ZOLDER

applied security research

ATTACKING & DEFENDING MICROSOFT 365

07-04-2022

WHOAMI

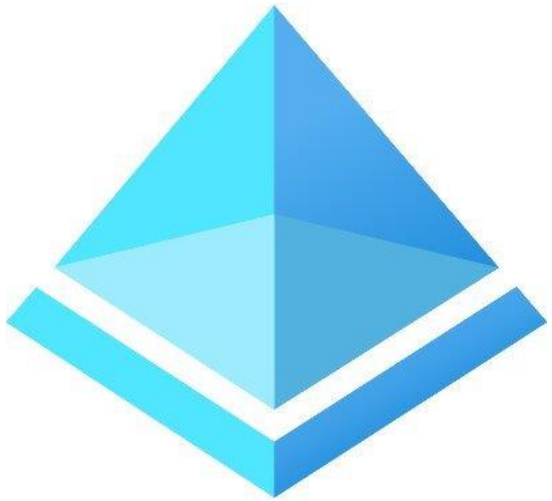
- Rik van Duijn
  - Ethical hacker
  - OSCP / OSCE
  - 8+ years of experience
  - Cybercrime / Malware analysis

ZOLDER

ATTACKING & DEFENDING MICROSOFT 365 | 7-12-2022

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:

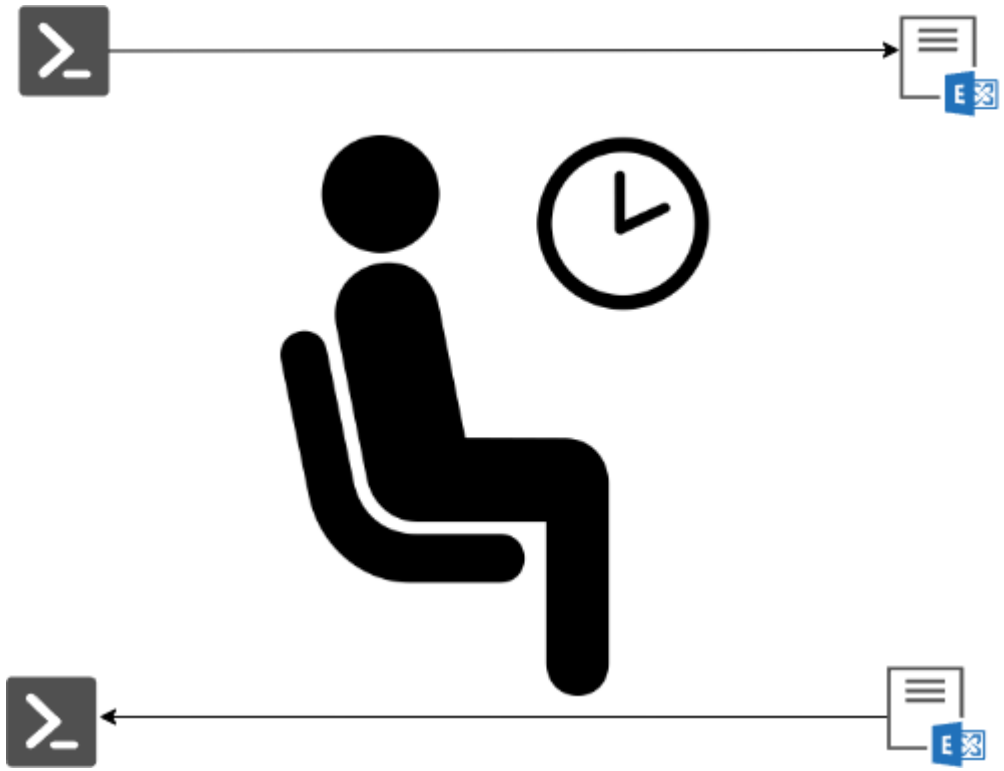
- Je bent niet volledig in control
- Afhankelijk van Microsoft (voorbeeld: sign-in logs)

Vanuit security perspectief is het niet ‘kopen en klaar’:

- Configuratie op je specifieke situatie aanpassen
- Monitoring inregelen

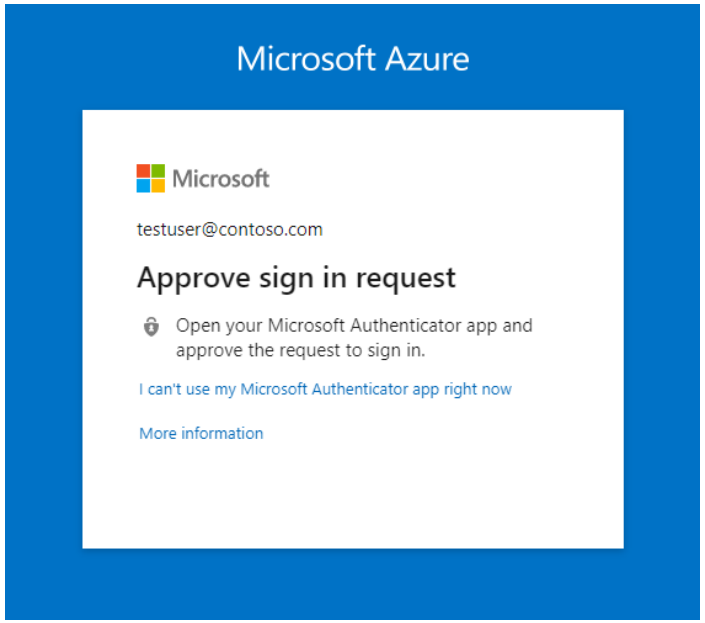
NIEUWE PROBLEMEN

CLOUDSYNC

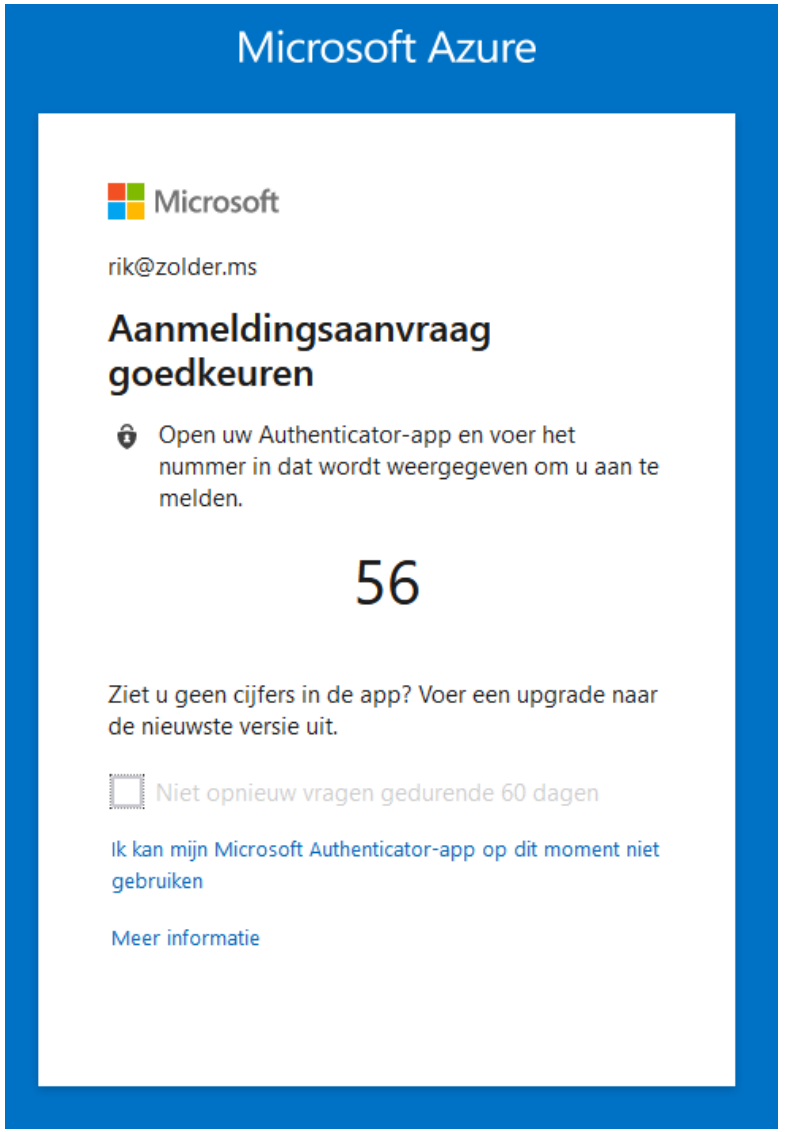


CLOUDDRIFT

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

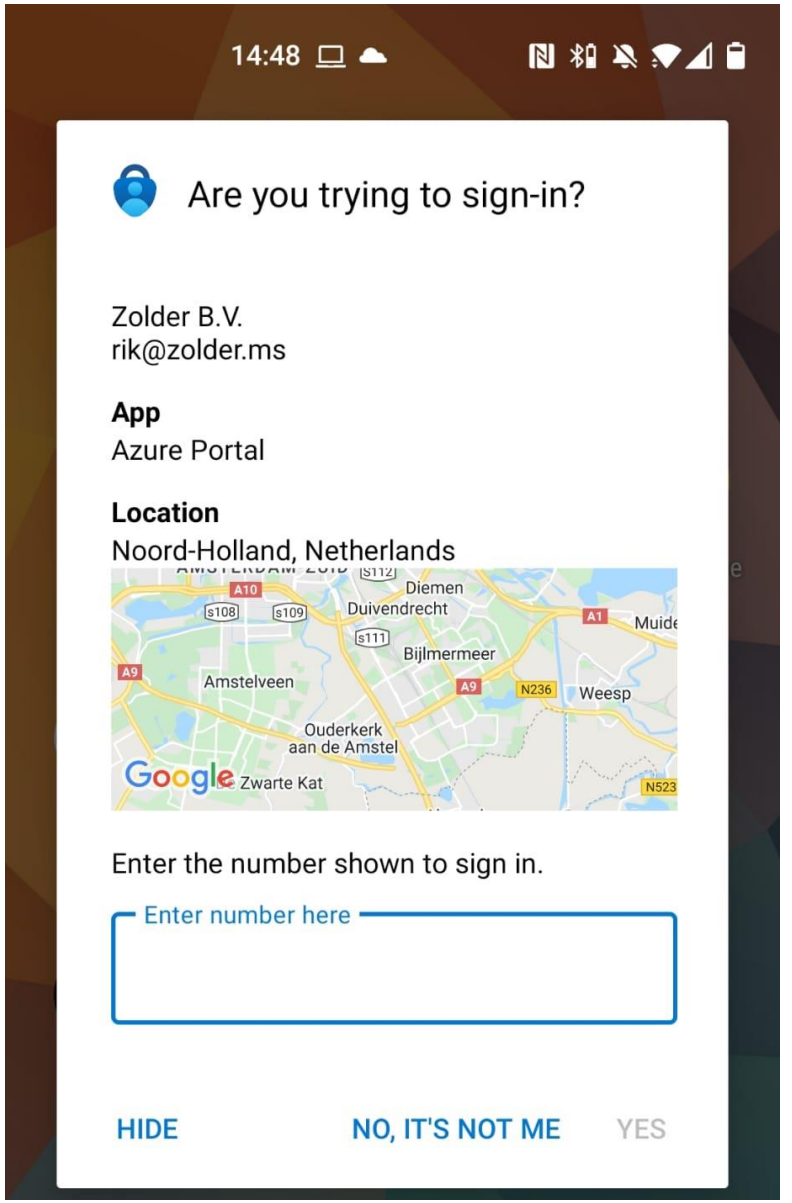


PATTERN MATCHING



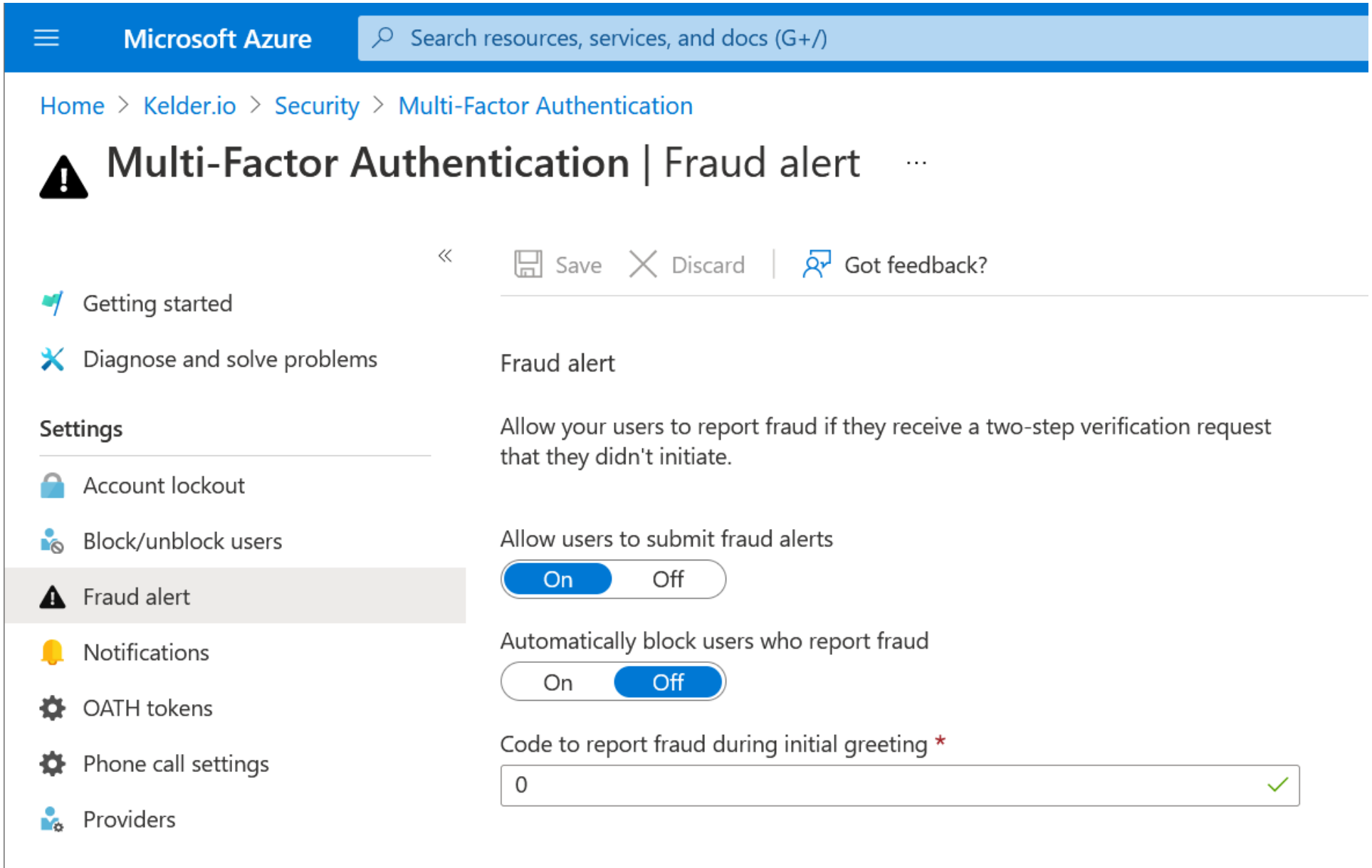
PATTERN MATCHING

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



FRAUD DETECTION

CONFIGURATIE



DETECTIE

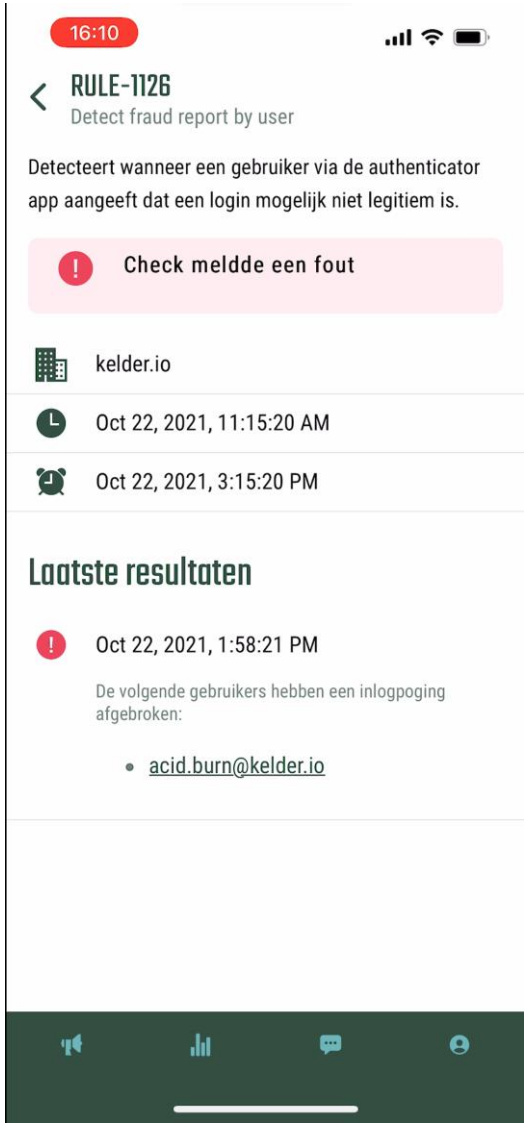
Run | Time range : Last 7 days | Save | Share | New alert rule | ...

```
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



SHAREPOINT SITES
==
SMB SHARES

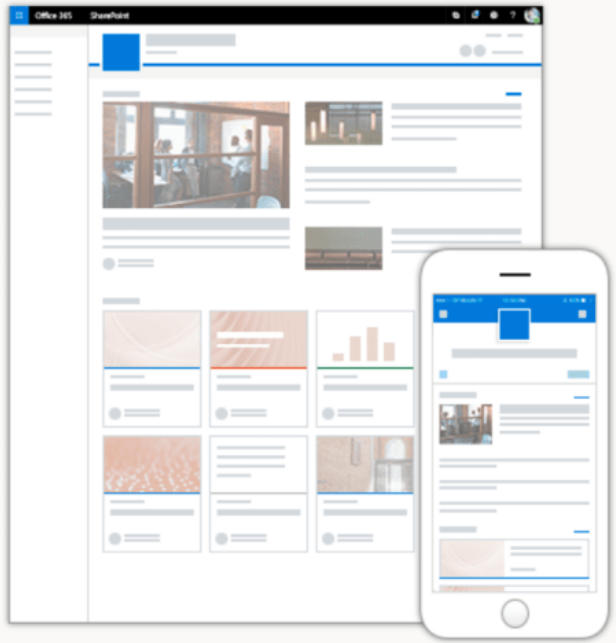
SMB SHARES

```
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

Example

The site name is available.

Group email address

Example

The group alias is available.

Site address

Example

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

The site address is available.

Site description

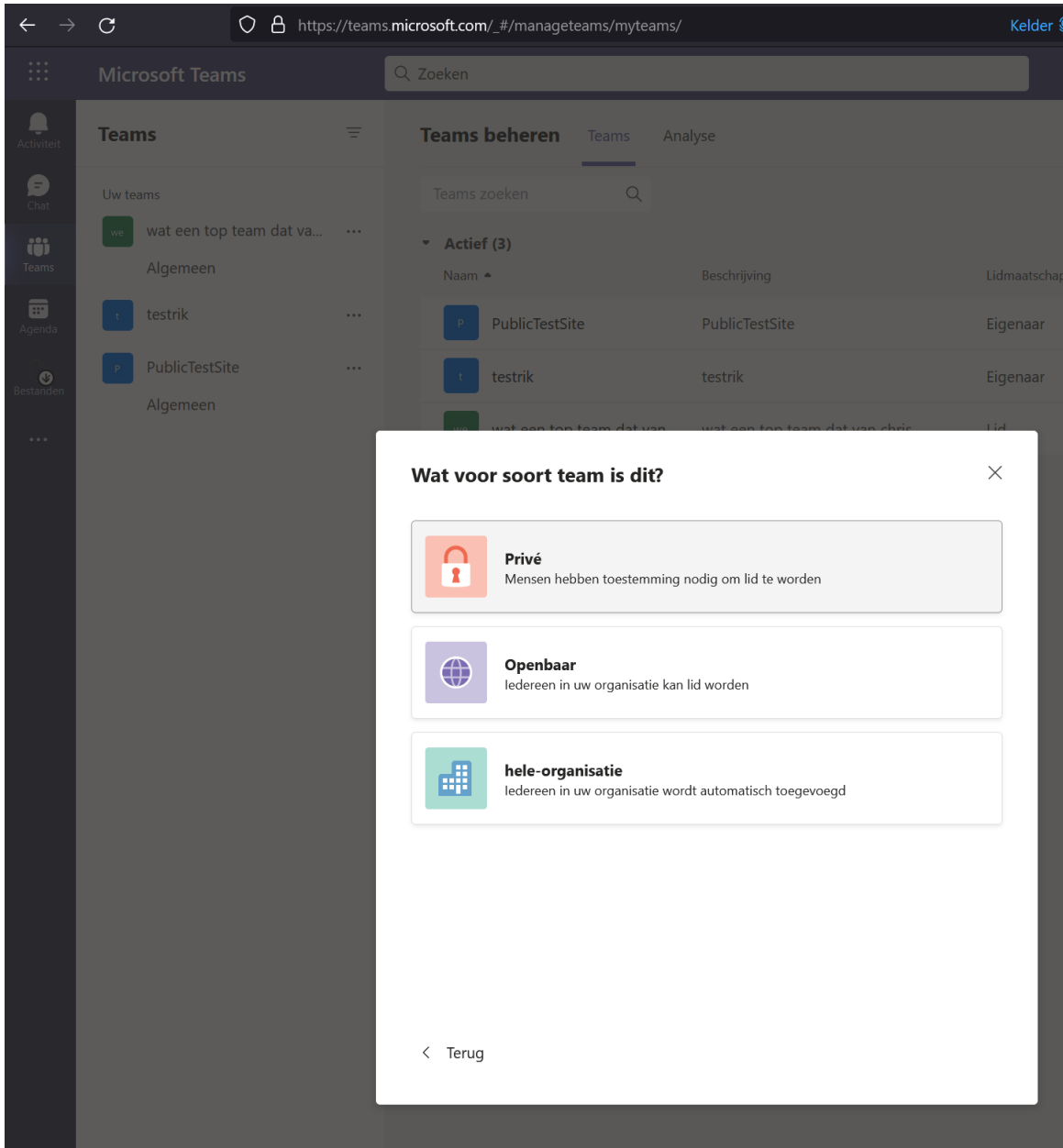
Tell people the purpose of this site

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



SHAREPOINT SITES

geheim

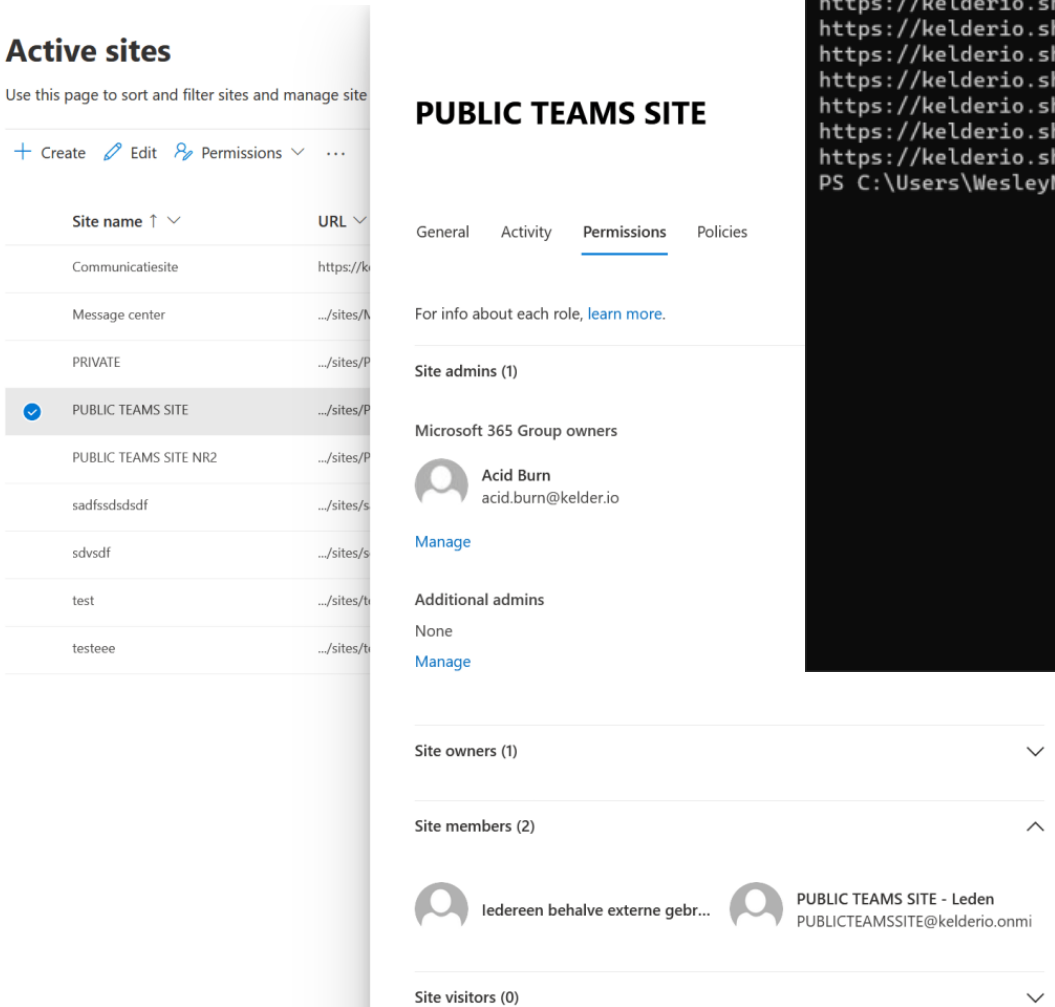
All Files Sites People News Images Power BI Feedback

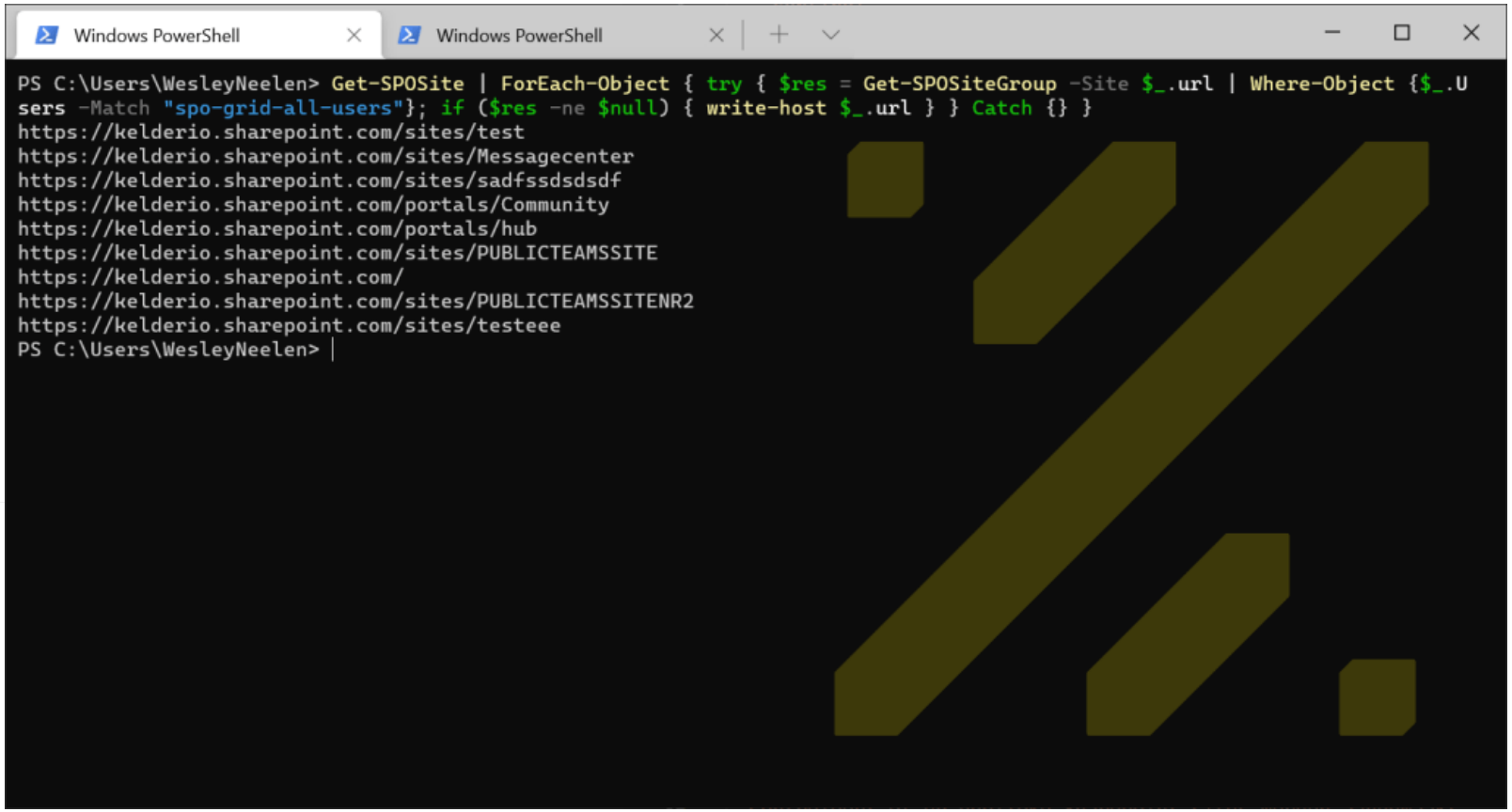
Filters File type Last modified

202107 Geheimhoudingsverklaring [redacted]

algemene-voorwaarden-saas-157277 (1)

VINDEN SITES





DETECTEREN NIEUWE SITES

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

```
let Translations = dynamic([
  "Everyone except external users",
  "Iedereen behalve externe gebruikers"
]);
OfficeActivity
| where OfficeWorkload == "SharePoint" or OfficeWorkload == "OneDrive"
| where Operation == "AddedToGroup"
| project TimeGenerated, Operation, UserId, Site_Url, TargetUserOrGroupName
| where TargetUserOrGroupName in (Translations)
```

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

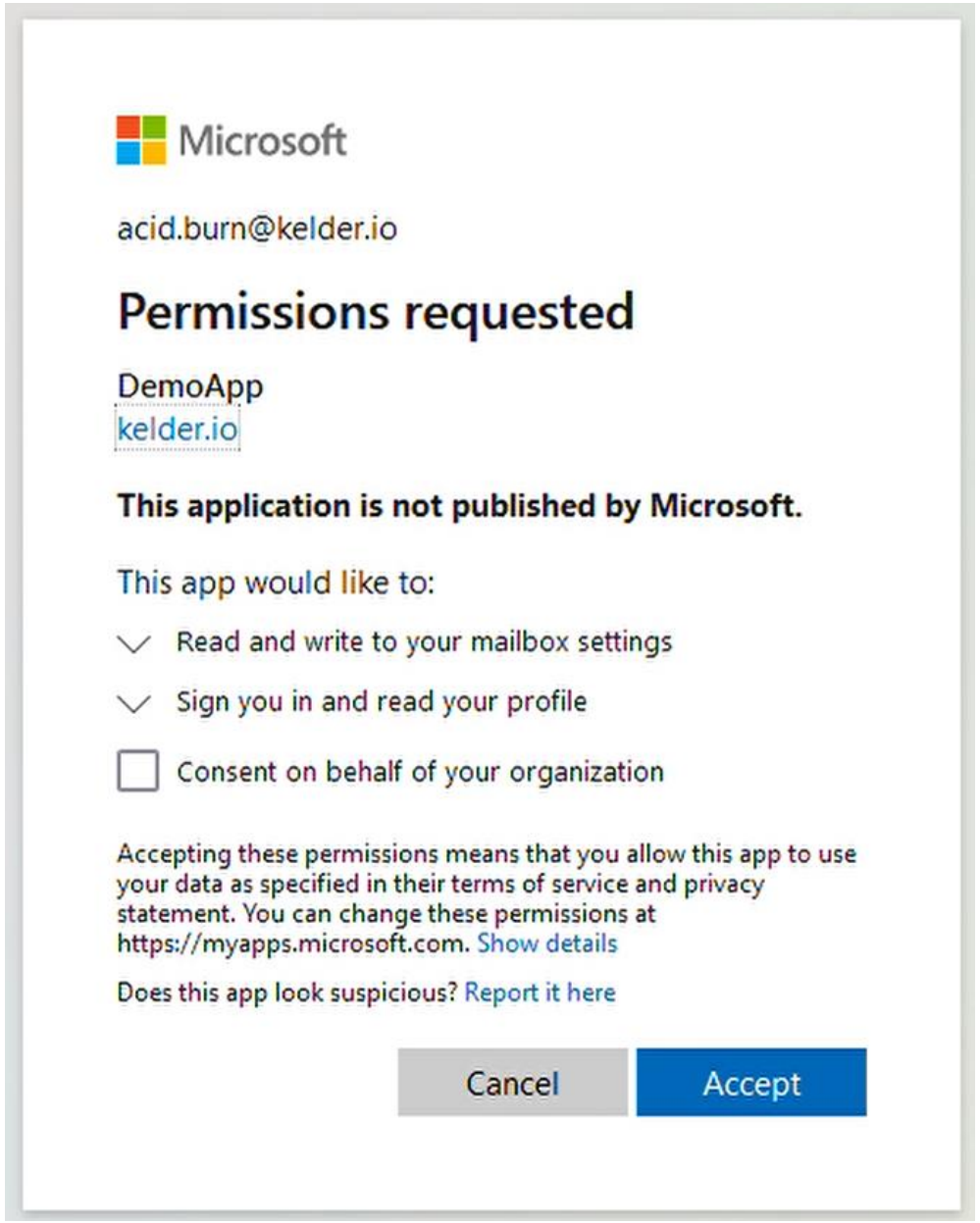
Completed. Showing results from the last 24 hours.

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

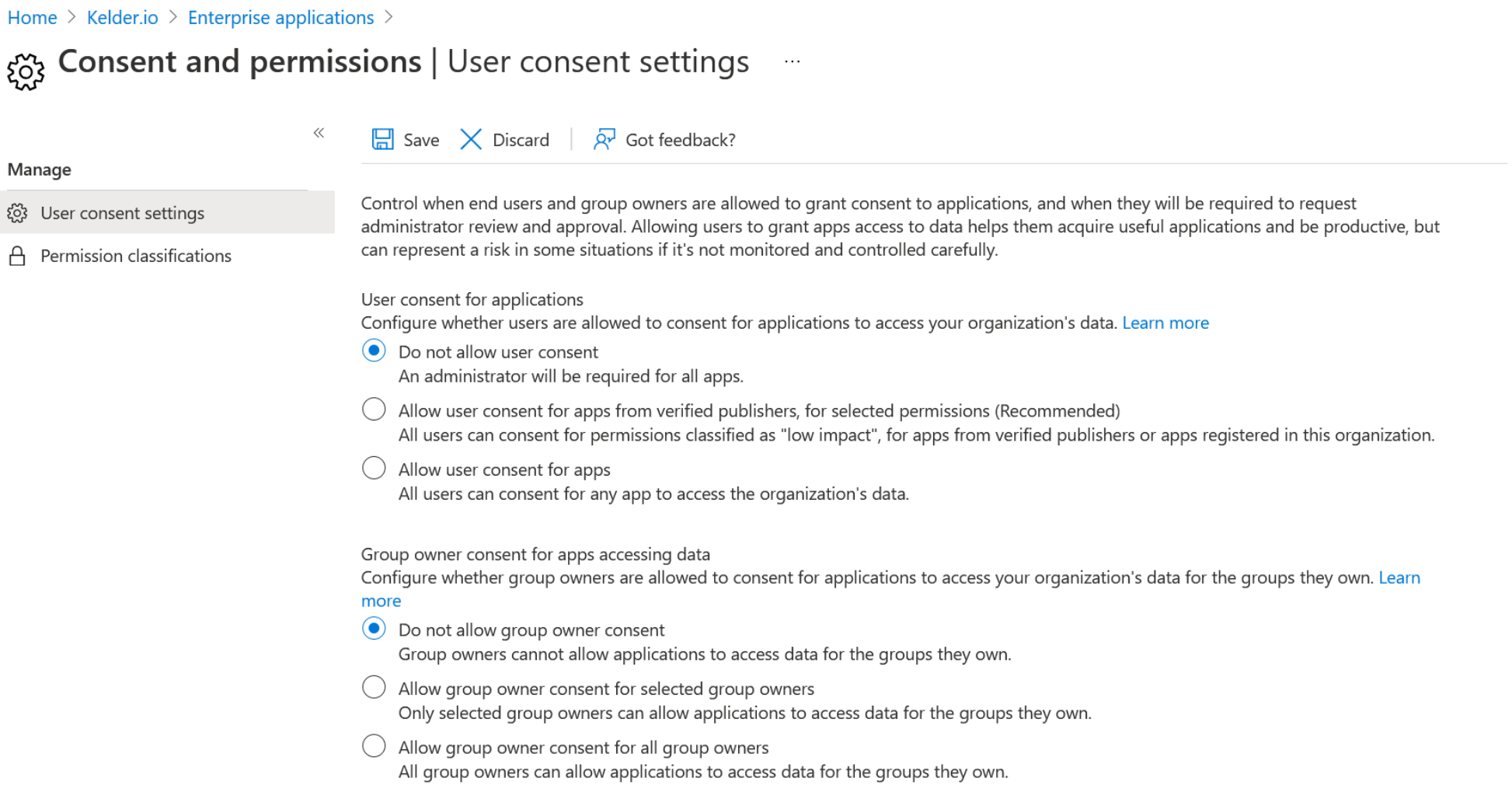
TimeGenerated [UTC]	2021-09-09T13:47:29Z
Operation	AddedToGroup

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

APP CONSENT PHISHING



CONFIGURATIE



DETECTIE

New Query 1*

sentinel | Run | Time range : Set in query | Save | Share | New alert rule | Export | Pin to dashboard | Format query

```
let detectionTime = 7d;
let joinLookback = 14d;
AuditLogs
| where TimeGenerated > ago(detectionTime)
| where LoggedByService =~ "Core Directory"
| where Category =~ "ApplicationManagement"
| where OperationName =~ "Consent to application"
| extend AppDisplayName = TargetResources.[0].displayName
| extend AppClientId = tolower(TargetResources.[0].id)
| extend ConsentFull = TargetResources[0].modifiedProperties[4].newValue
| parse ConsentFull with * "ConsentType: " GrantConsentType ", Scope: " GrantScope1 "]" *
| 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"
| extend GrantIpAddress = tostring(iff(isnotempty(InitiatedBy.user.ipAddress), InitiatedBy.user.ipAddress, InitiatedBy.app.ipAddress))
| extend GrantInitiatedBy = tostring(iff(isnotempty(InitiatedBy.user.userPrincipalName),InitiatedBy.user.userPrincipalName, InitiatedBy.app.displayName))
| extend GrantUserAgent = tostring(iff(AdditionalDetails[0].key =~ "User-Agent", AdditionalDetails[0].value, ""))
| project TimeGenerated, GrantConsentType, GrantScope1, GrantInitiatedBy, AppDisplayName, GrantIpAddress, GrantUserAgent, AppClientId, OperationName, ConsentFull, CorrelationId
| join kind = leftouter (AuditLogs
| where TimeGenerated > ago(joinLookback)
| where LoggedByService =~ "Core Directory"
| where Category =~ "ApplicationManagement"
| where OperationName =~ "Add service principal"
| extend AppClientId = tolower(TargetResources[0].id)
| extend AppReplyURLs = iff(TargetResources[0].modifiedProperties[1].newValue has "AddressType", TargetResources[0].modifiedProperties[1].newValue, "")
| distinct AppClientId, tostring(AppReplyURLs)
)
on AppClientId
| join kind = innerunique (AuditLogs
| where TimeGenerated > ago(joinLookback)
| where LoggedByService =~ "Core Directory"
| where Category =~ "ApplicationManagement"
| where OperationName =~ "Add OAuth2PermissionGrant" or OperationName =~ "Add delegated permission grant"
| extend GrantAuthentication = tostring(TargetResources[0].displayName)
| extend GrantOperation = OperationName
| project GrantAuthentication, GrantOperation, CorrelationId
) on CorrelationId
| project TimeGenerated, GrantConsentType, GrantScope1, GrantInitiatedBy, AppDisplayName, AppReplyURLs, GrantIpAddress, GrantUserAgent, AppClientId, GrantAuthentication, OperationName
| extend timestamp = TimeGenerated, AccountCustomEntity = GrantInitiatedBy, IPCustomEntity = GrantIpAddress

```

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","ReplyAddressClien...	20.67.242.110	EvoSTS	2ef89ebc-13dd-4b9c-bba

11:45

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

Laatste resultaten

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

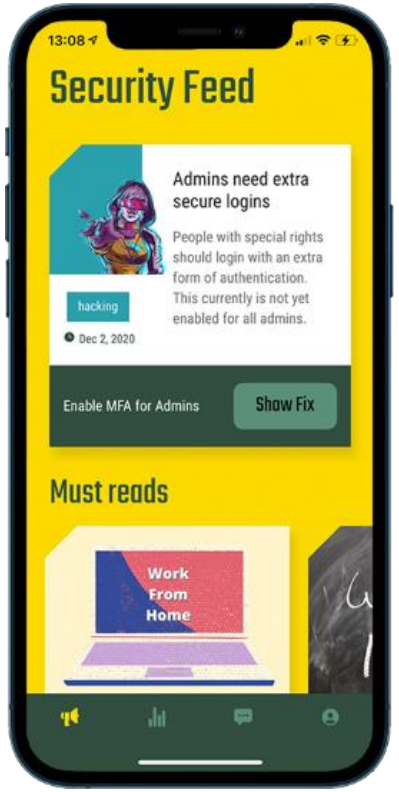
- Finetune de security configuratie van Microsoft 365
- Maak gebruik van Sentinel en de gratis logopslag (al is het voor IR/Forensics)

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

Mobiele 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.