

ZOLDER

ATTACKING & DEFENDING MICROSOFT 365

07-04-2022

applied security research



WHOAMI

- Rik van Duijn
 - Ethical hacker
 - OSCP / OSCE
 - 8+ years of experience
 - Cybercrime / Malware analysis

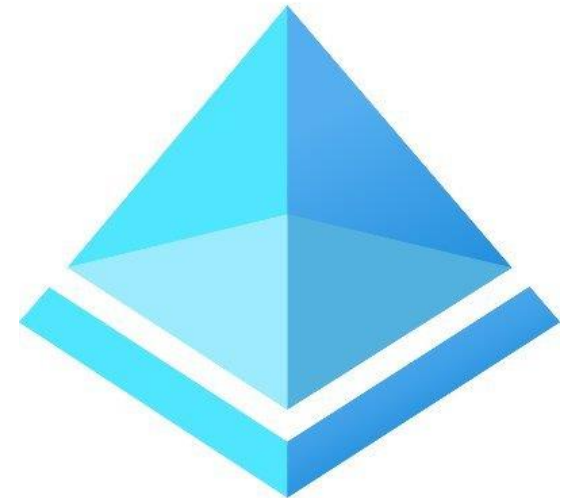


OVER
ONS



MICROSOFT 365

Microsoft 365 is meer dan e-mail...



VOOR- EN NADELEN

Voordelen:

- Onderhoud en patches worden gedaan door Microsoft
- Microsoft levert de tenant zo secure mogelijk op
- Microsoft heeft veel security budget

Nadelen:

- Je bent niet volledig in control
- Afhankelijk van Microsoft (voorbeeld: sign-in logs)

Vanuit security perspectief is het niet 'kopen en klaar':

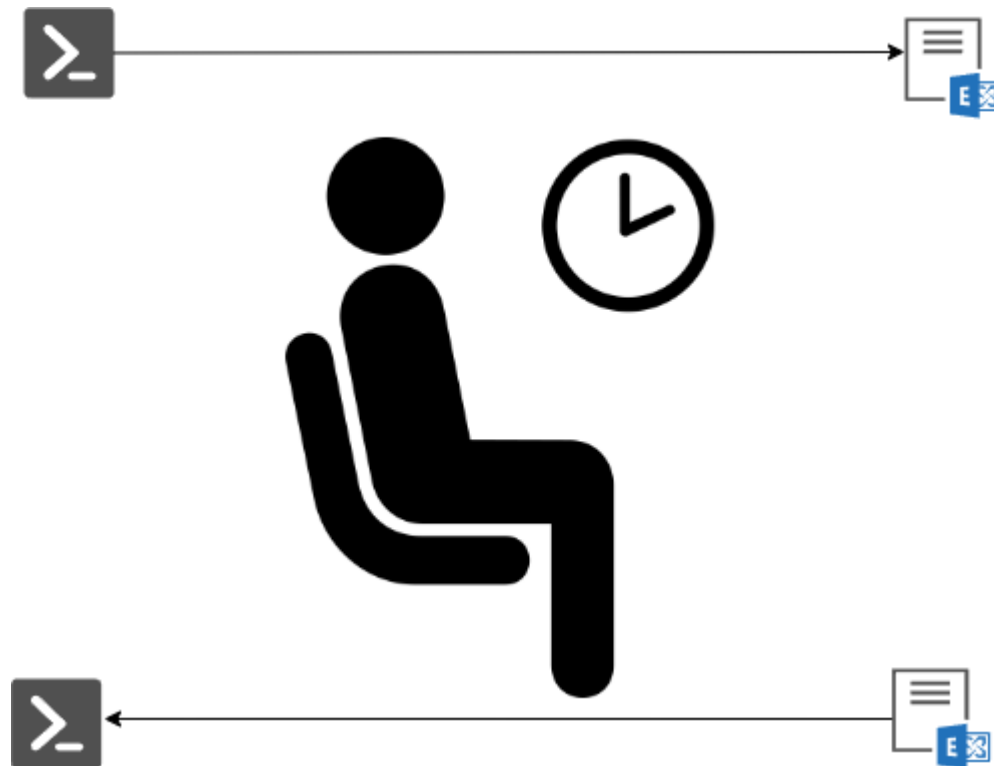
- Configuratie op je specifieke situatie aanpassen
- Monitoring inregelen

NIEUWE PROBLEMEN



There is no cloud
it's just someone else's computer

CLOUDSYNC



CLOUDDRIFT

Settings van vandaag kunnen met de features van morgen gebroken worden.

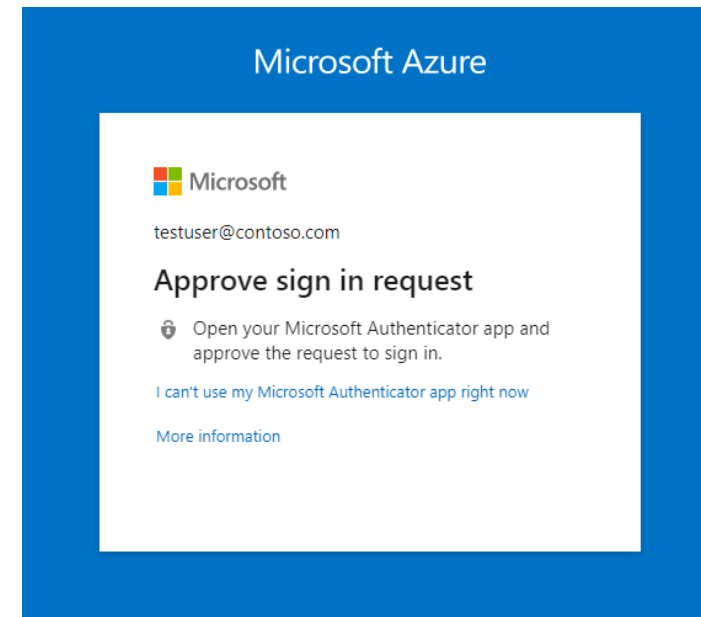
Twilio (Example Account)

765 286



Segment (Example Account)

003 457



PATTERN MATCHING

Microsoft Azure



rik@zolder.ms

Aanmeldingsaanvraag goedkeuren

- Open uw Authenticator-app en voer het nummer in dat wordt weergegeven om u aan te melden.

56

Ziet u geen cijfers in de app? Voer een upgrade naar de nieuwste versie uit.

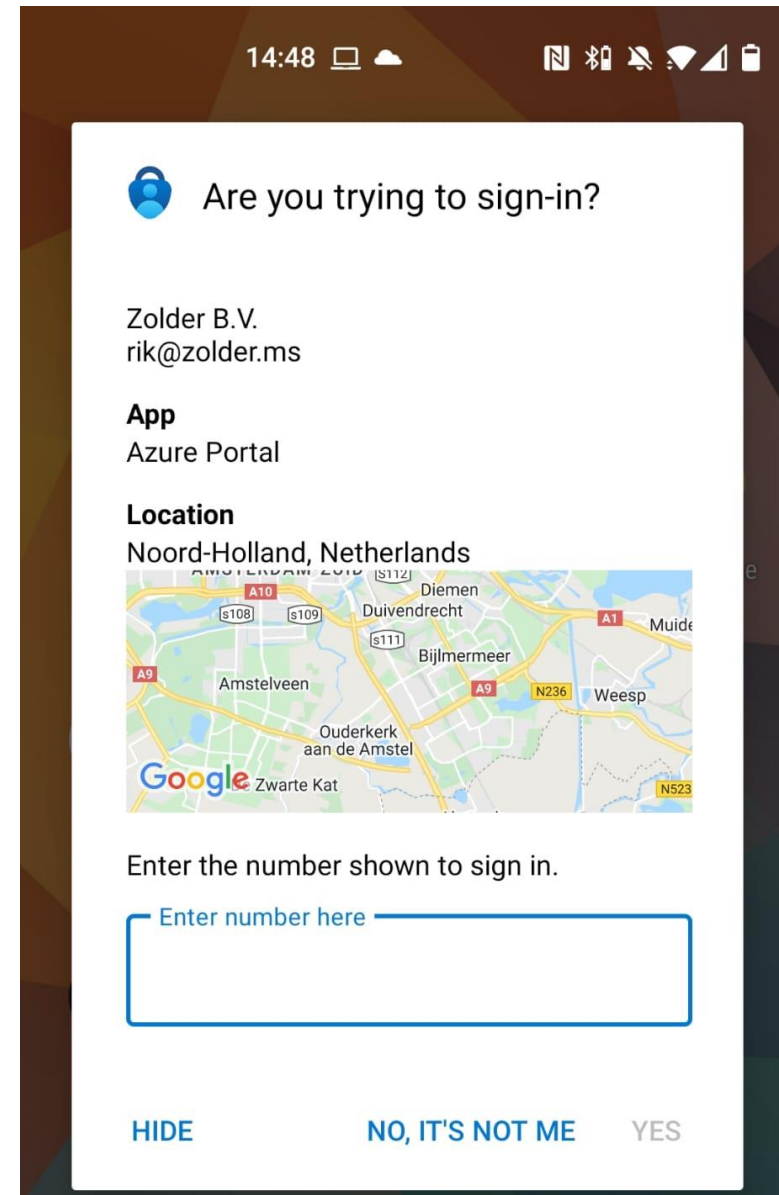
 Niet opnieuw vragen gedurende 60 dagen

Ik kan mijn Microsoft Authenticator-app op dit moment niet gebruiken

[Meer informatie](#)

PATTERN MATCHING

- Aanvallers spammen slachtoffers bij traditionele push.
- Belastingdienst als voorbeeld.



FRAUD DETECTION

Microsoft Azure



acid.burn@kelder.io

Aanvraag geweigerd

Er is een aanvraag voor identiteitverificatie verzonden naar uw mobiele apparaat, maar u hebt de aanvraag geweigerd. [Details weergeven](#)

[Een nieuwe aanvraag verzenden naar mijn Microsoft Authenticator-app](#)

Hebt u problemen?

In plaats hiervan moet u [een beveiligingscode invoeren](#) uit uw Microsoft-account of de Microsoft Authenticator-app.

Als u een app op dit moment niet kunt gebruiken, [gebruikt u een andere methode om een code te verkrijgen](#).

[Meer informatie](#)

Annuleren

CONFIGURATIE

Microsoft Azure Search resources, services, and docs (G+)

Home > Kelder.io > Security > Multi-Factor Authentication

Multi-Factor Authentication | Fraud alert

Save Discard | Got feedback?

- Getting started
- Diagnose and solve problems

Settings

- Account lockout
- Block/unblock users
- Fraud alert**
- Notifications
- OATH tokens
- Phone call settings
- Providers

Fraud alert

Allow your users to report fraud if they receive a two-step verification request that they didn't initiate.

Allow users to submit fraud alerts

On Off

Automatically block users who report fraud

On Off

Code to report fraud during initial greeting *

✓

DETECTIE

▶ Run | Time range: Last 7 days | Save | Share | + New alert rule | ...

```
1 AuditLogs
2 | where OperationName contains "Fraud reported"
3 | extend user = InitiatedBy.user.userPrincipalName
```

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00) | ...

Completed. Showing results from the last 7 days. 00:00.3 2 records

	TimeGenerated [UTC]	user	ResourceId
>	22-10-2021 13:58:21.707	acid.burn@kelde...	/tenants/f0020f3d-a0f8-44c7-b466-6f0df88dc9
>	22-10-2021 14:01:02.979	acid.burn@kelde...	/tenants/f0020f3d-a0f8-44c7-b466-6f0df88dc9

16:10

< RULE-1126
Detect fraud report by user

Detecteert wanneer een gebruiker via de authenticator app aangeeft dat een login mogelijk niet legitiem is.

! Check meldde een fout

kelder.io

Oct 22, 2021, 11:15:20 AM

Oct 22, 2021, 3:15:20 PM

Laatste resultaten

! Oct 22, 2021, 1:58:21 PM

De volgende gebruikers hebben een inlogpoging afgebroken:

- acid.burn@kelder.io

SHAREPOINT SITES

=

SMB SHARES

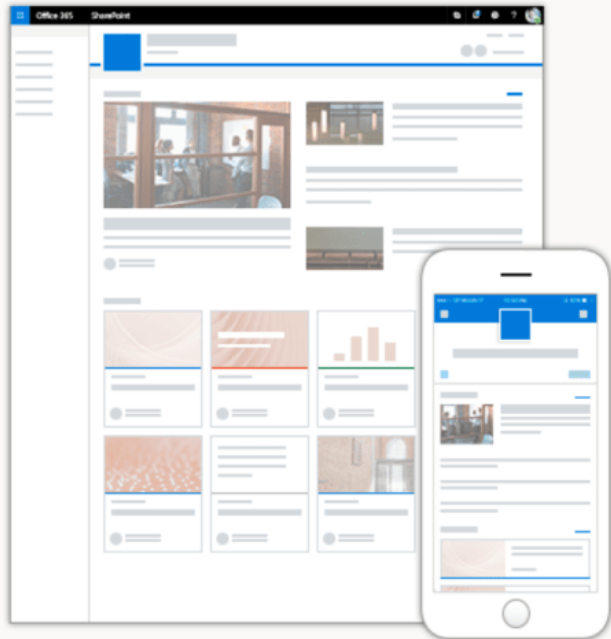
SMB SHARES

```
root@kali:~# smbmap -H 10.0.2.30
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.0.2.30...
[+] IP: 10.0.2.30:445    Name: 10.0.2.30
    Disk                               Permissions
    ----                               -
    print$                             NO ACCESS
    tmp                                 READ, WRITE
    opt                                 NO ACCESS
    IPC$                                NO ACCESS
    ADMIN$                              NO ACCESS
```

SHAREPOINT SITES

Get a team site connected to Microsoft 365 Groups

Use this design to collaborate with your team. Share documents, track events in a shared calendar, and manage project tasks.



Site name

The site name is available.

Group email address

The group alias is available.

Site address

<https://kelderio.sharepoint.com/sites/Example>

The site address is available.

Site description

Tell people the purpose of this site

Privacy settings

Private - only members can access this site

Public - anyone in the organization can access this site

Private - only members can access this site

The screenshot shows the Microsoft Teams management interface. On the left, there's a sidebar with navigation icons for 'Activiteit', 'Chat', 'Teams', 'Agenda', and 'Bestanden'. The main area is titled 'Microsoft Teams' and contains a search bar and a list of teams. The 'Teams' list shows three teams: 'wat een top team dat va...', 'testrik', and 'PublicTestSite'. The 'PublicTestSite' team is selected, and a dialog box titled 'Wat voor soort team is dit?' is open. The dialog box has three options: 'Privé' (Private), 'Openbaar' (Public), and 'hele-organisatie' (Entire organization). The 'Privé' option is selected. Below the dialog box, there's a 'Terug' (Back) button.

SHAREPOINT SITES

← geheim



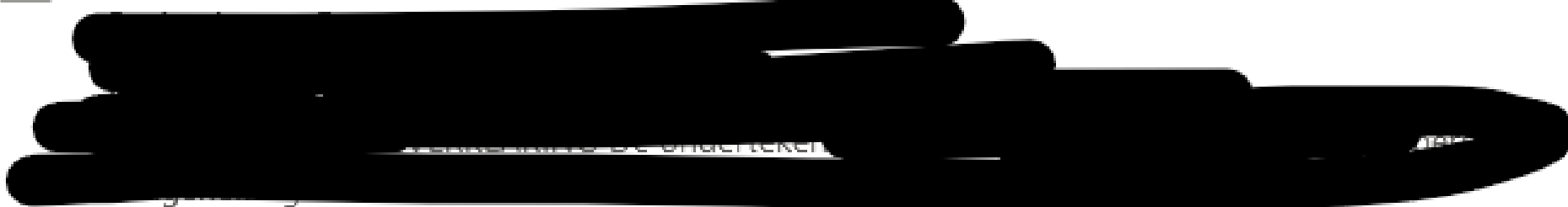
All Files Sites People News Images Power BI

Feedback

Filters File type ▾ Last modified ▾



202107 Geheimhoudingsverklaring [REDACTED]



algemene-voorwaarden-saas-157277 (1)



VINDEN SITES

Active sites

Use this page to sort and filter sites and manage site

+ Create Edit Permissions

Site name	URL
Communicatiesite	https://k
Message center	.../sites/M
PRIVATE	.../sites/P
PUBLIC TEAMS SITE	.../sites/P
PUBLIC TEAMS SITE NR2	.../sites/P
sadfssdsdsdf	.../sites/s
sdvsdf	.../sites/s
test	.../sites/t
testeee	.../sites/t


PUBLIC TEAMS SITE

General Activity **Permissions** Policies

For info about each role, [learn more](#).

Site admins (1)

Microsoft 365 Group owners

 **Acid Burn**
acid.burn@kelder.io

[Manage](#)

Additional admins

None

[Manage](#)

Site owners (1)

Site members (2)

 lederen behalve externe gebr...  **PUBLIC TEAMS SITE - Leden**
PUBLICTEAMSSITE@kelderio.onmi

Site visitors (0)

```
Windows PowerShell x Windows PowerShell x | + v - □ x
PS C:\Users\WesleyNeelen> Get-SPOSite | ForEach-Object { try { $res = Get-SPOSiteGroup -Site $_.url | Where-Object { $_.Users -Match "spo-grid-all-users"; if ($res -ne $null) { write-host $_.url } } Catch {} }
https://kelderio.sharepoint.com/sites/test
https://kelderio.sharepoint.com/sites/Messagecenter
https://kelderio.sharepoint.com/sites/sadfssdsdsdf
https://kelderio.sharepoint.com/portals/Community
https://kelderio.sharepoint.com/portals/hub
https://kelderio.sharepoint.com/sites/PUBLICTEAMSSITE
https://kelderio.sharepoint.com/
https://kelderio.sharepoint.com/sites/PUBLICTEAMSSITENR2
https://kelderio.sharepoint.com/sites/testeee
PS C:\Users\WesleyNeelen> |
```

DETECTEREN NIEUWE SITES

Run Time range: Last 24 hours Save Share + New alert rule Export Pin to dashboard Format query

```

1 let Translations = dynamic([
2   "Everyone except external users",
3   "Iedereen behalve externe gebruikers"
4 ]);
5 OfficeActivity
6 | where OfficeWorkload == "SharePoint" or OfficeWorkload == "OneDrive"
7 | where Operation == "AddedToGroup"
8 | project TimeGenerated, Operation, UserId, Site_Url, TargetUserOrGroupName
9 | where TargetUserOrGroupName in (Translations)

```

Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours.

TimeGenerated [UTC]	Operation	UserId	Site_Url	TargetUserOrGroupName
9-9-2021 13:47:29.000	AddedToGroup	chris.burn@kelde...	https://kelderio.sharepoint.com/sites/C...	ledereen behalve externe gebu...

```

1 $query = Invoke-WebRequest -Method GET -Uri 'https://graph.microsoft.com/v1.0/groups' -ContentType "application/json" -Headers $Headers -ErrorAction Stop -UseBasicParsing
2 $groups = $query | Select-Object -ExpandProperty content | ConvertFrom-Json
3 foreach ($group in $groups.value) {
4   if($group.proxyAddresses -match "SPO_"){
5     if($group.Visibility -eq "Public"){
6       Write-Host "SharePoint site $($group.displayName) is public."
7     }
8   }
9 }

```

APP CONSENT PHISHING



acid.burn@kelder.io

Permissions requested

DemoApp
kelder.io

This application is not published by Microsoft.

This app would like to:

- ✓ Read and write to your mailbox settings
- ✓ Sign you in and read your profile
- Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

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

Cancel

Accept

CONFIGURATIE


[Home](#) > [Kelder.io](#) > [Enterprise applications](#) >

Consent and permissions | User consent settings ...



 Save  Discard |  Got feedback?

Manage

 User consent settings

 Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- Do not allow user consent
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Allow user consent for apps
All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

- Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.
- Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.
- Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

DETECTIE

```
New Query 1* x +
sentinel [Run] Time range: Set in query [Save] [Share] [New alert rule] [Export] [Pin to dashboard] [Format query]

1 let detectionTime = 7d;
2 let joinLookback = 14d;
3 AuditLogs
4 | where TimeGenerated > ago(detectionTime)
5 | where LoggedByService =~ "Core Directory"
6 | where Category =~ "ApplicationManagement"
7 | where OperationName =~ "Consent to application"
8 | extend AppDisplayName = TargetResources.[0].displayName
9 | extend AppClientId = tolower(TargetResources.[0].id)
10 | extend ConsentFull = TargetResources[0].modifiedProperties[4].newValue
11 | parse ConsentFull with * "ConsentType: " GrantConsentType ", Scope: " GrantScope1 "]" *
12 | where ConsentFull contains "Directory.ReadWrite.All" and ConsentFull contains "Domain.ReadWrite.All" or ConsentFull contains "EAS.AccessAsUser.All" or ConsentFull contains "Group.ReadWrite" or ConsentFull contains "Organization.ReadWrite.All" or ConsentFull contains "User.ReadWrite.All" or ConsentFull contains "DeviceManagementConfiguration.ReadWrite.All"
13 | extend GrantIpAddress = toString(iff(isnotempty(InitiatedBy.user.ipAddress), InitiatedBy.user.ipAddress, InitiatedBy.app.ipAddress))
14 | extend GrantInitiatedBy = toString(iff(isnotempty(InitiatedBy.user.userPrincipalName), InitiatedBy.user.userPrincipalName, InitiatedBy.app.displayName))
15 | extend GrantUserAgent = toString(iff(AdditionalDetails[0].key =~ "User-Agent", AdditionalDetails[0].value, ""))
16 | project TimeGenerated, GrantConsentType, GrantScope1, GrantInitiatedBy, AppDisplayName, GrantIpAddress, GrantUserAgent, AppClientId, OperationName, ConsentFull, CorrelationId
17 | join kind = leftouter (AuditLogs
18 | where TimeGenerated > ago(joinLookback)
19 | where LoggedByService =~ "Core Directory"
20 | where Category =~ "ApplicationManagement"
21 | where OperationName =~ "Add service principal"
22 | extend AppClientId = tolower(TargetResources[0].id)
23 | extend AppReplyURLs = iff(TargetResources[0].modifiedProperties[1].newValue has "AddressType", TargetResources[0].modifiedProperties[1].newValue, "")
24 | distinct AppClientId, toString(AppReplyURLs)
25 )
26 on AppClientId
27 | join kind = innerunique (AuditLogs
28 | where TimeGenerated > ago(joinLookback)
29 | where LoggedByService =~ "Core Directory"
30 | where Category =~ "ApplicationManagement"
31 | where OperationName =~ "Add OAuth2PermissionGrant" or OperationName =~ "Add delegated permission grant"
32 | extend GrantAuthentication = toString(TargetResources[0].displayName)
33 | extend GrantOperation = OperationName
34 | project GrantAuthentication, GrantOperation, CorrelationId
35 ) on CorrelationId
36 | project TimeGenerated, GrantConsentType, GrantScope1, GrantInitiatedBy, AppDisplayName, AppReplyURLs, GrantIpAddress, GrantUserAgent, AppClientId, GrantAuthentication, OperationName
37 | extend timestamp = TimeGenerated, AccountCustomEntity = GrantInitiatedBy, IPCustomEntity = GrantIpAddress
38
```

Schema and Filter

Results Chart Columns Add bookmark Display time (UTC+00:00) Group columns

Completed	TimeGenerated [UTC]	GrantInitiatedBy	AppDisplayName	AppReplyURLs	GrantIpAddress	GrantUserAgent	AppClientId
>	18-10-2021 14:06:00.563	acid.burn@kelder.io	DemoApp	[{"AddressType":0,"Address":"http://localhost","ReplyAddressClie...	20.67.242.110	EvoSTS	2ef89ebc-13dd-4b9c-bba

11:45 [Signal] [Battery]

< **RULE-1122**
Detect app consent with specific permis

Detecteert wanneer gebruikers apps toevoegen met, door ons geselecteerde verdachte permissies.

Check meldde een fout

kelder.io

Oct 22, 2021, 6:07:59 AM

Oct 22, 2021, 10:07:59 AM

Oct 18, 2021, 2:06:00 PM

De gebruiker [acid.burn@kelder.io](#) heeft de OAuth app DemoApp toegevoegd. Deze app heeft de volgende rechten verkregen:

- MailboxSettings.ReadWrite
- User.Read



GUEST INVITES

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

GUEST INVITE HIJACK



TL;DR

- Every user could query for non-redeemed invites.
- Could redeem invite without any validation, link to arbitrary external account.
- No way for admins to find out which account it was actually linked to.

Dirk-Jan

@_dirkjan

MONITORING

Als je Microsoft 365 gebruikt, **zet Sentinel dan aan**

Gratis voor specifieke logs:

- Azure activity
- Office 365
 - Exchange
 - Teams
 - Sharepoint

90-day retentie

Audit logging moet ook nog expliciet aangezet worden (<https://zolder.io/2020/05/13/office-365-exchange-rules/>)



CONCLUSIE

- Finetune de security configuratie van Microsoft 365
- Maak gebruik van Sentinel en de gratis logopslag (al is het voor IR/Forensics)

Getoonde rules zelf implementeren?

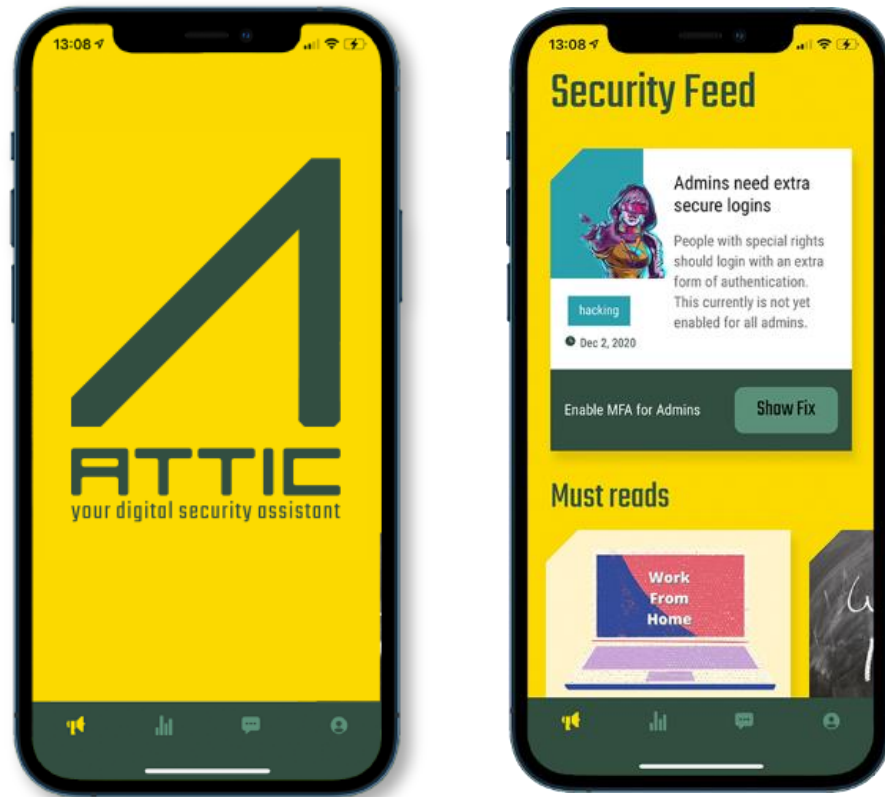
<https://github.com/zolderio/microsoft>









Or contact us directly:

 @RIKVDUIJN

ATTIC EEN BETAALBARE APP OM MICROSOFT 365 BETER TE BEVEILIGEN



	Mobile First Mobiële app, ontwikkeld in Ionic. Primair geschikt voor iOS, Android, maar ook benaderbaar vanuit web-browser.		Microsoft 365 Het meestgebruikte platform voor kantoorsoftware. Eenvoudige autorisatie voor on-boarding.
	Check & Fix Controleert continu uw configuratie op verbeteringen. Adviezen in 1-klik fixes.		Detect & Remedy Detecteer verdacht gedrag met Microsoft Sentinel. Pusht alarmen en biedt stappen om controle te krijgen..
	Nieuws Het laatste relevante security nieuws wordt gepusht via Attic@		24x7 Hulp De makkelijkste manier om in contact te komen met een cybersecurity expert van wereldklasse.