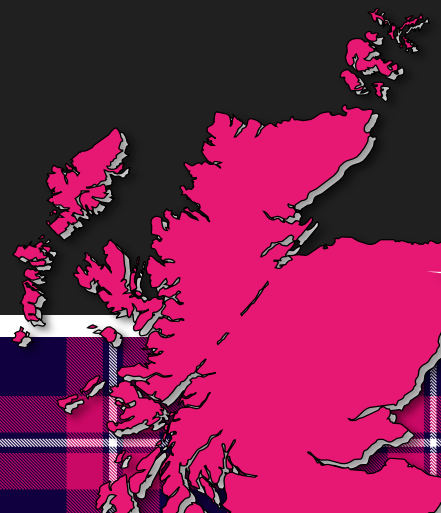
#ScottishSummit2024

Defence Against the Digital Dark Arts



SCOTTISH SUMMIT

Thank You to our Sponsors...

Platinum Sponsor

Capgemini

Gold Sponsors

resco

ARROW

dox42®
automate your documents
integrate your data

kerv Digital

#ScottishSummit2024

Thank You to our Sponsors...

With Thanks

AgileCadence
POWERING INNOVATION. SIMPLIFYING TECHNOLOGY.

Telefónica Tech

LightningTools

Cloud Surge
UNLEASH YOUR POWER

LOGIQAPPS

DYNAMICS MINDS
powered by
DOCENTRIC

mscrm-addons.com
Your company for MS-CRM ADD-ONS!

Noteworthy
.Support

ProMX

Syskit

Click

riada
CONSULTANCY

QUBIX

PROXIMO3

360

#ScottishSummit2024

Nate Hutchinson

- Microsoft Solutions Architect @ Threatscape
- natehutchinson.co.uk
- Dragonball Z fan (hence the tattoos)
- Video editor & filmmaker (2 x 48Hr Film Project Glasgow)
- Founding member of Experts Live UK User Group
- Love to travel & spend time with family

"If you get time while you're here go to Gairloch, it's beautiful...just pack your midge spray!"

LinkTr.ee Link

#ScottishSummit2024

Steve Simmons

- Azure Solutions Architect @ AirIT
- 2 x Hak5 payload winner & Defcon Black Badge hall of famer (Team Win)
- Wi-Fi Hacking Enthusiast (nerd)
- ‘67 Camaro drag racer (till I blew it up)

“Just plug this cable in...😈 ”

Linkedin.com/sasteve

#ScottishSummit2024

Intro to threat landscape

7,000
password attacks blocked per second over the past year

775 million
email messages contained malware (July 2023-June 2024)

54%
of phishing campaigns targeting consumers impersonated online software and service brands

$3 billion
in cryptocurrency stolen by North Korean hackers since 2017

2.75x increase in muggle-operated ransomware-linked encounters

By disabling or tampering with defenses, attackers buy themselves time to install malicious tools, exfiltrate data for espionage or extortion, and potentially launch attacks like ransomware.

80%
of organizations have attack paths that expose critical assets

600 million identity attacks per day

As multifactor authentication blocks most password-based attacks, threat actors are shifting their focus.

Source: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Microsoft’s unique vantage point

An extra 13 trillion security signals per day

2023: 65 trillion, 2024: 78 trillion

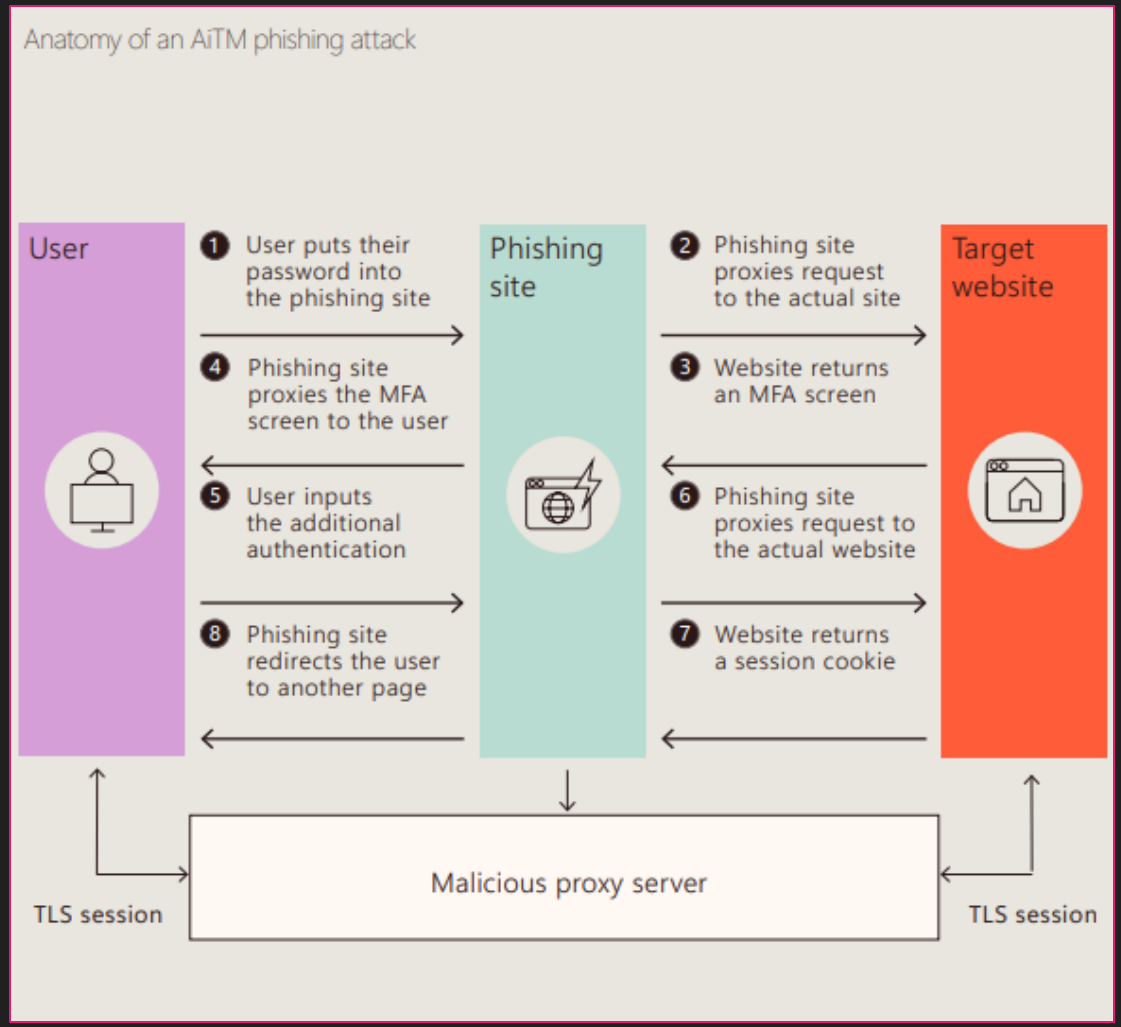
from the cloud, endpoints, software tools, and partner ecosystem, to understand and protect against digital threats and criminal cyberactivity.

1,500 unique threat groups tracked

Microsoft Threat Intelligence now tracks more than 1,500 unique threat groups—including more than 600 nation-state threat actor groups, 300 cybercrime groups, 200 influence operations groups, and hundreds of others.

Source: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Adversary In The Middle (AiTM)



Source: Microsoft Digital Defense Report 2023 (MDDR)

Offensive Tooling Used

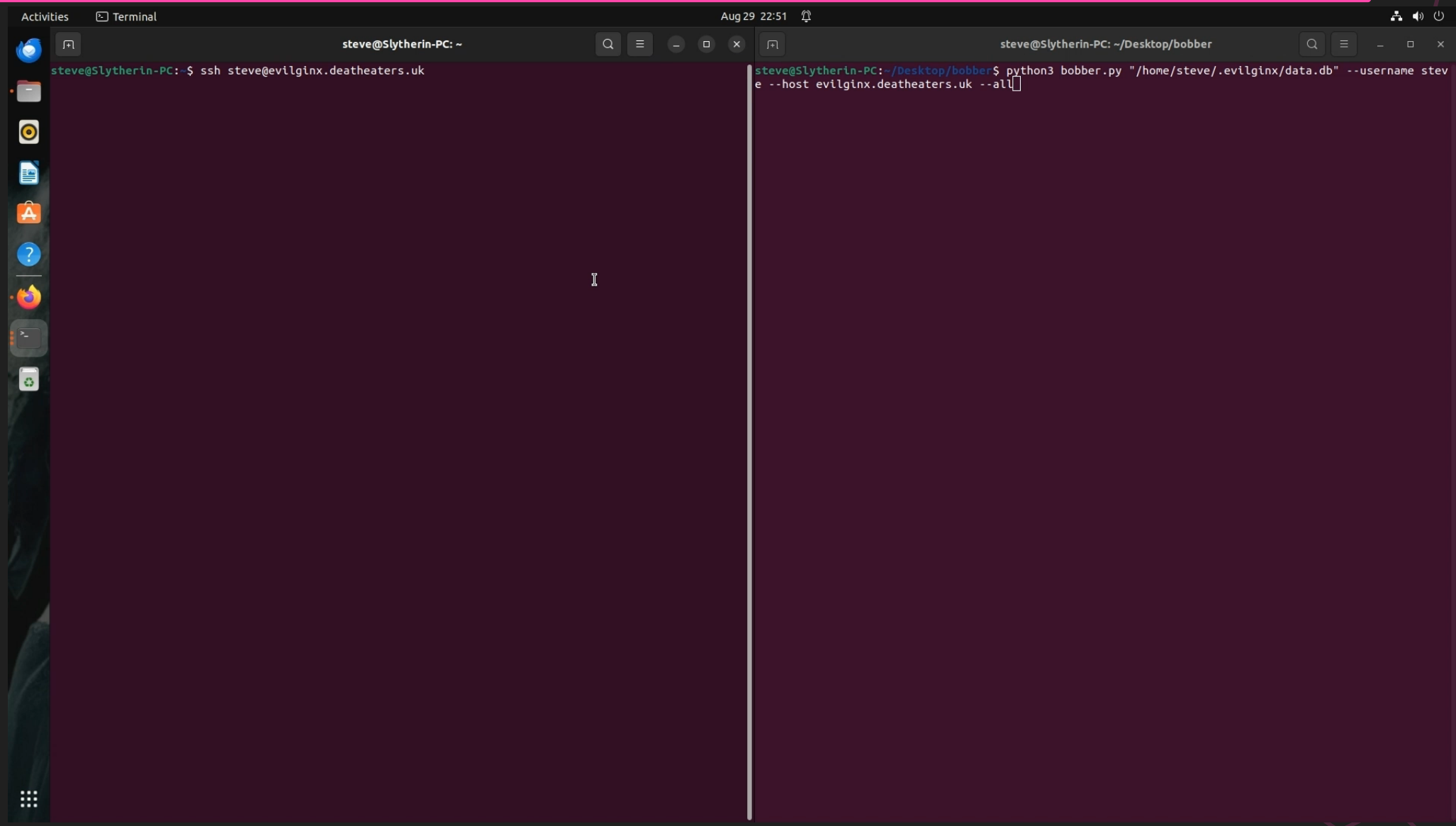
kgretzky/evilginx2: Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication (github.com)

dirkjanm/ROADtools: A collection of Azure AD/Entra tools for offensive and defensive security purposes (github.com)

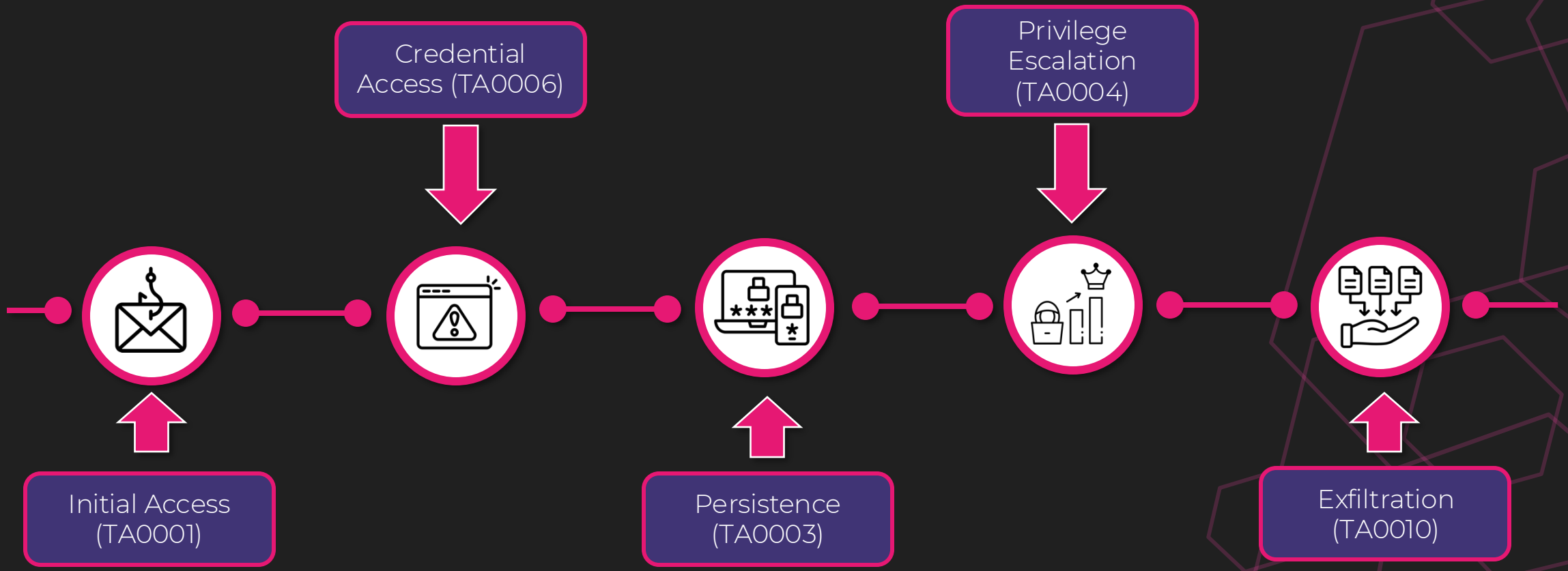
Flangvik/TeamFiltration: TeamFiltration is a cross-platform framework for enumerating, spraying, exfiltrating, and backdooring O365 AAD accounts (github.com)

Flangvik/Bobber: Bounces when a fish bites - Evilginx database monitoring with exfiltration automation (github.com)

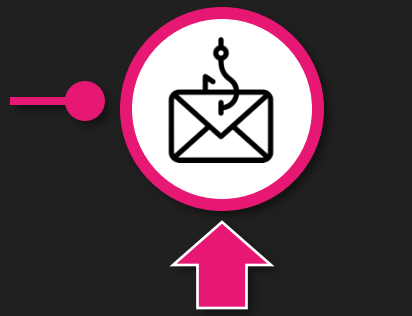
Attack Scenario



The Attack

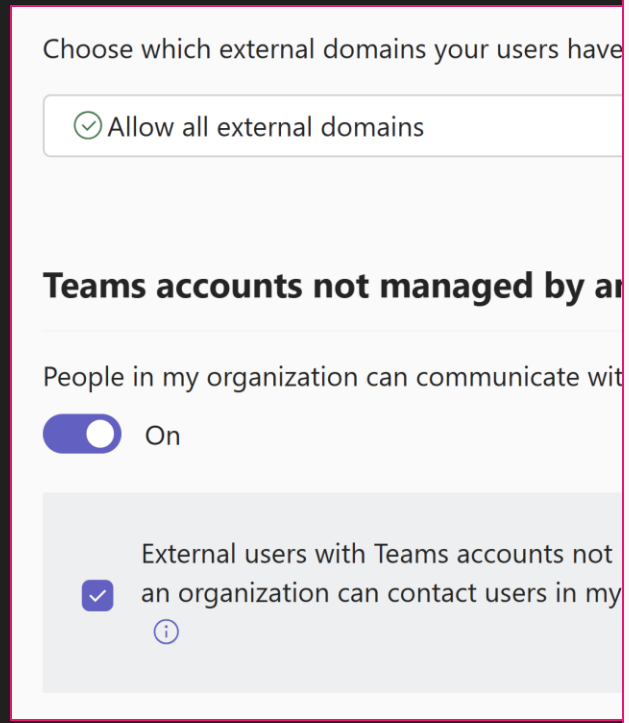

Credential Access (TA0006)
Privilege Escalation (TA0004)
Initial Access (TA0001)
Persistence (TA0003)
Exfiltration (TA0010)

Initial Access / Phishing (TA0001 / T1566)



Initial Access
(TA0001)

Teams – Domain Whitelisting



Choose which external domains your users have access to:

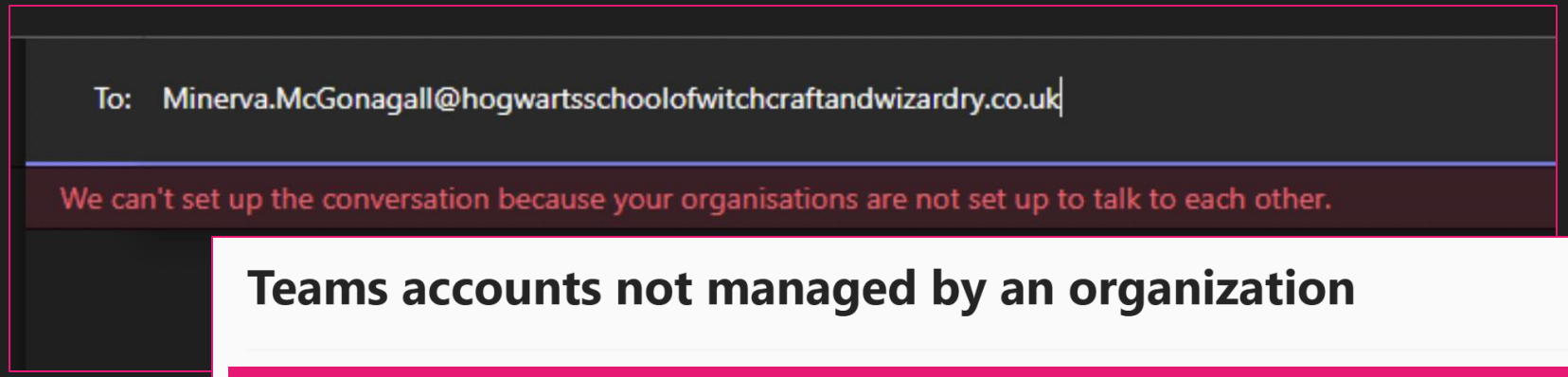
Allow only specific external domains

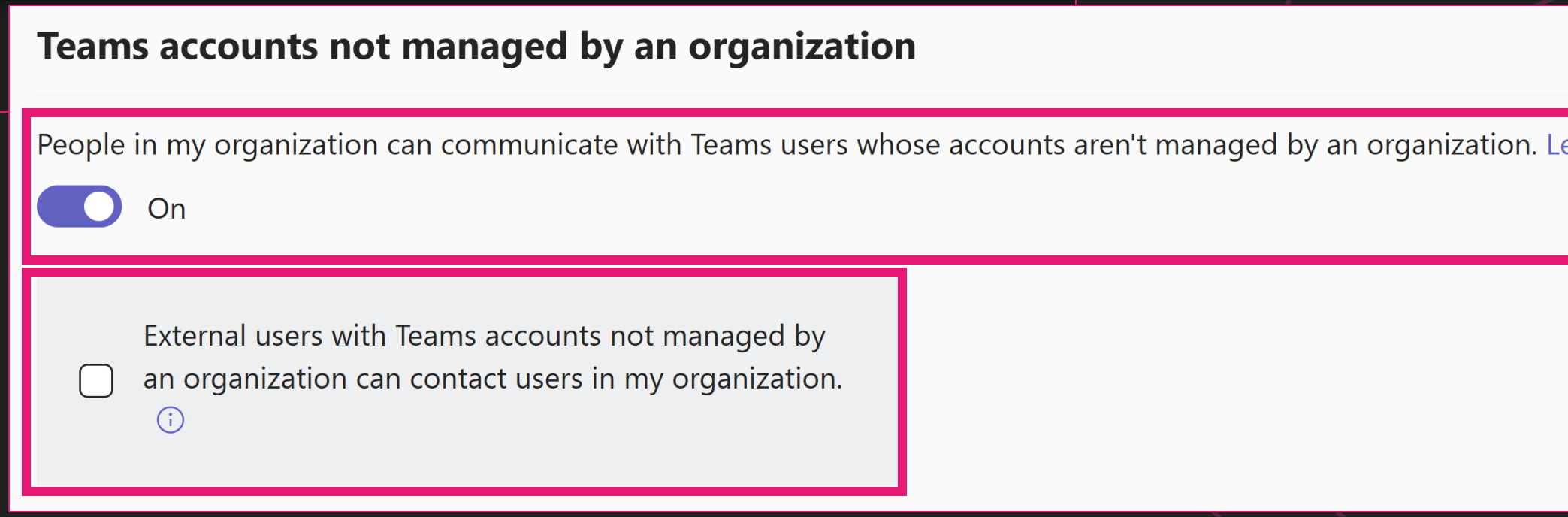
Add a domain | Remove | 2 items

Allowed domains
ministryofmagic.co.uk
gringotts.com

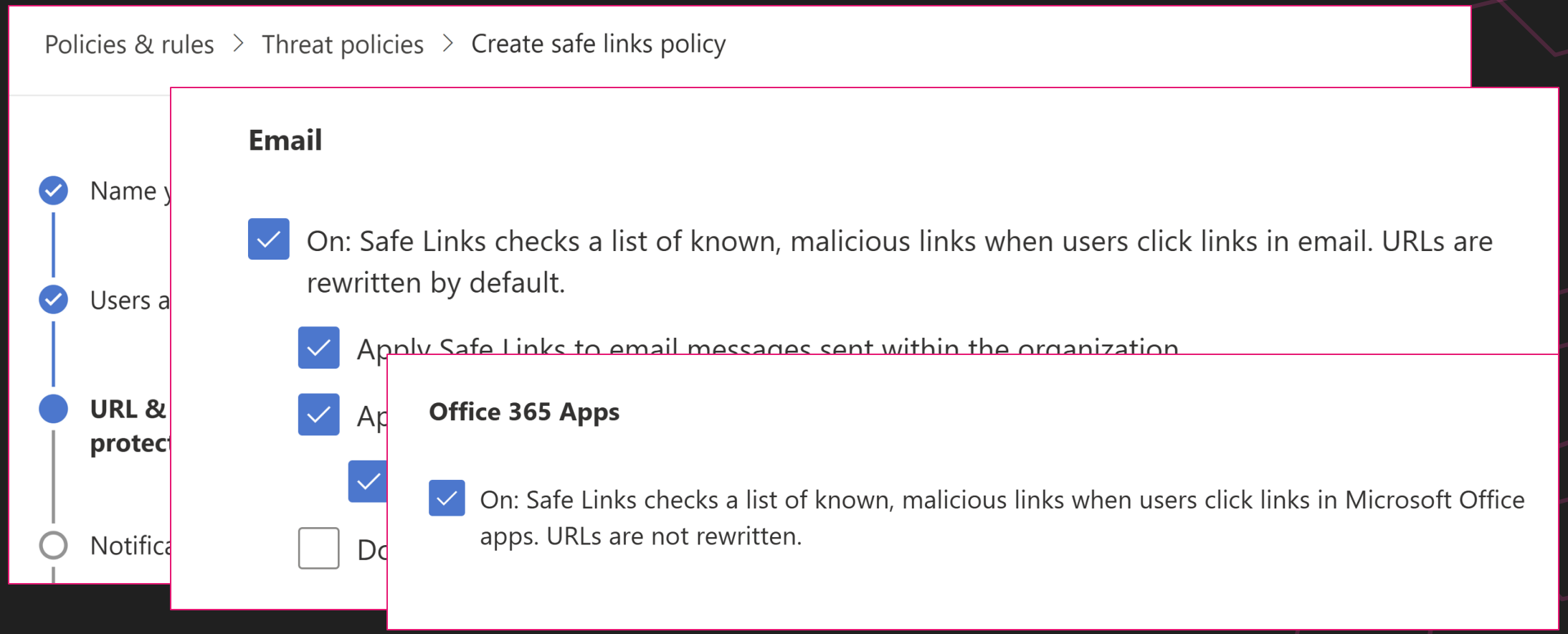
#ScottishSummit2024

Teams – Disable External / Personal account communication

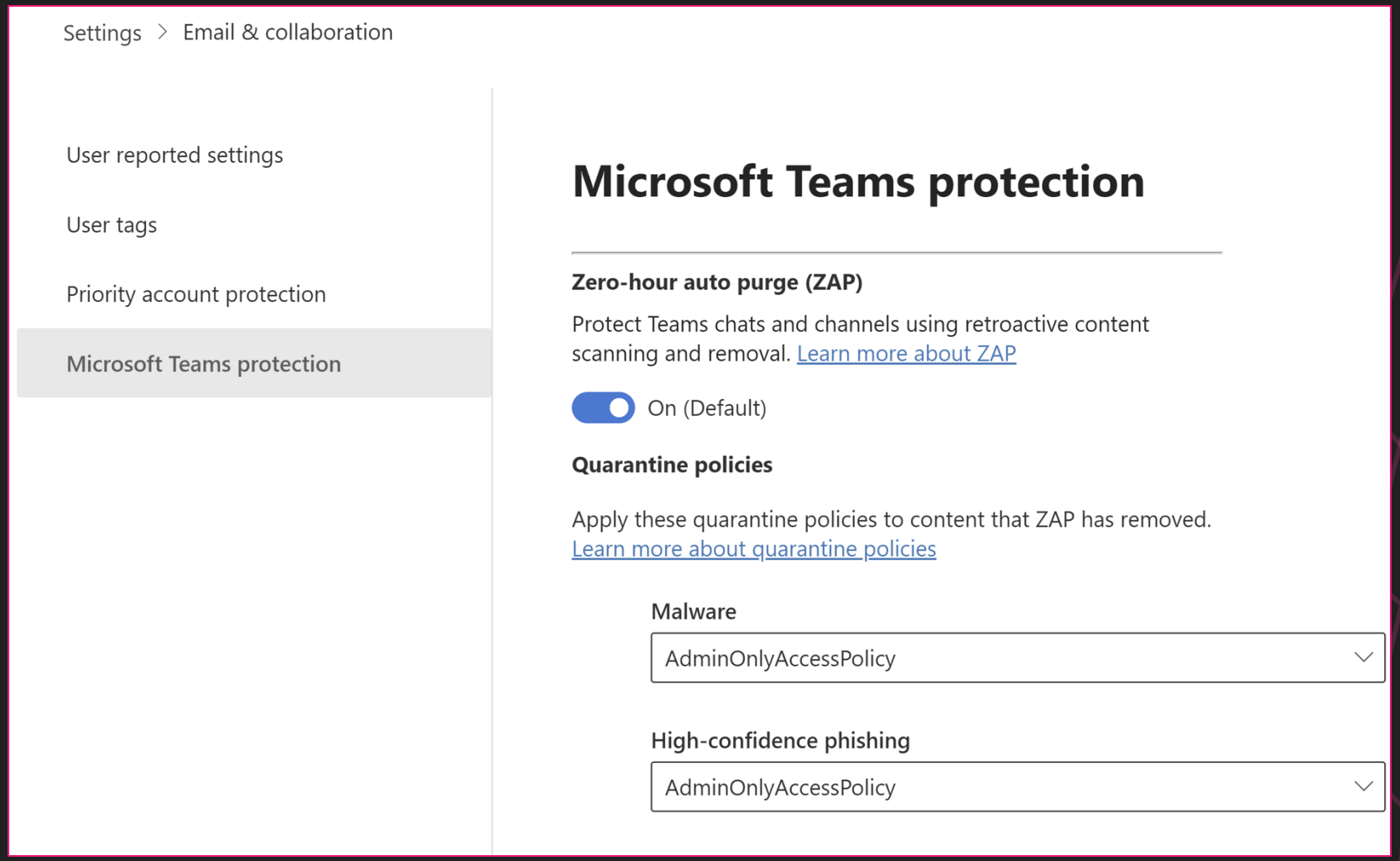




Defender for Office 365 – Safe Links



Teams – Zero-Hour Auto Purge (ZAP)



Defender for Office 365 – Anti-Phishing Policy

Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing protection. For example, you can refining the settings to better detect and prevent impersonation and spoofing attacks. T users within the organization. You can create custom, higher priority policies for specific users, groups or domains. Learn policies

We recommend enabling preset security policies to stay updated with new security controls and our recommended settings. View preset security policies

0 impersonated domain(s) and user(s) over the past 7 days. View impersonations

+ Create | Export | Refresh | 3 items | Search

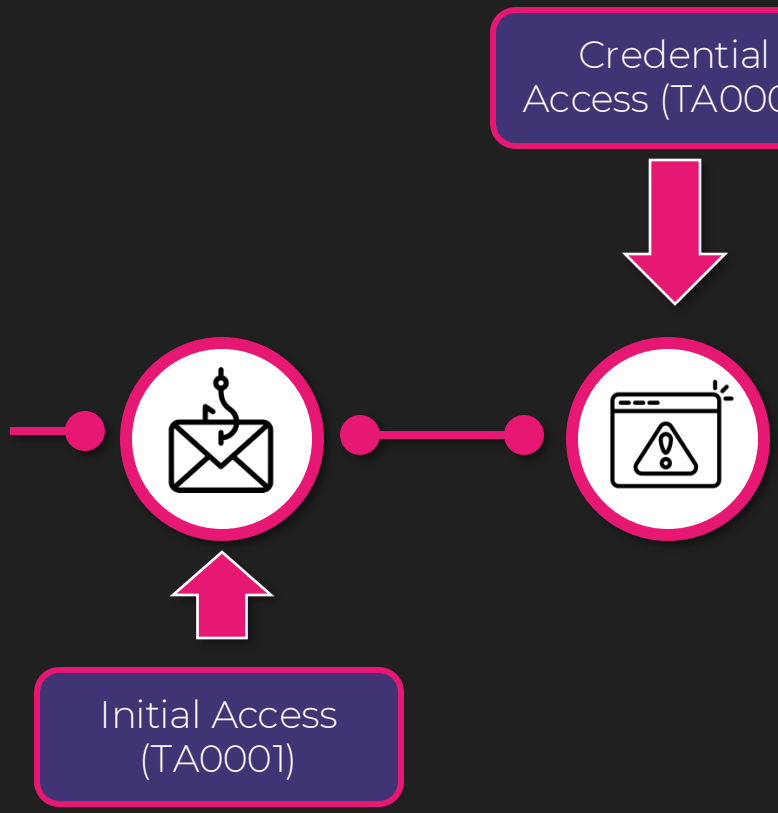
Name	Status	Priority
Strict Anti-Phishing Policy	On	0
Standard Anti-Phishing Policy	On	1
Office365 AntiPhish Default (Default)	Always on	Lowest

#ScottishSummit2024

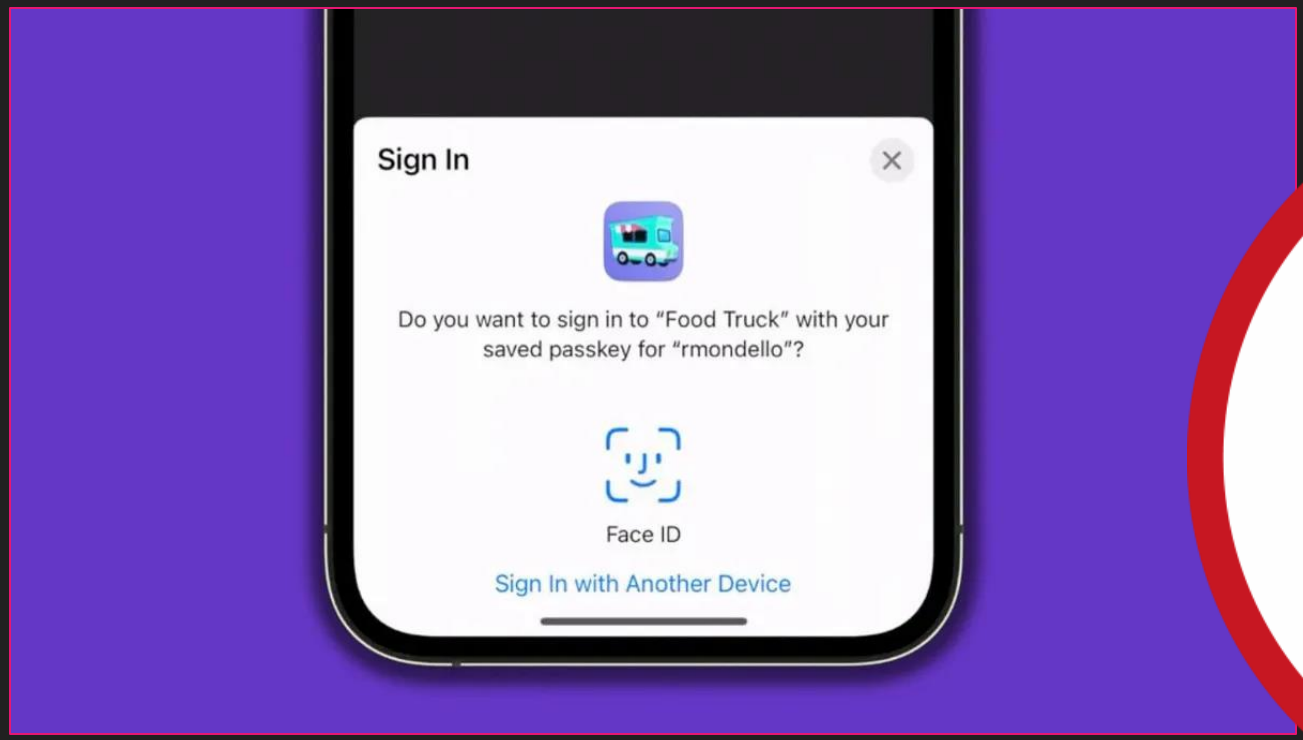
Wrap Up

- Use domain whitelisting in Teams
- Disable personal Teams account communication and 1st contact
- Enable Defender for Office 365 Safe Links policies
- Enable Zero-Hour Auto Purge (ZAP)
- Enable Defender for Office 365 Anti-Phishing policies

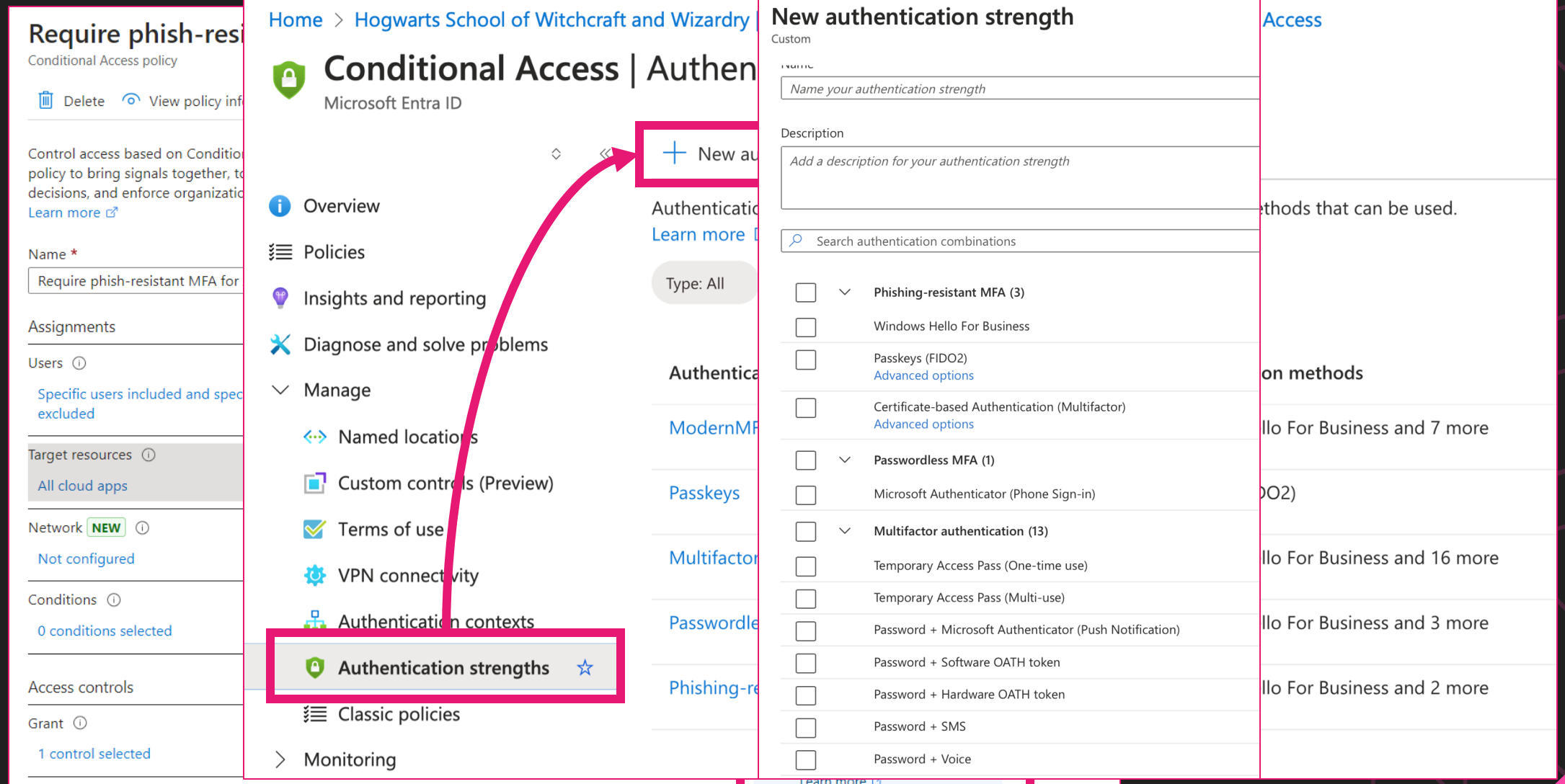
Credential Access / AiTM (TA0006 / T1557)



Phish-Resistant Authentication



Conditional Access - Authentication Strengths



#ScottishSummit2024

Conditional Access - Authentication Strengths

Require phish-resistant MFA for All Cloud Apps

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *
Require phish-resistant MFA for All Cloud A...

Assignments

Users
Specific users included and specific users excluded

Target resources
All cloud apps

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to
Cloud apps

Include | Exclude

- None
- All cloud apps
- Select apps

Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.
Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected. Learn more

Require authentication strength
Phishing-resistant MFA

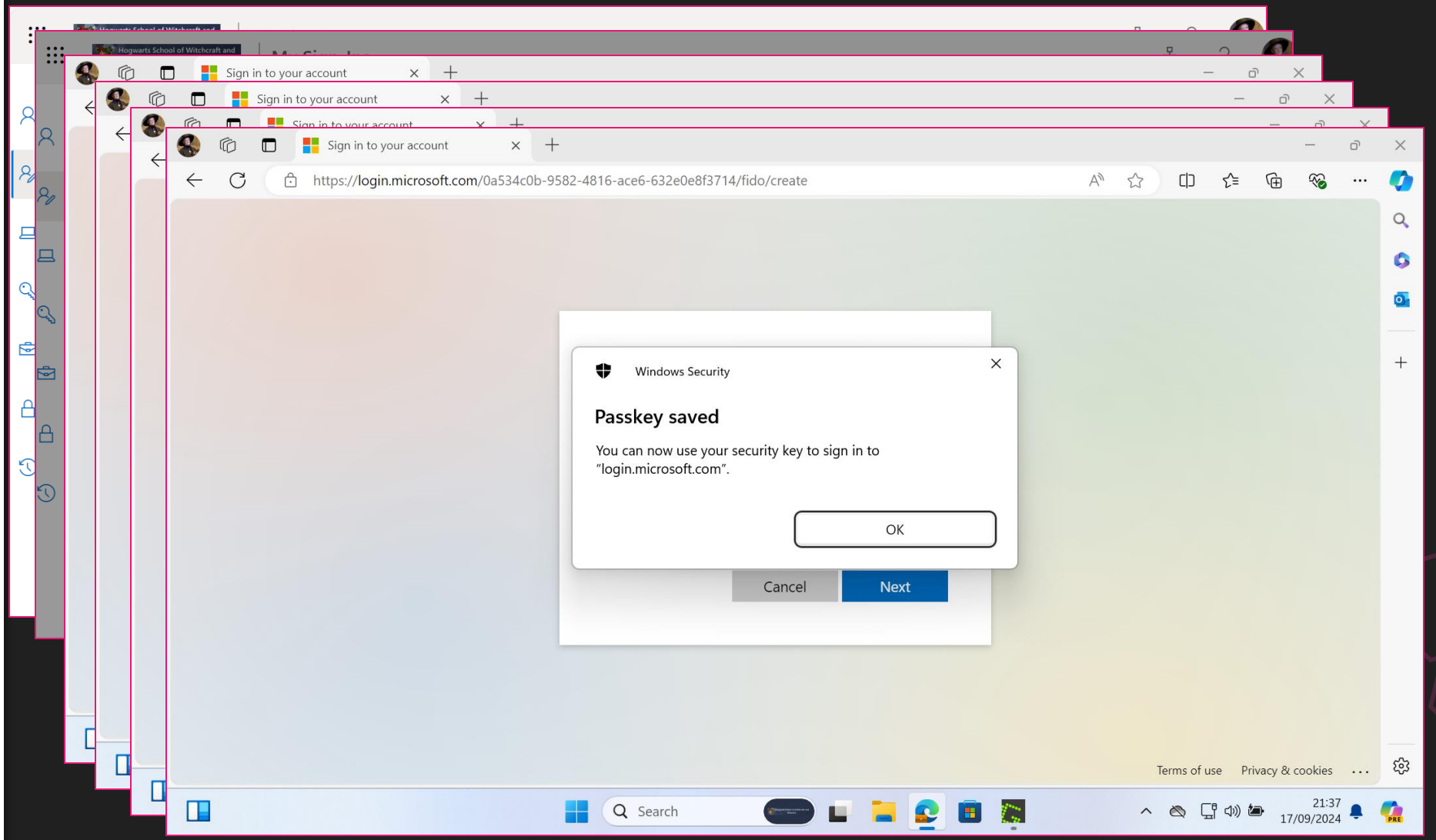
To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users.
Learn more

View Authentication Strength

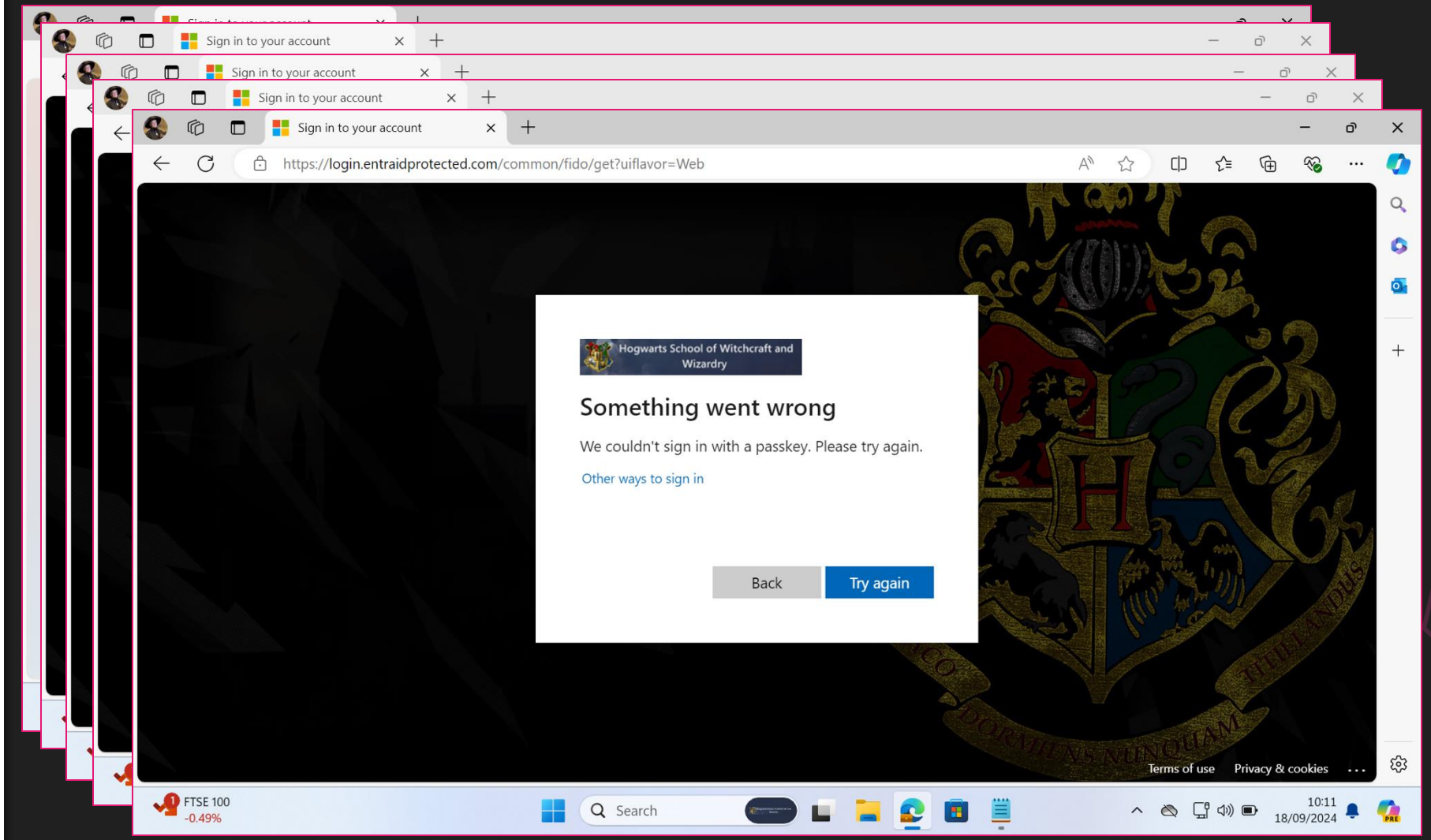
Name	Phishing-resistant MFA
Type	Built-in
Description	Include authentication methods that are phishing-resistant like Passkeys (FIDO2) and Windows Hello for Business
Authentication Flows	Windows Hello For Business **OR** Passkeys (FIDO2) **OR** Certificate-based Authentication (Multifactor)

#ScottishSummit2024

Authentication Strengths – Enforce Phish-Resistant MFA

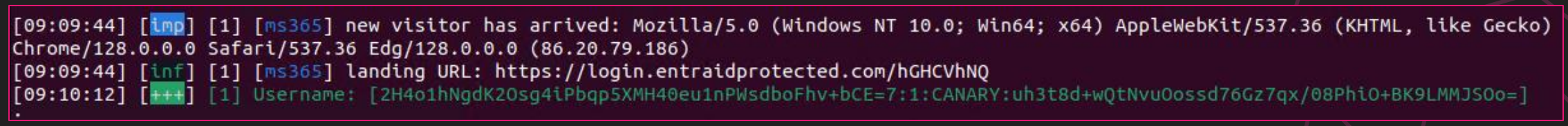


Authentication Strengths – Enforce Phish-Resistant MFA



#ScottishSummit2024

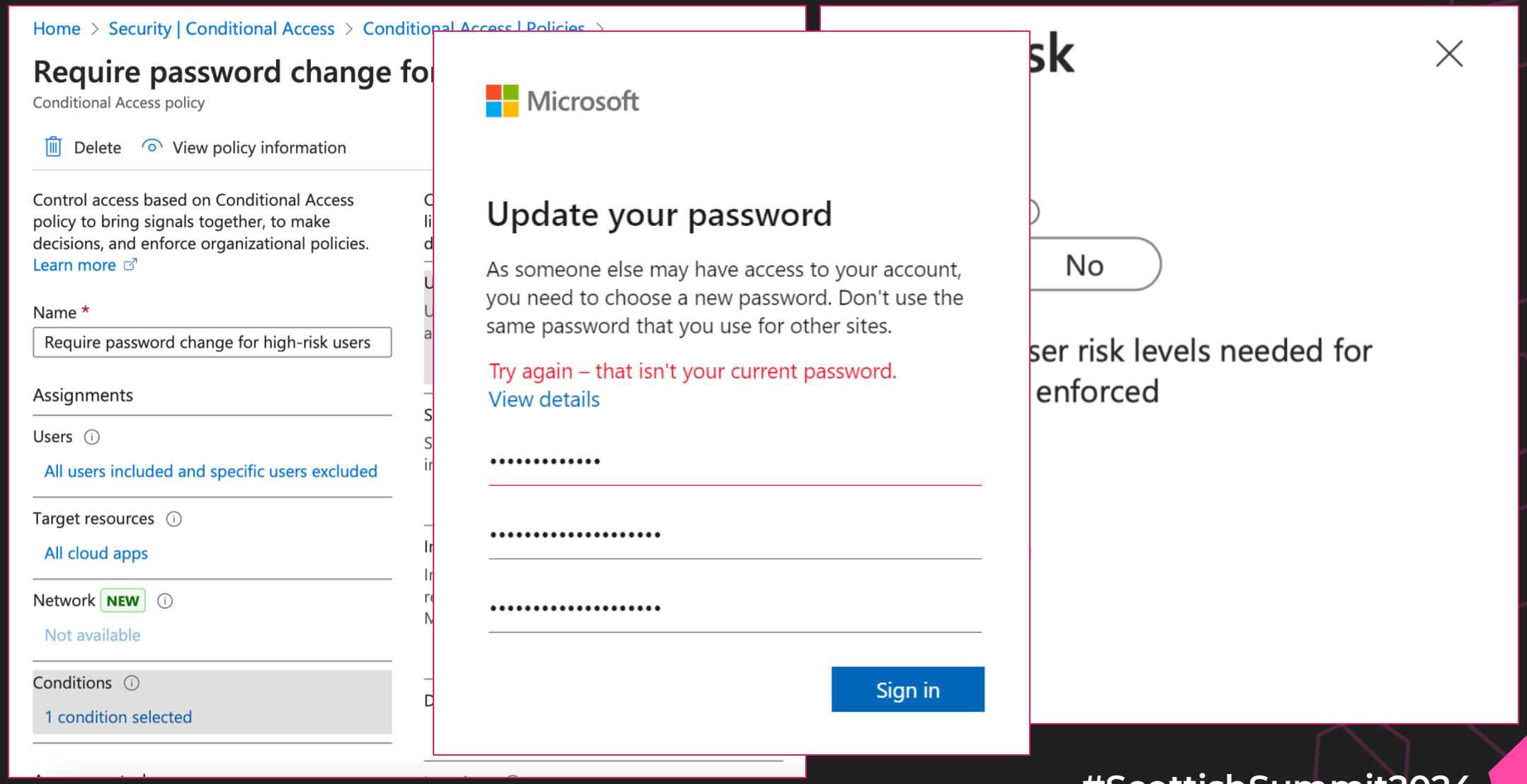
Authentication Strengths – Enforce Phish-Resistant MFA



SSPR Gotcha's

- SMS can still be used for MFA, even if disabled in AUTH methods policy if previously registered via SSPR (remove weaker AUTH methods)
- Admin roles have their own SSPR policy, this opens them up to AUTH downgrade attacks and can cause sign-in loops (disable SSPR for admins)
- Possible to reset user password from security info page using FIDO2, even with no previous knowledge of password (SSPR bypass)

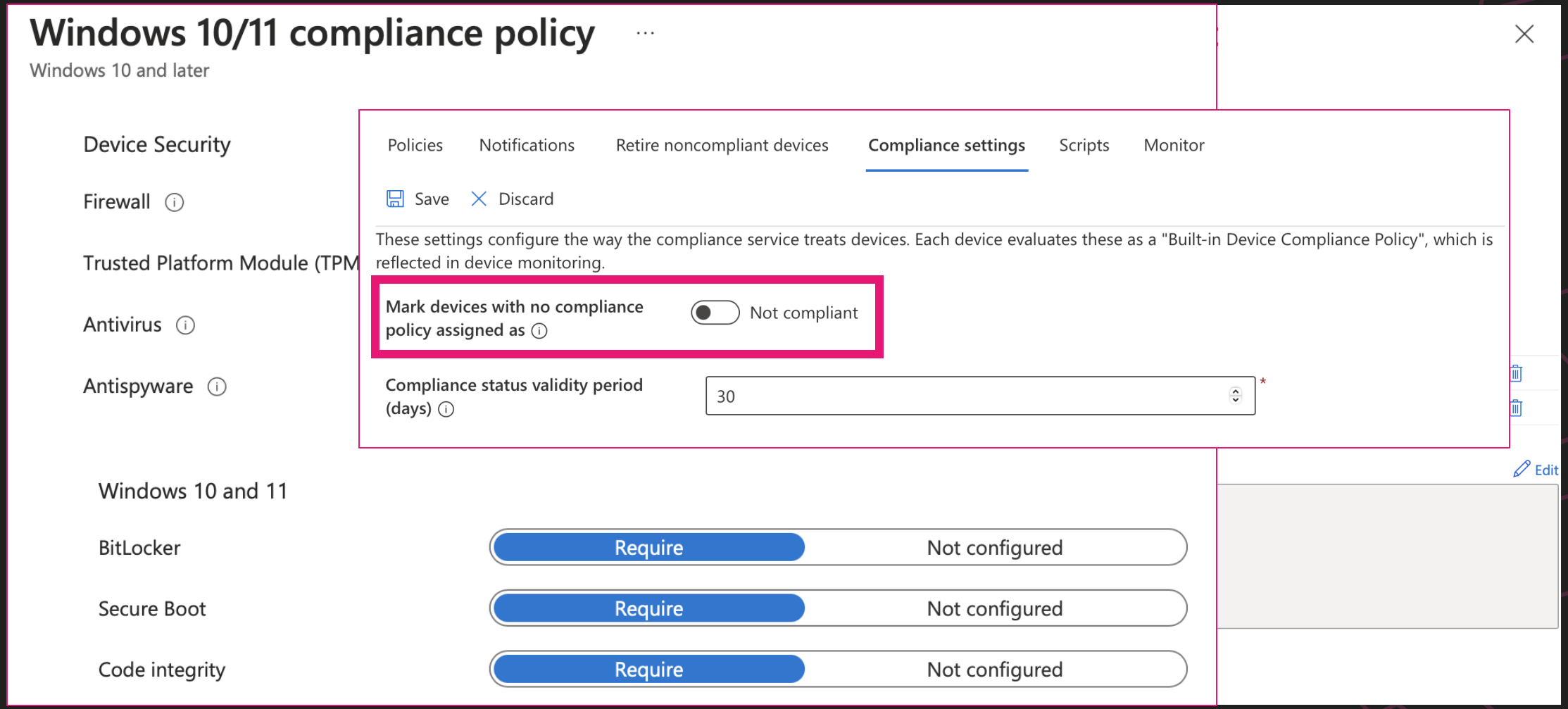
SSPR Gotcha's (Passwordless)



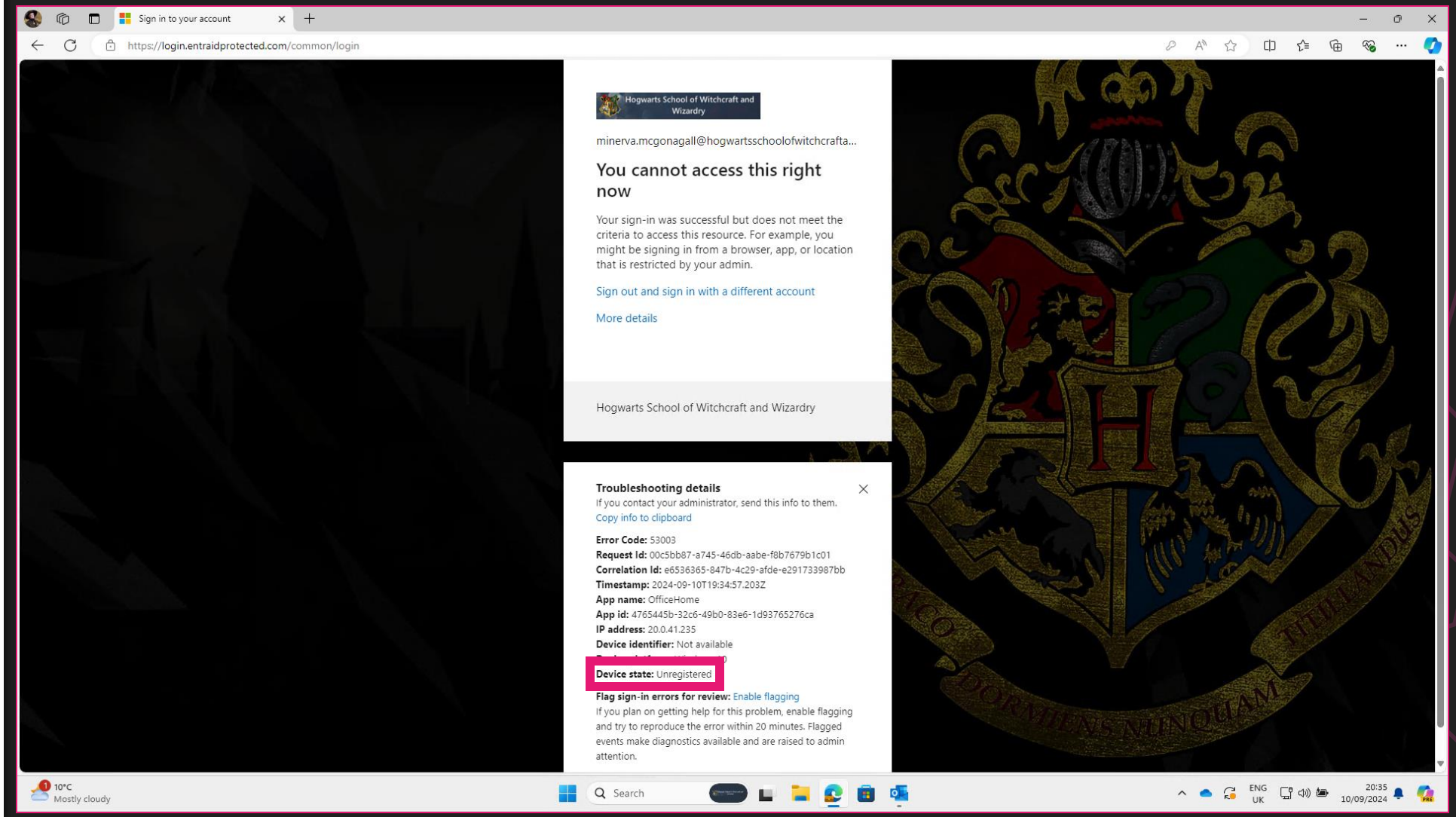
Wrap Up

- For true FIDO2 users, remove other Passwordless / MFA methods (prevent fallback)
- Disable SSPR for admins (prevent admins registering less secure methods)
- Exclude Passwordless & FIDO2 users from user risk policies (prevent sign-in / password reset loop) Use BLOCK instead
- Use authentication strengths NOT “Require MFA” checkbox (enforce strong auth methods)

Device Compliance

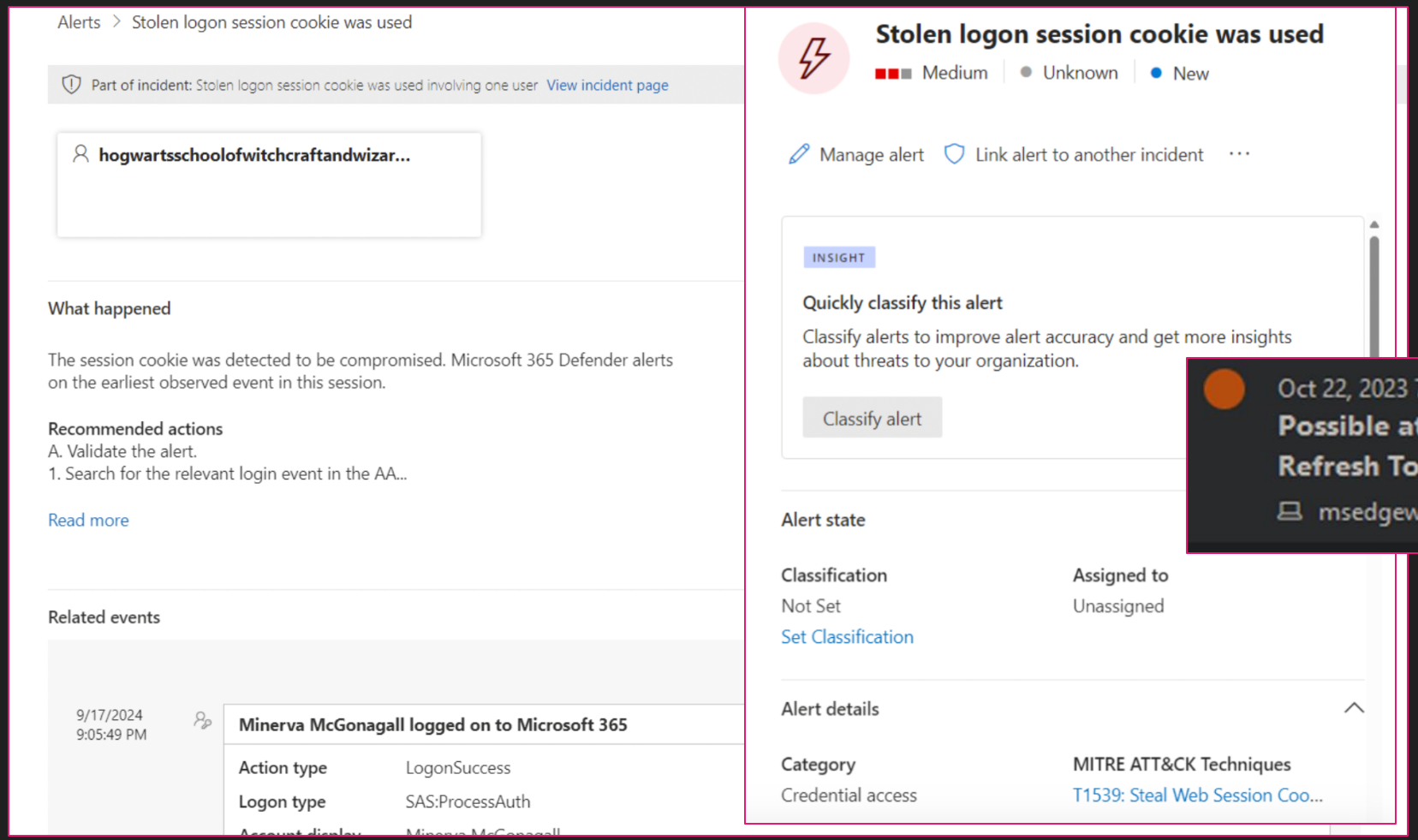


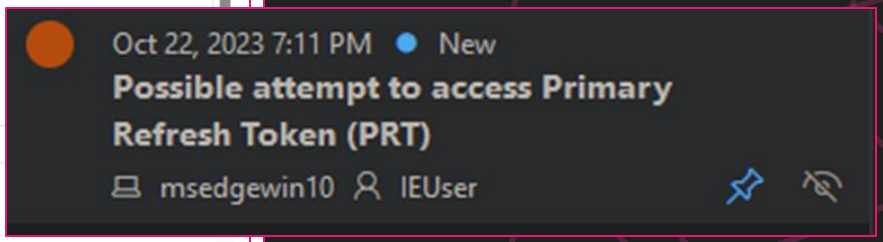
Device Compliance



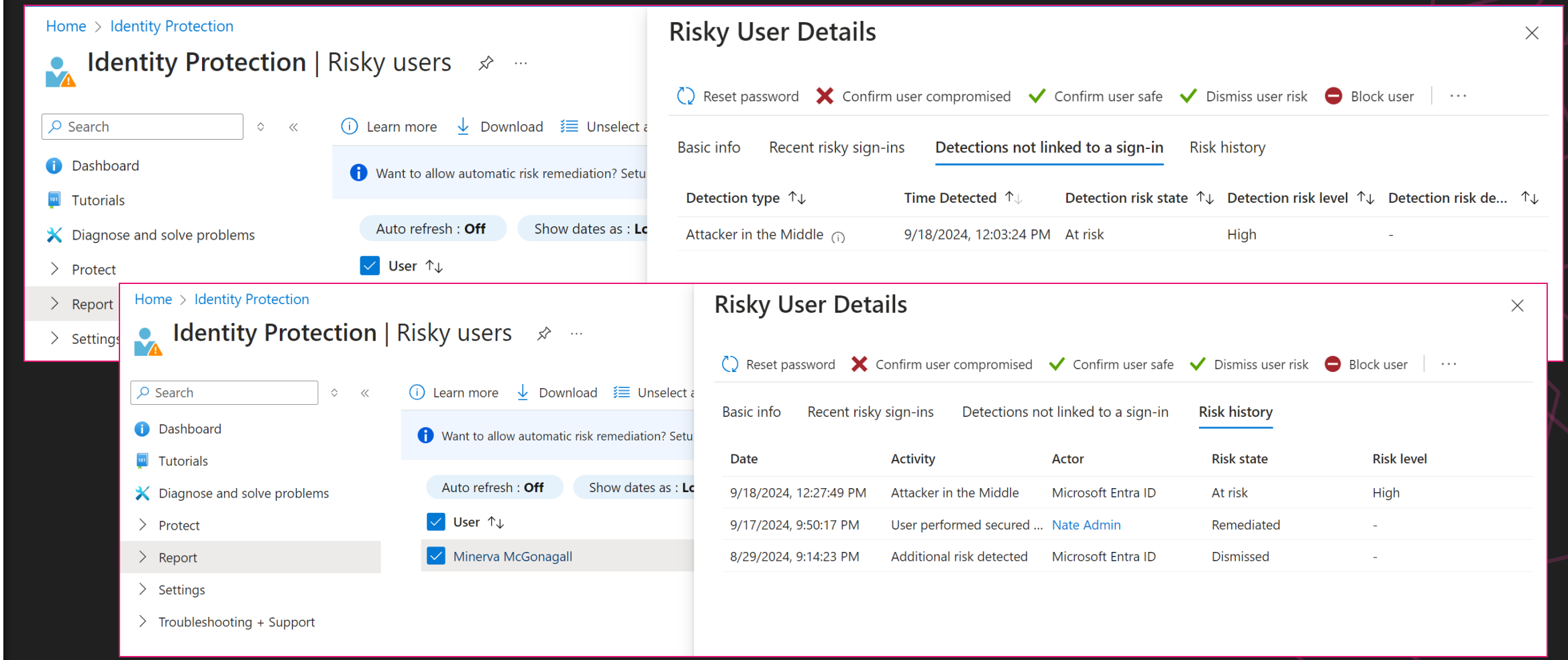
Device Compliance

Defender for Endpoint

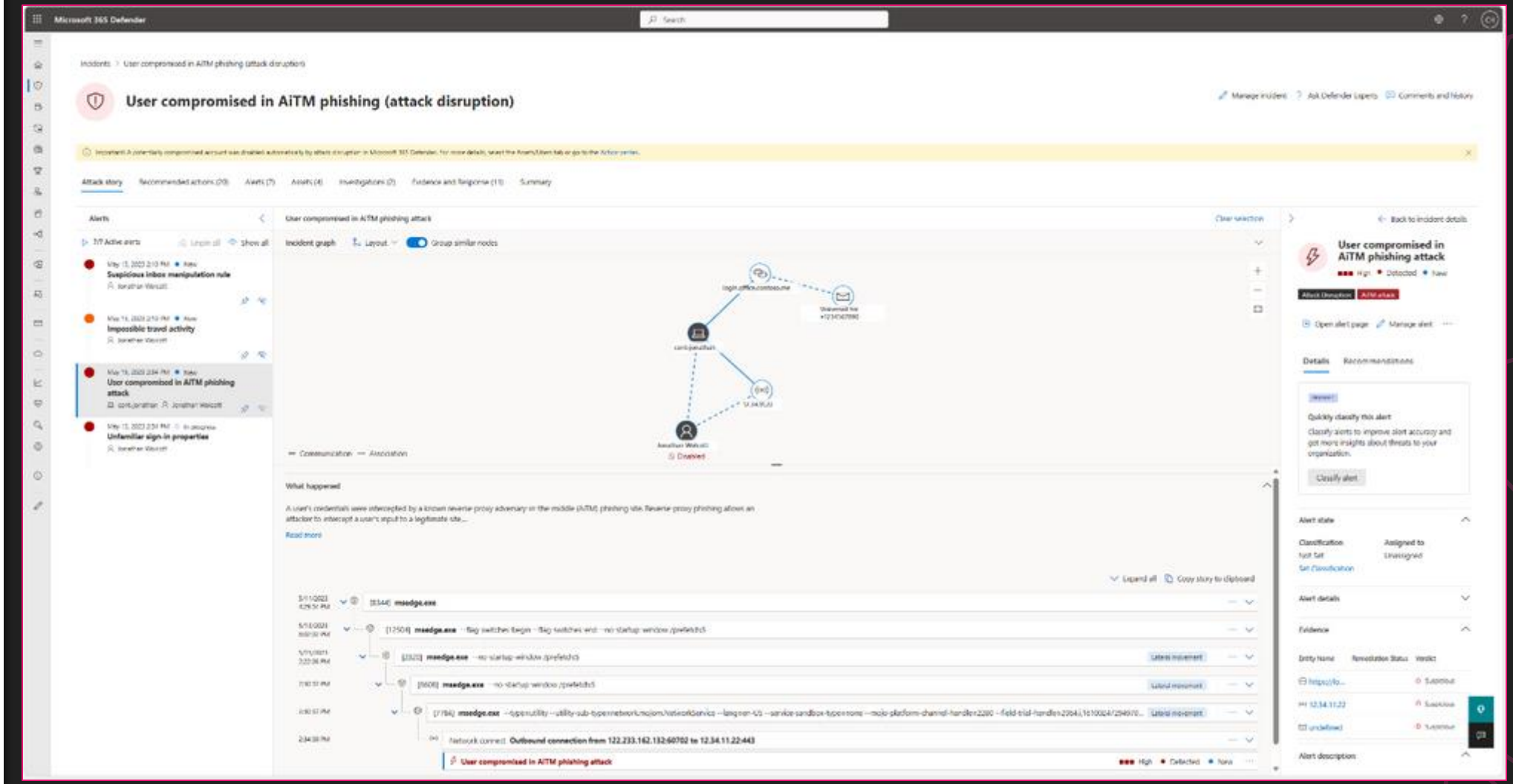




Entra ID Protection



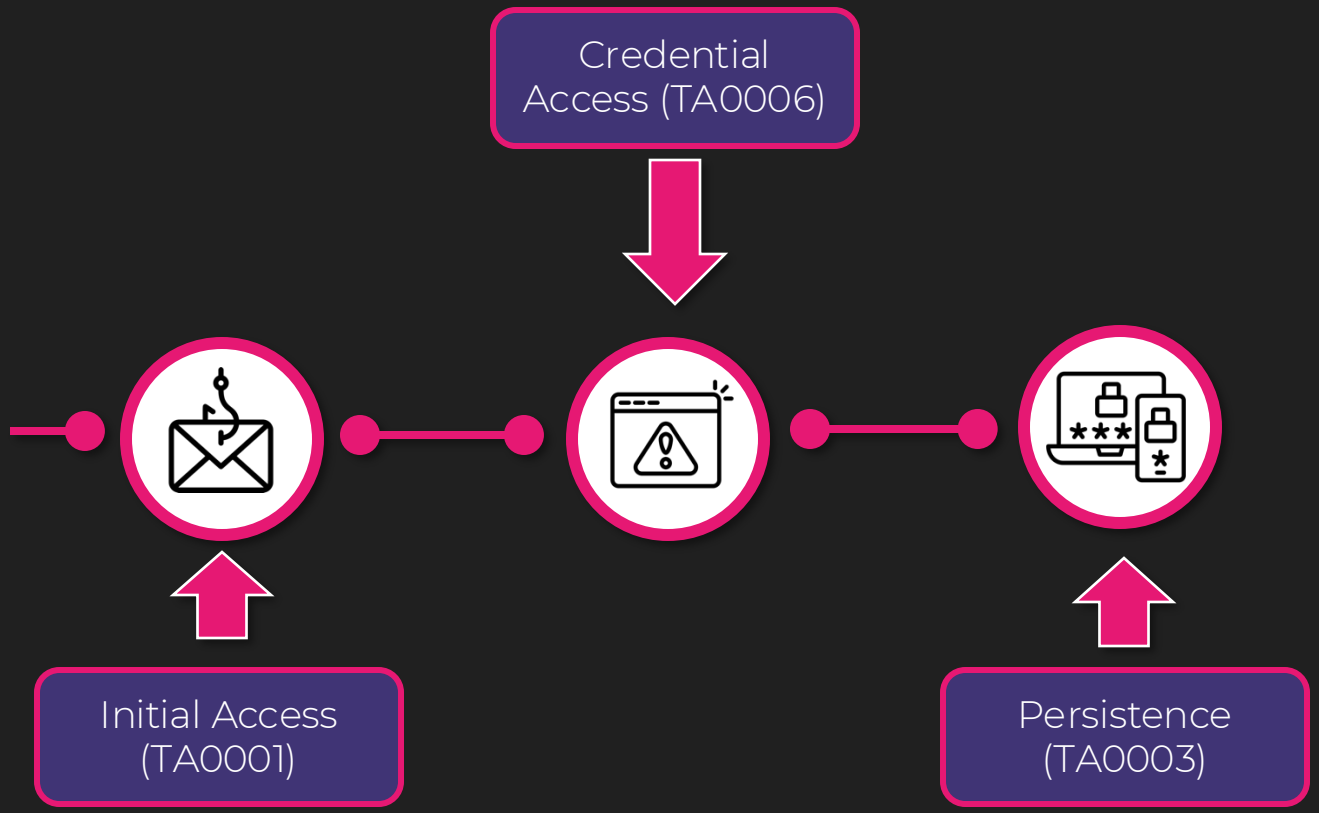
Defender XDR – Automatic Attack Disruption



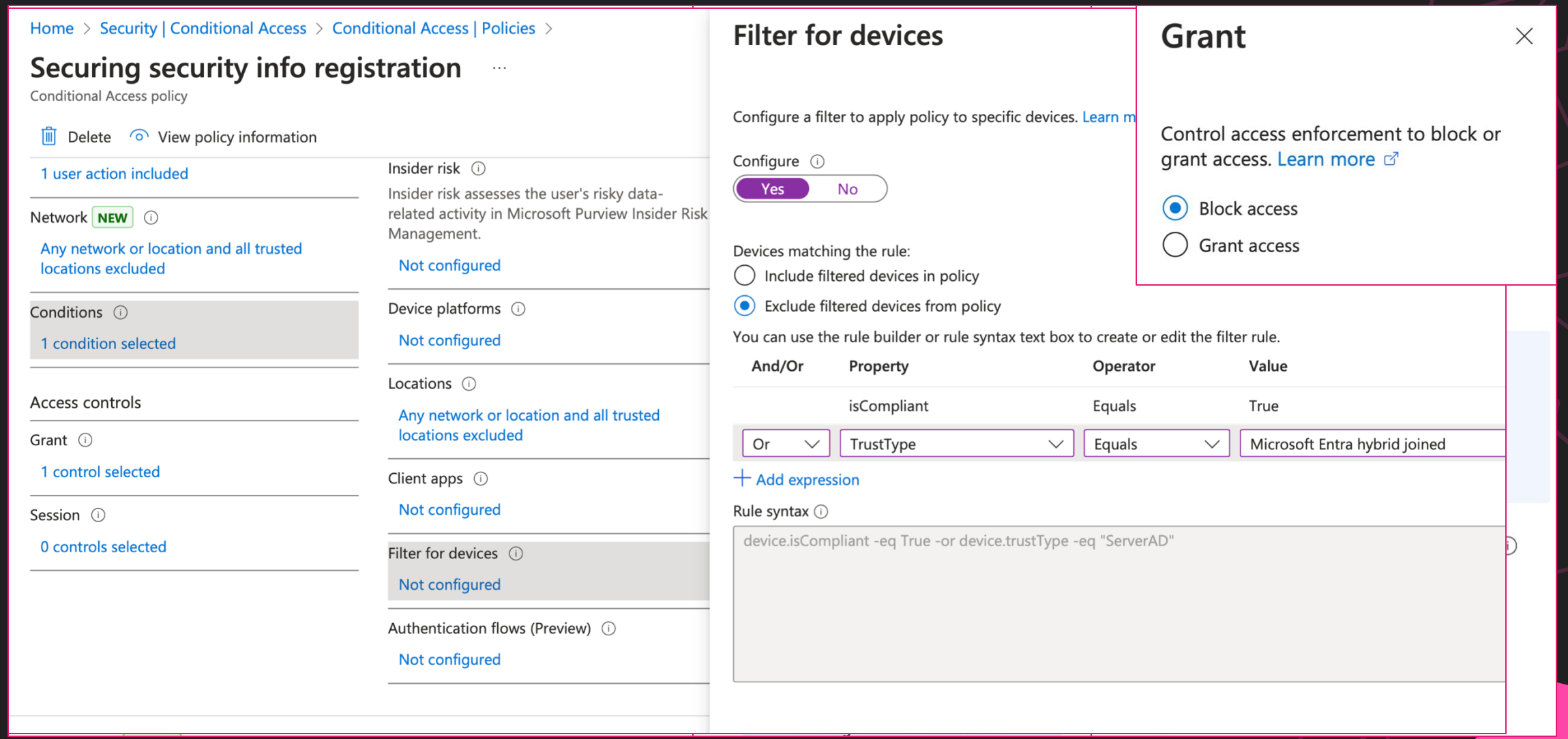
Wrap Up

- Global compliance set to “Not compliant”
- Assign device compliance policies (enroll to Intune)
- Require compliant or hybrid joined device in Conditional Access
- Use Entra ID Protection in CA policies and enable alert notification
- Onboard devices to MDE
- Defender XDR stack (automatic attack disruption)

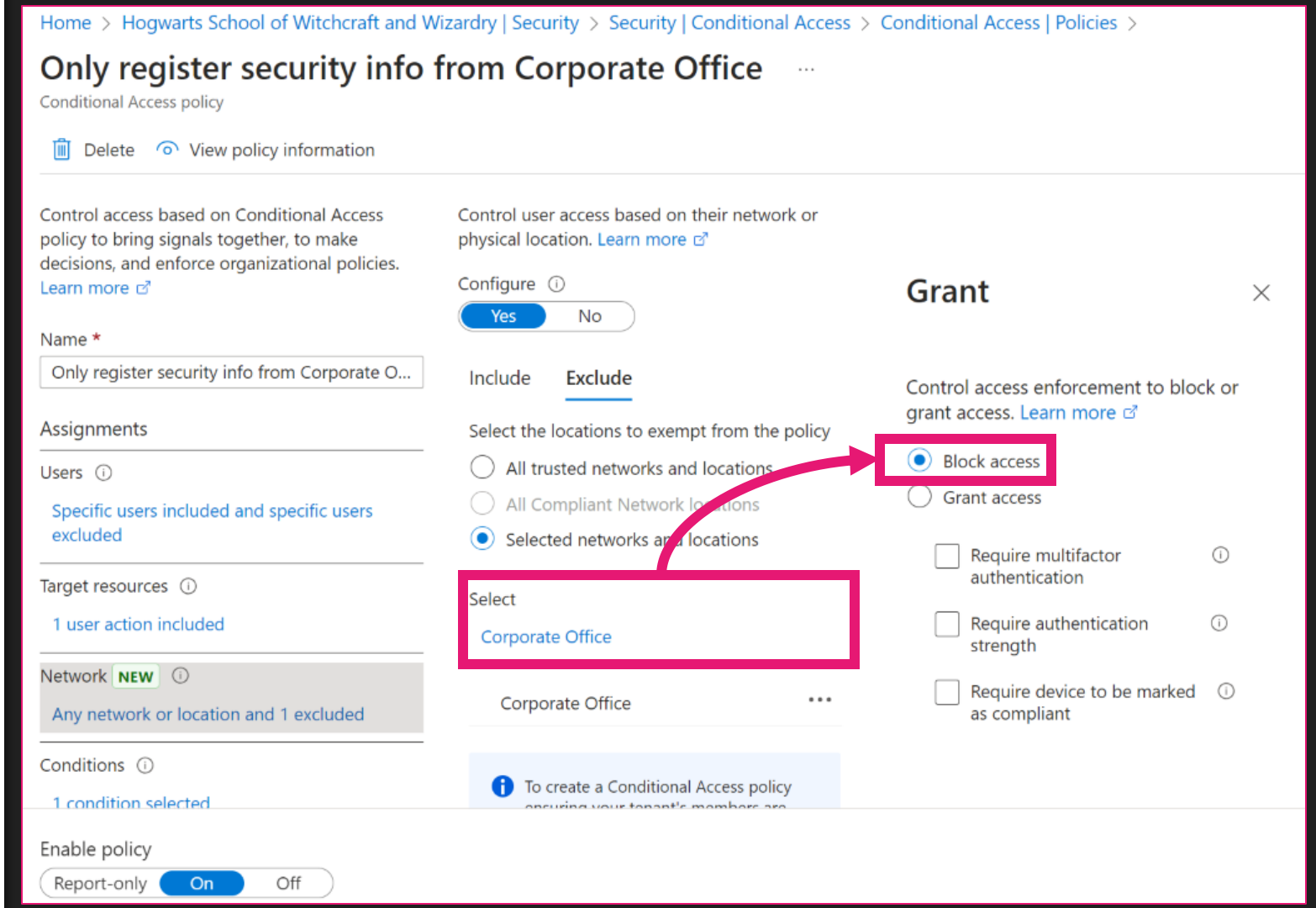
Persistence / Account Manipulation (TA0003 / T1098)



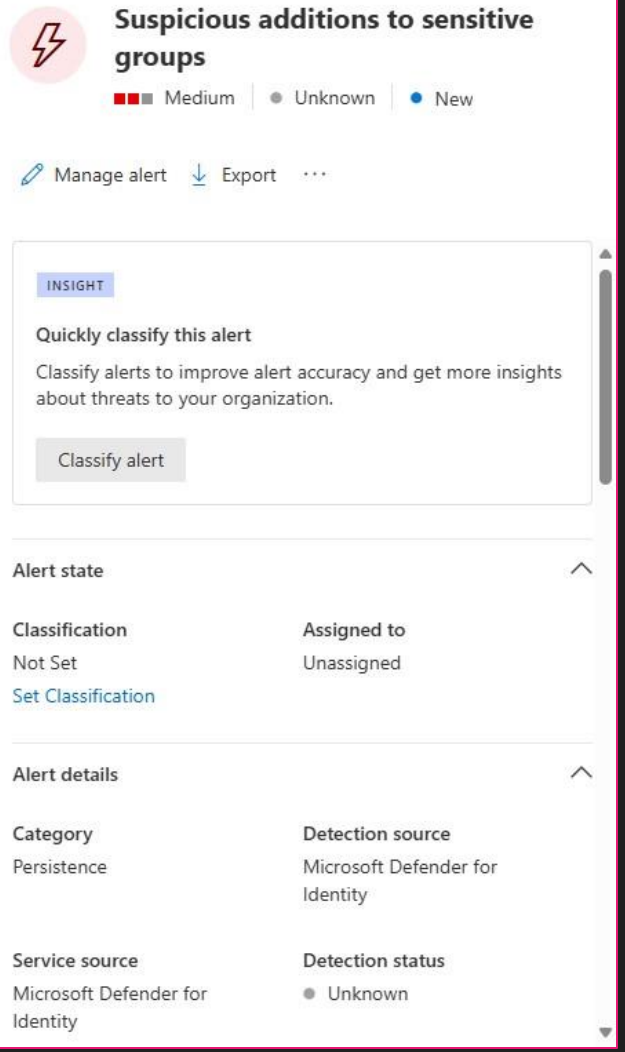
Secure Registration of Security Info

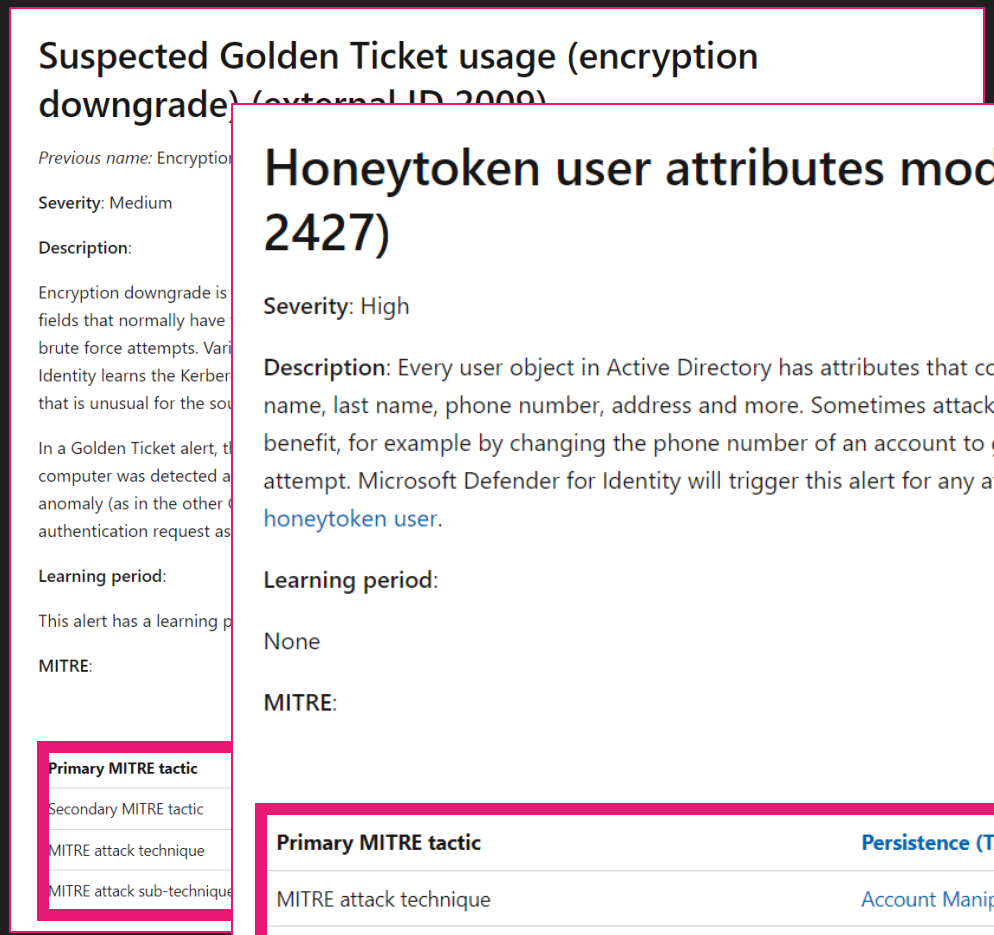


Secure Registration of Security Info



Defender for Identity





Proactive Threat Hunting

main Hunting-Queries-Detection-Rules / Sentinel / Malicious FIDO2 Registration Threat Detection.kql

mfa

SlimKQL Malicious FIDO2 Registration Threat Detection.kql ✓ 36f371d · 2 weeks ago History

Code Blame 32 lines (27 loc) · 2.33 KB Raw

```
1   // Malicious FIDO2 Registration Threat Detection
2   // https://www.linkedin.com/posts/activity-7219732839422992385-FHSM/
3
4   // In the event of a user account being compromised, a threat actor may attempt to register a passkey for persistence. This ensures that even if the account password is reset automatically, the passkey remains
5
6   let PasskeyAuthenticatorIP =
7   AuditLogs
8   | where ResultDescription contains "User registered Fido2 Authentication Method"
9   | extend AuthenticatorIP = tostring(InitiatedBy.user.ipAddress)
10  | distinct AuthenticatorIP;
11  BehaviorAnalytics
12  | where TimeGenerated > ago(90d)
13  | extend ThreatIntelIndicatorDescription = DevicesInsights.ThreatIntelIndicatorDescription
14  | where isnotempty( ThreatIntelIndicatorDescription )
15  | where SourceIPAddress has_any(PasskeyAuthenticatorIP)
16
17  // MITRE ATT&CK Mapping
18
19  // Based on the KQL code, the following MITRE ATT&CK techniques are relevant:
20
21  // T1078 - Valid Accounts:
22  // Description: The query identifies IP addresses associated with the registration of Fido2 authentication methods, which can be linked to the use of valid accounts for authentication.
23  // Detection: Monitoring for unusual or unauthorized registration of authentication methods.
24  // T1071 - Application Layer Protocol:
25  // Description: The query involves network traffic analysis by examining IP addresses and their associated threat intelligence indicators.
26  // Detection: Identifying suspicious network traffic patterns and correlating them with known threat indicators.
27  // T1087 - Account Discovery:
28  // Description: The query extends behavior analytics with threat intelligence descriptions, which can help in discovering accounts that may have been compromised.
29  // Detection: Analyzing behavior analytics data to detect unusual account activities.
30  // T1057 - Process Discovery:
31  // Description: The query's focus on behavior analytics and threat intelligence can also help in identifying processes or activities that are indicative of malicious behavior.
```

Source: SlimKQL (Steven Lim - KQLWizard) (github.com)

Proactive Threat Hunting

```
//Advanced Hunting query to parse modified StrongAuthenticationMethod

let AuthenticationMethods = dynamic(["TwoWayVoiceMobile","TwoWaySms","TwoWayVoiceOffice","TwoWayVoiceOtherMobile","TwoWaySmsOtherMobile","On
let AuthenticationMethodChanges = CloudAppEvents
| where ActionType == "Update user." and RawEventData contains "StrongAuthenticationMethod"
| extend Target = tostring(RawEventData.ObjectId)
| extend Actor = tostring(RawEventData.UserId)
| mv-expand ModifiedProperties = parse_json(RawEventData.ModifiedProperties)
| where ModifiedProperties.Name == "StrongAuthenticationMethod"
| project Timestamp,Actor,Target,ModifiedProperties,RawEventData,ReportId;
let OldValues = AuthenticationMethodChanges
| extend OldValue = parse_json(tostring(ModifiedProperties.OldValue))
| mv-apply OldValue on (extend Old_MethodType=tostring(OldValue.MethodType),Old_Default=tostring(OldValue.Default) | sort by Old_MethodType)
let NewValues = AuthenticationMethodChanges
| extend NewValue = parse_json(tostring(ModifiedProperties.NewValue))
| mv-apply NewValue on (extend New_MethodType=tostring(NewValue.MethodType),New_Default=tostring(NewValue.Default) | sort by New_MethodType)
let RemovedMethods = AuthenticationMethodChanges
| join kind=inner OldValues on ReportId
| join kind=leftouter  NewValues  on ReportId,$left.Old_MethodType==$right.New_MethodType
| project Timestamp,ReportId,ModifiedProperties,Actor,Target,Old_MethodType,New_MethodType
| where Old_MethodType != New_MethodType
| extend Action = strcat("Removed (" , AuthenticationMethods[toint(Old_MethodType)], ") from Authentication Methods.")
| extend ChangedValue = "Method Removed";
let AddedMeth
| join kind=i
| join kind=l
| project Tim
| where Old_M
| extend Acti
| extend Char
let DefaultMe
| join kind=i
| join kind=i
| where Old_D
| join kind=inner OldValues on ReportId | where Old_Default1 == "true" and Old_MethodType1 != New_MethodType | extend Old_MethodType = Old_M
| extend Action = strcat("Default Authentication Method was changed to (" , AuthenticationMethods[toint(New_MethodType)], ").")
| extend ChangedValue = "Default Method";
union RemovedMethods,AddedMethods,DefaultMethodChanges
| project Timestamp,Action,Actor,Target,ChangedValue,OldValue=case(isempty(Old_MethodType), "",strcat(Old_MethodType,": ", AuthenticationMet
| distinct *
```

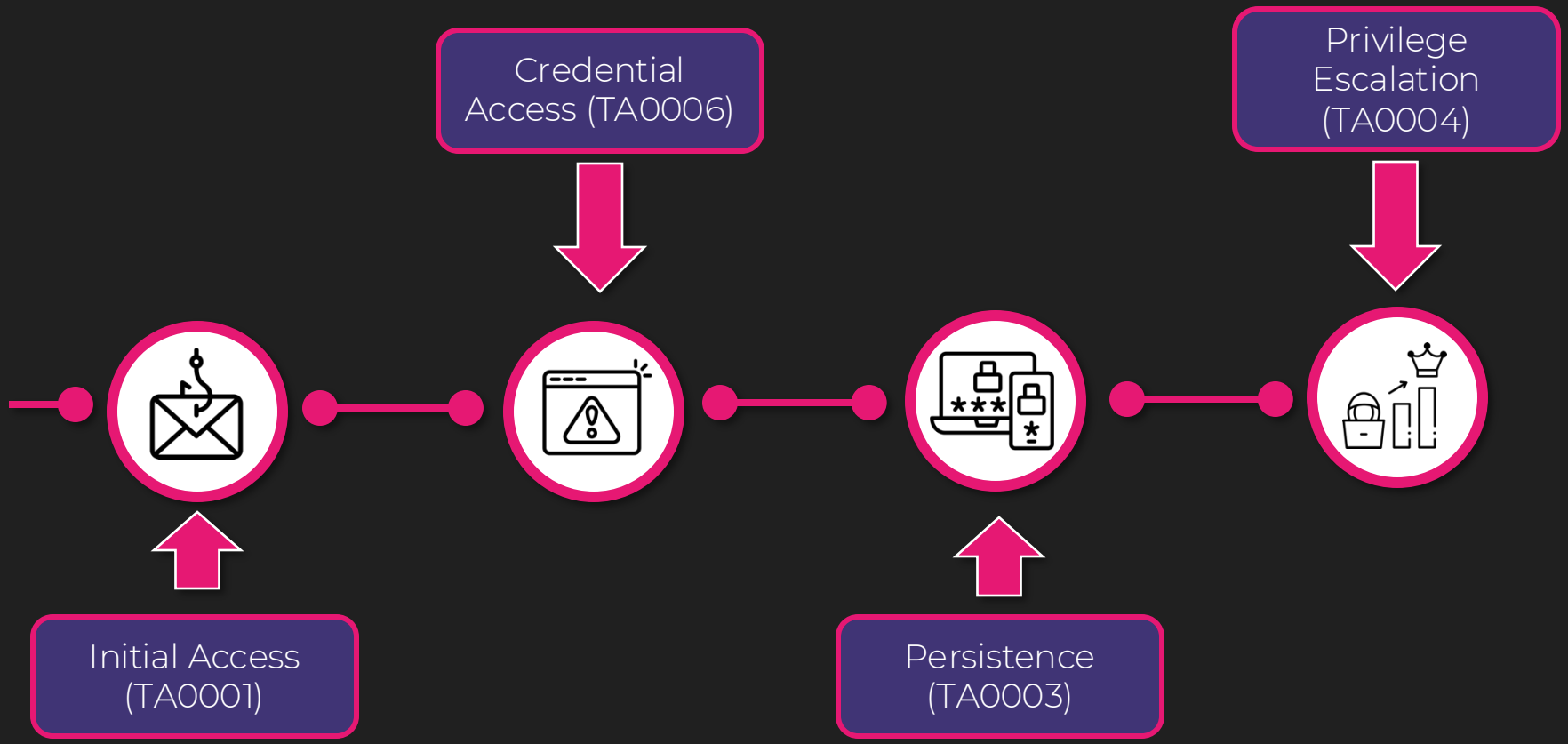
Timestamp (UTC)	Action	Actor	Target	ChangedValue	OldValue	NewValue
2024-04-16 15:37:56.0000	Added (TwoWayVoiceMobile) as Authentication Method.	Meran@contoso.com	Diego@contoso.com	Method Added		0: TwoWayVoiceMobile
2024-04-16 15:37:56.0000	Added (OneWaySms) as Authentication Method.	Meran@contoso.com	Diego@contoso.com	Method Added		5: OneWaySms
2024-04-16 15:45:06.0000	Default Authentication Method was changed to (OneWaySms).	Meran@contoso.com	Diego@contoso.com	Default Method	6: PhoneAppNotification	5: OneWaySms
2024-04-16 18:07:56.0000	Removed (OneWaySms) from Authentication Methods.	Diego@contoso.com	Diego@contoso.com	Method Removed	5: OneWaySms	
2024-04-16 18:07:56.0000	Removed (TwoWayVoiceMobile) from Authentication Methods.	Diego@contoso.com	Diego@contoso.com	Method Removed	0: TwoWayVoiceMobile	
2024-04-16 18:07:56.0000	Default Authentication Method was changed to (PhoneAppNotification).	Diego@contoso.com	Diego@contoso.com	Default Method	5: OneWaySms	6: PhoneAppNotification

Source: Hunting for MFA manipulations in Entra ID tenants using KQL - Microsoft Community Hub

Wrap Up

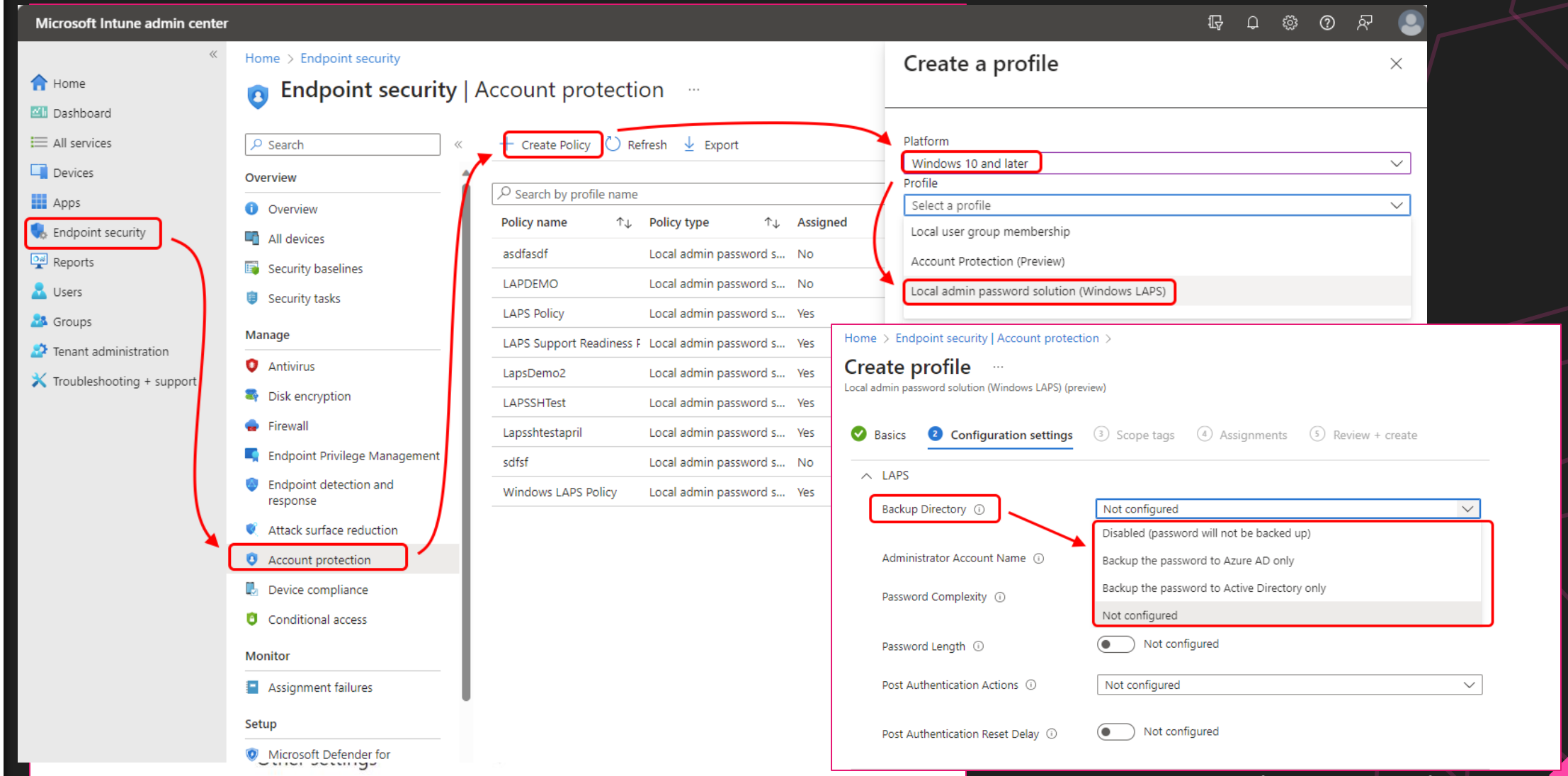
- Require device compliance, MFA and/or SIF every time for registration of security info
- Consider restricting security info registration to office IP or secure service edge (SSE)
- Deploy Defender for Identity in on-premises environments
- Proactive threat hunting with automation where possible

Privilege Escalation / Elevated Access (TA0004 / T1548)

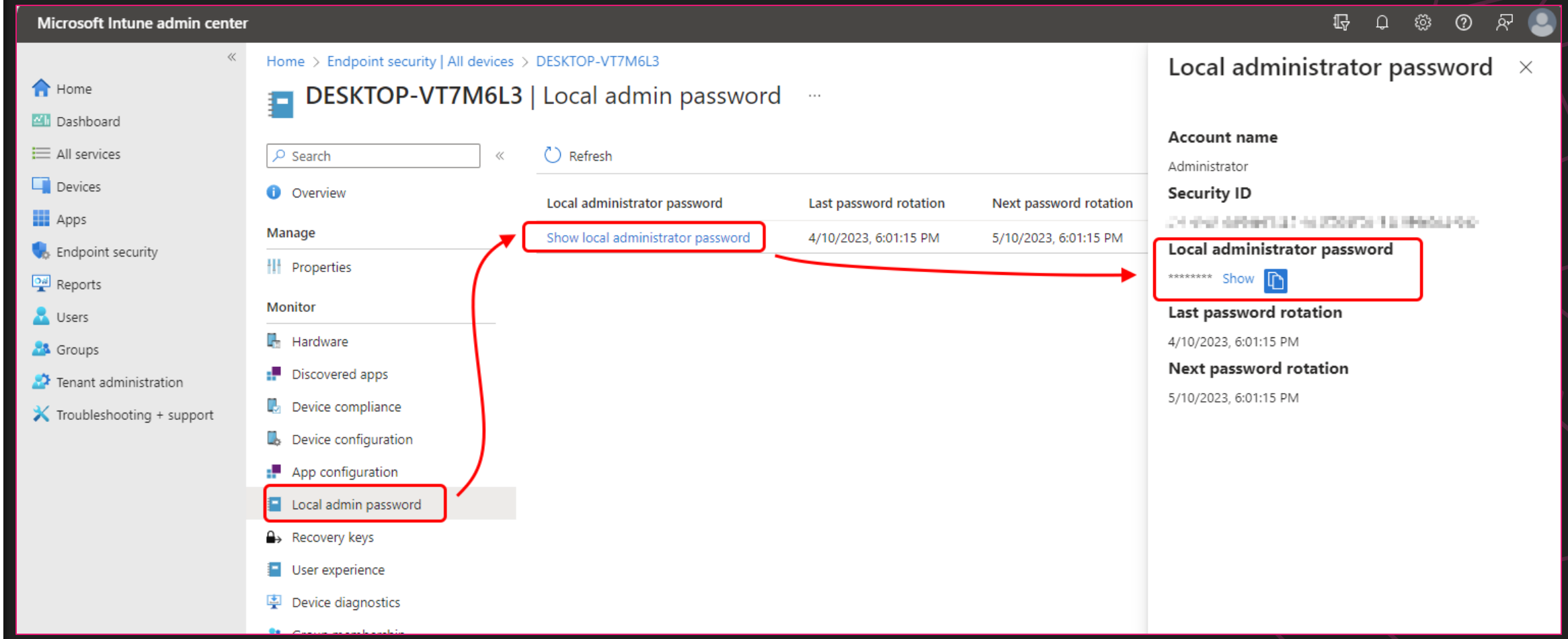


Protect Local Admin Accounts - LAPS

Local Admin Password Solution (LAPS)



Local Admin Password Solution (LAPS)



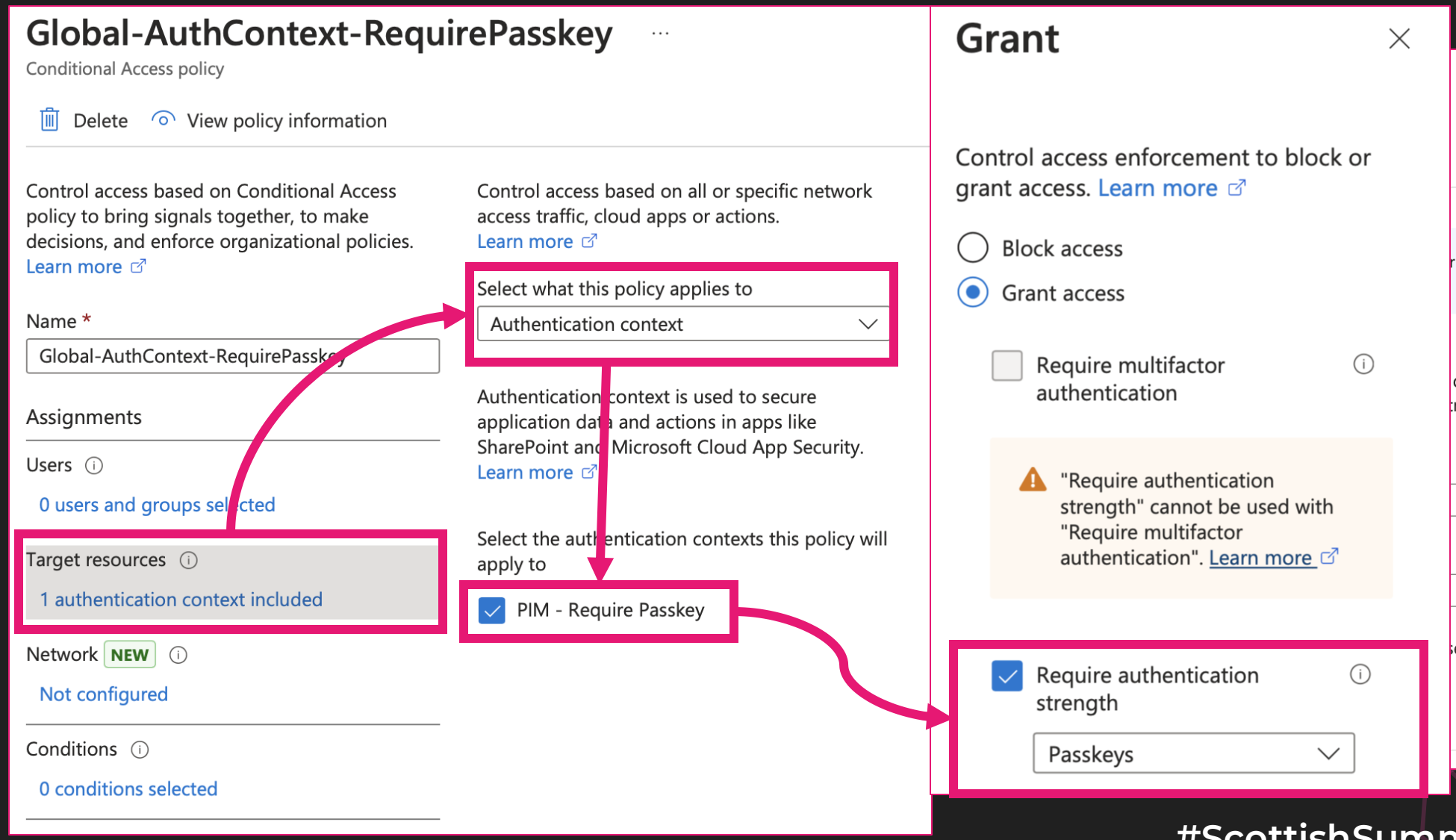
Security Principles / Best Practices

- No standing access
- Account separation
- Least privilege permissions
- Just-In-Time access (PIM)

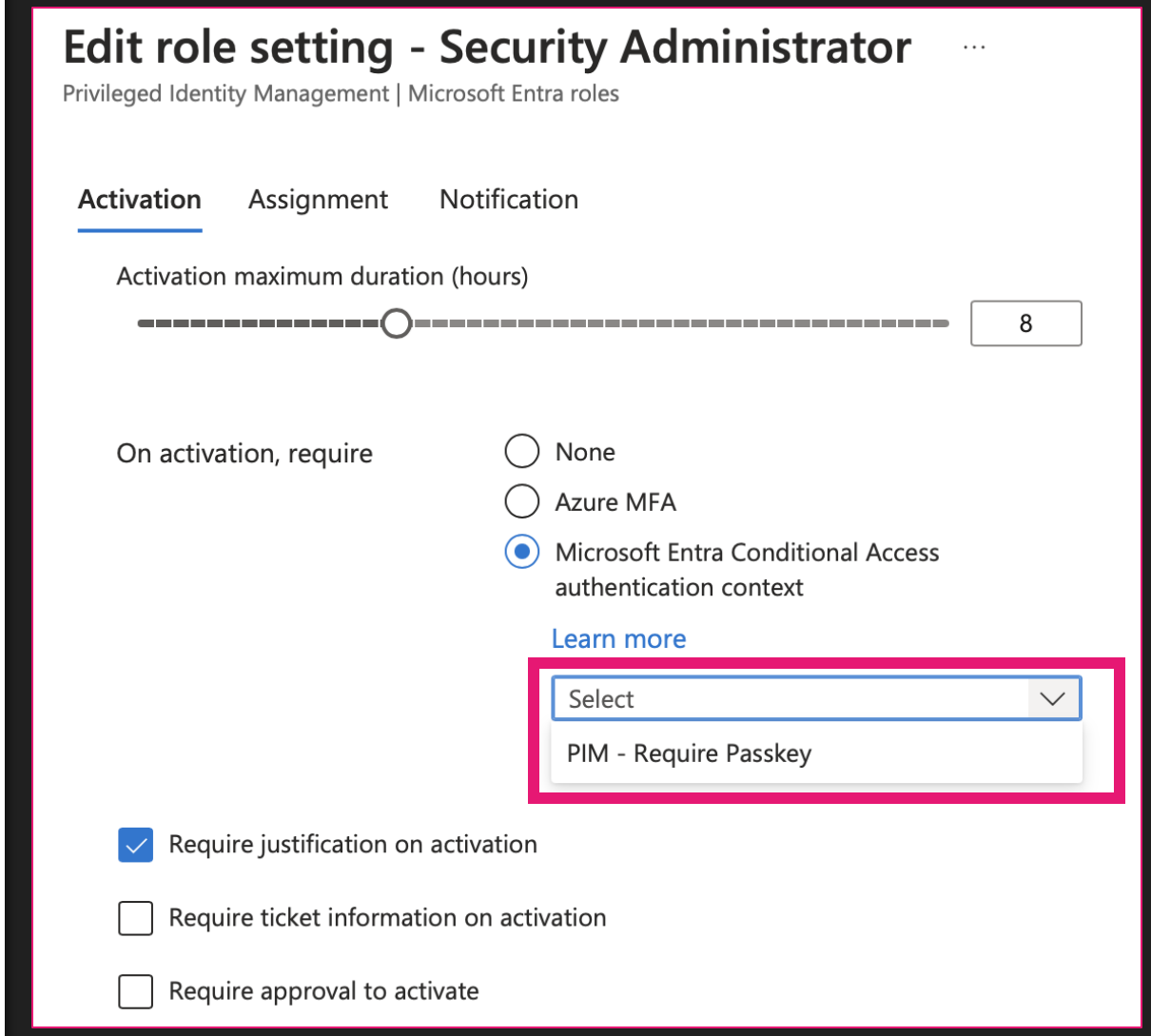
Privileged Identity Management (PIM)

- **Just-in-time** access to resources
- Assign **time-bound** access to resources
- Require **approval** to activate privileged roles
- **Enforce MFA** to activate roles (be careful here!)
- Require **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal/external audits
- Prevents removal of the **last active GA and PRA**

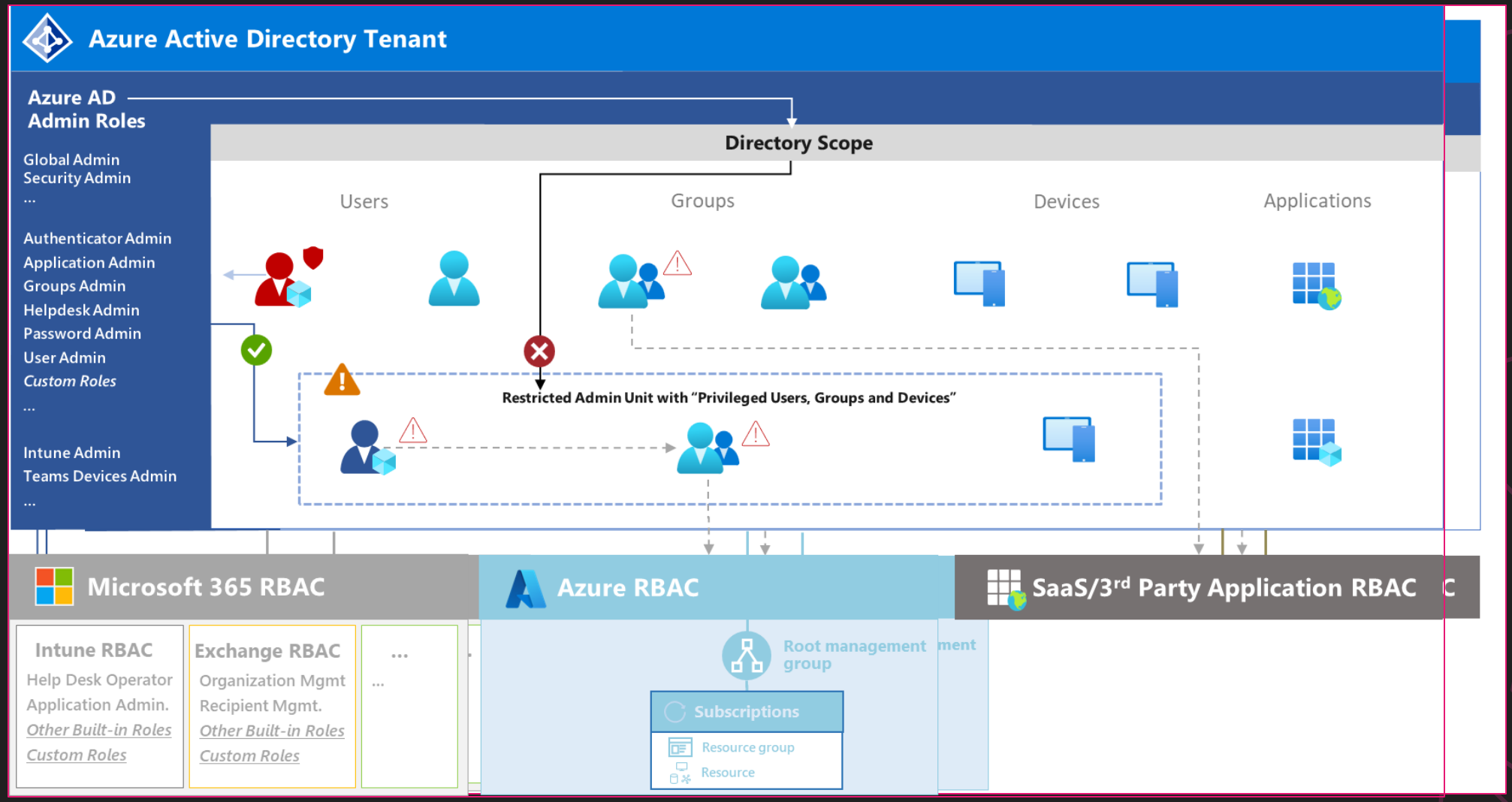
PIM – Authentication Contexts



PIM – Authentication Contexts



Administrative Units / RMAU's

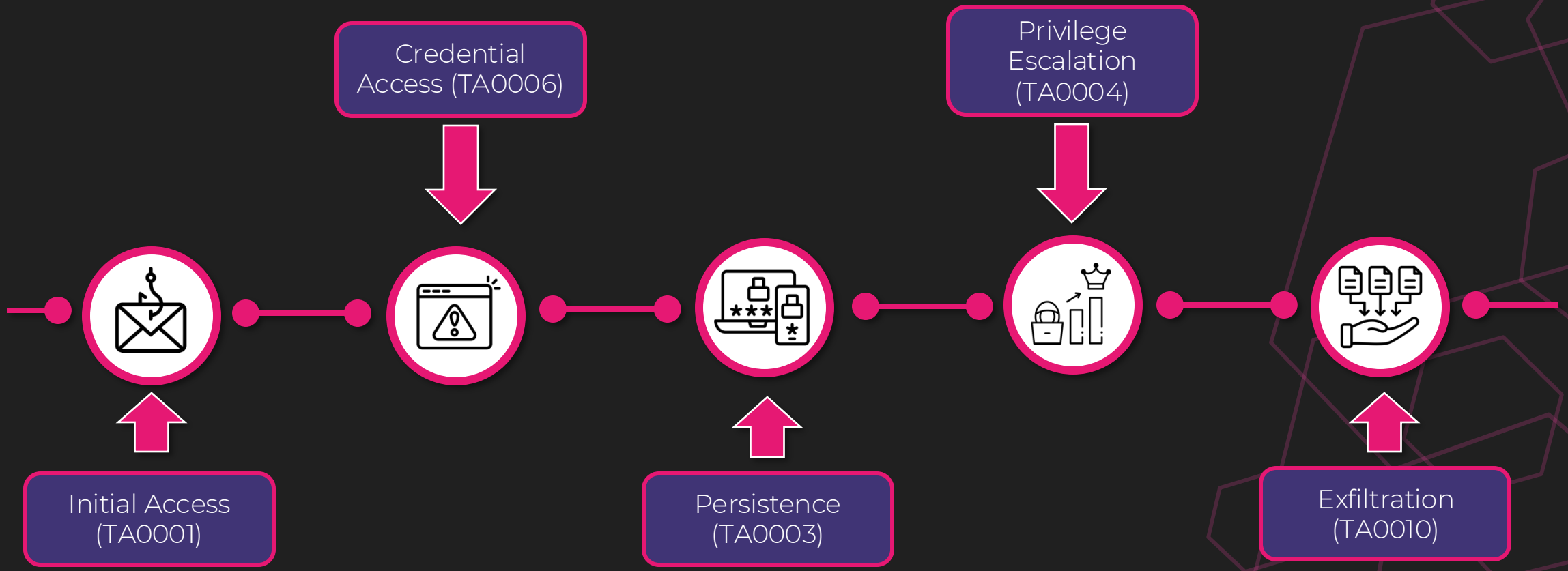


Source: https://www.cloud-architekt.net/restricted-management-administrative-unit/

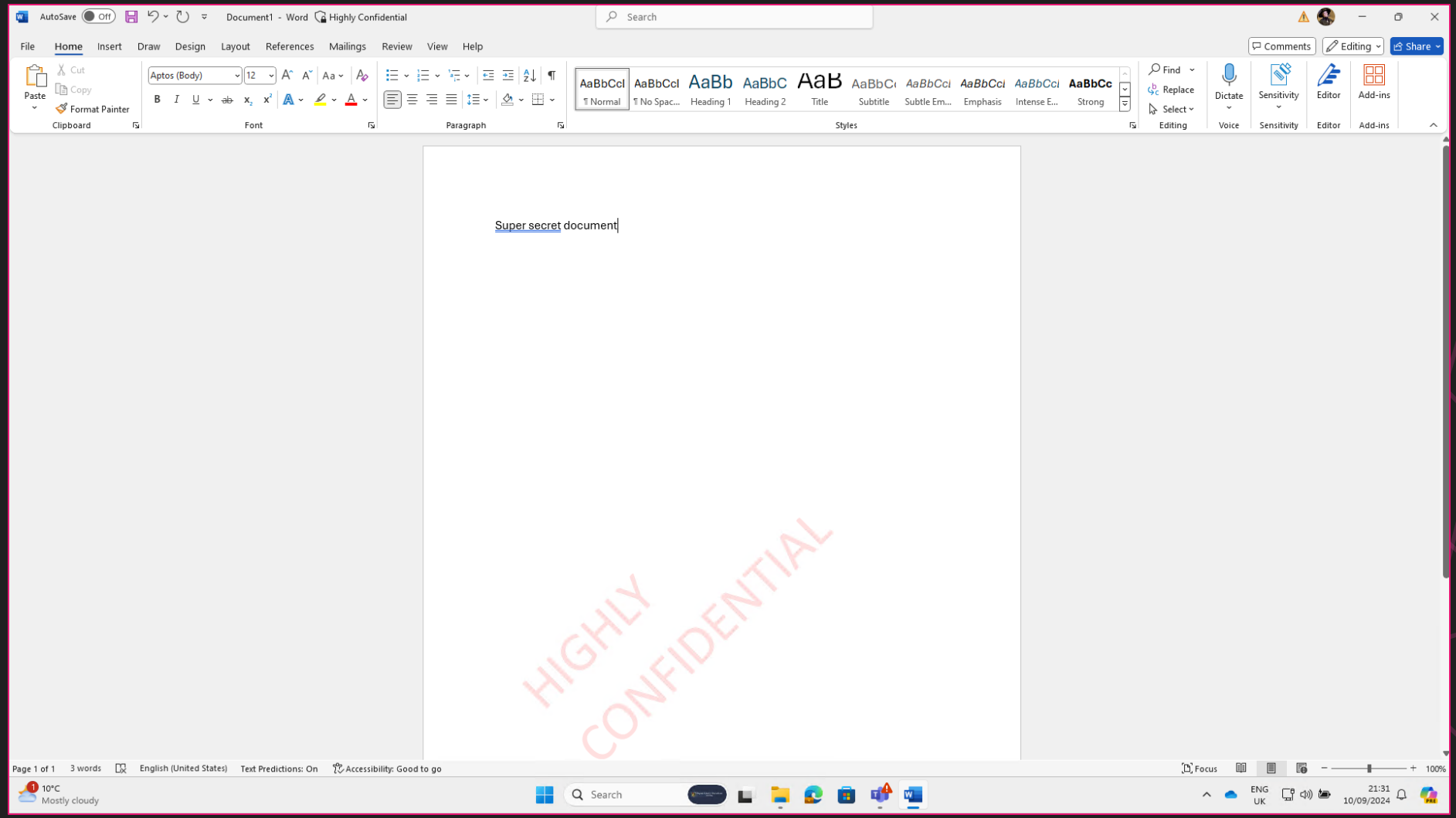
Wrap Up

- Use LAPS to secure local admin access
- Separate admin account from day-to-day account
- Use least privilege
- Use Privileged Identity Management (PIM)
- Do NOT use Azure MFA for role activation
- Use Authentication Context with Authentication Strengths and phish-resistant MFA methods for activation
- Use Administrative Units and RMAU's (Entra ID tiering)

Exfiltration / Automated Exfiltration (TA0010 / T1020)

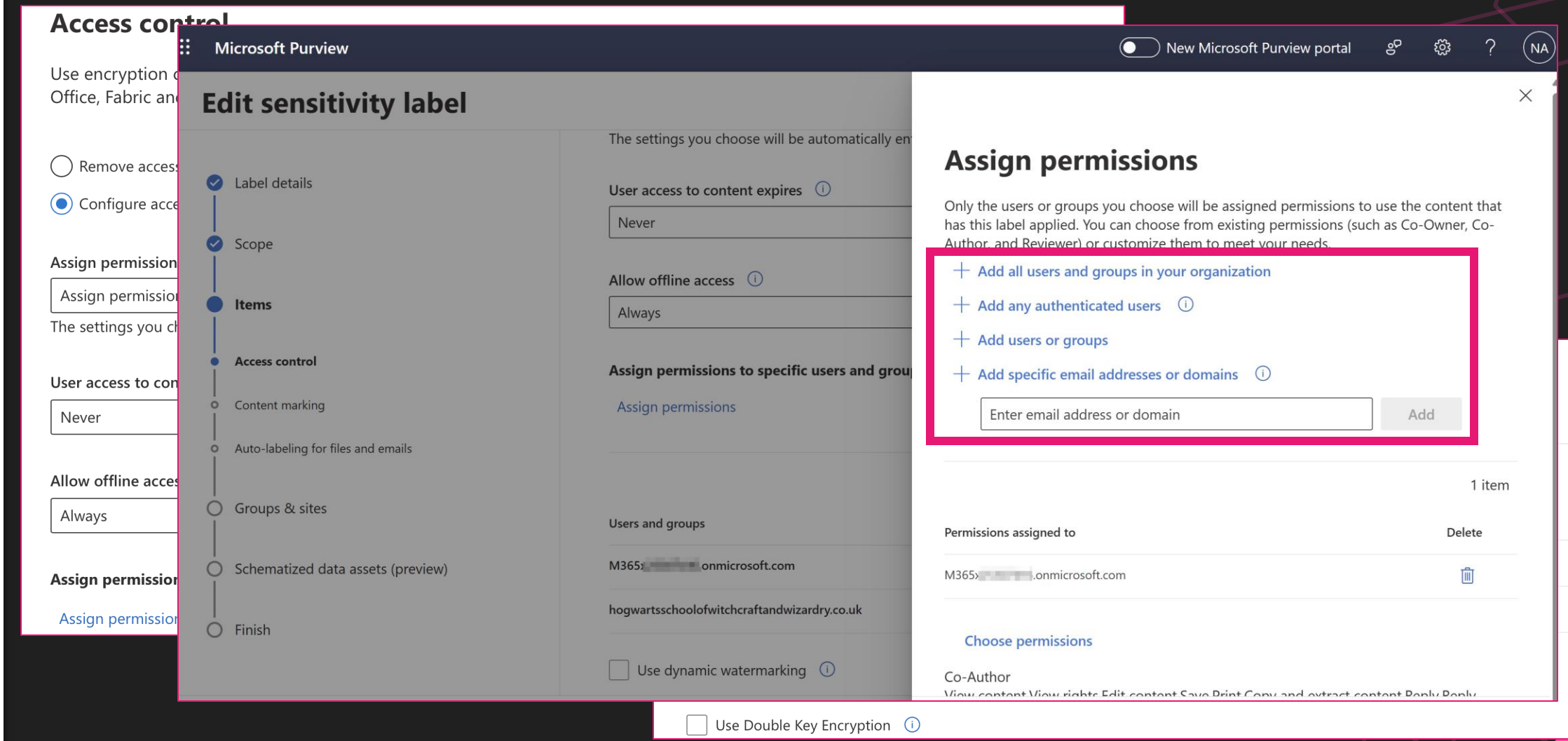


Sensitivity Labels

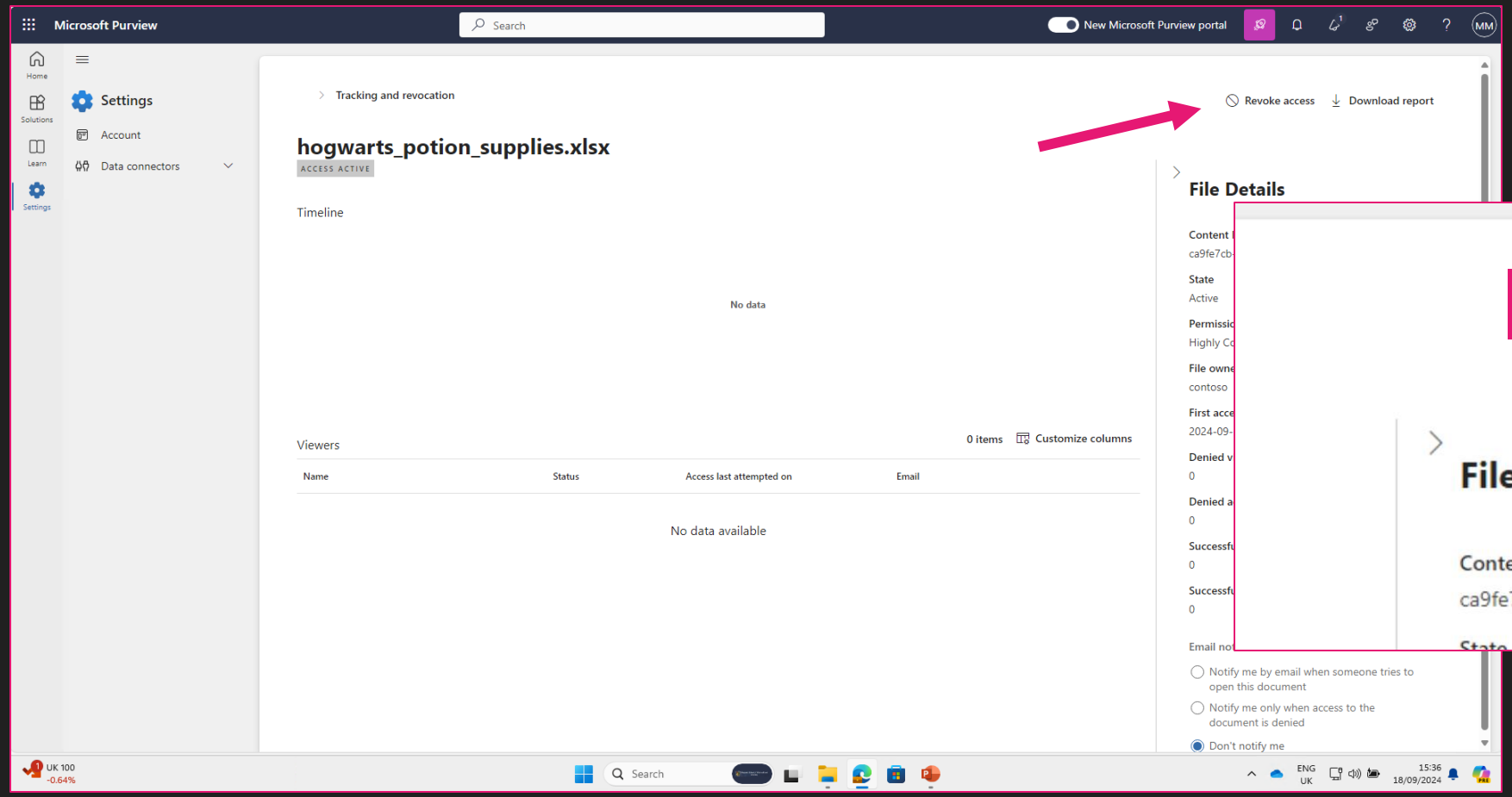


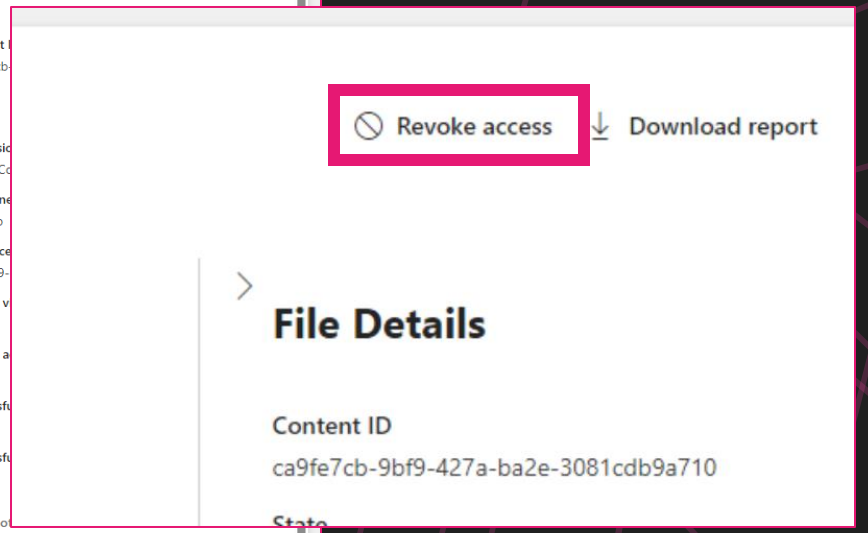
#ScottishSummit2024

Sensitivity Labels



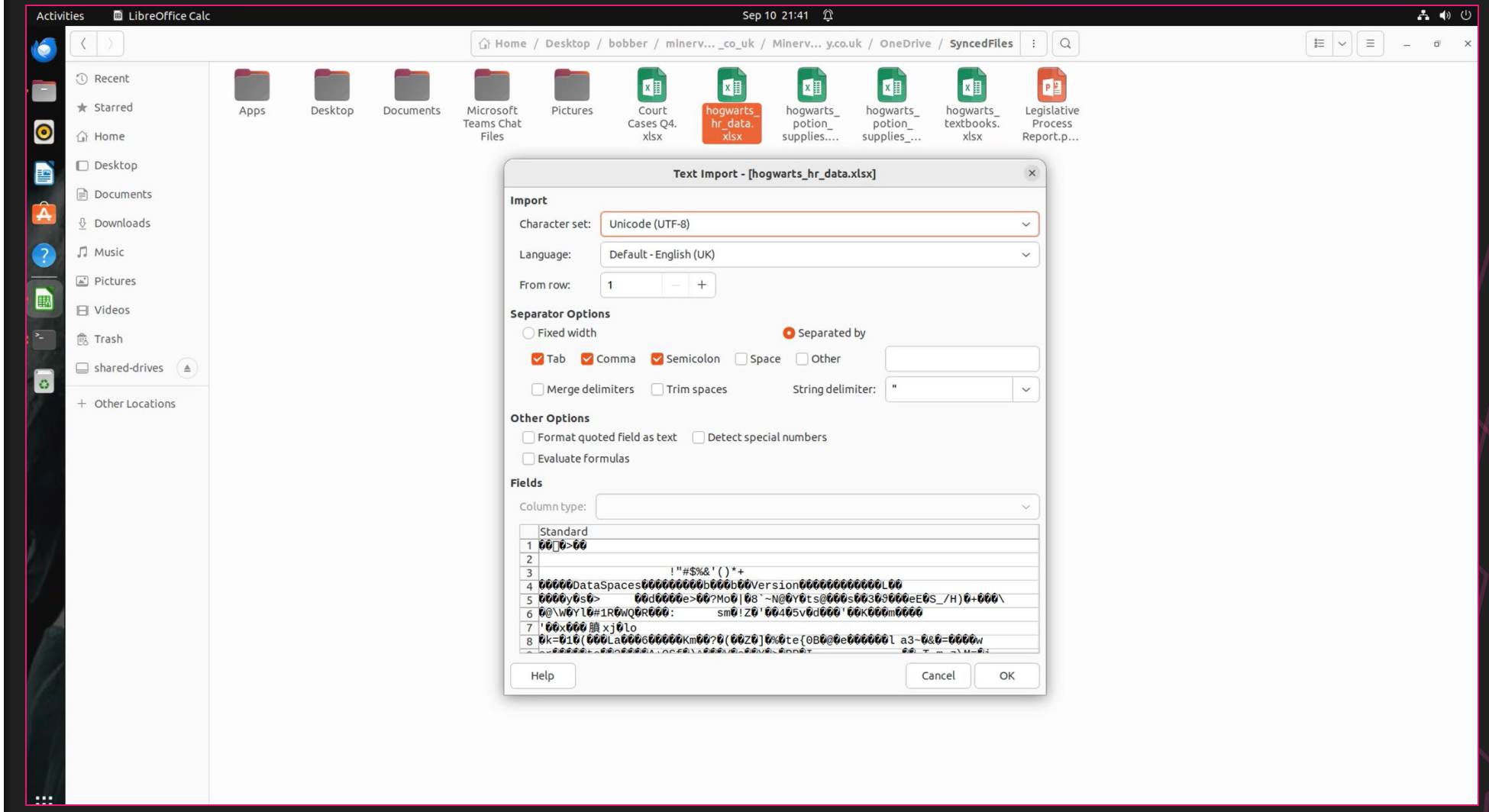
Sensitivity Labels



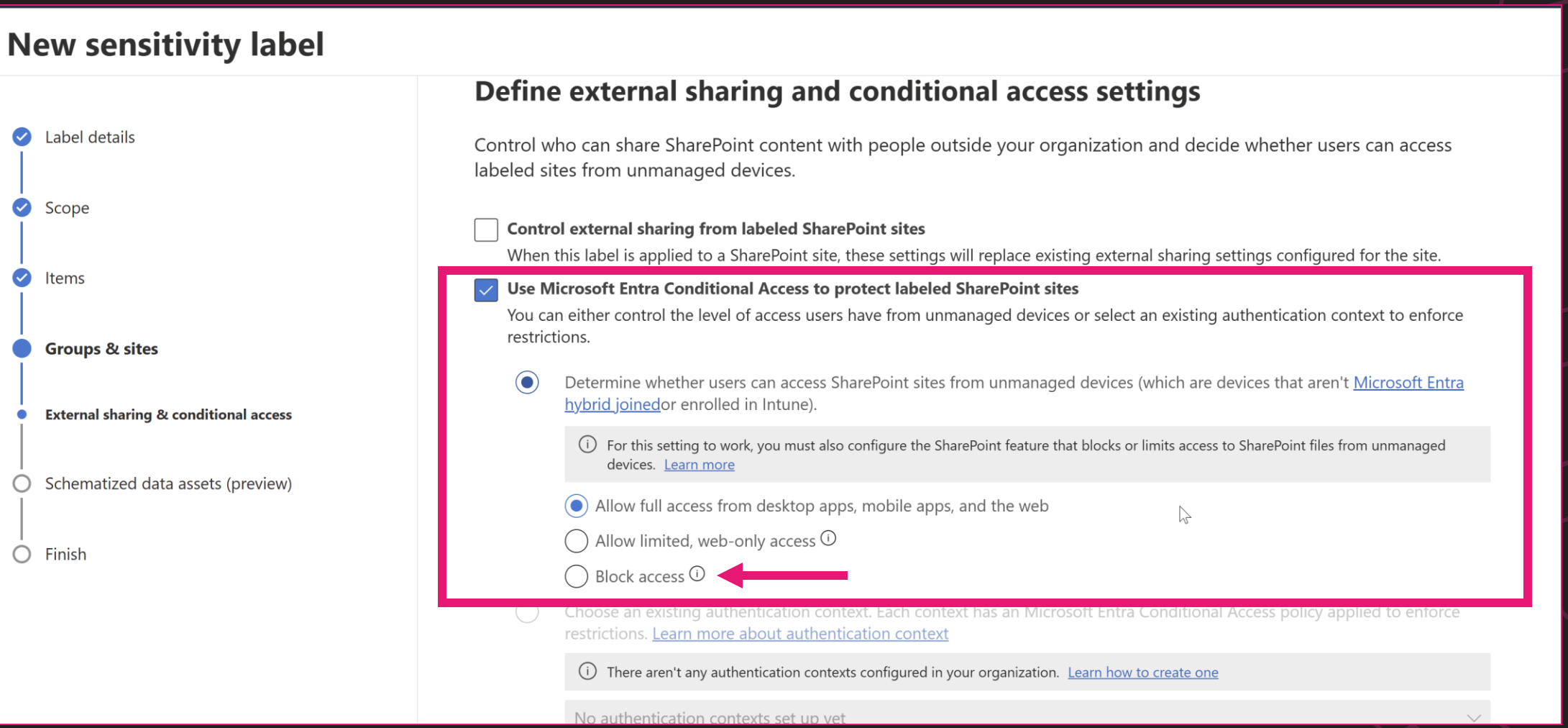


#ScottishSummit2024

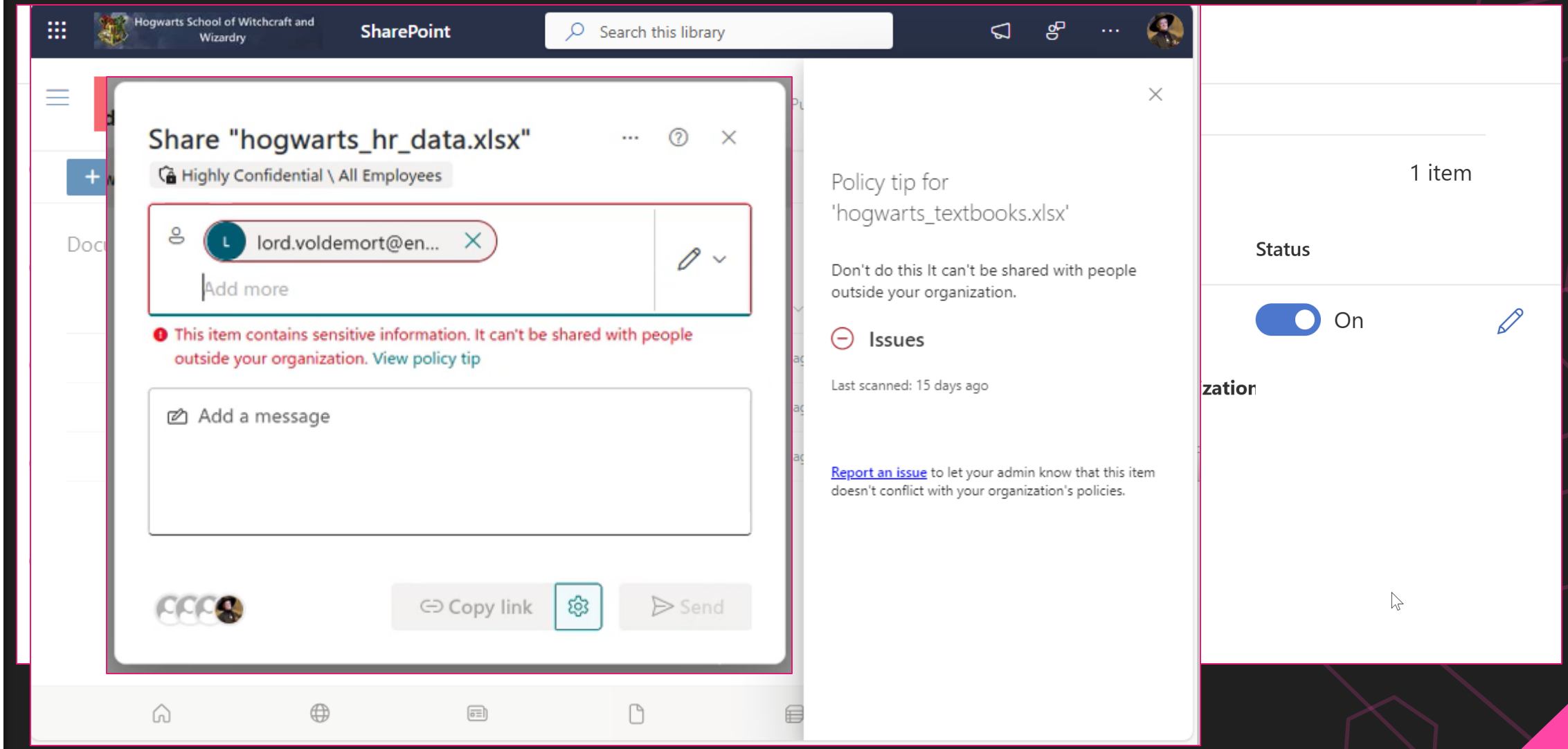
Sensitivity Labels



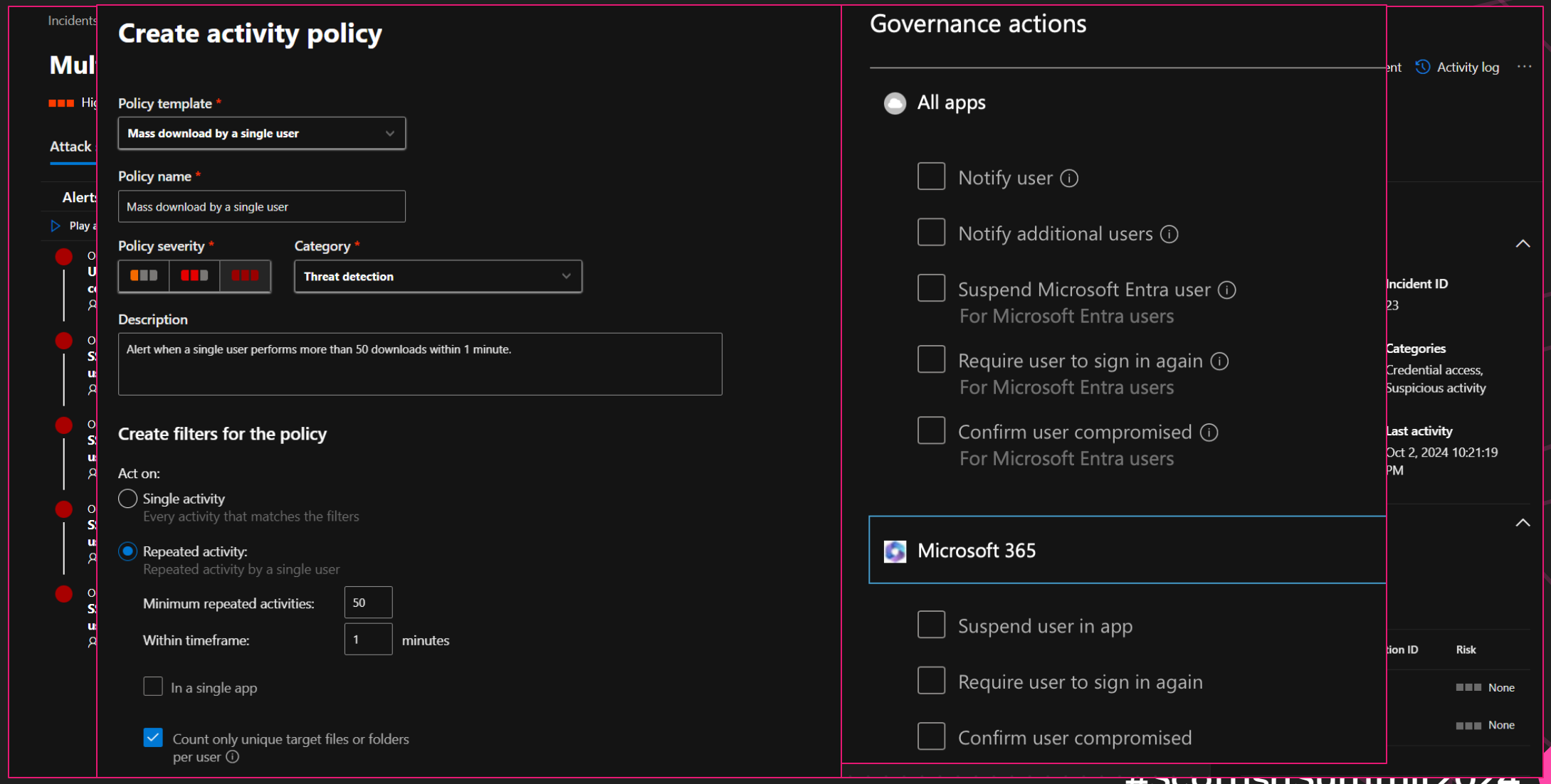
Sensitivity Labels



Data Loss Prevention



Defender for Cloud Apps



And everything else...

Insider Risk Management

Safe Attachments

SPF / DKIM / DMARC

Active Directory / Entra ID tiering

Token Protection

Credential Guard

AppLocker / WDAC

Entra Internet / Private Access (GSA)

Tenant Allow / Block Lists (TLDs)

Attack Surface Reduction Rules

Ingest into a SIEM (Sentinel)

Web Content Filtering (Newly Registered Domains)

Information Barriers

Edge Hardening

We all can, and must, do better…

"If you're faced with the tradeoff between security and another priority, your answer is clear: Do security"

Satya Nadella
Microsoft CEO

RIP - Dame Margaret Natalie Smith, CH DBE

#ScottishSummit2024

Thank You!

Please leave feedback in the Scottish Summit app