

Že štěstí přeje připraveným?



Petr Vlk

Microsoft MVP

Microsoft 365 Enterprise Security Architect @ KPCS CZ



vlk@kpcs.cz



← petr.vlk@kpcs.cz

Enter password

Password

[Forgotten my password](#)

Sign in

Permissions requested

Review for your organisation



This application is not published by Microsoft.

This app would like to:

- ✓ Read and write user mailbox settings
- ✓ Sign in and read user profile
- ✓ Send mail as a user
- ✓ Have full access to all files user can access

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

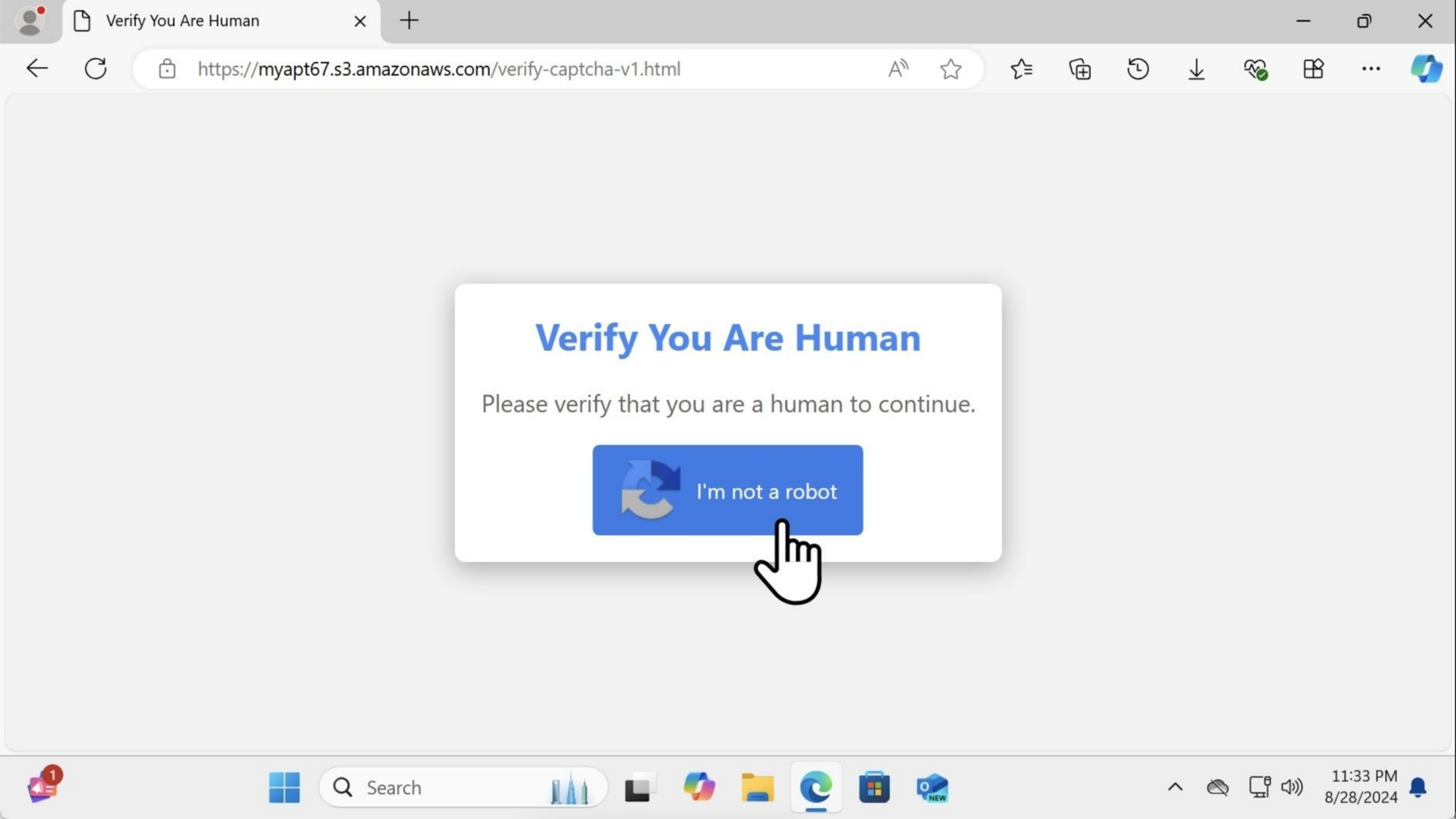


Update Microsoft Edge

Microsoft Edge is the only browser with built-in tools to help you save time and money when shopping online.

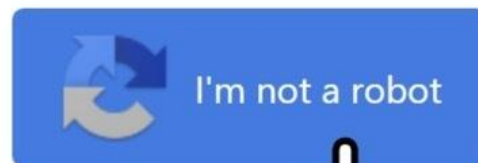
Update Microsoft Edge

1995-2021 Microsoft Edge



Verify You Are Human

Please verify that you are a human to continue.



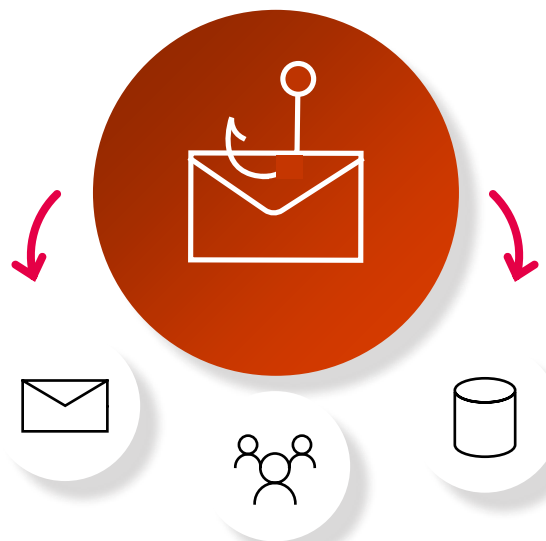
Search

11:33 PM
8/28/2024

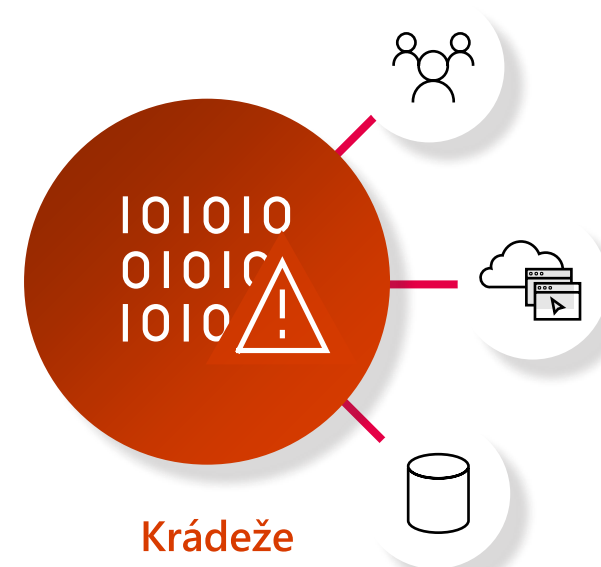
Sofistikované útoky jdou napříč doménami



Human-Operated
Ransomware



Business E-mail
Compromise (BEC)



Krádeže
dat a vydírání



E-mail



Zařízení



Identity



SaaS
aplikace



Data



Cloudová
infrastruktura



Ochrana nikdy nebyla náročnější



Narůstající frekvence, rychlost
a také sofistikovanost útoků



Nové systémy postavené
na starých základech



Vytížení IT operativou
a chybějící kompetence

Kritické zranitelnosti
se objevují každý den



Chybějící konfigurační
standards a logování



Malá adopce pokročilých
nástrojů pro obranu



Jak je vaše organizace schopna...



Detekovat a zastavit
pohyb útočníka
prostředím v reálném
čase?



Efektivně se bránit
ransomware a BEC
útokům na
zaměstnance?



Provést obnovu
systému a jeho
nastavení i dat ze
záloh?



Kontinuálně sledovat
hrozby a zranitelnosti
systémů i aplikací
v prostředí?

Plán ochrany vaší organizace



Mějte připraven Incident Response Plan

- › Adoptujte principy Zero Trust a připravte postupy pro krizové situace
- › Nasadíte zálohování systémů a dat a trénujte jejich obnovu

Doporučené technologie:

- › Microsoft Entra ID
- › Microsoft 365 Backup
- › Microsoft Azure Backup



Zvládněte základní bezpečnostní návyky

- › Zaveďte konfigurační standardy a eliminujte základní mezery v nastavení
- › Zvládněte včasné aktualizace systémů, aplikací a komponent

Doporučené technologie:

- › Microsoft Exposure Management
- › Microsoft Defender XDR
- › Microsoft Intune



Chraňte sensitivní data, identity a systémy

- › Minimalizujte prostor útočníka pro pohyb prostředím a elevaci práv
- › Klasifikujte citlivé firemní informace společně s řízením přístupu

Doporučené technologie:

- › Passwordless & Phishing Resistant MFA
- › Microsoft LAPS & PIM
- › Microsoft Purview

Nebo minimálně...

- Než jste to nasadili...
- ... útočníci už to umí obejít.

Microsoft Entra ID Protection Weekly Digest

New risky users detected

4 

New risky sign-ins detected
(in real-time)

214 

Bez MFA



Microsoft Entra ID Protection Weekly Digest

New risky users detected

0 

New risky sign-ins detected
(in real-time)

4 

S MFA



Malá případová studie

- Volají nám uživatelé...
- Do systémů se nelze přihlásit?!
- Na stanicích se objevuje ransomware výzva
- Na webovém fóru se objevuje zmínka útoku na organizaci

- Jak moc je organizace v háji?
- Zaplatit či nezaplatit?

Impact Severity	Impact Characteristics	Attack Examples
Critical	Severe disruption or complete unavailability of critical systems; significant portion of infrastructure or services are non-functional; high financial losses; lengthy recovery period (months).	Ransomware, destructive malware (e.g., NotPetya, WannaCry)
High	Major systems impacted, though not entire infrastructure; limited availability of key services; considerable financial losses; extended recovery period (weeks to months).	Targeted attack such as APT (Advanced Persistent Threat), large-scale data breach
Medium	Part of the infrastructure or specific critical systems or devices affected; limited impact on availability; shorter recovery period (days to weeks).	Malware affecting parts of the network (e.g., Emotet infecting multiple devices), server compromise, successful phishing leading to data compromise
Low	Limited-scope incident affecting only a small number of devices or users; minimal impact on availability; very rapid remediation (hours to days).	Malware on individual endpoint devices, minor password leaks
Negligible	Minimal or no real impact; incident managed within minutes or hours; no visible damage.	Short-lived DDoS attack without real impact, unsuccessful phishing

Co chybělo

- Plány, procedury, postupy
- Znalost systémů a infrastruktury, dokumentace
- Interní a externí kontakty na dodavatele
- Informace o rozsahu útoku
- Logy ze systémů
- XDR, EDR, cokoliv nad běžný AV
- A možná i ty zálohy...

Co bolí nejvíce

- Nevíme, kde útočník byl...
 - Musíme to postavit znovu?
- Nevíme, co si útočník vzal...
 - Čím nás bude vydírat?
- Nevíme, co na to zákazníci...
 - Jak moc to ovlivní finance a reputaci?
- Nevíme, jak funkční zálohy jsou...
 - Bude firma příští měsíc existovat, aby zaplatila faktury?

Jak tedy reagovat, VOL.1

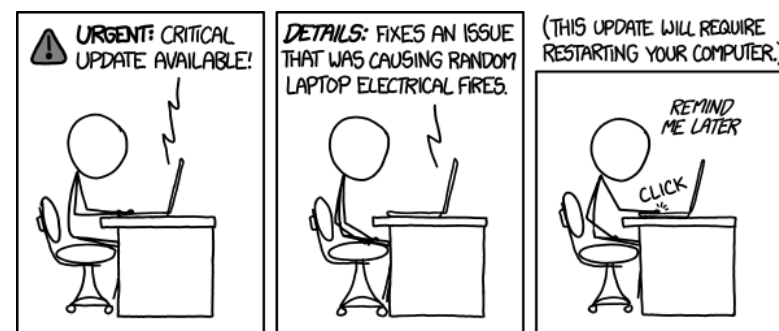
- Incident Response Plan
 - Incident Manager, CSIRT/IRT
 - Zapojení vedení organizace a jejich podpora
- Izolace systémů
 - Odpojení od sítě a internetu
 - Blokace účtů v systémech
 - Zachování forenzních stop
- Analýza a evidence
 - Logy, obrazy disků, časová osa
 - Dotčené systémy, ovlivněná data
- Zaléčení prostředí
 - Obnova záloha, změny hesel, aplikace aktualizací, odstranění zranitelností, ...

Jak tedy reagovat, VOL.2

- Obnova chodu firmy
 - Obnovení systémů a dat ze zálohy
 - Integrita služeb a monitoring změn
- Ohlášení incidentu
 - NÚKIB
 - Policie
 - ÚOOÚ
- Upřímná komunikace
 - Vedení, zaměstnanci, zákazníci, pravidelné aktualizace
- Poučení se
 - Změny nastavení, aktualizace systémů, komplexnější zálohy, lepší plány, znalosti...

Akce a reakce, nebo spíše prevence?

- Zlepšování konfiguračního standardu a modernizace systémů
- Včasné odstranění zranitelností, pravidelné aktualizace
- Nasazení dnes již standardních mechanismů a nástrojů
 - Heslo -> MFA > Passkeys, GPO -> MDM, AV -> EDR -> XDR, SIEM -> SOC
- Zálohování systémů, konfigurace i samotných dat, 3-2-1
- Definice IRP a jeho pravidelné cvičení
- Analýza rizik a prioritizace investic
- Pojištění kybernetických rizik
- Nestavějte nástroj bez lidí (byť externích)



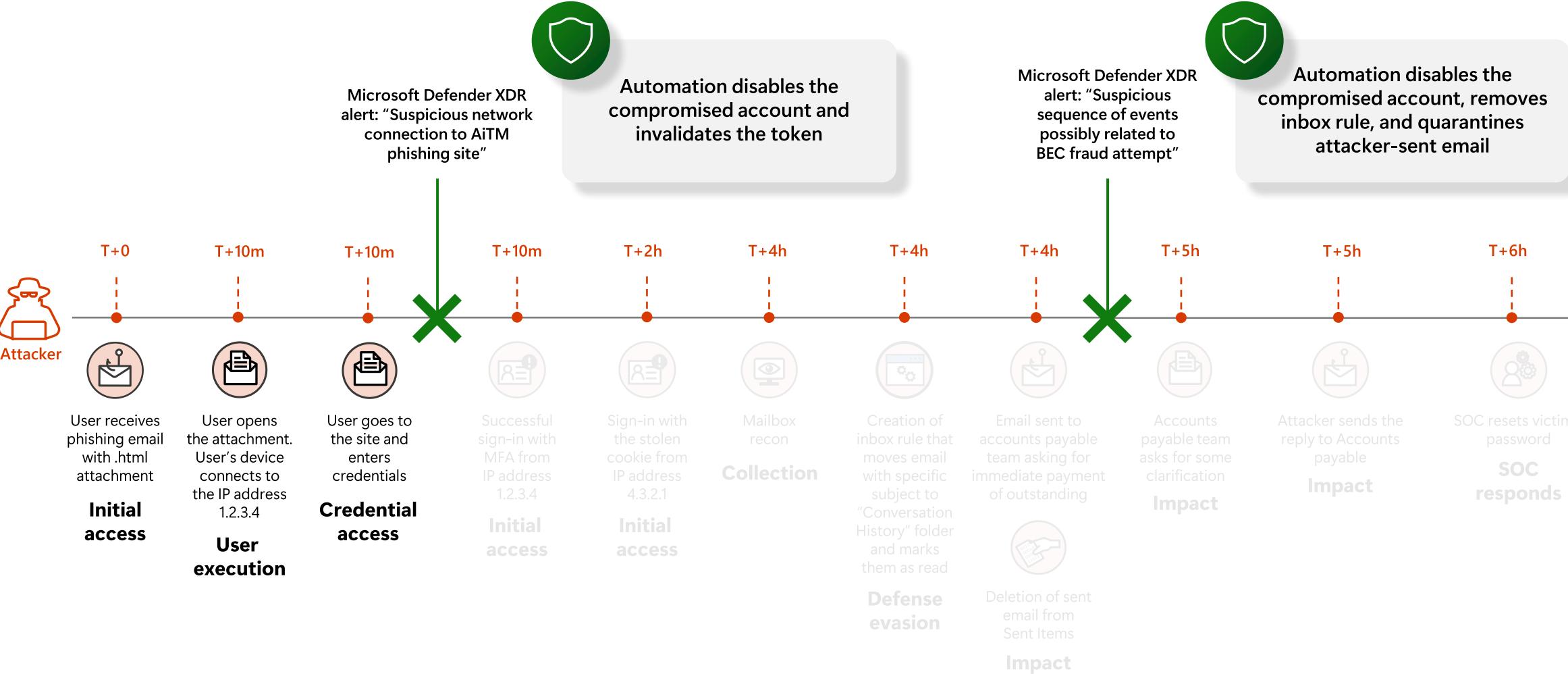
Logování aneb auditní stopa

- Přemýšlejte o otázkách, které můžete mít v případě řešení incidentu...
 - Kde budu hledat jaké informace a údaje?
 - Jak dlouho sahá historie mých logů?
 - Mám jistotu, že auditní stopa bude úplná a co obsahuje?
 - Kdo se přihlásil? Z jaké IP adresy, zařízení?
 - Které údaje využil pro přihlášení? Heslo, token, tiket?
 - Kdy se útočník nebo uživatel přihlásil a k jakým systémům?
 - Které dokumenty byly modifikovány, staženy, smazány?
 - Odkud se útočník přihlásil a jak získal přístup?
 - Jakou webovou stránku uživatel navštívil?
 - S jakými IP adresami komunikovaly které procesy a jak moc?
 - Kterou aplikaci či zranitelnost mohl útočník využít?

Pravidla pro podmíněný přístup

- Využívejte Conditional Access v Entra ID pro:
 - Administrátory a privilegové účty
 - Službám Microsoft 365
 - Ke vzdálenému přístupu (VPN)
 - Enterprise aplikacím registrovaným v Entra ID
 - Prostě ideálně ke všemu
- Adoptujte Phishing Resistant metody ověřování
 - Passkeys, Windows Hello for Business, Platform SSO
- Kontrolujte autentizační síly a frekvence přihlášení i oprávnění pro přístup a také PIM
- Vynucujte přístup ze spravovaných zařízení
 - MDM, MAM (i pro Windows v Microsoft Edge), Windows 365, AVD
 - Využijte standardní šablony pro výchozí a bezpečné nastavení systému (MSFT, CIS, STIG...)
 - Nastavte kontroly souladu (AV, EDR, verze, šifrování, detekce, ...) s rozumnou validitou
- Sledujte a řešte identifikované riziková přihlášení a identity

Adversary-in-the-Middle (AiTM)



Attack using AiTM phishing (attack disru...

Copilot ...

High | Active | Mimik Emails - AlpineSkiHouse | Ransomware Critical asset Credential Phish AiTM attack Attack Disruption +5

Important! Attack disruption has automatically taken multiple response actions. For more details, go to the [Action center](#).

Attack story Alerts (15) Assets (9) Investigations (5) Evidence and Response (29)

Alerts Incidents

Play attack story Unpin all Show all

- 3 Oct 2024 13:37 Resolved Activity from a Tor IP address Megan Bower Microsoft 365
- 3 Oct 2024 13:37 Resolved Suspicious inbox forwarding rule Megan Bower
- 3 Oct 2024 13:37 Resolved User accessed a link in an email subsequently quarantined by ZAP Megan Bower
- 3 Oct 2024 13:39 Resolved Malicious Url detected in Proxy logs 2 Devices
- 3 Oct 2024 13:44 Resolved Suspicious URL clicked vnevado-win11h.vnevado.alpineskihouse.co Megan Bower
- 3 Oct 2024 13:46 Resolved Anonymous IP address Megan Bower

RECOMMENDATIONS

Phishing Incident response playbook

View phishing investigation and response recommended steps for this incident

Open phishing playbook

RECOMMENDATIONS

Ransomware Incident response playbook

View ransomware investigation and response recommended steps for this incident

Open ransomware playbook

RELATED THREATS

Technique Profile: Cloud identity abuse (Threat Overview)

21 impacted assets

View threat analytics report

Incident summary

24 Oct 2024 18:03

The high severity incident "Attack using AiTM phishing (attack disruption)" occurred between 2024-10-03 12:37:44 UTC and 2024-10-03 13:07:23 UTC. It was tagged as Adversary in the Middle, Attack Disruption, Credential Phish, and Ransomware, and triggered an automatic Attack Disruption action. This incident impacted user 'meganb' and devices 'vnevado-win11h' and 'vnevado-dc'.

Collection: The incident began at 2024-10-03 12:37:44 UTC when a suspicious inbox

See more

AI-generated content may be incorrect. Check it for accuracy.

Guided response

24 Oct 2024 18:16

Completed recommendations 2/14

Status: All

Triage

Completed

Classify this incident

24 Oct 2024 18:04

AI-generated content may be incorrect. Check it for accuracy.

Containment

Completed

Disable the account Megan Bower

24 Oct 2024 18:04

- ☰
- 🏠 Home
- 🛡️ Investigation & response
- Incidents & Alerts
- Hunting
- Actions & submissions
- Partner catalog
- 🛡️ Microsoft Sentinel
- Search
- Threat management
- Content management
- Configuration
- 🌐 Threat intelligence
- 📁 Assets
- 🖥️ Endpoints
- ✉️ Email & collaboration
- ☁️ Cloud apps
- 🛠️ Optimize
- 📄 Reports
- 🎓 Learning hub
- 🧑 Trials

📖 Guided Tour

⚙️ Customize page

Unified incidents and alerts

145 active incidents

Service sources: Defender XDR, Sentinel, Defender for Cloud, Endpoint, Office, and Applications

In progress

24

Resolved

57

Active incidents by severity

High

Medium

Low

Informational

Closed incidents by classification

True positive

False positive

Benign positive

Undetermined

Closed incidents and alerts over time

Incidents

Alerts

View all incidents

Sentinel automation

33 automation rules

Closed incidents

6

Time saved

23 hours

Actions performed

259

Actions performed by type

Severity

Owner

Status

Comments

Configure automation rules

View workbook

Entities from Sentinel

Discovered entities related to incidents

12.3K Hosts

11.8K IPs

1.6k Azure resources

View all entities

Sentinel data connectors

48 data connectors

Active connectors

34/48

Unhealthy connectors

12/48

SOC optimization

Your optimized data

Active

7

Completed

2

Dismissed

2

Secure score

Secure Score: 50.91%

707.09/1389 points achieved

Microsoft Secure Score is a representation of your organizations's security posture, and your opportunity to improve it.

Featured Threat intelligence articles

Storm-0062 attempts to exploit CVE 2023-22515 in Atlassian Confluence

Storm-0062

1 day ago | 5 indicators

Diamond Sleet compromises TeamCity servers

Diamond Sleet

T1584-Compromise infrastru...

+2

6 day ago | 15 indicators

WS FTP Server critical vulnerabilities

T1190 - Exploit Public-Facin...

7 days ago | no indicators

Threat overview: Exfiltration

TA0010 - Exfiltration

9 days ago | no indicators

See more in Intel explorer

What's new

Using advanced

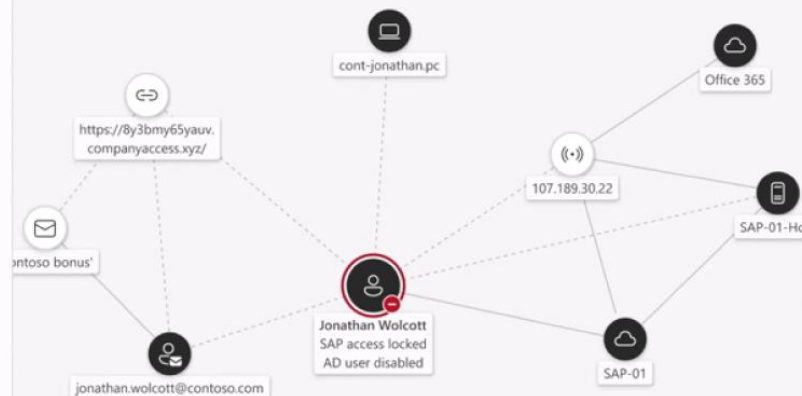
3,315

SAP financial process manipulation attack disrupted

 Copilot Manage incident Activity log ...

Alerts <  Layout  Group by

Nov 15, 2023 4:45 AM | Active
SAP - Multiple Files Download



Incident details

Incident ID	2356358
Assigned to	Unassigned
Classification	BEC financial fraud multi-stage attack
Categories	Credential access, Initial access, Persistence, Discovery, Collection, Impact
First activity	Nov 15, 2023 2:41 AM
Last activity	Nov 15, 2023 6:48 AM

Impacted assets

Devices	Risk score
cont-jonathan.pc	High
SAP-01-Host	High

Users	Investigation priority
Jonathan Wolcott	High

Mailboxes
jonathan.wolcott@contoso.com

Applications
 ☁ SAP-01
 ☁ Office 365

credentials the attacker signed in from IP 107.189.30.22 to the organization's SAP application...

Nov 15, 2023 6:48 AM

All (7) Unfinished

Triage

● Completed

Classified as 'BEC financial fraud multi-stage attack'

- New

Contact the user jonathan.wolcott@microsoft.com on Teams, and ask them to confirm their activity

Dear Jonathan Wolcott, we have identified suspicious activities for your account on Nov 15, which we would like to verify with you.

- At 2:45am, suspicious logon attempts were identified for your account to the organizational SAP application, initiating from an uncommon lo...

[See more](#)

 **Contact user in Teams** [view user](#)

AI generated. Verify for accuracy.

Contain

● Completed

User 'Jonathan Wolcott' was suspended by automatic attack disruption

Incidents > SAP financial process manipulation attack disrupted

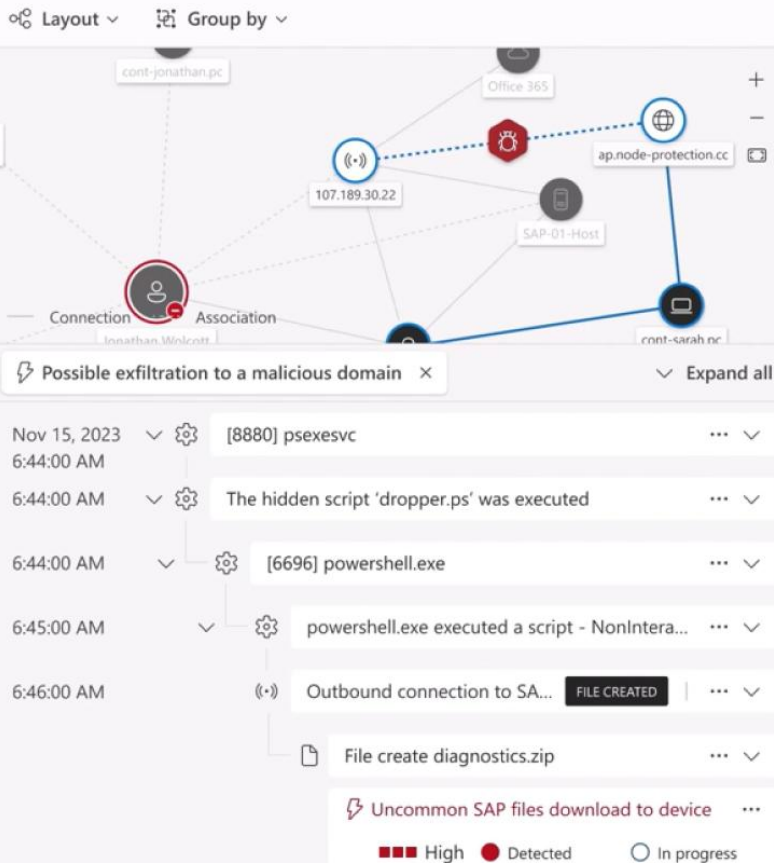
SAP financial process manipulation attack disrupted

High Active Attack disruption SAP fraud BEC fraud Chain event detection

Attack story Alerts (13) Assets (7) Evidence & Response (4)

Alerts

- Jonathan Wolcott SAP-U1 SAP-U1-Host
Nov 15, 2023 4:45 AM | Resolved
SAP - Multiple Files Download
Jonathan Wolcott
- Nov 15, 2023 5:47 AM | Resolved
Suspicious user attempted to modify SAP financial info
Jonathan Wolcott SAP-01 SAP-01-Host
- Nov 15, 2023 4:48 AM | Resolved
SAP fraud attack
Jonathan Wolcott SAP-01 SAP-01-Host
Attack disruption
- Nov 15, 2023 6:16 AM | Resolved
Suspicious inbox manipulation rule
jonathan.wolcott@contoso.com
- Nov 15, 2023 6:17 AM | Resolved
BEC financial fraud
Jonathan Wolcott
Attack disruption
- Nov 15, 2023 6:46 AM | Resolved
Possible exfiltration to a malicious domain
cont-sarah.pc
- Nov 15, 2023 6:48 AM | Resolved



Information

Possible exfiltration to a malicious domain
High risk In progress

Alert state

Classification Not set
Assigned to Multi-stage attack
Set classification Assign to

Alert details

Category Exfiltration
Techniques Exfiltration
Service source Microsoft Defender XDR
Detection source MDE
Generated on 06:46:03.722 AM
First activity 04:45:13.003 AM
Last activity 06:46:03.722 AM

Description

Country Finland
Company site HelsinkiMainSite
IT team

Copilot

Teams

Contain

Completed
User 'Jonathan Wolcott' was suspended by automatic attack disruption
Attack disruption

Investigate

Completed
IP '107.189.30.22' is matching known actor: Storm-0928

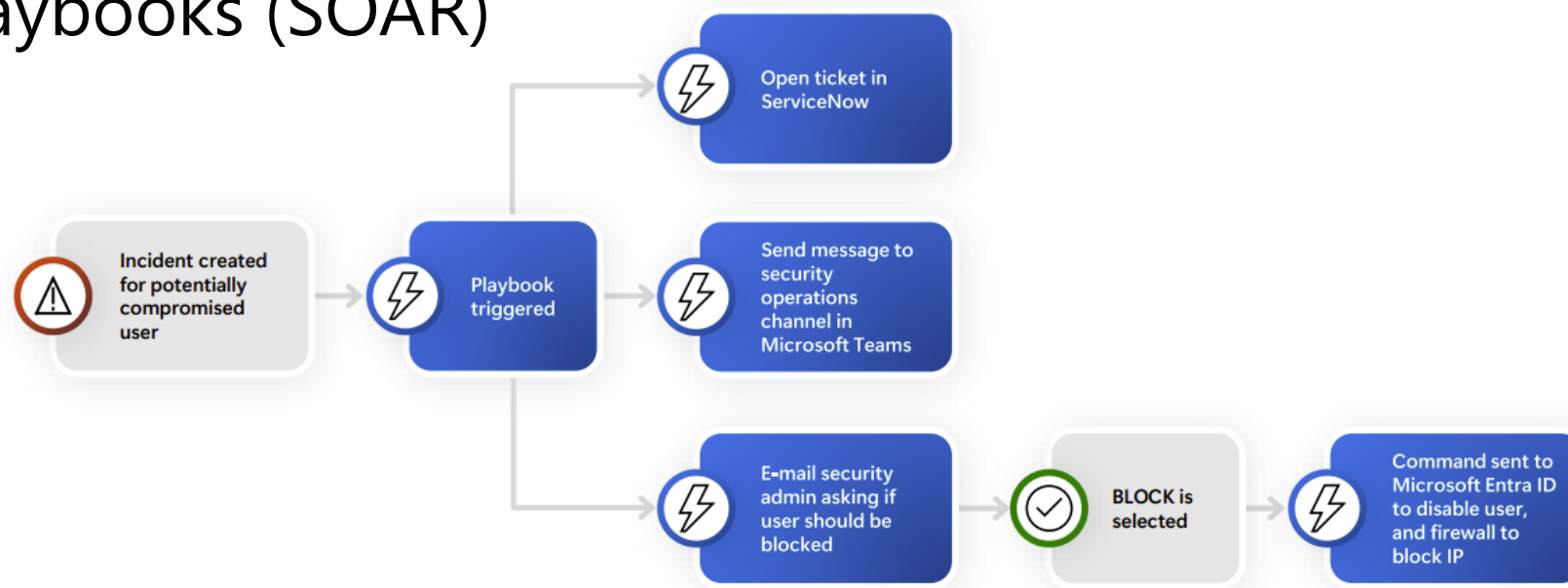
Remediate

New
Remediate the compromised account
To remediate the compromised account, run the 'User remediation' playbook to reset their password, force new sign-in and re-enable the account.
Run 'User remediation' playbook
View or edit 'User remediation' playbook

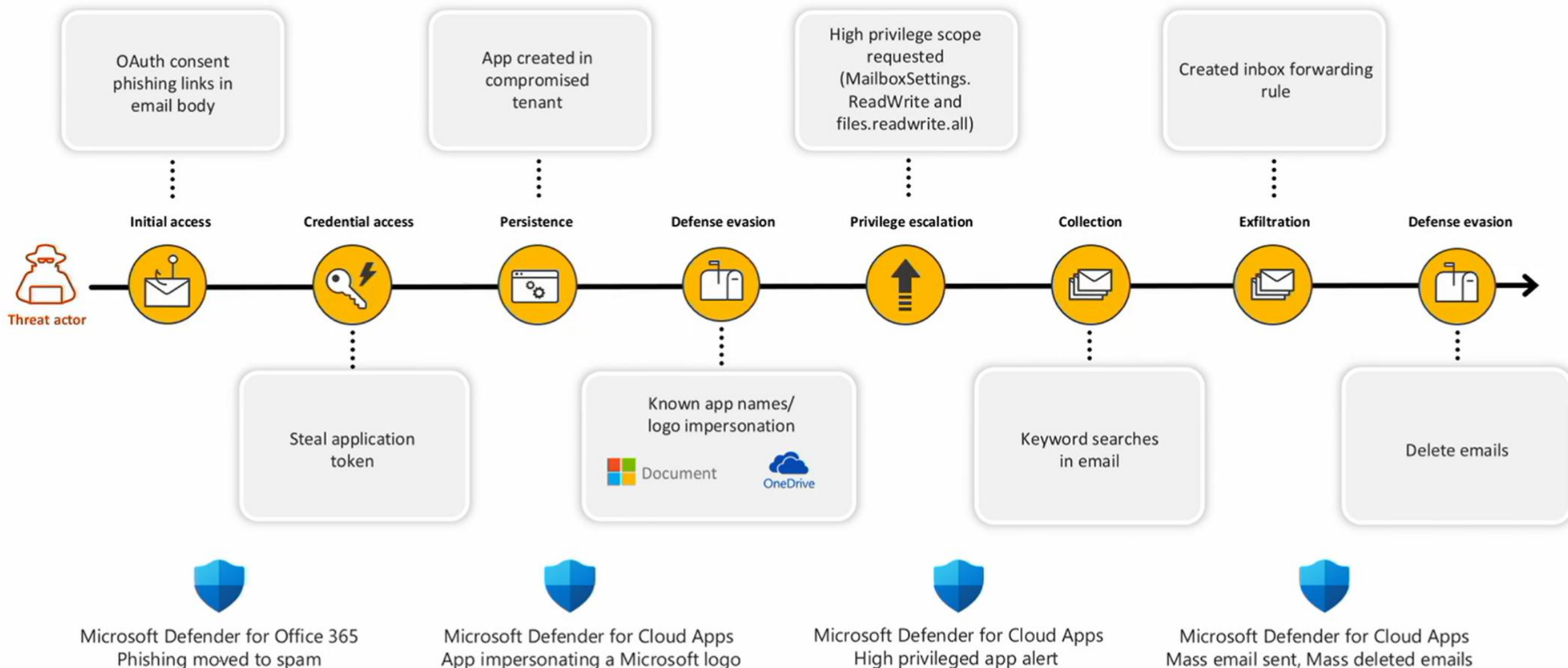
New
Resolve incident and generate a summary report
Resolve and generate report

A to možná i když spíte...

- Automatická investigace a reakce (AIR)
- Automatic Attack Disruption (XDR)
- Automation a Playbooks (SOAR)



Case study: OAuth application consent phishing campaign attack flow



Dívejme se do těch konzolí

The screenshot displays the Microsoft Defender web interface. On the left is a navigation sidebar with options like Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Secure score, Data connectors, and Assets. The main content area is titled 'App impersonating a Microsoft logo' and shows a card for 'Office O365 Mail Outlook App (Microsoft)' identified as an 'OAuth app'. Below this, the 'Alert story' section is empty, and the 'What happened' section explains that a machine learning algorithm found a logo very similar to the proprietary Outlook logo, suggesting an attempt to impersonate Microsoft software. The 'Recommended actions' section lists three steps: investigate registration details, check for spoofing, and verify if the app is critical before deactivation. On the right, a detailed alert card shows the title 'App impersonating a Microsoft logo' with a 'Medium' severity and 'Unknown' status. It includes an 'INSIGHT' box with a 'Classify alert' button and an 'Alert state' section showing 'Classification: Not Set' and 'Assigned to: Unassigned'.

Microsoft Defender

Search

Home

Incidents & alerts

Hunting

Actions & submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

Overview

Attack surface

Exposure insights

Secure score

Data connectors

Assets

App impersonating a Microsoft logo

Part of incident: Suspicious activity incident [View incident page](#)

Office O365 Mail Outlook App (Microsoft)
OAuth app

Alert story [Maximize](#)

What happened

The non-Microsoft cloud app (Office O365 Mail Outlook App (Microsoft)) is using a logo that was found by a machine learning algorithm to be very similar to the proprietary logo for Outlook. This can be an attempt to impersonate Microsoft software products and appear legitimate.

Recommended actions

1. Investigate the app's registration details on app governance and visit Azure AD for more details.
2. Check the app for other signs of spoofing or impersonation as well as any suspicious activity.
3. Verify whether the app is critical to your organization before considering any containment actions. Deactivate the app using app governance to prevent it from accessing resources. Existing app governance policies might have already deactivated the app.

App impersonating a Microsoft logo
Medium Unknown
New

[Manage alert](#)

INSIGHT

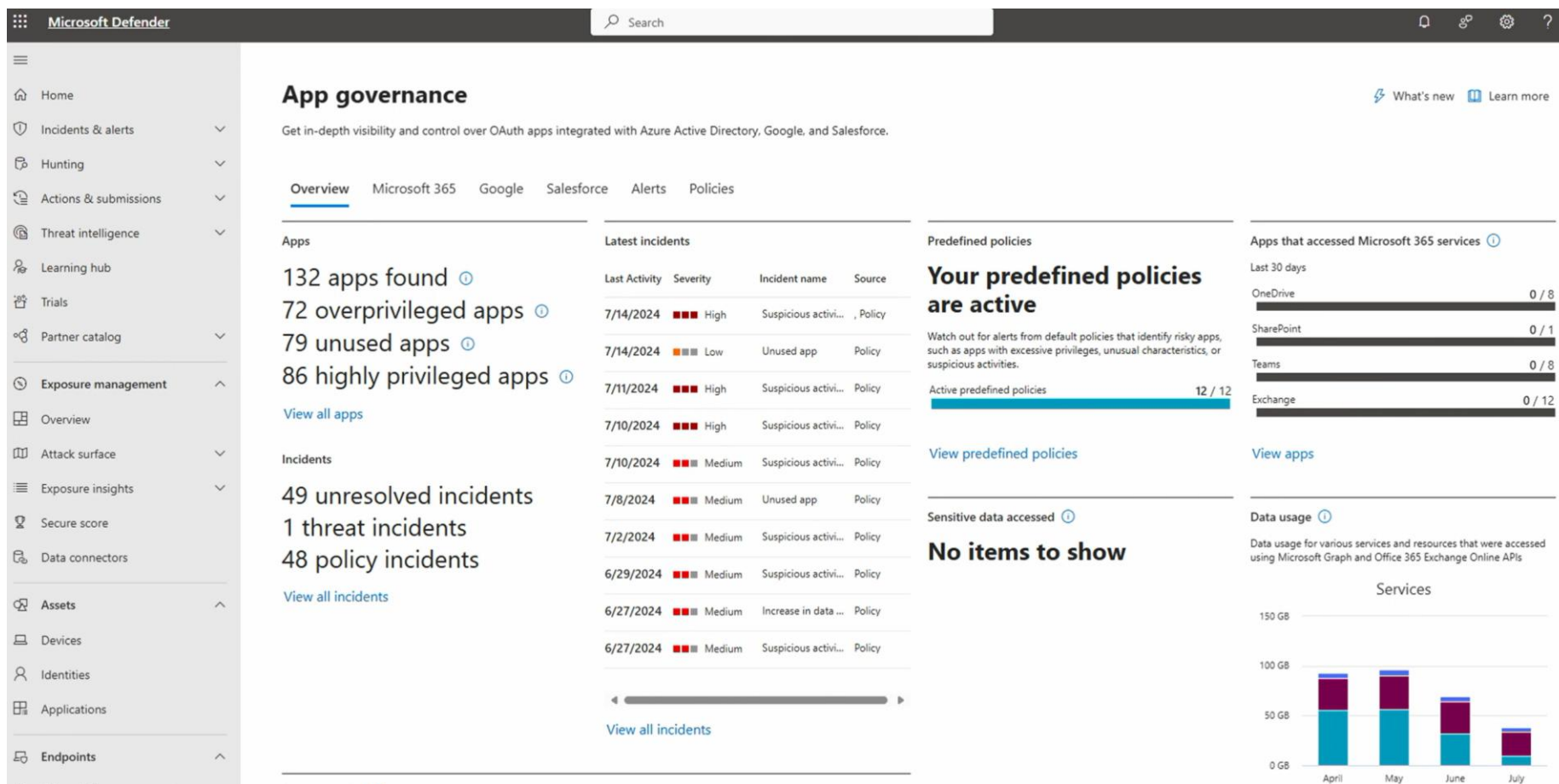
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

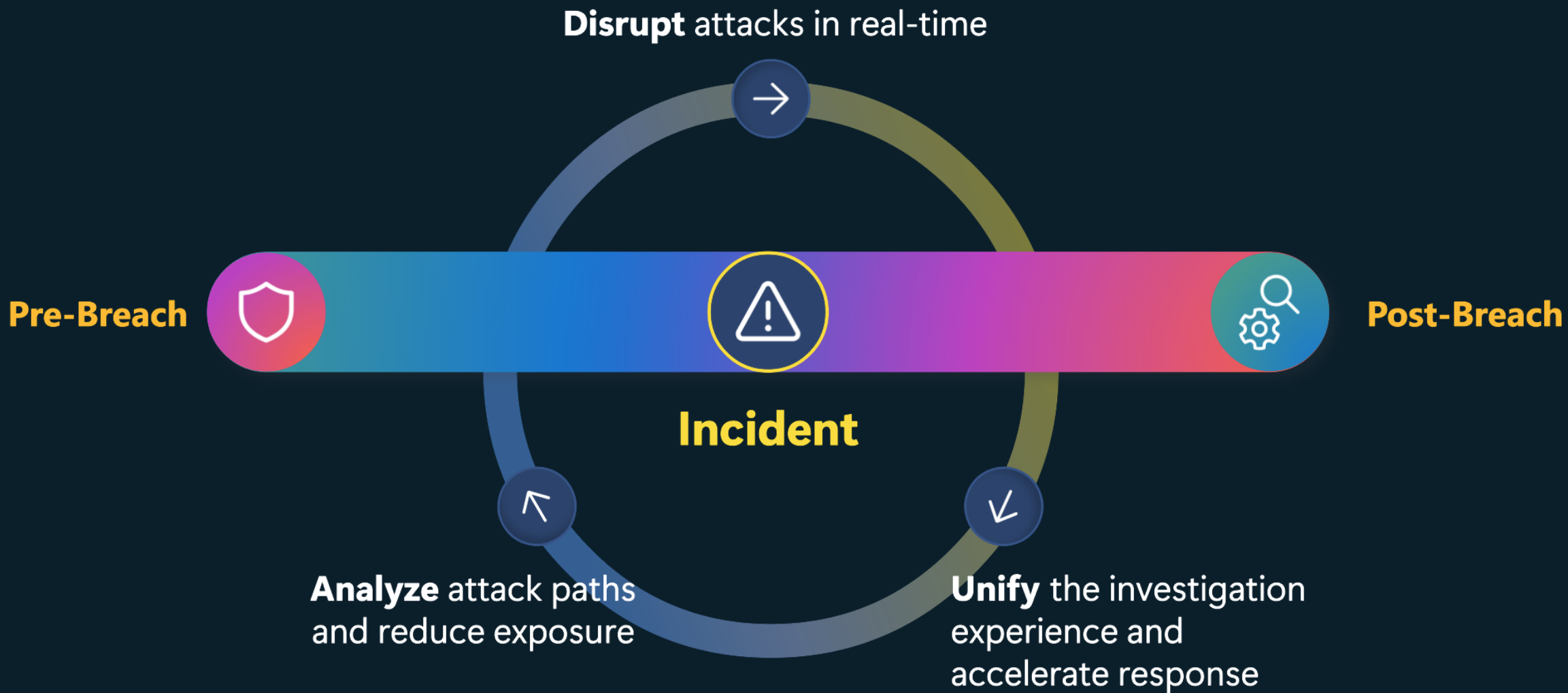
[Classify alert](#)

Alert state

Classification	Assigned to
Not Set	Unassigned

Generátor chaosu, uživatelé





The combined defensive stack

The flywheels of defense

Posture

Protection

SOC team
(detect, investigate, respond)

Pre-breach

Attack Paths / Blast Radius

Map (Graph)

Common Reputation

Entity Inventory

Post breach

Incidents

Detections

Behaviors

Activity store

'Toolbox'

Copilot

Automation

Queue / investigation

Hunting

Analytics

Data Connectors

Defender

Sentinel

The "Security Graph" – a map of the enterprise

Entity resolution and enrichment

Clean, normalize, aggregate, de-duplicate, contextualize

Vulnerability management

Email security

Identity security

Endpoint security

SaaS security

Application security

Cloud security

External attack surface

Asset metadata

Activity logs

Admin actions

Configuration data

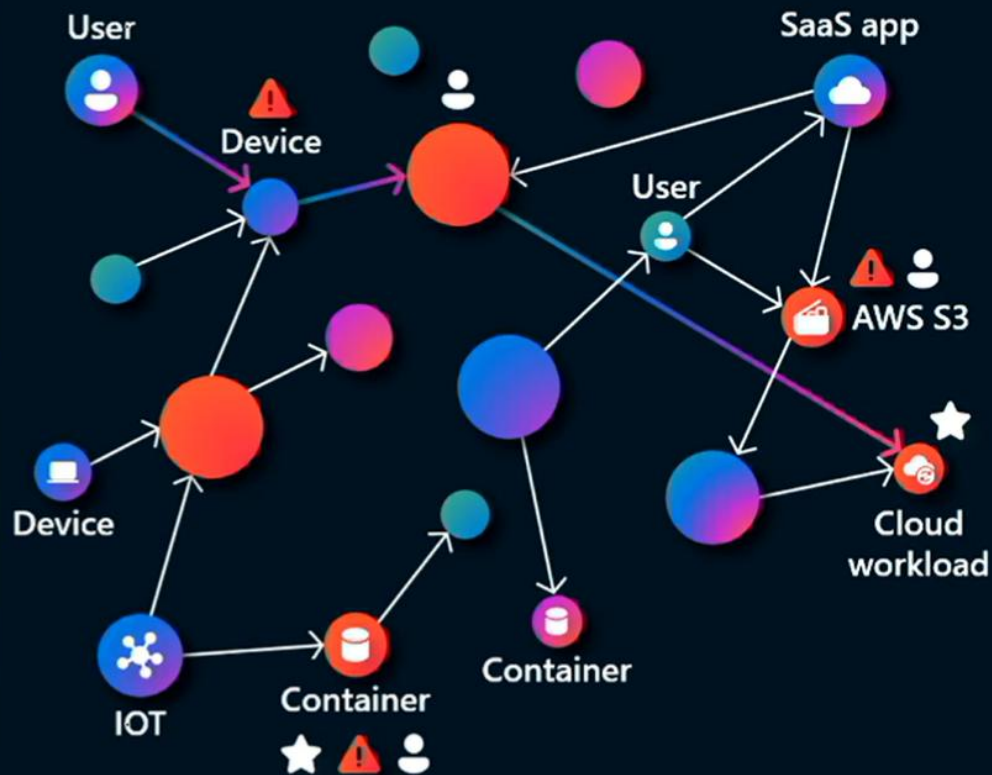
Policy state

Security findings

Health state

Input

Output



Attack surface discovery

Continuously discover, inventory and contextualize the organization's asset attack surface

Attack path analysis

Prioritize weaknesses by considering the attacker's perspective, moving away from the traditional siloed approach

Critical assets identification

Identify the assets in your org you should care more about

Understand blast radius

Understand potential downstream impact of attack as they happen and take appropriate measures

- 
-  Exposure management

 Overview

 Attack surface

 Exposure insights

Initiatives

Metrics

Recommendations

Events

 Secure score

 Data connectors

 Assets

 Endpoints

 Identities

 Email & collaboration

 Cloud apps

 Reports

 Health

 Permissions

 Settings

 More resources

Exposure management overview

 Add a suggestion

 Guided tour

How protected is your organization?

Our security exposure management tool offers key insights, metrics and customized initiatives for a centralized overview of your risk landscape.

Your assets, at a glance



Vulnerability status



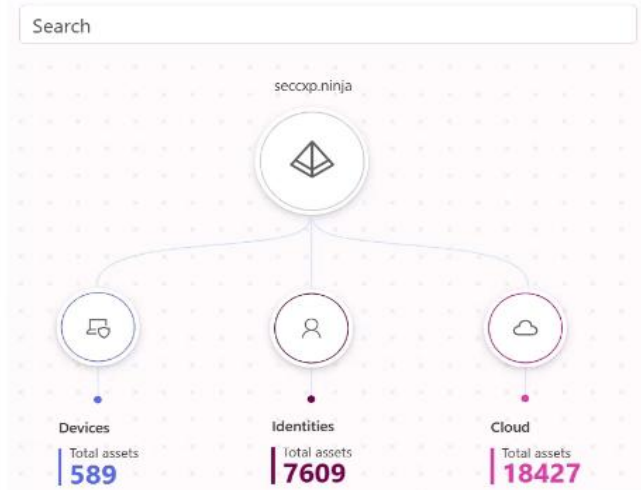
Key initiatives

[See all](#)

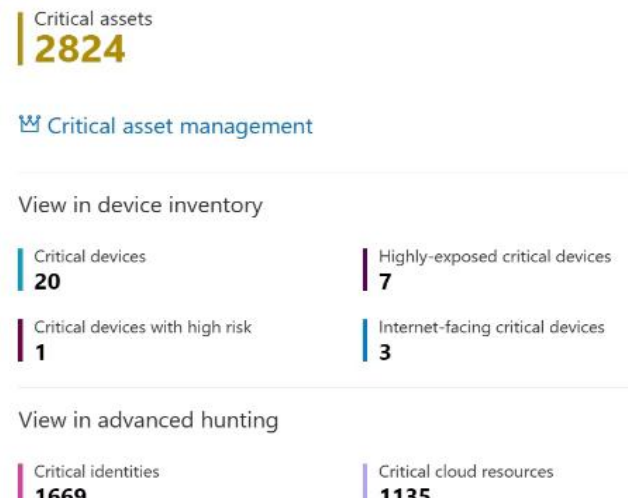
Top metrics

Name	Current V
% of missing best practices for devices against "On-premise...	100%
% of endpoints where the host Firewall is disabled or misco...	100%
% Azure relational database without geo-redundant backup...	100%
% containers images with high severity vulnerabilities	100%
% of missing best practices in Sharepoint Admin Center to ...	100%
% storage accounts without network access restriction usin...	99.17%

Attack surface map



Critical asset summary





Aktualizujte SW i HW
Nastavte SPF, DKIM, DMARC
Zakažte uživatelům registraci OAuth aplikací
Nasadte Conditional Access politiky
Používejte Phishing Resistant metody
Zapněte Defender for Endpoint
Vynuťte Tamper Protection
Dokumentujte a logujte
Využijte Identity Protection
Kontrolujte MDM Compliance

Koukněte se občas do stávajících konzolí a řešte ty upozornění...
Uložte si kontakty na KPCS CZ ;-)

Agents to empower roles across security and IT



Microsoft Security

 Phishing Triage

 Alert Triage in DLP and IRM

 Conditional Access Optimization

 Vulnerability Remediation

 Threat Intelligence Briefing

Partner ecosystem

 Privacy Breach Response
by OneTrust

 SecOps Tooling
by BlueVoyant

 Network Supervisor
by Aviatix

 Alert Triage
by Tanium

 Task Optimizer
by Fletch

Že už používáte a platíte za služby Microsoft 365?
Využijte jejich benefitů na maximum!



Definujte priority bezpečnosti: [Zero Trust Workshop by KPCS](#)

Ověřte si realitu IT prostředí: [Security Risk Assessment by KPCS](#)

Dotazy a diskuse

Petr Vlk

Microsoft MVP

Microsoft 365 Enterprise Security Architect @ KPCS CZ

vlk@kpcs.cz



KPCS