Monitor Intune with API from different perspectives

Sander Rozemuller & Peter Klapwijk

10TH ANNIVERSARY EDITION

Experts Live Netherlands

MICROSOFT 365

Thank you partners!

ULTIMATE

cegeka IN CLOSE COOPERATION

LIQUIT

INSPARK

Delta-N Connecting the Cloud

ARROW

Microsoft

GOLD

PROXSYS*

orange™ Business Services

wortell

vijfhart IT-OPLEIDINGEN

ScriptRunner®

eG Innovations

OGD ict-diensten

Motion10 Maak(t) uw digitale innovatie succesvol

DELL Technologies

SPLIT BRAIN

Insight.

rubrik

COMMUUNITY

Dutch Microsoft & Security Meetup

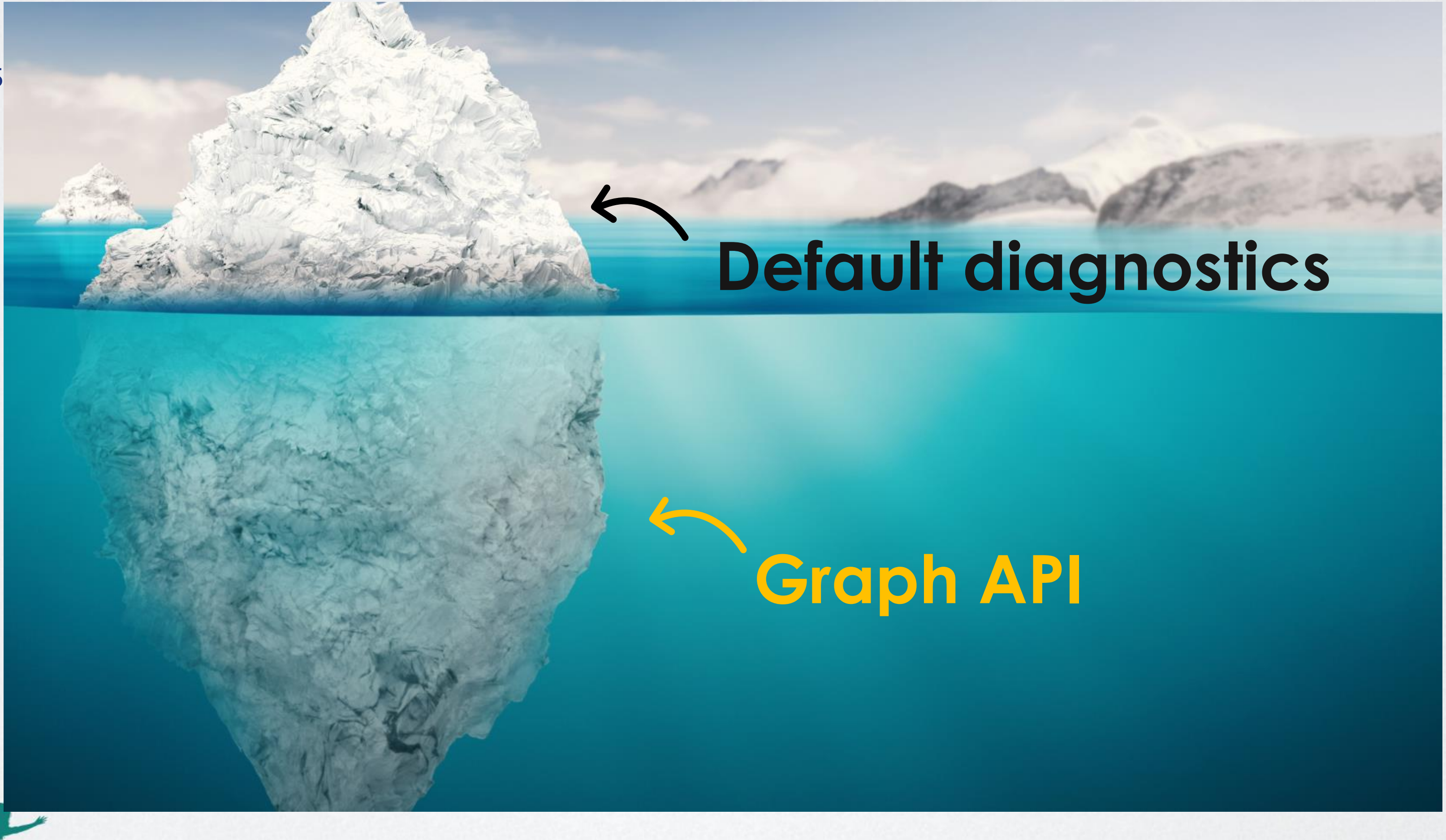
Workplace Ninja User Group Netherlands

dutch women in tech

DUTCH AZURE MEETUP

Lowlands.Community

Is default reporting enough?


Default diagnostics
Graph API

TO CODE OR NOT TO CODE

Who we are

Sander Rozemuller

Architect Center of Excellence – Exite ICT

Like: Photography, #membeer, athletics

Award: MVP Enterprise Mobility

#MEMBEER

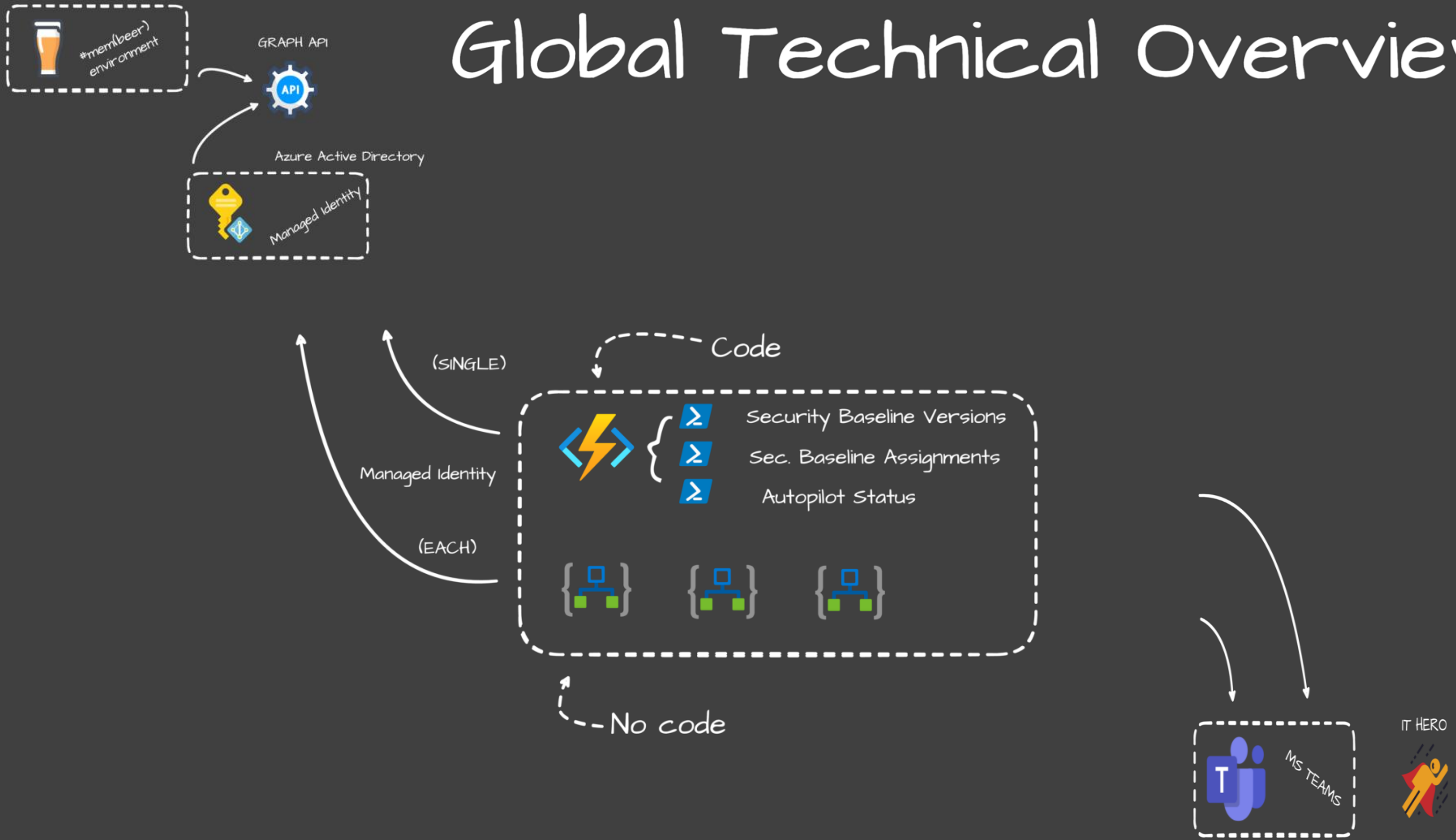
Peter Klapwijk

Modern Workplace engineer – NN Group

Like: Football, blogging, #MEMbeer

Award: MVP Enterprise Mobility

Global Technical Overview



#mem(beer) environment

GRAPH API

Azure Active Directory

Managed Identity

(SINGLE)

Code

Managed Identity

(EACH)

Security Baseline Versions

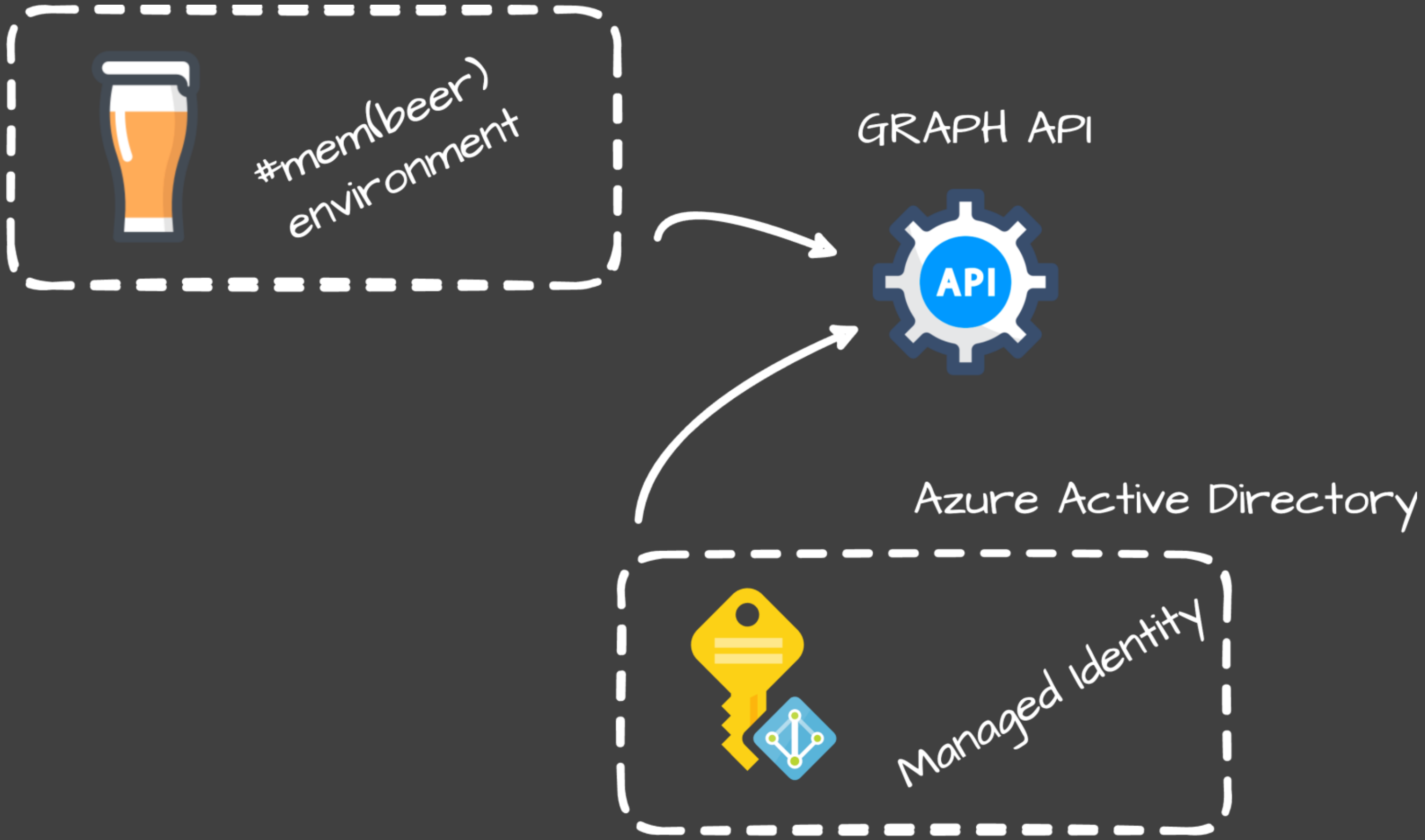
Sec. Baseline Assignments

Autopilot Status

No code

MS TEAMS

IT HERO



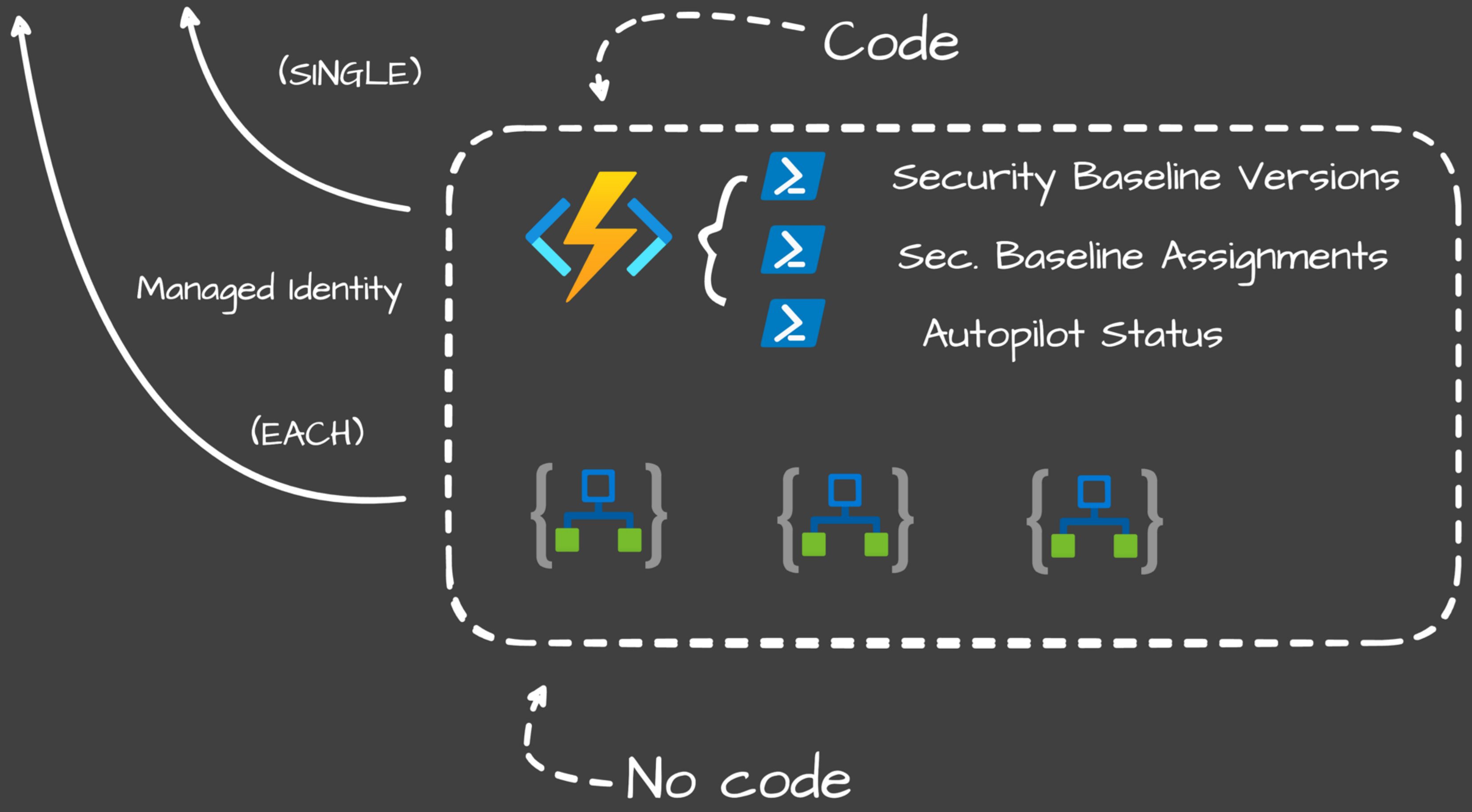
#mem(beer) environment

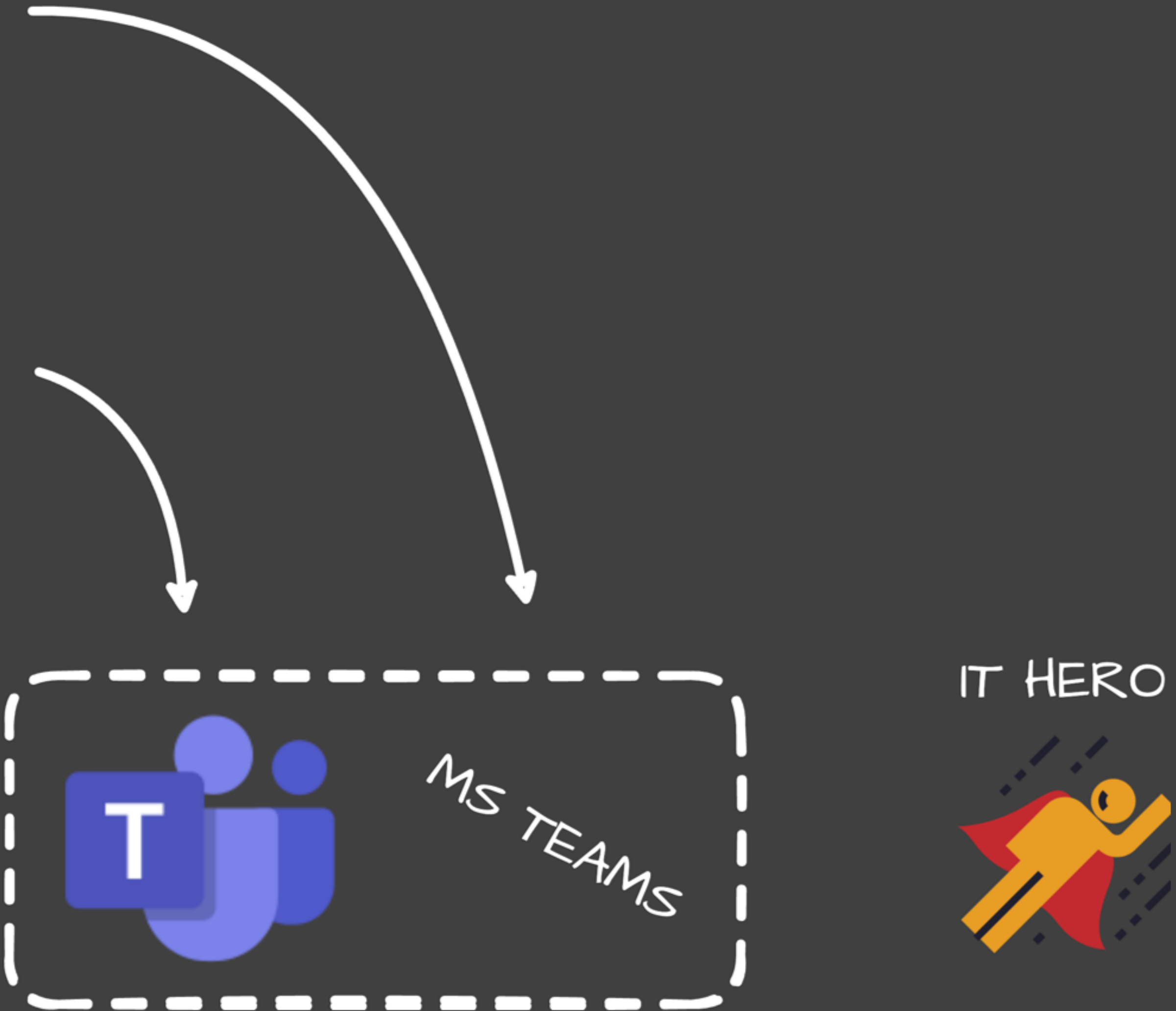
GRAPH API

API

Azure Active Directory

Managed Identity

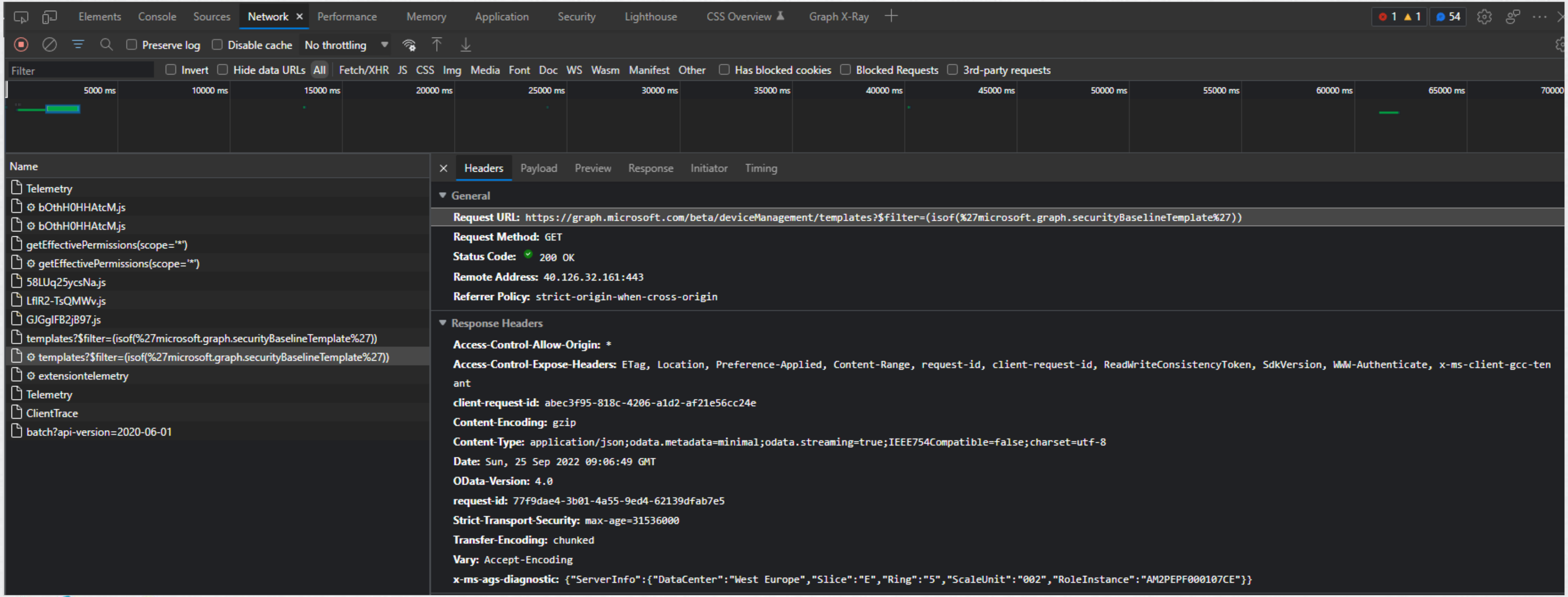

Code
(SINGLE)
Managed Identity
(EACH)
Security Baseline Versions
Sec. Baseline Assignments
Autopilot Status
No code



MS TEAMS

IT HERO

MICROSOFT 365



Name

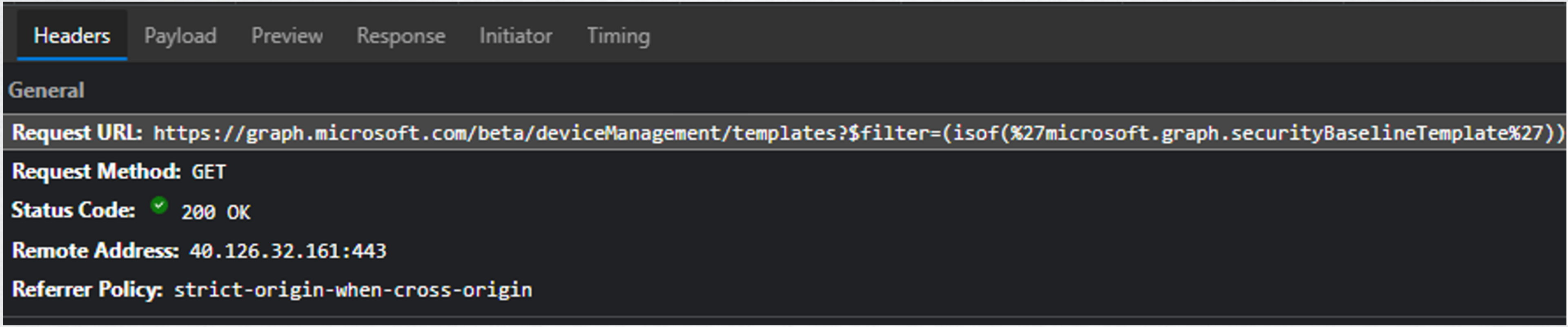
```
Telemetry
⚙ bOthH0HHAtcM.js
⚙ bOthH0HHAtcM.js
getEffectivePermissions(scope='*')
⚙ getEffectivePermissions(scope='*')
58LUq25ycsNa.js
LfIR2-TsQMWv.js
GJGglFB2jB97.js
templates?$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27))
⚙ templates?$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27))
⚙ extensiontelemetry
Telemetry
ClientTrace
batch?api-version=2020-06-01
```

▼ General

```
Request URL: https://graph.microsoft.com/beta/deviceManagement/templates?$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27))
Request Method: GET
Status Code: ✓ 200 OK
Remote Address: 40.126.32.161:443
Referrer Policy: strict-origin-when-cross-origin
```

▼ Response Headers

```
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: ETag, Location, Preference-Applied, Content-Range, request-id, client-request-id, ReadWriteConsistencyToken, SdkVersion, WWW-Authenticate, x-ms-client-gcc-ten
ant
client-request-id: abec3f95-818c-4206-a1d2-af21e56cc24e
Content-Encoding: gzip
Content-Type: application/json;odata.metadata=minimal;odata.streaming=true;IEEE754Compatible=false;charset=utf-8
Date: Sun, 25 Sep 2022 09:06:49 GMT
OData-Version: 4.0
request-id: 77f9dae4-3b01-4a55-9ed4-62139dfab7e5
Strict-Transport-Security: max-age=31536000
Transfer-Encoding: chunked
Vary: Accept-Encoding
x-ms-ags-diagnostic: {"ServerInfo":{"DataCenter":"West Europe","Slice":"E","Ring":"5","ScaleUnit":"002","RoleInstance":"AM2PEPF000107CE"}}
```



General

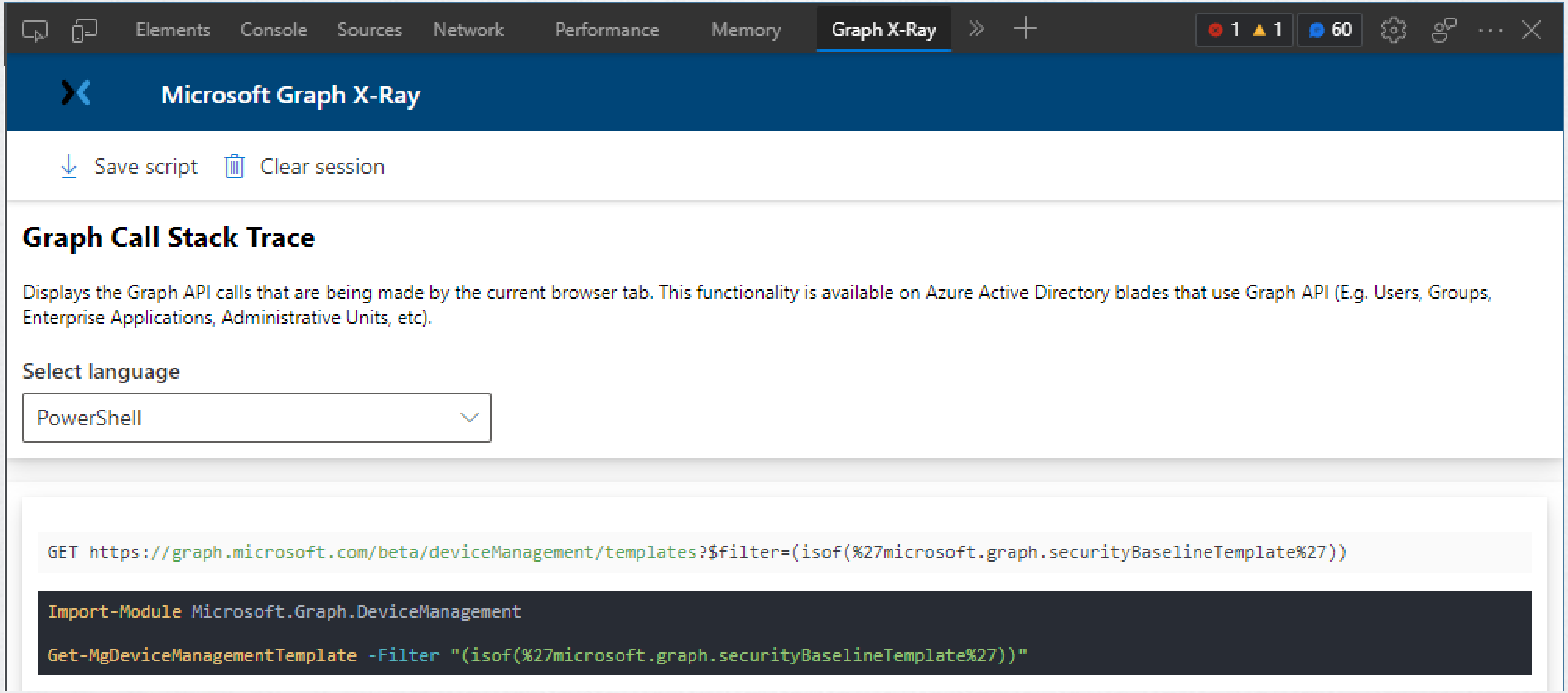
Request URL: https://graph.microsoft.com/beta/deviceManagement/templates?$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27))

Request Method: GET

Status Code: ✓ 200 OK

Remote Address: 40.126.32.161:443

Referrer Policy: strict-origin-when-cross-origin



Graph Call Stack Trace

Displays the Graph API calls that are being made by the current browser tab. This functionality is available on Azure Active Directory blades that use Graph API (E.g. Users, Groups, Enterprise Applications, Administrative Units, etc).

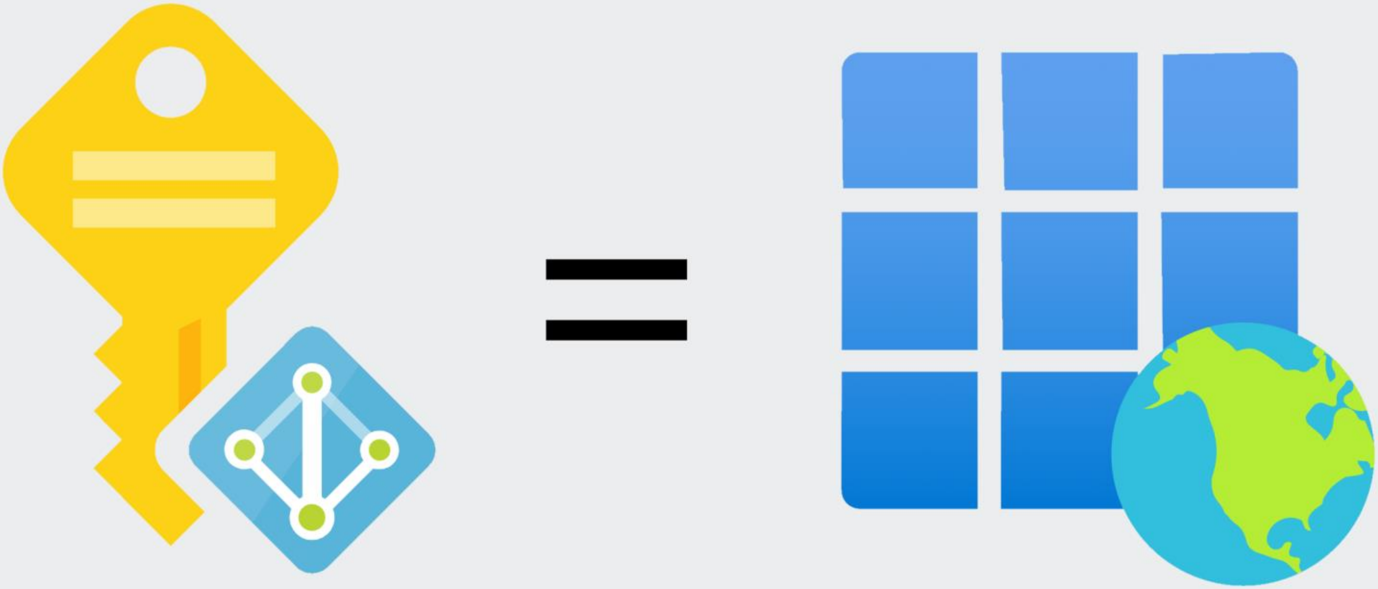
Select language

PowerShell

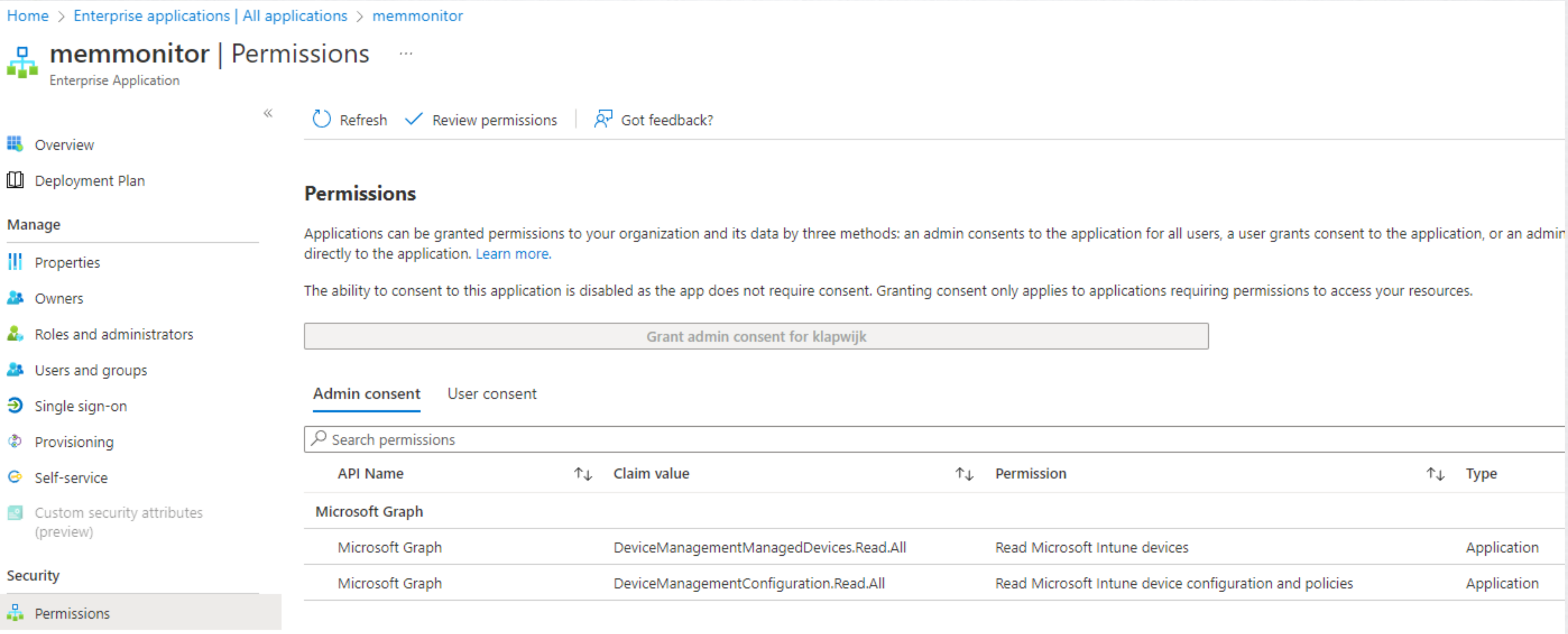
```
GET https://graph.microsoft.com/beta/deviceManagement/templates?$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27))
```

```
Import-Module Microsoft.Graph.DeviceManagement

Get-MgDeviceManagementTemplate -Filter "(isof(%27microsoft.graph.securityBaselineTemplate%27))"
```



MICROSOFT 365



Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin directly to the application. Learn more.

The ability to consent to this application is disabled as the app does not require consent. Granting consent only applies to applications requiring permissions to access your resources.

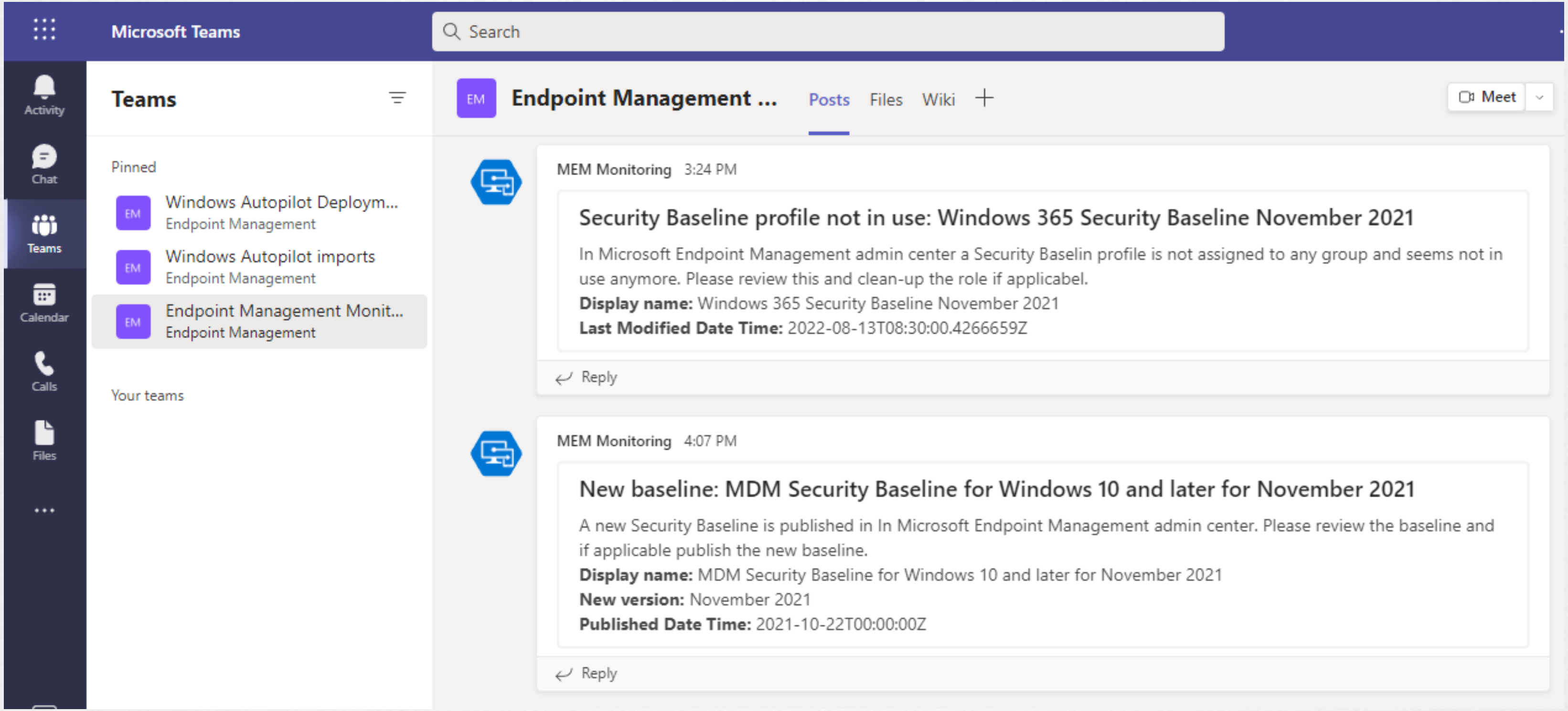
API Name ↑↓	Claim value ↑↓	Permission ↑↓	Type
Microsoft Graph			
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Read Microsoft Intune devices	Application
Microsoft Graph	DeviceManagementConfiguration.Read.All	Read Microsoft Intune device configuration and policies	Application

Delta-N Connecting the Cloud   cegeka   ARROW   LIQUIT   INSPARK   Microsoft

No code – Logic Apps

MICROSOFT 365

Teams notification!



MEM Monitoring 3:24 PM

Security Baseline profile not in use: Windows 365 Security Baseline November 2021

In Microsoft Endpoint Management admin center a Security Baselin profile is not assigned to any group and seems not in use anymore. Please review this and clean-up the role if applicabel.

Display name: Windows 365 Security Baseline November 2021
Last Modified Date Time: 2022-08-13T08:30:00.4266659Z

Reply

MEM Monitoring 4:07 PM

New baseline: MDM Security Baseline for Windows 10 and later for November 2021

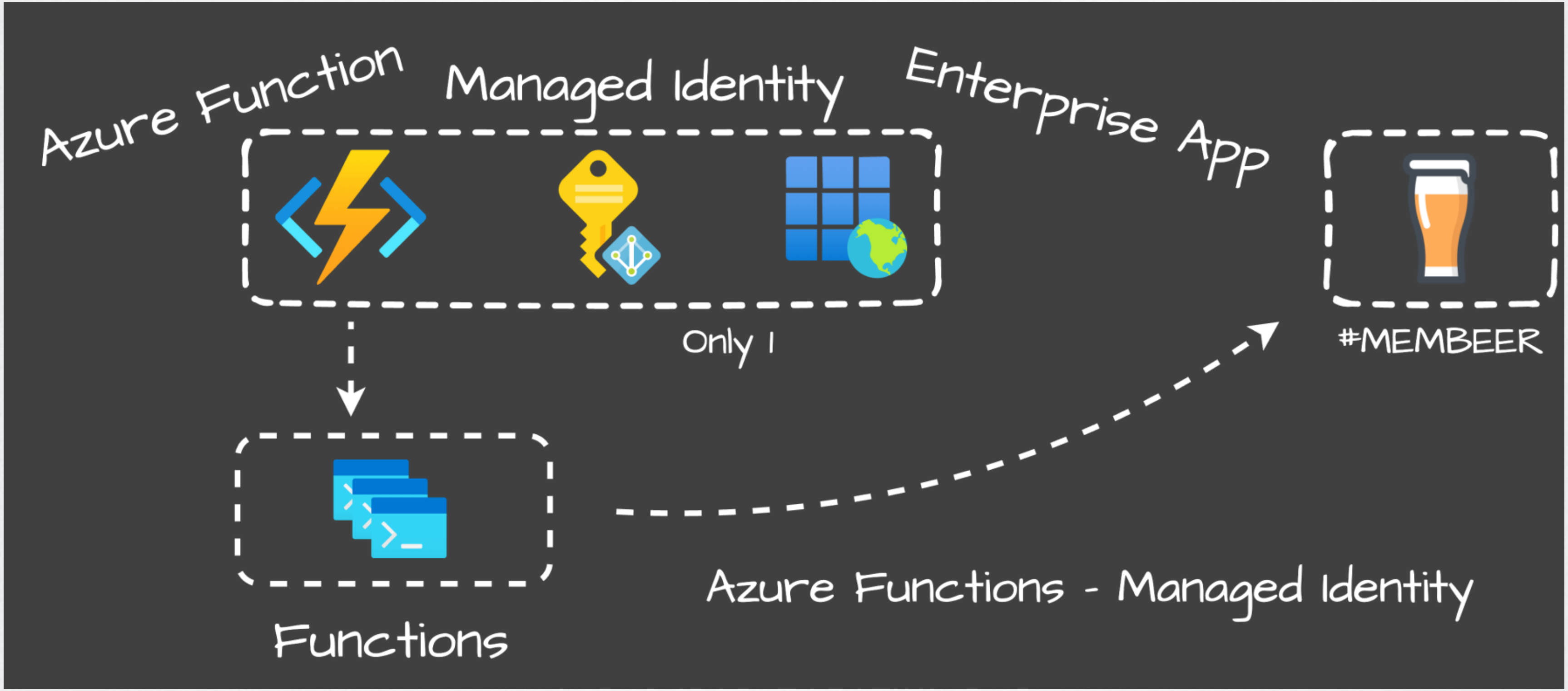
A new Security Baseline is published in In Microsoft Endpoint Management admin center. Please review the baseline and if applicable publish the new baseline.

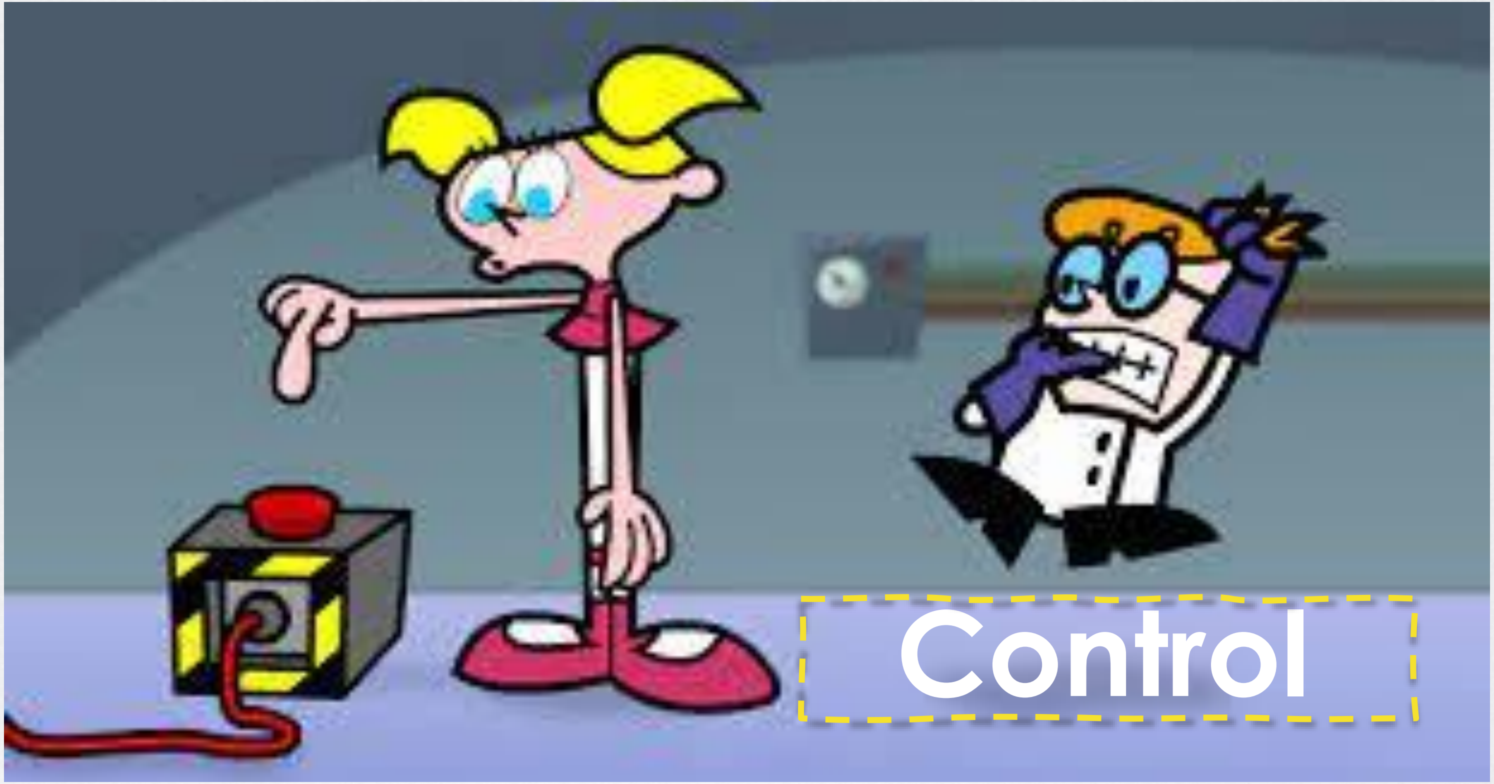
Display name: MDM Security Baseline for Windows 10 and later for November 2021
New version: November 2021
Published Date Time: 2021-10-22T00:00:00Z

Reply

Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

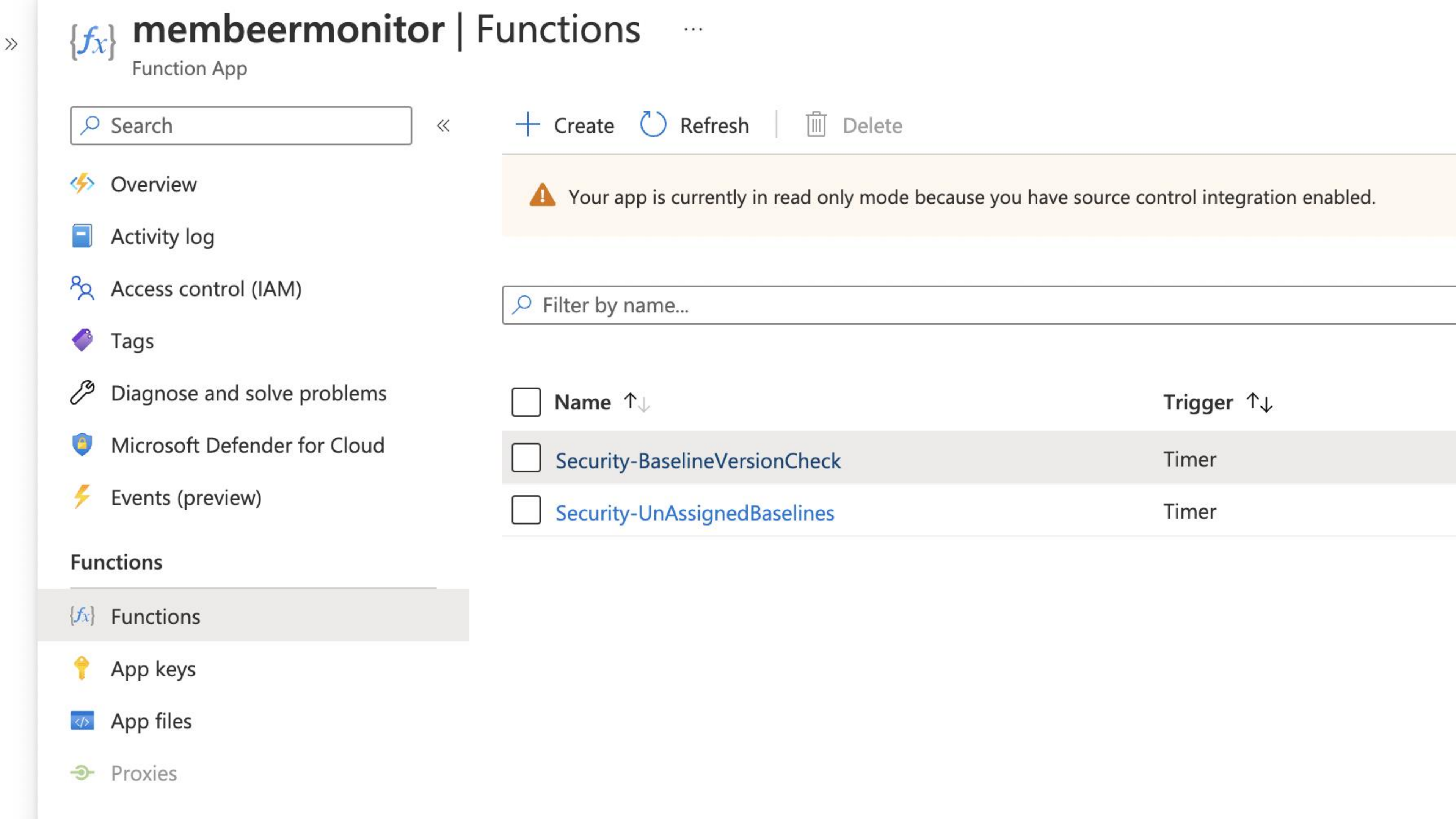
Azure Functions?


Azure Function
Managed Identity
Enterprise App
#MEMBEER
Only 1
Functions
Azure Functions - Managed Identity


Control

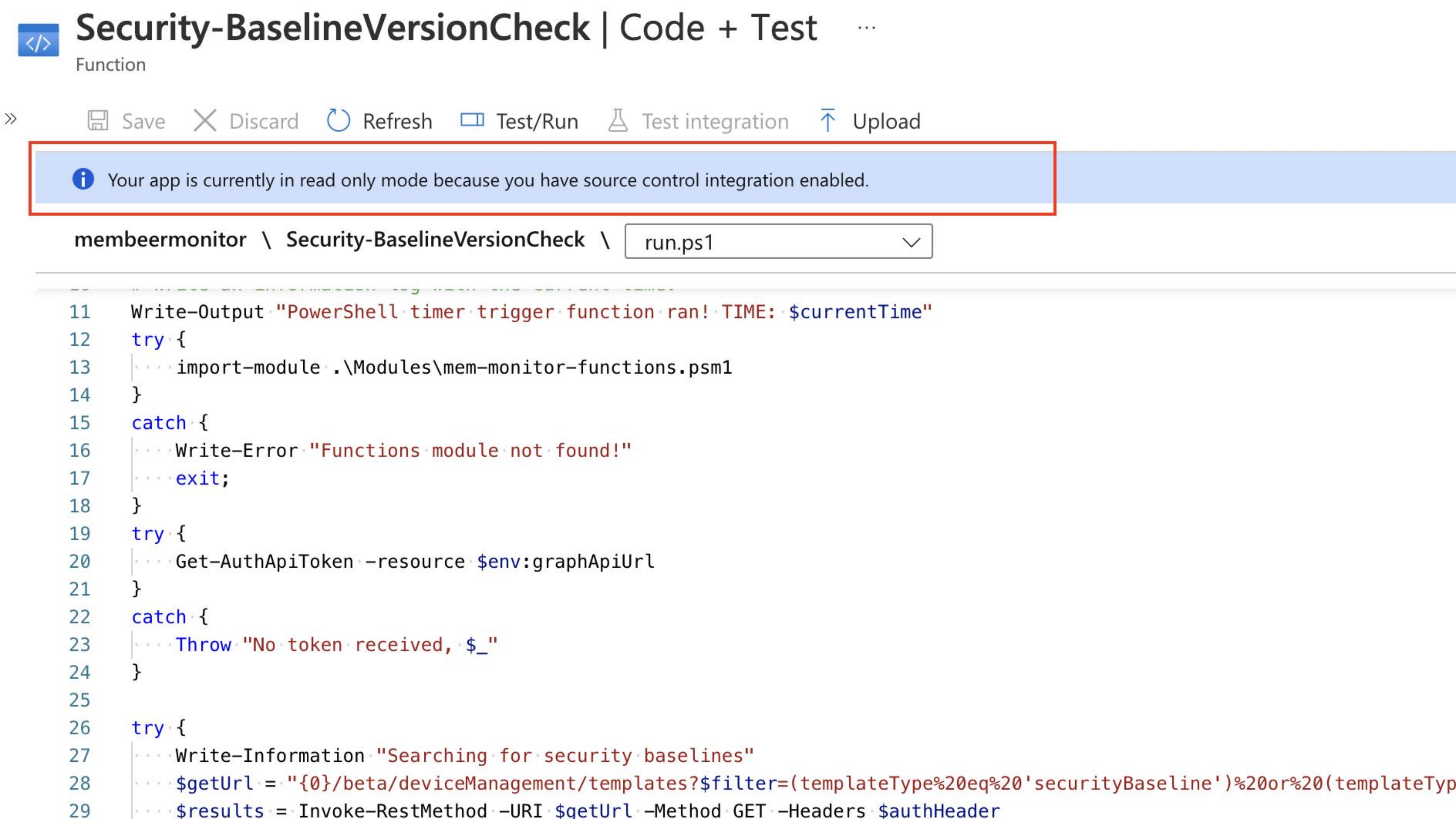
Efficiency

Be DRY



Your app is currently in read only mode because you have source control integration enabled.

□	Name ↑↓	Trigger ↑↓
□	Security-BaselineVersionCheck	Timer
□	Security-UnAssignedBaselines	Timer



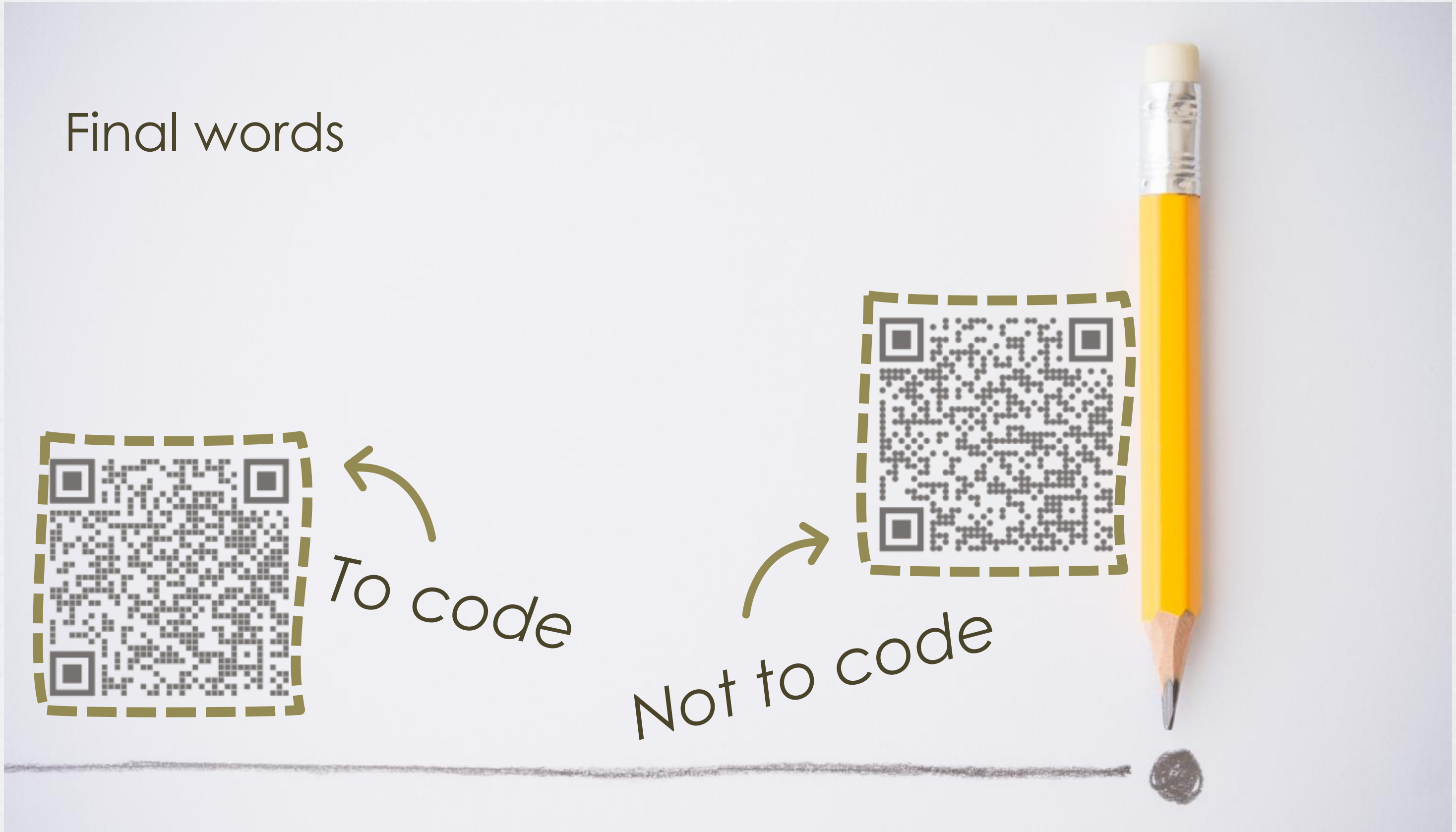
Security-BaselineVersionCheck | Code + Test
Function
Save
Discard
Refresh
Test/Run
Test integration
Upload
membeermonitor \ Security-BaselineVersionCheck \ run.ps1

Your app is currently in read only mode because you have source control integration enabled.

```
# Write an information log with the current time.
Write-Output "PowerShell timer trigger function ran! TIME: $currentTime"
try {
    import-module .\Modules\mem-monitor-functions.psm1
}
catch {
    Write-Error "Functions module not found!"
    exit;
}
try {
    Get-AuthApiToken -resource $env:graphApiUrl
}
catch {
    Throw "No token received, $_"
}

try {
    Write-Information "Searching for security baselines"
    $getUrl = "{0}/beta/deviceManagement/templates?$filter=(templateType%20eq%20'securityBaseline')%20or%20(templateTyp
    $results = Invoke-RestMethod -URI $getUrl -Method GET -Headers $authHeader
```

Final words



To code

Not to code

Please provide feedback

Delta-N Connecting the Cloud cegeka ARROW LIQUIT INSPARK Microsoft

14:00 – 14:50

Building and testing your Incident Response Plan. Be Prepared when the sh*t hits the fan

Erik Loef

10TH ANNIVERSARY EDITION

Experts Live Netherlands