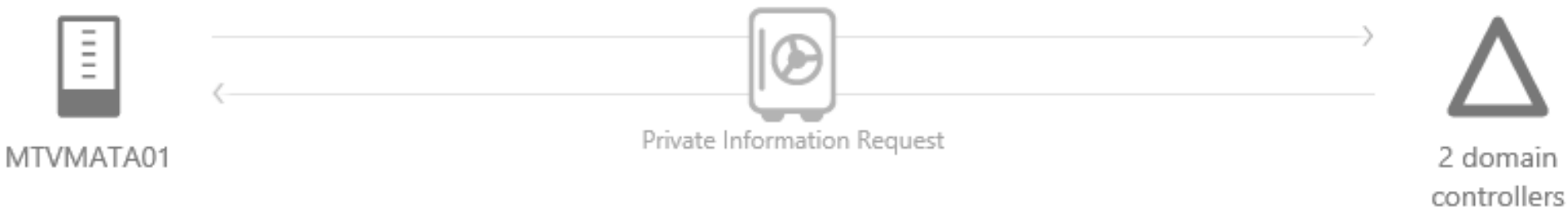


Credential Access – DPAPI Backup Key Request

Malicious Data Protection Private Information Request

An unknown user performed 4 successful attempts from MTVMATA01 to retrieve DPAPI domain backup key from 2 domain controllers.

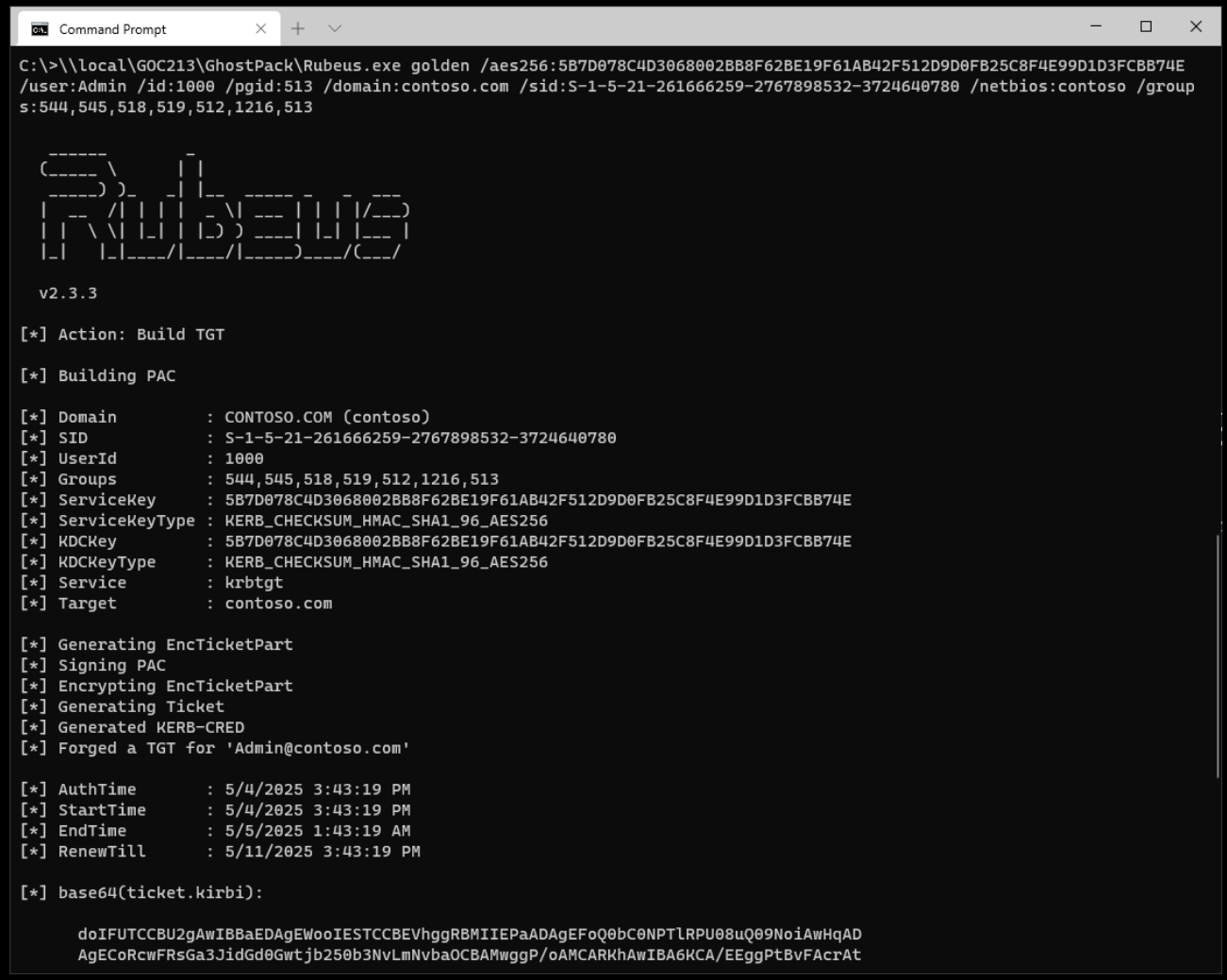
Note Share Export to Excel Details Open



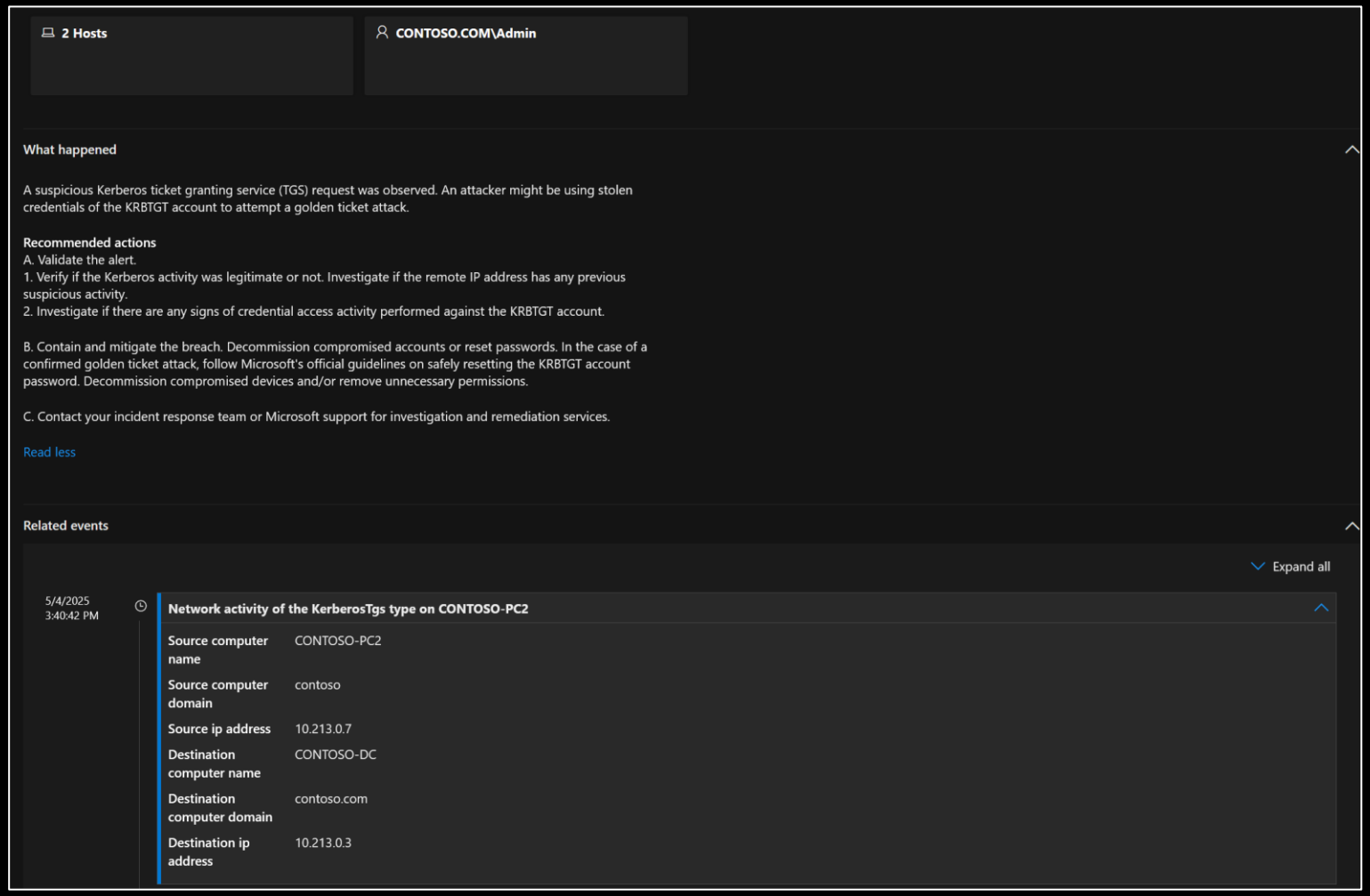
Recommendations

- Disconnect MTVMATA01 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable the relevant accounts

Credential Access – Golden Ticket Attack



Credential Access – Golden Ticket Attack

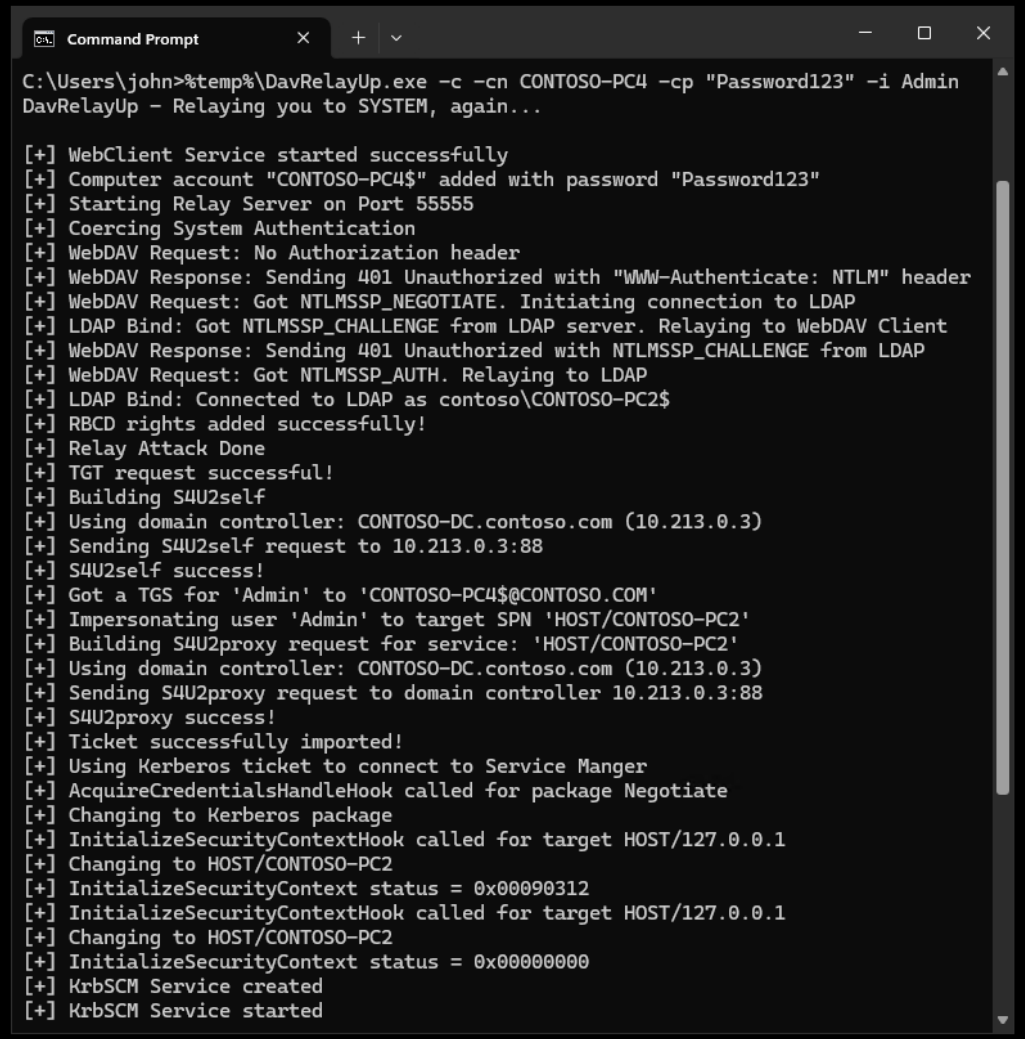


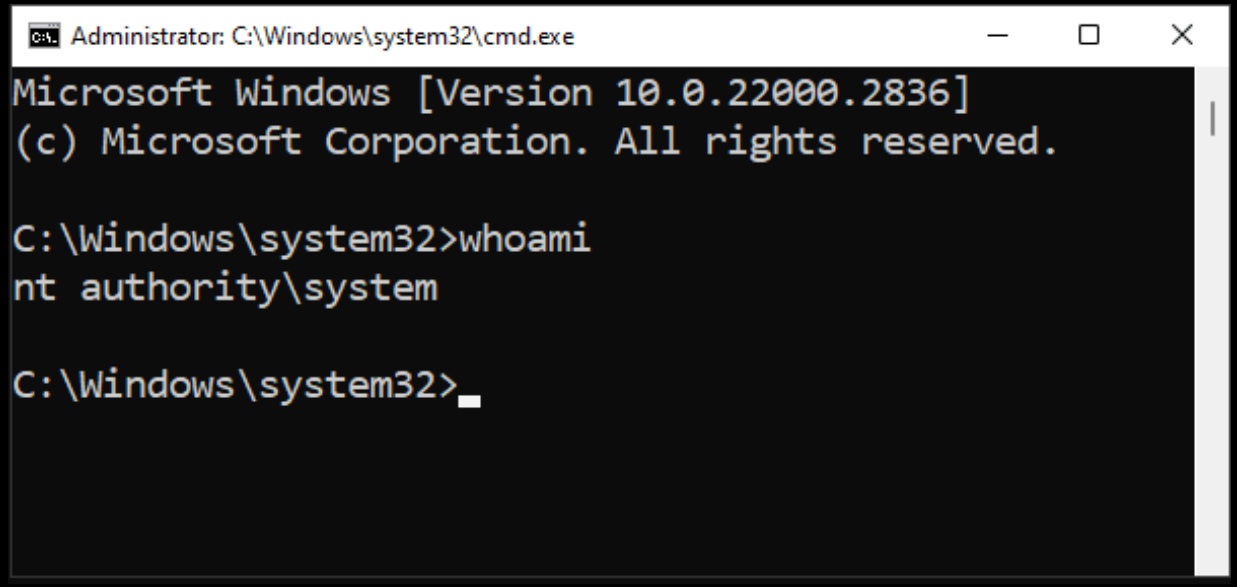
Golden Ticket Attack Detection Methods

- Encryption downgrade
- Forged authorization data
- Time anomaly
- Nonexistent account
- Ticket anomaly using RBCD

Privilege Escalation

Privilege Escalation – KrbRelayUp



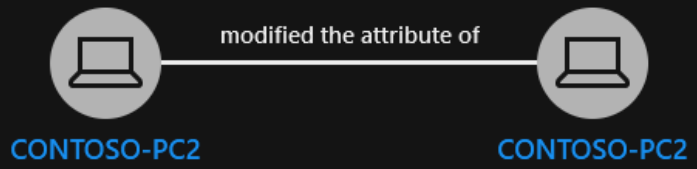


Privilege Escalation – NTLM Relay + RBCD

What happened

CONTOSO-PC2 edited the attribute msDS-AllowedToActOnBehalfOfOtherIdentity of CONTOSO-PC2.

Alert graph



Important information

- This alert is associated with the KrbRelayUp exploitation

Attempts:

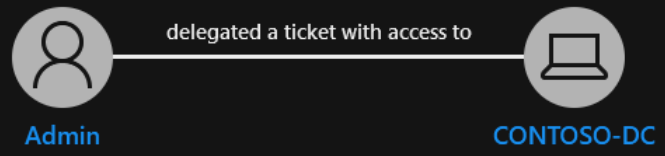
- May 4, 2024 7:46 PM
  msDS-AllowedToActOnBehalfOfOtherIdentity edited for CONTOSO-PC2

Privilege Escalation – NTLM Relay + RBCD

What happened

Admin on CONTOSO-PC4 used a ticket to delegate access to CONTOSO-PC2.

Alert graph



Important information

- Resource based constrained delegation is configured on the resource with the Admin as allowed to delegate.
- CONTOSO-PC4 was created on 5/4/24 7:46 PM

Delegation attempts:

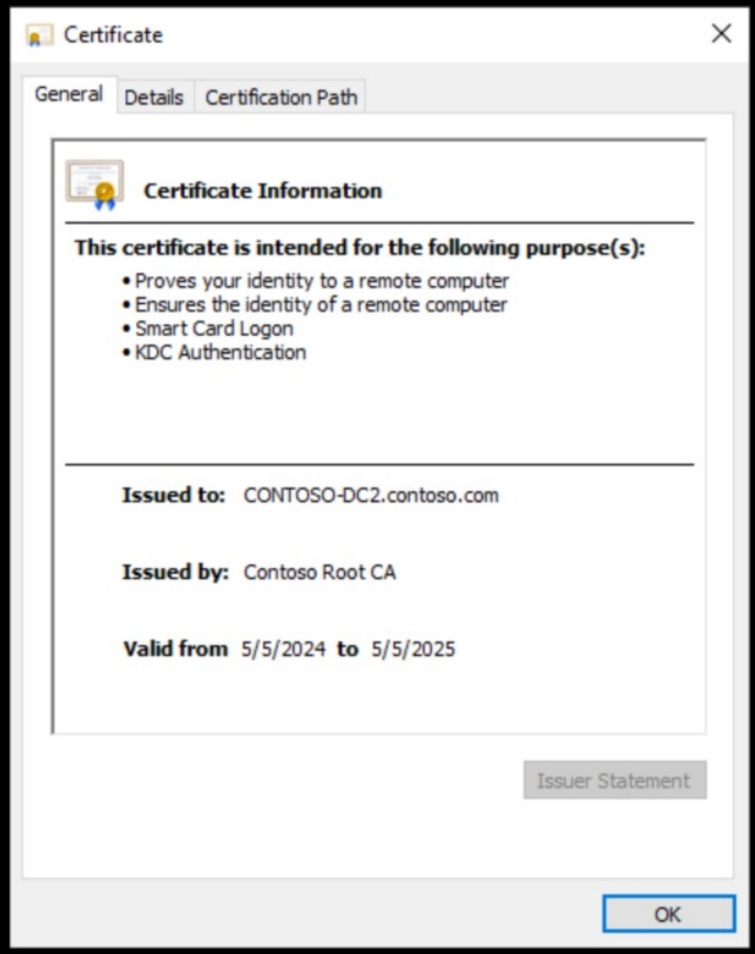
- 5/4/24 7:46 PM User Admin attempted to delegate to CONTOSO-DC with CONTOSO-PC2

- This alert is associated with the KrbRelayUp exploitation

Privilege Escalation – NTLM Relay to AD CS

```
└─# sudo impacket-ntlmrelayx --adcs --target http://contoso-dc.contoso.com/certsrv --template KerberosAuthentication -smb2support
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Protocol Client SMTP loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 10.213.0.9, attacking target http://contoso-dc.contoso.com
[*] HTTP server returned error code 301, treating as a successful login
[*] Authenticating against http://contoso-dc.contoso.com as CONTOSO/CONTOSO-DC2$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Connection from 10.213.0.9 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 6
[*] Base64 certificate of user CONTOSO-DC2$:
MIIR1QIBAzCCEY8GCSqGSIb3DQEHAaCCEYAEghF8MIIReDCCB68GCSqGSIb3DQEHBqCCB6AwggecAgEAMIIHlQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQItxIXjd
gPBgHanb7NKkXuis6u5q3UiFlYrjJbvLg/GS4VgUMTQ11aVDQNsNcpoUSOo2jb4uFV5iO2uLKQXBDVV1J3PV3bbTKn0CLSrZ3RmiRBlsCAjHCQOdr1zn+ArMRWqEcxpG3g
```

Privilege Escalation – NTLM Relay to AD CS

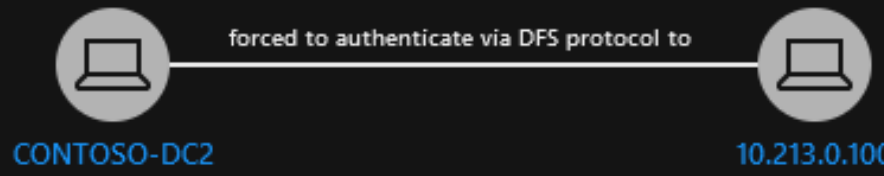


Privilege Escalation – DFCoerce Attack

What happened

CONTOSO-DC2 was forced to authenticate to 10.213.0.100 due to exploiting an operation in the DFS Protocol

Alert graph



Important information

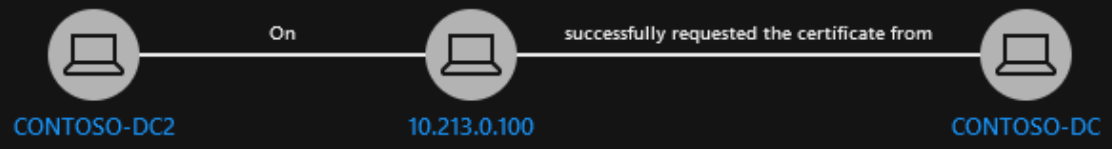
- This alert is associated with the DFSCoerce attack
- DFS connection attempt:
  - CONTOSO-DC2 was forced to authenticate to 10.213.0.100 using share test

Privilege Escalation – NTLM Relay to AD CS

What happened

CONTOSO-DC2 (Domain Controller) on 10.213.0.100 requested a certificate from CONTOSO-DC.

Alert graph



Important information

- This attack method is primarily combined with NTLM relay attack, in which DC authentication is coerced and relayed to ADCS server.
- The attack can be mitigated by revoking the certificate.
- The AD CS server which processed the requests was CONTOSO-DC.
- CONTOSO-DC2 is a Domain Controller.

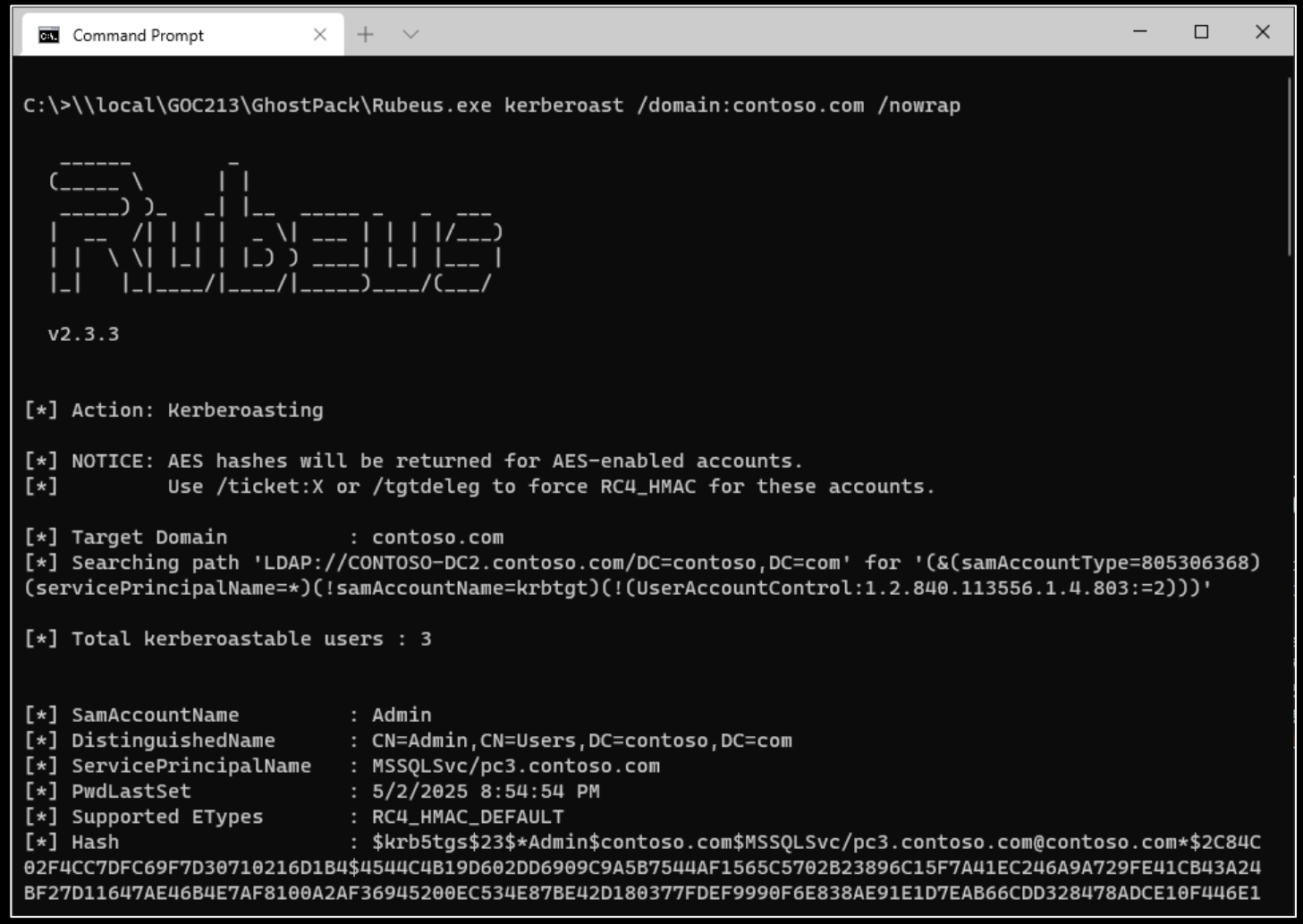
Certificates details:

- Issue date: 5/5/24 11:13 AM, Subject Key Identifier: 6, Request ID: 26 29 fd 4f 4e 14 eb e6 66 73 a4 89 aa 6e 3d 86 08 01 92 3a, Enrollment Method: Unknown

DEMO

Domain Controller
NTLM Authentication
Coercion

Privilege Escalation – Kerberoasting Attack



Privilege Escalation – Kerberoasting Attack

What happened

Admin on CONTOSO-PC2 sent a suspected kerberos Service Principal Name and exposed 2 accounts.

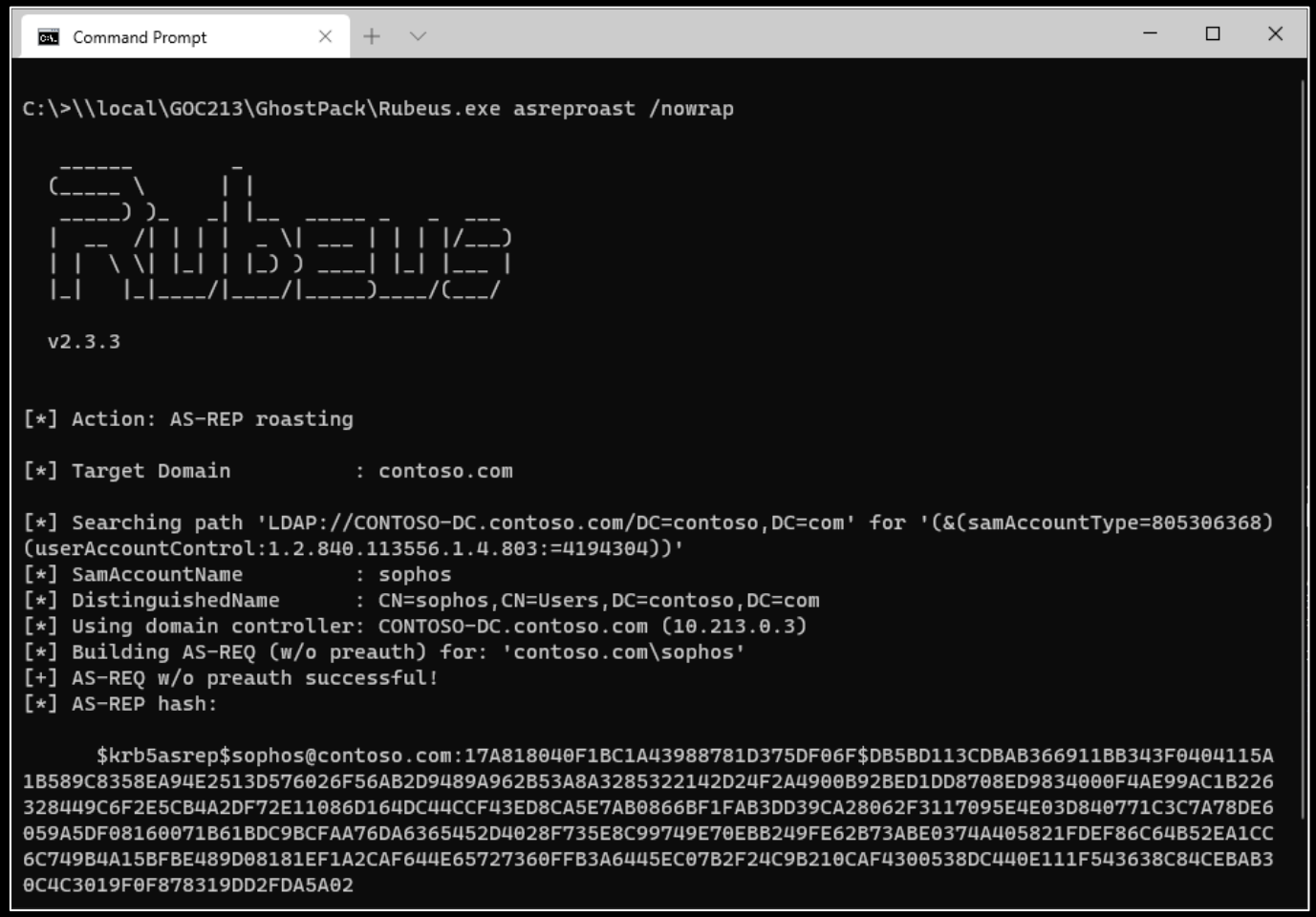
Alert graph

Important information

Kerberos successful exposure details:

- May 4, 2025 1:03 PM
  Admin exposed MSSQLSvc/pc01.contoso.com of Honorato Lott, which resulted with Rc4Hmac ticket.
- May 4, 2025 1:03 PM
  Admin exposed MSSQLSvc/pc02.contoso.com of Nash Whitaker, which resulted with Rc4Hmac ticket.

Privilege Escalation – AS-REP Roasting



Privilege Escalation – AS-REP Roasting – Phase 1

What happened

An actor on CONTOSO-PC2 sent a suspicious LDAP query, searching for DontRequirePreAuth on contoso.com.

Alert graph

Privilege Escalation – AS-REP Roasting – Phase 2

What happened

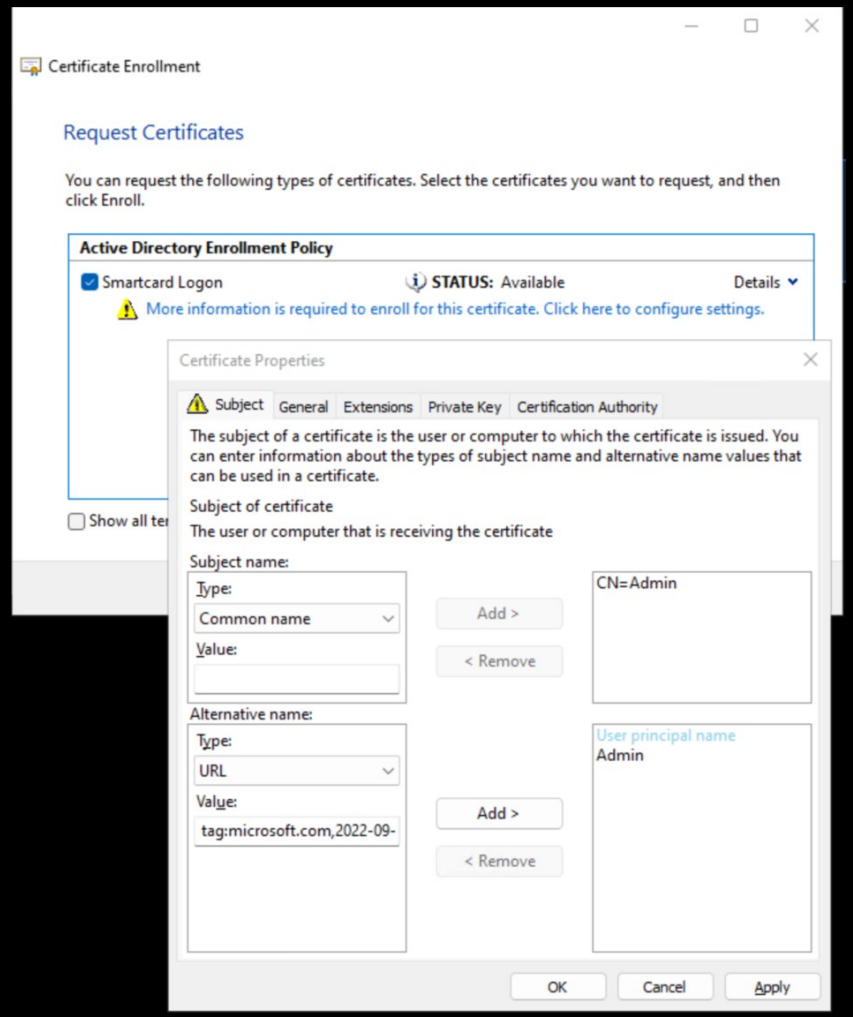
CONTOSO-PC2 enumerated users without preauthentication and exposed sophos

Alert graph

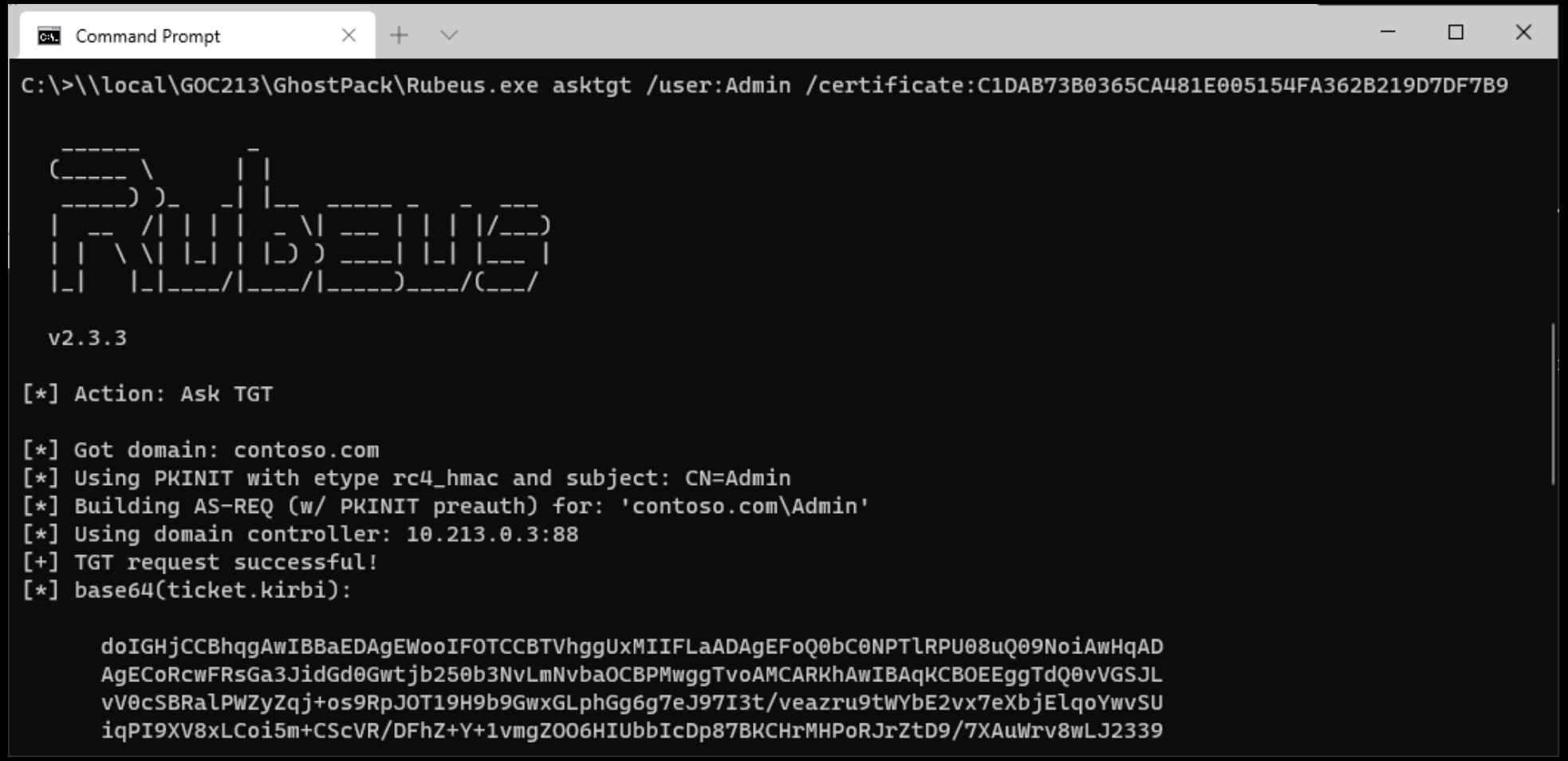
Important information

May 4, 2025 1:22 PM - May 4, 2025 1:22 PM
Exposed sophos
- May 4, 2025 1:22 PM
  exposed sophos that has a ticket encrypted using Rc4Hmac

Privilege Escalation – AD CS ESC1 Exploitation



Privilege Escalation – AD CS ESC1 Exploitation



Privilege Escalation – AD CS ESC1 Exploitation

Overview | **Recommended actions** | History | Metrics & trends

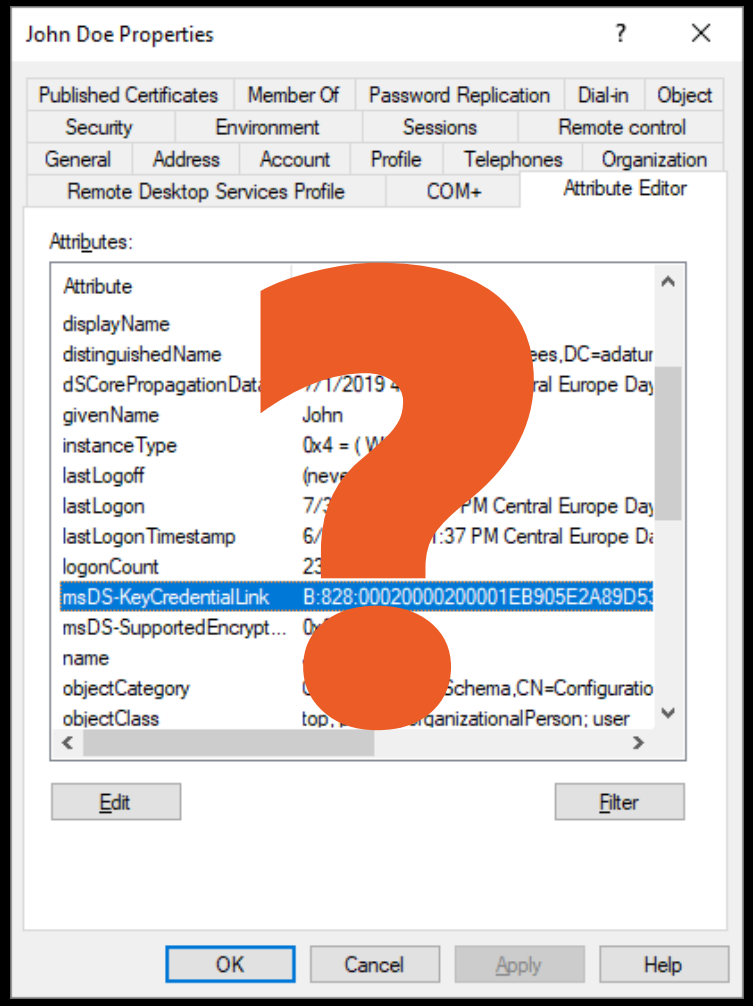
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export

Filters: Product: Defender for Identity

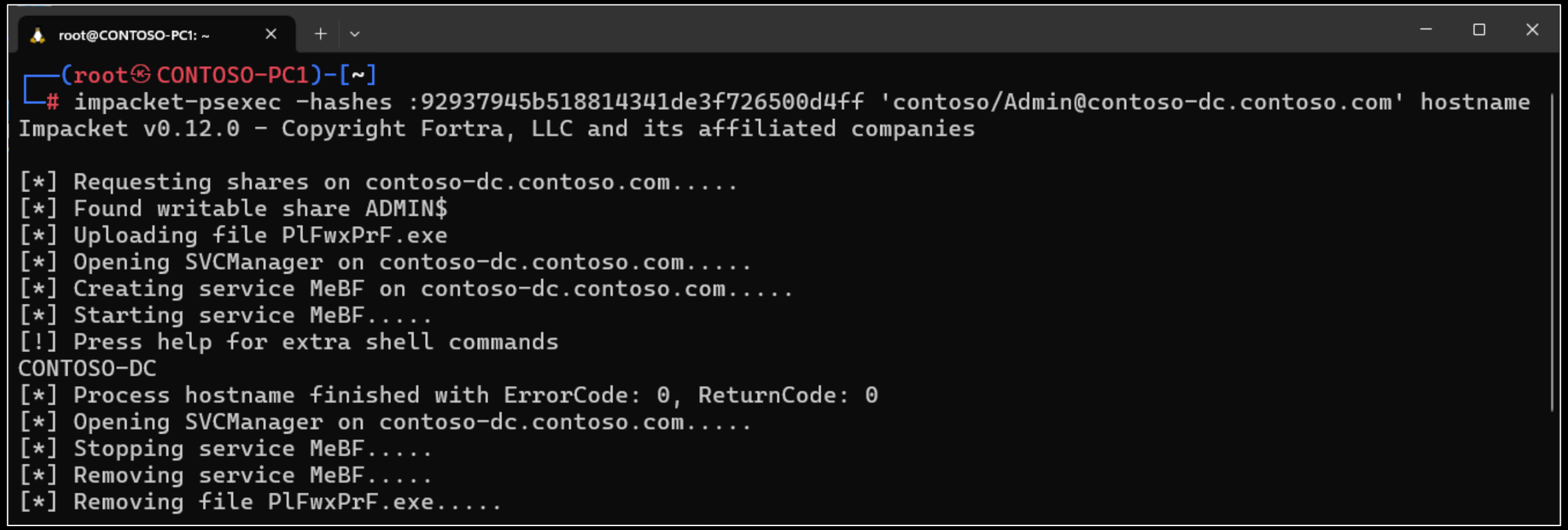
	Rank	Recommended action	Score impact	Points achieved	Status
☐	2	Prevent Certificate Enrollment with arbitrary Application Policies (ESC15)	+1.54%	0/5	To address
☐	3	Prevent users to request a certificate valid for arbitrary users based on the certificate template (ESC1)	+1.54%	0/5	To address
☐	17	Edit insecure certificate enrollment IIS endpoints (ESC8)	+1.54%	5/5	Completed
☐	18	Enforce encryption for RPC certificate enrollment interface (ESC8)	+1.54%	5/5	Completed
☐	19	Edit vulnerable Certificate Authority setting (ESC6)	+1.54%	5/5	Completed
☐	20	Edit misconfigured Certificate Authority ACL (ESC7)	+1.54%	5/5	Completed
☐	21	Edit misconfigured certificate templates owner (ESC4)	+1.54%	5/5	Completed
☐	22	Edit overly permissive Certificate Template with privileged EKU (Any purpose EKU or No EKU) (ESC2)	+1.54%	5/5	Completed
☐	23	Edit misconfigured enrollment agent certificate template (ESC3)	+1.54%	5/5	Completed
☐	24	Edit misconfigured certificate templates ACL (ESC4)	+1.54%	5/5	Completed

Credential Access – Shadow Credentials Attack

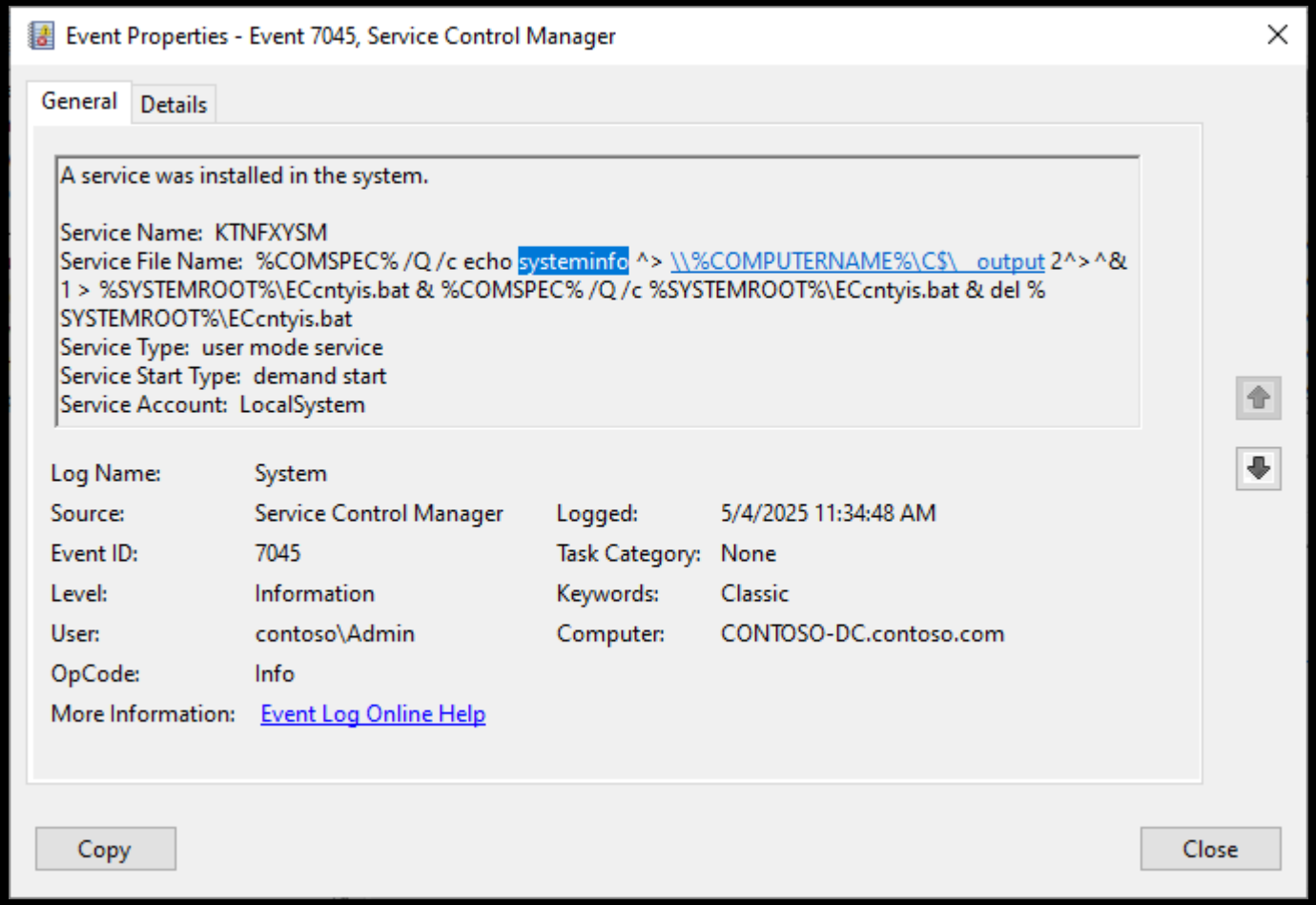


Lateral Movement

Lateral Movement – Pass-the-Hash Attack



Lateral Movement – Remote Code Execution



Lateral Movement – Pass-the-Hash Attack

What happened

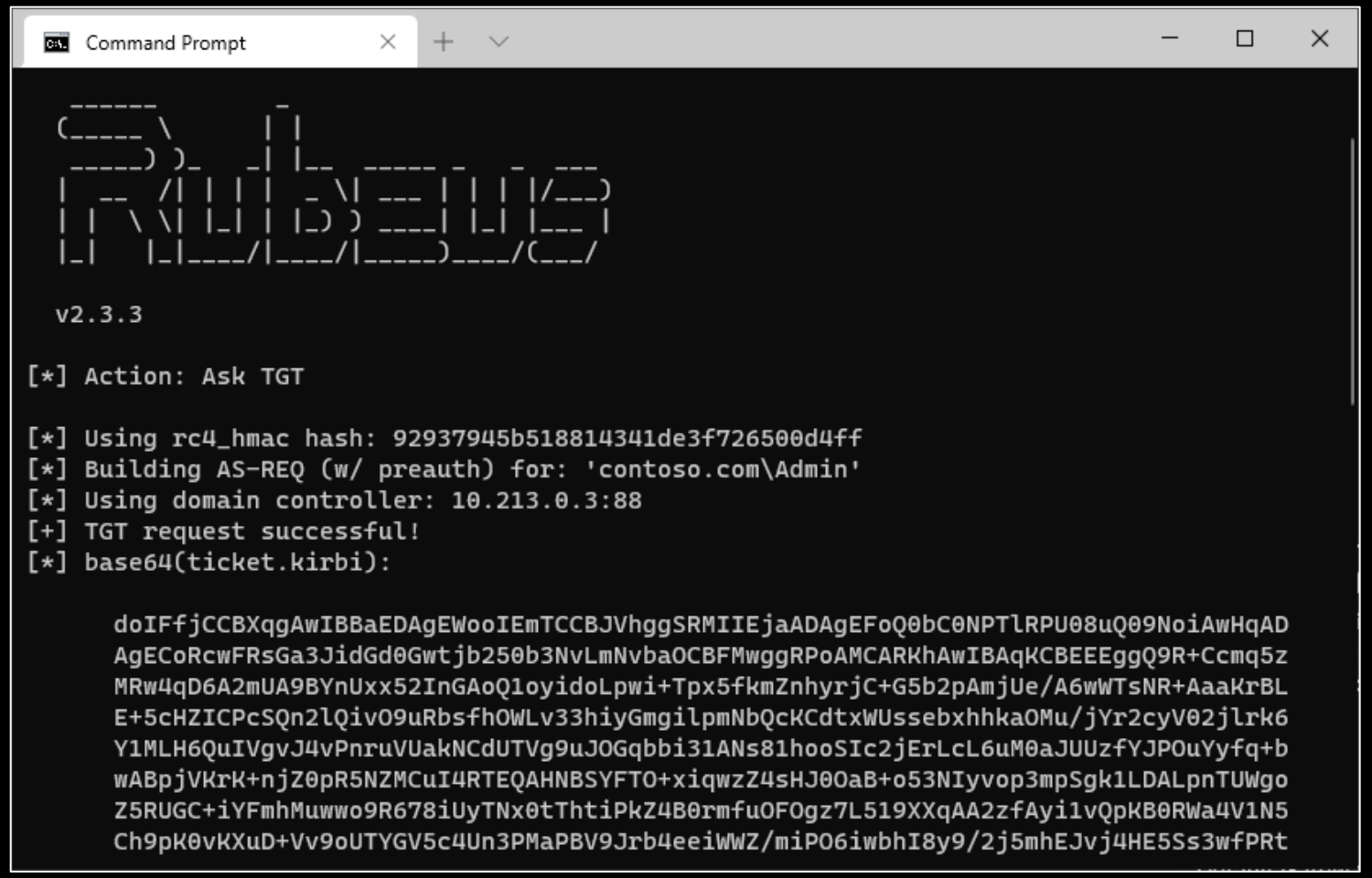
Admin created KIKyqutX in order to execute potentially malicious commands on CONTOSO-DC.

Alert graph

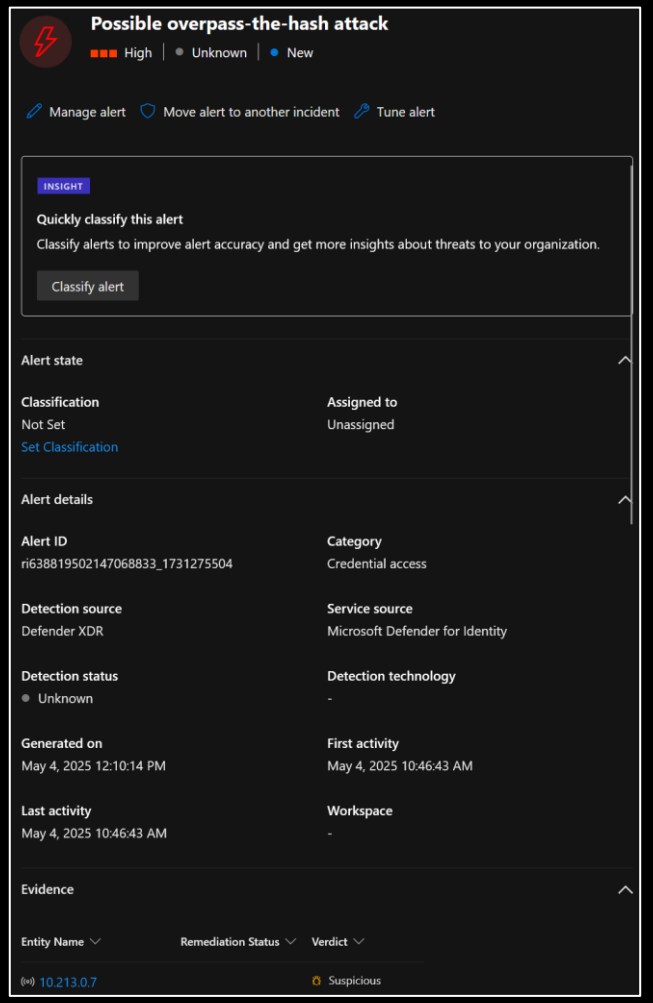
Important information

- Admin created services on CONTOSO-DC during the 30 days before this suspicious activity occurred.
- Admin not previously observed logging into CONTOSO-DC during the 30 days before this suspicious activity occurred.

Lateral Movement – Overpass-the-Hash Attack



Lateral Movement – Overpass-the-Hash Attack



Lateral Movement – Remote Code Execution

root@CONTOSO-PC1: ~

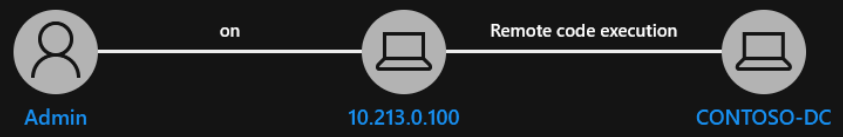
```
└─# impacket-wmiexec -hashes :92937945b518814341de3f726500d4ff 'contoso/Admin@contoso-dc.contoso.com' systeminfo
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used

Host Name:                 CONTOSO-DC
OS Name:                   Microsoft Windows Server 2022 Standard
OS Version:                10.0.20348 N/A Build 20348
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          NA
Registered Organization:   vm.net
Product ID:                00454-10000-00001-AA653
Original Install Date:     5/2/2025, 8:33:23 PM
System Boot Time:          5/3/2025, 9:33:46 PM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2200 Mhz
```

Lateral Movement – Remote Code Execution

What happened

Admin made 3 attempts to run commands remotely on CONTOSO-DC from 10.213.0.100 using WMI.

Alert graph



Important information

- Admin not previously observed logging into 10.213.0.100 during the 30 days before this suspicious activity occurred.

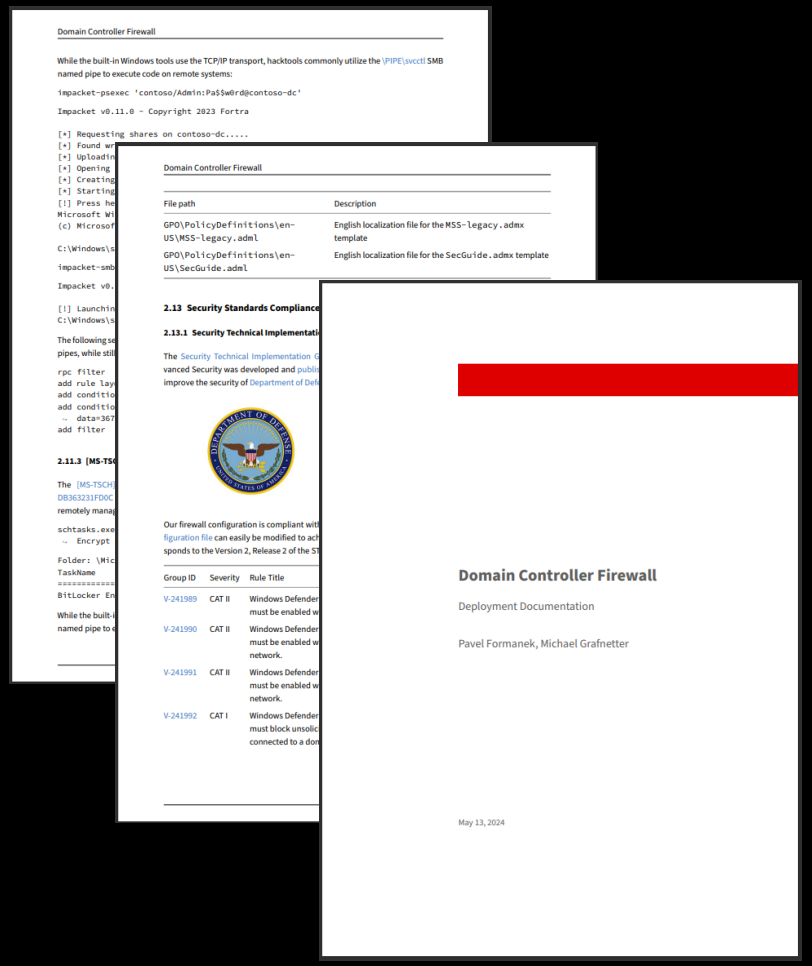
Remote code execution attempted:

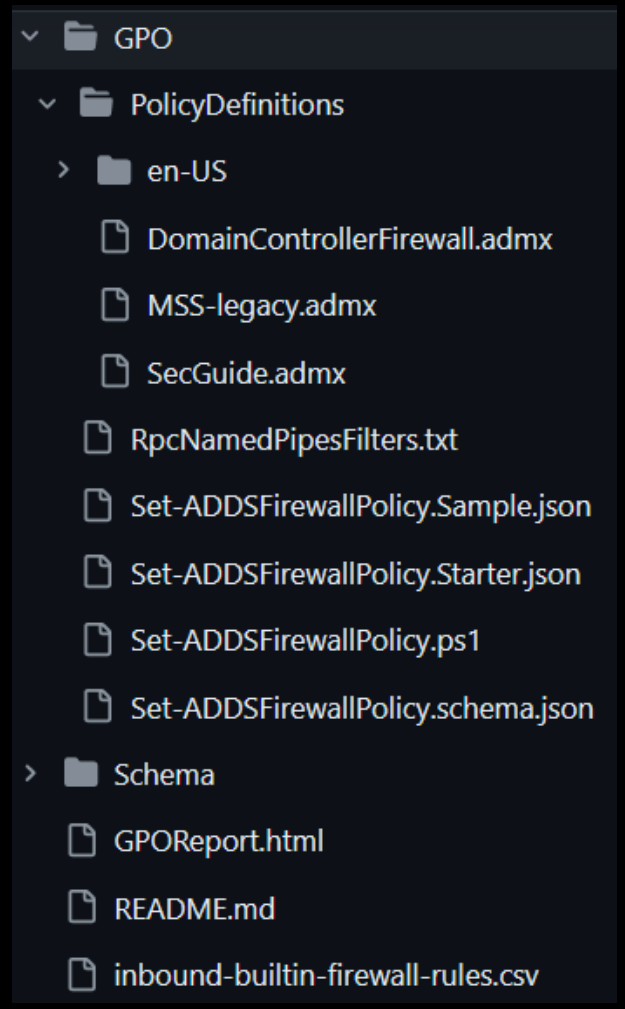
- May 4, 2025 11:31 AM
  User Admin attempted to execute Win32_Process Create (cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$__1746351090.710315 2>&1) on CONTOSO-DC via Wmi. The remote execution succeeded.
- May 4, 2025 11:31 AM
  User Admin attempted to execute Win32_Process Create (cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1746351090.710315 2>&1) on CONTOSO-DC via Wmi. The remote execution succeeded.
- May 4, 2025 11:31 AM
  User Admin attempted to execute Win32_Process Create (cmd.exe /Q /c hostname 1> \\127.0.0.1\ADMIN$__1746351090.710315 2>&1) on CONTOSO-DC via Wmi. The remote execution succeeded.

DEMO

Remote Code Execution

Side Note: Domain Controller Firewall



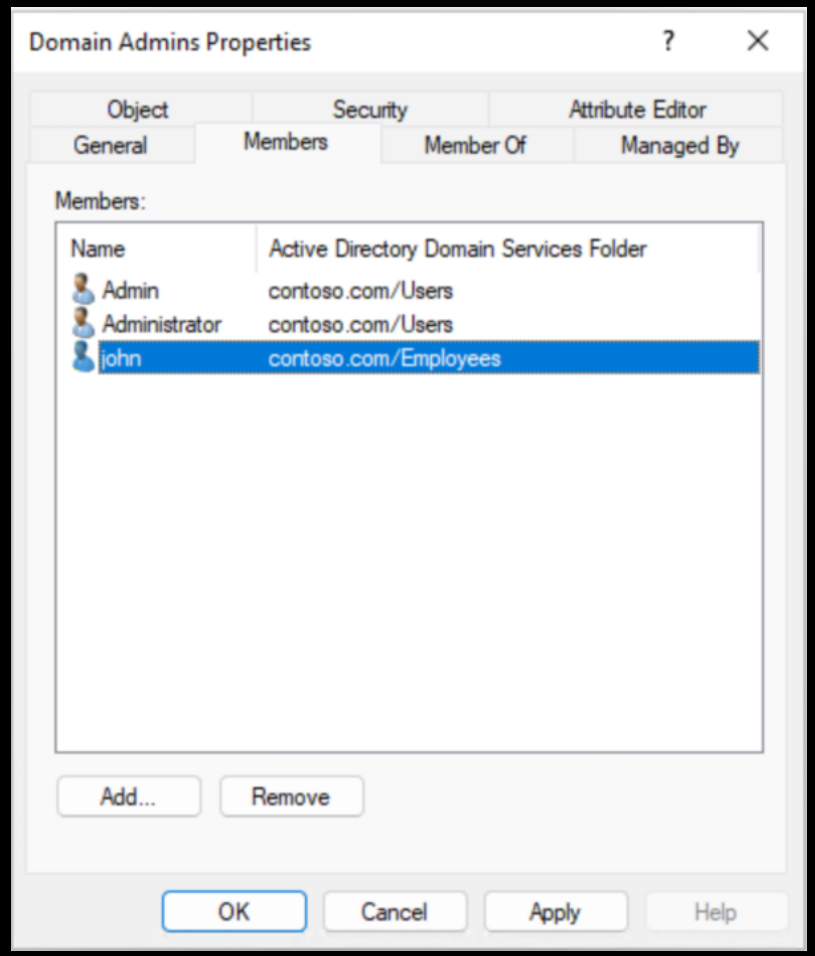


firewall.dsinternals.com

CQURE

Active Directory
Persistence

Persistence – Domain Admins Membership

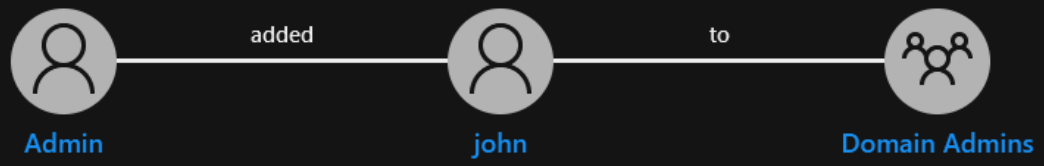


Persistence – Domain Admins Membership

What happened

Admin added john to the sensitive Domain Admins group.

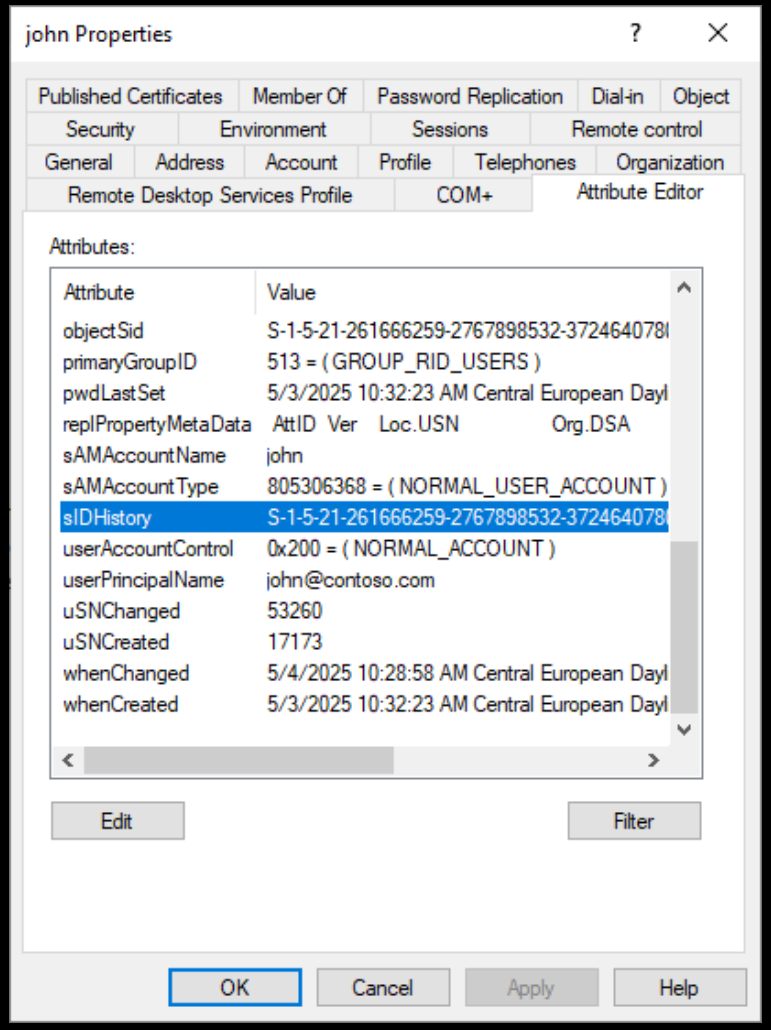
Alert graph

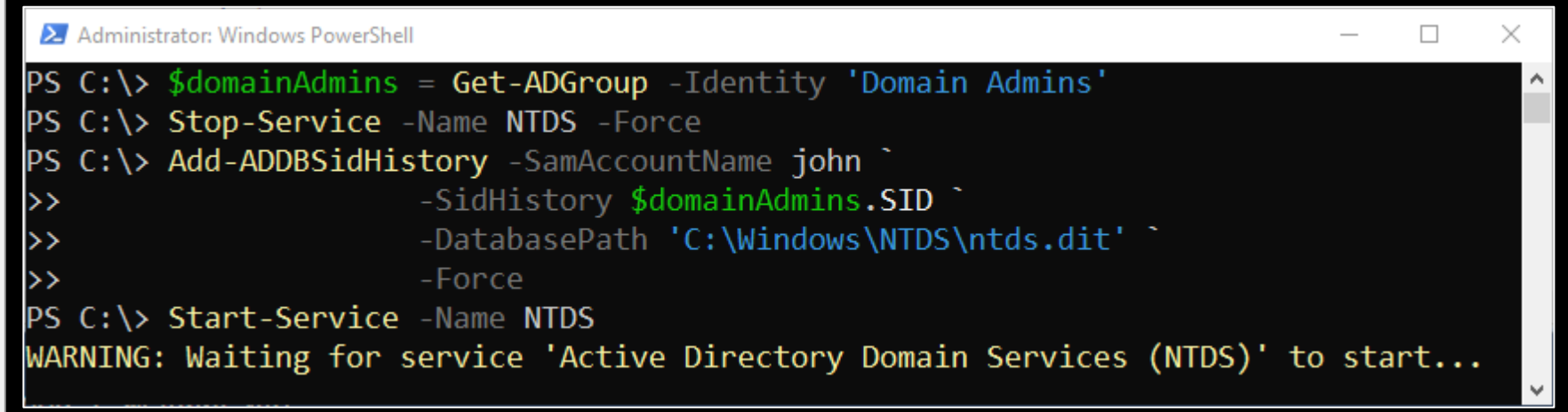


Important information

- Group additions made on CONTOSO-DC.
- Admin was not observed adding members to sensitive groups during the 30 days before this suspicious activity occurred.
- In the 2 days prior the addition, Admin was observed logging into 7 computers.

Persistence – SID History Injection



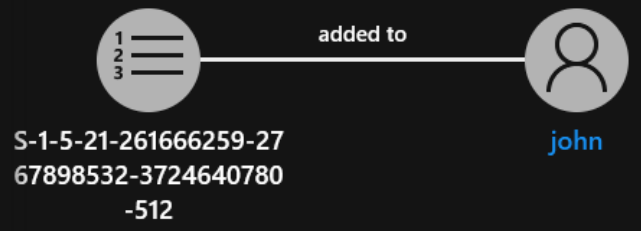


Persistence – SID History Injection

What happened

S-1-5-21-261666259-2767898532-3724640780-512 injected into the SID-History attribute of john.

Alert graph



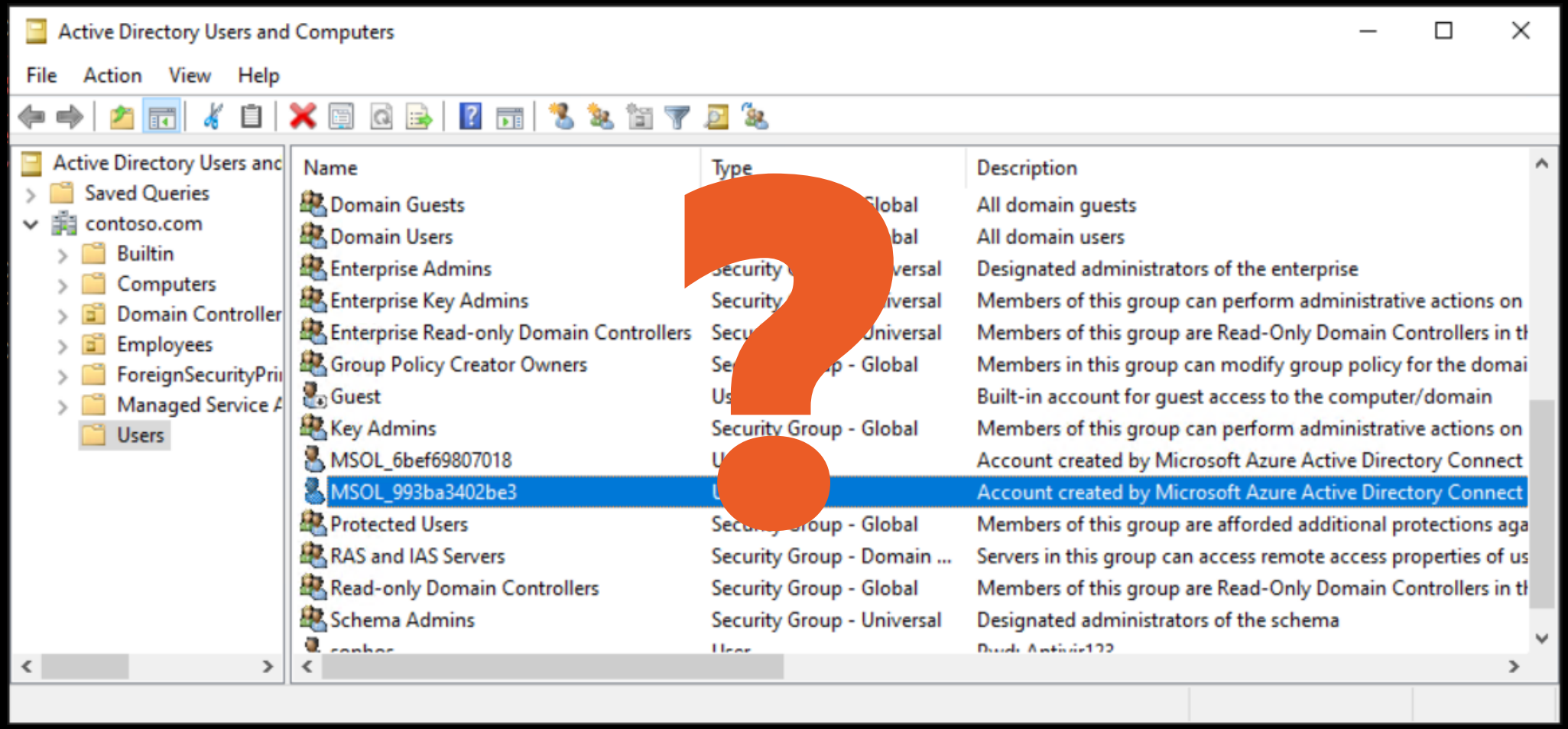
Important information

- May 4, 2025 10:28 AM - May 4, 2025 10:28 AM
  S-1-5-21-261666259-2767898532-3724640780-512 providing privileges of Domain Admins added to the SID-History attribute of john.

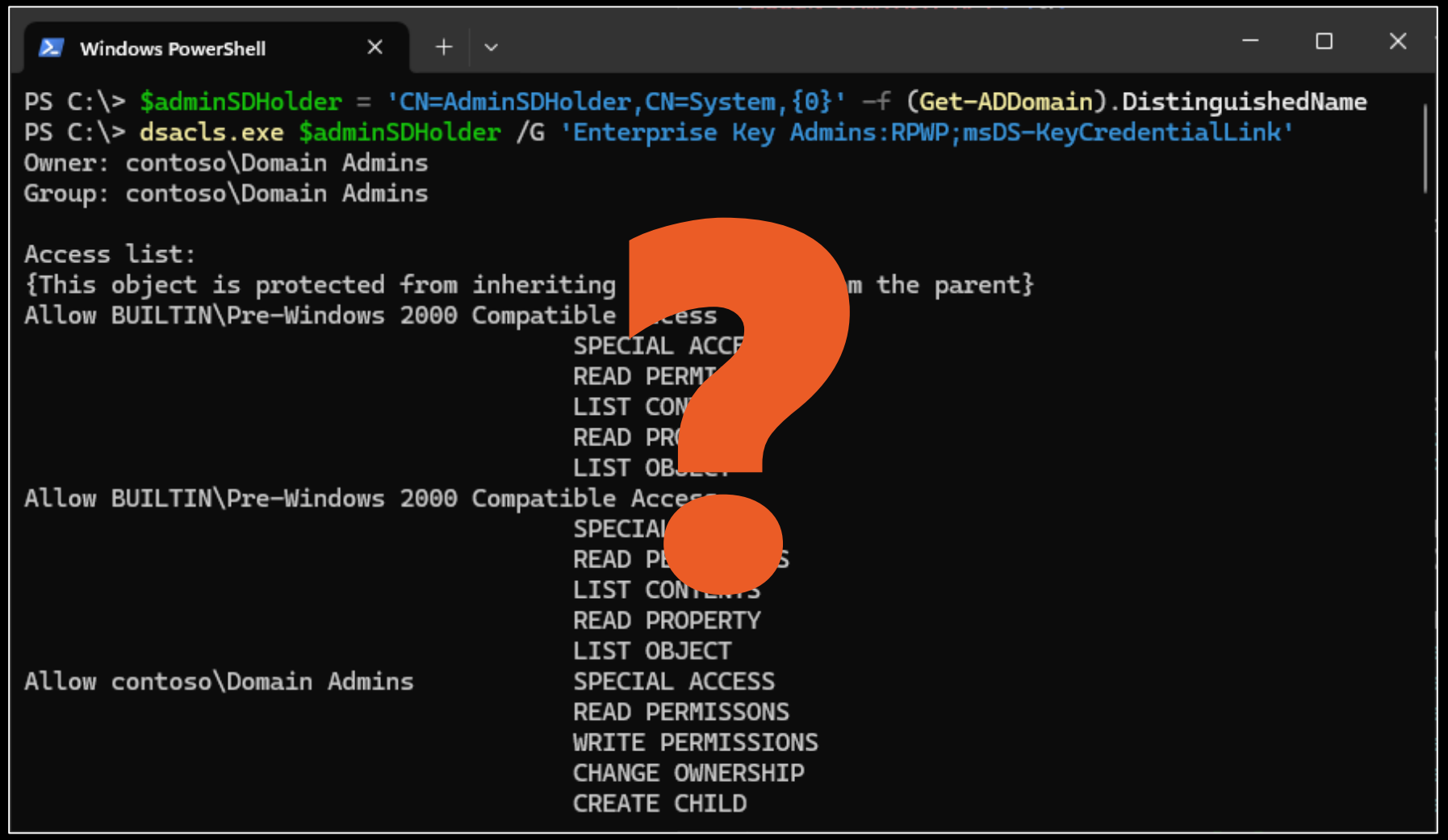
Same-domain SIDs: The SID-History attribute is expected to contain SIDs from different domains so as to support account migration between domains.

- The injected SID S-1-5-21-261666259-2767898532-3724640780-512 is providing privileges of Domain Admins in john's domain.

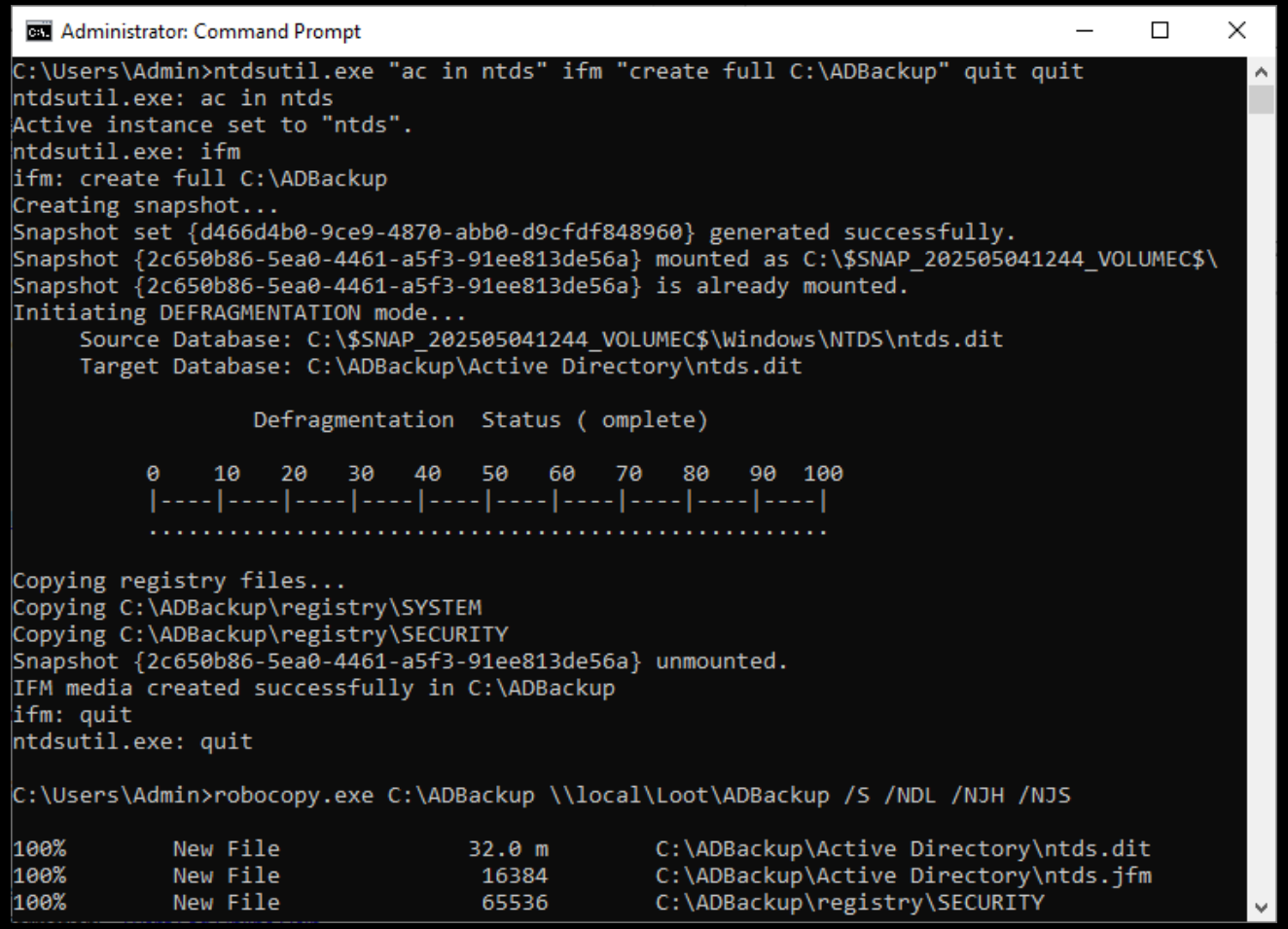
Persistence – Duplicate AD Connect Account



Persistence - AdminSdHolder ACL Modification



Data Exfiltration over SMB – ntds.dit



Data Exfiltration over SMB – ntds.dit

What happened

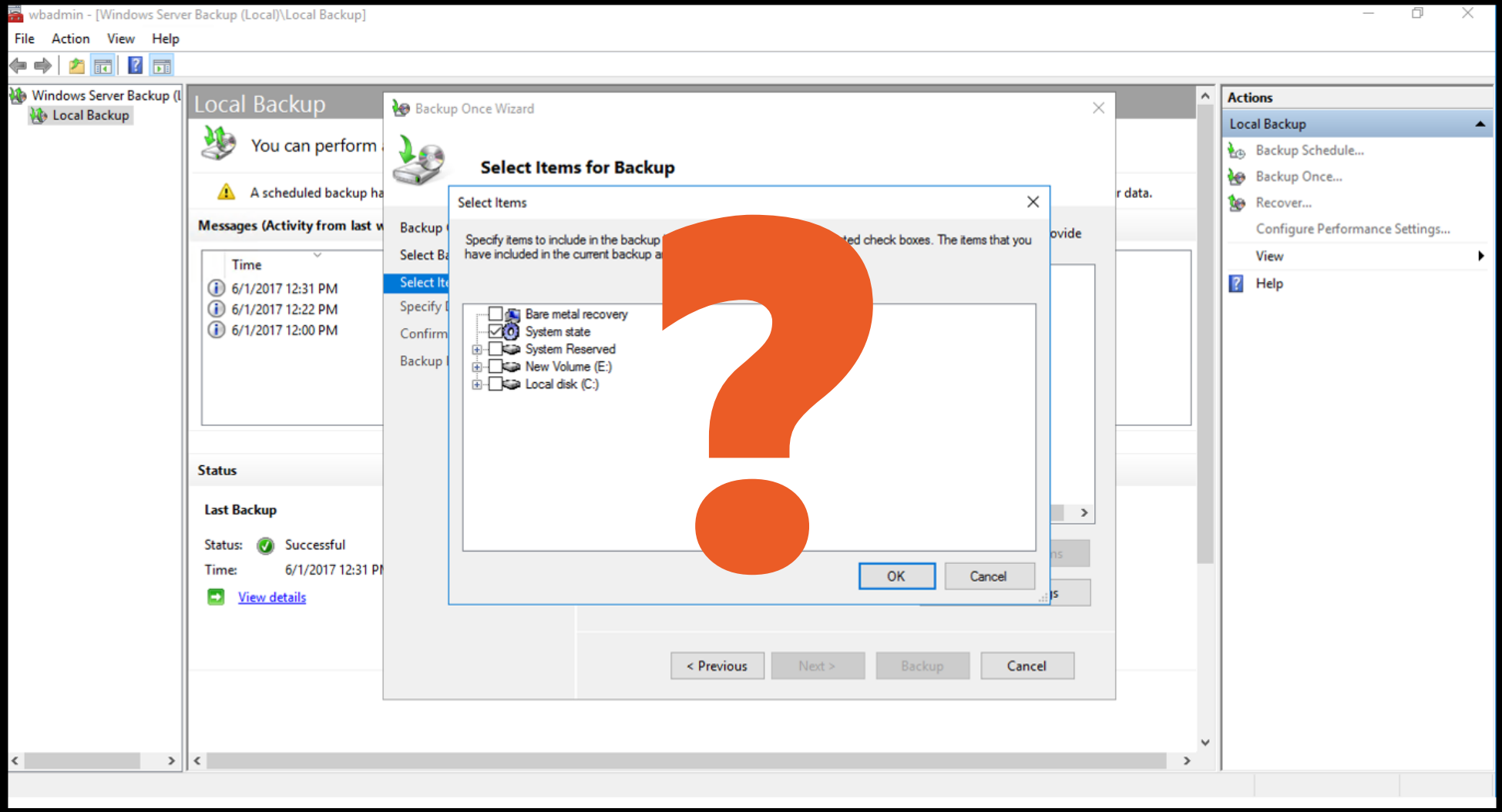
Admin on CONTOSO-DC suspiciously copied files to GRAFVM-W2K22.

Alert graph

Important information

- ADBackup\Active Directory\ntds.dit, size: 32.0 MB was copied.

Data Exfiltration over SMB – Windows Backup

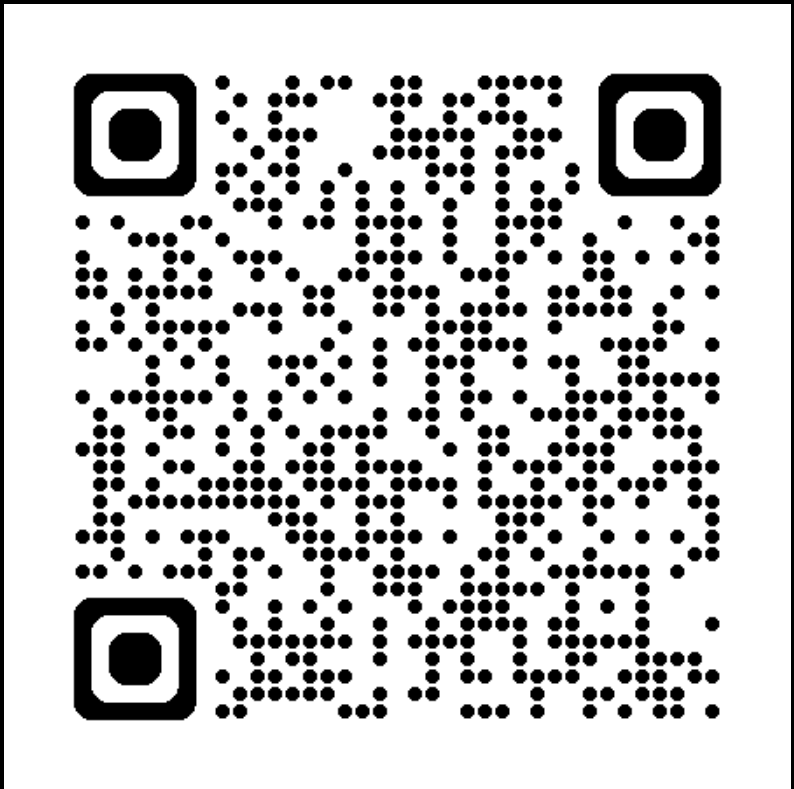


Other Detection Examples

- Modification of a sAMAccountName (CVE-2021-42278)
- Skeleton key attack
- Suspicious modification of the trust relationship of AD FS server
- Remote code execution attempt over DNS
- Exchange Server Remote Code Execution (CVE-2021-26855)
- Use of Metasploit hacking framework
- DCShadow Attack
- Suspicious VPN connection
- Disable of audit filters of AD CS
- Group Policy Tampering
- Okta account Enumeration
- Password spray against OneLogin

...

Get to know us better!



Scan the QR code or visit
https://cqureacademy.com/msd25
to get access to this presentation
and find out more about CQURE!

Active Directory
Under Attack

Michael Grafnetter

@MGrafnetter

www.dsinternals.com

Microsoft MVP Most Valuable Professional

SwissMicrosoft SECURITY SUMMIT

COURE