Adversary in the Middle – Notes from the field

Kenneth van Surksum & Erik Loef

DEMO 1 – Adversary in The Middle

- Login with demousera
- MFA with number matching
- Copy session cookie to new browser

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

Kopiëren naar | Beantwoorden | Allen beantwoorden | Doorsturen | In-/uitzoomen | Afdrukken | ...

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

E

Egbert van der Ven (via Dropbox)<no-reply@dropbox.com>

Aan: [redacted]

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

Afzender vertrouwen | Geblokkeer

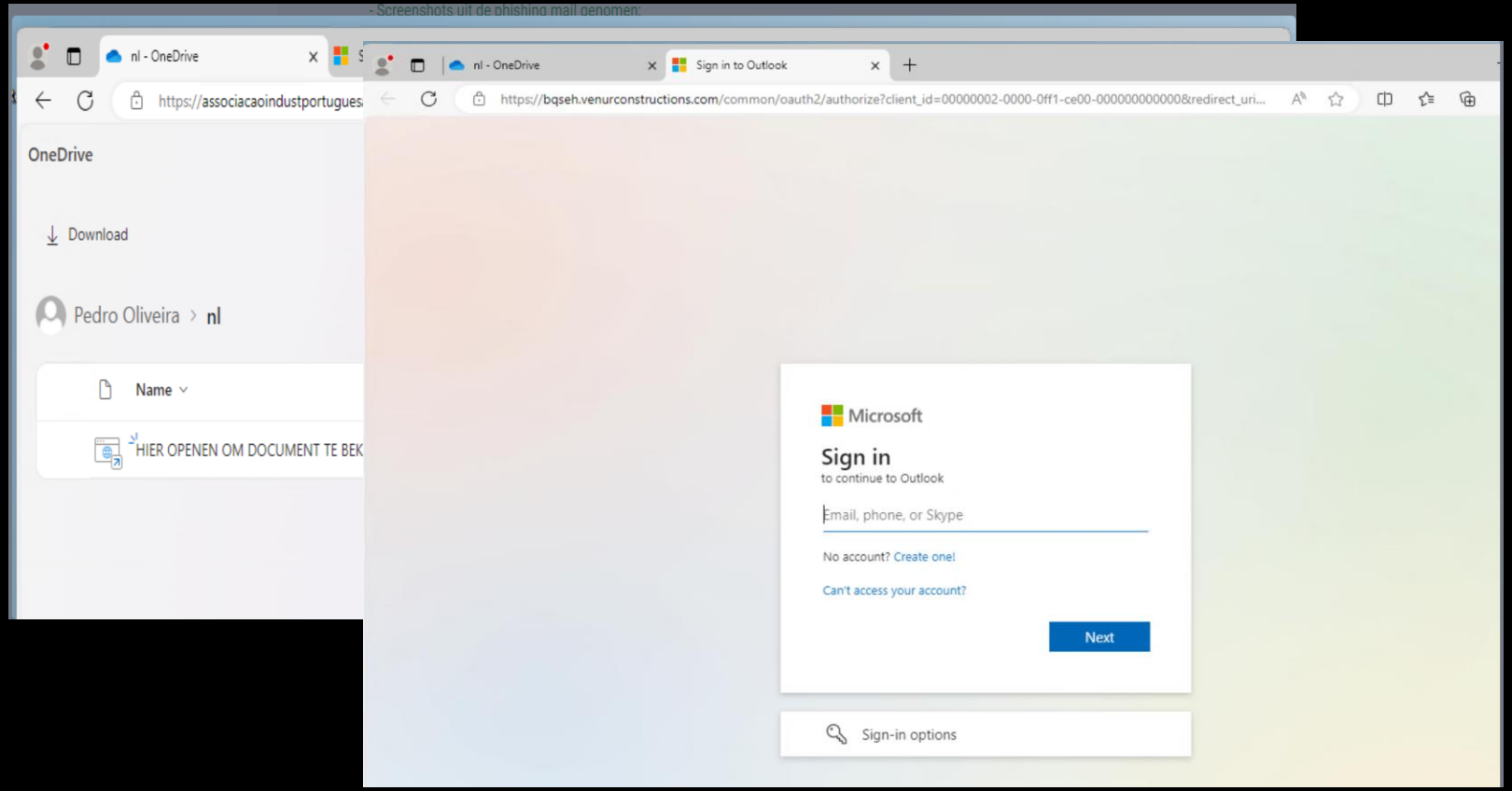
Egbert van der Ven (egbertvanderven@multical.nl) heeft je uitgenodigd om het bestand **Ingenieursbureau Multical BV Persoonlijk en vertrouwelijk - Bijlage.pdf** te bekijken in Dropbox.

Bestand openen

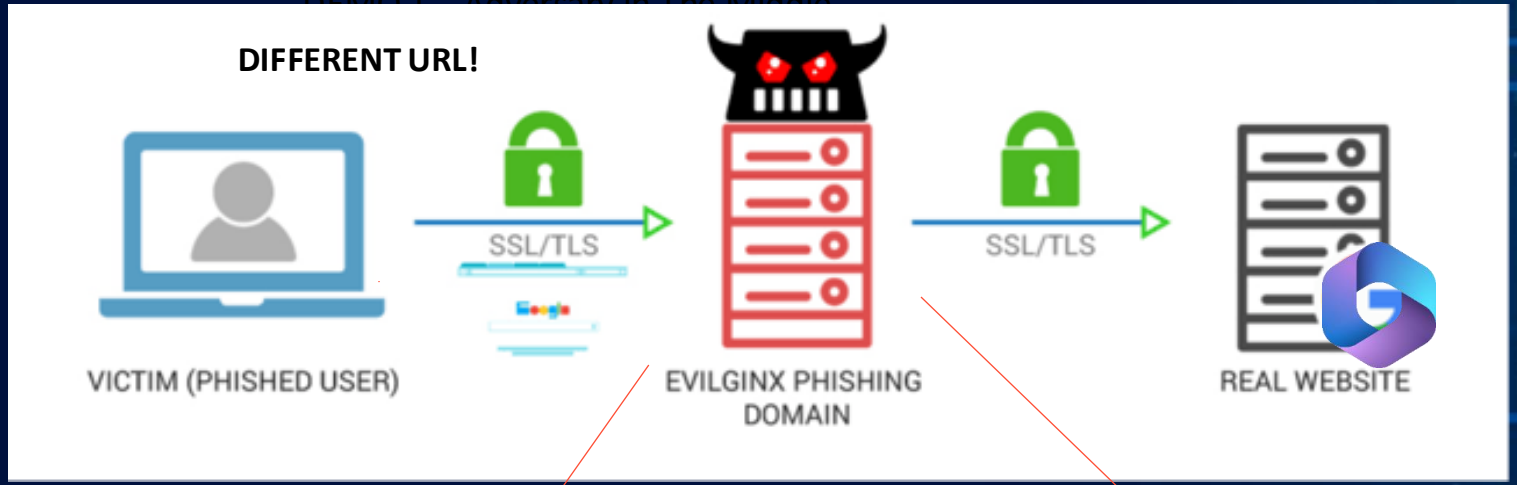
From: Bertjan
Sent on: Tuesday
To: Bertjan
Subject: Bertjan

Sommige persone

- Screenshots uit de phishing mail genomen:



Our setup



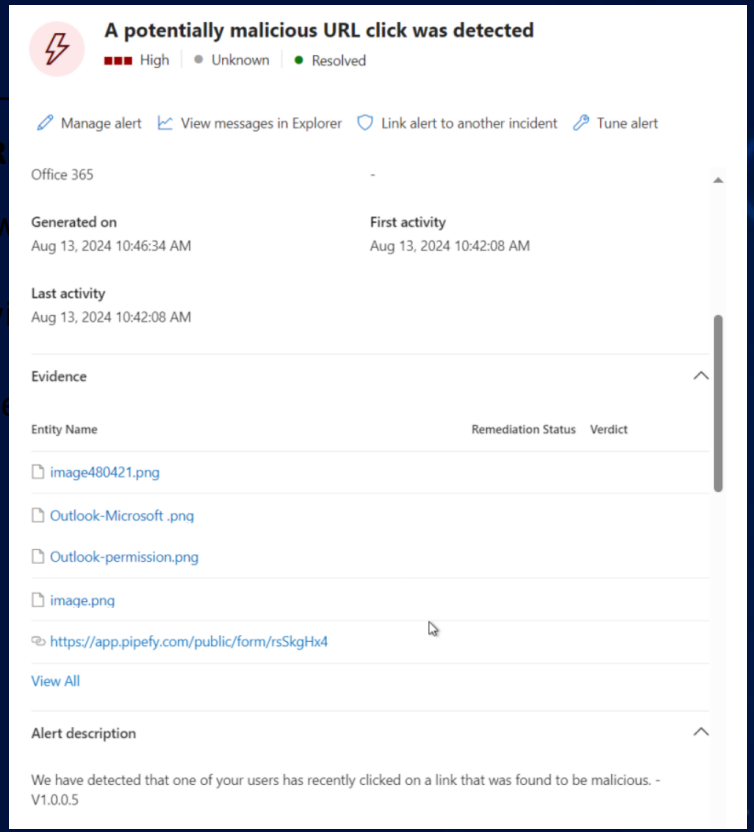
DIFFERENT DEVICE

DIFFERENT IP ADDRESS

Meanwhile @ SOC

DEMO 1 –
DIFFERENT URL

- Login w
- MFA wi
- Copy se



Real Life Example

Microsoft Sentinel 16-1 19:03

Risky User [redacted] found

Severity: Medium
Workspace: stra1-proxsys-sentinel
Description: Risky User [redacted] Risklevel hidden
Please check if the user is compromised

Alerts:

Displayname	Description
Risky User [redacted] found	Risky User [redacted] Risklevel hidden Please check if the user is compromised

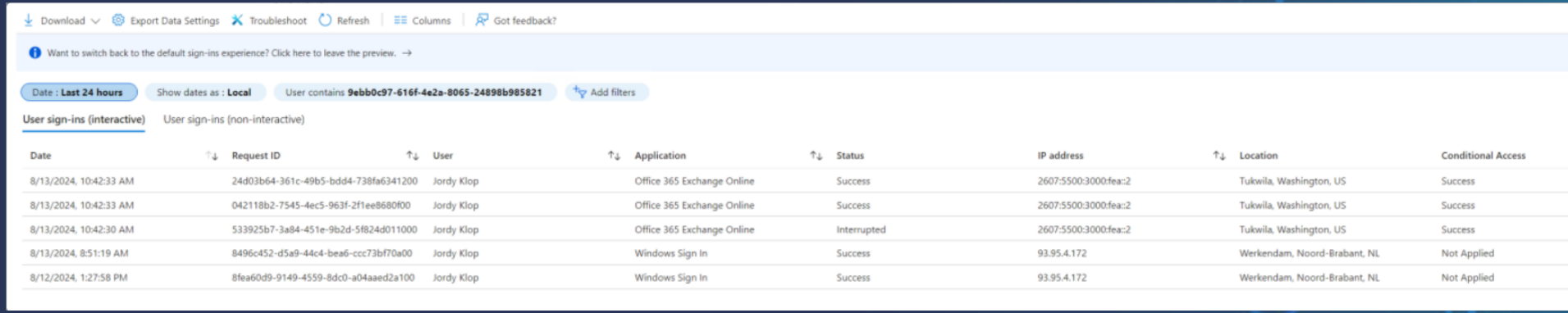
Related Entities:

Type	Entity
Account	[redacted]

Recent Example 17-01-2025

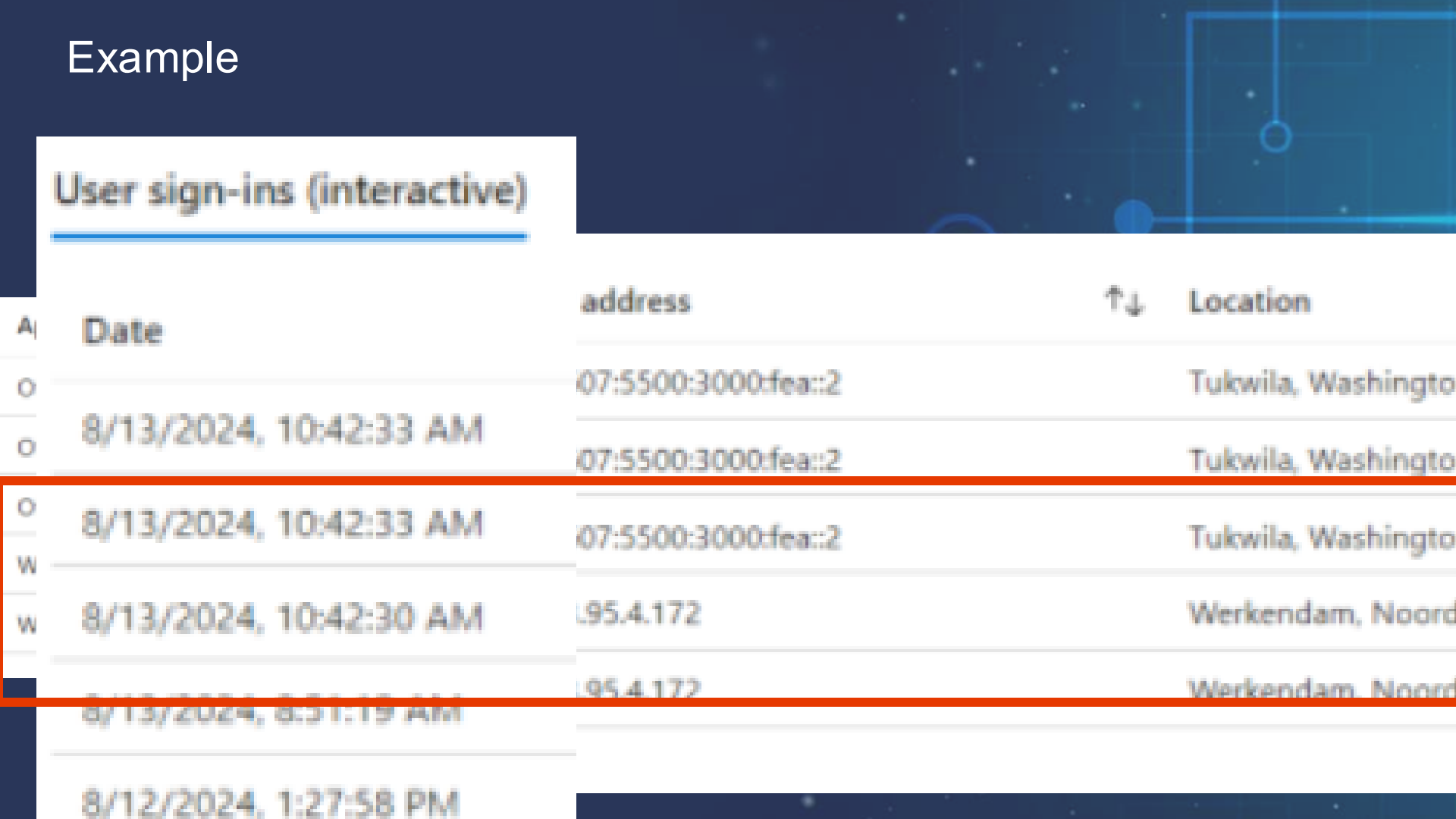
1/17/2025, 5:53:25 AM	87d8d544-ff8e-4ecd-bf79-f7ba9a4c1500	[redacted]	Office 365 Exchange Online	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:23 AM	8590fe6a-3103-4776-902a-a6f27996a000	[redacted]	Office 365 Exchange Online	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:23 AM	9dd1a0a9-d6ca-46a2-abd9-048744742d00	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:23 AM	2e4cc499-1344-45b1-8bcc-346972b11d00	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:22 AM	e3371929-d45e-44ad-9c88-6fd85aeac200	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:21 AM	9dd1a0a9-d6ca-46a2-abd9-048715742d00	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:20 AM	0a62f004-be5f-4f1a-9be1-4f9cf2869100	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:20 AM	2997ed7b-6a76-4545-8407-7089ab617600	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:18 AM	8590fe6a-3103-4776-902a-a6f23a96a000	[redacted]	OfficeHome	Failure	154.117.184.142	Auckland Park, Gauteng,
1/17/2025, 5:53:16 AM	f55d559a-378c-488e-92e6-3725e3b34d00	[redacted]	OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 7:05:11 PM	783e0a2d-6d49-40d6-adc8-a8fcf3c47c00	[redacted]	Office 365 Exchange Online	Failure	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 7:05:09 PM	fcee2140-b396-405f-bec5-a2e7951d7700	[redacted]	Office 365 Exchange Online	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 6:50:12 PM	8dc80775-cacf-49c7-8ad0-39a60cbf5100	[redacted]	Office 365 Exchange Online	Success	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 6:50:11 PM	8dc80775-cacf-49c7-8ad0-39a6f3be5100	[redacted]	Office 365 Exchange Online	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 6:49:59 PM	b1910d74-be48-4b10-ad07-8666858c7600	[redacted]	OfficeHome	Success	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 6:49:58 PM	c36179ee-3767-4f99-98f3-65dc98a78800	[redacted]	OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 6:49:12 PM	0e73393c-3909-45e1-a1ed-87339047a600	[redacted]	OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 6:49:10 PM	bad21405-f117-42dc-8f05-a50a39666c00	[redacted]	OfficeHome	Interrupted	154.117.184.142	Auckland Park, Gauteng,
1/16/2025, 1:01:33 PM	fc3c14fe-19fa-4368-bbd8-e441c3437b00	[redacted]	Windows Sign In	Success	93.95.4.19	Gorinchem, Zuid-Holland
1/16/2025, 10:54:10 AM	c9e220f6-03cc-41c3-ad7d-4d8a071a0d00	[redacted]	Office 365	Success	217.147.18.83	Moskva, Moskva, RU
1/16/2025, 10:54:08 AM	6b7e4102-e326-412a-bd01-48bd1a972500	[redacted]	Office 365	Interrupted	217.147.18.83	Moskva, Moskva, RU

Real Life Example



Date	Request ID	User	Application	Status	IP address	Location	Conditional Access
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
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
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
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
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

Example


User sign-ins (interactive)
Date
address
Location
8/13/2024, 10:42:33 AM
07:5500:3000:fea::2
Tukwila, Washingto
8/13/2024, 10:42:33 AM
07:5500:3000:fea::2
Tukwila, Washingto
8/13/2024, 10:42:33 AM
07:5500:3000:fea::2
Tukwila, Washingto
8/13/2024, 10:42:30 AM
95.4.172
Werkendam, Noord
8/12/2024, 1:27:58 PM

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

Erik Loef
@erikloef

Kenneth van Surksum
@kennethvs

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			

Phishing Resistant MFA Methods

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

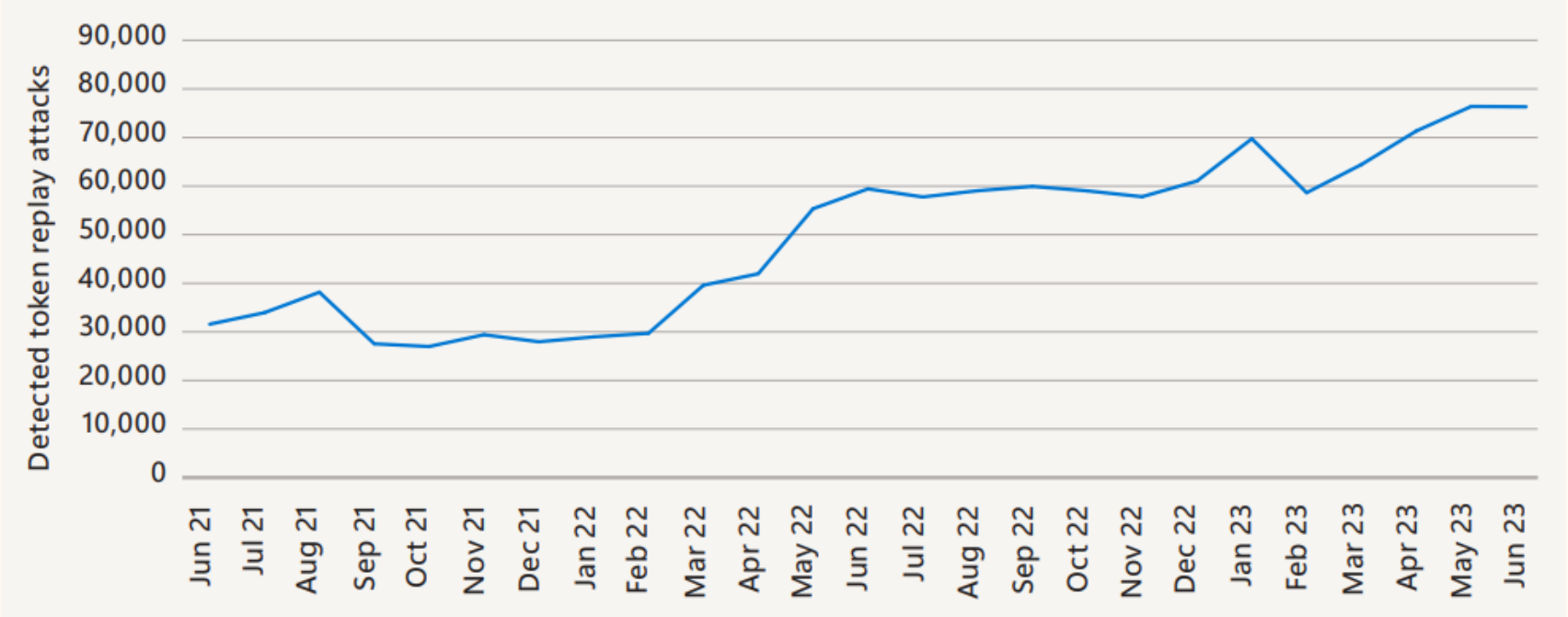
Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated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

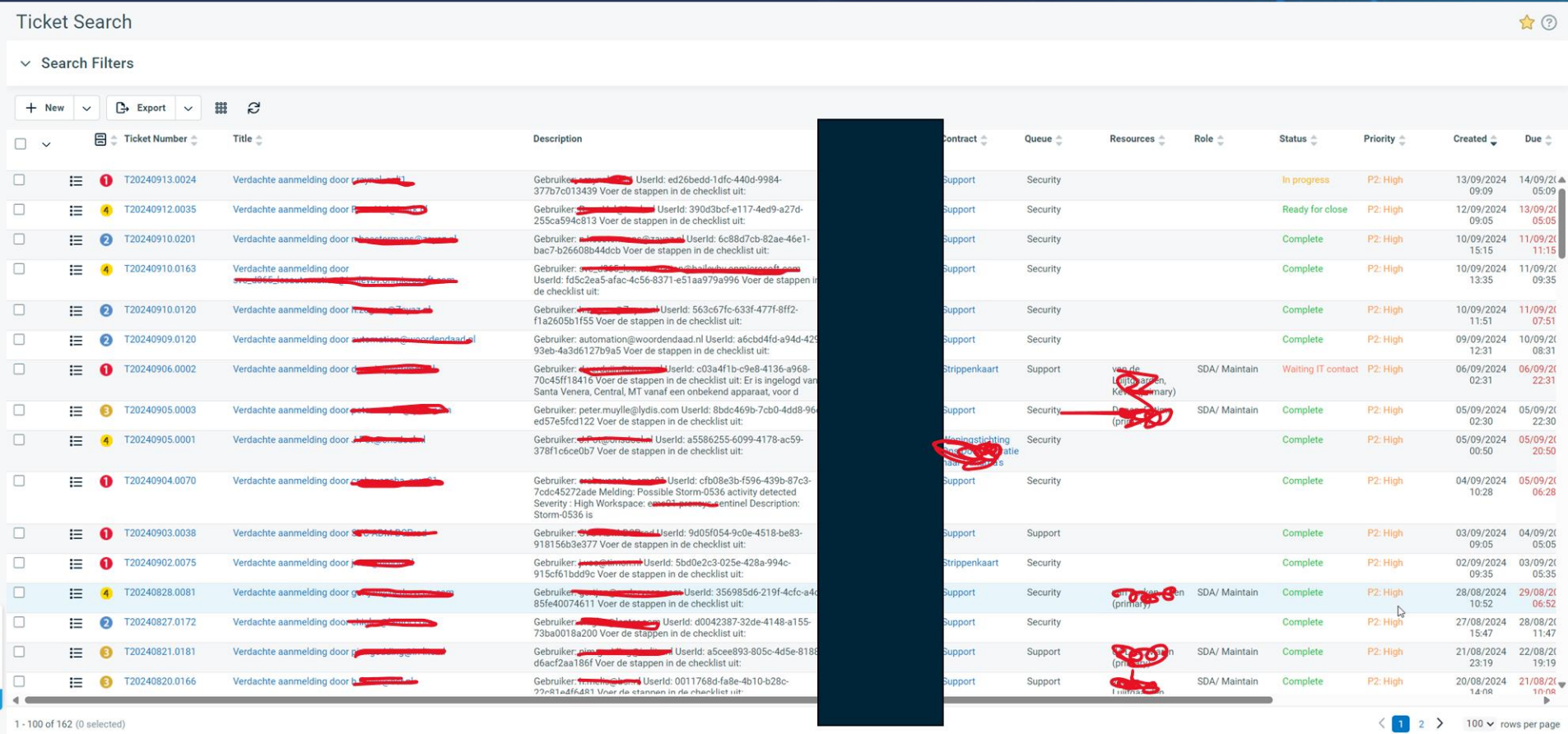
Source: Microsoft Threat Intelligence

Token replay attacks consistently growing since early 2022

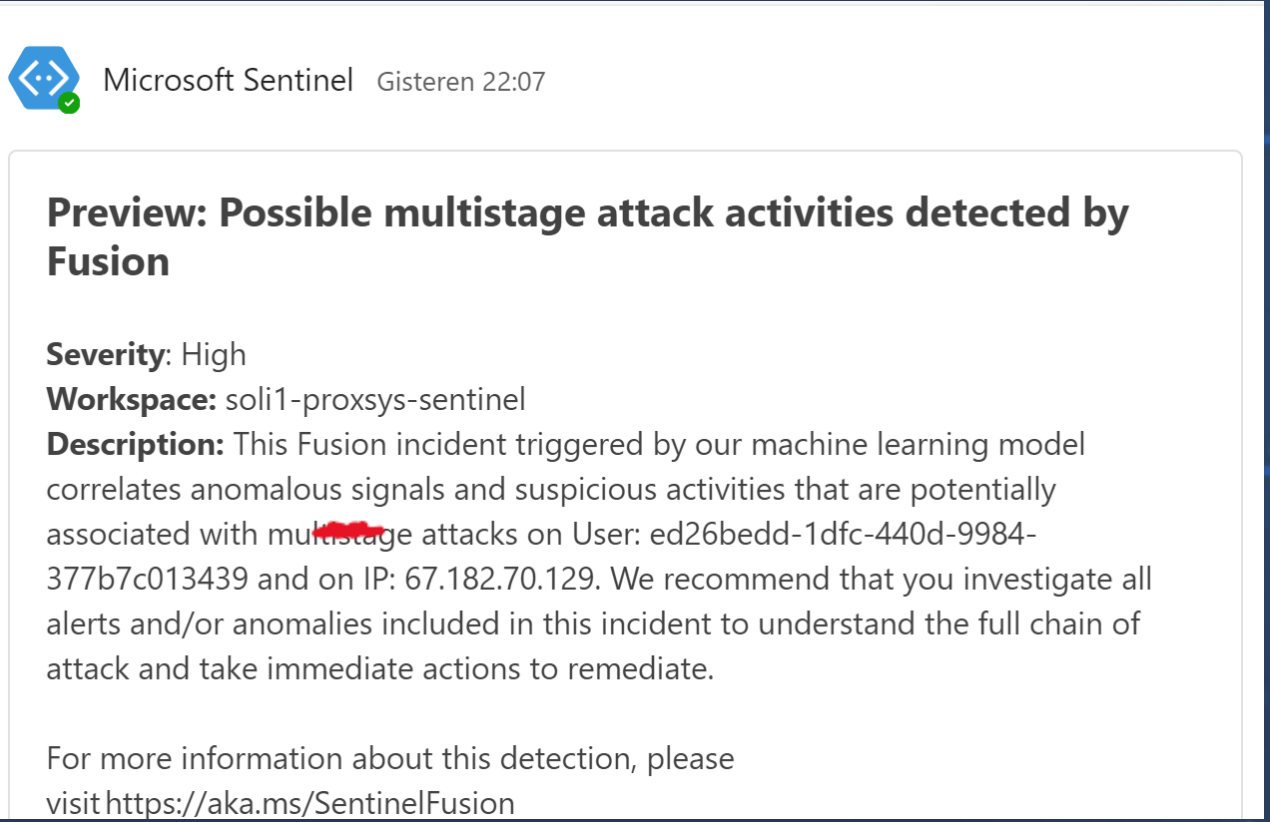


Source: Azure Active Directory Identity Protection data

Data from 2 weeks



Sentinel Fusion



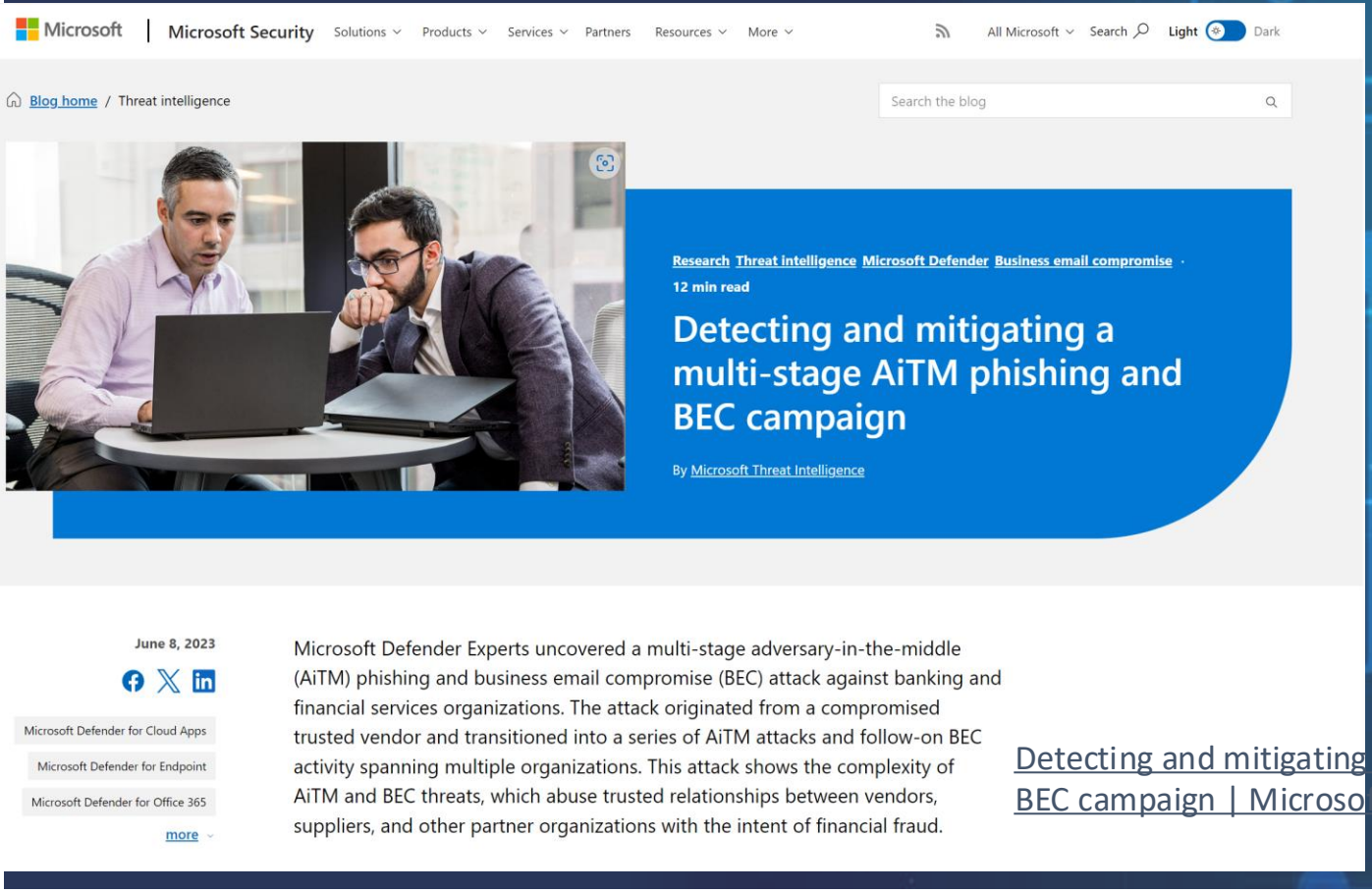
Microsoft Sentinel Gisteren 22:07

Preview: Possible multistage attack activities detected by Fusion

Severity: High
Workspace: soli1-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

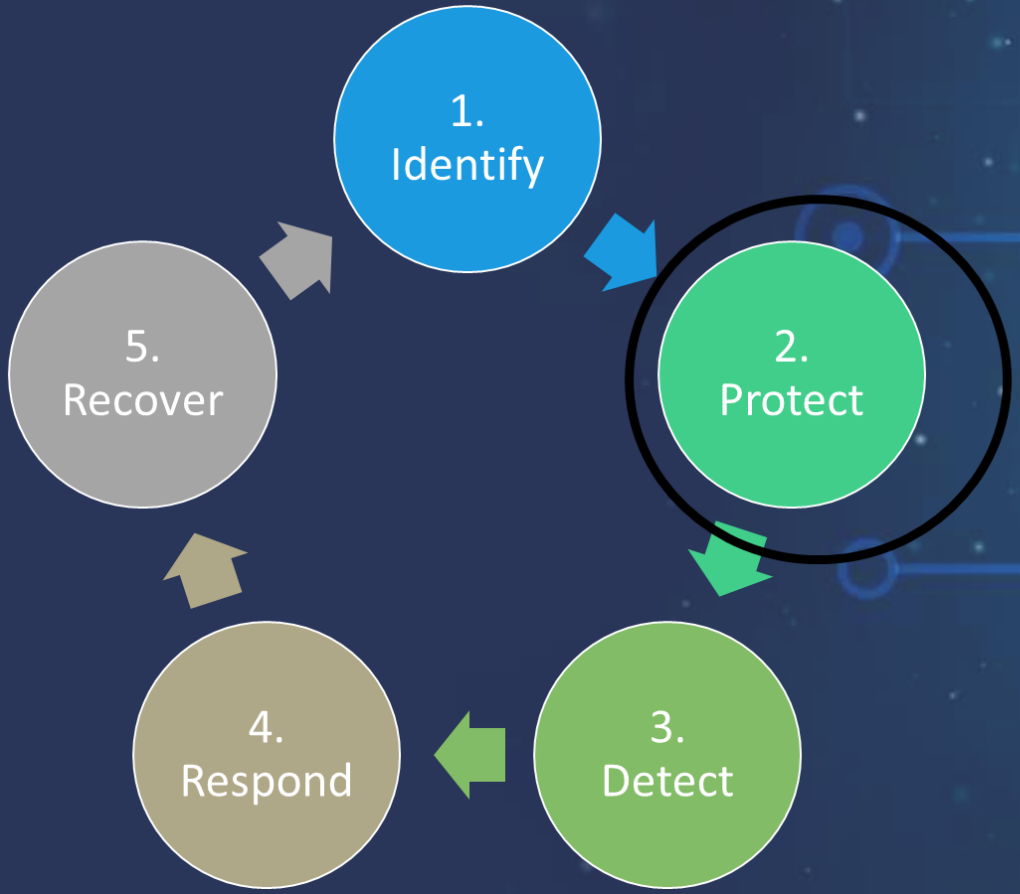
What is Microsoft advising?



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

WHAT is NCSC saying?

In het najaar van 2024 heeft het NCSC meerdere meldingen van phishing-e-mails ontvangen waarbij een Adversary-in-the-Middle-techniek (AiTM) wordt toegepast. Deze techniek is gericht op het bemachtigen van inloggegevens en sessiecookies waarmee kwaadwillenden toegang tot gebruikersaccounts verkrijgen. De verkregen toegang kan vervolgens worden misbruikt voor het verkrijgen van gevoelige bedrijfsinformatie of het uitvoeren van verdere aanvallen.


1.
Identify
2.
Protect
3.
Detect
4.
Respond
5.
Recover

Protect – phishing resistant MFA

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

Demo 2: *Adversary in the Middle*

With hardened Identity, AiTM is mitigated

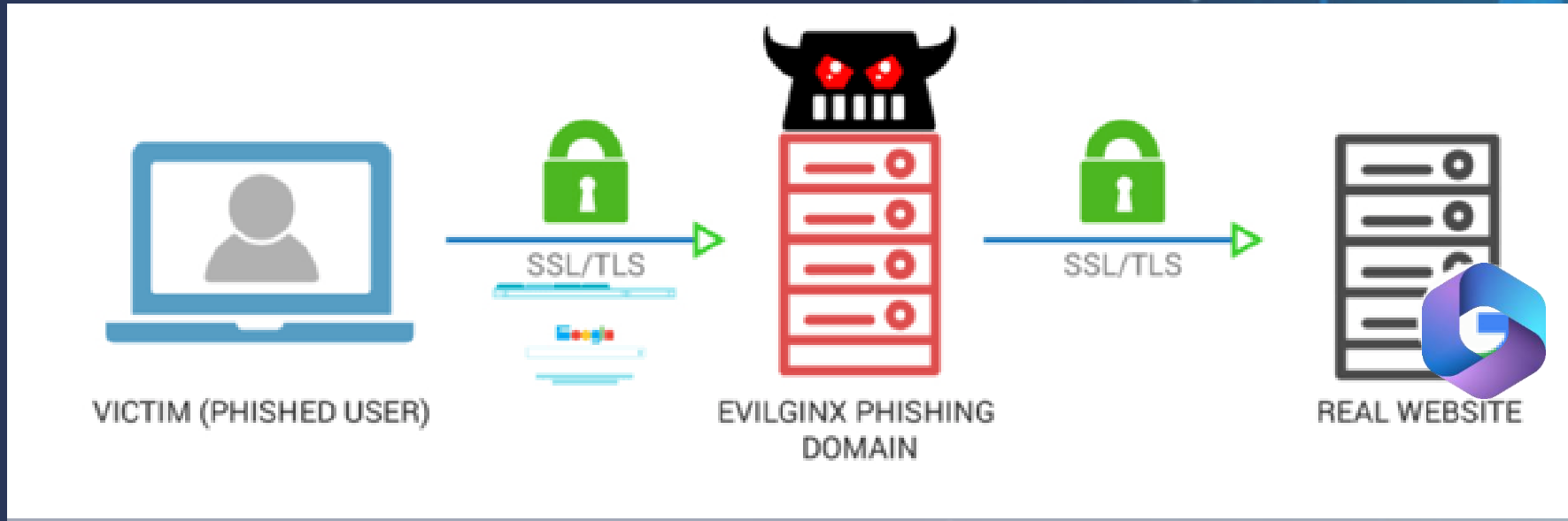
Demo with Fido Security key

Pro/Cons

- Certificate Based Authentication
  - Issue on mobile especially BYOD scenarios
- Passkeys/FIDO security key
  - Passkeys (now GA)
  - FIDO key support for mobile
  - Complex process onboarding/offboarding and lost
- Windows Hello or Business
  - Windows only
  - Platform SSO (macOS)

Protect – CA options

- Allow only managed devices
- Allow only public IPs from your country
- Use Microsoft Entra Global Secure Access (GSA)/Compliant Networks



Demo 3

Part 1:

Block and allow specific IP ranges

Part 2:

Allow only managed devices

Pro/Cons

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

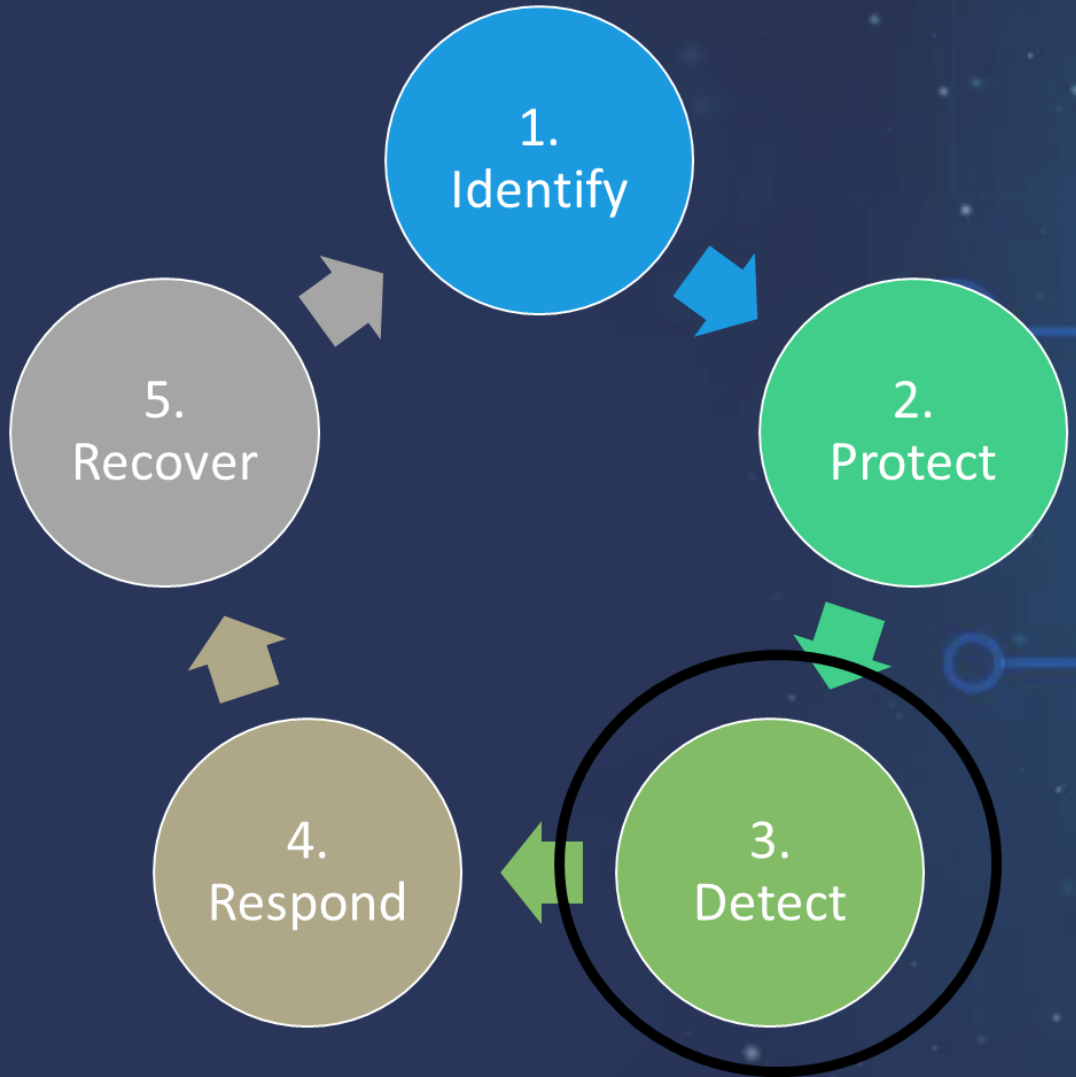
Protect – CA options with P2

- Block Risky Sign ins (Risk adaptive access)
- Token Protection
  Token protection in Microsoft Entra Conditional Access - Microsoft Entra ID | Microsoft Learn

Demo 4

Part 1:
Risky Sign in CA policy

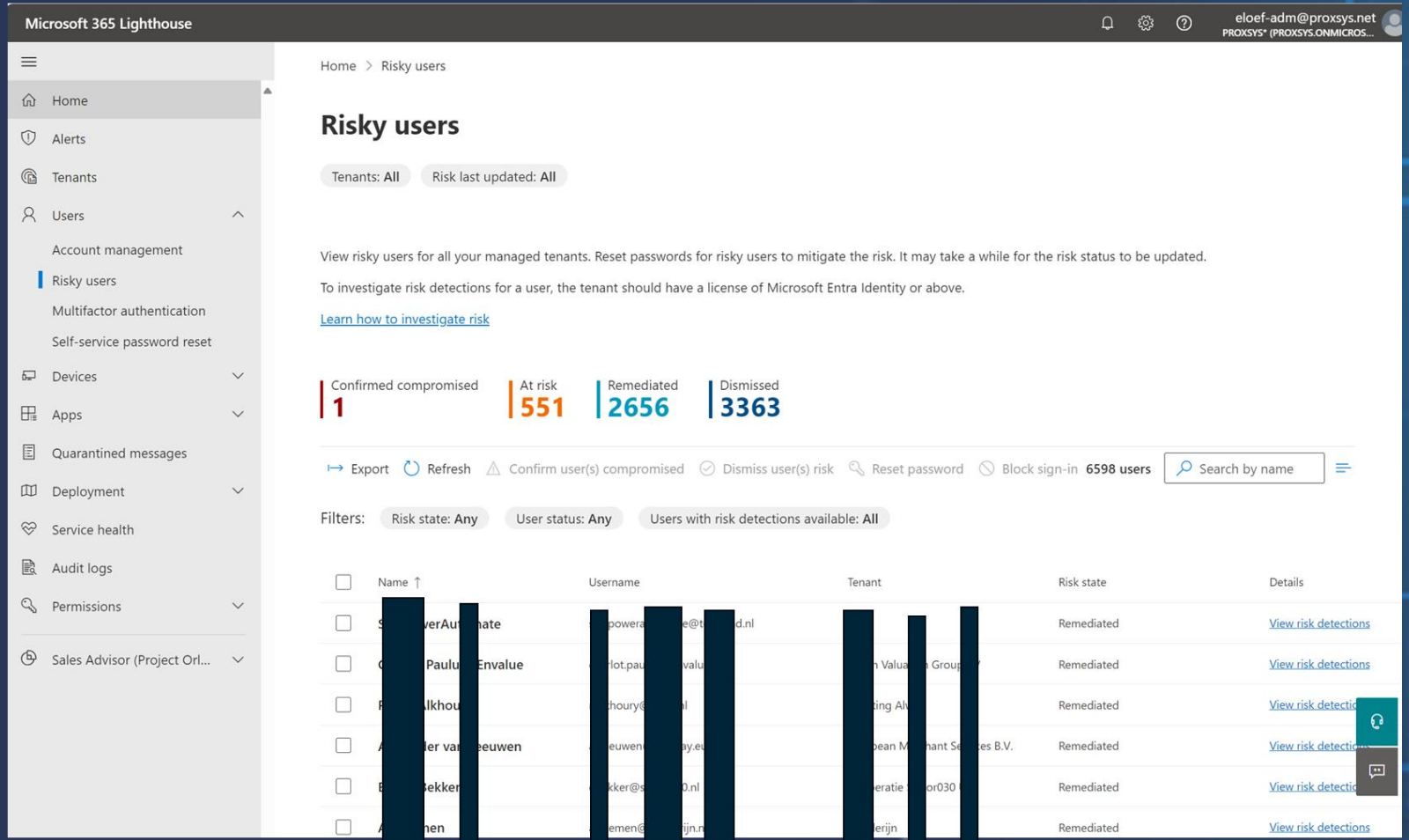
Part 2:
(new) Token Protection Policy


1.
Identify
2.
Protect
3.
Detect
4.
Respond
5.
Recover

Detect – free options

- M365 Lighthouse
- Powershell script
- Sentinel

M365 Lighthouse



Home >

Microsoft Sentinel

PROXSYS* (PROXSYS.onmicrosoft.com)

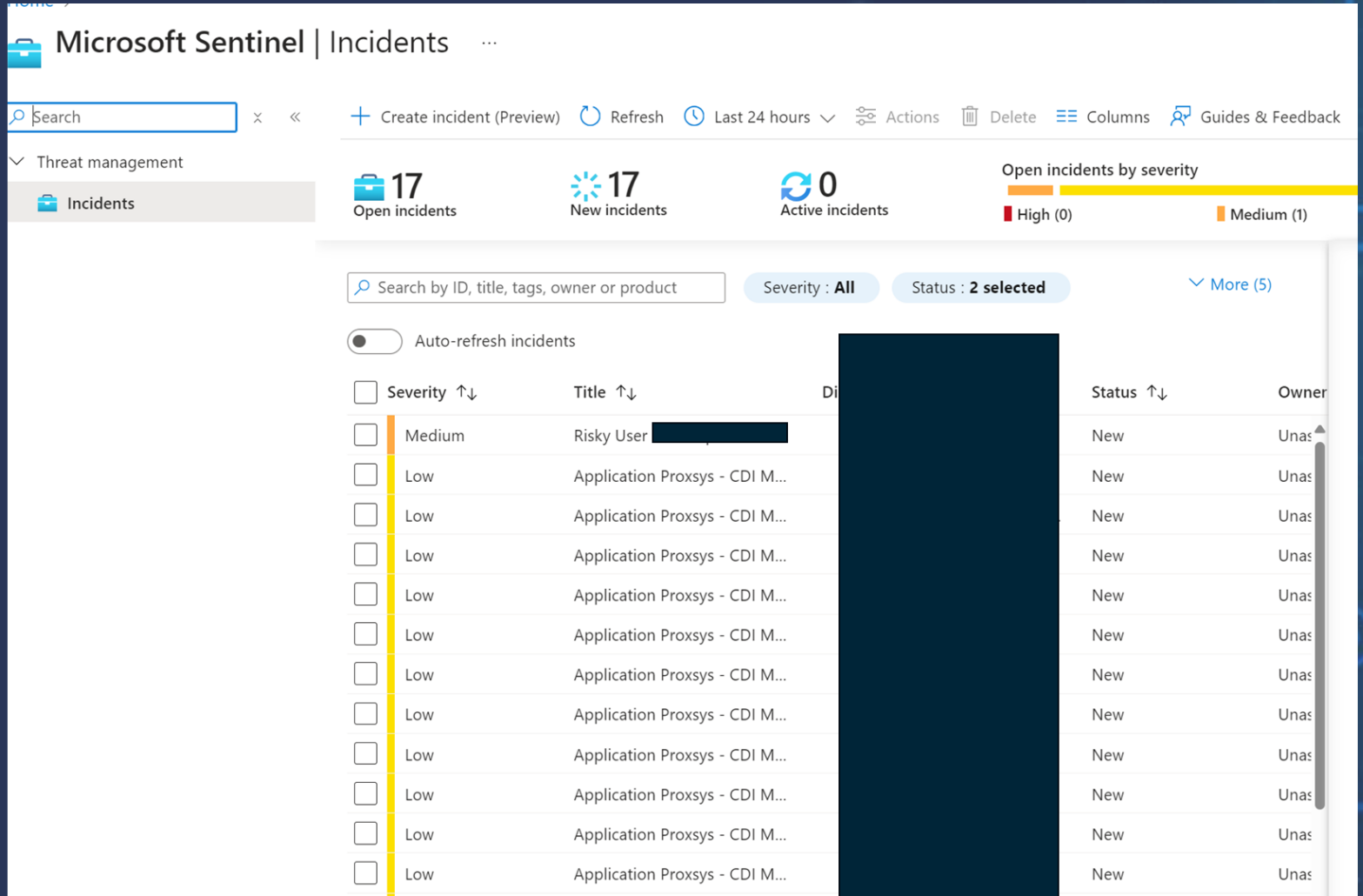
+ Create | Manage view | Refresh | Export to CSV | Open query | View incidents

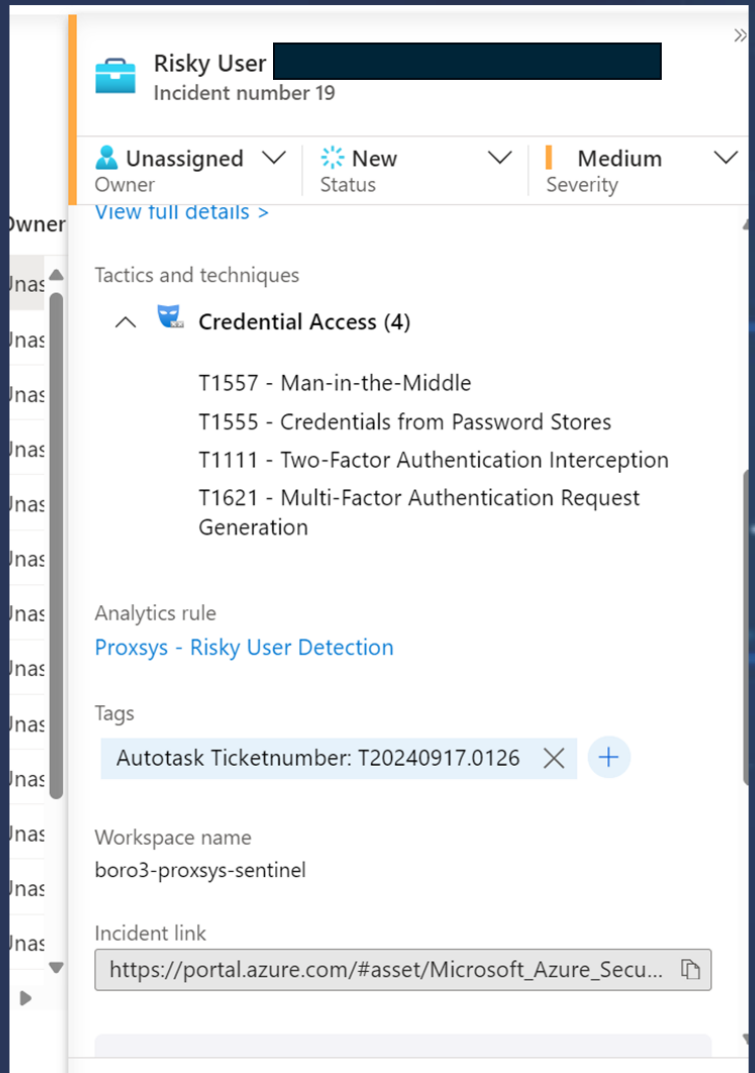
Filter for any field... | Subscription equals **16 of 98 selected** | Resource group equals **all** | Location equals **all** | Add filter

Showing 1 to 16 of 16 records.

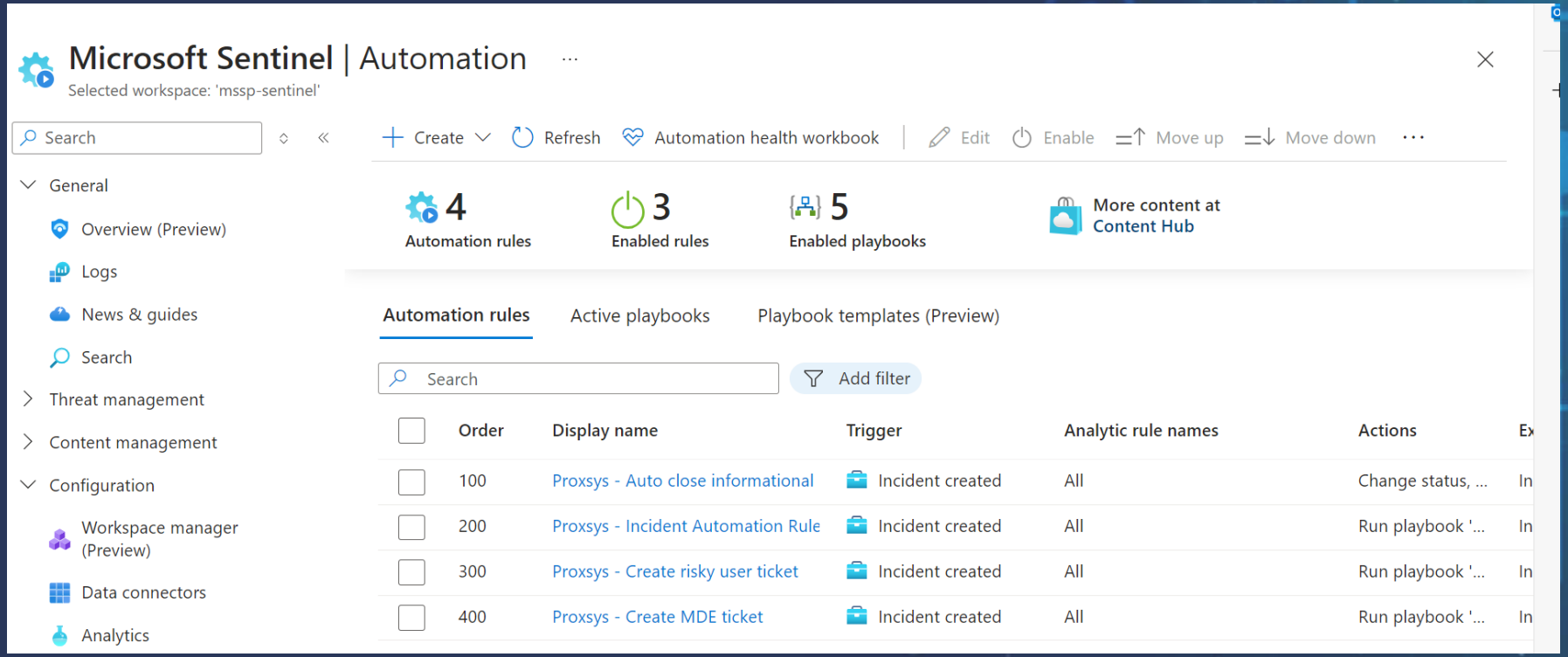
No grouping | List view

Name	Resource group	Location	Subscription	Directory
[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	4fig1 - Proxsys Sentinel Subsc	
[redacted]1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	abal1 - Proxsys Sentinel Subsc	
[redacted]1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	acco1 - Proxsys Sentinel Subs	Limborgh & ...
[redacted]r1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	amar1 - Proxsys Sentinel Subs	
[redacted]o1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	anbo1 - Proxsys Sentinel Subs	
[redacted]1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	atro1 - Proxsys Sentinel Subsc	
[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	bail1 - Proxsys Sentinel Subsc	nics bv
[redacted]o1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	beco1 - Proxsys Sentinel Subs	
[redacted]1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	bela1 - Proxsys Sentinel Subsc	Rivierenland
[redacted]h1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	bokh1 - Proxsys Sentinel Subs	hiek B.V.
[redacted]2-proxsys-sentinel	proxsys-sentinel-rg	West Europe	boro2 - Proxsys Sentinel Subs	
[redacted]3-proxsys-sentinel	proxsys-sentinel-rg	West Europe	boro3 - Proxsys Sentinel Subs	BV
[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	city1 - Proxsys Sentinel Subsc	
[redacted]-proxsys-sentinel	proxsys-sentinel-rg	West Europe	clai1 - Proxsys Sentinel Subsc	work B.V.
[redacted]1-proxsys-sentinel	proxsys-sentinel-rg	West Europe	conc1 - Proxsys Sentinel Subs	.V.
[redacted]2-proxsys-sentinel	proxsys-sentinel-rg	West Europe	inte2 - Proxsys Sentinel Subsc	

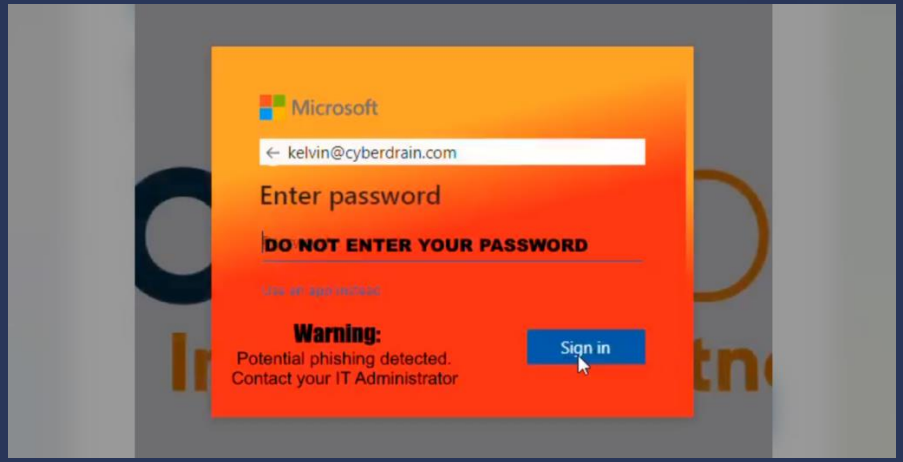

Microsoft Sentinel | Incidents
Search
Threat management
Incidents
Create incident (Preview)
Refresh
Last 24 hours
Actions
Delete
Columns
Guides & Feedback
17
Open incidents
17
New incidents
0
Active incidents
Open incidents by severity
High (0)
Medium (1)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
More (5)
Auto-refresh incidents
Severity
Title
Status
Owner
Medium
Risky User
New
Low
Application Proxsys - CDI M...
New


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



Demo 5:



Inform your users with a simple CSS Trick

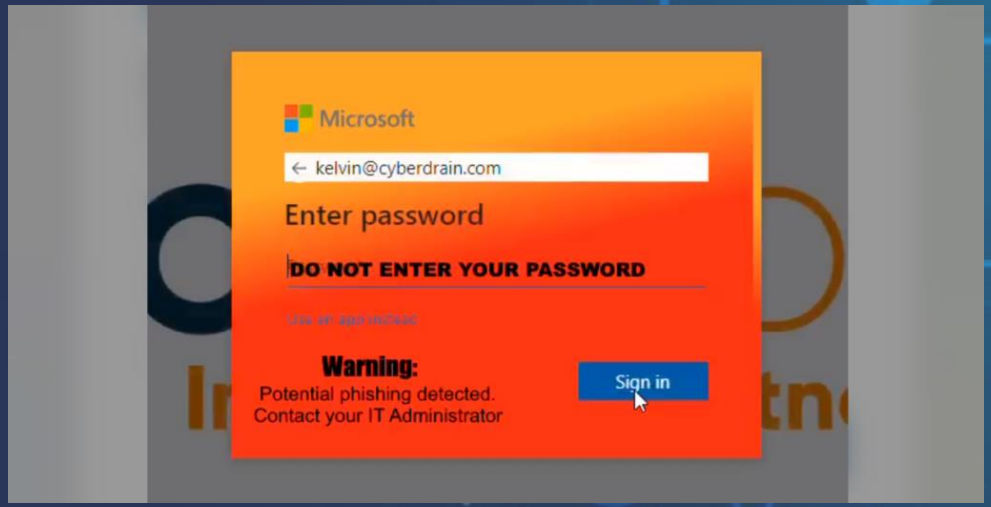
Change logi CSSs

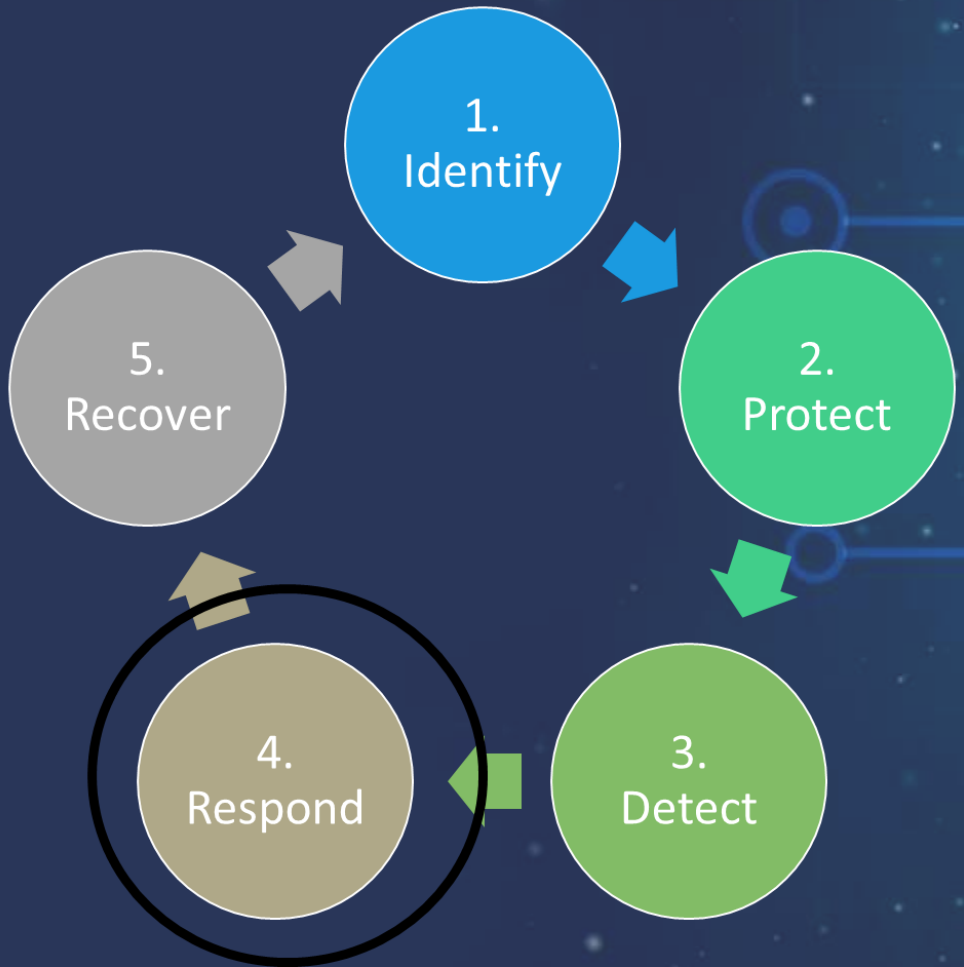
Cipp.app | zolder.io

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 !!




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

Respond

Step 1: revoke sessions

Step 2: check for logged in sessi

Step 3: disable account

Step 4: reset password

Step 5: collect all audit logs

Step 6: check for extra MFA meth

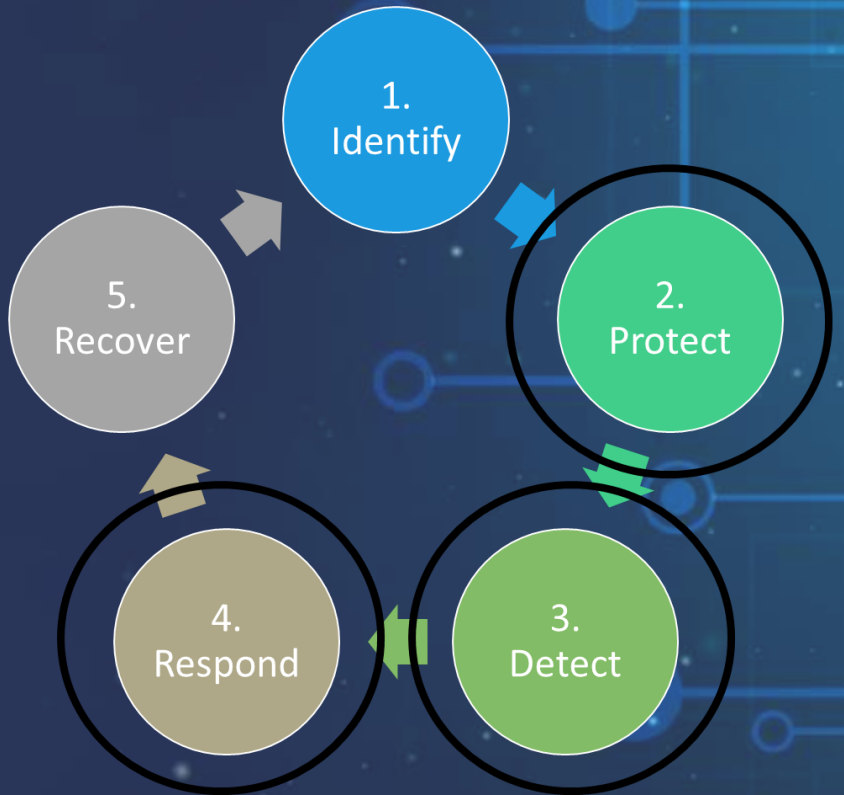
Step 7: check for mail forwards

Step 8: take the phising mail

Step 9: 4 eyes with security cons

Take Away

- Summary and takeaways
- Protect | Detect | Respond



THANK YOU