One year of fighting adversary-in-the-middle, notes from the field

Erik Loef & Kenneth van Surksum

DEMO

Adversary in the Middle

Successful session stealing in a LAB

About “Kenneth van Surksum”

Focus

Modern Workplace Consultant, Microsoft Certified Trainer, Co-founder and organizer at Workplace Ninja User Group Netherlands

From

The Netherlands

My Blog

https://www.vansurksum.com

Certifications

Microsoft 365 Certified Enterprise Administrator

Microsoft Certified Azure Solutions Architect

Hobbies

Cooking on my Kamado Joe & Sports

Contact

kenneth@vansurksum.com

https://twitter.com/kennethvs

https://www.linkedin.com/in/kennethvansurksum

About “Erik Loef”

Focus

Security for SMB & MSP

From

The Netherlands

My Blog

LinkedIn : Erik Loef

Certifications

Msc Computer Science
MVP security

Hobbies

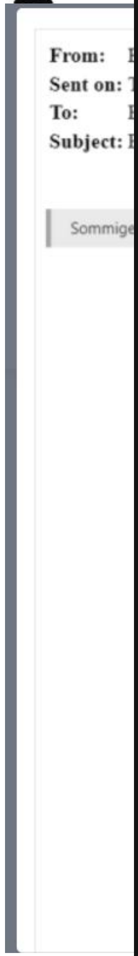
(beach) Volleybal

Contact

eloef@proxsys.nl
x: @erikloef

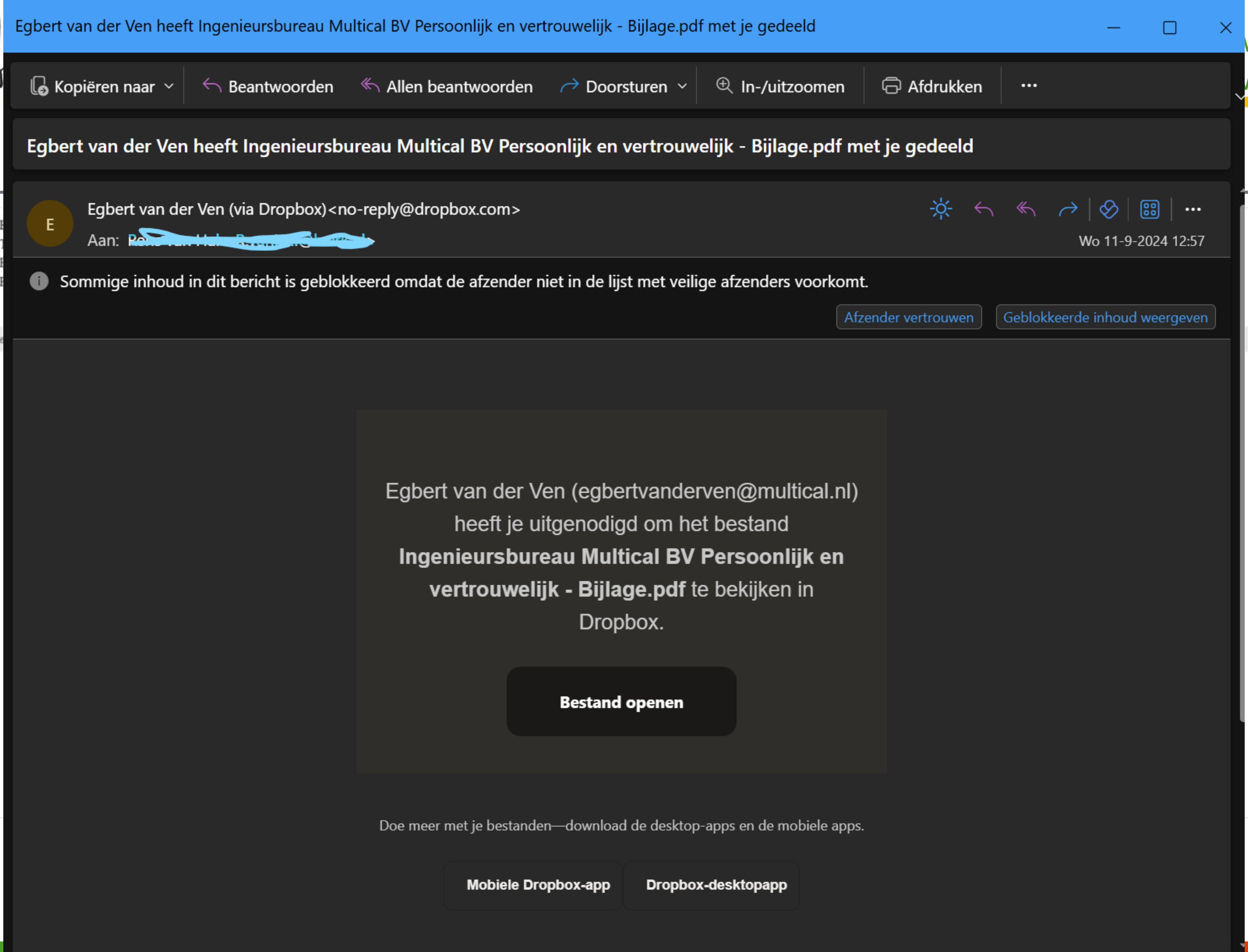
FOLLOW A LIVE CASE

vw.wpninjas.eu
/PNinjaS



From: E
Sent on: T
To: E
Subject: E

Sommige



Egbert van der Ven heeft Ingenieursbureau Multical BV Persoonlijk en vertrouwelijk - Bijlage.pdf met je gedeeld

Egbert van der Ven heeft Ingenieursbureau Multical BV Persoonlijk en vertrouwelijk - Bijlage.pdf met je gedeeld

Egbert van der Ven (via Dropbox)<no-reply@dropbox.com>
Aan: [redacted]

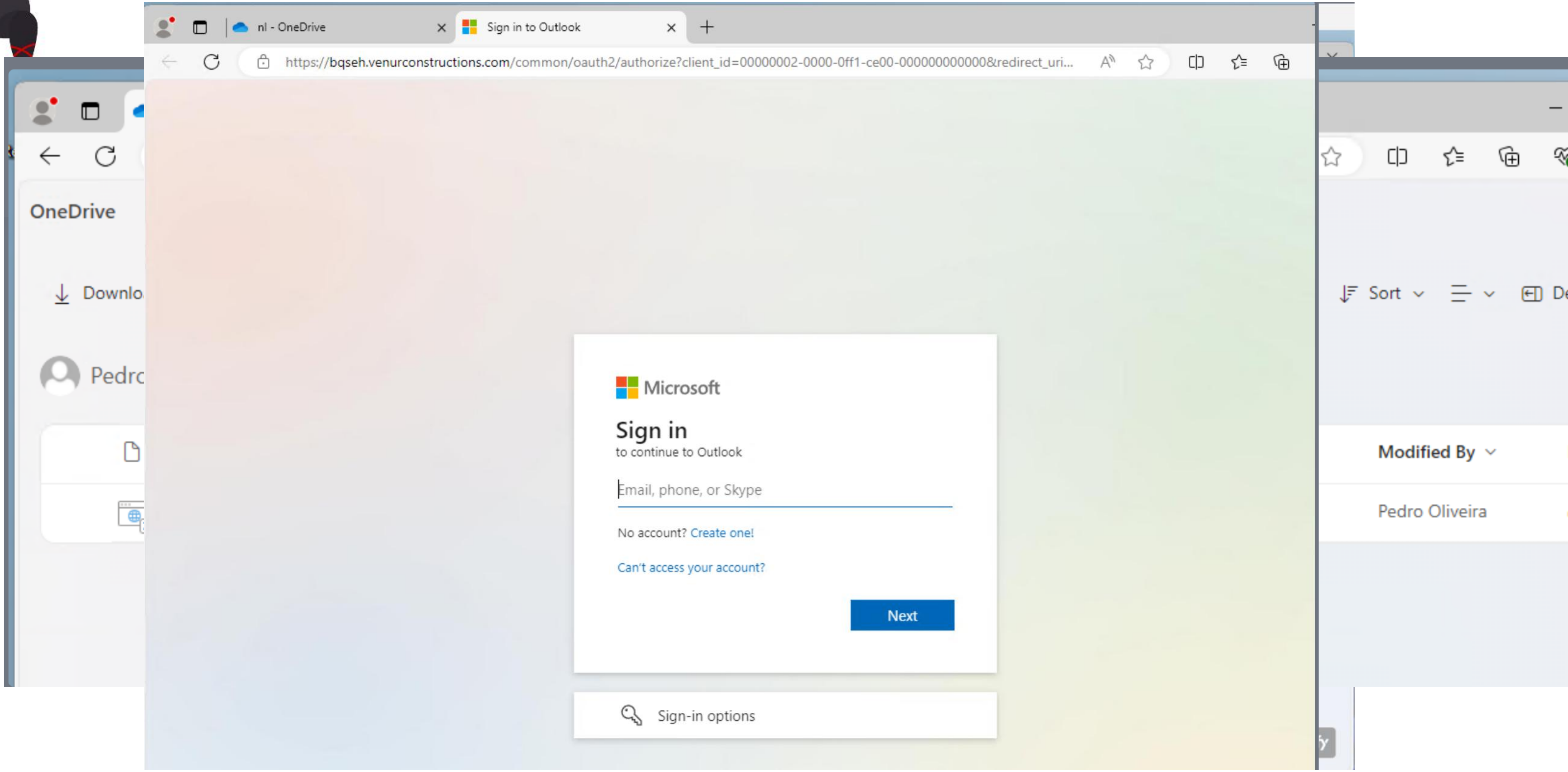
Wo 11-9-2024 12:57

Sommige inhoud in dit bericht is geblokkeerd omdat de afzender niet in de lijst met veilige afzenders voorkomt.

Egbert van der Ven (egbertvanderven@multical.nl) heeft je uitgenodigd om het bestand **Ingenieursbureau Multical BV Persoonlijk en vertrouwelijk - Bijlage.pdf** te bekijken in Dropbox.

Doe meer met je bestanden—download de desktop-apps en de mobiele apps.

The phishing link



https://bqseh.venurconstructions.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&redirect_uri...

Microsoft

Sign in

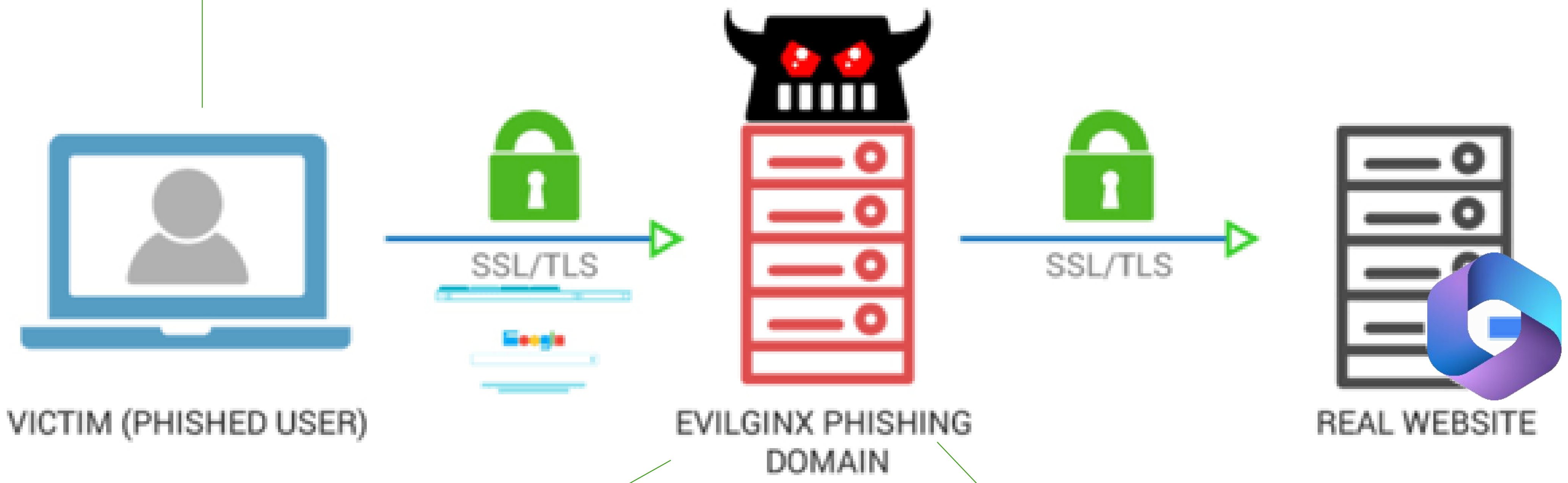
to continue to Outlook

No account? Create one!

Can't access your account?

Our setup

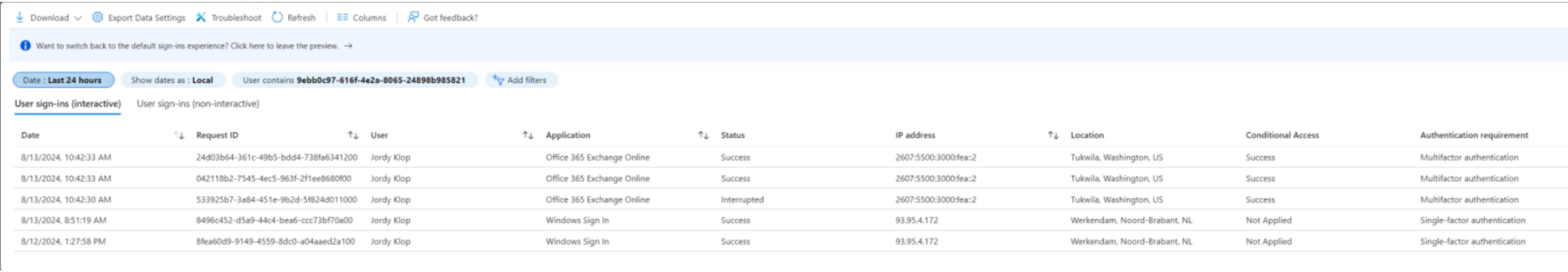
DIFFERENT URL!



DIFFERENT IP ADDRESS

DIFFERENT DEVICE

Recent Example



Want to switch back to the default sign-ins experience? Click here to leave the preview. →

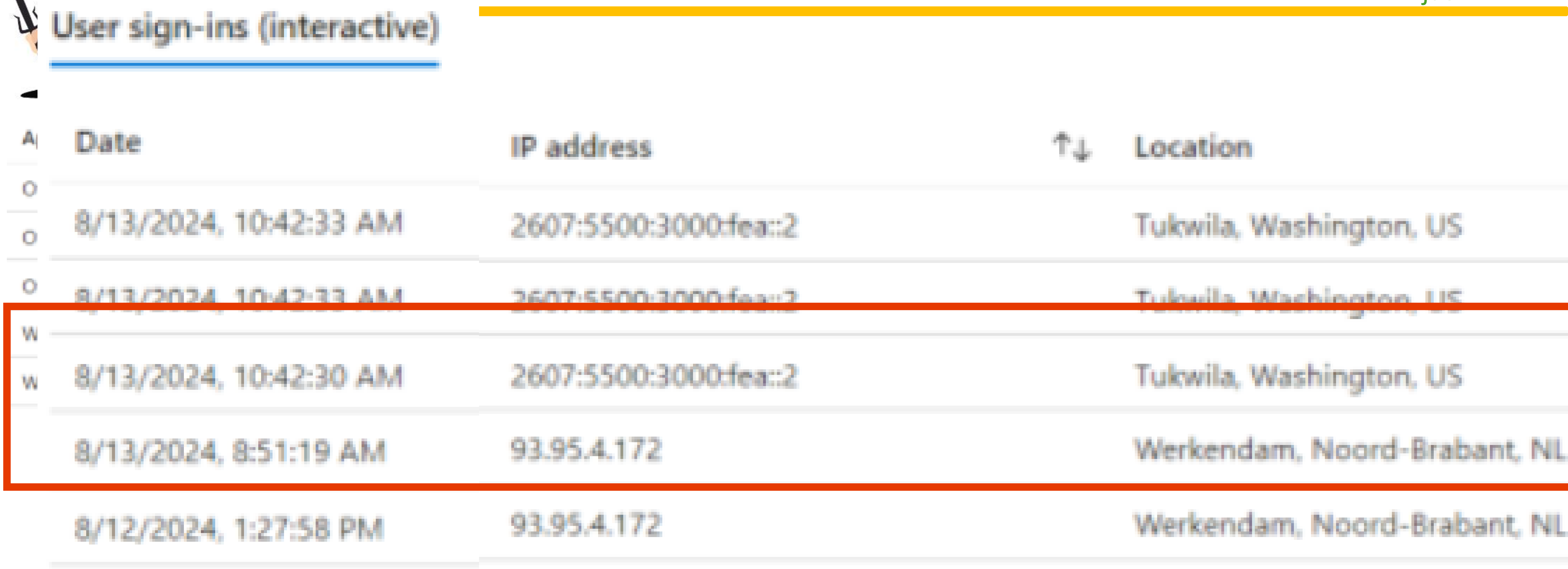
Date : **Last 24 hours** | Show dates as : **Local** | User contains **9ebb0c97-616f-4e2a-8065-24898b985821** | Add filters

User sign-ins (interactive) | User sign-ins (non-interactive)

Date	Request ID	User	Application	Status	IP address	Location	Conditional Access	Authentication requirement
8/13/2024, 10:42:33 AM	24d03b64-361c-49b5-bdd4-738fa6341200	Jordy Klop	Office 365 Exchange Online	Success	2607:5500:3000:fea::2	Tukwila, Washington, US	Success	Multifactor authentication
8/13/2024, 10:42:33 AM	042118b2-7545-4ec5-963f-2f1ee8680f00	Jordy Klop	Office 365 Exchange Online	Success	2607:5500:3000:fea::2	Tukwila, Washington, US	Success	Multifactor authentication
8/13/2024, 10:42:30 AM	533925b7-3a84-451e-9b2d-5f824d011000	Jordy Klop	Office 365 Exchange Online	Interrupted	2607:5500:3000:fea::2	Tukwila, Washington, US	Success	Multifactor authentication
8/13/2024, 8:51:19 AM	8496c452-d5a9-44c4-bea6-ccc73bf70a00	Jordy Klop	Windows Sign In	Success	93.95.4.172	Werkendam, Noord-Brabant, NL	Not Applied	Single-factor authentication
8/12/2024, 1:27:58 PM	8fea60d9-9149-4559-8dc0-a04aaed2a100	Jordy Klop	Windows Sign In	Success	93.95.4.172	Werkendam, Noord-Brabant, NL	Not Applied	Single-factor authentication

Recent Example 13-8-2024

www.wpninjas.eu
#WPNinjaS



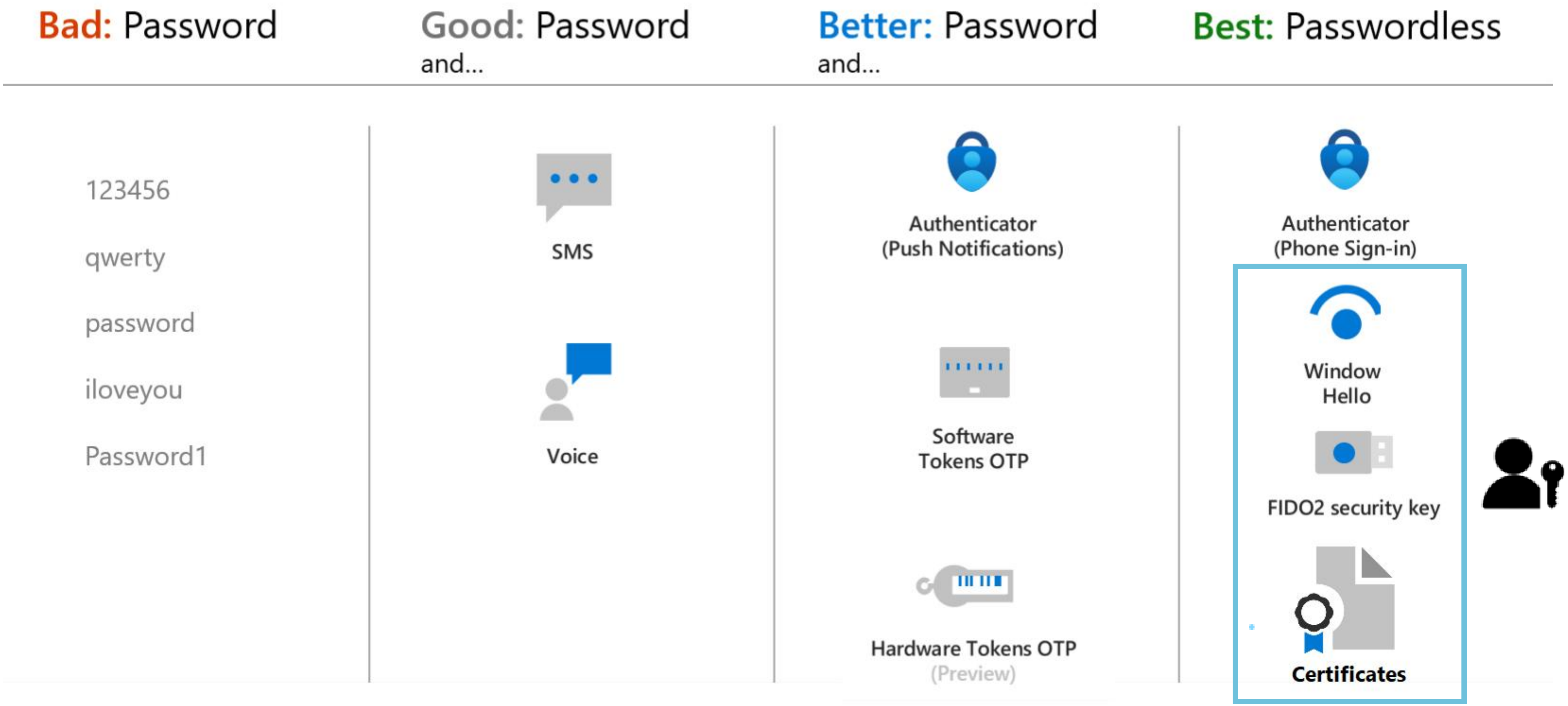
User sign-ins (interactive)

Date	IP address	Location
8/13/2024, 10:42:33 AM	2607:5500:3000:fea::2	Tukwila, Washington, US
8/13/2024, 10:42:33 AM	2607:5500:3000:fea::2	Tukwila, Washington, US
8/13/2024, 10:42:30 AM	2607:5500:3000:fea::2	Tukwila, Washington, US
8/13/2024, 8:51:19 AM	93.95.4.172	Werkendam, Noord-Brabant, NL
8/12/2024, 1:27:58 PM	93.95.4.172	Werkendam, Noord-Brabant, NL

MFA Methods

Bad: Password	Good: Password and…	Better: Password and…	Best: Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty	Voice	Software Tokens OTP	Window Hello
password		Hardware Tokens OTP (Preview)	FIDO2 security key
iloveyou			**Certificates**
Password1			

MFA Methods



Bad: Password

- 123456
- qwerty
- password
- iloveyou
- Password1

Good: Password and…

- SMS
- Voice

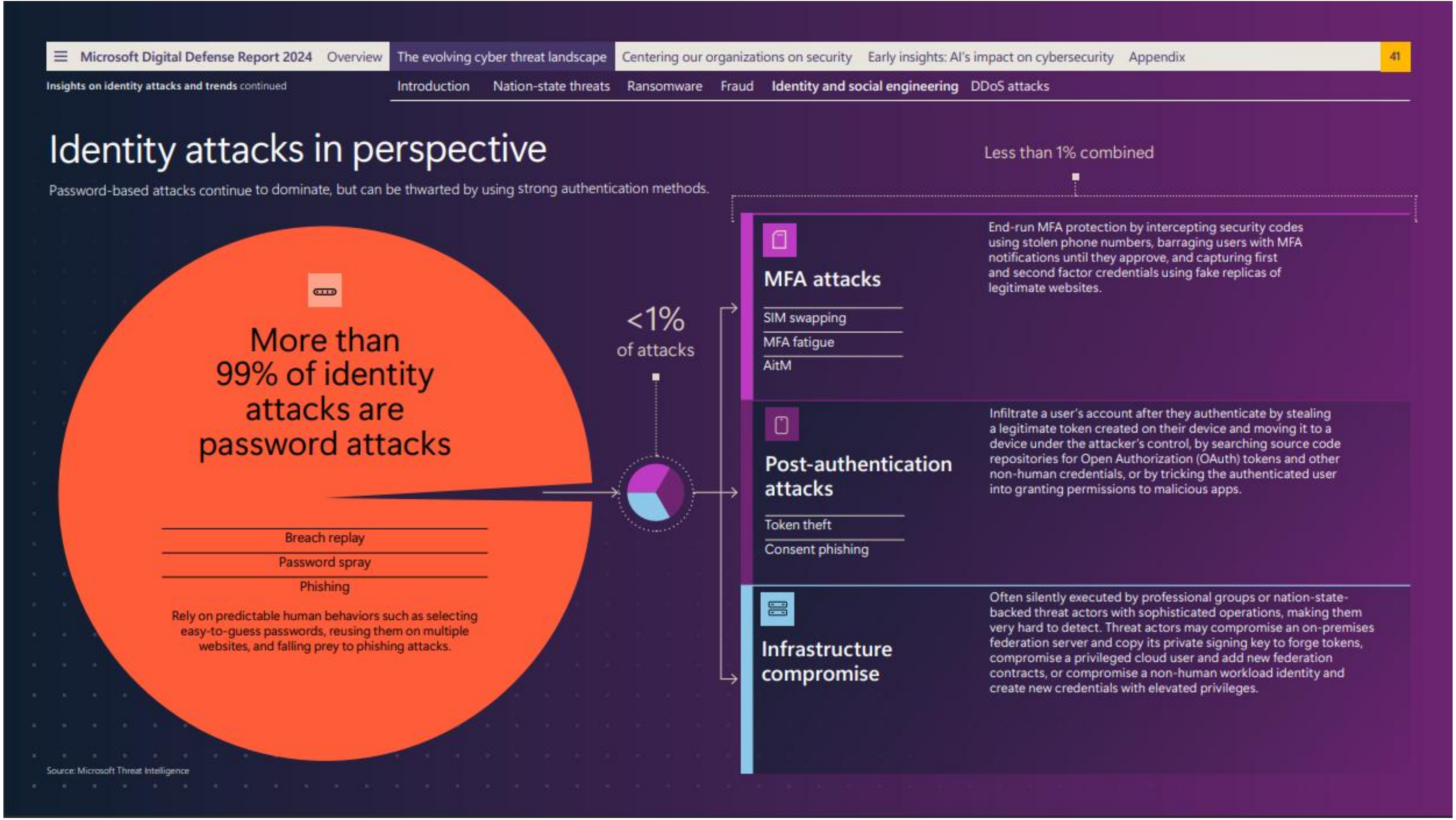
Better: Password and…

- Authenticator (Push Notifications)
- Software Tokens OTP
- Hardware Tokens OTP (Preview)

Best: Passwordless

- Authenticator (Phone Sign-in)
- Window Hello
- FIDO2 security key
- Certificates

What is Microsoft saying?



☰ Microsoft Digital Defense Report 2024 | Overview | The evolving cyber threat landscape | Centering our organizations on security | Early insights: AI's impact on cybersecurity | Appendix | 41

Insights on identity attacks and trends continued

Introduction | Nation-state threats | Ransomware | Fraud | **Identity and social engineering** | DDoS attacks

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks

- Breach replay
- Password spray
- Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks

Less than 1% combined

MFA attacks

- SIM swapping
- MFA fatigue
- AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

Post-authentication attacks

- Token theft
- Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

Infrastructure compromise

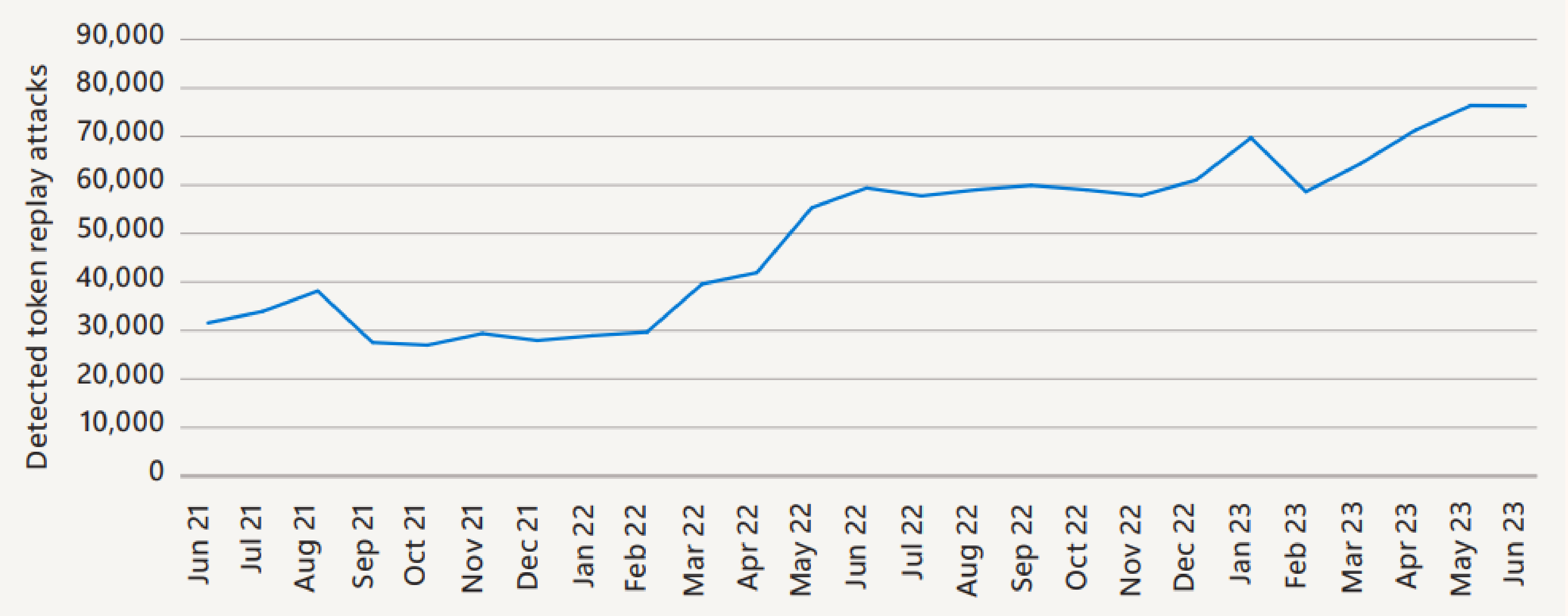
Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

Microsoft Digital Defense Report 2024

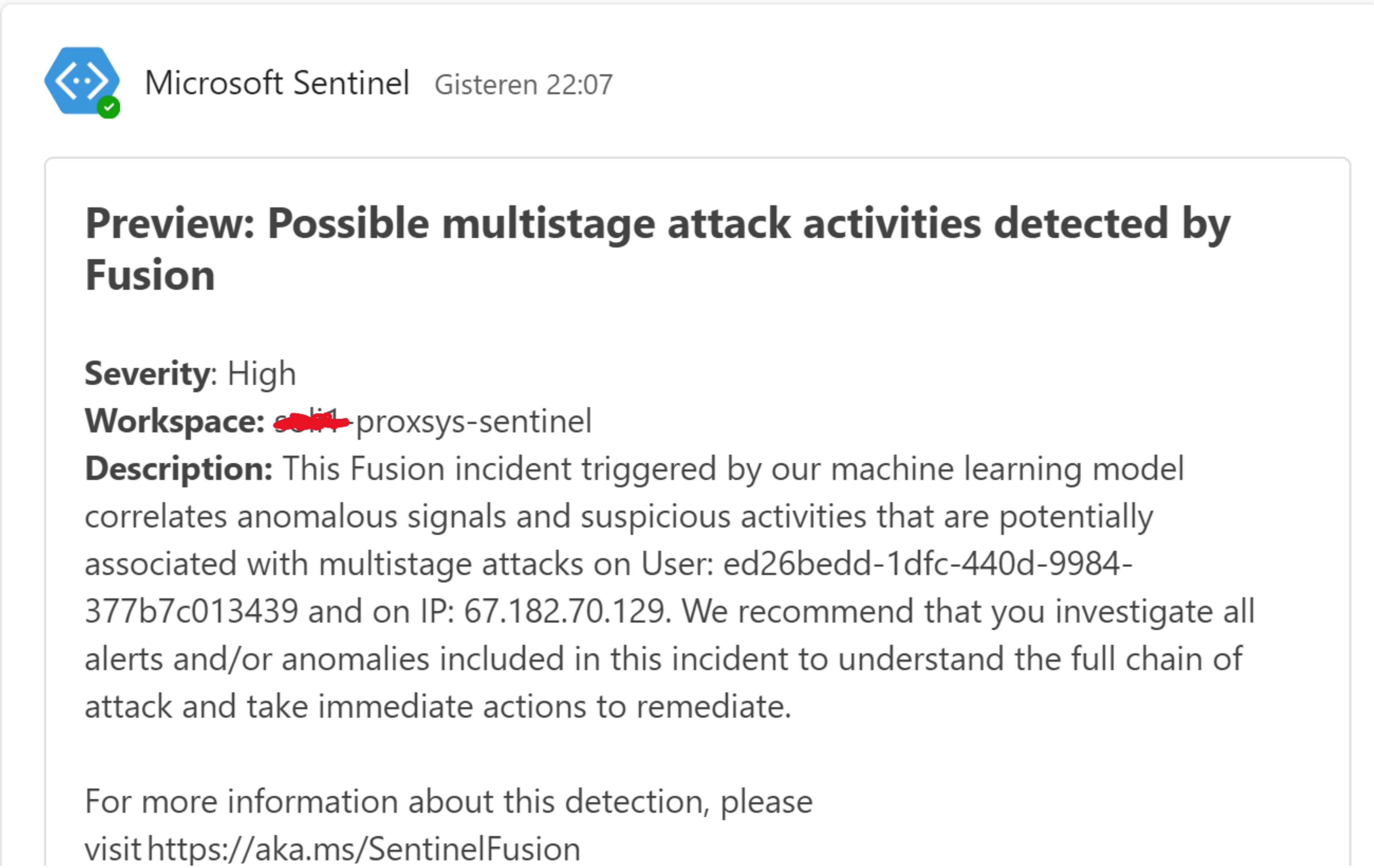
MICROSOFT DDR

Token replay attacks consistently growing since early 2022



Source: Azure Active Directory Identity Protection data

Last week



Microsoft Sentinel Gisteren 22:07

Preview: Possible multistage attack activities detected by Fusion

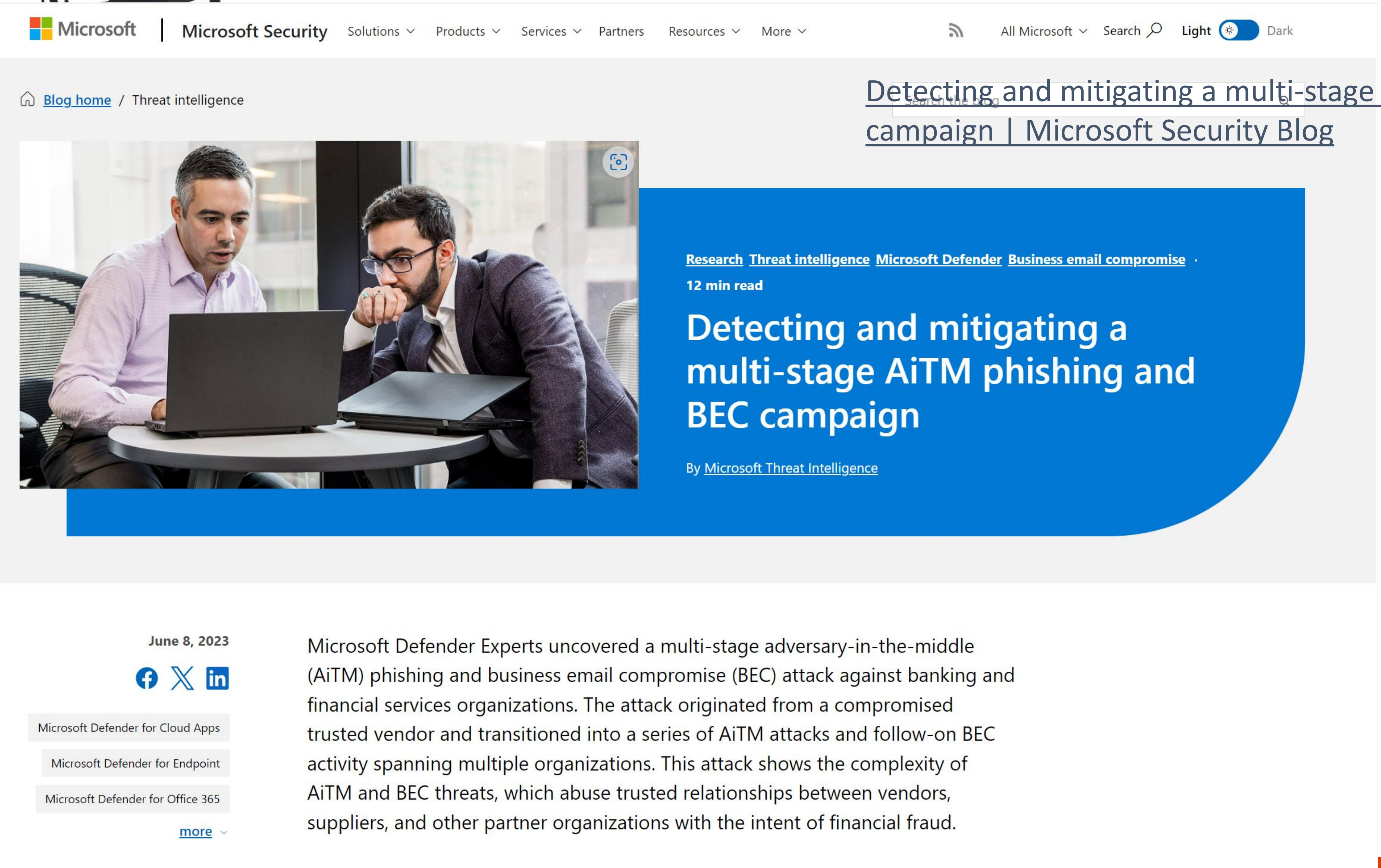
Severity: High
Workspace: [redacted]-proxsys-sentinel
Description: This Fusion incident triggered by our machine learning model correlates anomalous signals and suspicious activities that are potentially associated with multistage attacks on User: ed26bedd-1dfc-440d-9984-377b7c013439 and on IP: 67.182.70.129. We recommend that you investigate all alerts and/or anomalies included in this incident to understand the full chain of attack and take immediate actions to remediate.

For more information about this detection, please visit https://aka.ms/SentinelFusion

What is Microsoft saying?

www.wpninjas.eu
#WPNinjaS

[Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft Security Blog]



Blog home / Threat intelligence

Research Threat intelligence Microsoft Defender Business email compromise ·

12 min read

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign

By Microsoft Threat Intelligence

June 8, 2023

Microsoft Defender for Cloud Apps

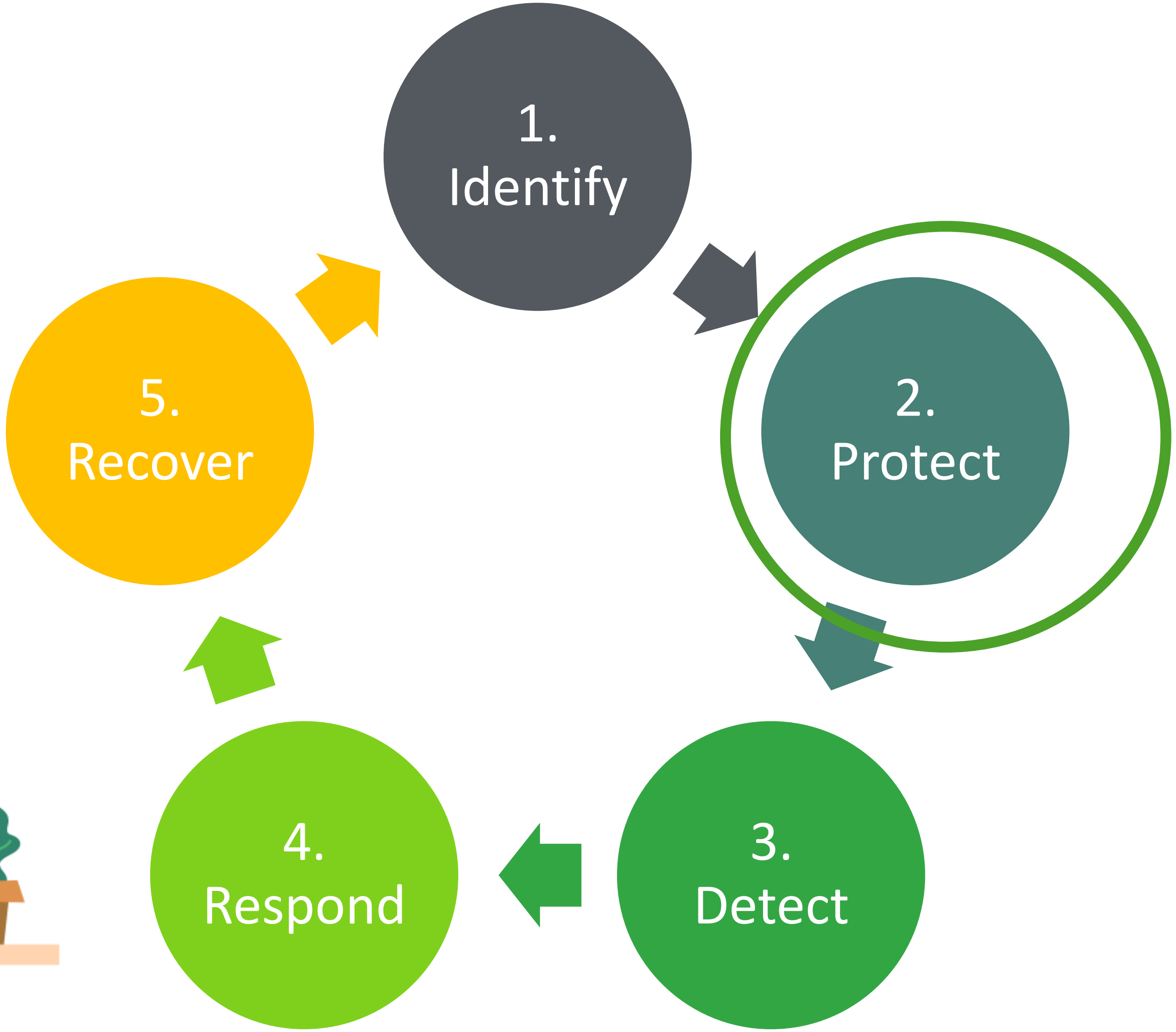
Microsoft Defender for Endpoint

Microsoft Defender for Office 365

more

Microsoft Defender Experts uncovered a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) attack against banking and financial services organizations. The attack originated from a compromised trusted vendor and transitioned into a series of AiTM attacks and follow-on BEC activity spanning multiple organizations. This attack shows the complexity of AiTM and BEC threats, which abuse trusted relationships between vendors, suppliers, and other partner organizations with the intent of financial fraud.

www.wpninjas.eu
#WPNinjaS



Protect – phishing resistant MFA

- Certificate Based Authentication
- Passkeys/FIDO security key
- Windows Hello or Business

DEMO

Adversary in the Middle

With hardened Identity,
AiTM is mitigated

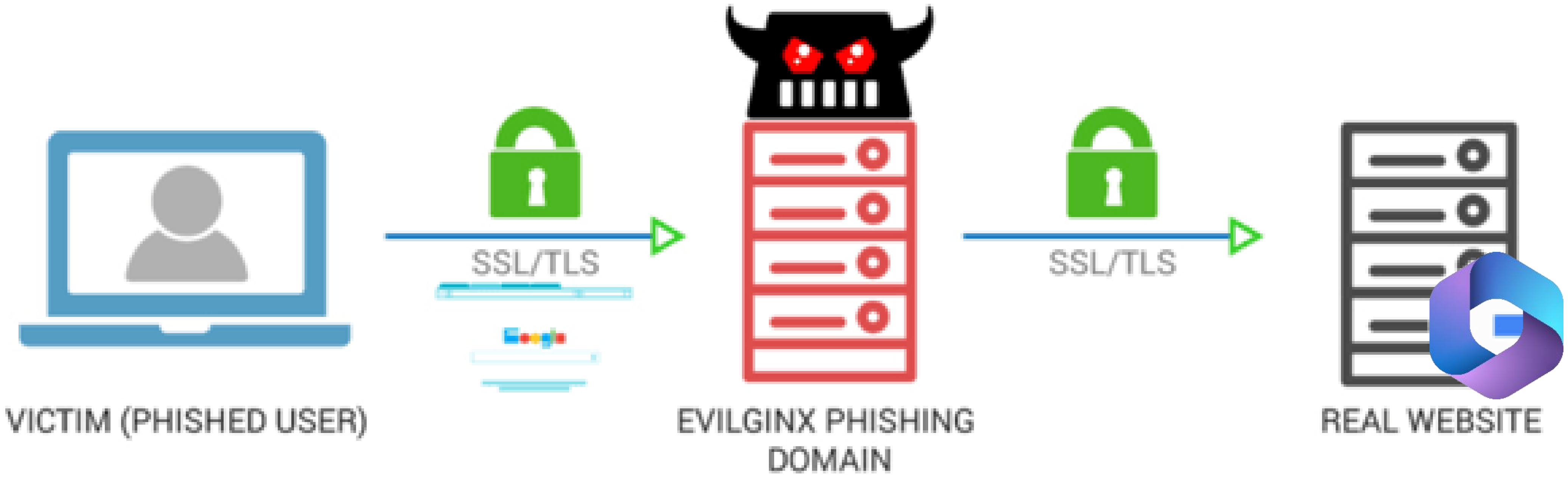
Demo with fido key

Pro/Cons

- Certificate Based Authentication
  - Issue on mobile especially BYOD scenarios
- Passkeys/FIDO security key
  - Passkeys still preview
  - FIDO key support for mobile
  - Complex process onboarding/offboarding and lost
- Windows Hello or Business
  - Windows only

Protect – CA options

- Allow only managed devices
- Allow only public IPs from your country



Part 1
Block and allow specific IP ranges

Part 2

Allow only managed devices

Pro/Cons

- When holiday many changes
- Not working for 4G/5G internet (roam home)
- BYOD isn’t possible anymore

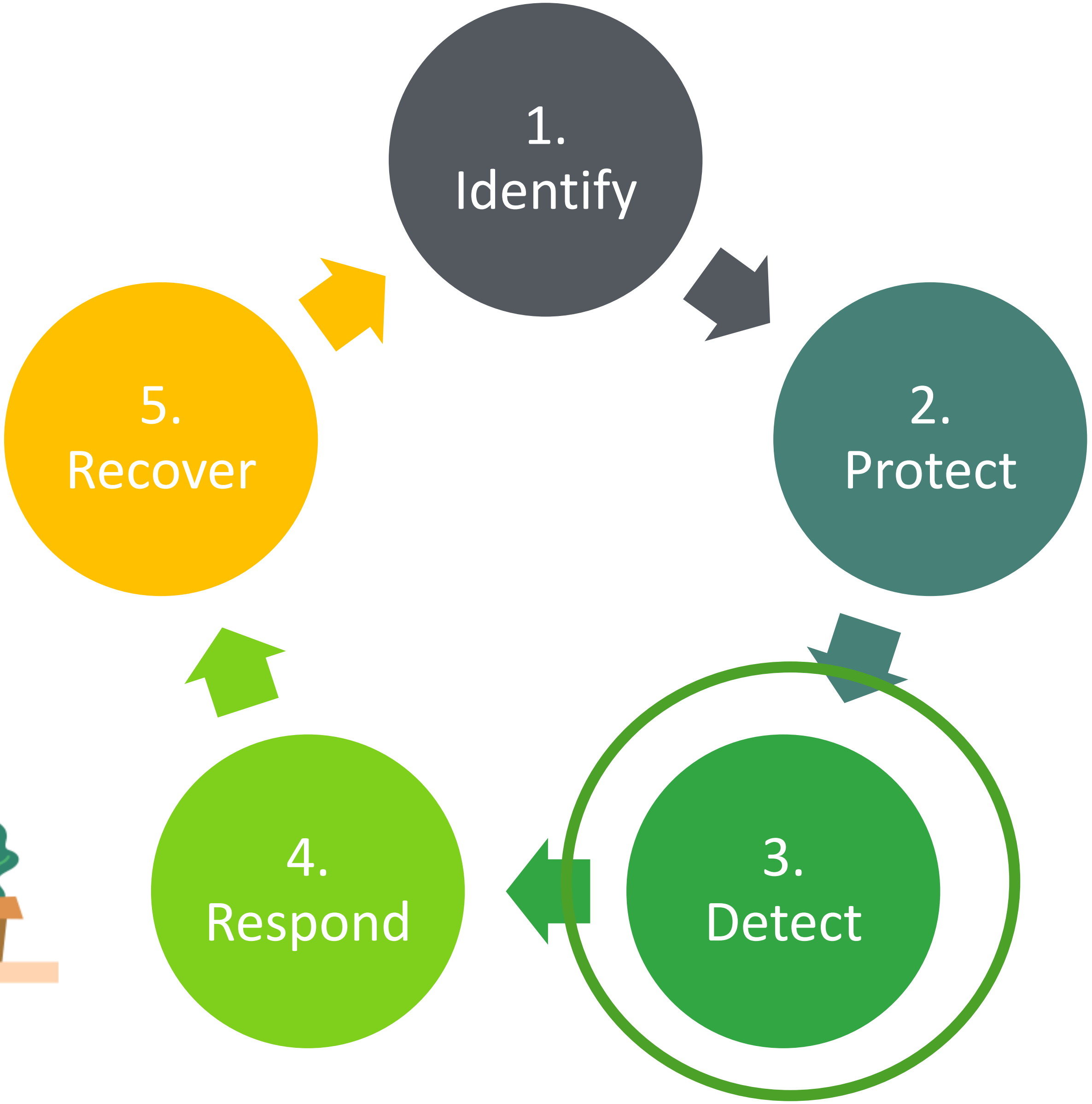
Protect – CA options with P2

- Block Risky Sign ins
- Token Protection
  Token protection in Microsoft Entra Conditional Access - Microsoft Entra ID | Microsoft Learn

Part 1

Risky Sign in CA policy

Part 2
(new) Token Protection Policy



1. Identify

2. Protect

3. Detect

4. Respond

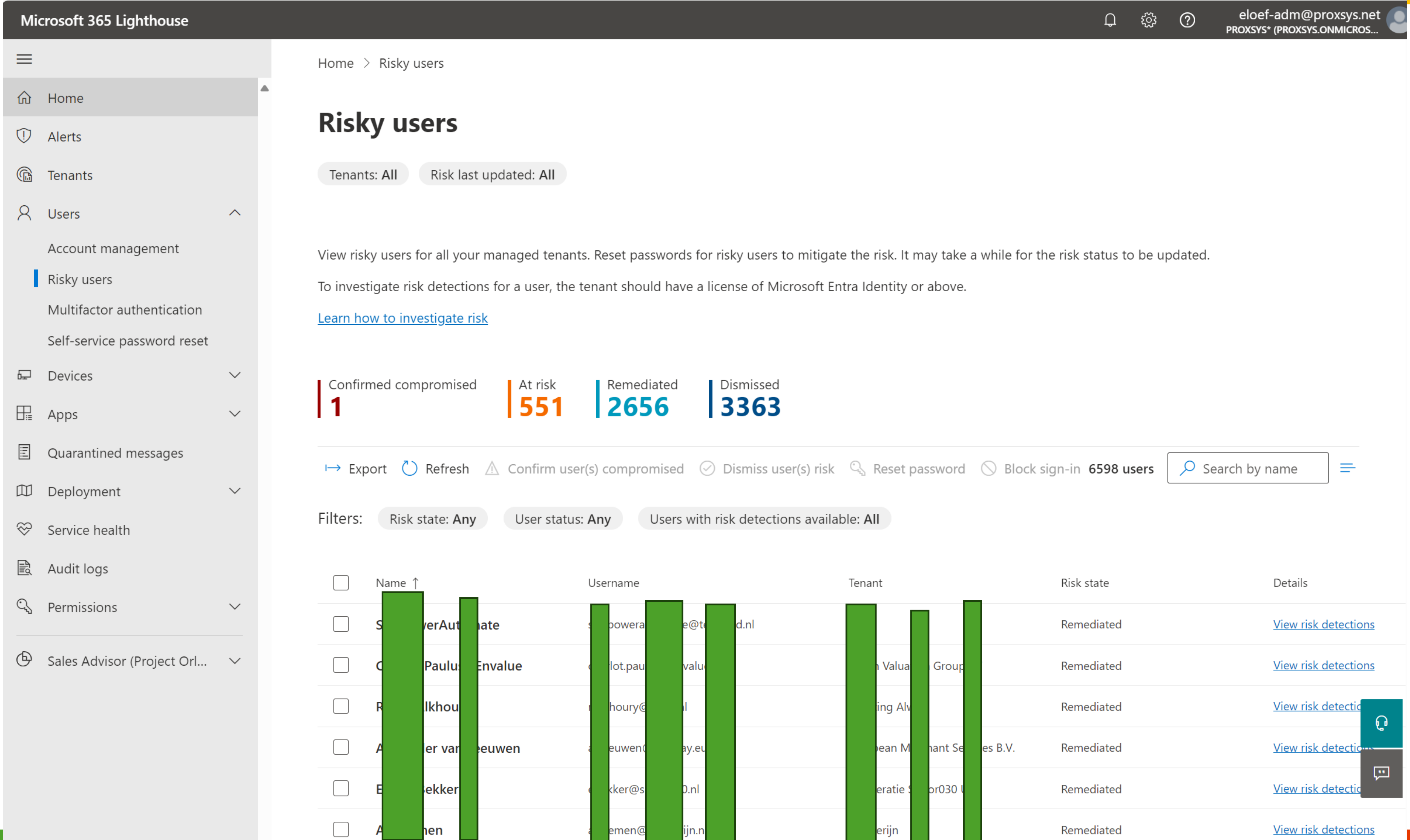
5. Recover

Detect – free options

- Azure Lighthouse
- Powershell script
- Sentinel

Lighthouse

www.wpninjas.eu
#WPNinjaS



Risky users

Tenants: **All** Risk last updated: **All**

View risky users for all your managed tenants. Reset passwords for risky users to mitigate the risk. It may take a while for the risk status to be updated.

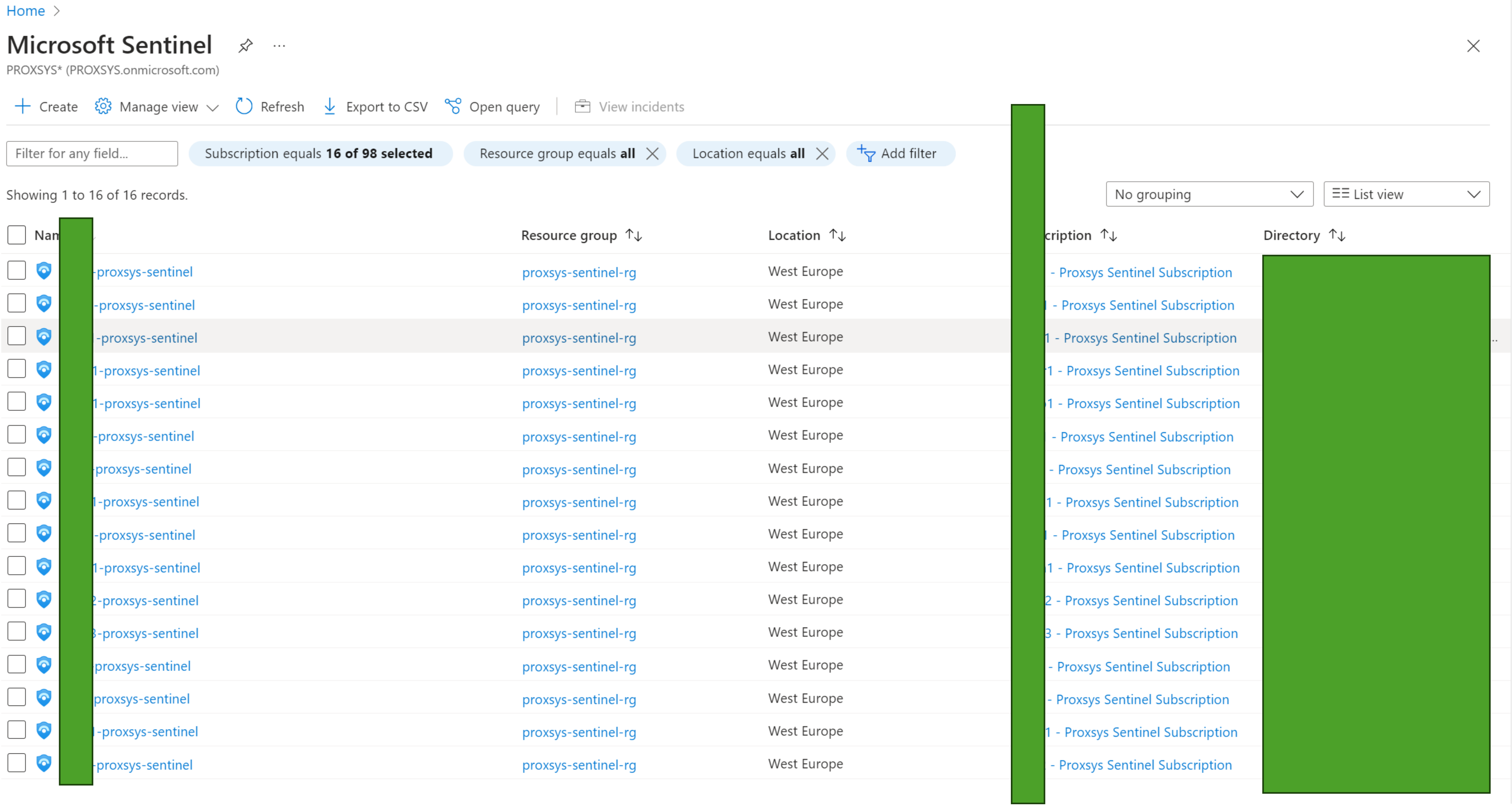
To investigate risk detections for a user, the tenant should have a license of Microsoft Entra Identity or above.

Learn how to investigate risk

Confirmed compromised	At risk	Remediated	Dismissed
1	551	2656	3363

Filters: Risk state: **Any** User status: **Any** Users with risk detections available: **All**

□	Name ↑	Username	Tenant	Risk state	Details
□	[redacted]	[redacted]	[redacted]	Remediated	View risk detections
□	[redacted]	[redacted]	[redacted]	Remediated	View risk detections
□	[redacted]	[redacted]	[redacted]	Remediated	View risk detectio
□	[redacted]	[redacted]	[redacted]	Remediated	View risk detectio
□	[redacted]	[redacted]	[redacted]	Remediated	View risk detectio
□	[redacted]	[redacted]	[redacted]	Remediated	View risk detections



Home >

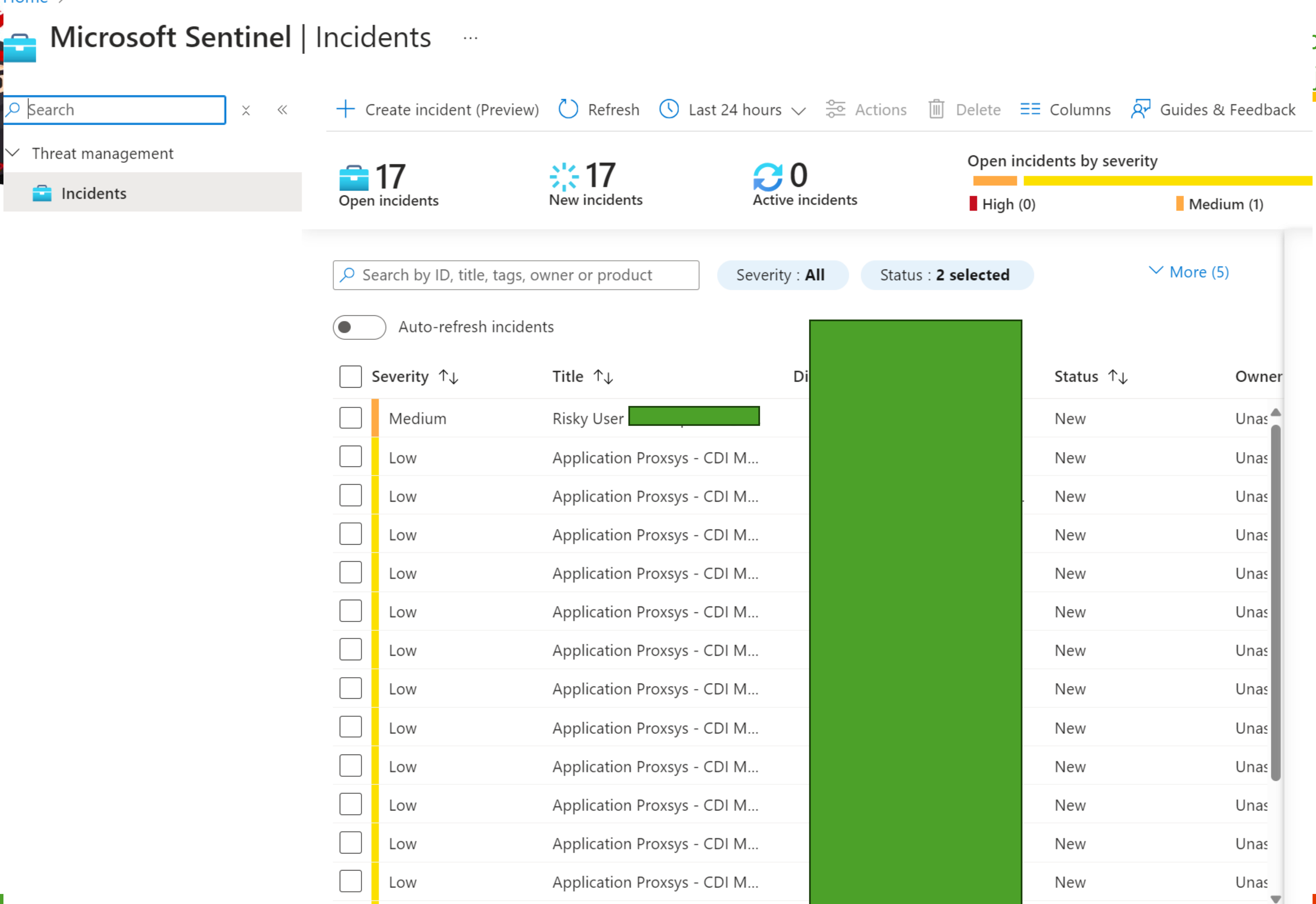
Microsoft Sentinel

PROXSYS* (PROXSYS.onmicrosoft.com)

Subscription equals **16 of 98 selected** | Resource group equals **all** | Location equals **all** | Add filter

Showing 1 to 16 of 16 records.

□	Nam[redacted]	Resource group ↑↓	Location ↑↓	[redacted]cription ↑↓	Directory ↑↓
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]
□	[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	[redacted] - Proxsys Sentinel Subscription	[redacted]



Microsoft Sentinel | Incidents

17 Open incidents

17 New incidents

0 Active incidents

Open incidents by severity

High (0)

Medium (1)

Search by ID, title, tags, owner or product

Severity : **All**

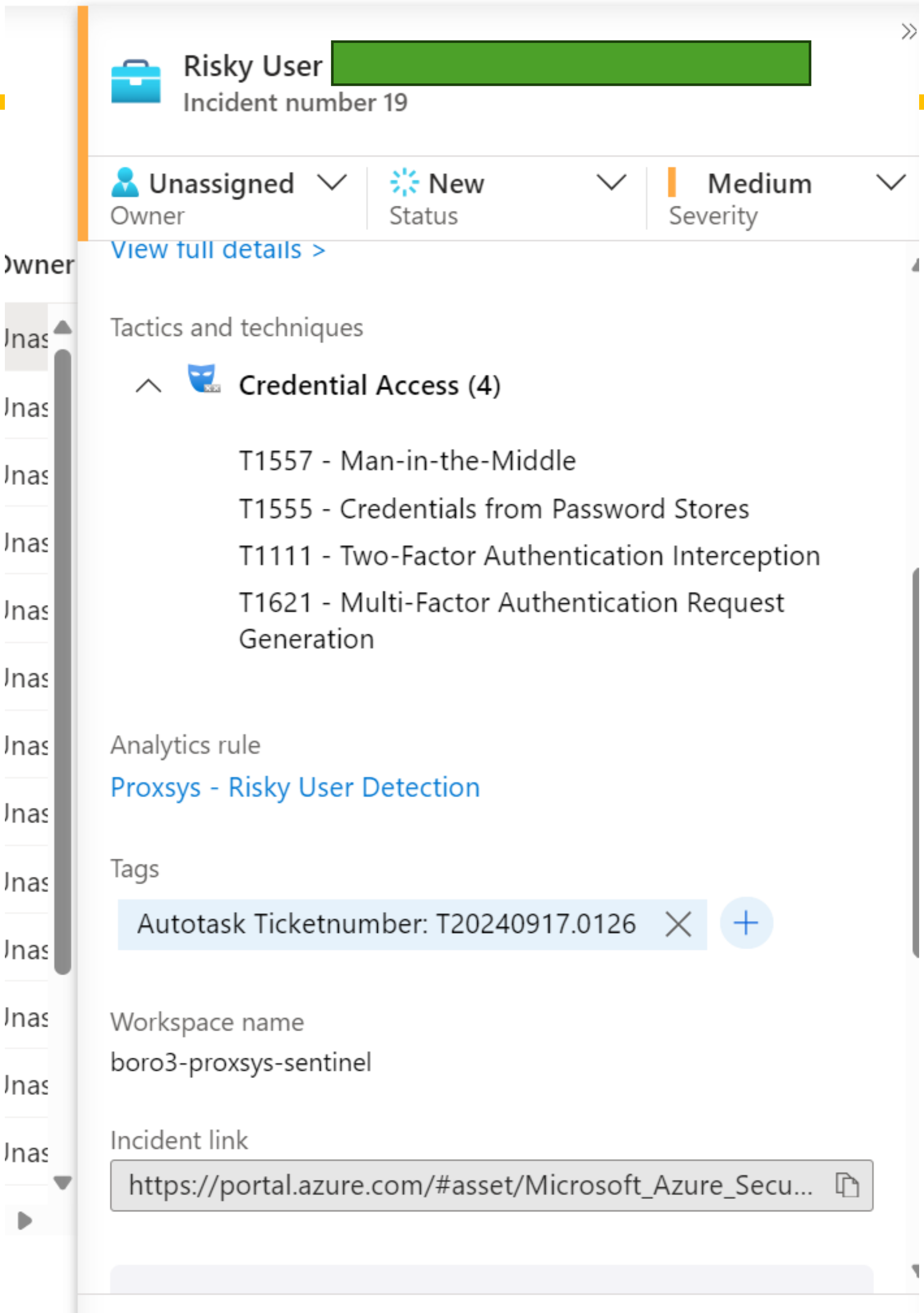
Status : **2 selected**

More (5)

○ Auto-refresh incidents

□	Severity ↑↓	Title ↑↓	Di[redacted]	Status ↑↓	Owner
□	Medium	Risky User [redacted]	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas
□	Low	Application Proxsys - CDI M...	[redacted]	New	Unas

oninjas.eu
jaS



Risky User [redacted]

Incident number 19

Unassigned
Owner

New
Status

Medium
Severity

View full details >

Tactics and techniques

Credential Access (4)

- T1557 - Man-in-the-Middle
- T1555 - Credentials from Password Stores
- T1111 - Two-Factor Authentication Interception
- T1621 - Multi-Factor Authentication Request Generation

Analytics rule

Proxsys - Risky User Detection

Tags

Autotask Ticketnumber: T20240917.0126

Workspace name

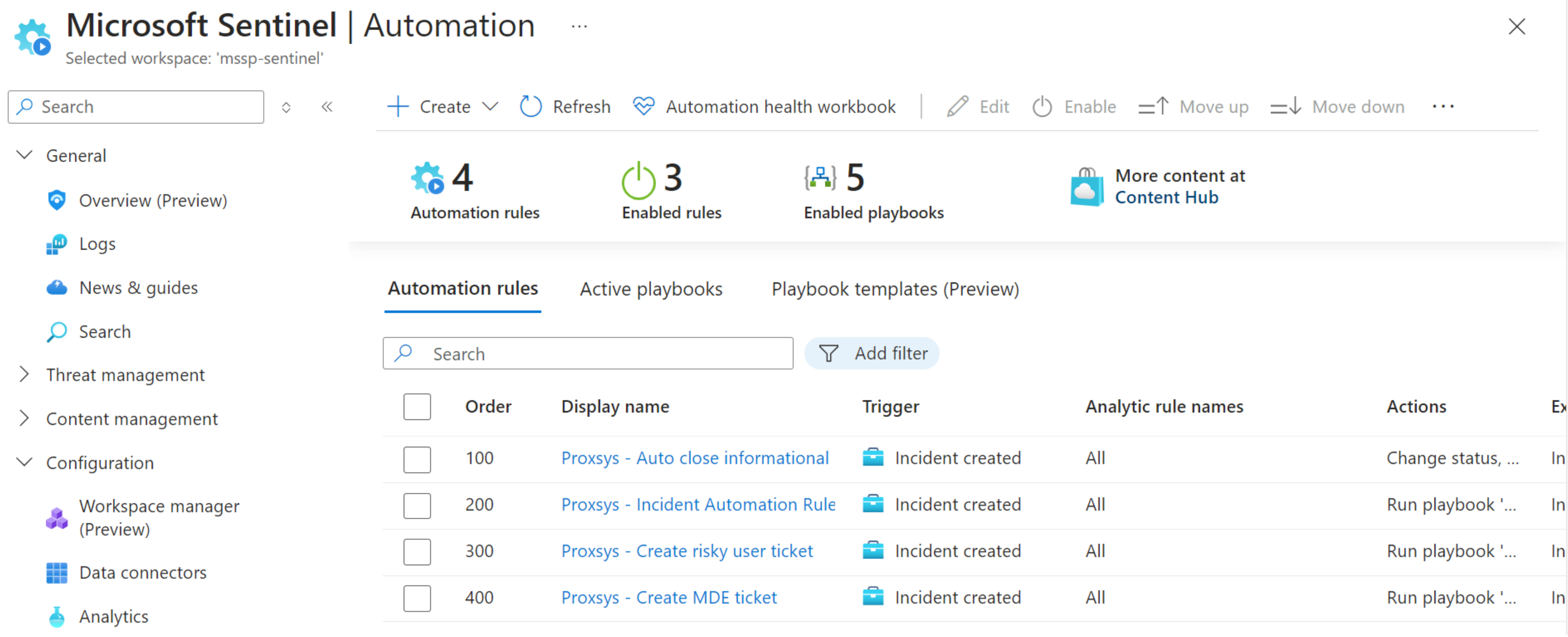
boro3-proxsys-sentinel

Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Secu...

Sentinel automation

www.wpninjas.eu
#WPNinjaS

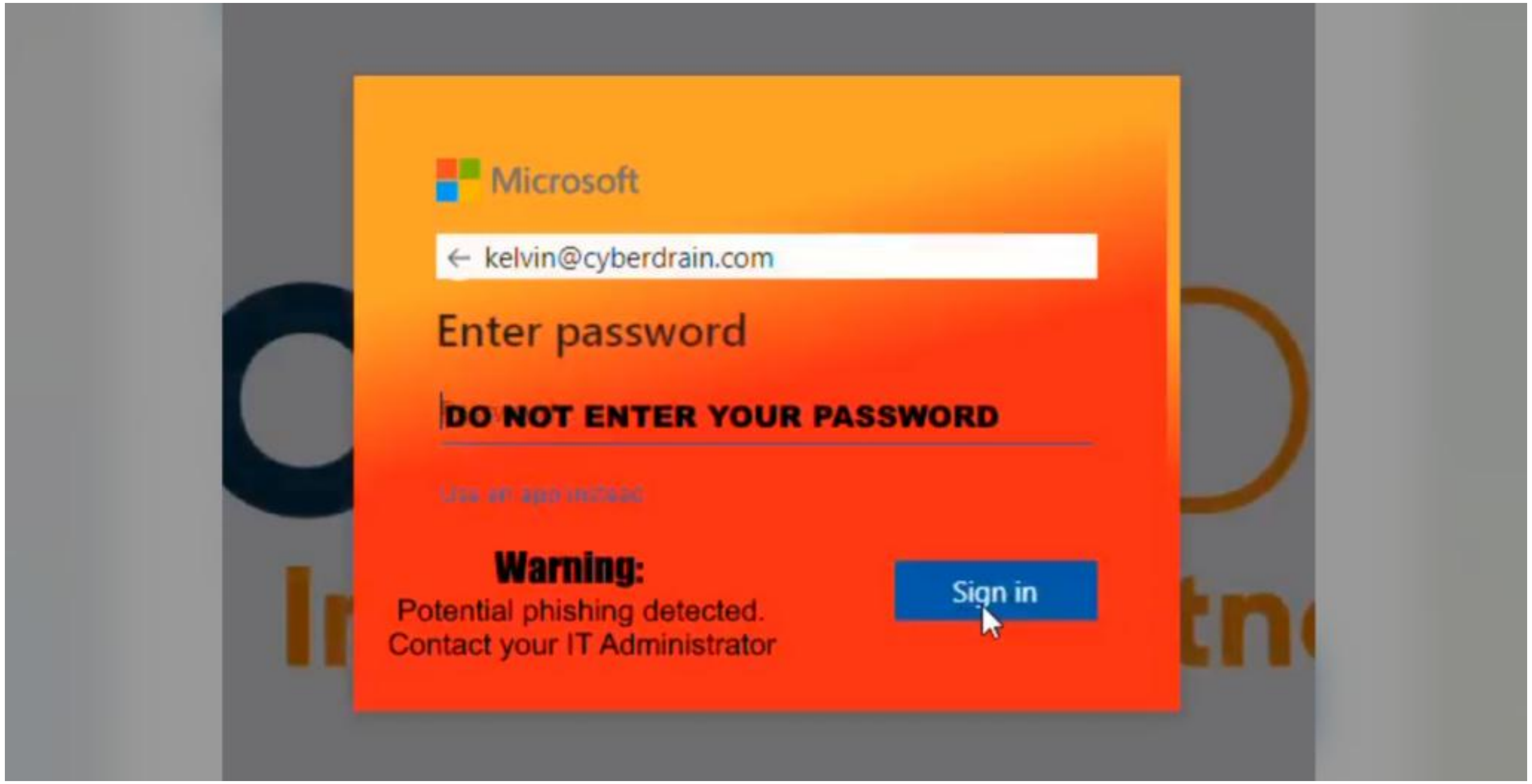


□	Order	Display name	Trigger	Analytic rule names	Actions	Ex
□	100	Proxsys - Auto close informational	Incident created	All	Change status, ...	In
□	200	Proxsys - Incident Automation Rule	Incident created	All	Run playbook '...	In
□	300	Proxsys - Create risky user ticket	Incident created	All	Run playbook '...	In
□	400	Proxsys - Create MDE ticket	Incident created	All	Run playbook '...	In

Inform your users with a simple CSS Trick

Change login

- Cipp.app | zolder.io
- Change the CSS
- Using honeytokens to detect (AiTM) phishing attacks on your Microsoft 365 tenant – Zolder B.V.
- Be careful with modifying CSS, it can also break stuff !!



Microsoft

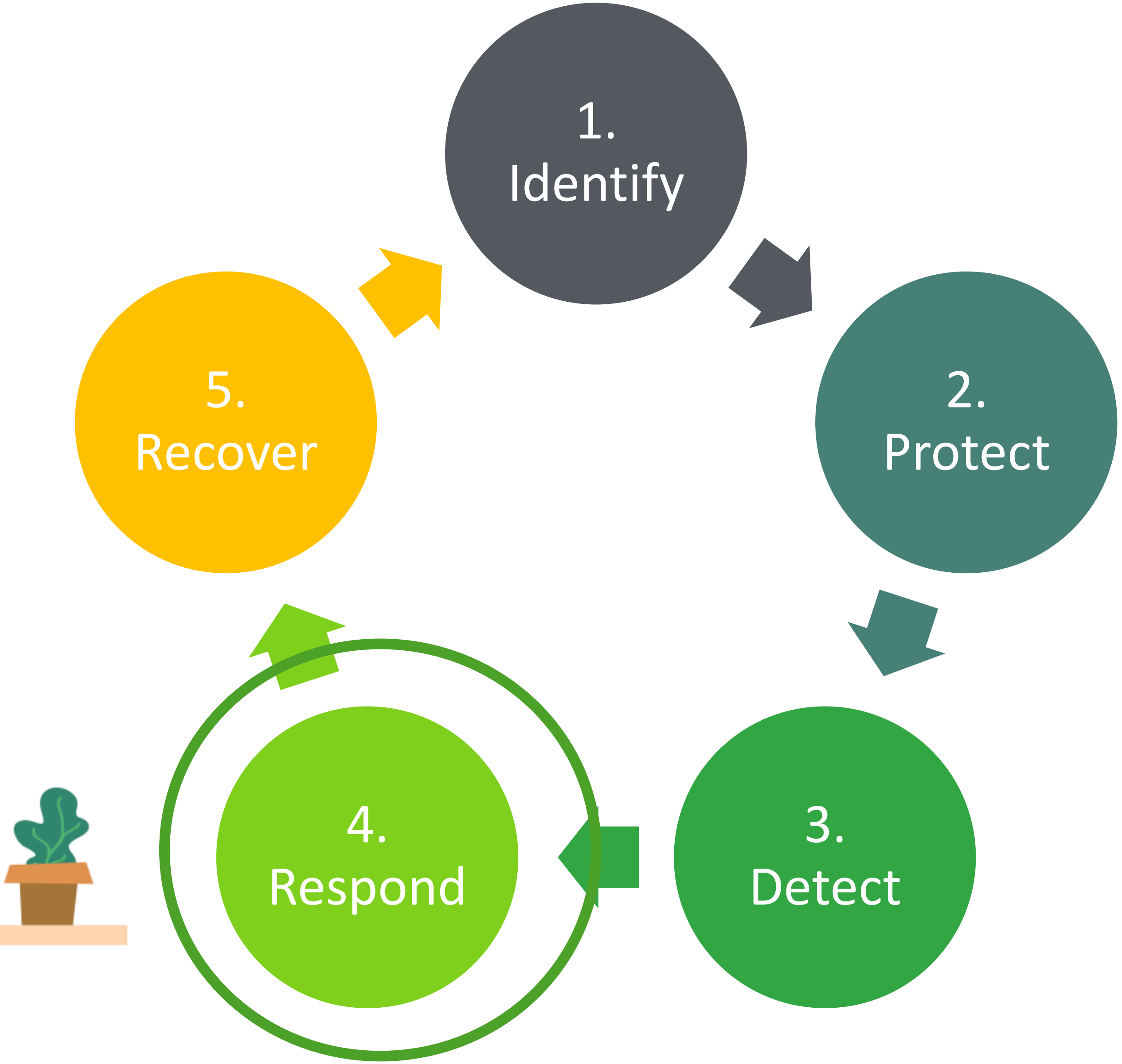
← kelvin@cyberdrain.com

Enter password

DO NOT ENTER YOUR PASSWORD

Use an app instead

Warning:
Potential phishing detected.
Contact your IT Administrator



1. Identify

2. Protect

3. Detect

4. Respond

5. Recover

Respond – What to do ?

- Revoke session
- Check for extra MFA methods
- Check Sign in Logs

Step 1: revo

Step 2: chec

Step 3: disal

Step 4: rese

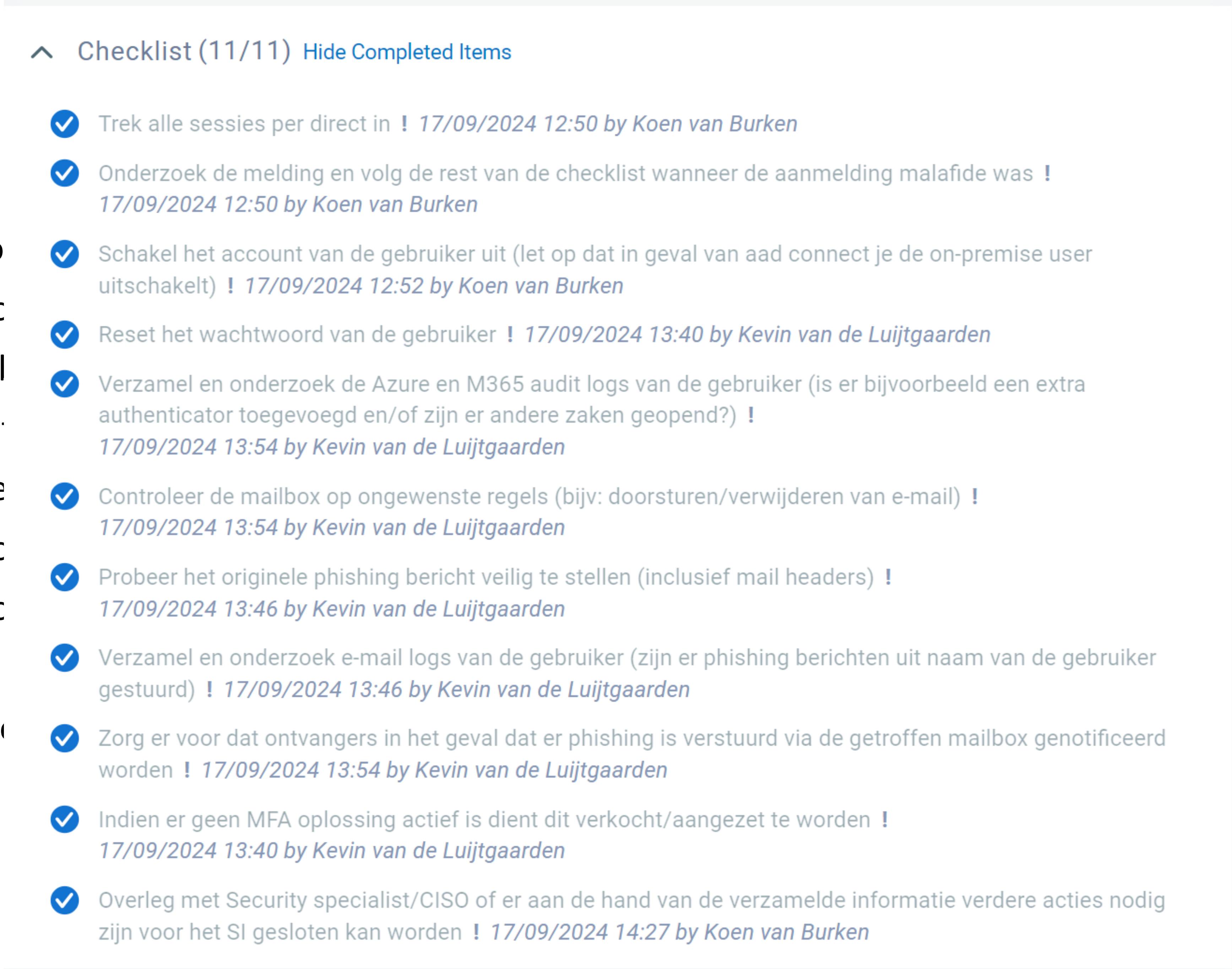
Step 5: colle

Step 6: chec

Step 7: chec

Step 8: take

Step 9: 4 ey

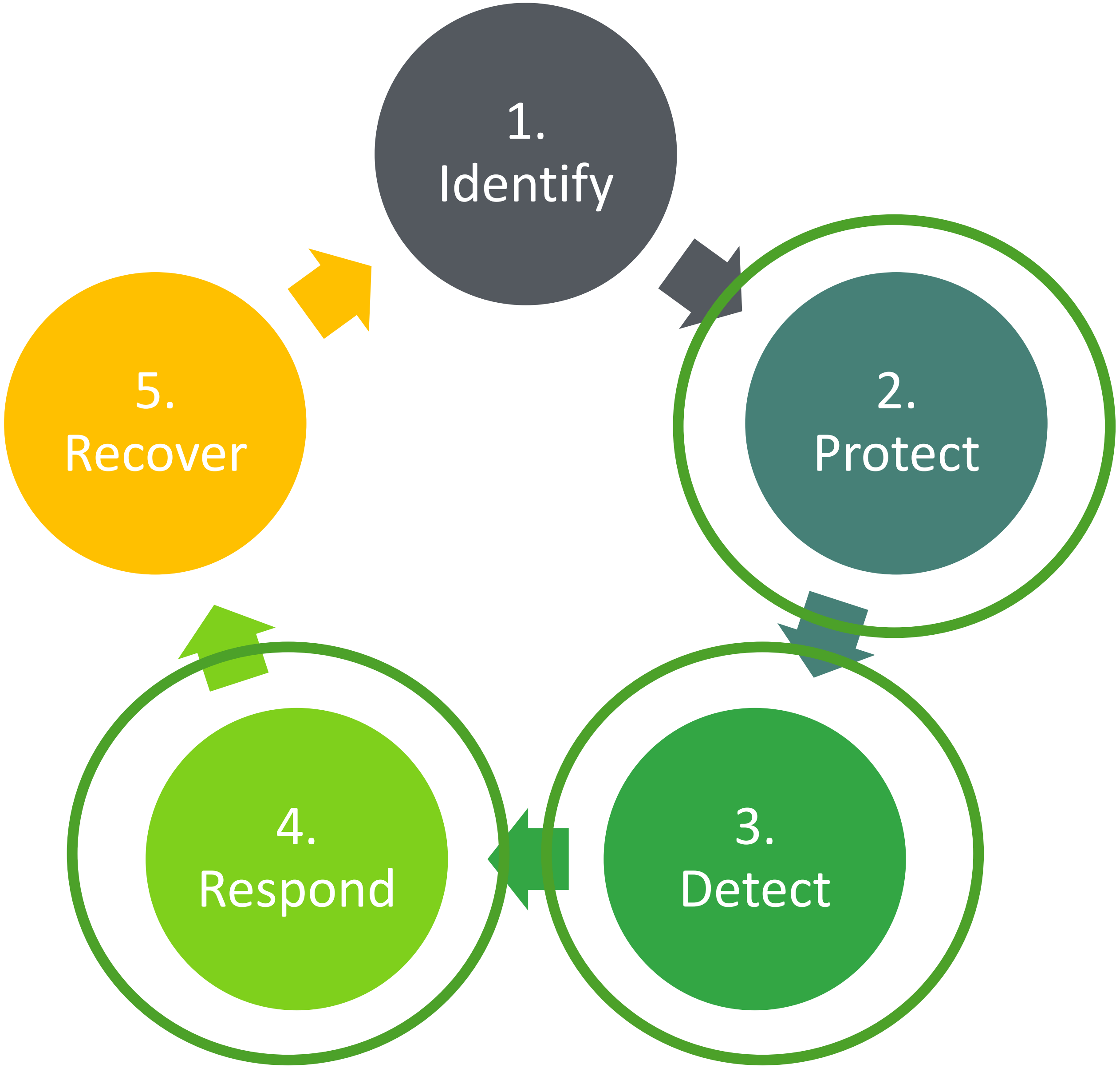


Checklist (11/11)

- ☑ Trek alle sessies per direct in ! *17/09/2024 12:50 by Koen van Burken*
- ☑ Onderzoek de melding en volg de rest van de checklist wanneer de aanmelding malafide was ! *17/09/2024 12:50 by Koen van Burken*
- ☑ Schakel het account van de gebruiker uit (let op dat in geval van aad connect je de on-premise user uitschakelt) ! *17/09/2024 12:52 by Koen van Burken*
- ☑ Reset het wachtwoord van de gebruiker ! *17/09/2024 13:40 by Kevin van de Luijtgaarden*
- ☑ Verzamel en onderzoek de Azure en M365 audit logs van de gebruiker (is er bijvoorbeeld een extra authenticator toegevoegd en/of zijn er andere zaken geopend?) ! *17/09/2024 13:54 by Kevin van de Luijtgaarden*
- ☑ Controleer de mailbox op ongewenste regels (bijv: doorsturen/verwijderen van e-mail) ! *17/09/2024 13:54 by Kevin van de Luijtgaarden*
- ☑ Probeer het originele phishing bericht veilig te stellen (inclusief mail headers) ! *17/09/2024 13:46 by Kevin van de Luijtgaarden*
- ☑ Verzamel en onderzoek e-mail logs van de gebruiker (zijn er phishing berichten uit naam van de gebruiker gestuurd) ! *17/09/2024 13:46 by Kevin van de Luijtgaarden*
- ☑ Zorg er voor dat ontvangers in het geval dat er phishing is verstuurd via de getroffen mailbox genotificeerd worden ! *17/09/2024 13:54 by Kevin van de Luijtgaarden*
- ☑ Indien er geen MFA oplossing actief is dient dit verkocht/aangezet te worden ! *17/09/2024 13:40 by Kevin van de Luijtgaarden*
- ☑ Overleg met Security specialist/CISO of er aan de hand van de verzamelde informatie verdere acties nodig zijn voor het SI gesloten kan worden ! *17/09/2024 14:27 by Koen van Burken*

Take Aways

- Summary and takeaways
- Protect | Detect | Respond



👍

Thank You