MICROSOFT SECURE SCORE V PRAKSI

MATEJ KLEMENČIČ

Cyber Security Architect

- www.span.eu/**si**
- www.linkedin.com/company/**span**
- www.linkedin.com/in/**matejklemencic**
- matej.klemencic@span.eu
- www.matej.guru

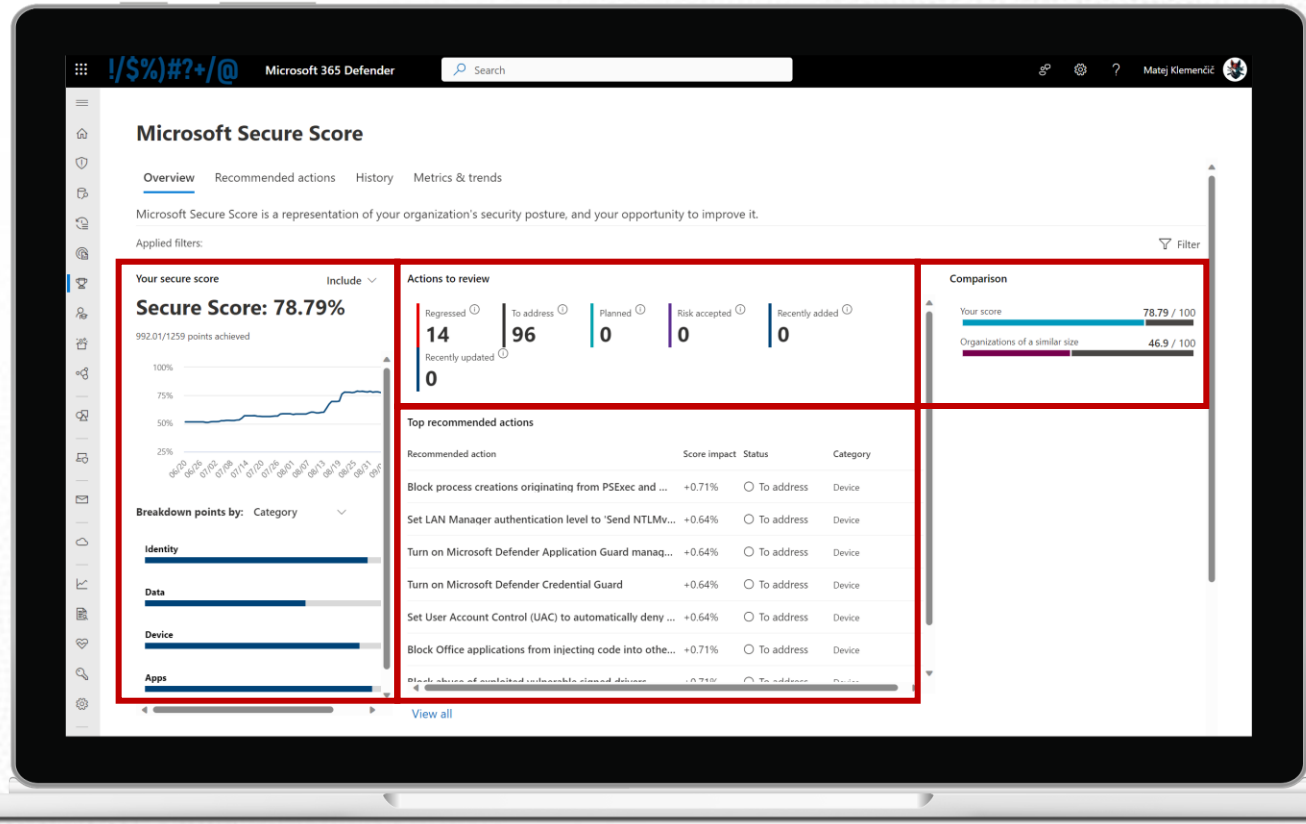
span

MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetske higiene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?



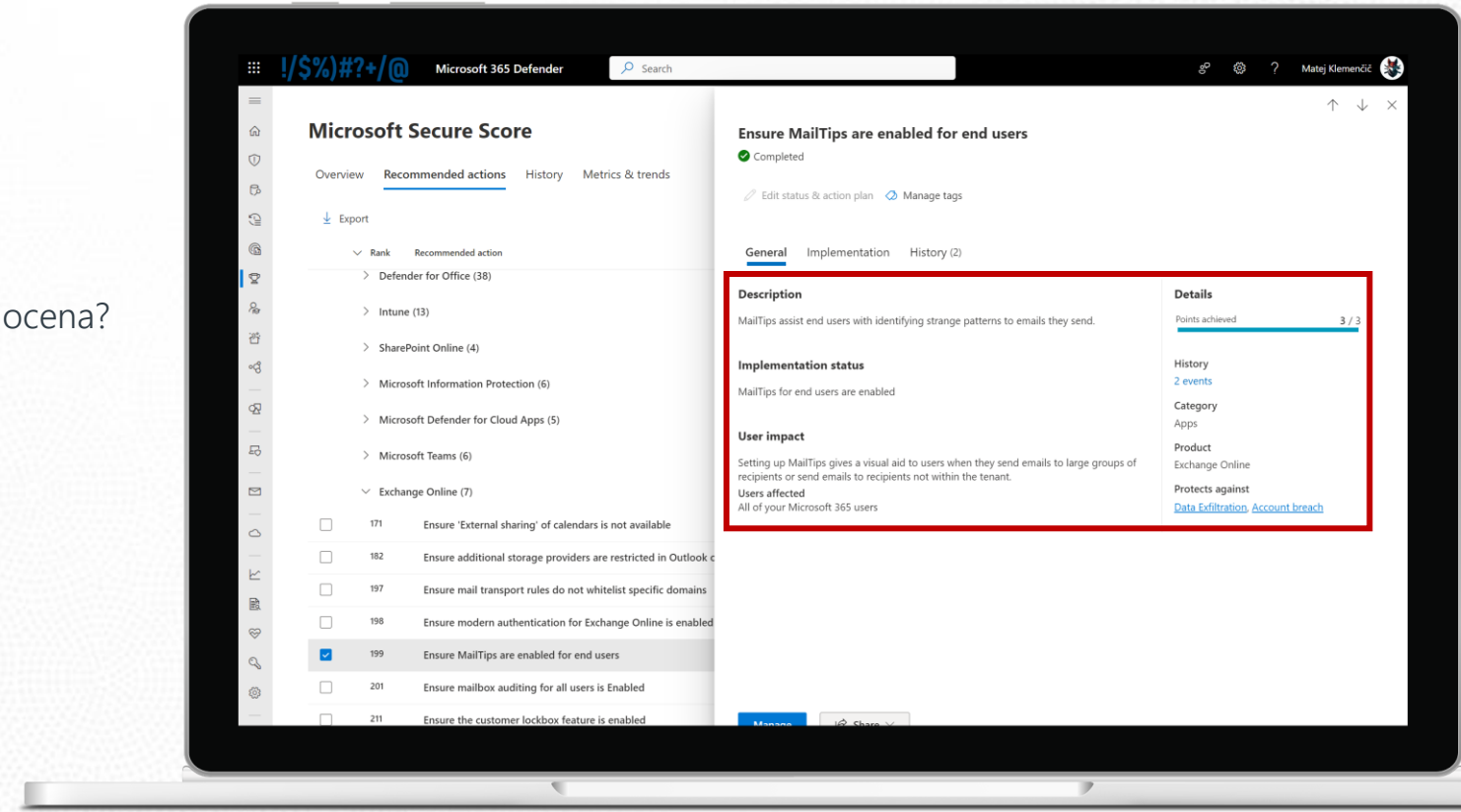
span

MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetske higiene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?

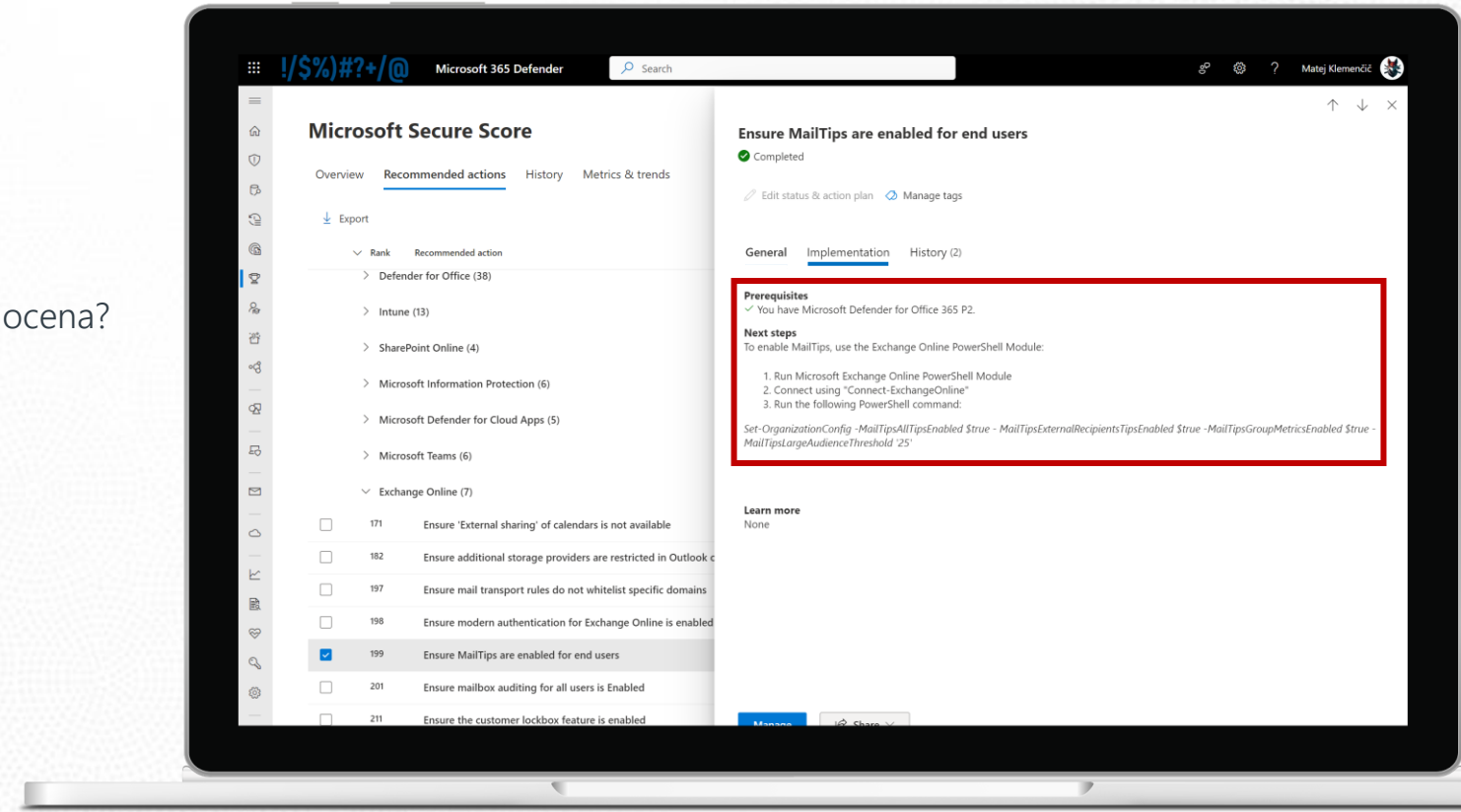


MICROSOFT SECURE SCORE

Vidljivost in smernice za krepitev kibernetske higiene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?

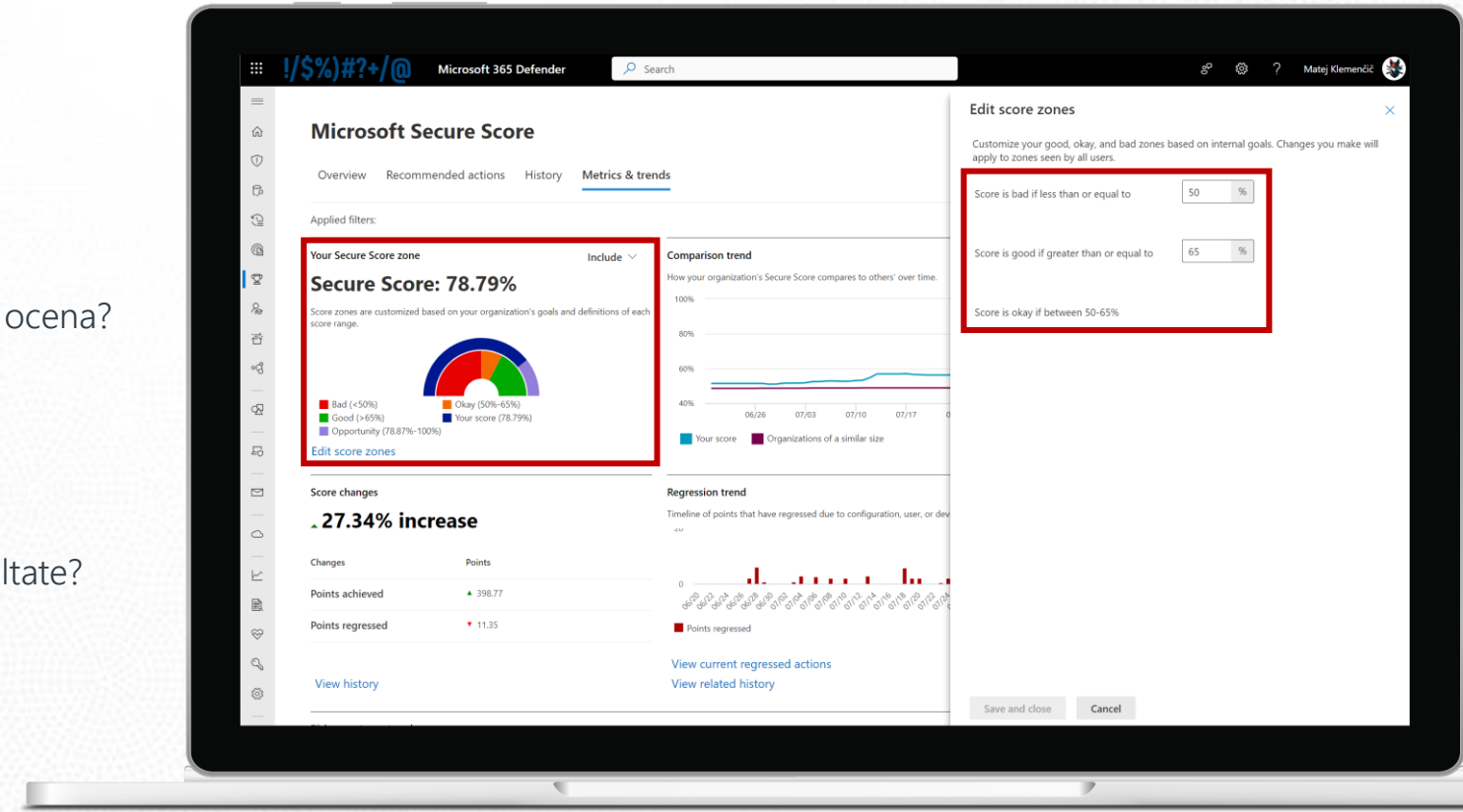


MICROSOFT SECURE SCORE

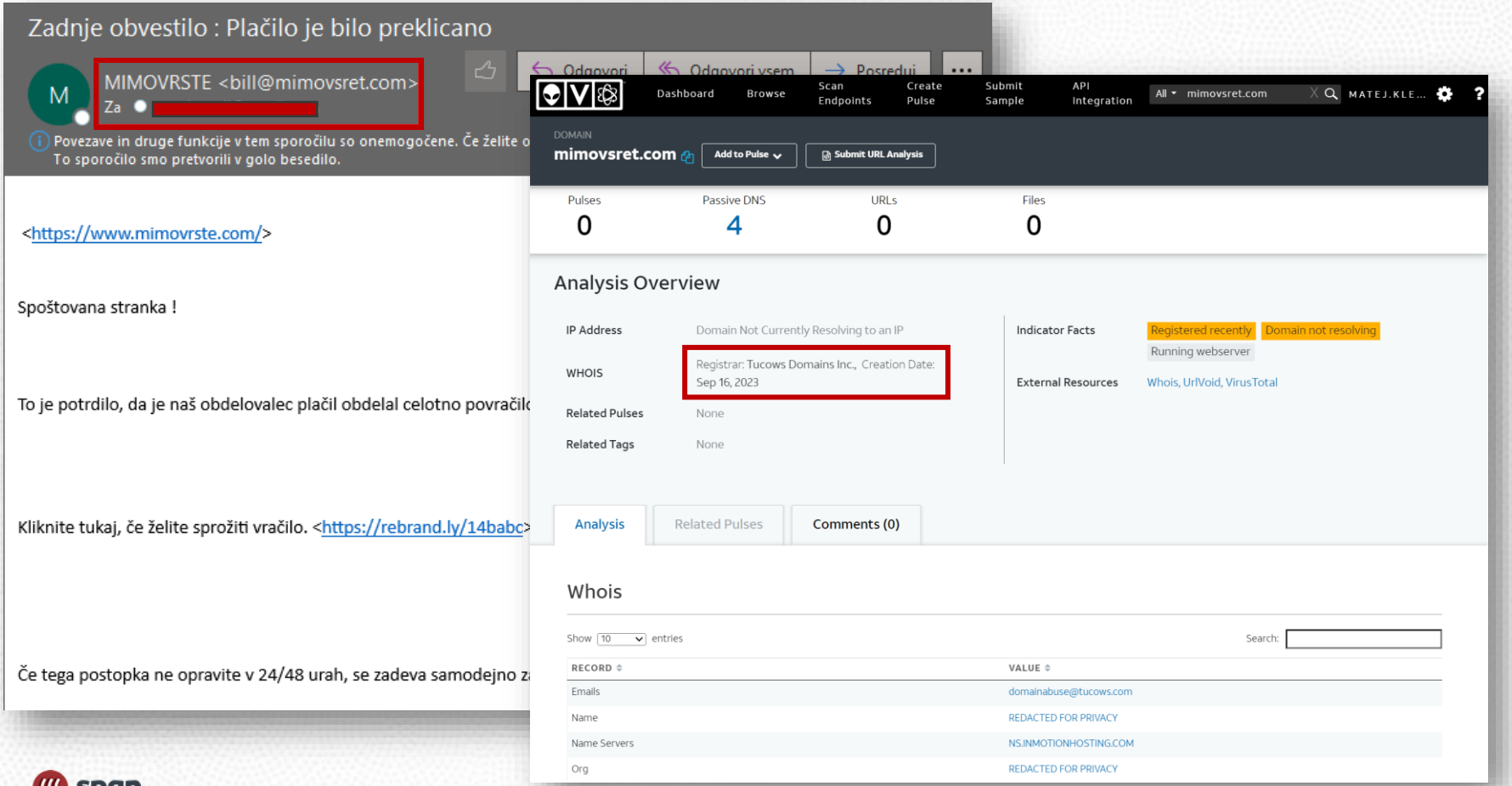
Vidljivost in smernice za krepitev kibernetske higiene

ODGOVORI NA VARNOSTNA VPRAŠANJA

- Kakšna je varnostna ocena?
- Kje začeti?
- Kako ukrepati?
- Kako spremljati rezultate?
- Kako poročati?



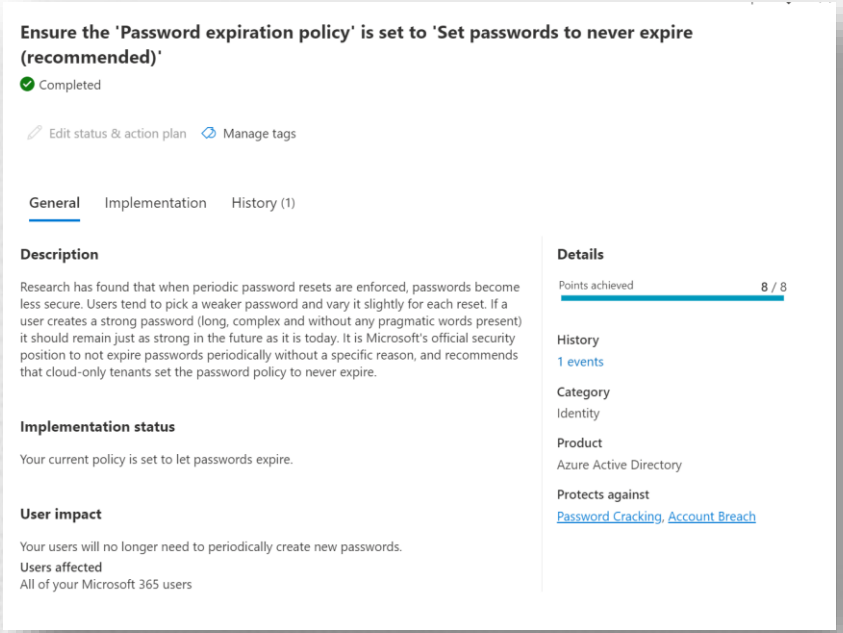
DEMO


Zadnje obvestilo : Plačilo je bilo preklicano
MIMOVRSTE <bill@mimovsret.com>
Za
Povezave in druge funkcije v tem sporočilu so onemogočene. Če želite o
To sporočilo smo pretvorili v golo besedilo.
<https://www.mimovrste.com/>
Spoštovana stranka !
To je potrdilo, da je naš obdelovalec plačil obdelal celotno povračil
Kliknite tukaj, če želite sprožiti vračilo. <https://rebrand.ly/14babc>
Če tega postopka ne opravite v 24/48 urah, se zadeva samodejno z
Dashboard
Browse
Scan Endpoints
Create Pulse
Submit Sample
API Integration
mimovsret.com
DOMAIN
mimovsret.com
Add to Pulse
Submit URL Analysis
Pulses 0
Passive DNS 4
URLs 0
Files 0
Analysis Overview
IP Address
Domain Not Currently Resolving to an IP
WHOIS
Registrar: Tucows Domains Inc., Creation Date: Sep 16, 2023
Related Pulses
None
Related Tags
None
Indicator Facts
Registered recently
Domain not resolving
Running webserver
External Resources
Whois, UrlVoid, VirusTotal
Analysis
Related Pulses
Comments (0)
Whois
Show 10 entries
Search:
RECORD
VALUE
Emails
domainabuse@tucows.com
Name
REDACTED FOR PRIVACY
Name Servers
NS.INMOTIONHOSTING.COM
Org
REDACTED FOR PRIVACY

ENHANCES EOP/MDO POLICIES

- Configuration Analyzer for EOP and Microsoft Defender for Office 365
  - *https://security.microsoft.com/**configurationAnalyzer***
- Microsoft Defender for Office 365 Recommended Configuration Analyzer (ORCA)
  - *https://github.com/cammurray/**orca***
  - ***Install-Module ORCA***
  - ***Get-ORCAReport***
  - *Developed by Product Managers at Microsoft, however, is not an official Microsoft utility.*

PASSWORD POLICY



The following Microsoft Entra password policy requirements apply for all passwords that are created, changed, or reset in Microsoft Entra ID. Requirements are applied during user provisioning, password change, and password reset flows. You can't change these settings except as noted.

Property	Requirements
Characters allowed	Uppercase characters (A - Z) Lowercase characters (a - z) Numbers (0 - 9) Symbols: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > - blank space
Characters not allowed	Unicode characters
Password length	Passwords require - A minimum of eight characters - A maximum of 256 characters
Password complexity	Passwords require three out of four of the following categories: - Uppercase characters - Lowercase characters - Numbers - Symbols Note: Password complexity check isn't required for Education tenants.
Password not recently used	When a user changes their password, the new password should not be the same as the current password.
Password isn't banned by Microsoft Entra Password Protection	The password can't be on the global list of banned passwords for Microsoft Entra Password Protection, or on the customizable list of banned passwords specific to your organization.

span

PASSWORD POLICY (NIST - 2022)

- *…password policy that requires all **user-created passwords** to have **at least the length of eight**, and all **auto-generated passwords** to be at least **six characters** in length.*

- *Passwords **should be reset once a year** in order to maintain digital security.*

- *Changing your password more **frequently** than necessary can actually have a **negative effect** on security since users may use **simple variations of the same password** over time instead of creating stronger ones with each resetting period.*

- *Passwords which are **known to be frequently used or compromised should be prohibited.***

span

National Institute of Standards and Technology

PASSWORD POLICY (CIS - 2021)

- *…an **eight-character minimum password length** is recommended **for an MFA account**, and **14 characters for a password only account.***
- *Password expiration requirements **offer no containment benefits** because attackers will often use credentials as soon as they compromise them.*
- *…we also recommend **a yearly password change**. This is primarily because for all their good intentions users will share credentials across accounts.*
- *Organizations **should ban the use of common bad passwords.***

AZURE ACTIVE DIRECTORY PASSWORD PROTECTION

Ensure password protection is enabled for on-prem Active Directory

Completed

NTK

Edit status & action plan Manage tags

General Implementation History (2)

Description

Enable Azure Active Directory Password Protection to Active Directory to protect against the use of common passwords.
Note: This recommendation applies to Hybrid deployments only, and will have no impact unless working with on-premises Active Directory.

Implementation status

Azure Active Directory Password Protection is enabled

User impact

The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, implementation of Azure Active Directory Password Protection may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to.

Users affected
All of your Microsoft 365 users

Details

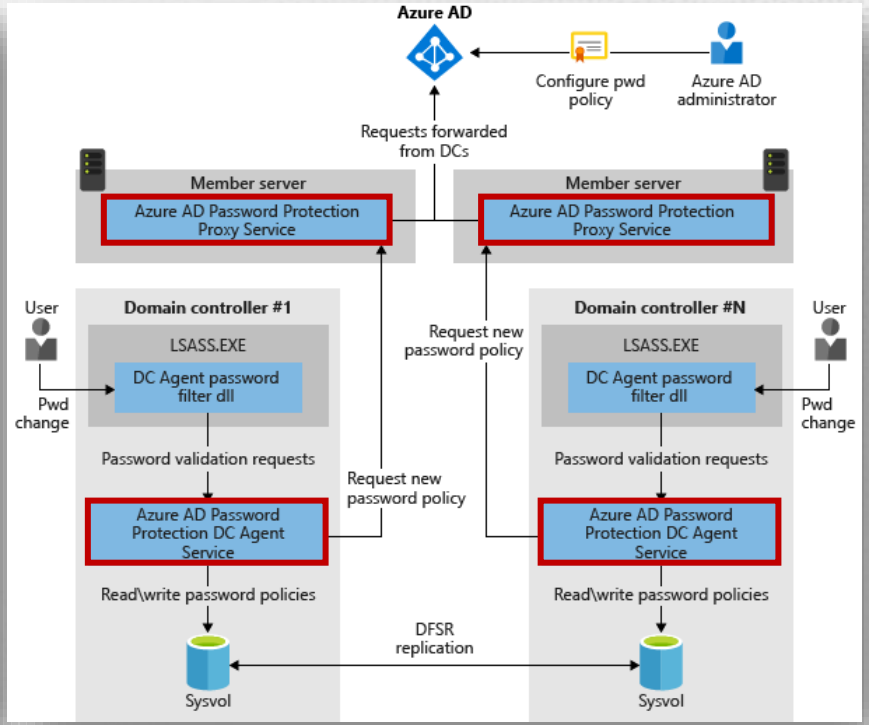
Points achieved 6 / 6

History
2 events

Category
Apps

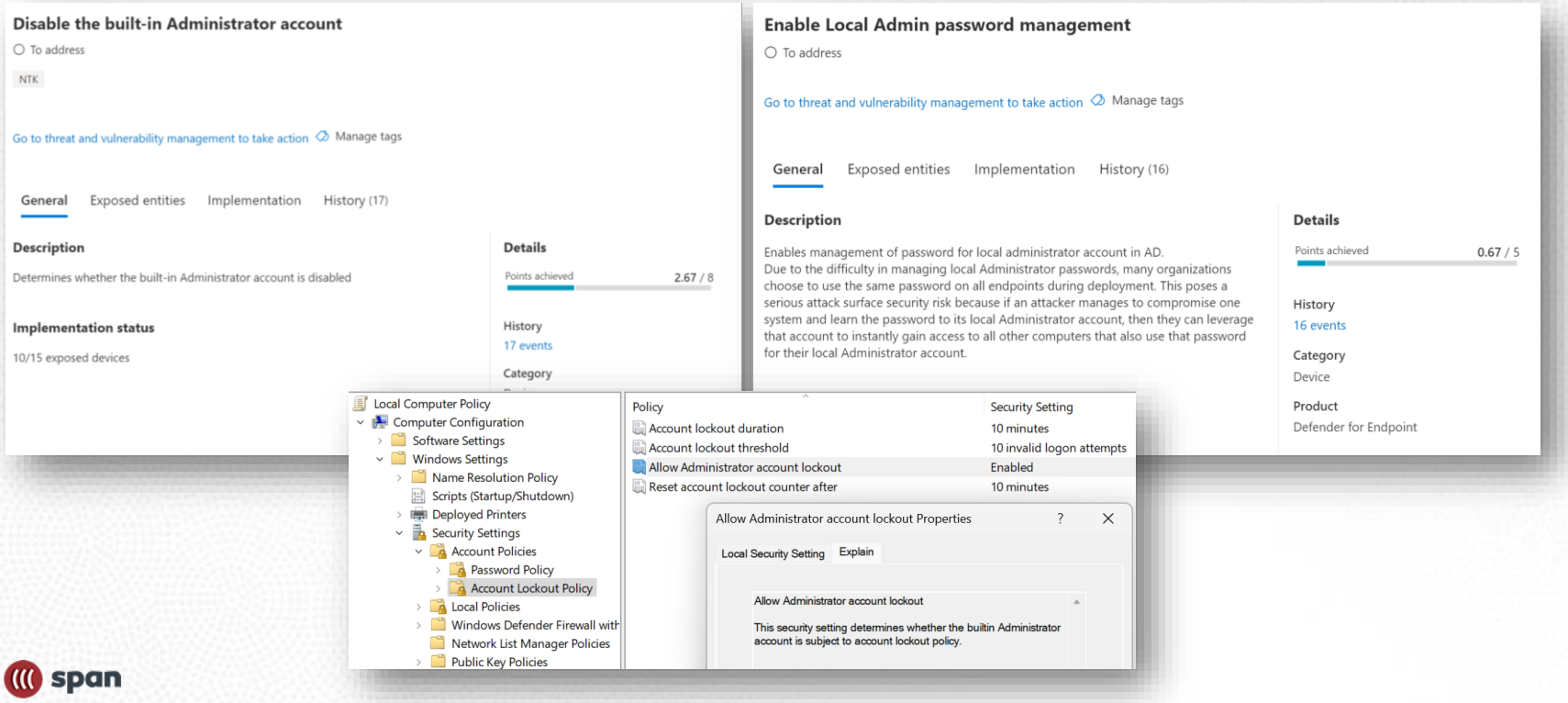
Product
Azure Active Directory

Protects against
Data Exfiltration, Password Cracking, Account breach



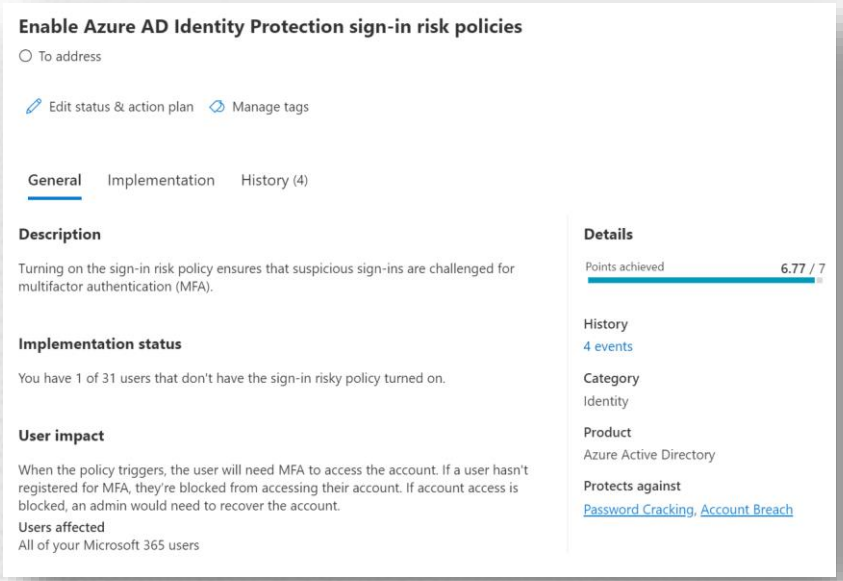
span

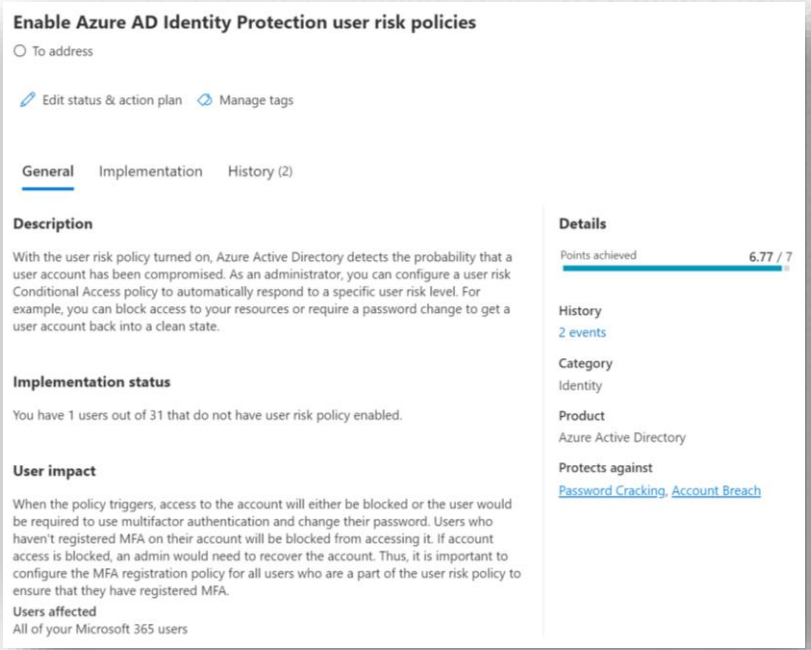
LOCAL ADMINISTRATOR ACCOUNT



span

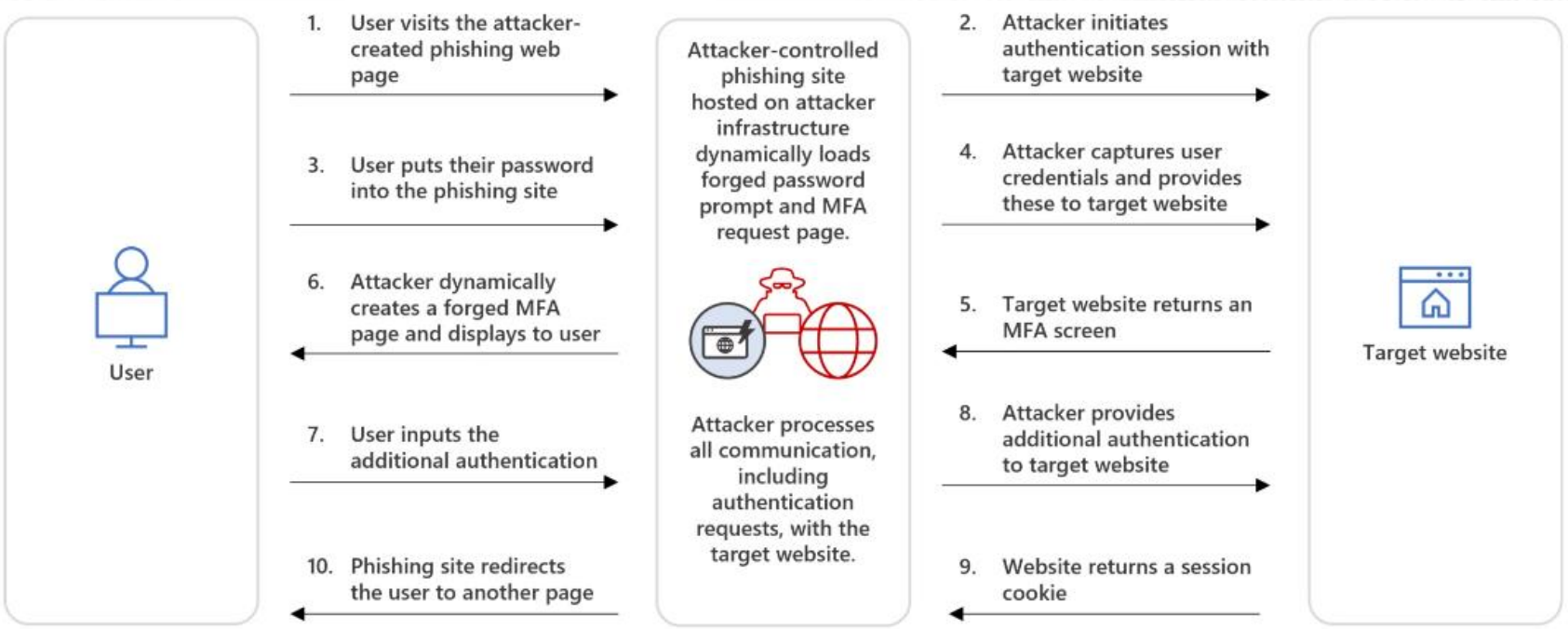
IDENTITY PROTECTION





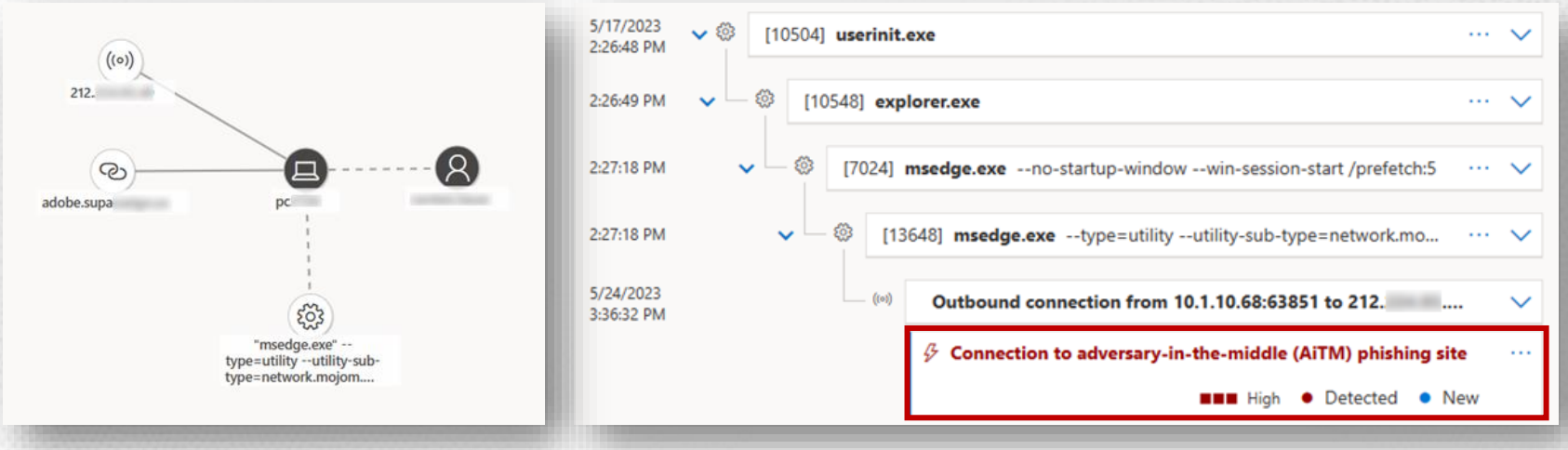
span

ADVERSARY-IN-THE-MIDDLE (AiTM)



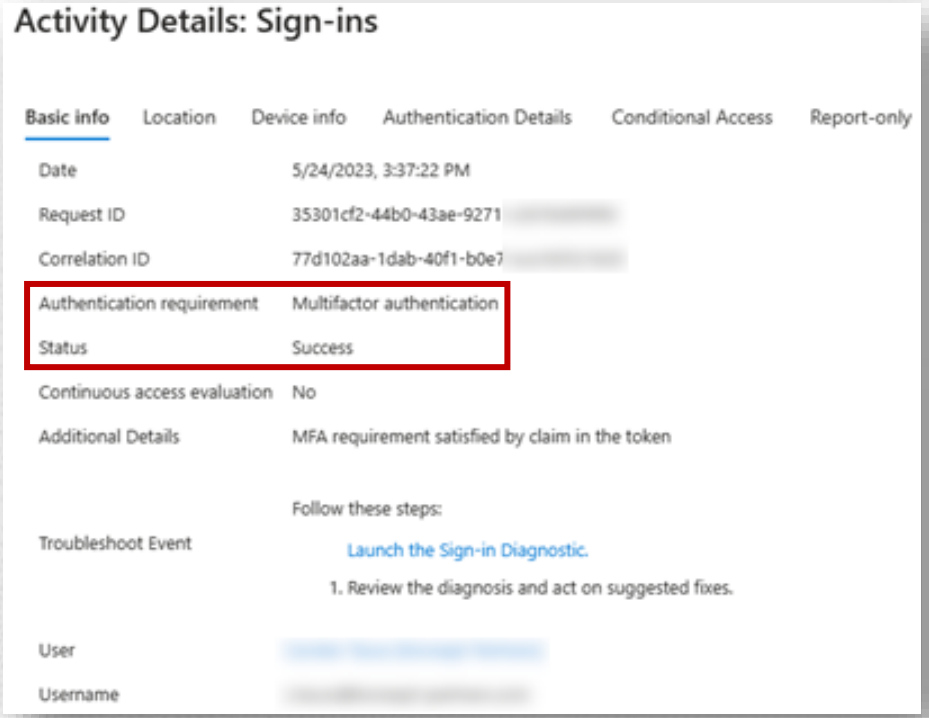
span

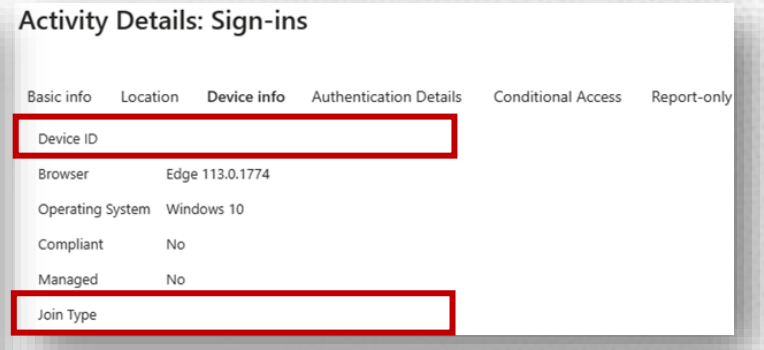
ADVERSARY-IN-THE-MIDDLE (AiTM)

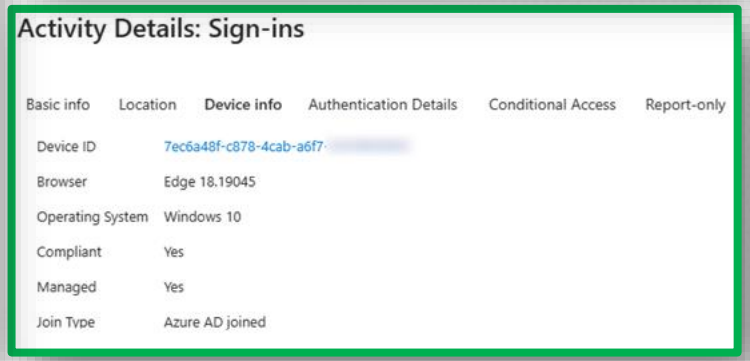


span

ADVERSARY-IN-THE-MIDDLE (AiTM)

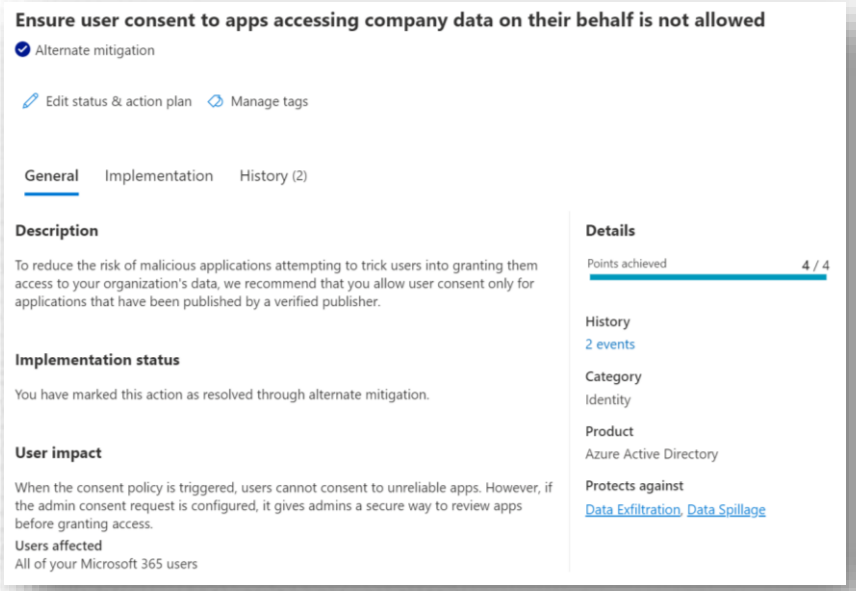


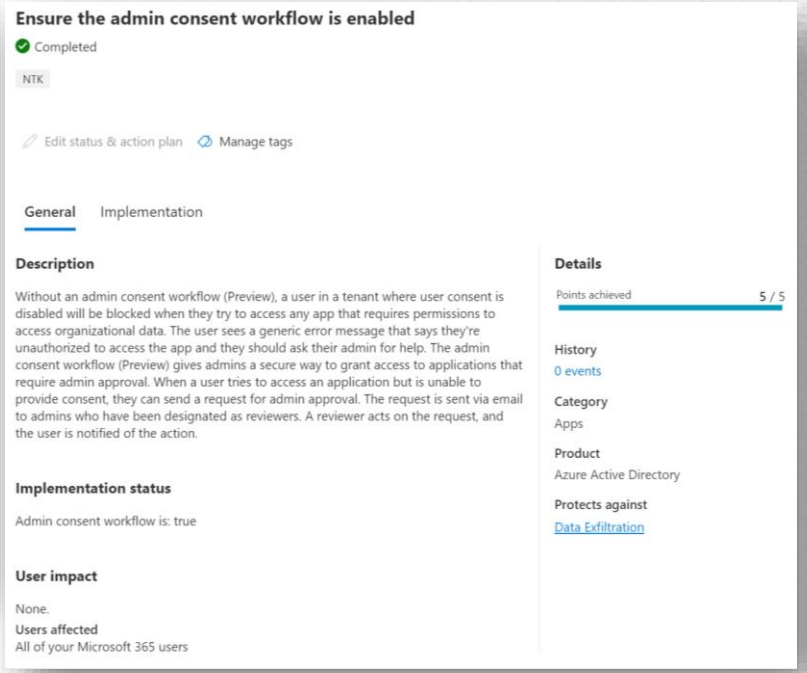




span

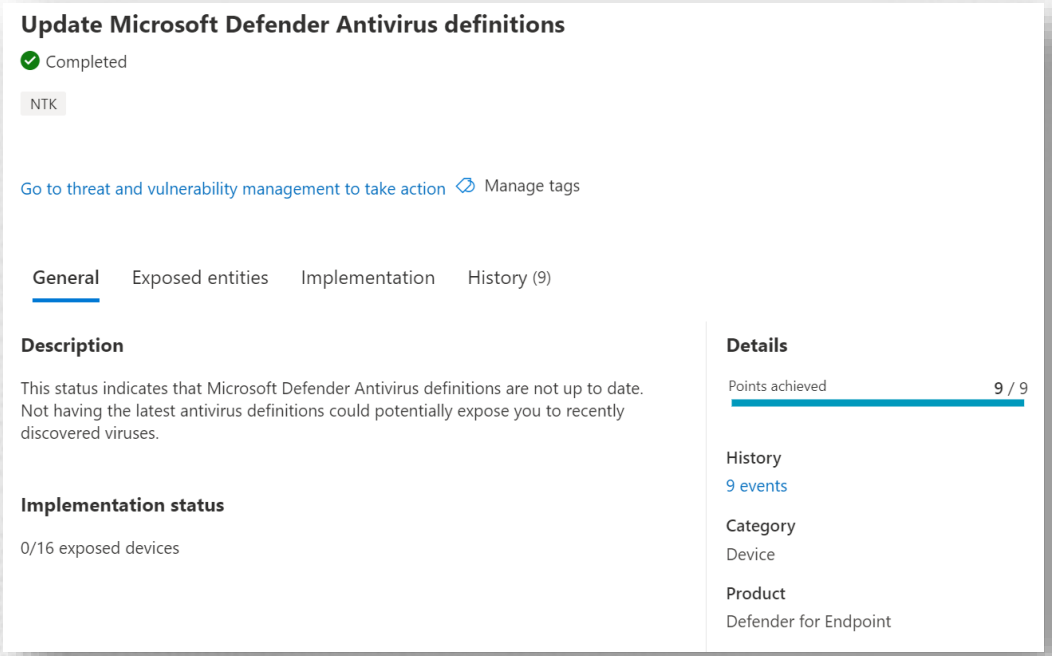
ENTERPRISE APPLICATIONS





span

MICROSOFT DEFENDER ANTIVIRUS UPDATES



span

QUESTIONS?

THANK YOU

www.span.eu