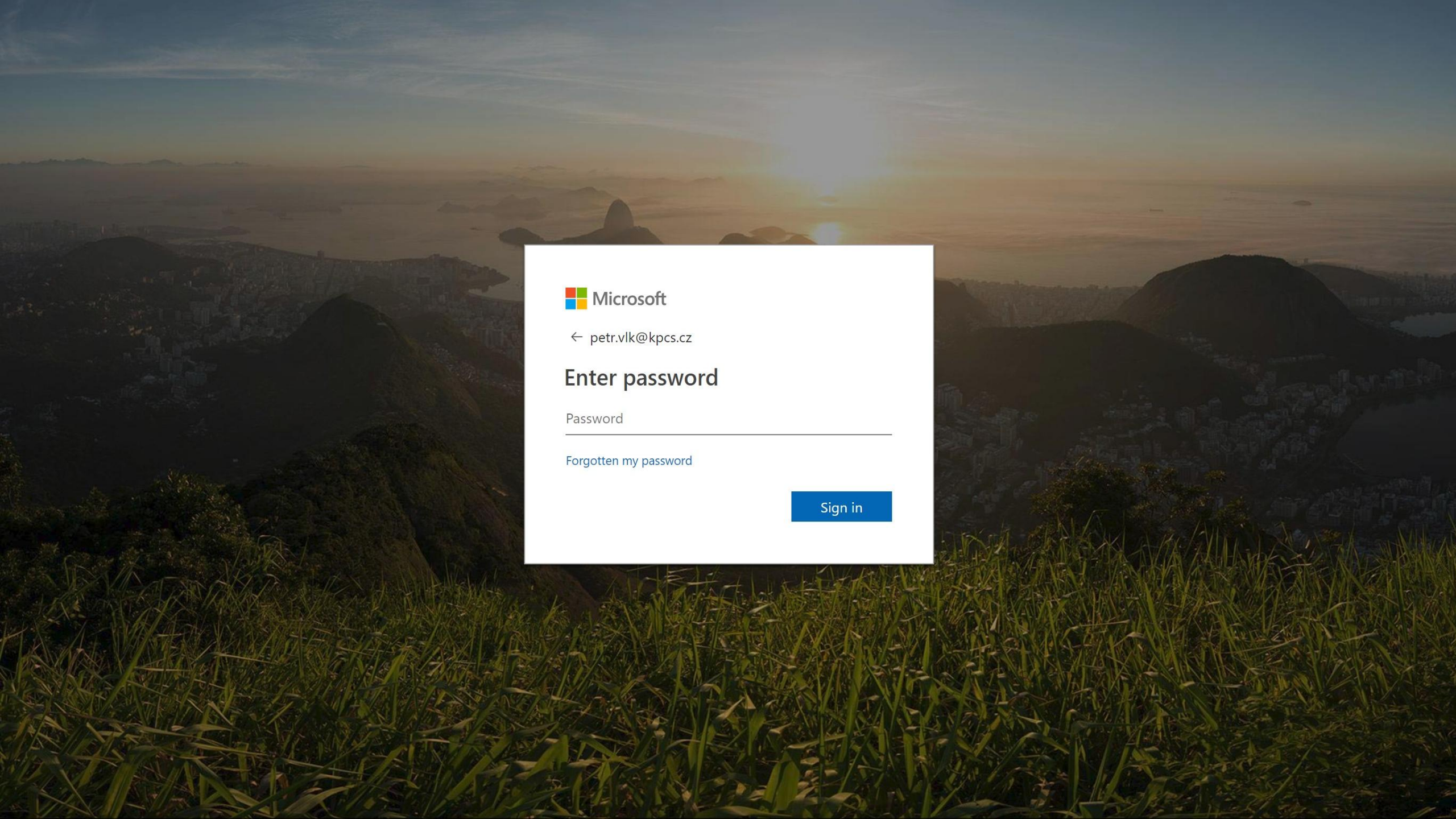
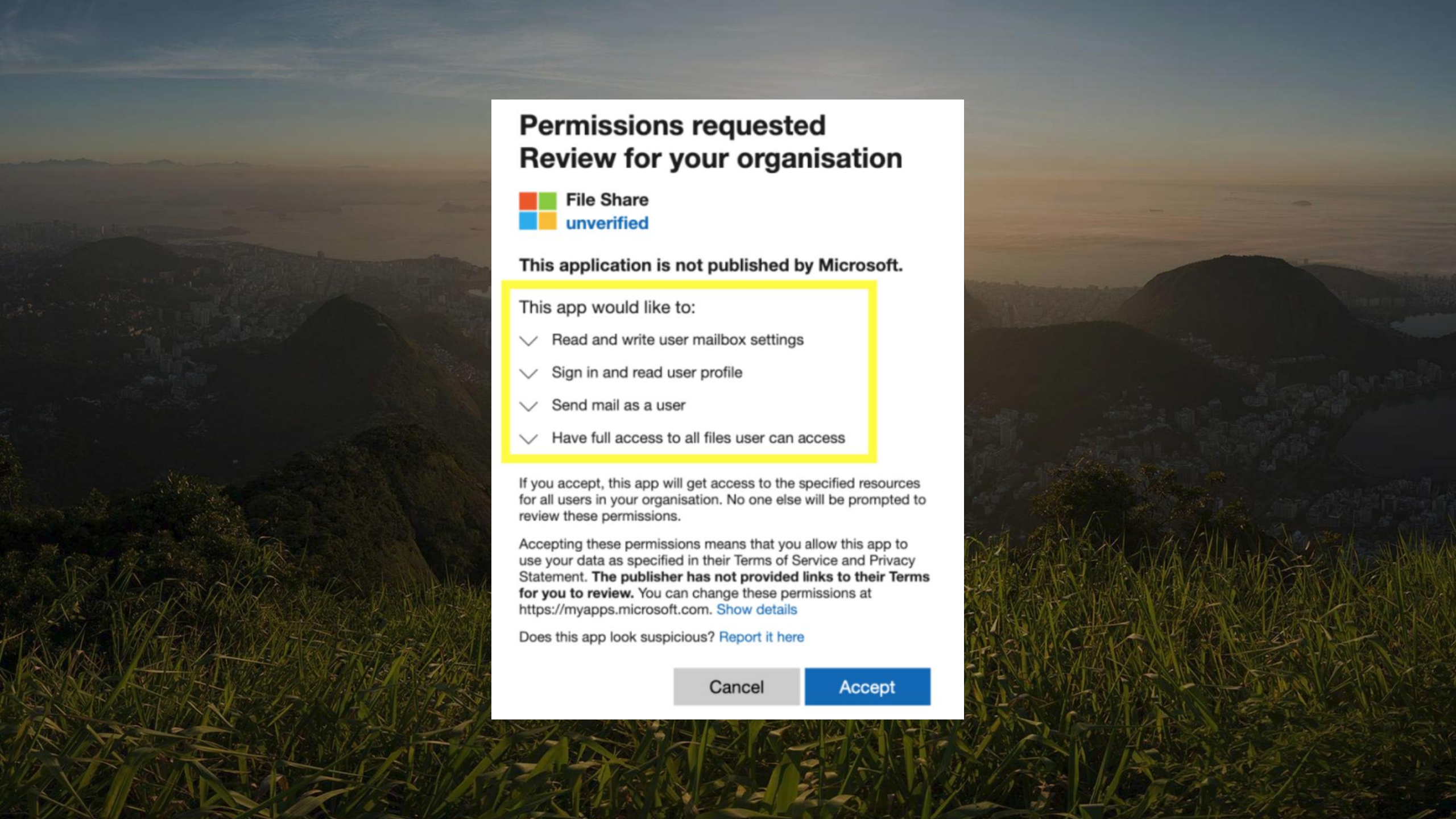
Že štěstí přeje připraveným?

Petr Vlk
Microsoft MVP
Microsoft 365 Enterprise Security Architect @ KPCS CZ
KPCS vlk@kpcs.cz


Microsoft
petr.vlk@kpcs.cz
Enter password
Password
Forgotten my password
Sign in

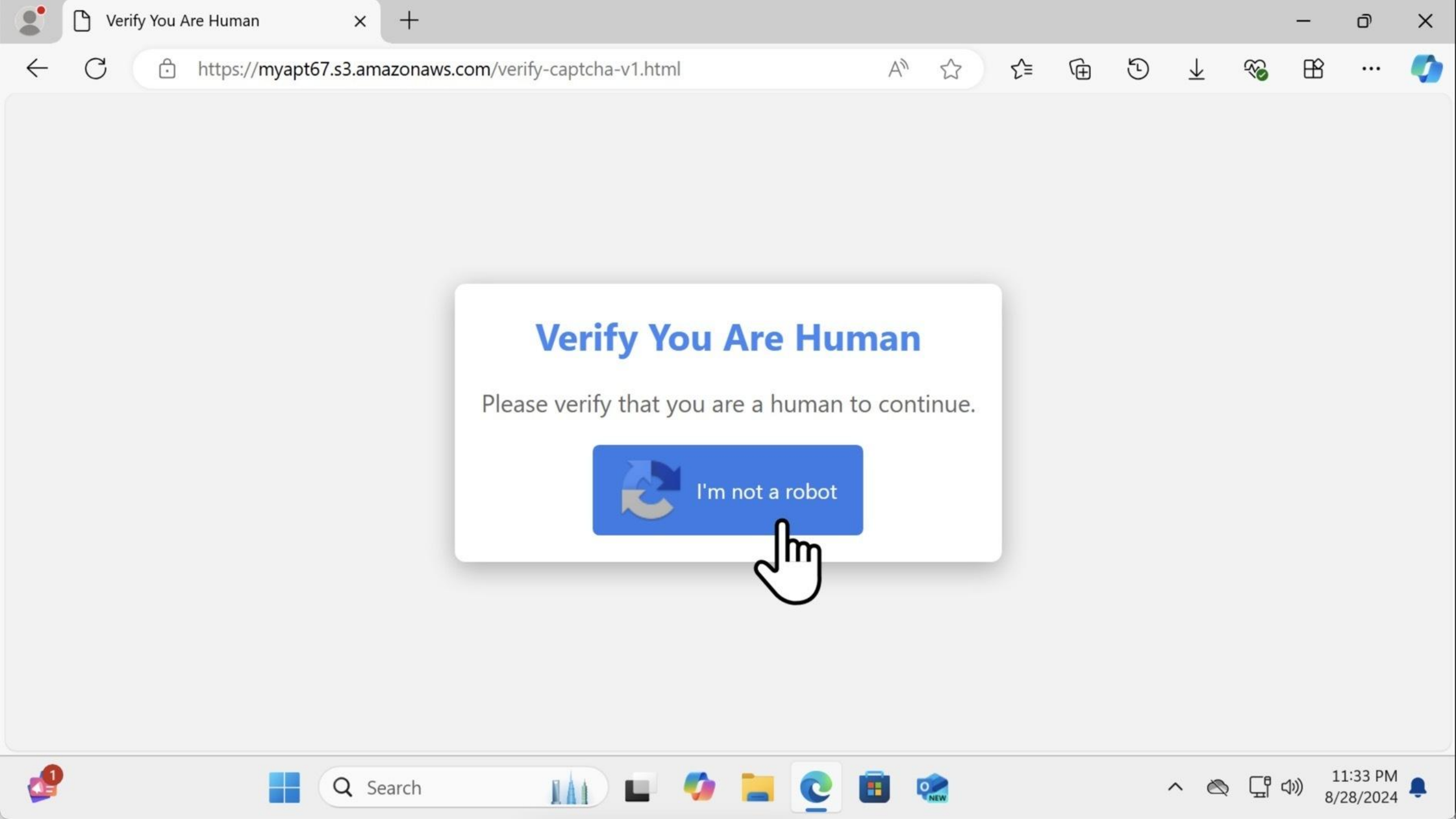

Permissions requested
Review for your organisation
File Share
unverified
This application is not published by Microsoft.
This app would like to:
Read and write user mailbox settings
Sign in and read user profile
Send mail as a user
Have full access to all files user can access
If you accept, this app 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

Microsoft

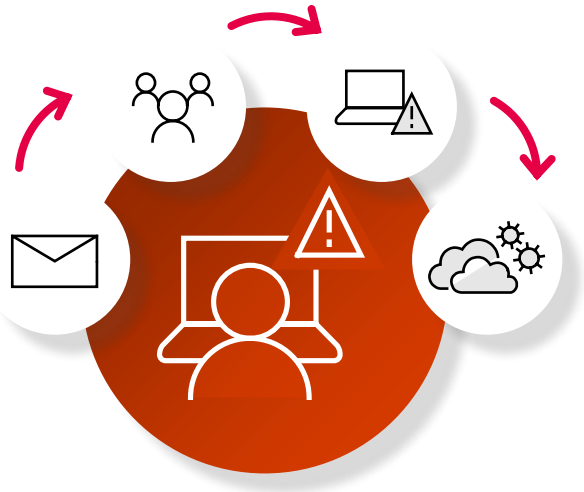
Update Microsoft Edge

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

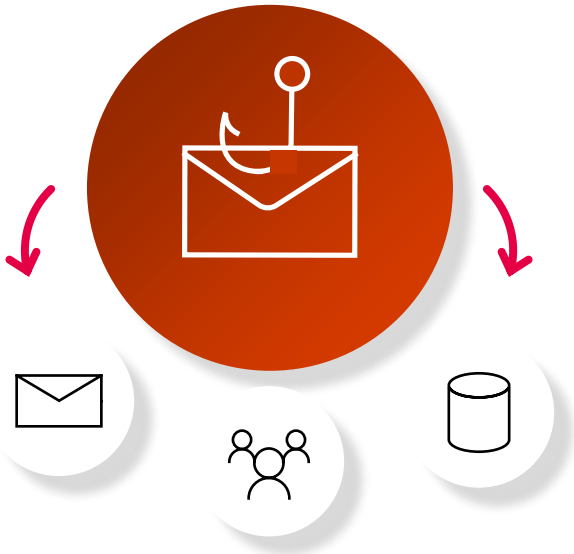
Update Microsoft Edge


Verify You Are Human
https://myapt67.s3.amazonaws.com/verify-captcha-v1.html
Verify You Are Human
Please verify that you are a human to continue.
I'm not a robot
Search
11:33 PM
8/28/2024

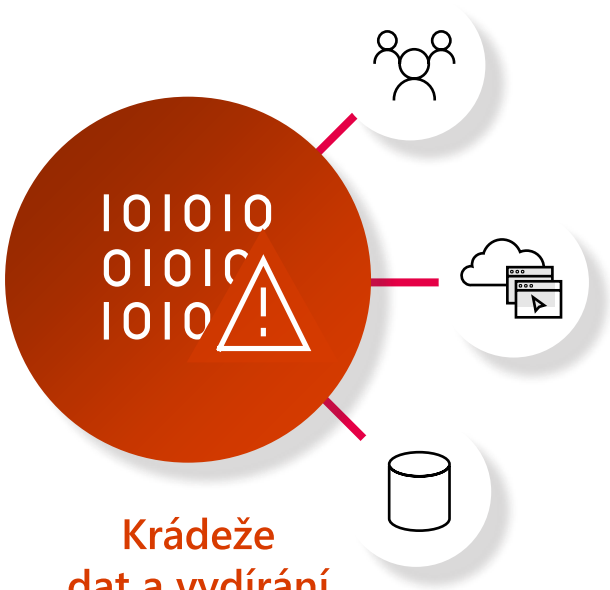
Sofistikované útoky jdou napříč doménami



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 standardy 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
- Nasaďte 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.

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

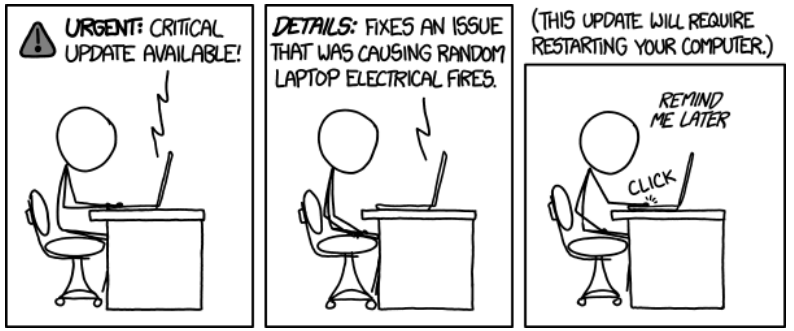
- Incident Response Plan
  - Incident Manager, CSIRT/IRT
  - Zapojení vedení organizace a jejich podpora
- Izolace systémů
  - Odpojení od sítě a internetu
  - Blokace účtů v systémech
  - Zachování forenzních stop
- Analýza a evidence
  - Logy, obrazy disků, časová osa
  - Dotčené systémy, ovlivněná 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)



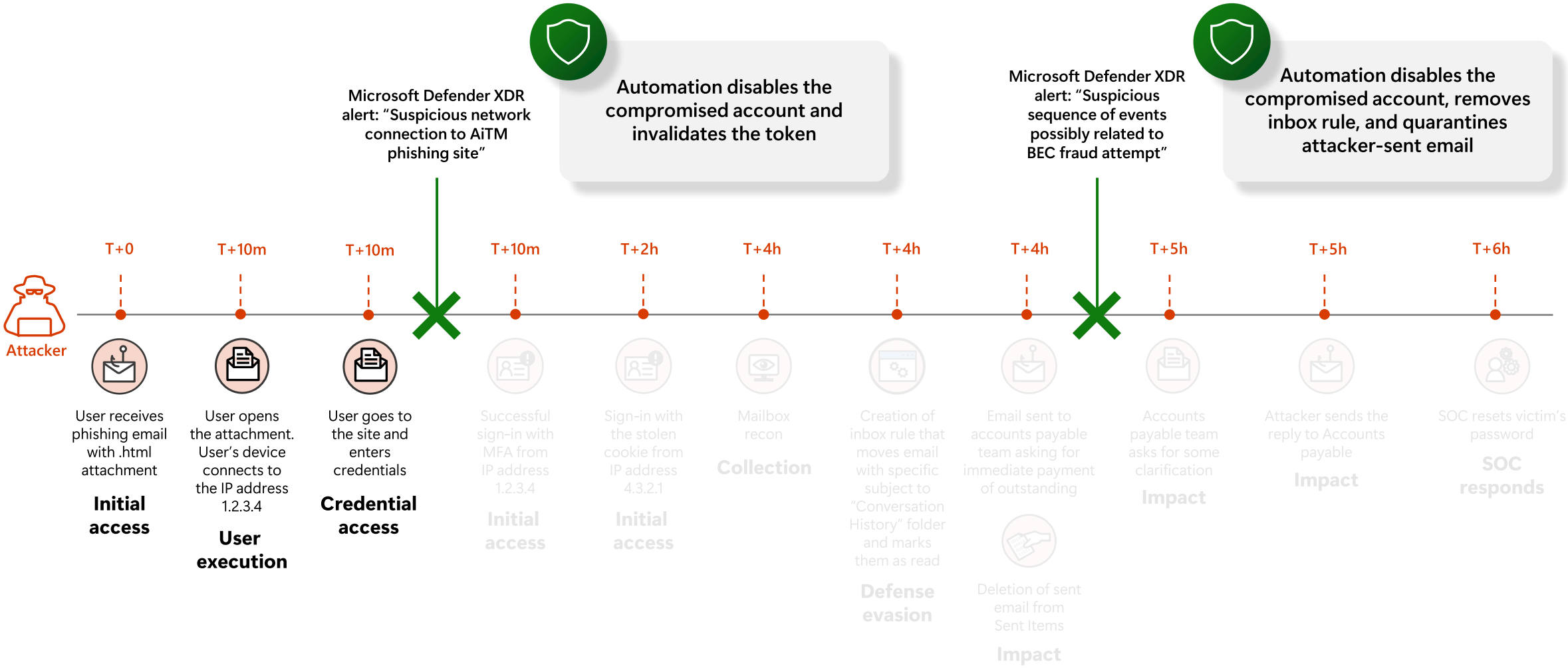
Logování aneb auditní stopa

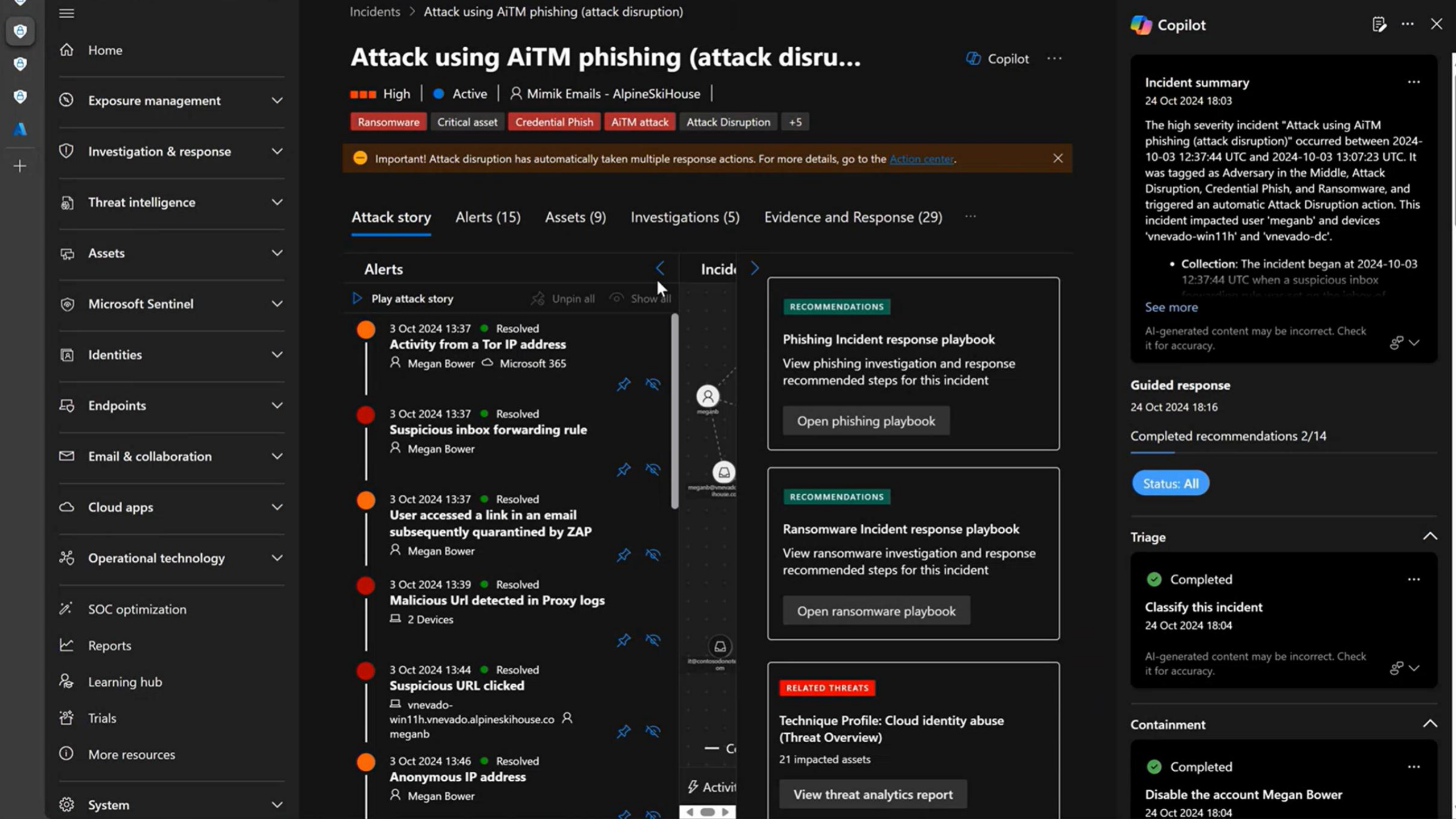
- Přemýšlejte o otázkách, které můžete mít v případě řešení incidentu…
  - Kde budu hledat jaké informace a údaje?
  - Jak dlouho sahá historie mých logů?
  - Mám jistotu, že auditní stopa bude úplná a co obsahuje?
  - Kdo se přihlásil? Z jaké IP adresy, zařízení?
  - Které údaje využil pro přihlášení? 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)




Incidents > Attack using AiTM phishing (attack disruption)
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
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
meganb
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
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Operational technology
SOC optimization
Reports
Learning hub
Trials
More resources
System
Copilot
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

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Guided Tour | Customize page

- 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

Unified incidents and alerts

145 active incidents

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

In progress	Resolved
24	57

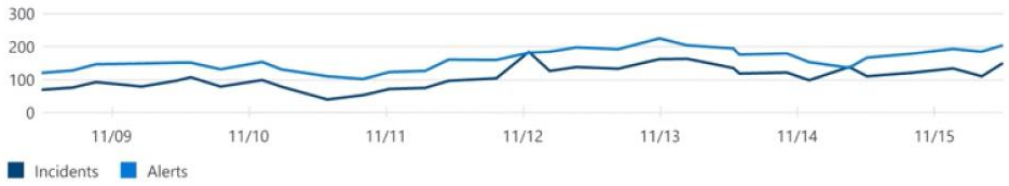
Active incidents by severity

High | Medium | Low | Informational

Closed incidents by classification

True positive | False positive | Benign positive | Undetermined

Closed incidents and alerts over time



View all incidents

Sentinel automation

33 automation rules

Closed incidents	Time saved	Actions performed
6	23 hours	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

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-Comrimise 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

Sentinel data connectors

48 data connectors

Active connectors	Unhealthy connectors
34/48	12/48

SOC optimization

Your optimized data

Active	Completed	Dismissed
7	2	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.

What's new

https://defender.microsoft.com

Contoso | Microsoft Defender

Search

Incidents > SAP financial process manipulation attack disrupted

SAP financial process manipulation attack disrupted

Copilot | Manage incident | Activity log | ...

High | Active | Attack disruption | SAP fraud | BEC fraud | Chain event detection

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

Alerts

13/13 Active alerts | Unpin all | Show all

Nov 15, 2023 2:41 AM | Active
A potentially malicious URL click was detected
jonathan.wolcott@contoso.com

Nov 15, 2023 2:42 AM | Active
Possibly malicious URL clicked
cont-jonathan.pc | Jonathan Wolcott

Nov 15, 2023 2:43 AM | Active
Zscaler - phishing URL click detected
Jonathan Wolcott

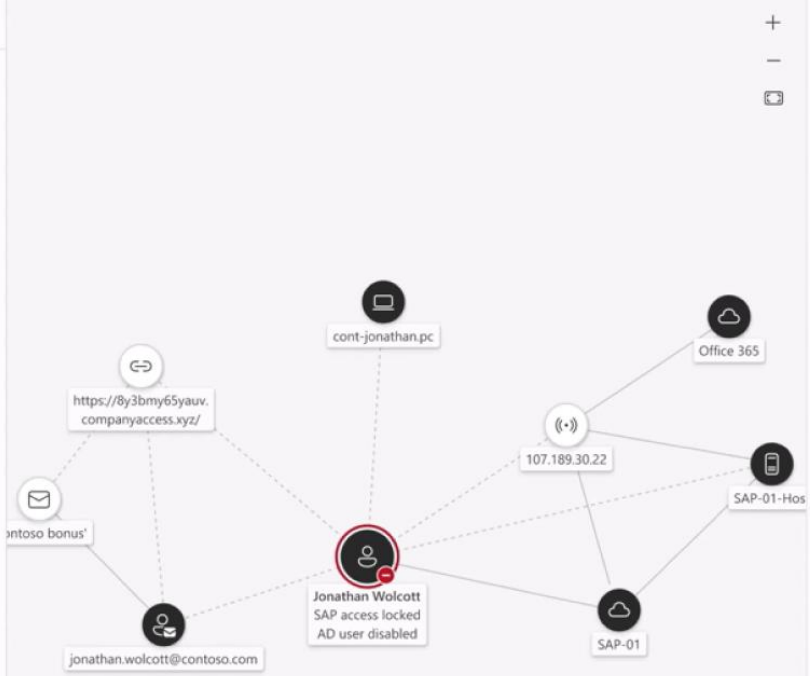
Nov 15, 2023 2:45 AM | Active
Unfamiliar sign-in properties
Jonathan Wolcott

Nov 15, 2023 2:43 AM | Active
Suspicious SAP authentication
Jonathan Wolcott | SAP-01 | SAP-01-Host

Nov 15, 2023 4:44 AM | Active
Suspicious user viewed SAP financial info
Jonathan Wolcott | SAP-01 | SAP-01-Host

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

Layout | Group by



Information

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@conto...

Applications
SAP-01
Office 365

Copilot

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

Recommended actions
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...

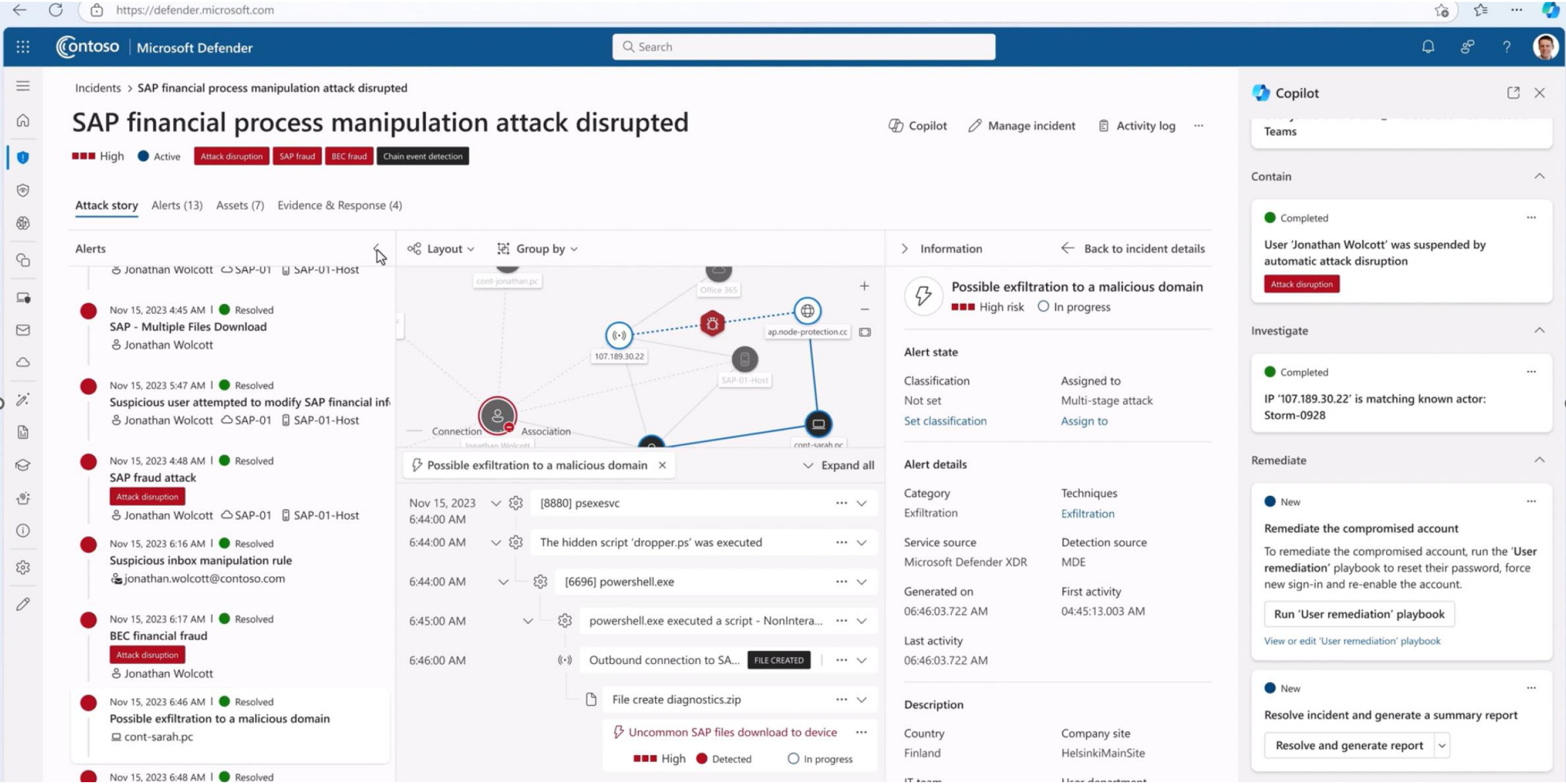
See more

Contact user in Teams | view user

AI generated. Verify for accuracy.

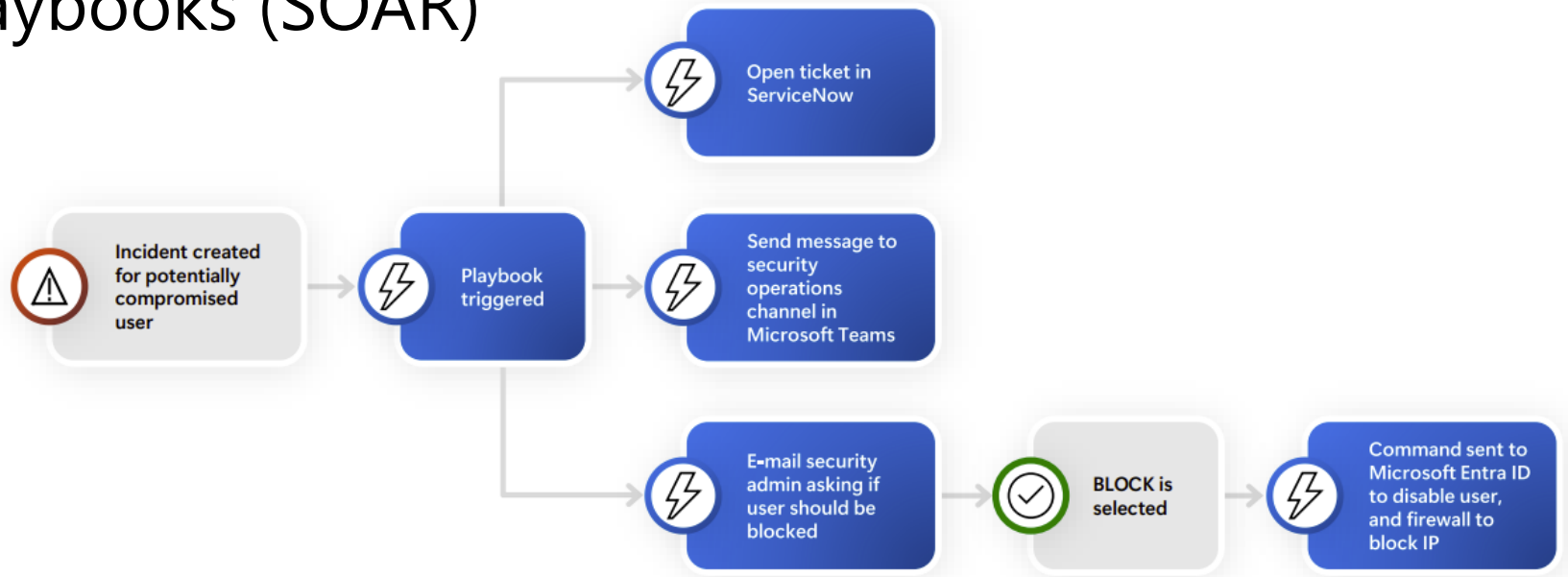
Contain

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

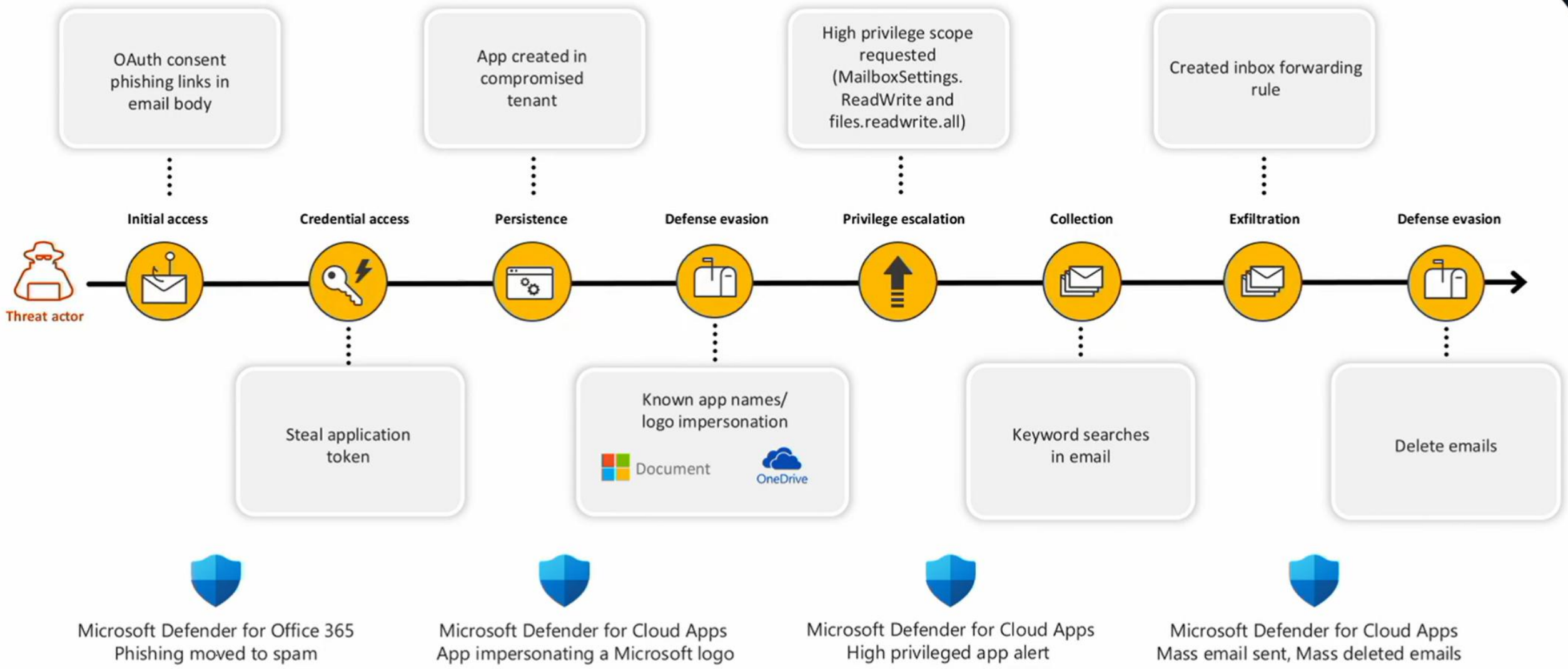

https://defender.microsoft.com
Contoso | Microsoft Defender
Search
Incidents > SAP financial process manipulation attack disrupted
SAP financial process manipulation attack disrupted
Copilot
Manage incident
Activity log
High
Active
Attack disruption
SAP fraud
BEC fraud
Chain event detection
Attack story
Alerts (13)
Assets (7)
Evidence & Response (4)
Alerts
Jonathan Wolcott SAP-01 SAP-01-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 inf
Jonathan Wolcott SAP-01 SAP-01-Host
Nov 15, 2023 4:48 AM | Resolved
SAP fraud attack
Attack disruption
Jonathan Wolcott SAP-01 SAP-01-Host
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
Attack disruption
Jonathan Wolcott
Nov 15, 2023 6:46 AM | Resolved
Possible exfiltration to a malicious domain
cont-sarah.pc
Nov 15, 2023 6:48 AM | Resolved
Layout
Group by
cont-jonathan.pc
Office 365
ap.node-protection.cc
107.189.30.22
SAP-01-Host
Connection
Association
cont-sarah.pc
Possible exfiltration to a malicious domain
Expand all
Nov 15, 2023 6:44:00 AM
[8880] psexesvc
6:44:00 AM
The hidden script 'dropper.ps' was executed
6:44:00 AM
[6696] powershell.exe
6:45:00 AM
powershell.exe executed a script - NonIntera...
6:46:00 AM
Outbound connection to SA...
FILE CREATED
File create diagnostics.zip
Uncommon SAP files download to device
High
Detected
In progress
Information
Back to incident details
Possible exfiltration to a malicious domain
High risk
In progress
Alert state
Classification
Not set
Set classification
Assigned to
Multi-stage attack
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
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…

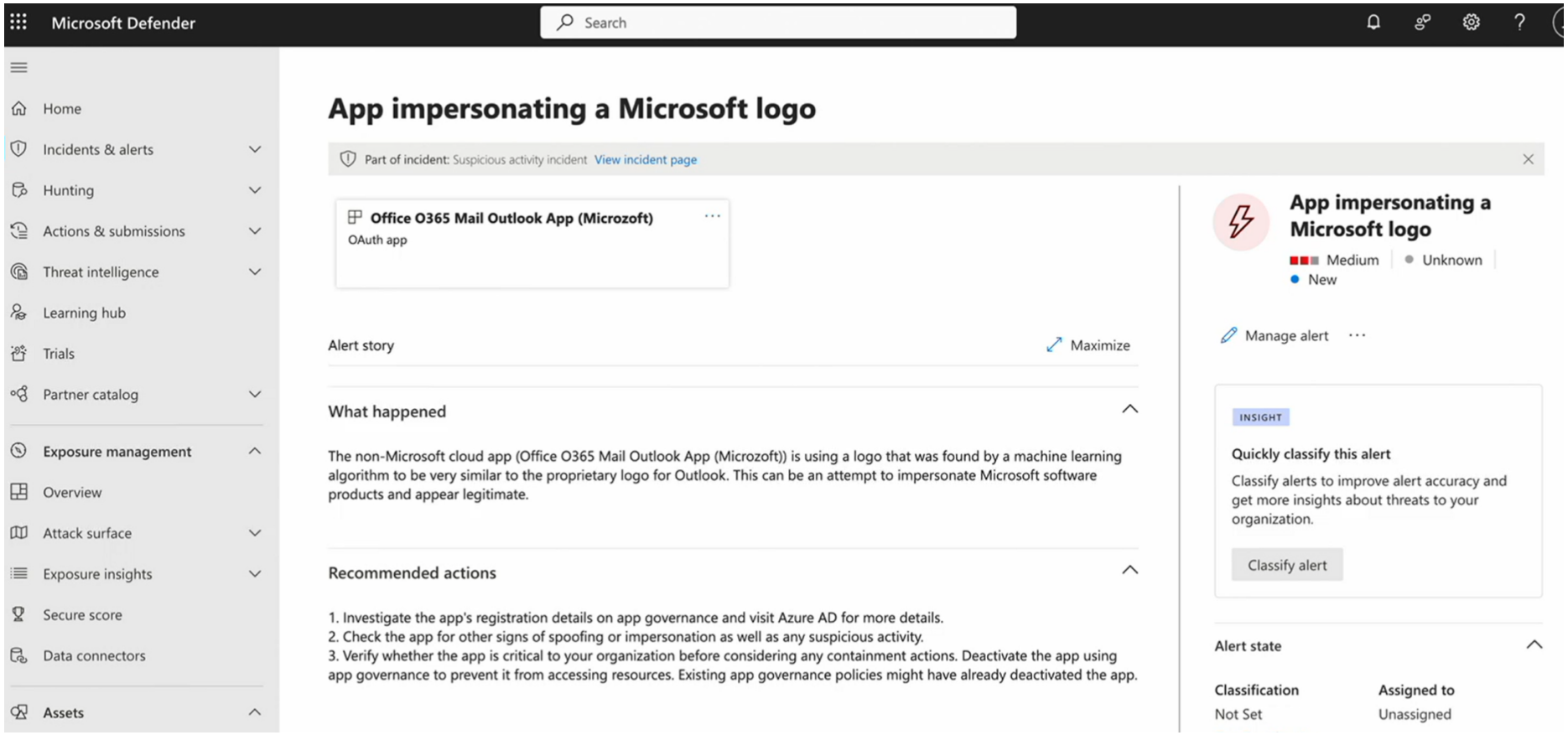
- Automatická investigace a reakce (AIR)
- Automatic Attack Disruption (XDR)
- Automation a Playbooks (SOAR)



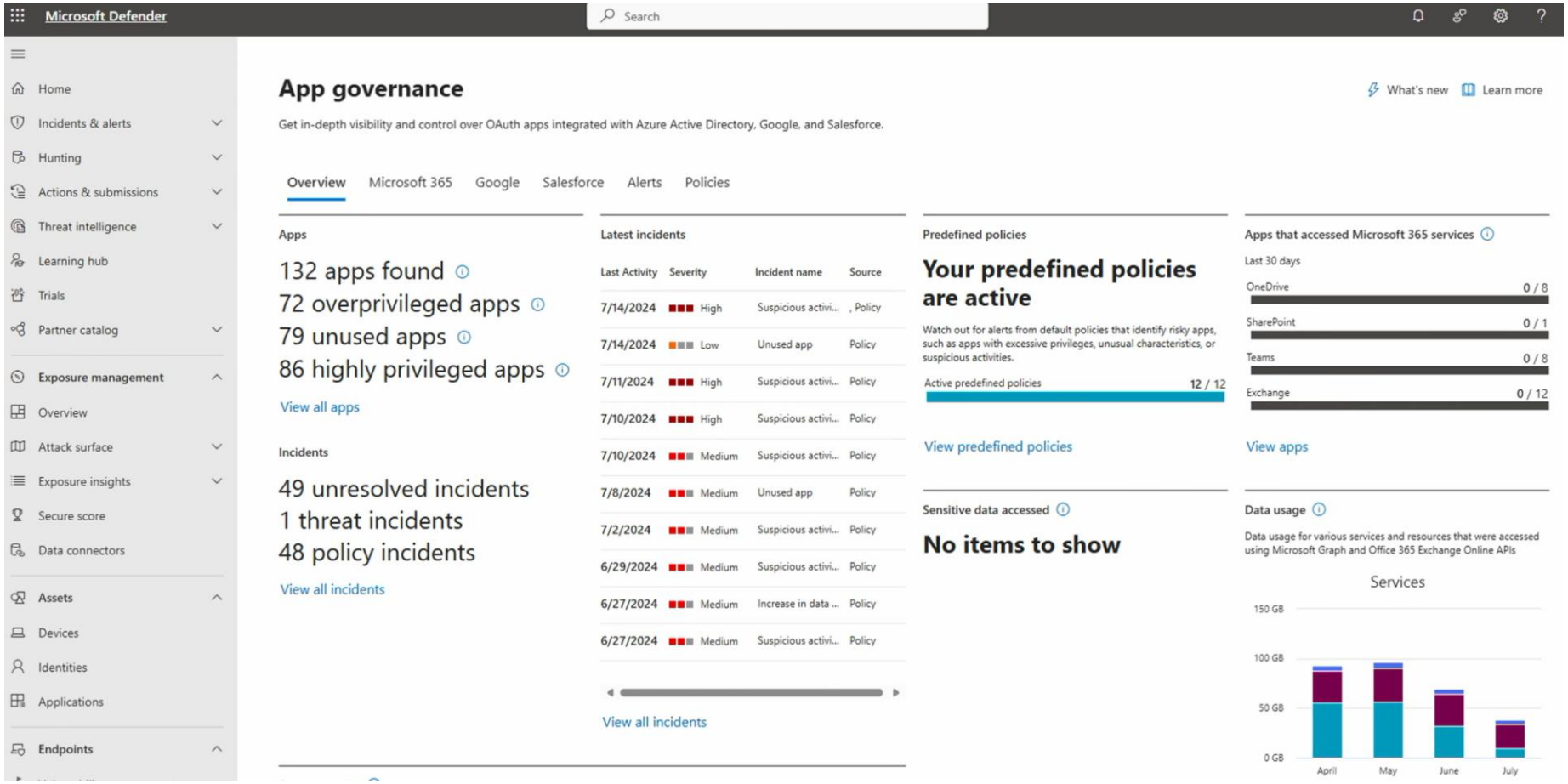
Case study: OAuth application consent phishing campaign attack flow



Dívejme se do těch konzolí



Generátor chaosu, uživatelé



Aktualizujte SW i HW
Nastavte SPF, DKIM, DMARC
Zakažte uživatelům registraci OAuth aplikací
Nasaďte 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 ;-)

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