

Tobias Kritten

Defender Security Center – was nun?

# Vielen Dank an unsere Sponsoren!

## PLATINUM SPONSOR



## GOLD SPONSOR



# Cloud (Security) ist meine Leidenschaft

Seit über 15 Jahren helfe ich Unternehmen beim sicheren Einsatz von Microsoft-Technologien: zu Beginn mit meinem eigenen Systemhaus, später durch das Hosting von Exchange, SharePoint- und Microsoft-basierten Applikationen und heute schwerpunktmäßig in der Cloud durch den Einsatz von Microsoft Security-Lösungen und Konzepte wie Azure AD, der Defender-Produktreihe oder Zero Trust.

## Cloud Security Portfolio (Auszug)

- Einführung Security-Lösungen (Microsoft Defender for X, Intune, DarkTrace, etc.)
- Durchführung von Security-related Best Practice Workshops und Audits
- Einführung von und Beratung rund um Zero Trust-Konzepte

## Cloud Networking Portfolio (Auszug)

- Integration von Networking-Themen in Cloud-Umgebungen
- Beratung und Problem-Solving in komplexen Networking-Architekturen
- Fokus auf die Integration von Fortinet-Lösungen in Azure-Umgebungen

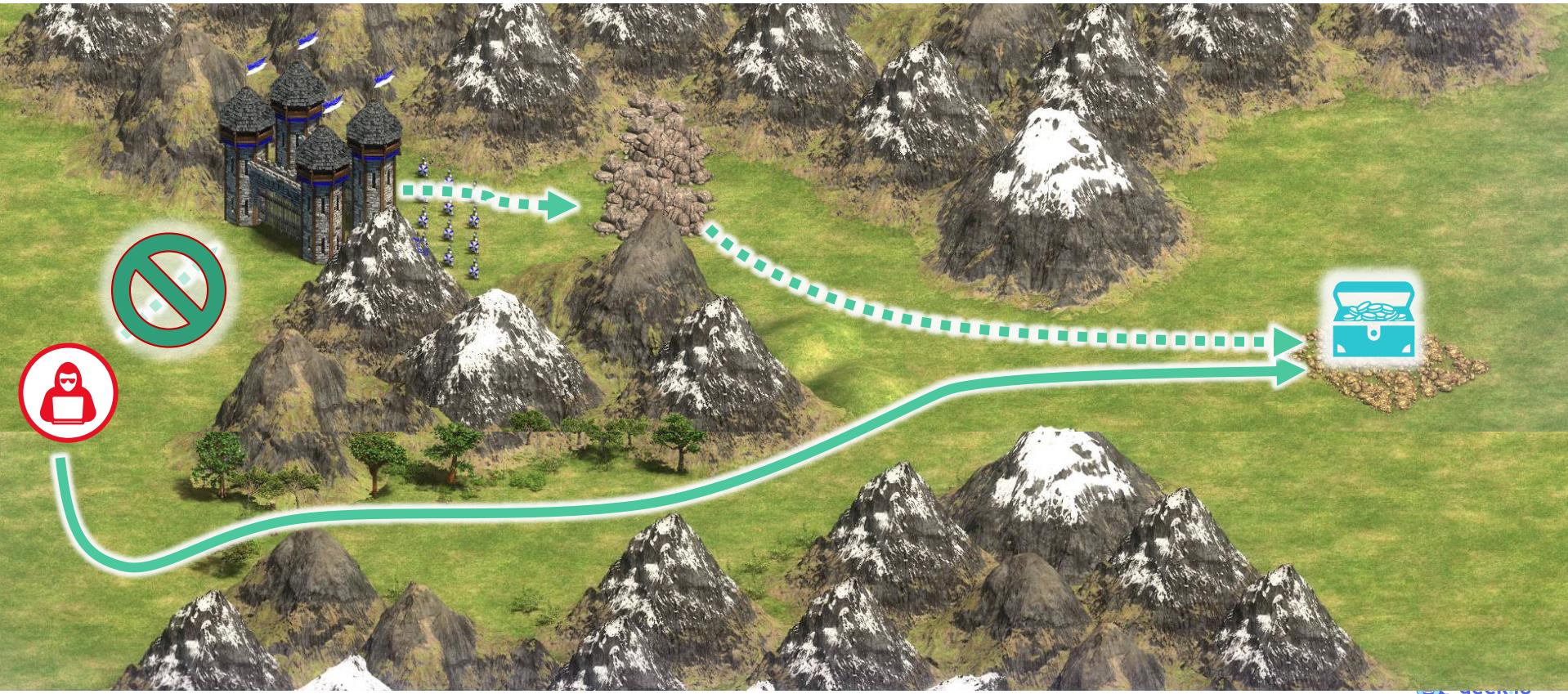




# Recap

... Angreifer nutzen den Weg des geringsten Widerstand/Kosten!

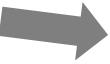
Angreifer folgen unseren "geplanten" Angriffs-Szenarien



# Defender Security Center - Datenquellen



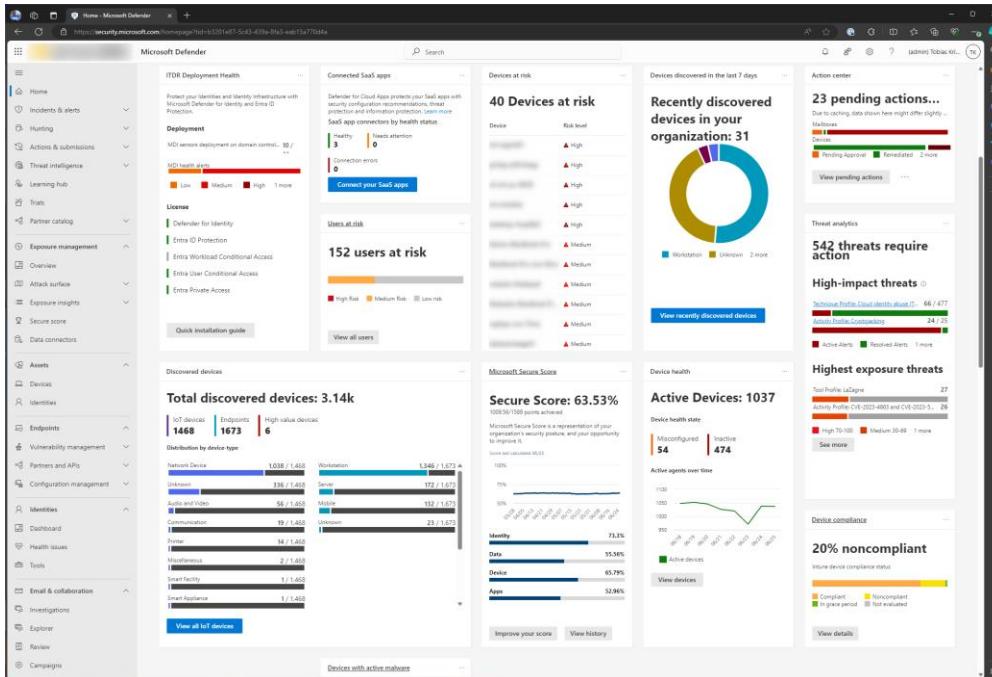
Defender for  
Office 365



Defender for  
Endpoint / XDR



Entra ID  
Identity Protection



Defender for  
Identity



Defender for  
Cloud Apps



# Alerts

- Meldung über ein spezifisches Ereignis
- Entspricht einem “Signal”
- Isolierte Sicht

The screenshot shows the Microsoft Defender for Cloud interface under the 'Alerts' section. The left sidebar contains navigation links for 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, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Configuration management, and Identities. The main area is titled 'Alerts' and displays a table of detected threats. The table includes columns for Alert name, Tags, Severity, Investigation state, Status, Category, Detection source, Impacted assets, First activity, Last activity, Classification, and Date. A filter bar at the top allows users to export data over 1 week, set severity levels (High, Medium, Low), and apply status filters (New, In progress, Resolved). Buttons for 'Add filter' and 'Reset all' are also present.

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity	Last activity	Classification	Date
Unsanctioned cloud app access was blocked		Low	New	Suspicious activity	Custom TI			Jun 25, 2024 9:45 AM	Jun 25, 2024 9:45 AM	Not Set	Not
Unsanctioned cloud app access was blocked		Low	Queued	New	Suspicious activity	Custom TI		Jun 20, 2024 9:17 AM	Jun 25, 2024 9:13 AM	Not Set	Not
Email reported by user as junk		Low	No threats found	Resolved	Threat management	MDO		Jun 25, 2024 8:48 AM	Jun 25, 2024 8:49 AM	Not Set	Not
Email reported by user as malware or phish		Low	New	Suspicious activity	Custom TI			Jun 25, 2024 7:06 AM	Jun 25, 2024 7:07 AM	False positive	Not
Unsanctioned cloud app access was blocked		Low	New	Suspicious activity	Custom TI			Jun 24, 2024 2:57 PM	Jun 24, 2024 2:57 PM	Not Set	Not
Email reported by user as junk		Low	Queued	New	Threat management	MDO		Jun 24, 2024 9:47 AM	Jun 24, 2024 9:48 AM	Not Set	Not
Email reported by user as junk		Low	Queued	New	Threat management	MDO		Jun 24, 2024 9:45 AM	Jun 24, 2024 9:46 AM	Not Set	Not
Unsanctioned cloud app access was blocked		Low	New	Suspicious activity	Custom TI			Jun 24, 2024 9:03 AM	Jun 24, 2024 9:03 AM	Not Set	Not
Email reported by user as malware or phish		Low	No threats found	Resolved	Threat management	MDO		Jun 24, 2024 7:57 AM	Jun 24, 2024 7:58 AM	Not Set	Not
Messages containing malicious entity not removed		Medium	Pending action	In progress	Threat management	MDO		Jun 22, 2024 11:11 PM	Jun 22, 2024 6:13 PM	Not Set	Not
Messages containing malicious entity not removed		Medium	Pending action	In progress	Threat management	MDO		Jun 22, 2024 5:38 PM	Jun 22, 2024 5:40 PM	Not Set	Not
Messages containing malicious entity not removed		Medium	Pending action	In progress	Threat management	MDO		Jun 22, 2024 5:00 PM	Jun 22, 2024 5:02 PM	Not Set	Not
Messages containing malicious entity not removed		Medium	Pending action	In progress	Threat management	MDO		Jun 22, 2024 4:43 PM	Jun 22, 2024 4:45 PM	Not Set	Not
Messages containing malicious entity not removed		Medium	Pending action	In progress	Threat management	MDO		Jun 22, 2024 4:42 PM	Jun 22, 2024 4:44 PM	Not Set	Not
An active 'RDPWrap' unwanted software was detected		Low	Terminated by system	New	Unwanted software	Antivirus		Jun 22, 2024 8:53 AM	Jun 22, 2024 8:53 AM	Not Set	Not
Email reported by user as malware or phish		Low	Some findings might...	In progress	Threat management	MDO		Jun 21, 2024 3:06 PM	Jun 21, 2024 3:07 PM	Not Set	Not
Email reported by user as junk		Low	Queued	New	Threat management	MDO		Jun 21, 2024 10:46 AM	Jun 21, 2024 10:47 AM	Not Set	Not
Email reported by user as junk		Low	Queued	New	Threat management	MDO		Jun 21, 2024 10:06 AM	Jun 21, 2024 10:07 AM	Not Set	Not
Email reported by user as junk		Low	Queued	New	Threat management	MDO		Jun 21, 2024 9:40 AM	Jun 21, 2024 9:41 AM	Not Set	Not
Email reported by user as not junk		Low	Queued	New	Threat management	MDO		Jun 21, 2024 9:39 AM	Jun 21, 2024 9:40 AM	Not Set	Not
Email reported by user as not junk		Low	Queued	New	Suspicious activity	Custom TI		Jun 14, 2024 4:07 PM	Jun 20, 2024 3:59 PM	Not Set	Not
Email reported by user as not junk		Low	Queued	New	Threat management	MDO		Jun 20, 2024 7:52 AM	Jun 20, 2024 7:53 AM	Not Set	Not
Email reported by user as not junk		Low	Queued	New	Threat management	MDO		Jun 19, 2024 11:59 AM	Jun 19, 2024 12:00 PM	Not Set	Not
Email reported by user as not junk		Low	Queued	New	Threat management	MDO		Jun 19, 2024 11:58 AM	Jun 19, 2024 11:58 AM	Not Set	Not
Email reported by user as not junk		Low	Queued	New	Threat management	MDO		Jun 19, 2024 11:59 AM	Jun 19, 2024 11:59 AM	Not Set	Not
Unsanctioned cloud app access was blocked		Low	New	Suspicious activity	Custom TI			Jun 19, 2024 11:04 AM	Jun 19, 2024 11:04 AM	Not Set	Not

# Incidents

- Sammlung von Alerts zusammenhängender Signals
- Erzählen eine “Story”

The screenshot shows the Microsoft Defender for Cloud interface under the 'Incidents & alerts' section. On the left is a navigation sidebar with various categories like Home, Incidents & alerts (selected), Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Secure score, Data connectors, Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Configuration management, and more. The main area is titled 'Incidents' and displays a table of 'Most recent incidents and alerts'. The table columns include: Incident name, Tags, Severity (with a color scale from green to red), Investigation state, Categories, Impacted assets, Active alerts, Service sources, Detection sources, First activity, and Last activity. There are 26 incidents listed, each with a detailed description and status. Some incidents are marked with 'Credential Phish' or 'Remediated' status. The table has sorting and filtering options at the top.

# Action Center: Single Pane of Glass

Home

Incidents & alerts

- Incidents
- Alerts

Hunting

- Advanced hunting
- Custom detection rules

Actions & submissions

- Action center
- Submissions

Threat intelligence

- Learning hub
- Triage
- Partner catalog

Exposure management

- Overview
- Attack surface
- Exposure insights
- Secure score
- Data connectors

Assets

- Devices
- Identities

Endpoints

- Vulnerability management
- Partners and APIs
- Configuration management

Identities

- Dashboard
- Health issues
- Tools

Email & collaboration

- Investigations

Action Center

Pending History Export

Action update time	Investigation ID	Action type	Details	Entity type	Asset	Decision	Status	Service name
Jun 24, 2024 7:01 PM	99e350	Soft delete emails	NormalizedURL("http://www.wordfence.com/z25/") and Content...	Email Cluster		Pending	Pending	
Jun 24, 2024 1:01 PM	99e350	Soft delete emails	NormalizedURL("http://www.wordfence.com/z25/") and Content...	Email Cluster		Pending	Pending	
Jun 24, 2024 6:41 PM	535890	Soft delete emails	NormalizedURL("http://www.wordfence.com/z25/") and Content...	Email Cluster		Pending	Pending	
Jun 24, 2024 6:41 PM	535890	Soft delete emails	NormalizedURL("http://www.wordfence.com/z25/") and Content...	Email Cluster		Pending	Pending	
Jun 24, 2024 6:41 PM	6d182a	Soft delete emails	NormalizedURL("http://www.wordfence.com/z25/") and Content...	Email Cluster		Pending	Pending	
Jun 24, 2024 6:41 PM	6d182a	Soft delete emails	NormalizedURL("http://www.wordfence.com/z25/") and Content...	Email Cluster		Pending	Pending	
Jun 23, 2024 6:21 AM	4ec302	Soft delete emails	NormalizedURL("https://... verify-account-case...")	Email Cluster		Pending	Pending	
Jun 23, 2024 6:21 AM	4ec302	Soft delete emails	NormalizedURL("https://... verify-account-case...")	Email Cluster		Pending	Pending	
Jun 23, 2024 6:15 AM	F53ff1	Soft delete emails	NormalizedURL("https://... verify-account-case...")	Email Cluster		Pending	Pending	
Jun 23, 2024 6:15 AM	f35ef1	Soft delete emails	NormalizedURL("https://... verify-account-case...")	Email Cluster		Pending	Pending	
Jun 22, 2024 6:15 PM	8294c2	Soft delete emails	From: info@mercedes.de Email [REDACTED]			Pending	Pending	
Jun 22, 2024 6:15 PM	8294c2	Soft delete emails	Subject:[wir gratulieren recht herzlich] and SenderIP("83.24...")	Email Cluster		Pending	Pending	
Jun 22, 2024 6:15 PM	8294c2	Soft delete emails	Subject:[wir gratulieren recht herzlich] and P25SenderDomain(...)	Email Cluster		Pending	Pending	
Jun 22, 2024 6:15 PM	8294c2	Soft delete emails	NormalizedURL("https://shorturl.at/2ICic") and ContentType(...)	Email Cluster		Pending	Pending	
Jun 22, 2024 4:52 PM	3269b0	Soft delete emails	Subject:[wir gratulieren recht herzlich] and SenderIP("83.24...")	Email Cluster		Pending	Pending	
Jun 22, 2024 4:52 PM	3269b0	Soft delete emails	NormalizedURL("https://shorturl.at/2ICic") and ContentType(...)	Email Cluster		Pending	Pending	
Jun 22, 2024 4:52 PM	3269b0	Soft delete emails	Subject:[wir gratulieren recht herzlich] and P25SenderDomain(...)	Email Cluster		Pending	Pending	
Jun 22, 2024 4:52 PM	3269b0	Soft delete emails	From: info@mercedes.de To: [REDACTED]			Pending	Pending	
Jun 21, 2024 9:44 AM	c1d77d	Soft delete emails	Subject:[WG: Die automatische Verlängerung der Domain gr...	Email Cluster		Pending	Pending	
Jun 21, 2024 9:44 AM	c1d77d	Soft delete emails	BodyFingerprintBin1("30352964999") and P25SenderDomain(...)	Email Cluster		Pending	Pending	
Jun 21, 2024 9:44 AM	c1d77d	Soft delete emails	NormalizedURL("https://...") and ContentType(...)	Email Cluster		Pending	Pending	
Jun 19, 2024 9:06 AM	259840	Soft delete emails	NormalizedURL("https://support.google.com/mail/?p=NoSuc...")	Email Cluster		Pending	Pending	
Jun 19, 2024 8:03 AM	98d227	Soft delete emails	NormalizedURL("https://support.google.com/mail/?p=NoSuc...")	Email Cluster		Pending	Pending	

Email notifications 23 items Customize columns Filter

# Submissions

Home

Incidents & alerts

Hunting

Actions & submissions

- Submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

- Overview
- Attack surface
- Exposure insights
- Secure score
- Data connectors

Assets

Devices

Endpoints

- Vulnerability management
- Configuration management

Email & collaboration

- Investigations
- Explorer
- Real-time detections
- Review
- Campaigns
- Threat tracker

## Submissions

Emails Email attachments URLs Files User reported

Totals for past 30 days

Pending Completed

0 2

+ Submit to Microsoft for analysis Export Refresh

Filters: Date submitted (UTC+02:00): 27/5/2024-25/6/2024

Submission name	Sender	Submitted by	Date submitted (UTC+02:00)	Reason
<input checked="" type="checkbox"/> Post & DHL Geschäftskundenportal - Passwort zurücksetzen	DHL Geschäftskundenportal <DHLGeschäfts...		17 Jun 2024 12:06	No threat found
<input type="checkbox"/> Fwd:			28 May 2024 10:11	No threat found

### Post & DHL Geschäftskundenportal - Pa...

✉ Open email entity ⚡ Take action 🛡 View alert

**Result details**

**Result**

No threats found. This item has been identified as clean. It might have been blocked for a variety of reasons (for example, sender reputation). To prevent similar items from being blocked in the future, you can create allow entries (domain or address, URL, file) in the Tenant Allow/Block List. After a period of evaluation, the filters might be updated using the information from the submission.

Recommended steps for email submissions

- Allow via Tenant Allow Block List
- View this message in Real-time detections
- Search for similar messages in Real-time detections

**Submission details**

Date submitted (UTC+02:00)  
17 Jun 2024 12:06

Submission name  
Post & DHL Geschäftskundenportal - Passwort zurücksetzen

Submission Type  
Email

Reason for submitting  
Not junk

Submission ID  
6f945548-fbd0-47df-7a8b-08dc8eb52ce2

Submitted by

Submission status  
Completed

**Allow details**

Name	Type
dhlgeschaeftskundenportal@deutschepost.de	Sender

**Delivery details**

Original Threats	Latest Threats
Phish / High	Phish / High

# Secure Scores

Advanced mining  
Custom detection rules

Actions & submissions ▾  
Action center  
Submissions

Threat intelligence ▾  
Learning hub

Trials

Partner catalog ▾

Exposure management ▾  
Overview  
Attack surface ▾  
Map  
Attack paths

Exposure insights ▾  
Initiatives  
Metrics  
Recommendations  
Events

Secure score

Data connectors

Assets ▾  
Devices  
Identities

Endpoints ▾

## Microsoft Secure Score

Overview Recommended actions History Metrics & trends

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

Applied filters:

Your secure score Include ▾

**Secure Score: 63.53%**  
1009.56/1509 points achieved

100%  
75%  
50%  
25%  
0%  
01/02 02/03 03/04 04/05 05/06 06/07 07/08 08/09 09/10 10/11 11/12 12/13 13/14 14/15 15/16 16/17 17/18 18/19 19/20 20/21 21/22 22/23 23/24 24/25 25/26 26/27 27/28 28/29 29/30 30/31 31/32 32/33 33/34 34/35 35/36 36/37 37/38 38/39 39/40 40/41 41/42 42/43 43/44 44/45 45/46 46/47 47/48 48/49 49/50 50/51 51/52 52/53 53/54 54/55 55/56 56/57 57/58 58/59 59/60 60/61 61/62 62/63 63/64 64/65 65/66 66/67 67/68 68/69 69/70 70/71 71/72 72/73 73/74 74/75 75/76 76/77 77/78 78/79 79/80 80/81 81/82 82/83 83/84 84/85 85/86 86/87 87/88 88/89 89/90 90/91 91/92 92/93 93/94 94/95 95/96 96/97 97/98 98/99 99/100

**Actions to review**

Regressed	To address	Planned	Risk accepted	Recently added
34	193	0	2	0
Recently updated	0			

**Comparison**

Your score	Organizations of a similar size
63.53 / 100	43.01 / 100

**History**

Date/Time	Activity
Jun 25, 2024 2:00 AM	0.01 points gained for Encrypt all BitLocker-supported drives because Syst...
Jun 25, 2024 2:00 AM	0.01 points gained for Disable the built-in Administrator account because ...
Jun 25, 2024 2:00 AM	0.04 points gained for Fix Microsoft Defender for Endpoint sensor data coll...
Jun 25, 2024 2:00 AM	0.02 points gained for Enable Microsoft Defender Antivirus email scanning...
Jun 24, 2024 2:00 AM	0.02 points gained for Block all Office applications from creating child proc...

**Top recommended actions**

Recommended action	Score impact	Status	Category
Create Safe Links policies for email messages	+0.57%	<input type="radio"/> To address	Apps
Turn on Microsoft Defender Antivirus PUA protection	+0.57%	<input type="radio"/> To address	Device
Turn on Microsoft Defender Antivirus PUA protection	+0.57%	<input type="radio"/> To address	Device
Turn on Microsoft Defender Application Guard management	+0.5%	<input type="radio"/> To address	Device
Disable 'Allow Basic authentication' for WinRM Client	+0.5%	<input type="radio"/> To address	Device
Enable 'Local Security Authority (LSA) protection'	+0.5%	<input type="radio"/> To address	Device
Set User Account Control (UAC) to automatically prompt for elevation	+0.5%	<input type="radio"/> To address	Device
Set LAN Manager authentication level to 'Send NTLM only'	+0.5%	<input type="radio"/> To address	Device

**Breakdown points by: Category**

Category	Percentage
Identity	73.3%
Data	55.56%
Device	65.79%
Apps	52.96%

Legend: Points achieved (dark blue), Opportunity (light grey)

[View all](#)

**Resources**

**Messages from Microsoft**

[Read about Secure Score capabilities](#)  
Learn about the recommended actions and how to improve your score.

[See recent blogs](#)

**Partner experience updates**

[Learn about temporary incompatibility with Identity Secure Score.](#)

# Vulnerability Management - Recommendations

Menu expanded. Select to collapse

## Security recommendations

41 discovered devices are not protected Onboard them now

5 devices exposed to CVE-2023-21716 (Microsoft Word Remote Code Execution) Learn more

5 devices exposed to CVE-2023-23397 (Microsoft Outlook Elevation of Privilege) Learn more

How well are you handling critical vulnerabilities? See key insights and metrics in your exposure management oversight page.

Export

534 items Filter by device groups (5/5)

Filter: Status: Active +1

Security recommendation	OS platform	Weaknesses	Related component	Threats	Exposed devices	Remediation type	Remediation activities	Impact	Tags
<input type="checkbox"/> Update Microsoft Teams	Windows	5	Microsoft Teams	295 / 517	<div style="width: 58.0%"></div>	Software update	0	▼ 18.29	+ 0
<input type="checkbox"/> Update Google Chrome	Windows	122	Google Chrome	634 / 656	<div style="width: 95.4%"></div>	Software update	0	▼ 17.02	+ 0
<input type="checkbox"/> Update Oracle Jre	Windows	727	Oracle Jre	179 / 256	<div style="width: 69.7%"></div>	Software update	0	▼ 8.83	+ 0 EOS versions
<input type="checkbox"/> Attention required: vulnerabilities in Openssl	Windows	31	Openssl	506 / 686	<div style="width: 74.1%"></div>	Attention Required	0	▼ 7.29	+ 0 EOS versions
<input type="checkbox"/> Update Adobe Acrobat Reader Dc to version 2024.2.20857.0	Windows	987	Adobe Acrobat Reader Dc	148 / 153	<div style="width: 96.7%"></div>	Software update	0	▼ 6.98	+ 0
<input type="checkbox"/> Update Fortinet Forticlient	Windows	10	Fortinet Forticlient	309 / 319	<div style="width: 97.4%"></div>	Software update	0	▼ 6.79	+ 0
<input type="checkbox"/> Update Google Chrome for Mac	Other	344	Google Chrome for Mac	242 / 261	<div style="width: 92.4%"></div>	Software update	0	▼ 6.64	+ 0
<input type="checkbox"/> Update 7-zip to version 24.7.0.0	Windows	9	7-zip	161 / 443	<div style="width: 36.0%"></div>	Software update	0	▼ 6.16	+ 0
<input type="checkbox"/> Update Mozilla Firefox Esr to version 115.12.0.0	Windows	442	Mozilla Firefox Esr	112 / 136	<div style="width: 82.6%"></div>	Software update	0	▼ 5.25	+ 0
<input type="checkbox"/> Attention required: vulnerabilities in Webmproject Libwebp	Windows	13	Webmproject Libwebp	80 / 80	<div style="width: 100.0%"></div>	Attention Required	0	▼ 4.96	+ 0
<input type="checkbox"/> Block persistence through WMI event subscription	Windows	1	Security controls (Attack Surface Reduction)	284 / 751	<div style="width: 37.4%"></div>	Configuration change	0	▼ 4.63	+ 3 User impact assessment
<input type="checkbox"/> Block untrusted and unsigned processes that run from USB	Windows	1	Security controls (Attack Surface Reduction)	276 / 795	<div style="width: 34.3%"></div>	Configuration change	0	▼ 4.69	+ 3 User impact assessment
<input type="checkbox"/> Block Adobe Reader from creating child processes	Windows	1	Security controls (Attack Surface Reduction)	276 / 795	<div style="width: 34.3%"></div>	Configuration change	0	▼ 4.69	+ 3 User impact assessment
<input type="checkbox"/> Update Adobe Acrobat Dc to version 2024.2.20857.0	Windows	323	Adobe Acrobat Dc	177 / 355	<div style="width: 49.4%"></div>	Software update	0	▼ 4.16	+ 0
<input type="checkbox"/> Block JavaScript or VBScript from launching downloaded executable content	Windows	1	Security controls (Attack Surface Reduction)	237 / 751	<div style="width: 31.5%"></div>	Configuration change	0	▼ 4.03	+ 2 User impact assessment
<input type="checkbox"/> Block executable files from running unless they meet a prevalence, age, or trusted list criterion	Windows	1	Security controls (Attack Surface Reduction)	461 / 795	<div style="width: 58.0%"></div>	Configuration change	0	▼ 3.97	+ 5 User impact assessment
<input type="checkbox"/> Update Microsoft Office	Windows	147	Microsoft Office	94 / 655	<div style="width: 14.4%"></div>	Software update	0	▼ 3.63	+ 0
<input type="checkbox"/> Update Mozilla Firefox for Mac	MacOs	762	Mozilla Firefox for Mac	96 / 171	<div style="width: 56.2%"></div>	Software update	0	▼ 3.40	+ 0 EOS versions +1

# Exposure Management - Recommendations

Home

Incidents & alerts

Incidents

Alerts

Hunting

Advanced hunting

Custom detection rules

Actions & submissions

Action center

Submissions

Threat intelligence

Learning hub

Trials

Partner catalog

Exposure management

Overview

Attack surface

Map

Attack paths

Exposure insights

Initiatives

Metrics

Recommendations

Events

Secure score

Data connectors

Assets

Devices

Identities

Endpoints

Vulnerability management

Dashboard

Recommendations

Remediation

Inventories

Weaknesses

Event timeline

## Recommendations

Complete cloud data is available for environments where Defender CSM is turned on. If it's missing, only partial cloud data will be displayed. Learn more

Export

Filters: State: Compliant + 3

298 items | Search | Filter

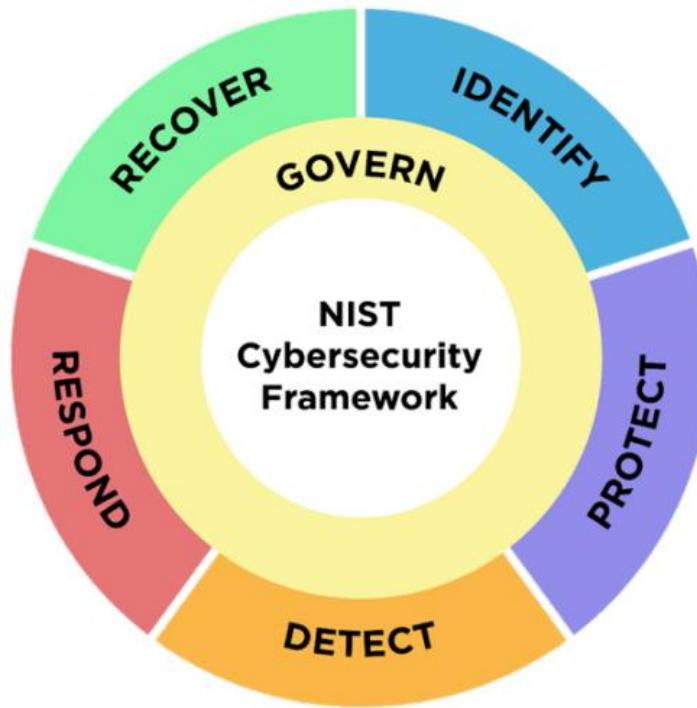
Name	State	Impact	Last calculated	Last state change	Related initiatives	Related metrics	Workload	Domain
Atlassian mobile app security - App access requirement	NOT COMPLIANT	■■■ Medium	Jun 25, 2024 1:11 AM	None in 90 days	-	-	Atlassian	Apps
Atlassian mobile app security - App data protection	NOT COMPLIANT	■■■ Medium	Jun 25, 2024 1:11 AM	None in 90 days	-	-	Atlassian	Apps
Atlassian mobile app security - Users that are affected by policies	COMPLIANT	■■■■ Low	Jun 25, 2024 1:11 AM	None in 90 days	-	-	Atlassian	Apps
Block abuse of exploited vulnerable signed drivers	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	4	1	Defender for Endpoint	Device
Block Adobe Reader from creating child processes	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	1	1	Defender for Endpoint	Device
Block all Office applications from creating child processes	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	15	2	Defender for Endpoint	Device
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	18	3	Defender for Endpoint	Device
Block executable content from email client and webmail	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	3	1	Defender for Endpoint	Device
Block executable files from running unless they meet a prevalence, age, or trusted list criterion	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	37	2	Defender for Endpoint	Device
Block execution of potentially obfuscated scripts	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	12	2	Defender for Endpoint	Device
Block Flash activation in Office documents	COMPLIANT	■■■ Medium	Jun 25, 2024 8:58 AM	None in 90 days	-	-	Defender for Endpoint	Device
Block JavaScript or VBScript from launching downloaded executable content	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	9	3	Defender for Endpoint	Device
Block Office applications from creating executable content	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	13	2	Defender for Endpoint	Device
Block Office applications from injecting code into other processes	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	6	2	Defender for Endpoint	Device
Block Office communication application from creating child processes	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	6	2	Defender for Endpoint	Device
Block OneDrive for Business sync from unmanaged devices	NOT COMPLIANT	■■■■ Low	Jun 25, 2024 7:57 AM	None in 90 days	1	1	SharePoint Online	Apps
Block outdated ActiveX controls for Internet Explorer	NOT COMPLIANT	■■■ Medium	Jun 25, 2024 8:58 AM	None in 90 days	-	-	Defender for Endpoint	Device
Block persistence through WMI event subscription	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	1	-	Defender for Endpoint	Device
Block process creations originating from PSEXEC and WMI commands	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	18	2	Defender for Endpoint	Device
Block untrusted and unsigned processes that run from USB	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	3	-	Defender for Endpoint	Device
Block users who reached the message limit	NOT COMPLIANT	■■■ Low	Jun 24, 2024 6:24 PM	None in 90 days	-	-	Defender for Office	Apps
Block Win32 API calls from Office macros	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	4	2	Defender for Endpoint	Device
Change service account to avoid cached password in windows registry	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	1	1	Defender for Endpoint	Device
Change service executable path to a common protected location	NOT COMPLIANT	■■■ High	Jun 25, 2024 8:58 AM	None in 90 days	1	1	Defender for Endpoint	Device
Configure VPN integration	COMPLIANT	■■■■ Low	Jun 24, 2024 8:53 PM	None in 90 days	3	2	Defender for Identity	Identity
Configure which users are allowed to present in Teams meetings	NOT COMPLIANT	■■■■ Low	May 28, 2024 8:34 PM	None in 90 days	-	-	Microsoft Teams	Apps
Configure which users can use the Microsoft 365 Cloud App Security feature	NOT COMPLIANT	■■■■ Low	Jun 25, 2024 5:57 AM	None in 90 days	2	2	Defender for Cloud	Cloud





... und jetzt?!

# Pragmatische IT-Security-Strategie für SMB



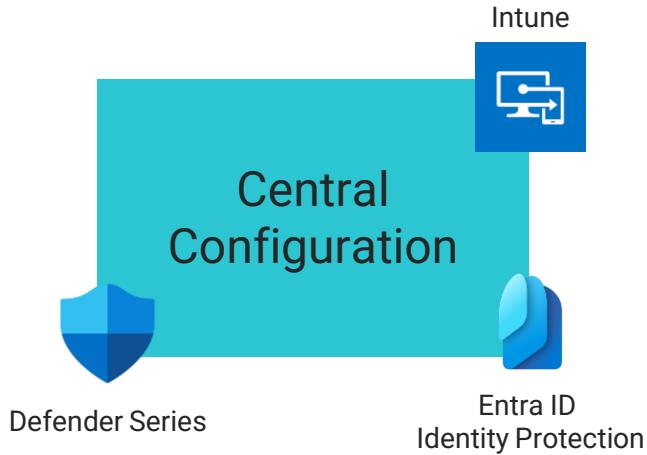
# Dimension “Configuration”



Update  
Deployment



Best  
Practices



Application  
Hardening



Identity  
Hardening



OS Hardening

# Dimension “Operations”



Alert &  
Incident  
Management



Defender Security  
Center



Vulnerability  
Monitoring



# Gängige Alerts & Incidents

# E-Mail reported as junk / not junk / malware / phish

The screenshot displays four alert cards side-by-side, each representing a different category of user-reported email incidents:

- Email reported by user as junk**: Shows a summary of alerts triggered when any email message is reported as junk by users. It includes an alert story and an activity list.
- Email reported by user as not junk**: Shows a summary of alerts triggered when email is reported as not junk.
- Email reported by user as malware or phish**: Shows a summary of alerts triggered when email is reported as malware or phish.
- Email reported by user as malware or phish** (Details): A detailed view of a specific alert for a malware or phish report. It includes an insight section, alert state, and alert details.

**Email reported by user as junk** (Leftmost Card):

- Alert story**: Summary of alerts triggered when any email message is reported as junk by users - V1.0.0.0.
- Activity list**:

Date (UTC)	Activity	User	Item	IP address
May 15, 2024 12:16 PM	UserSubmission	[REDACTED]	3f5c4230-74e8-4e81-2af0...	185. [REDACTED]
May 15, 2024 12:16 PM	UserSubmission	[REDACTED]	a392dbc1-4cee-4f76-42ca...	185. [REDACTED]

**Email reported by user as not junk** (Second Card):

- Alert story**: Summary of alerts triggered when email is reported as not junk.
- Activity list**: (Table structure identical to the first card)

**Email reported by user as malware or phish** (Third Card):

- Alert story**: Summary of alerts triggered when email is reported as malware or phish.
- Activity list**: (Table structure identical to the first card)

**Email reported by user as malware or phish** (Rightmost Card):

- 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

**Set Classification**
- Alert details**:

Category	MITRE ATT&CK Techniques
Threat management	T1566: Phishing
Detection source	Service source
MDO	Office 365
Detection technology	Generated on
-	May 14, 2024 10:24:16 AM
First activity	Last activity
May 14, 2024 9:19:00 AM	May 14, 2024 9:20:00 AM

# Atypical Travel

**Atypical travel**

Part of incident: Initial access incident involving one user. [View incident page](#)

2 ips

Technical Customercare

Alert story

Maximize

What happened

Sign-in from an atypical location based on the user's recent sign-ins. This risk event type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past b... [Read more](#)

This alert is triggered by an AAD IP detection [View detection page in Identity Protection](#)

Activities

Timeline Risky sign-in events

5/14/2024 3:56:35 AM

Attempted to sign-in from IP address 95.182.125.227

IP address 95.182.125.227

Sign-in location Zelenograd. Moskva. RU

Sign-in request Id 15b3c75d-4f41-43eb-bffc-87d92bd68300

Previous IP details Attempted to sign-in from IP address 95.223.76.237

Atypical travel

High Unknown Resolved

Manage alert Link alert to another incident ...

Alert state

Classification False positive Assigned to 75d91d9f-e300-4725-a109-3ef3a73419c7

Set Classification

Alert details

Category Initial access MITRE ATT&CK Techniques

Detection source AAD Identity Protection Service source Identity Protection

Generated on May 14, 2024 9:49:00 AM First activity May 14, 2024 3:56:35 AM

Last activity May 14, 2024 3:56:35 AM

Evidence

Entity Name	Remediation Status	Verdict
(v) 95.182.125.227	<span style="color: red;">○</span>	Suspicious
(v) 95.223.76.237	<span style="color: red;">○</span>	Suspicious

Alert description

# Unfamiliar sign-in properties

 Part of incident: Unfamiliar sign-in properties involving one user [View incident page](#)

Applicationsupport (31.4) ...

Alert story 

**What happened**

Sign-in with properties we have not seen recently for the given user. This risk event type considers past sign-in properties (e.g. device, location, network) to determine sign-ins with unfamiliar properties. The system stores properties of previous logins.

[Read more](#)

This alert is triggered by an AAD IP detection [View detection page in Identity Protection](#)

**Activities**

Timeline Risky sign-in events

5/16/2024 1:08:44 PM Attempted to sign-in from IP address 31.4. [REDACTED]

User name [REDACTED]  
User account [REDACTED]  
IP address [REDACTED]  
Sign-in location DE  
User Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0 OS/10.0.17763  
Sign-in request Id aea17e9c-3d67-4b64-9166-0d2123e01b00

**Unfamiliar sign-in properties**

High Unknown Resolved

Manage alert Link alert to another incident ...

**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 Not Set Assigned to Unassigned  
[Set Classification](#)

**Alert details**

Category MITRE ATT&CK Techniques  
Initial access T1078: Valid Account +1 More [View all techniques](#)

Detection source AAD Identity Protection Service source Identity Protection

Generated on May 16, 2024 1:48:47 PM First activity May 16, 2024 1:08:44 PM

Last activity May 16, 2024 1:08:44 PM

Evidence

# Anomalous Token

Part of incident: Anomalous Token involving one user [View incident page](#)

[REDACTED] 107.150.23.244

Tier 1 Support Engineer

Alert story

**What happened**

Anomalous token indicates that there are abnormal characteristics in the token such as token duration and authentication from unfamiliar IP address. Anomalous token indicates that there are abnormal characteristics in the token such as token duration... [Read more](#)

This alert is triggered by an AAD IP detection [View detection page in Identity Protection](#)

**Activities**

Timeline Risky sign-in events

5/30/2024 7:26:23 PM Attempted to sign-in from IP address 107.150 [REDACTED]

IP address	107.150.
Sign-in location	Atlanta, Georgia, US
Sign-in request Id	7dd43f29-5171-42c6-8ae0-99b57e77c500

**Anomalous Token**

**Anomalous Token** Medium | Unknown | New

Manage alert Link alert to another incident

**INSIGHT**

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

**Alert state**

Classification	Assigned to
Not Set	Unassigned
<a href="#">Set Classification</a>	

**Alert details**

Category	MITRE ATT&CK Techniques
Initial access	-
Detection source	Service source
AAD Identity Protection	Identity Protection
Generated on	First activity
May 31, 2024 6:00:38 AM	May 30, 2024 7:26:23 PM
Last activity	
May 30, 2024 7:26:23 PM	

**Evidence**

# Malware was blocker / hacktool was prevented

An active 'Wacatac' malware was blocked  
Microsoft Defender ATP detected 'Trojan:AndroidOS/ZkarletFlash' malware

'Crack' hacktool was prevented

Part of incident: 'Crack' hacktool was prevented on one endpoint. View incident page

Risk level: Low

Windows11 Internal IT - Clients

Alert story

Process tree

Alert timeline

10:48:40 PM [14948] IDMan.exe /onboot

6/9/2024 11:51:14 AM [20012] BingWallpaperApp.exe

12:21:23 PM [30224] Terminus.exe

explorer.exe interacted with file URET NFO v2.2.exe

Quickly classify this alert

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

Classify alert

Classification: Not Set

Assigned to: Unassigned

Set Classification

Alert details

Category: Malware

MITRE ATT&CK Techniques: -

Detection source: Antivirus

Service source: Microsoft Defender for Endpoint

Detection status: Prevented

Detection technology: Client

Generated on: Jun 9, 2024 12:25:33 PM

First activity: May 24, 2024 7:00:25 PM

MITRE ATT&CK Techniques: -

Service source: Microsoft Defender for Endpoint

Detection technology: Client,Cloud,MachineLearning

First activity: May 24, 2024 7:00:25 PM

Microsoft Defender ATP detected 'Trojan:AndroidOS/ZkarletFlash' malware

Medium | Detected | Resolved

See in timeline | Tune alert

Recommendations

Actions you should take

Based on your alert classification

Assigned to: [Redacted]

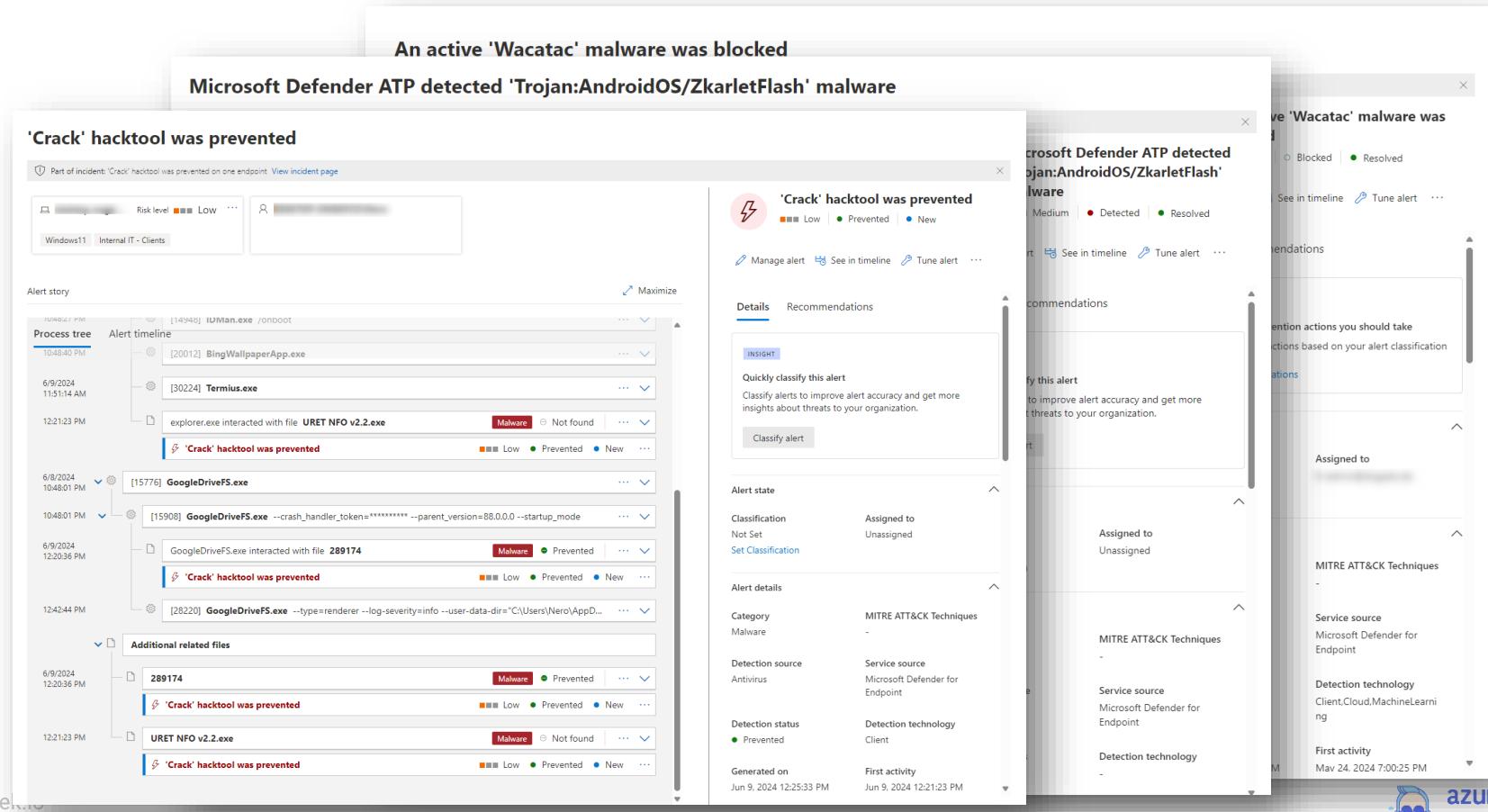
MITRE ATT&CK Techniques: -

Service source: Microsoft Defender for Endpoint

Detection technology: Client,Cloud,MachineLearning

First activity: May 24, 2024 7:00:25 PM

azuregeek.io



# Activity from TOR IP

## Activity from a Tor IP address

⚠ Part of incident: Activity from a Tor IP address involving one user [View incident page](#)

🔍 Priority ▲ 5 (89.58.26.216) Microsoft 365

Senior Software Developer II

Alert story Maximize

What happened

The Tor IP address 89.58.26.216 was accessed by [REDACTED]

Important information:

- Germany was visited for the first time in 180 days by this user.
- ISP netcup gmbh was used for the first time in 180 days by this user.

Activity from a Tor IP address

⚡ Medium Unknown New

Manage alert Link alert to another incident

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  
[Set Classification](#)

Alert details

Category MITRE ATT&CK Techniques  
Defense evasion T1078: Valid Acc... +1 More  
[View all techniques](#)

Detection source Service source  
Microsoft Defender for Microsoft Defender for  
Cloud Apps Cloud Apps

Detection status Detection technology  
Unknown -

Generated on First activity  
Apr 26, 2024 6:37:33 PM Apr 26, 2024 6:30:23 PM

# Connection to adversary-in-the-middle (AiTM) phishing Site

Part of incident: Connection to adversary-in-the-middle (AiTM) phishing site on multiple endpoints [View incident page](#)

Windows10 Internal IT - Clients

Alert story

Process tree Alert timeline

4/30/2024 7:53:05 AM [7488] userinit.exe

7:53:05 AM [11168] explorer.exe

11:19:42 AM [8644] OUTLOOK.EXE

7:43:54 PM [13444] chrome.exe --single-argument https://postoffice.adobe.com/po-server/link/redirect?target=...

7:43:55 PM [15684] chrome.exe --type=utility --utility-sub-type=network.mojom.NetworkService --lang=de...

7:44:27 PM [15684] chrome.exe... Outbound connection from 10.0.0.10:50159 to 188.114.96.10:4...

Connection to adversary-in-the-middle (AiTM) phishing site (True positive)

Manage alert See in timeline Tune alert

Connection to adversary-in-the-middle (AiTM) phishing site

High | Detected | Resolved

Details Recommendations

RECOMMENDATIONS

Remediation & prevention actions you should take  
See recommended actions based on your alert classification  
[View all recommendations](#)

Alert state

Classification True positive Assigned to

Set Classification

Alert details

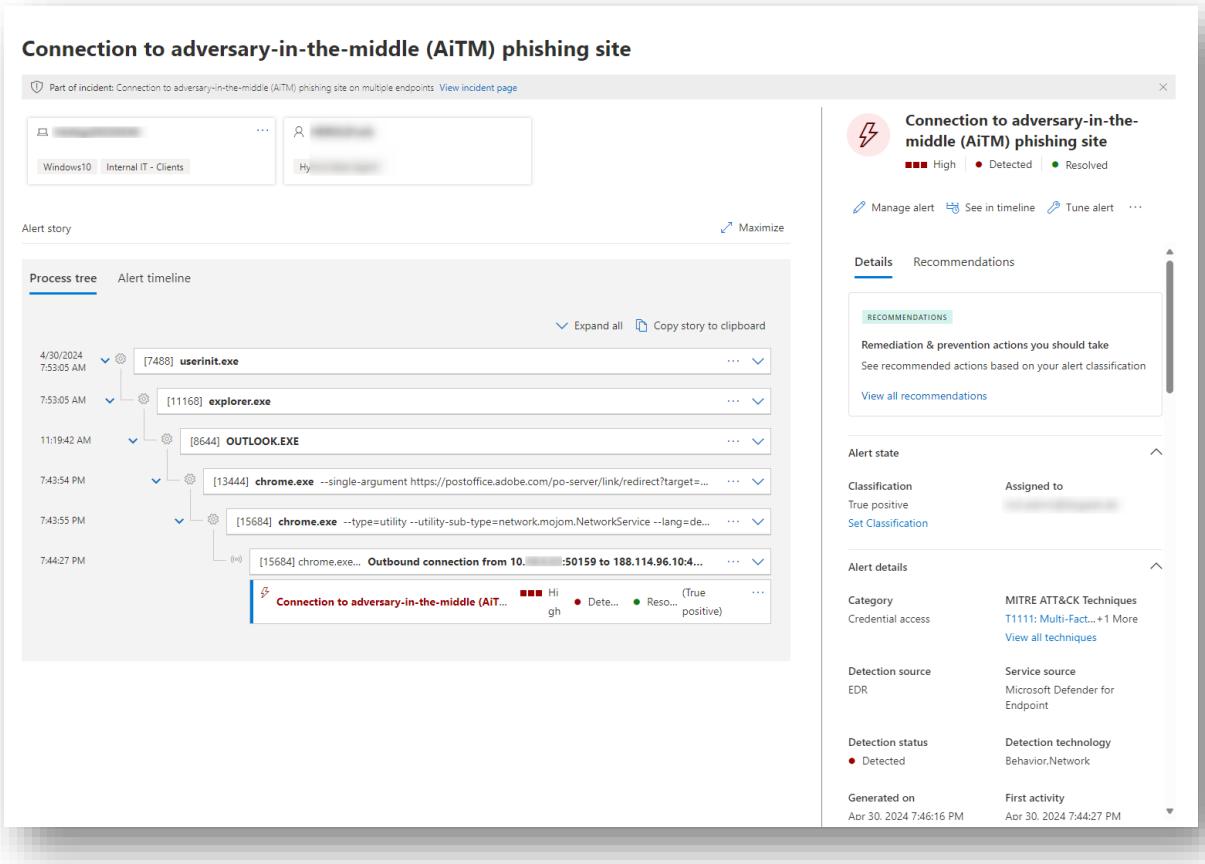
Category MITRE ATT&CK Techniques T1111: Multi-Factor Authentication

Credential access View all techniques

Detection source Service source EDR Microsoft Defender for Endpoint

Detection status Detection technology ● Detected Behavior:Network

Generated on First activity Apr 30, 2024 7:46:16 PM Apr 30, 2024 7:44:27 PM



# Kritische Alerts: AD CS Attack tool, DPAPI, etc.

Active Directory Certificate Services attack tool activity

Suspicious PowerShell command line

Part of incident: desktop - Windows11

Process tree

Alert timeline

11:28:20 AM [23168] netsh.exe  
11:28:38 AM [23168] netsh.exe created file 0x21.pif  
11:28:38 AM [996] 0x21.pif  
11:28:59 AM 0x21.pif attempted to decrypt credentials  
11:28:59 AM 0x21.pif accessed browser saved passwords file Login Data  
11:28:59 AM 0x21.pif accessed browser web data file Web Data  
11:30:40 AM 0x21.pif accessed browser saved passwords file Login Data

Possible theft of passwords and other sensitive web browser information  
Suspicious DPAPI Activity  
Possible theft of passwords and other sensitive web browser information  
Possible theft of passwords and other sensitive web browser information  
Possible theft of passwords and other sensitive web browser information  
Possible theft of passwords and other sensitive web browser information

High (Detected) | Resolved (True positive)

Back to alert details

PurpleKnight.exe executed a script

AMSI Content

Script

```
function Test-RODCPrivilegedCreds {  
    [CmdletBinding()]  
    [CmdletBinding()]
```

# Advanced Hunting - USB

Advanced hunting

New query +

Schema Functions Queries ...

Search

Alerts & behaviors

- AlertEvidence
- AlertInfo
- BehaviorEntities
- BehaviorInfo

Apps & identities

- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- CloudAppEvents
- IdentityDirectoryEvents
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents

Email & collaboration

- EmailAttachmentInfo
- EmailEvents
- EmailPostDeliveryEvents
- EmailUrlInfo
- UriClickEvents

Devices

- DeviceEvents
- DeviceFileCertificateInfo
- DeviceFileEvents
- DeviceImageLoadEvents

Run query Last 30 days Save Share link

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

14 InitiatingProcessAccountName,InitiatingProcessAccountUpn,  
15 FileName,FolderPath,SHA256,TimeStamp,SensitivityLabel,IsAzureInfoProtectionApplied  
16 | order by DeviceId asc, Timestamp desc;  
17 FileCreation | lookup kind=inner (UsbDriveMount) on DeviceId  
18 | where FolderPath startsWith DriveLetter  
19 | where Timestamp >= MountTime  
20 | order by DeviceId asc, Timestamp desc

Don't want to see it again

Getting started Results Query history

Export 28196 items 00:01:54 Search Chart type Customize columns

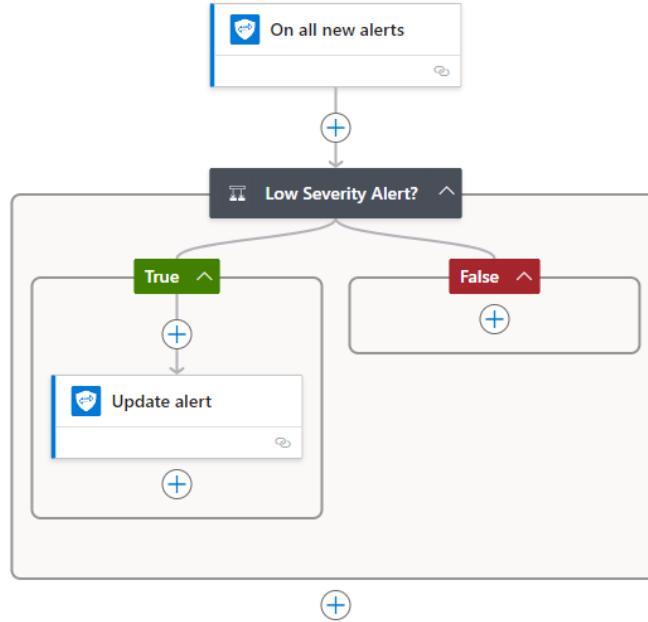
FileName	FolderPath	SHA256	Timestamp
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:19 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:19 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
Screensho	... D:\Smartphone Datensicherung'		Jun 22, 2024 7:23:18 AM
20171123,	D:\Smartphone Datensicherung'		Jun 22, 2024 7:21:41 AM
20171123,	D:\Smartphone Datensicherung'		Jun 22, 2024 7:21:41 AM
20171123,	D:\Smartphone Datensicherung'		Jun 22, 2024 7:21:41 AM
20171123,	D:\Smartphone Datensicherung'		Jun 22, 2024 7:21:41 AM



# Automatisierung

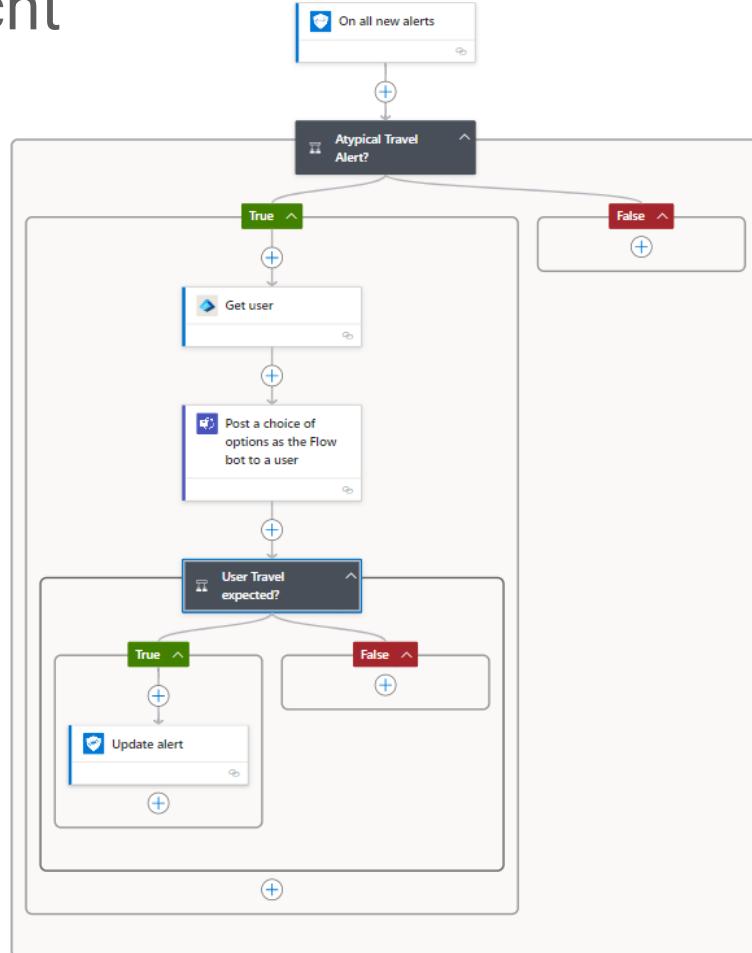
# Auto Close für Informational Messages

- Trigger: neuer Alert
- Bedingung: Alert von Severity "Informational"
- Aktion: Alert schließen



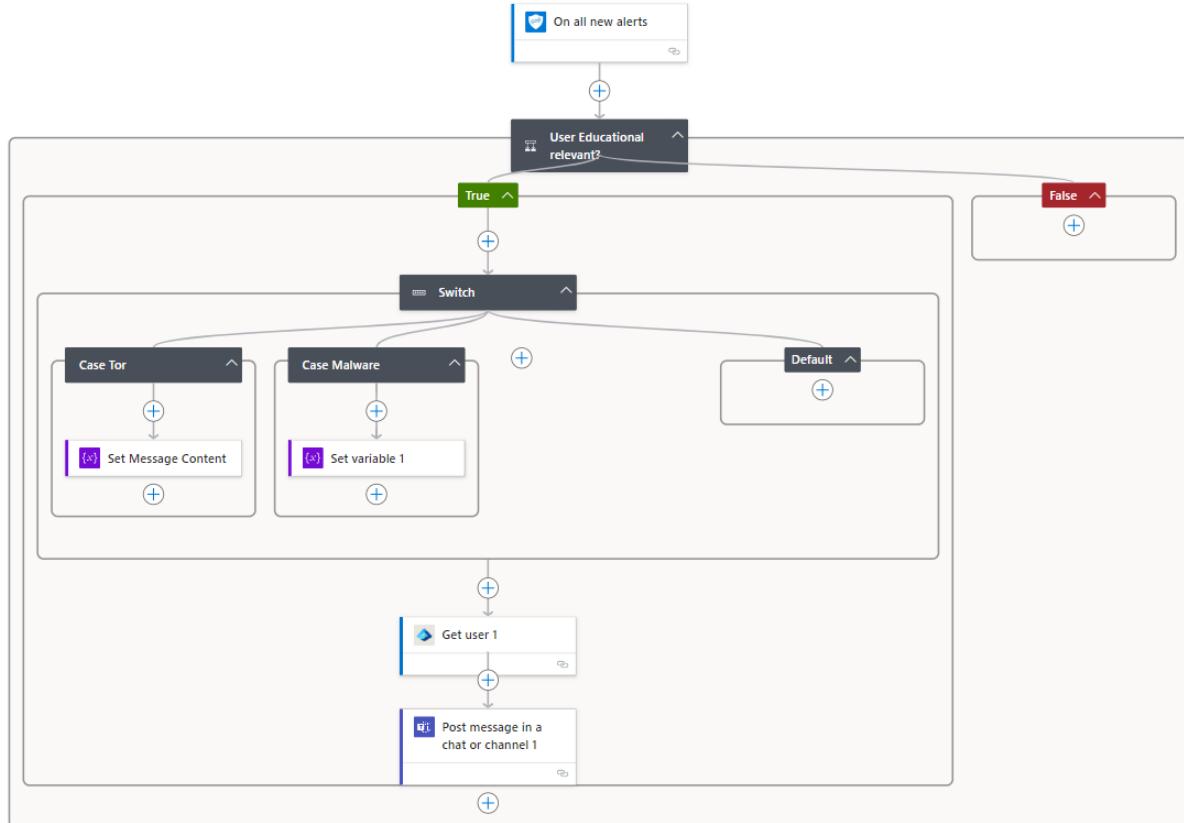
# Atypical Travel – Teams-Nachricht an Manager

- Trigger: neuer Alert
- Bedingung: Alert vom Typ atypical Travel
- Aktionen:
  - Nutzer aus Entra ID abrufen
  - Manager fragen, ob Nutzer wirklich im Land
  - Alert ggf. schließen



# Phishing / Tor-Nutzung / Unwanted Software: Info an User

- Trigger: neuer Alert
- Bedingung: diverse Alert-Typen
- Aktion: Nutzer per Teams über Erkennung informieren und bitten, Aktion zukünftig zu unterlassen



# Vielen Dank für eurer Interesse! Fragen?

Gerne stehe ich bei Fragen, Ideen und zur Diskussion zur Verfügung

