

#ScottishSummit2024

Defence Against the Digital Dark Arts



Thank You to our Sponsors...



Platinum Sponsor



Gold Sponsors

resco

dox42®
automate your documents
integrate your data

MROW

kerv Digital

#ScottishSummit2024

Thank You to our Sponsors...



With Thanks



#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](https://www.linkedin.com/in/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.



Microsoft's unique vantage point

An extra 13 trillion security signals per day

2023: 65 trillion, 2024: 78 trillion

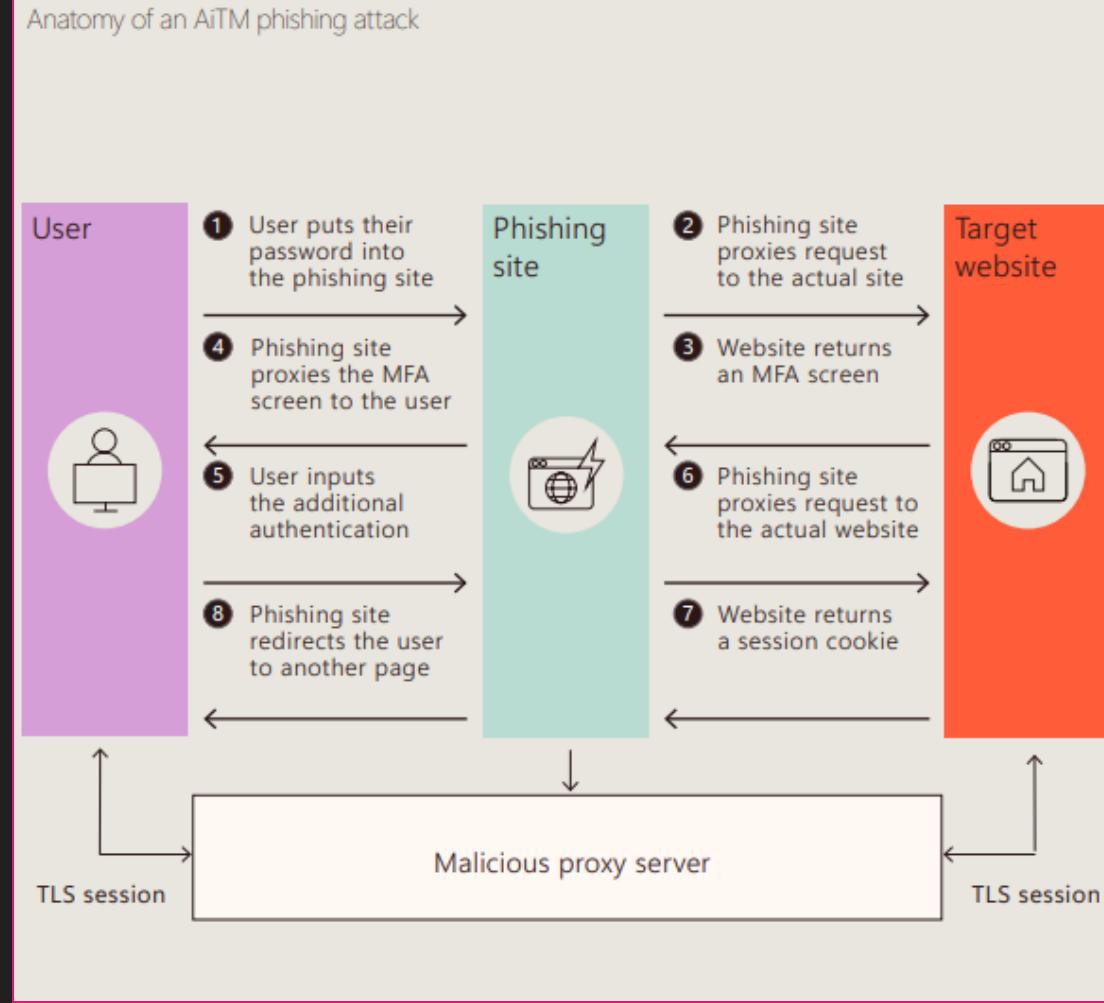
from the cloud, endpoints, software tools, and partner ecosystem, to understand and protect against digital threats and criminal cyberactivity.

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.



Adversary In The Middle (AiTM)



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)

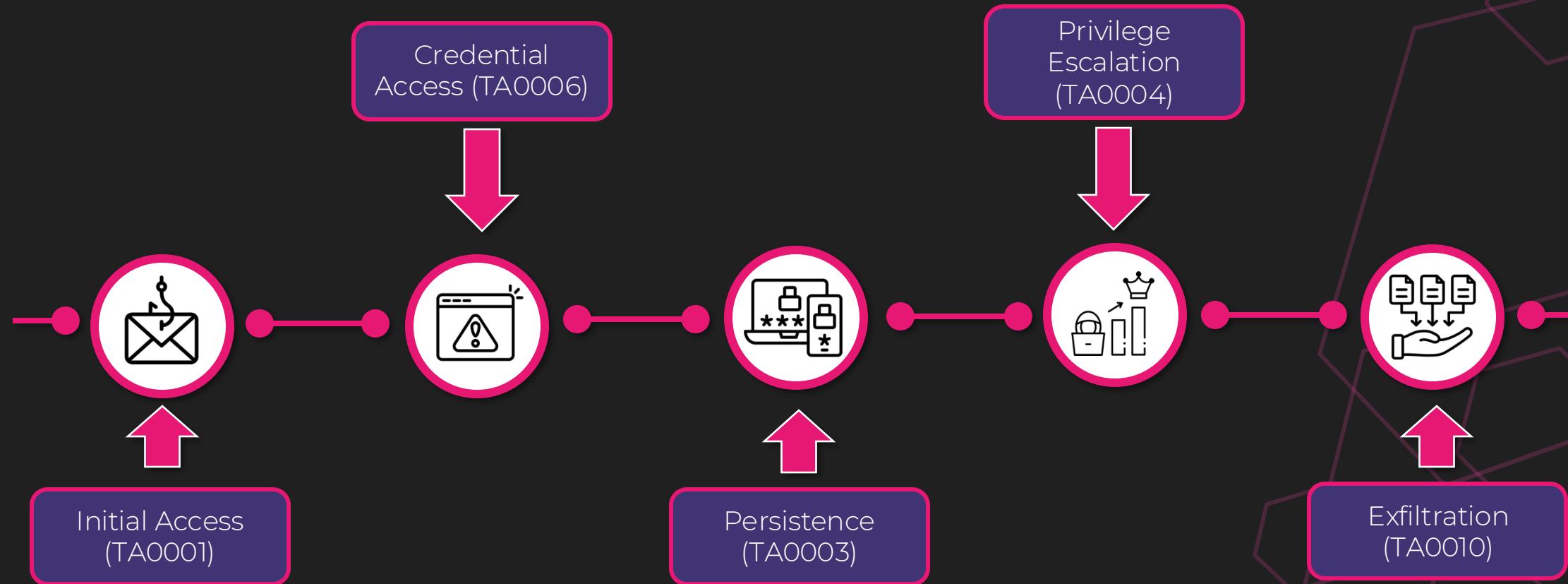
[Flangvik/Bobber](#): Bounces when a fish bites - Evilginx database monitoring with exfiltration automation (github.com)



Attack Scenario

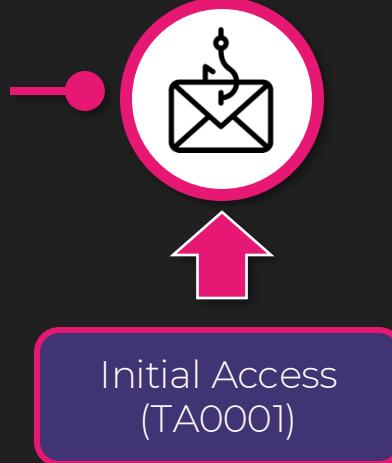
```
Activities Terminal steve@Slytherin-PC: ~ Aug 29 22:51 steve@Slytherin-PC: ~/Desktop/bobber
steve@Slytherin-PC:~$ ssh steve@evilginx.deatheaters.uk
steve@Slytherin-PC:~/Desktop/bobber$ python3 bobber.py "/home/steve/.evilginx/data.db" --username steve --host evilginx.deatheaters.uk --all
```

The Attack





Initial Access / Phishing (TA0001 / ΤΙ566)



Teams – Domain Whitelisting



Choose which external domains your users have

Allow all external domains

Teams accounts not managed by an organization

People in my organization can communicate with external users



External users with Teams accounts not managed by an organization can contact users in my organization

Choose which external domains your users have access to:

Allow only specific external domains

+ Add a domain X Remove | 2 items

✓ Allowed domains

ministryofmagic.co.uk

gringotts.com

Teams – Disable External / Personal account communication



To: Minerva.McGonagall@hogwartsschoolofwitchcraftandwizardry.co.uk

We can't set up the conversation because your organisations are not set up to talk to each other.

Teams accounts not managed by an organization

People in my organization can communicate with Teams users whose accounts aren't managed by an organization. [Learn more](#)



On

- External users with Teams accounts not managed by an organization can contact users in my organization.



Defender for Office 365 – Safe Links



Policies & rules > Threat policies > Create safe links policy

Email

Name your policy

Users affected

URL & protection

Notifications

On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.

Apply Safe Links to email messages sent within the organization

Apply

Office 365 Apps

On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten.

Do not apply

Teams – Zero-Hour Auto Purge (ZAP)



Settings > Email & collaboration

User reported settings

User tags

Priority account protection

Microsoft Teams protection

Microsoft Teams protection

Zero-hour auto purge (ZAP)

Protect Teams chats and channels using retroactive content scanning and removal. [Learn more about ZAP](#)

On (Default)

Quarantine policies

Apply these quarantine policies to content that ZAP has removed.
[Learn more about quarantine policies](#)

Malware

AdminOnlyAccessPolicy

High-confidence phishing

AdminOnlyAccessPolicy

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. To users within the organization. You can create custom, higher priority policies for specific users, groups or domains. [Learn more about security 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

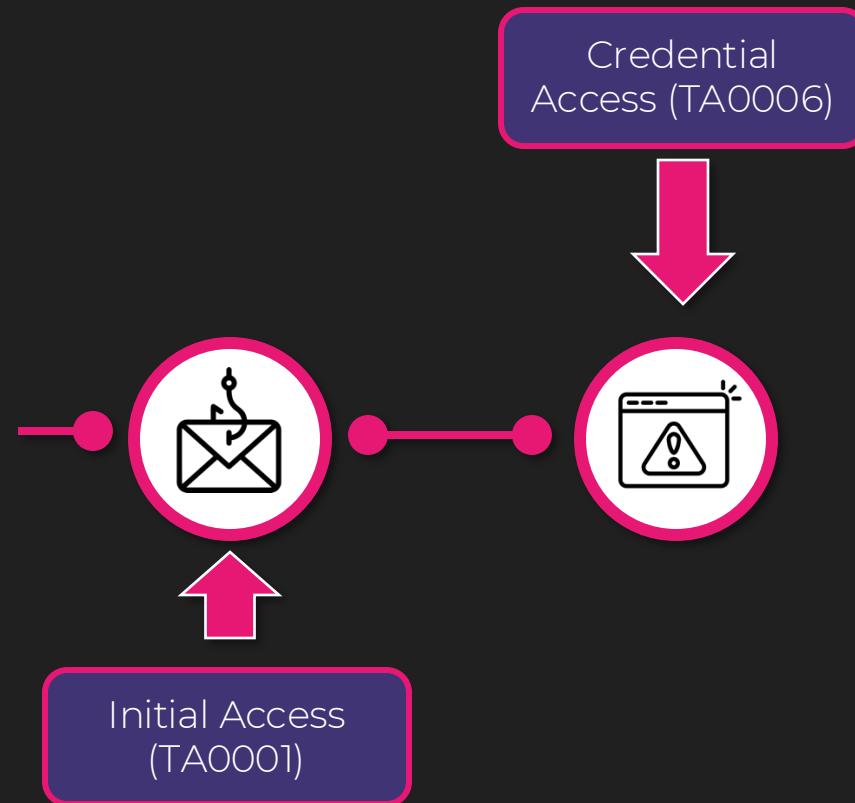
Wrap Up



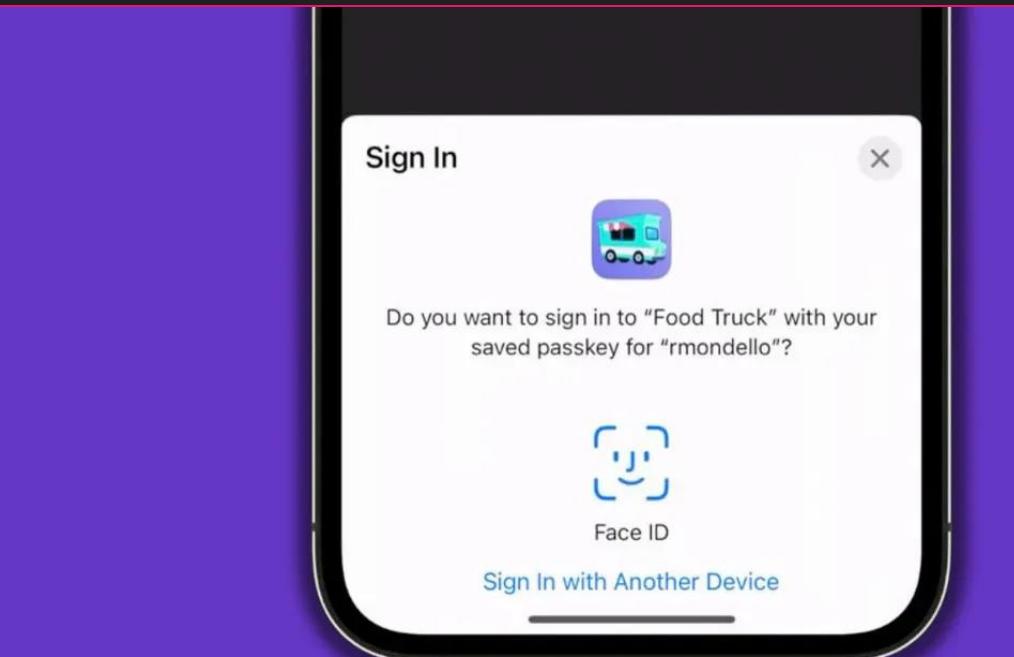
- Use domain whitelisting in Teams
- Disable personal Teams account communication and contact
- Enable Defender for Office 365 Safe Links policies
- Enable Zero-Hour Auto Purge (ZAP)
- Enable Defender for Office 365 Anti-Phishing policies



Credential Access / AiTM (TA0006 / T1557)



Phish-Resistant Authentication



#ScottishSummit2024

Conditional Access - Authentication Strengths



Require phish-resistant MFA for

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organization-wide policies.

Name *

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

Home > Hogwarts School of Witchcraft and Wizardry

Conditional Access | Authentication strengths

Microsoft Entra ID

- Overview
- Policies
- Insights and reporting
- Diagnose and solve problems
- Manage
 - Named locations
 - Custom controls (Preview)
 - Terms of use
 - VPN connectivity
 - Authentication contexts
- Authentication strengths ★
- Classic policies
- Monitoring

New authentication strength

Custom

Name

Description

Search authentication combinations

Type: All

Method	Description
<input type="checkbox"/>	Phishing-resistant MFA (3)
<input type="checkbox"/>	Windows Hello For Business
<input type="checkbox"/>	Passkeys (FIDO2) Advanced options
<input type="checkbox"/>	Certificate-based Authentication (Multifactor) Advanced options
<input type="checkbox"/>	Passwordless MFA (1)
<input type="checkbox"/>	Microsoft Authenticator (Phone Sign-in)
<input type="checkbox"/>	Multifactor authentication (13)
<input type="checkbox"/>	Temporary Access Pass (One-time use)
<input type="checkbox"/>	Temporary Access Pass (Multi-use)
<input type="checkbox"/>	Password + Microsoft Authenticator (Push Notification)
<input type="checkbox"/>	Password + Software OATH token
<input type="checkbox"/>	Password + Hardware OATH token
<input type="checkbox"/>	Password + SMS
<input type="checkbox"/>	Password + Voice

Access

Methods that can be used.

on methods

Illo For Business and 7 more

FIDO2

Illo For Business and 16 more

Illo For Business and 3 more

Illo For Business and 2 more

#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

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](#)

View Authentication Strength

X

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)

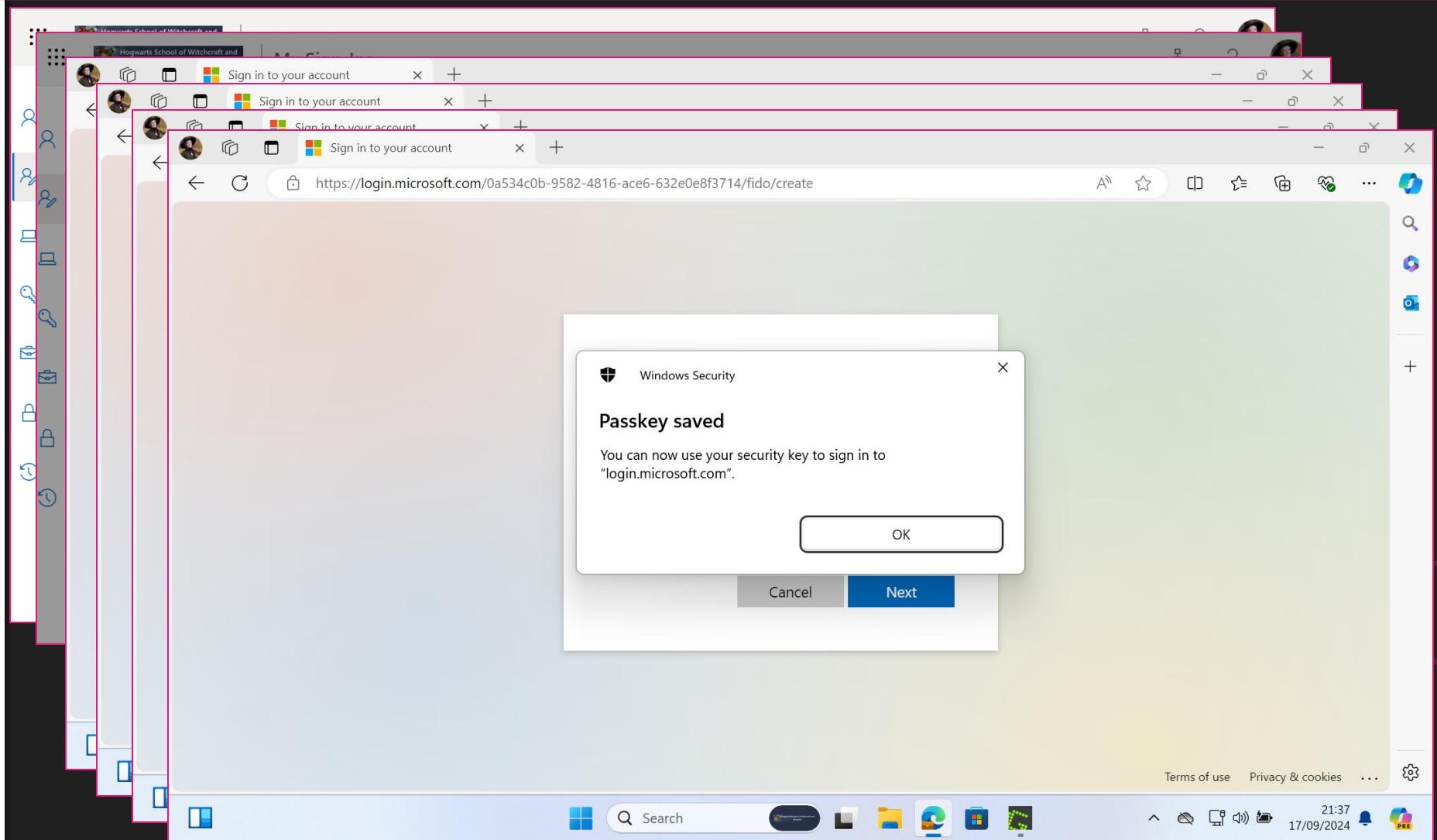
Require authentication strength

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](#)

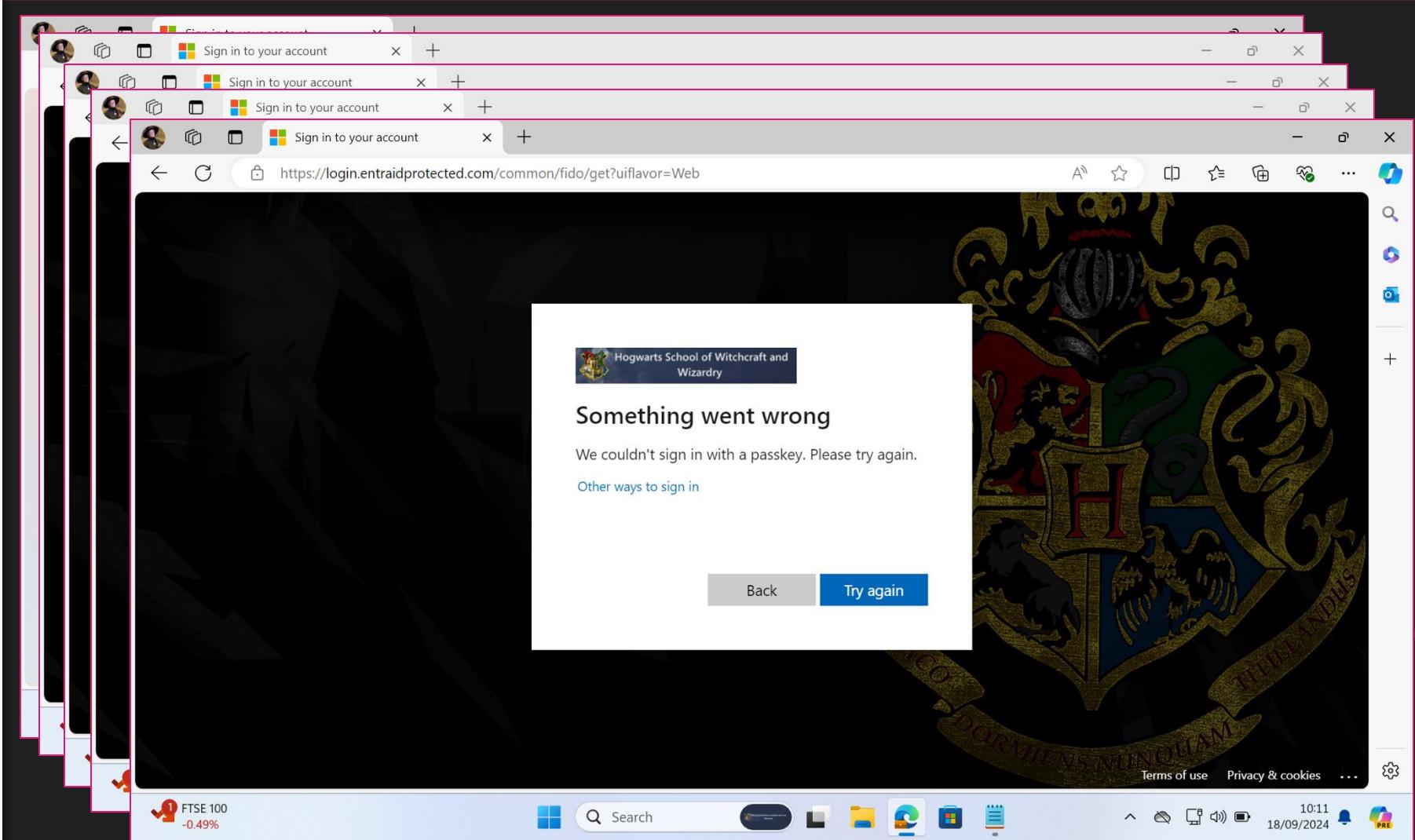
#ScottishSummit2024

Authentication Strengths – Enforce Phish-Resistant MFA



#ScottishSummit2024

Authentication Strengths – Enforce Phish-Resistant MFA



Authentication Strengths – Enforce Phish-Resistant MFA



```
[09:09:44] [imp] [1] [ms365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/128.0.0.0 Safari/537.36 Edg/128.0.0.0 (86.20.79.186)  
[09:09:44] [inf] [1] [ms365] landing URL: https://login.entrailprotected.com/hGHCvhnQ  
[09:10:12] [+++] [1] Username: [2H4o1hNgdK20sg4iPbqp5XMH40eu1nPwsdboFhv+bCE=7:1:CANARY:uh3t8d+wQtNvu0ossd76Gz7qx/08Phi0+BK9LMMJS0o=]  
.
```

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)



Home > Security | Conditional Access > Conditional Access Policies >

Require password change for high-risk users

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 password change for high-risk users

Assignments

Users

All users included and specific users excluded

Target resources

All cloud apps

Network

Not available

Conditions

1 condition selected



Update your password

As someone else may have access to your account, you need to choose a new password. Don't use the same password that you use for other sites.

Try again – that isn't your current password.

[View details](#)

.....

.....

.....

Sign in

sk

X

No

ser risk levels needed for
enforced

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



Windows 10/11 compliance policy

Windows 10 and later

Device Security

Firewall

Trusted Platform Module (TPM)

Antivirus

Antispyware

Windows 10 and 11

BitLocker

Secure Boot

Code integrity

Policies

Notifications

Retire noncompliant devices

Compliance settings

Scripts

Monitor

Save

Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as Not compliant

Not compliant

Compliance status validity period (days)

30

X

Delete

Edit

Device Compliance



The screenshot shows a web browser window with a dark theme. The address bar says "Sign in to your account" and the URL is <https://login.entrainprotected.com/common/login>. A modal dialog box is displayed, showing the Hogwarts School of Witchcraft and Wizardry logo at the top. The message in the box reads: "You cannot access this right now. Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin." Below the message are links for "Sign out and sign in with a different account" and "More details". At the bottom of the dialog is a link to "Hogwarts School of Witchcraft and Wizardry". A smaller "Troubleshooting details" window is overlaid on the bottom left of the dialog, containing technical information such as Error Code: 53003, Request Id: 00c5bb87-a745-46db-aabe-f8b7679b1c01, Correlation Id: e6536365-847b-4c29-afde-e291733987bb, Timestamp: 2024-09-10T19:34:57.203Z, App name: OfficeHome, App id: 4765445b-32c6-49b0-83e6-1d93765276ca, IP address: 20.0.41.235, Device identifier: Not available, and Device state: Unregistered. The background of the browser window shows the Hogwarts crest.

#ScottishSummit2024

Device Compliance

A terminal window titled "steve@DeathEaters-Evilginx: ~" showing the Evilginx Community Edition interface. The interface includes a red pixelated map of the Hogwarts castle, a menu bar with "File", "Edit", "View", "Tools", "Help", and "Community Edition", and a status bar indicating "version 3.3.0".

```
[19:33:12] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[19:33:12] [inf] loading phishlets from: /home/steve/evilginx/phishlets
[19:33:12] [inf] loading configuration from: /home/steve/.evilginx
[19:33:12] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
[19:33:12] [inf] obtaining and setting up 3 TLS certificates - please wait up to 60 seconds...
[19:33:12] [inf] successfully set up all TLS certificates

+-----+-----+-----+-----+-----+
| phishlet | status | visibility | hostname | unauth_url |
+-----+-----+-----+-----+-----+
| ms365 | enabled | visible | entraidprotec... |           |
+-----+-----+-----+-----+-----+

[19:33:19] [imp] [0] [ms365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36 Edg/128.0.0.0 (86.20.79.186)
[19:33:19] [inf] [0] [ms365] landing URL: https://login.entraidprotected.com/hGCVhNQ
[19:34:44] [+++] [0] Password: [Triwizard-Tourney123!]
[19:34:44] [+++] [0] Username: [minerva.mcgonagall@hogwartsschoolofwitchcraftandwizardry.co.uk]
[19:34:44] [+++] [0] Username: [minerva.mcgonagall@hogwartsschoolofwitchcraftandwizardry.co.uk]
:
```

Defender for Endpoint



Alerts > Stolen logon session cookie was used

Part of incident: Stolen logon session cookie was used involving one user [View incident page](#)

hogwartsschoolofwitchcraftandwizar...

What happened

The session cookie was detected to be compromised. Microsoft 365 Defender alerts on the earliest observed event in this session.

Recommended actions

- Validate the alert.
- Search for the relevant login event in the AA...

[Read more](#)

Related events

9/17/2024
9:05:49 PM



Minerva McGonagall logged on to Microsoft 365

Action type	LogonSuccess
Logon type	SAS:ProcessAuth
Account display	Minerva McGonagall



Stolen logon session cookie was used

■ Medium | ● Unknown | ● New



Manage alert



Link alert to another incident

...

INSIGHT

Quickly classify this alert

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

[Classify alert](#)

Alert state

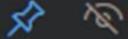
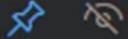
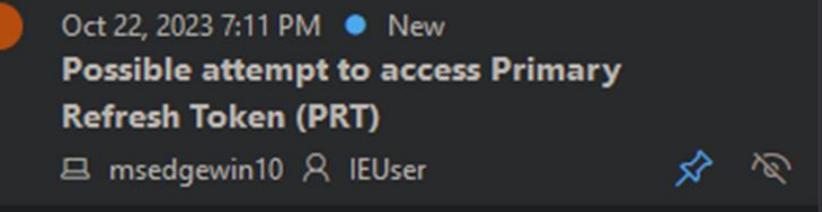
Classification

Not Set

[Set Classification](#)

Assigned to

Unassigned



#ScottishSummit2024

Entra ID Protection



Home > Identity Protection

Identity Protection | Risky users

Search

Dashboard

Tutorials

Diagnose and solve problems

> Protect

> Report

> Settings

Learn more

Download

Unselect all

Want to allow automatic risk remediation? Set up

Auto refresh : **Off**

Show dates as : **Last 7 days**

User ↑↓

Risky User Details

Reset password

Confirm user compromised

Confirm user safe

Dismiss user risk

Block user

...

Basic info

Recent risky sign-ins

Detections not linked to a sign-in

Risk history

Detection type ↑↓

Time Detected ↑↓

Detection risk state ↑↓

Detection risk level ↑↓

Detection risk de... ↑↓

Attacker in the Middle

9/18/2024, 12:03:24 PM

At risk

High

Home > Identity Protection

Identity Protection | Risky users

Search

Dashboard

Tutorials

Diagnose and solve problems

> Protect

> Report

> Settings

> Troubleshooting + Support

Learn more

Download

Unselect all

Want to allow automatic risk remediation? Set up

Auto refresh : **Off**

Show dates as : **Last 7 days**

User ↑↓

Minerva McGonagall

Risky User Details

Reset password

Confirm user compromised

Confirm user safe

Dismiss user risk

Block user

...

Basic info

Recent risky sign-ins

Detections not linked to a sign-in

Risk history

Date

Activity

Actor

Risk state

Risk level

9/18/2024, 12:27:49 PM

Attacker in the Middle

Microsoft Entra ID

At risk

High

9/17/2024, 9:50:17 PM

User performed secured ... [Nate Admin](#)

Remediated

8/29/2024, 9:14:23 PM

Additional risk detected

Microsoft Entra ID

Dismissed

-

Defender XDR – Automatic Attack Disruption



Microsoft 365 Defender

Incidents > User compromised in AiTM phishing (attack disruption)

User compromised in AiTM phishing (attack disruption)

Implement a potentially compromised account was detected automatically by alert disruptor in Microsoft 365 Defender. For more details, select the Alerts tab or go to the Alerts series.

Attack Story Recommended actions (0) Alerts (7) Assets (4) Investigations (2) Evidence and Response (11) Summary

Alerts

17 Active alerts

May 13, 2023 2:10 PM Suspicious inbox manipulation rule A. Jonathan Wescott

May 13, 2023 2:10 PM Suspicious inbox manipulation rule A. Jonathan Wescott

May 13, 2023 2:10 PM Impossible travel activity A. Jonathan Wescott

May 13, 2023 2:14 PM User compromised in AiTM phishing attack B. compromised A. Jonathan Wescott

May 13, 2023 2:14 PM Unfamiliar sign-in properties A. Jonathan Wescott

Incident graph

Layout Group similar nodes

Clear selection

Back to incident details

User compromised in AiTM phishing attack

logoff/composite

Shared file #1234567890

compromised

12.34.1.1.0

A. Jonathan Wescott

Details Recommendations

Quickly classify this alert

classy alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification Not set Assigned to Unassigned

Sanitization

Alert details

Evidence

Entity Name Revocation Status Verdict

https://... Success

IP 123.45.67.89 Success

URL undefined Success

Alert description

User compromised in AiTM phishing attack

High Detected None

#ScottishSummit2024

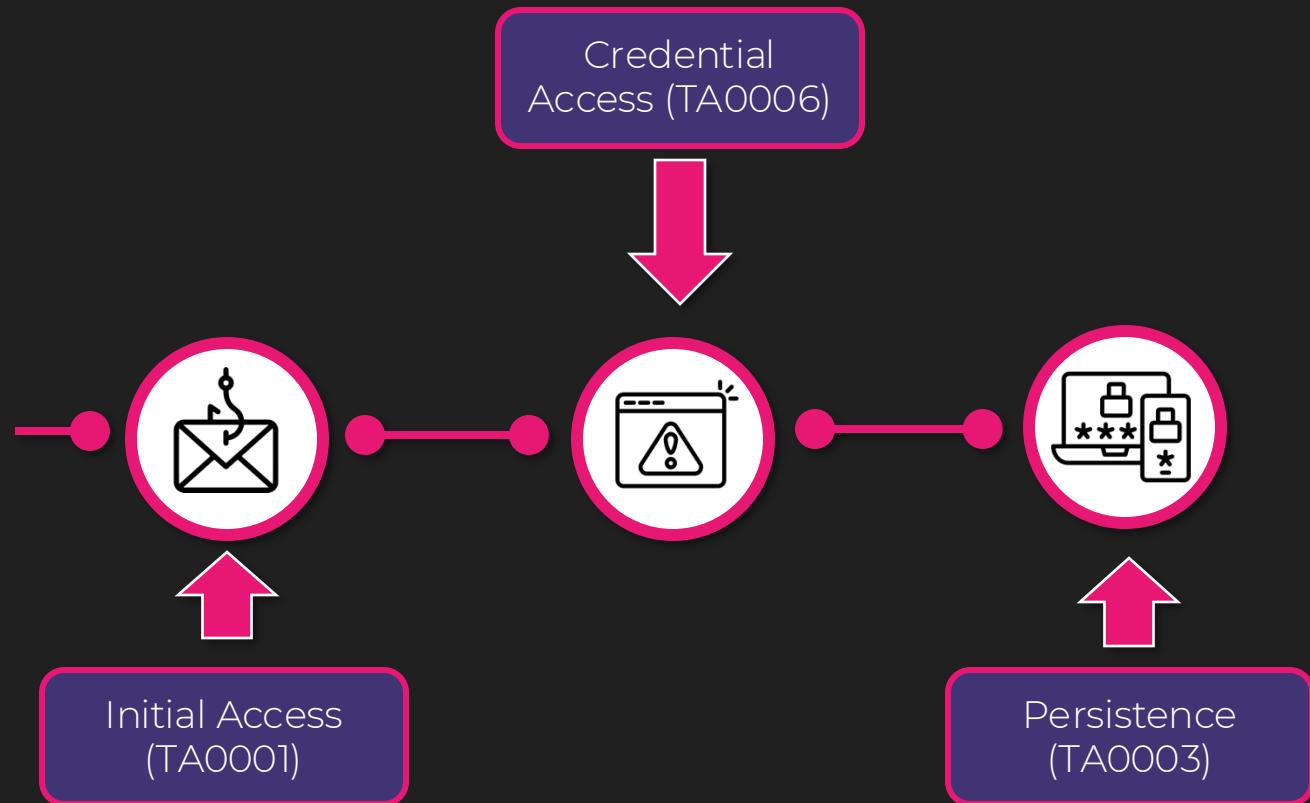
Wrap Up



- 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



Home > Security | Conditional Access > Conditional Access | Policies >

Securing security info registration

Conditional Access policy

Delete View policy information

1 user action included

Network Any network or location and all trusted locations excluded

Conditions 1 condition selected

Access controls

Grant 1 control selected

Session 0 controls selected

Insider risk

Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.

Not configured

Device platforms

Not configured

Locations

Any network or location and all trusted locations excluded

Client apps

Not configured

Filter for devices

Not configured

Authentication flows (Preview)

Not configured

Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure

Yes No

Devices matching the rule:

- Include filtered devices in policy
 Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	isCompliant	Equals	True
Or	TrustType	Equals	Microsoft Entra hybrid joined

[+ Add expression](#)

Rule syntax

```
device.isCompliant -eq True -or device.trustType -eq "ServerAD"
```

Grant

Control access enforcement to block or grant access. [Learn more](#)

- Block access
 Grant access

Secure Registration of Security Info



Home > Hogwarts School of Witchcraft and Wizardry | Security > Security | Conditional Access > Conditional Access | Policies >

Only register security info from Corporate Office

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 *****
Only register security info from Corporate O...

Assignments

Users [①](#)
[Specific users included and specific users excluded](#)

Target resources [①](#)
1 user action included

Network [NEW](#) [①](#)
Any network or location and 1 excluded

Conditions [①](#)
1 condition selected

Enable policy
[Report-only](#) [On](#) [Off](#)

Control user access based on their network or physical location. [Learn more ↗](#)

Configure [①](#)
[Yes](#) [No](#)

Include [Exclude](#)
Select the locations to exempt from the policy

All trusted networks and locations
 All Compliant Network locations
 Selected networks and locations

Select
Corporate Office

Grant

Control access enforcement to block or grant access. [Learn more ↗](#)

Block access
 Grant access

Require multifactor authentication [①](#)
 Require authentication strength [①](#)
 Require device to be marked as compliant [①](#)

[To create a Conditional Access policy ensuring your tenant's members are...](#)

Defender for Identity



Suspicious additions to sensitive groups

Medium | Unknown | New

[Manage alert](#) [Export](#) ...

INSIGHT

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

[Classify alert](#)

Alert state

Classification Not Set **Assigned to** Unassigned

[Set Classification](#)

Alert details

Category Persistence **Detection source** Microsoft Defender for Identity

Service source Microsoft Defender for Identity **Detection status** Unknown

Suspected Golden Ticket usage (encryption downgrade) (external ID 2000)

Previous name: Encryption

Severity: Medium

Description:

Encryption downgrade is fields that normally have brute force attempts. Various Identity learns the Kerberos that is unusual for the source.

In a Golden Ticket alert, the computer was detected an anomaly (as in the other authentication request as

Learning period:

This alert has a learning p

MITRE:

Primary MITRE tactic

Secondary MITRE tactic

MITRE attack technique

MITRE attack sub-technique

Honeytoken user attributes modified (external ID 2427)

Severity: High

Description: Every user object in Active Directory has attributes that contain information such as first name, middle name, last name, phone number, address and more. Sometimes attackers will try and manipulate these objects for their benefit, for example by changing the phone number of an account to get access to any multifactor authentication attempt. Microsoft Defender for Identity will trigger this alert for any attribute modification against a pre-configured honeytoken user.

Learning period:

None

MITRE:

Primary MITRE tactic

Persistence (TA0003)

MITRE attack technique

Account Manipulation (T1098)

MITRE attack sub-technique

N/A

[Expand table](#)

#ScottishSummit2024

Proactive Threat Hunting



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

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
| 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.
```



Proactive Threat Hunting

```
1 //Advanced Hunting query to parse modified StrongAuthenticationMethod
2
3 let AuthenticationMethods = dynamic(["TwoWayVoiceMobile", "TwoWaySms", "TwoWayVoiceOffice", "TwoWayVoiceOtherMobile", "TwoWaySmsOtherMobile", "On
4 let AuthenticationMethodChanges = CloudAppEvents
5 | where ActionType == "Update user." and RawEventData contains "StrongAuthenticationMethod"
6 | extend Target = tostring(RawEventData.ObjectId)
7 | extend Actor = tostring(RawEventData.UserId)
8 | mv-expand ModifiedProperties = parse_json(RawEventData.ModifiedProperties)
9 | where ModifiedProperties.Name == "StrongAuthenticationMethod"
10 | project Timestamp,Actor,Target,ModifiedProperties,RawEventData,ReportId;
11 let OldValues = AuthenticationMethodChanges
12 | extend OldValue = parse_json(tostring(ModifiedProperties.OldValue))
13 | mv-apply OldValue on (extend Old_MethodType=tostring(OldValue.MethodType),Old_Default=tostring(OldValue.Default) | sort by Old_MethodType)
14 let NewValues = AuthenticationMethodChanges
15 | extend NewValue = parse_json(tostring(ModifiedProperties.NewValue))
16 | mv-apply NewValue on (extend New_MethodType=tostring(NewValue.MethodType),New_Default=tostring(NewValue.Default) | sort by New_MethodType)
17 let RemovedMethods = AuthenticationMethodChanges
18 | join kind=inner OldValues on ReportId
19 | join kind=leftouter NewValues on ReportId,$left.Old_MethodType==$right.New_MethodType
20 | project Timestamp,ReportId,ModifiedProperties,Actor,Target,Old_MethodType,New_MethodType
21 | where Old_MethodType != New_MethodType
22 | extend Action = strcat("Removed (", AuthenticationMethods[toint(Old_MethodType)], ") from Authentication Methods.")
23 | extend ChangedValue = "Method Removed".
24 let AddedMethods = NewValues
25 | join kind=inner NewValues on ReportId
26 | join kind=inner OldValues on ReportId, where Old_MethodType == New_MethodType
27 | project Timestamp,ReportId,ModifiedProperties,Actor,Target,Old_MethodType,New_MethodType
28 | where Old_MethodType != New_MethodType
29 | extend Action = strcat("Added (", NewValue.Name, ") as Authentication Method.")
30 | extend ChangedValue = "Method Added".
31 let DefaultMethodChanges = NewValues
32 | join kind=inner NewValues on ReportId, where Old_MethodType == New_MethodType
33 | project Timestamp,ReportId,ModifiedProperties,Actor,Target,Old_MethodType,New_MethodType
34 | where Old_MethodType == New_MethodType
35 | join kind=inner OldValues on ReportId, where Old_Default == true and Old_MethodType != New_MethodType | extend Old_MethodType = Old_MethodType
36 | extend Action = strcat("Default Authentication Method was changed to (", NewValue.Name, ").")
37 | extend ChangedValue = "Default Method".
38 union RemovedMethods,AddedMethods,DefaultMethodChanges
39 | project Timestamp,Action,Actor,Target,ChangedValue,OldValue=case(isempty(Old_MethodType), "",strcat(Old_MethodType, ":", AuthenticationMet
40 | distinct *
```

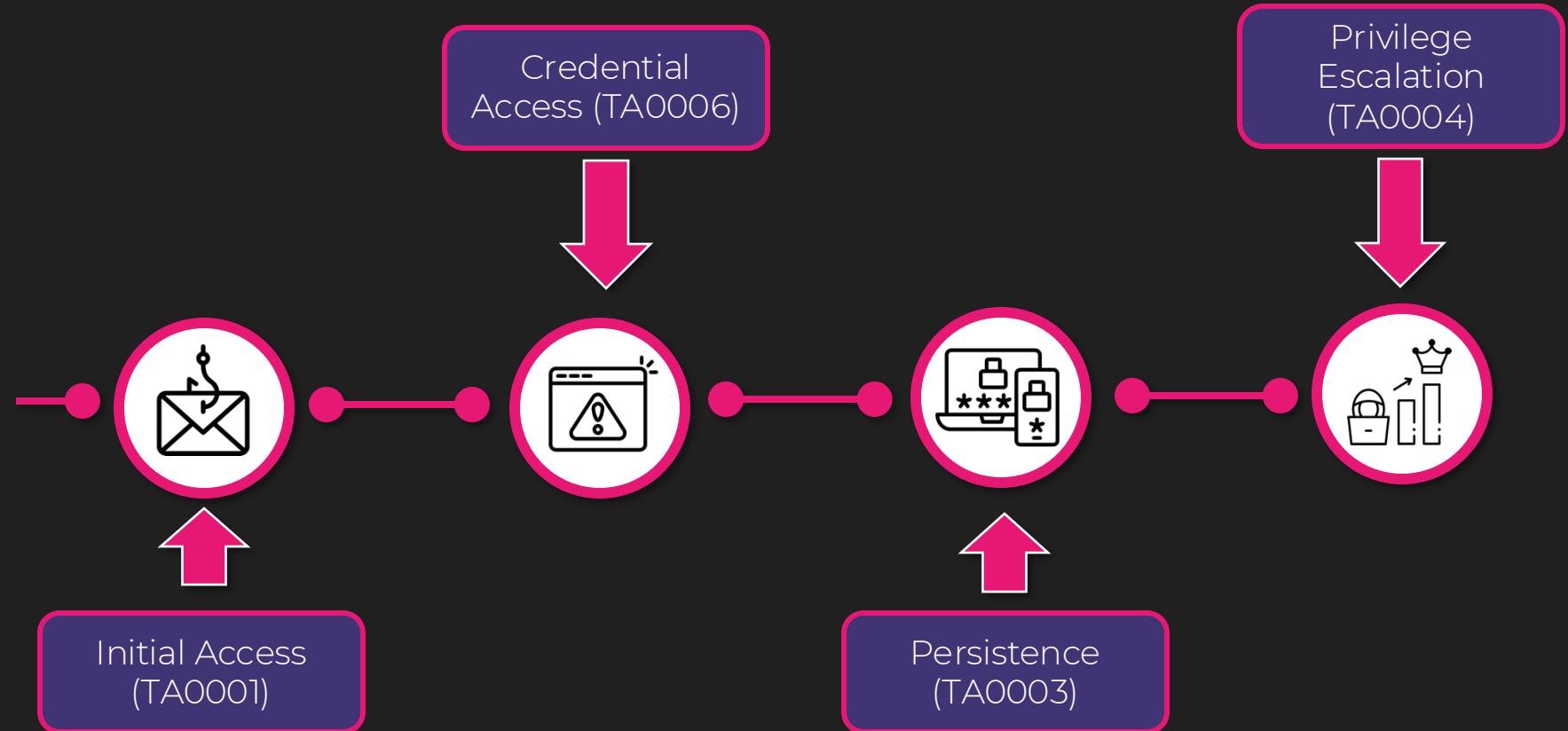
Timestamp (UTC)	Action	Actor	Target	ChangedValue	OldValue	NewValue
2024-04-16 15:37:56.0000	Added (TwoWayVoiceMobile) as Authentication Method.	Meran@contoso.com	Diego@contoso.com	Method Added	0: TwoWayVoiceMobile	
2024-04-16 15:37:56.0000	Added (OneWaySms) as Authentication Method.	Meran@contoso.com	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

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



#ScottishSummit2024

Local Admin Password Solution (LAPS)



The screenshot illustrates the process of creating a Local Admin Password Solution (Windows LAPS) profile in the Microsoft Intune admin center.

Left Panel (Navigation):

- Microsoft Intune admin center
- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security** (highlighted with a red box)
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Middle Panel (Endpoint security | Account protection):

- Search bar
- Create Policy (button)
- Refresh
- Export
- Search by profile name
- Policy name: asdfasdf, Policy type: Local admin password solution, Assigned: No
- Policy name: LAPDEMO, Policy type: Local admin password solution, Assigned: No
- Policy name: LAPS Policy, Policy type: Local admin password solution, Assigned: Yes
- Policy name: LAPS Support Readiness F, Policy type: Local admin password solution, Assigned: Yes
- Policy name: LapsDemo2, Policy type: Local admin password solution, Assigned: Yes
- Policy name: LAPSSHTest, Policy type: Local admin password solution, Assigned: Yes
- Policy name: Lapshtestapril, Policy type: Local admin password solution, Assigned: Yes
- Policy name: sdfsf, Policy type: Local admin password solution, Assigned: No
- Policy name: Windows LAPS Policy, Policy type: Local admin password solution, Assigned: Yes

Right Panel (Create a profile):

- Platform: Windows 10 and later
- Profile: Select a profile (dropdown menu)
 - Local user group membership
 - Account Protection (Preview)
 - Local admin password solution (Windows LAPS)** (highlighted with a red box)

Bottom Panel (Create profile - Configuration settings):

- Basics (selected)
- Configuration settings (selected)
- Scope tags
- Assignments
- Review + create

LAPS Settings:

- Backup Directory: Not configured (dropdown menu)
 - Disabled (password will not be backed up)
 - Backup the password to Azure AD only
 - Backup the password to Active Directory only
 - Not configured
- Administrator Account Name: (dropdown menu)
- Password Complexity: (dropdown menu)
- Password Length: (dropdown menu)
- Post Authentication Actions: (dropdown menu)
- Post Authentication Reset Delay: (dropdown menu)

#ScottishSummit2024

Local Admin Password Solution (LAPS)



Microsoft Intune admin center

Home > Endpoint security | All devices > DESKTOP-VT7M6L3

DESKTOP-VT7M6L3 | Local admin password

Search Refresh

Overview Manage Local administrator password Last password rotation Next password rotation

Local administrator password	Last password rotation	Next password rotation
Show local administrator password	4/10/2023, 6:01:15 PM	5/10/2023, 6:01:15 PM

Properties Monitor

- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Local admin password**
- Recovery keys
- User experience
- Device diagnostics
- Create new admin user

Local administrator password

Account name: Administrator
Security ID: S-1-5-21-1024-1024-1024-1024-1024-1024
Local administrator password: ***** Show

Last password rotation: 4/10/2023, 6:01:15 PM
Next password rotation: 5/10/2023, 6:01:15 PM

The screenshot illustrates the Microsoft Intune admin center interface for managing local administrator passwords. On the left, the navigation pane shows various service categories like Home, Dashboard, and Devices. Under the Devices category, the 'Local admin password' link is highlighted with a red box and a red arrow pointing to it. In the main content area, a table displays the local administrator password information for the device 'DESKTOP-VT7M6L3'. The 'Show local administrator password' button is also highlighted with a red box and a red arrow pointing to it. To the right, a detailed view of the 'Local administrator password' settings is shown, including the account name ('Administrator'), security ID ('S-1-5-21-1024-1024-1024-1024-1024-1024'), and the password itself (represented by five asterisks). It also shows the last password rotation date ('4/10/2023, 6:01:15 PM') and the next password rotation date ('5/10/2023, 6:01:15 PM').

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



Global-AuthContext-RequirePasskey

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 *

Global-AuthContext-RequirePasskey

Assignments

Users

0 users and groups selected

Target resources

1 authentication context included

Network

Not configured

Conditions

0 conditions selected

Control access based on all or specific network access traffic, cloud apps or actions.
[Learn more](#)

Select what this policy applies to

Authentication context

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security.
[Learn more](#)

Select the authentication contexts this policy will apply to

PIM - Require Passkey

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

"Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require authentication strength

Passkeys

#ScottishSummit2024

PIM – Authentication Contexts



Edit role setting - Security Administrator

Privileged Identity Management | Microsoft Entra roles

Activation Assignment Notification

Activation maximum duration (hours)

On activation, require

- None
- Azure MFA
- Microsoft Entra Conditional Access authentication context

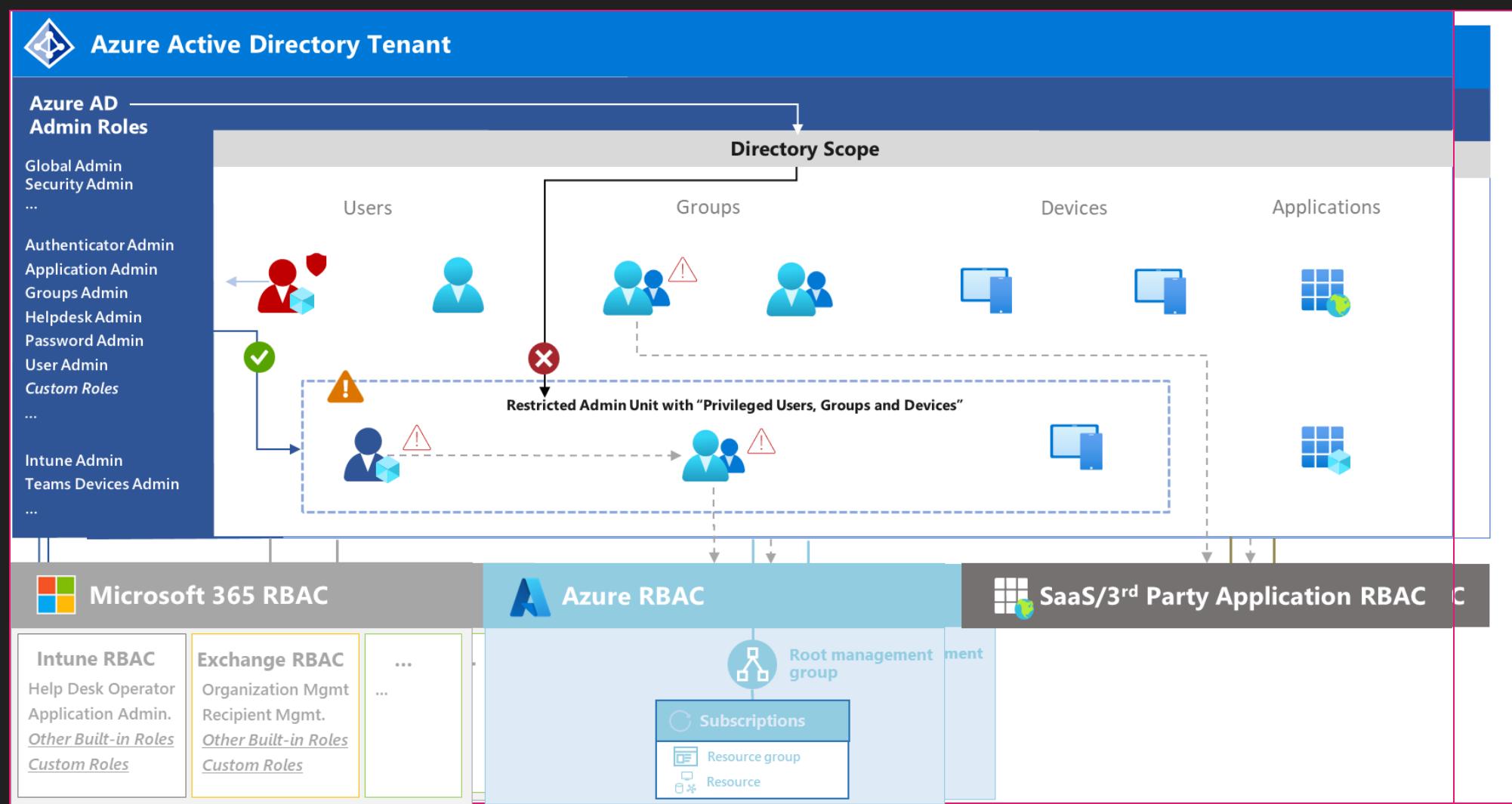
[Learn more](#)

Select ▼

- PIM - Require Passkey

- Require justification on activation
- Require ticket information on activation
- Require approval to activate

Administrative Units / RMAU's



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

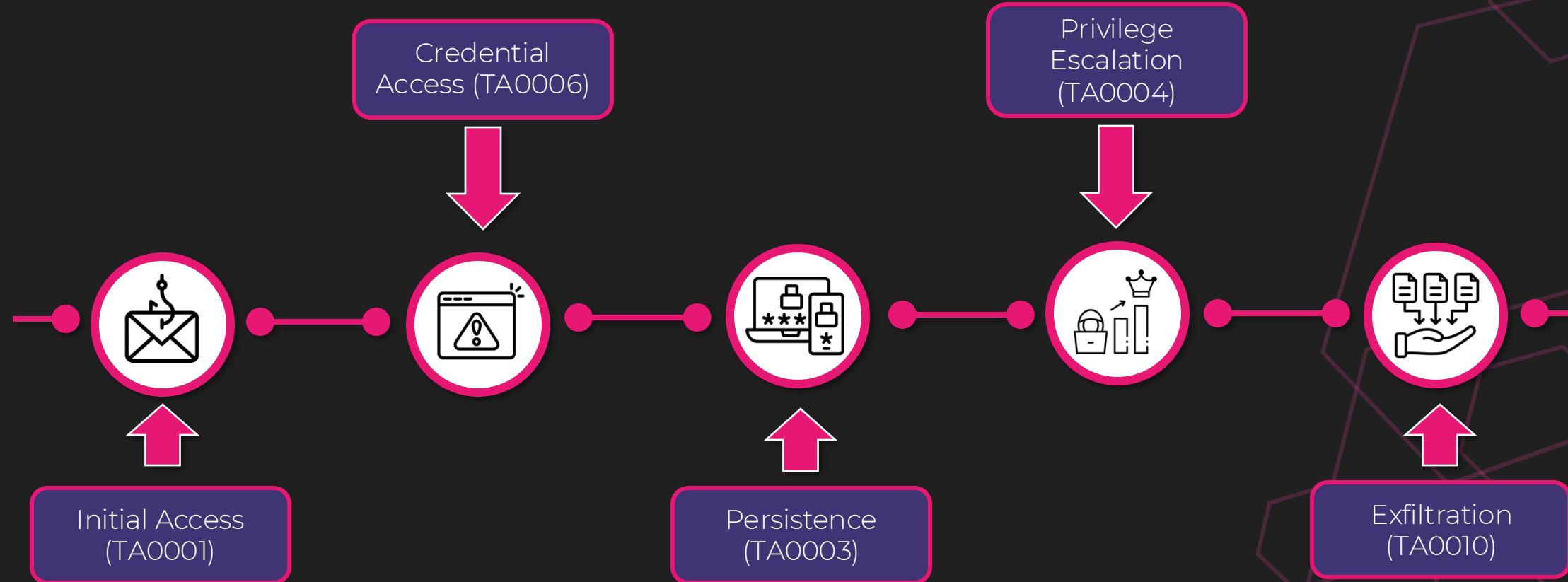
#ScottishSummit2024

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



Super secret document

HIGHLY CONFIDENTIAL

This screenshot shows a Microsoft Word document window titled "Document1 - Word Highly Confidential". The ribbon menu is visible at the top, showing tabs like File, Home, Insert, Draw, Design, Layout, References, Mailings, Review, and View. The Home tab is selected. The ribbon also includes a "Sensitivity" tab. The main content area contains the text "Super secret document". A large, diagonal watermark reading "HIGHLY CONFIDENTIAL" is overlaid across the page. The status bar at the bottom shows "Page 1 of 1", "3 words", "English (United States)", "Text Predictions: On", "Accessibility: Good to go", "10°C Mostly cloudy", and the date/time "10/09/2024 21:31". The taskbar at the bottom of the screen shows various pinned icons.

Sensitivity Labels



Access control

Microsoft Purview

The settings you choose will be automatically enforced across Office, Fabric and Power BI.

Remove access
 Configure access

Assign permission

Assign permission

The settings you choose will be automatically enforced across Office, Fabric and Power BI.

User access to content expires

Never

Allow offline access

Always

Assign permission

Assign permission

The settings you choose will be automatically enforced across Office, Fabric and Power BI.

Items

Label details
 Scope
 Items
 Access control
 Content marking
 Auto-labeling for files and emails
 Groups & sites
 Schematized data assets (preview)
 Finish

Edit sensitivity label

The settings you choose will be automatically enforced across Office, Fabric and Power BI.

User access to content expires

Never

Allow offline access

Always

Assign permissions to specific users and groups

Assign permissions

Users and groups

M365: [REDACTED]@onmicrosoft.com
hogwartsschoolofwitchcraftandwizardry.co.uk

Use dynamic watermarking

Use Double Key Encryption

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

+ Add all users and groups in your organization
+ Add any authenticated users
+ Add users or groups
+ Add specific email addresses or domains

Enter email address or domain Add

1 item

2 items

Delete

Choose permissions

Co-Author

View content View rights Edit content Save Print Copy and extract content Reply Reply

Sensitivity Labels



The screenshot shows the Microsoft Purview interface for tracking and revocation of a file named "hogwarts_potion_supplies.xlsx". The file status is listed as "ACCESS ACTIVE". The "File Details" sidebar on the right provides information about the file, including its Content ID (ca9fe7cb-9bf9-427a-ba2e-3081cdb9a710), State (Active), and Permissions (Highly Confidential). It also shows the file owner as "contoso" and the first access date as "2024-09-18". The "File Details" sidebar includes a "Revoke access" button and a "Download report" button, both of which are highlighted with a red box and a red arrow pointing to the "Revoke access" button.

hogwarts_potion_supplies.xlsx
ACCESS ACTIVE

Timeline

No data

Viewers

Name	Status	Access last attempted on	Email
No data available			

0 items Customize columns

Content ID
ca9fe7cb-9bf9-427a-ba2e-3081cdb9a710

State
Active

Permissions
Highly Confidential

File owner
contoso

First access
2024-09-18

Denied views
0

Denied access
0

Successful views
0

Successful access
0

Email notifications

- Notify me by email when someone tries to open this document
- Notify me only when access to the document is denied
- Don't notify me

Revoke access Download report

#ScottishSummit2024

Sensitivity Labels



The screenshot shows a Linux desktop environment with a pink and purple plaid wallpaper. An 'Activities' dock on the left lists various applications and locations. The main window is LibreOffice Calc, displaying a file import dialog for 'hogwarts_hr_data.xlsx'. The dialog has the following settings:

- Import:** Character set: Unicode (UTF-8), Language: Default - English (UK), From row: 1.
- Separator Options:** Separated by Comma.
- Other Options:** Format quoted field as text, Detect special numbers, Evaluate formulas.
- Fields:** Column type: Standard. The preview area shows the following data rows:

1	Standard
2	"#\$%&!"*+
3	!#\$%&!"*+DataSpacesVersion
4	!#\$%&!"*+DataSpacesVersion
5	!#\$%&!"*+DataSpacesVersion
6	!#\$%&!"*+DataSpacesVersion
7	!#\$%&!"*+DataSpacesVersion
8	!#\$%&!"*+DataSpacesVersion

#ScottishSummit2024

Sensitivity Labels



New sensitivity label

- Label details
- Scope
- Items
- Groups & sites
- External sharing & conditional access
- Schematized data assets (preview)
- Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Use Microsoft Entra Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

- Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't [Microsoft Entra hybrid joined](#) or enrolled in Intune).

(i) For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web-only access (i)

Block access (i) 

Choose an existing authentication context. Each context has an Microsoft Entra Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

(i) There aren't any authentication contexts configured in your organization. [Learn how to create one](#)

No authentication contexts set up yet 

Data Loss Prevention



Hogwarts School of Witchcraft and Wizardry SharePoint Search this library

Share "hogwarts_hr_data.xlsx" ... ? X

Highly Confidential \ All Employees lord.voldemort@en... Add more

This item contains sensitive information. It can't be shared with people outside your organization. View policy tip

Add a message

Copy link Send

Policy tip for 'hogwarts_textbooks.xlsx'

Don't do this It can't be shared with people outside your organization.

- Issues

Last scanned: 15 days ago

Report an issue to let your admin know that this item doesn't conflict with your organization's policies.

1 item Status On

#ScottishSummit2024

Defender for Cloud Apps



The screenshot shows the Microsoft 365 Security & Compliance Center interface. On the left, a navigation bar includes 'Incidents', 'Multi-factor authentication', 'Attack detection', 'Alerts', and 'Playbooks'. The main area is titled 'Create activity policy' and contains fields for 'Policy template *' (set to 'Mass download by a single user'), 'Policy name *' (set to 'Mass download by a single user'), 'Policy severity *' (set to 'Medium'), 'Category *' (set to 'Threat detection'), and a 'Description' box containing the text 'Alert when a single user performs more than 50 downloads within 1 minute.' Below this, a section titled 'Create filters for the policy' allows selecting 'Act on:' as 'Repeated activity:' (selected) or 'Single activity'. For 'Repeated activity:', settings include 'Minimum repeated activities:' (50), 'Within timeframe:' (1 minutes), and checkboxes for 'In a single app' (unchecked) and 'Count only unique target files or folders per user' (checked). To the right, a 'Governance actions' section lists actions for 'All apps' and 'Microsoft 365', each with checkboxes for 'Notify user', 'Notify additional users', 'Suspend Microsoft Entra user', 'Require user to sign in again', and 'Confirm user compromised'. A vertical sidebar on the right displays 'Incident ID: 23', 'Categories: Credential access, Suspicious activity', and 'Last activity: Oct 2, 2024 10:21:19 PM'. At the bottom, there are sections for 'Risk' and 'None'.

And everything else...

Insider Risk Management

Active Directory / Entra ID tiering

Credential Guard

Entra Internet / Private Access (GSA)

Tenant Allow / Block Lists (TLDs)

Ingest into a SIEM (Sentinel)

Edge Hardening

Safe Attachments

SPF / DKIM / DMARC

Token Protection

AppLocker / WDAC

Attack Surface Reduction Rules

Web Content Filtering (Newly Registered Domains)

Information Barriers



We all can, and must, do better...



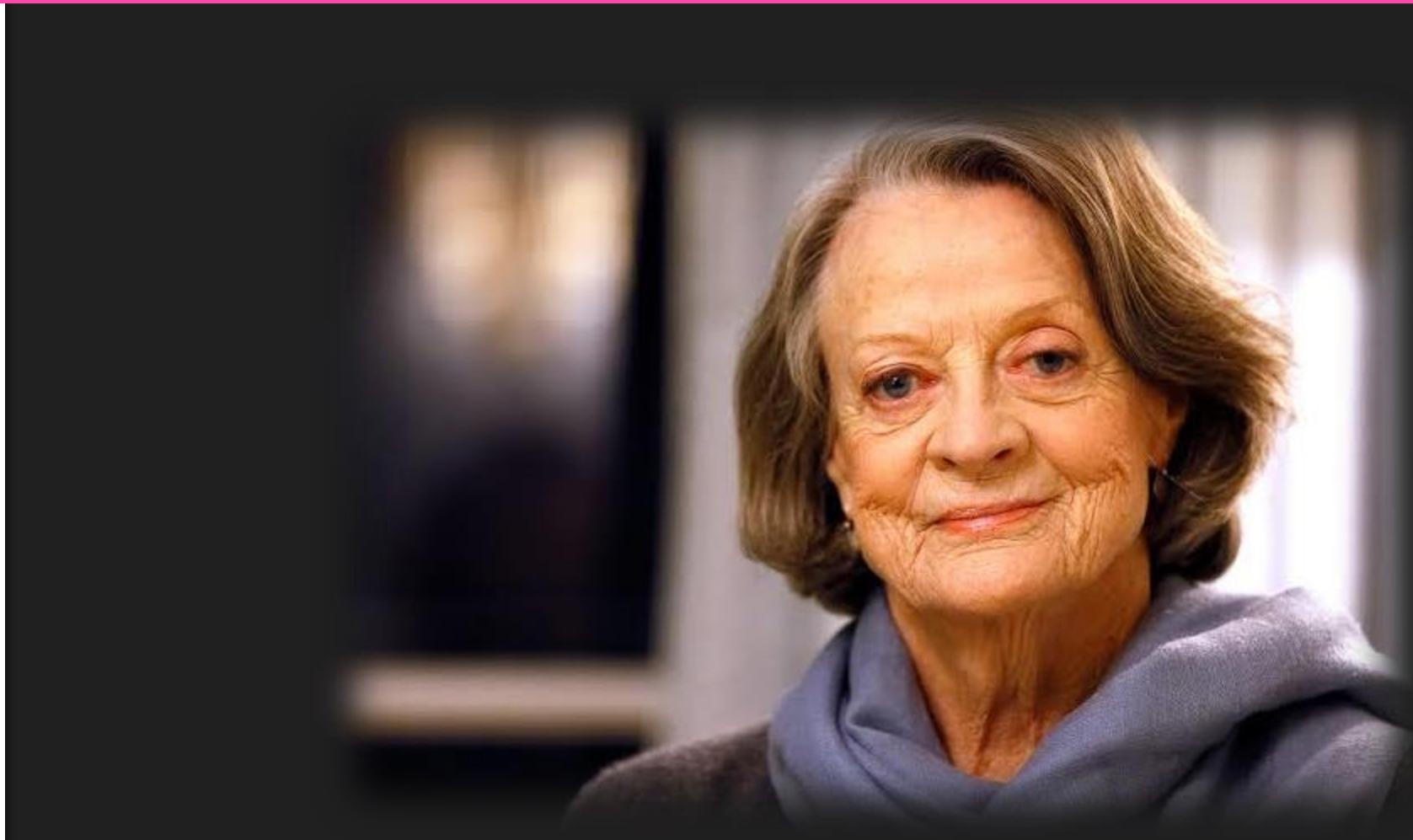
“If you’re faced with the tradeoff between security and another priority, your answer is clear: Do security”

Satya Nadella
Microsoft CEO

#ScottishSummit2024



RIP - Dame Margaret Natalie Smith, CH DBE



#ScottishSummit2024

Defence Against The Dark Arts



Thank You!

Please leave feedback in the Scottish Summit app