

# Defend Your Organization from Identity-Based Attacks with Microsoft Defender for Identity



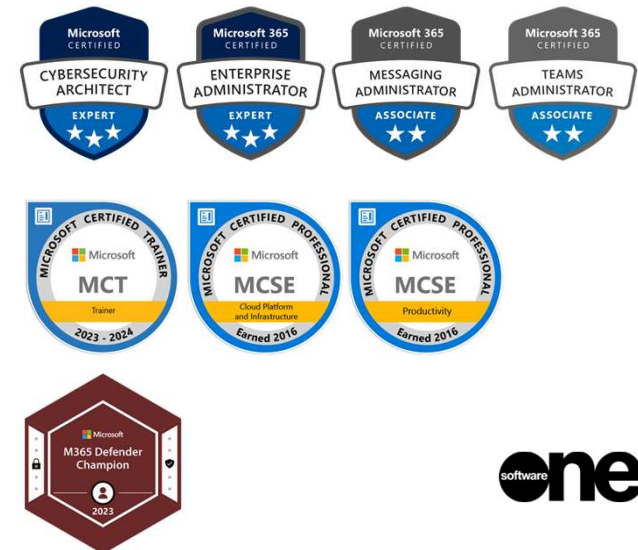
March 19 2024

# software one step ahead.



Erik Stiphout

Sr. Consultant Digital Workplace

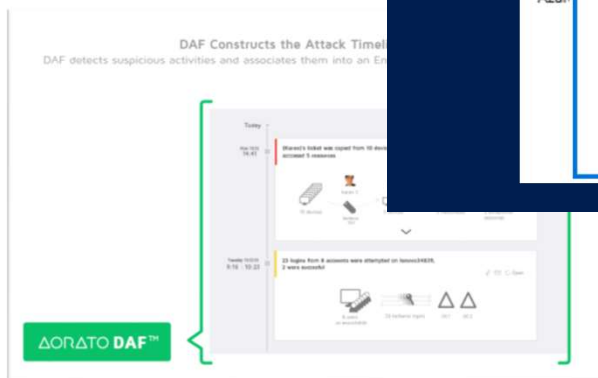
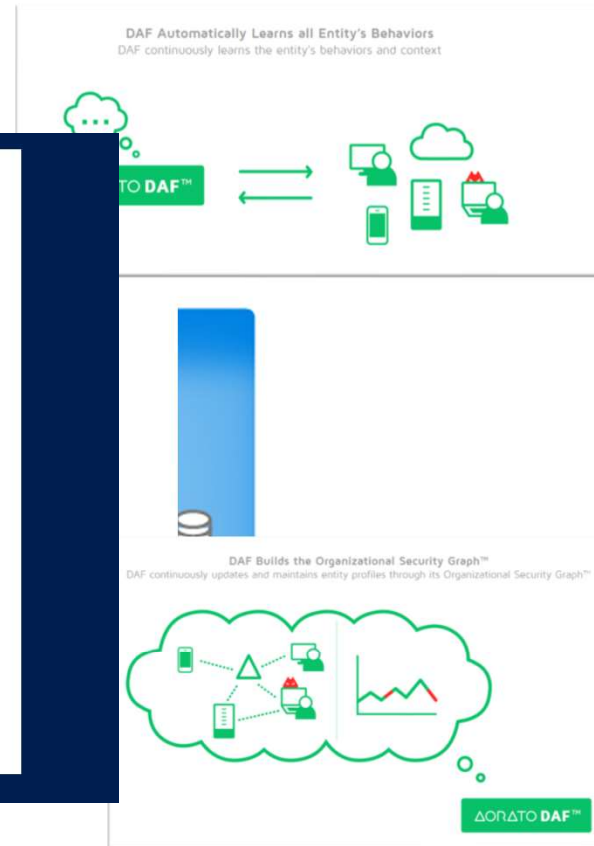
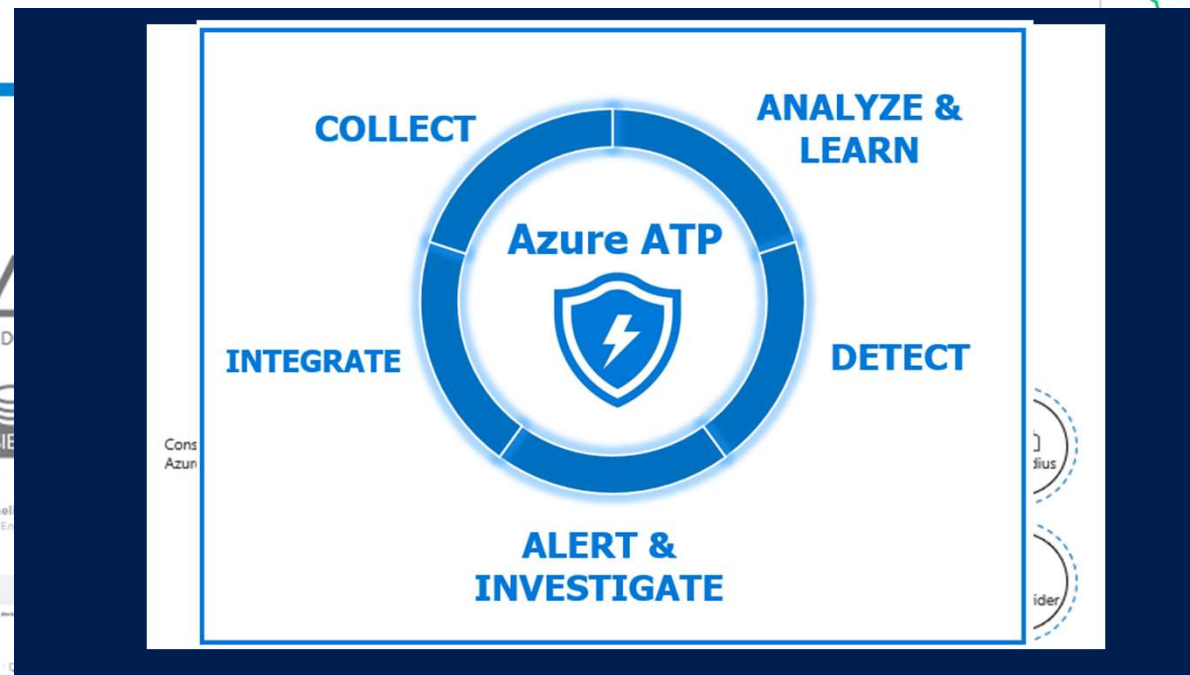


# Before we start a quick question

By a show of hands

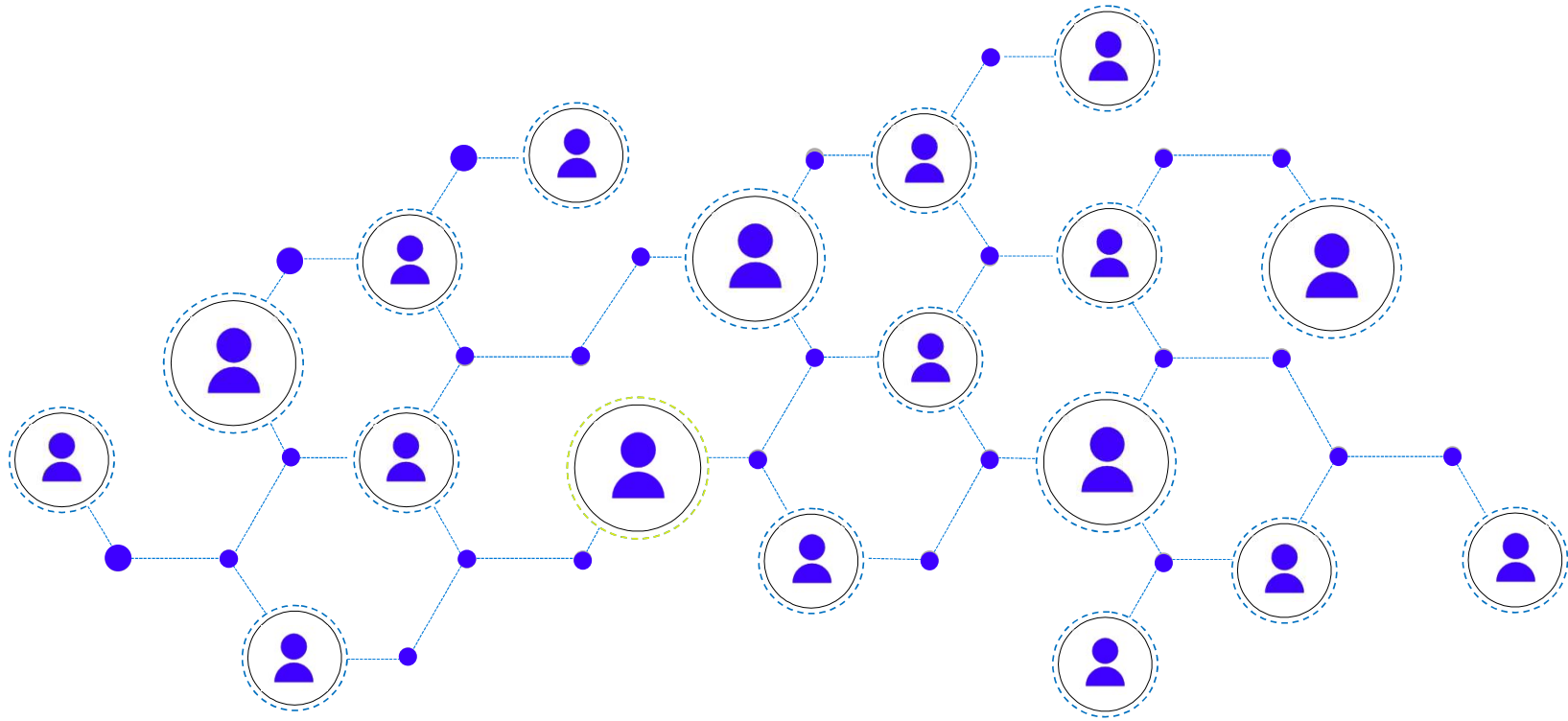


# Starting with a bit of history



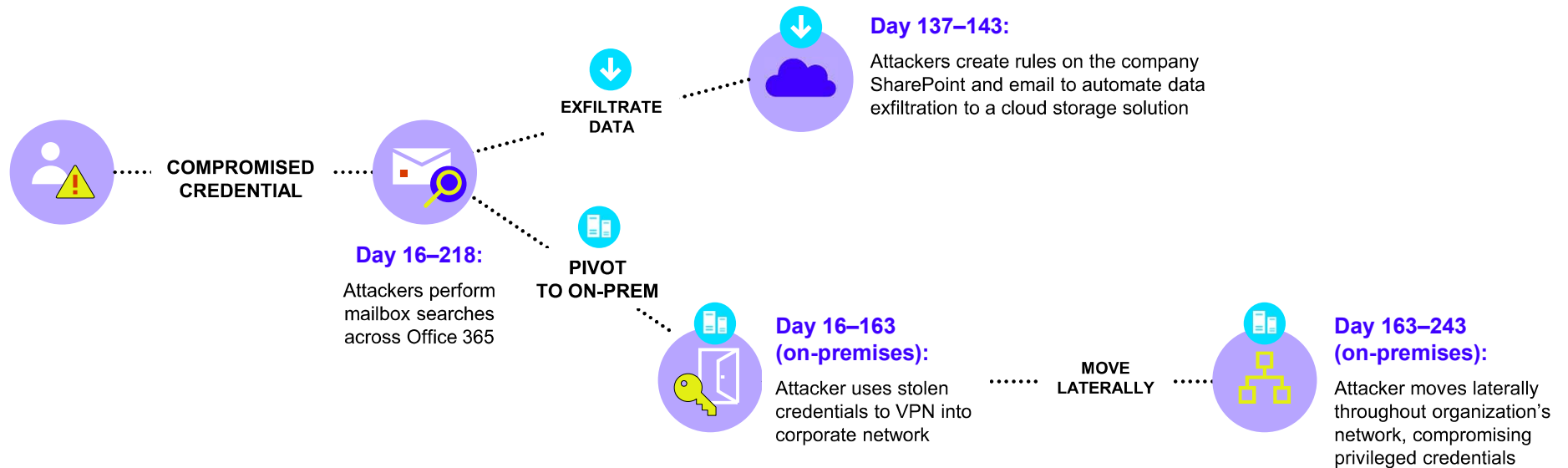
# User Identity as a security perimeter

We're only a single compromised user away from a business' shutdown.

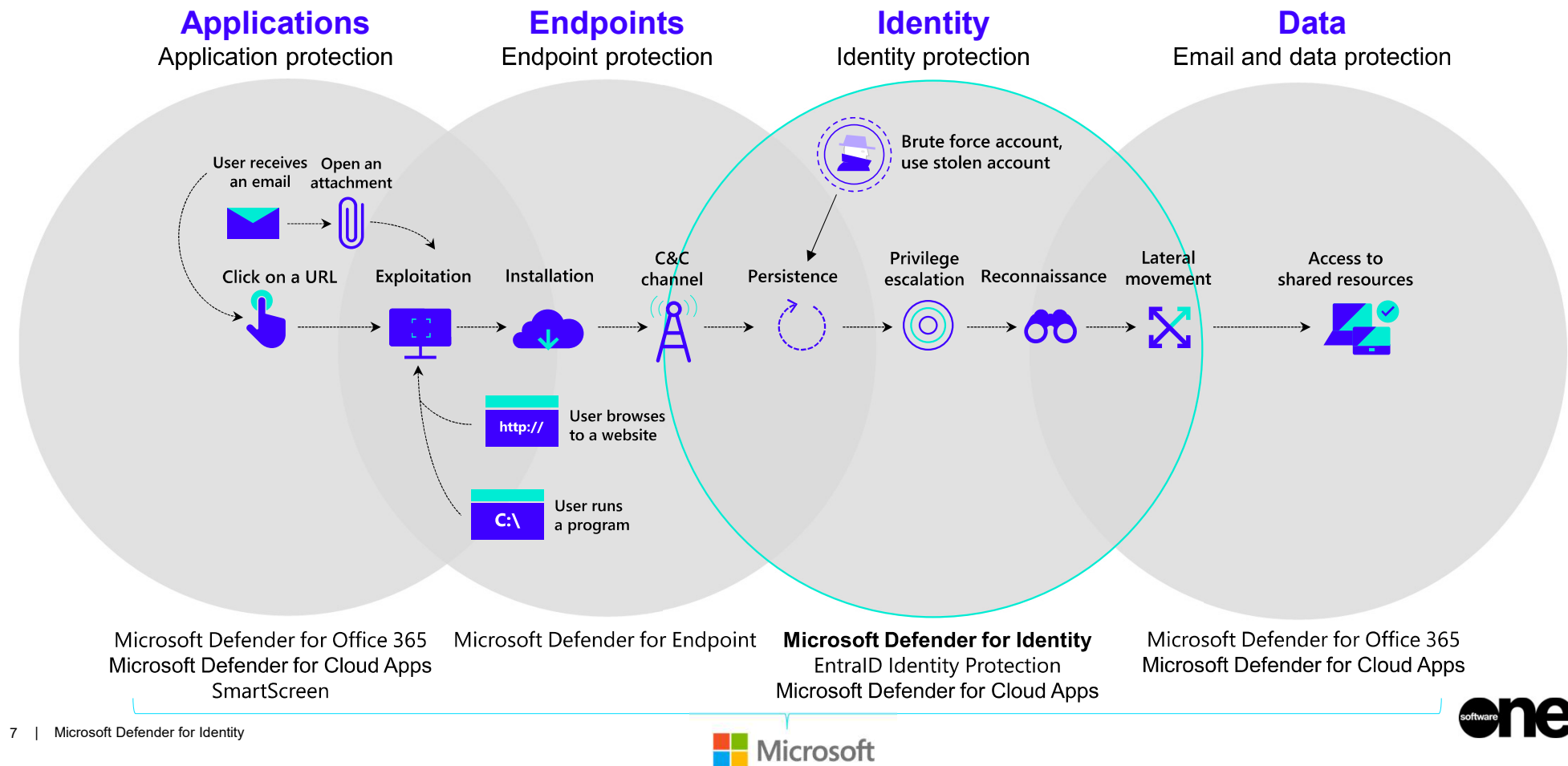


# Why Microsoft Defender for Identity matters

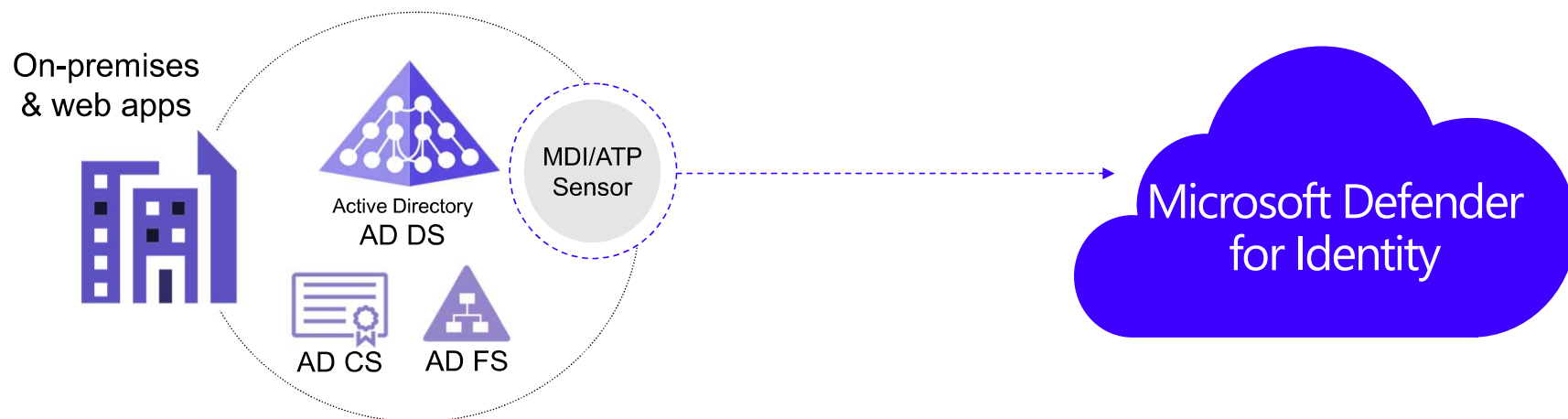
One example of how an attack happens and compromises an entire organization.



# Fitting in identity protection across the IT landscape



# Overview of Microsoft Defender for Identity capabilities



## Network traffic analytics

Inspect network traffic:  
NTLM, Kerberos, LDAP,  
RPC, DNS, SMB

## Security events and Active Directory data

Inspect events, event  
tracing and profile active  
directory entities

## User behavior analytics

Profile users & entities  
behavior, identify  
behavior anomalies

## Cloud based real-time detections

Data enrichment and  
correlation in the cloud, for  
real time detections



# MDI Detection capabilities of On-premises Identity Attacks

Account enumeration

Security principal enumeration (LDAP)

Users group membership enumeration

Users & IP address enumeration

Hosts & server name enumeration (DNS)

Resource access suspicious activities

NTLM Relay & NTLM tampering

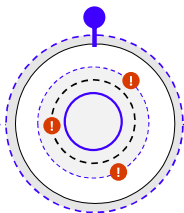
Pass-the-Ticket

Pass-the-Hash

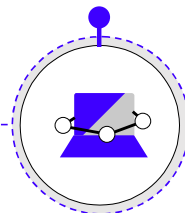
Overpass-the-Hash

Suspicious groups membership changes

## Reconnaissance



## Lateral movement



## Credential access

Brute force attempts

Suspicious VPN connection

Honey Token account suspicious activities

Logon/Failed logon suspicious activities

## Persistence

Golden ticket attack

DCShadow, DCSync

Data exfiltration

Code execution/Service creation on DC

SMB packet manipulation

Skeleton Key

# Getting started with Microsoft Defender for Identity

Topics to think about and discuss with the security- and networking-teams

- What Sensor type to install (direct install or standalone);
- Server Sizing and capacity planning;
- Multi-forest deployment;
- Use a “regular” service account or gMSA as a Directory Service account (DSA).

# Who gets to use Microsoft Defender for Identity



Hang on! We're preparing your  
Microsoft defender for identity  
workspace



# Taking care of the pre-requisites (1/2)

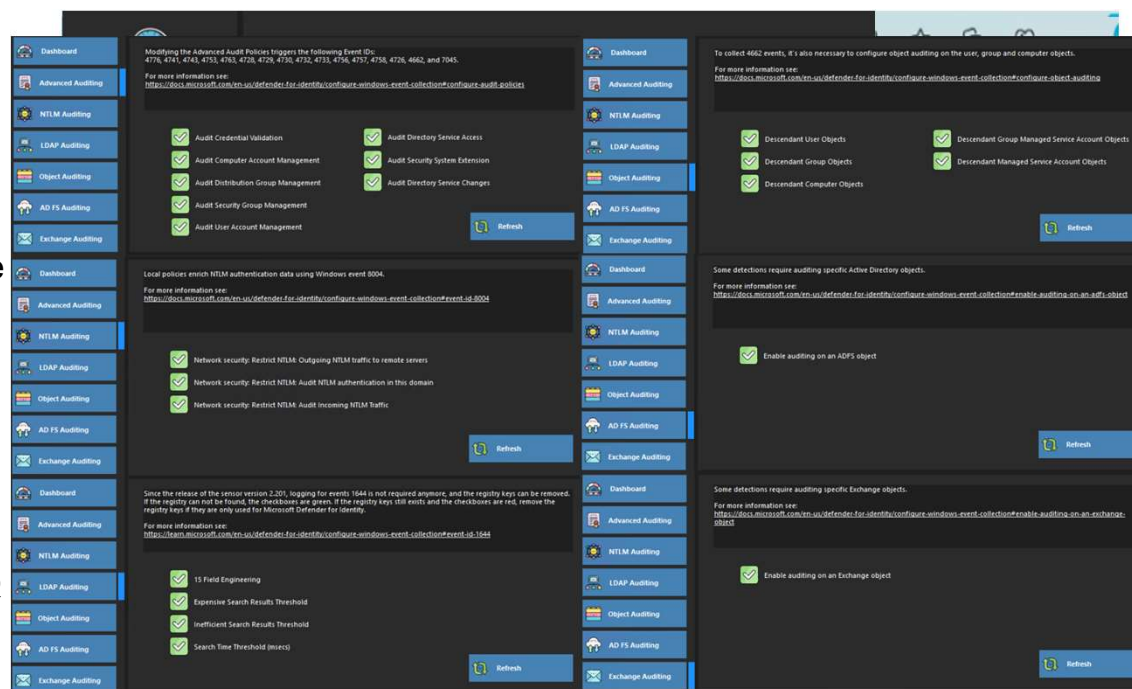
## Readiness and policies

- First run the Test-MDlreadiness script available under Tools on the Defender portal
- Setup of Auditing and settings can be done manually in your own group policies or....
- Released this year, is a PowerShell Module which can be found under the tools section of the Identities menu on the Microsoft Defender Portal which takes out a lot of the manual configuration.

<https://www.powershellgallery.com/packages/DefenderForIdentity/>

- Verification with of settings can be done with the readiness script or a 3<sup>rd</sup> party (home brew) executable @

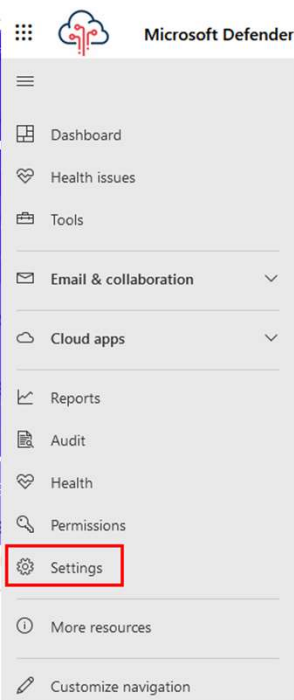
<https://github.com/thalpius/Microsoft-Defender-for-Identity-Configuration-Checker>



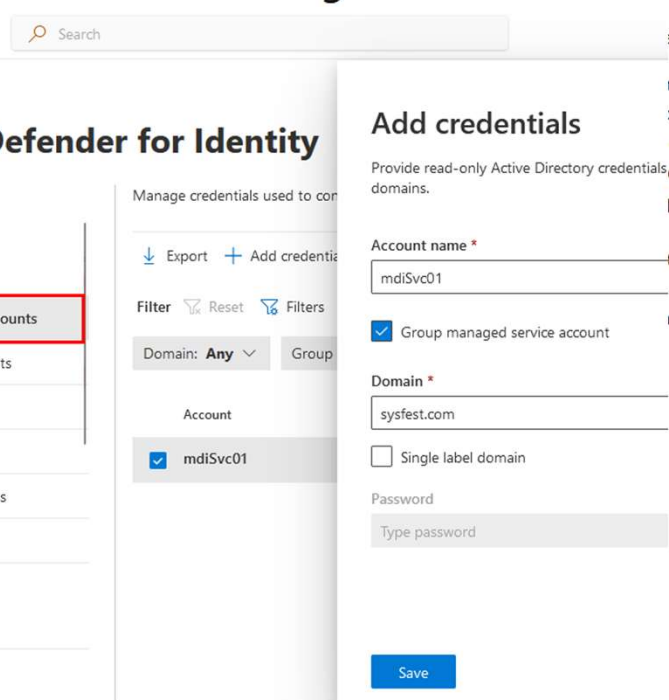
# Taking care of the pre-requisites (2/2)

## Directory Services Account (DSA)

```
Next you need to install the sensor.
will have a sensor.
# Get the deleted objects
# Install the gMSA account
# Install ADServiceAccount
# Take ownership on the vds
$params = @"($deletedObject)
C:\Windows\System32\dsac1
Regular user account
# Grant the 'List Content'
user or group:
$params = @"($deletedObject)
C:\Windows\System32\dsac1
$gmsa_Name.Senv:USERMSR
KerberosEncryptionType:AES
-PrincipalsAllowedToRetri
both the
```



## Benefits of gMSAs



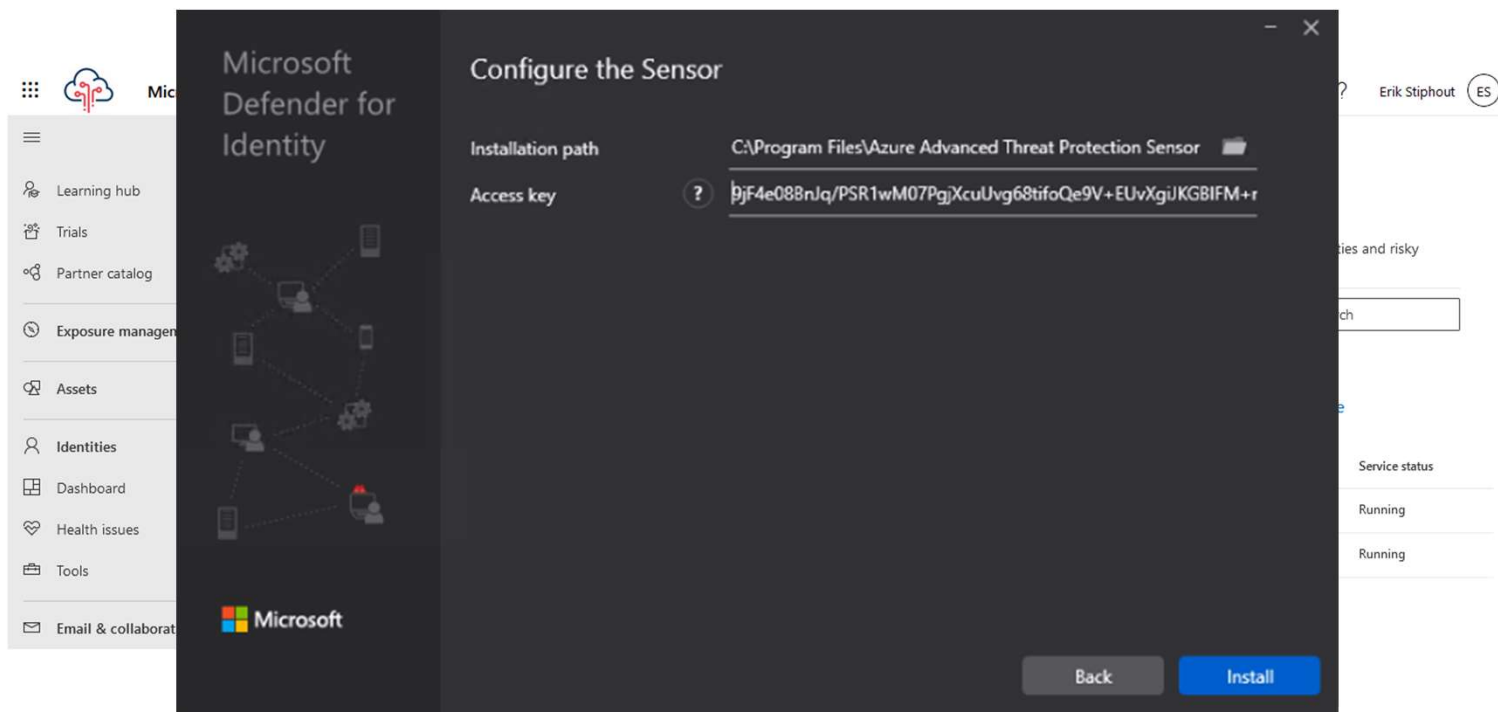
administrative overhead:

- reduces the complexity and length of gMSA passwords
- reduces binary attacks
- reduces the Windows OS, which changes the password every
- reduces the number of password changes, or manage service outages.
- reduces the number of servers to support load balanced solutions where

t - set up an SPN with PowerShell, when you create

is might do so against the gMSA, if the gMSA

# Installing the MDI sensor(s)



# Checking if the sensor is alive

Services

File Action View Help

## Microsoft Defender for Identity

General

Sensors

Directory services accounts

Manage action accounts

VPN

Health issues

Adjust alerts thresholds

About

Deploying sensors enables you to monitor your on-premises Active Directory environment for suspicious activities and risky configurations. [Learn more](#)

Export Add sensor

Filter Reset Filters

Type: Any Domain: Any Delayed update: Any Service status: Any Sensor status: Any Health status: Any

Sensor	Type	Domain	Service status	Sensor status	Version	Delayed update	Health status
<input type="checkbox"/> DC01	Domain controller Sensor	sysfest.com	Running	Up to date	2.232.17747.34902	Disabled	Healthy
<input type="checkbox"/> FS01	AD FS Sensor	sysfest.com	Running	Up to date	2.232.17747.34902	Disabled	Healthy

Background Intelligent Transfer Service

Background Tasks Infrastructure Service

Base Filtering Engine

BitLocker Drive Encryption Service

Bluetooth Support Service

Transfers fil...

Windows in...

The Base Fil...

BDESVC hos...

The Bluetoo...

Running

Running

Automatic

Manual (Trig...

Manual (Trig...

Automatic (D...

Automatic

Automatic

Local (Trig...

Local (Trig...

Local Syste...

Local Syste...

Local Service

Local Syste...

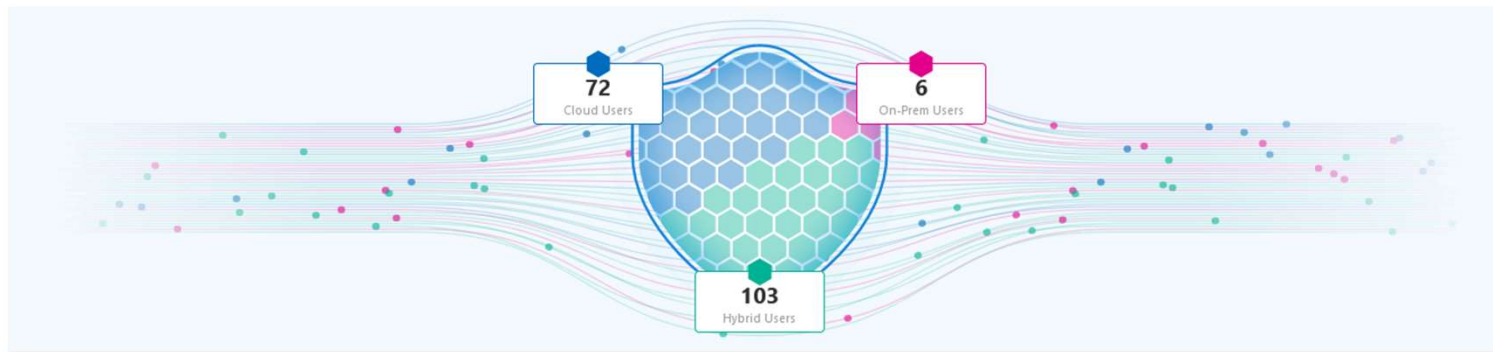
Local Service

15 | Microsoft Defender for Identity

<https://learn.microsoft.com/en-us/defender-for-identity/troubleshooting-known-issues>

## ITDR Dashboard

This dynamic dashboard is offering a centralized view of critical insights and real-time data about identity threat detection and response. By providing an intuitive interface that showcases important information related to unauthorized access, account compromise, insider threats and abnormal activities, our dashboard enables you to proactively monitor and manage potential identity-related security risks.



### Top insights

 0 users were identified in a risky lateral movement path

 0 users are considered dormant in AD

#### ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Entra ID Protection.

##### Deployment

MDI sensors deployment on domain controllers 1 / 1

##### MDI health alerts

Low Medium High 1 more

##### License

Defender for Identity  
**Available**

Entra ID Protection  
**Available**

##### Quick guides

[What is Microsoft Defender for Identity?](#)

#### Identity posture (Secure score)

**Identity: 65.18%**

Identity secure score is a representation of your organisation's identity security posture and your opportunity to improve it.



#### Highly privileged identities

2 Entra ID Global Admin 0 Entra ID Security Administrator 3 Tagged as sensitive

User name	Source	Type	Role / Tag
Nilda Figgs	Hybrid	User	Sensitive
Chris Green	Cloud	User	Global admin
Erik Stiphout	Cloud	User	Global admin

#### Identity related incidents

3 incidents

High (3)

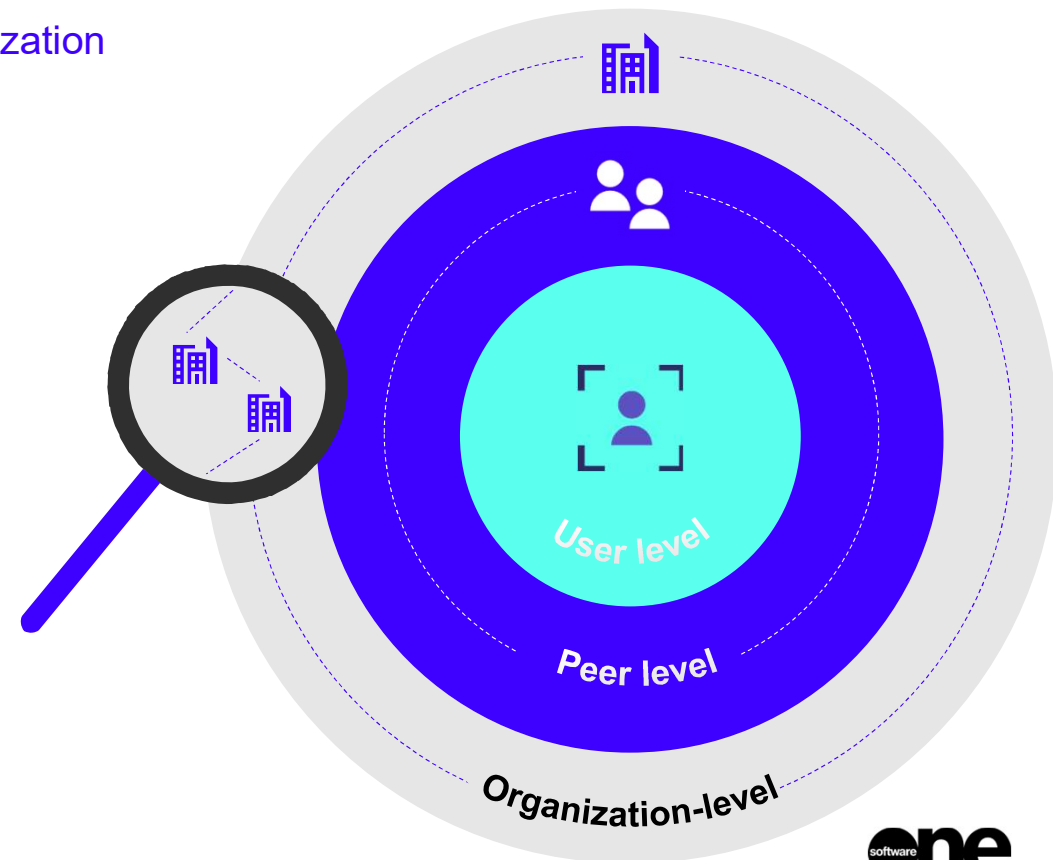
Incident name	Severity	Active alerts	Scope	Last Activity
Multi-stage incident involving Credential access...	High	2/2	1 1 0	Mar 18, 2024 11:...
Suspected DCSync attack (replication of directo...	High	1/1	1 1 0	Mar 18, 2024 12:...
Honeytoken user attributes modified involving ...	High	2/2	0 3 0	Mar 16, 2024 11:...



# End-user behavior analysis by the MDI Sensor

## Activity Behavior Analysis by User, Peers, and Organization

- Login to devices
- Access to on-premises resources
- Remote connections to servers
- Access to cloud applications
- Usage of SharePoint Online sites
- User agent, location & ISP analytics
- Mailbox behavior
- Failed logins behavior



# Suspicious Activity Analysis

Example: User accesses the 'finance' server.

Is the 'finance server' accessed by many users in the organization?

Has this user accessed this server before?

Does this user have a usual pattern of logons to servers?

Do the peers of this user login to this server?

Normal

Suspicious



# Microsoft Defender for Identity settings

## Microsoft Defender for Identity

Directory services accounts

Manage action accounts

VPN

Health issues

Adjust alerts thresholds

About

Entity tags

Sensitive

Honeytoken

Exchange server

Actions and exclusions

Global excluded entities

Exclusions by detection rule

Automated response exclusions

Notifications

Health issues notifications

Alert notifications

Syslog notifications

Exclude entities by detection rule

65 items [Customize columns](#)

Detection rule	Excluded entities
Abnormal ADFS authentication using a suspicious certificate	-
Suspected overpass-the-hash attack (Kerberos)	-
Suspected NTLM authentication tampering	-
Suspicious additions to sensitive groups	-
Suspected brute-force attack (SMB)	-
Suspected use of Metasploit hacking framework	-
Suspected WannaCry ransomware attack	-
Suspicious VPN Connection	-
Account enumeration reconnaissance	-
Suspected AD FS DKM key read	-
Suspicious modification of domain AdminSdHolder	-
Suspected AS-REP Roasting attack	-
Suspicious Kerberos delegation attempt using BronzeBit method (CVE-2020-17049 exploitation)	-
Suspected brute-force attack (Kerberos, NTLM)	-
Suspected DFSCoerce attack using Distributed File System Protocol	-

# Microsoft Defender for Identity configuration

Microsoft Defender

Search

Learning hub

Trials

Partner catalog

Exposure management

Assets

Identities

Dashboard

Health issues

Tools

Email & collaboration

Cloud apps

Settings

More resources

## Health Issues

The Microsoft Defender for Identity Health Center lets you know when there's a problem with your Defender for Identity in

Global health issues (0) Sensor health issues (0)

Export

Filter Reset Filters

Status: Open Issue: Any Severity: Any

Issue	Severity	Status	Action
-------	----------	--------	--------

4 items Search

Schedule

Weekly, Sunday, 02:00 PM

software one

① There are new permissions options available for Secure Score. You can now configure users' Secure Score data visibility based on data source. [Learn more about this change](#)

Overview Recommended actions History Metrics & trends

 Export

24 items

Filters: Product: Defender for Identity 

Rank	Recommended action	Score impact	Points achieved	Status	Regression	Have license?	Category	Product	Last synced	Microsoft update
1	Resolve unsecure domain configurations	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
2	Remove the attribute 'password never expires' from accounts in your doma	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
3	Stop weak cipher usage	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
4	Resolve unsecure account attributes	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
5	Protect and manage local admin passwords with Microsoft LAPS	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
6	Disable Print spooler service on domain controllers	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
7	Remove non-admin accounts with DCSync permissions	+1.23%	0/5	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
8	Configure VPN integration	+0.25%	0/1	To address	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
9	Start your Defender for Identity deployment, installing Sensors on Domain C	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	None
10	Prevent users to request a certificate valid for arbitrary users based on the c	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	17/03/2024 01:00
11	Edit misconfigured certificate templates owner (ESC4)	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	17/03/2024 01:00
12	Edit overly permissive Certificate Template with privileged ECU (Any purpos	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	17/03/2024 01:00
13	Edit misconfigured enrollment agent certificate template (ESC3)	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	17/03/2024 01:00
14	Edit misconfigured certificate templates ACL (ESC4)	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	17/03/2024 01:00
15	Remove unsecure SID history attributes from entities	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
16	Reduce lateral movement path risk to sensitive entities	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
17	Modify unsecure Kerberos delegations to prevent impersonation	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
18	Manage accounts with passwords more than 180 days old	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
19	Remove dormant accounts from sensitive groups	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00
20	Remove local admins on identity assets	+1.23%	5/5	Completed	No	Yes	Identity	Defender for Identity	3/18/2024	11/03/2024 01:00

# Microsoft Defender for Cloud apps Activity log

The screenshot shows the Microsoft Defender for Cloud apps Activity log interface. The left sidebar contains the navigation menu with the following items: Exposure management, Assets, Identities, Dashboard, Health issues, Tools, Email & collaboration, Cloud apps (highlighted), Cloud discovery, Cloud app catalog, OAuth apps, App governance, Files, Activity log (highlighted), Governance log, and Policies. The main area displays the 'Activity log' with a search bar and a table of activity records. The table has columns for App, User, and Activity type. The 'App' column is currently expanded, showing a list of applications including Active Directory, Microsoft 365 admin center, Microsoft 365 Defender, Microsoft MyAccount, Microsoft Online Services, Microsoft 365, Microsoft Delve, and Microsoft Exchange Online. The 'User' column shows 'Erik Stiphout' for all entries. The 'Activity type' column shows 'Log on' for all entries. The 'App' column also shows 'Active Directory' for the first entry and 'Microsoft 365' for the others.

App	User	Activity type
Active Directory	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on
Microsoft 365	Erik Stiphout	Log on



Its Demo Time!

## Takeaways and final thoughts

- Use a gMSA account for sensor deployment. Its more effort to setup, but much more secure and less maintenance.
- Onboard all the possible services MDI has such as: AD-DS, -FS, -CS & Radius accounting (VPN) more signals means more chance of alerts when something is up.
- Take your time, MDI will need 30 days to be truly reliable in your environment. Do not start excluding entities before thinking it through and if you're excluding try to exclude by detection rule not globally.
- MDI is a great tool in your arsenal for managing threats to identities in your on-premises Active Directory. However, MDI isn't bombproof, and it can be (and has been) circumvented. Deploy MDI as a puzzle piece among other pieces to your security puzzle. Do not solely rely on MDI to alert you to an issue on-premises.



## Inspiration taken from sites:

<https://techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/introducing-the-new-powershell-module-for-microsoft-defender-for/ba-p/4028734>

<https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-defender-for-identity-ninja-training/ba-p/2117904>

<https://jeffreyappel.nl/how-to-implement-defender-for-identity-and-configure-all-prerequisites/>

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-for-identity-azure-atp-daily-operation/ba-p/1831024>

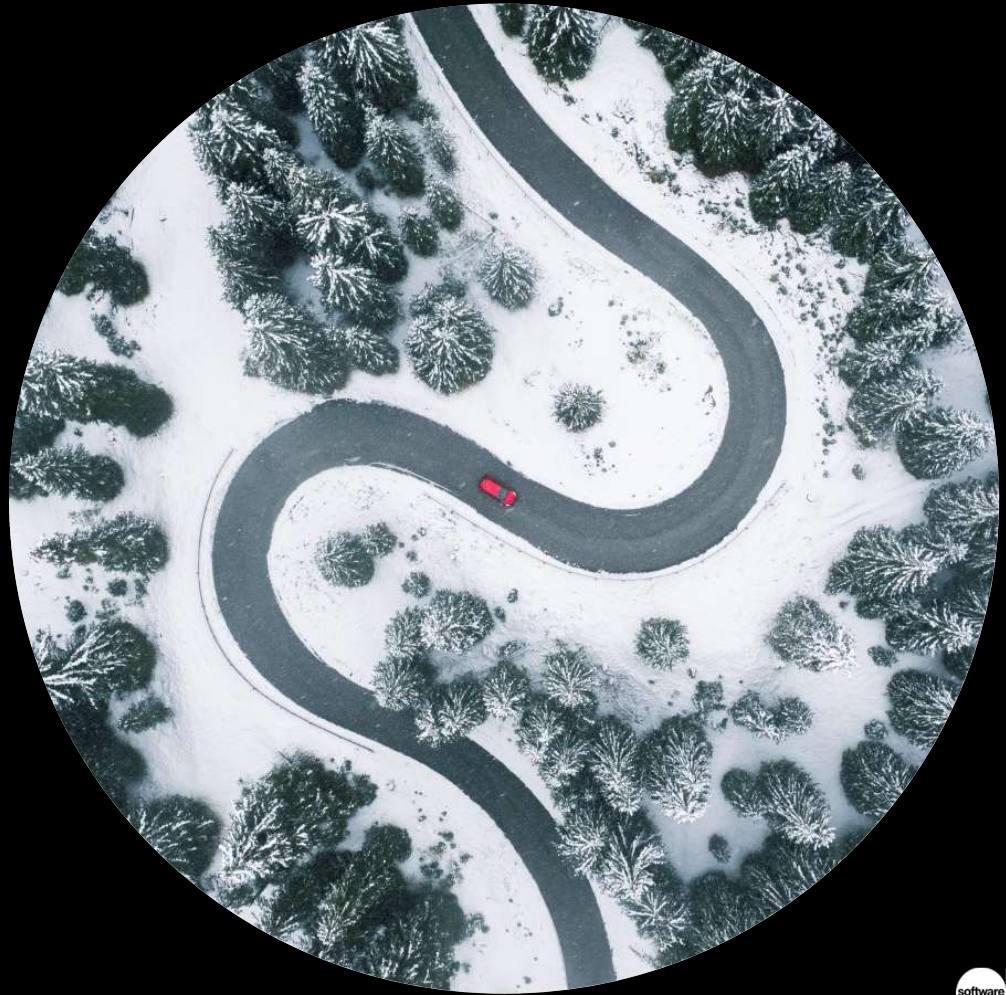
[https://www.slideshare.net/nikhil\\_mittal/0wnpremises-bypassing-microsoft-defender-for-identity](https://www.slideshare.net/nikhil_mittal/0wnpremises-bypassing-microsoft-defender-for-identity)

<https://thalpius.com/2022/07/30/microsoft-defender-for-identity-auditing/>

<https://techcommunity.microsoft.com/t5/microsoft-defender-xdr-blog/securing-ad-cs-microsoft-defender-for-identity-s-sensor-unveiled/ba-p/3980265>

[https://dcaddick.github.io/gsd\\_public/MDI/#validate-and-test](https://dcaddick.github.io/gsd_public/MDI/#validate-and-test)

# Q & A



---

# Thank You

## Get in Touch

+31 (0)20 25 86 800

[Info\\_nl@softwareone.com](mailto:Info_nl@softwareone.com)

Naritaweg 177

1043 BW Amsterdam

The Netherlands

---



# Disclaimer

This publication contains proprietary information that is protected by copyright. SoftwareOne reserves all rights thereto.

SoftwareOne shall not be liable for possible errors in this document. Liability for damages directly and indirectly associated with the supply or use of this document is excluded as far as legally permissible.

The information presented herein is intended exclusively as a guide offered by SoftwareOne. The publisher's product use rights, agreement terms and conditions and other definitions prevail over the information provided herein. The content must not be copied, reproduced, passed to third parties or used for any other purposes without written permission of SoftwareOne

Copyright © 2023 by SoftwareOne. All Rights Reserved. SoftwareOne is a registered trademark of SoftwareOne. All other trademarks, service marks or trade names appearing herein are the property of their respective owners.