

Monitor Intune with API from different perspectives

Sander Rozemuller & Peter Klapwijk



Thank you partners!

ULTIMATE



GOLD



COMMUNITY





MICROSOFT 365



Is default reporting enough?



Delta-N
Connecting the Cloud

cegeka

ANNO

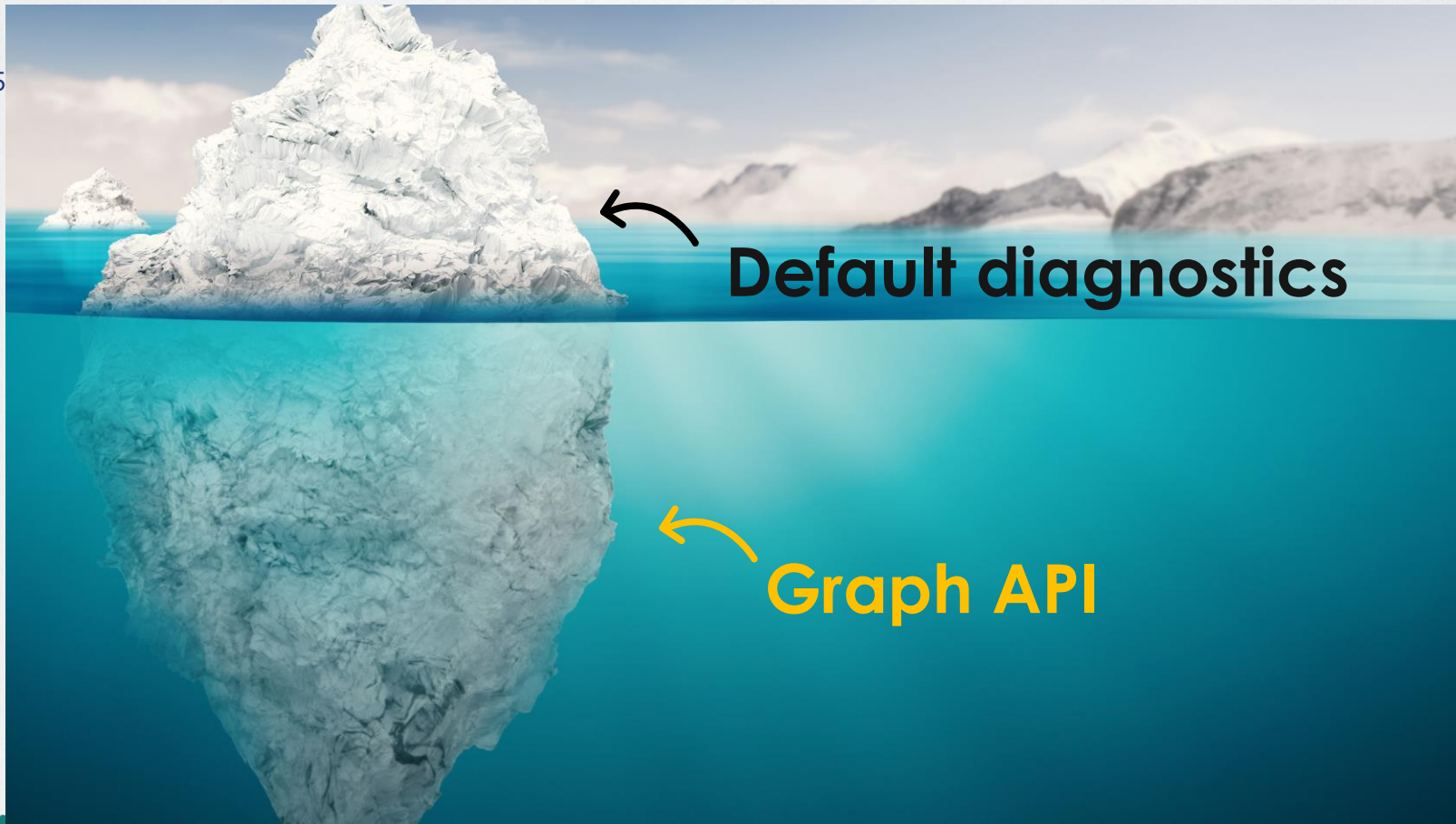
LIQUIT

INSPARK

Microsoft



MICROSOFT 365



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft



MICROSOFT 365

TO CODE OR NOT TO CODE



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft



MICROSOFT 365

Who we are



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft



Sander Rozemuller

Architect Center of Excellence – Exite ICT

Like: Photography, #member, athletics

Award: MVP Enterprise Mobility





MICROSOFT 365

#MEMBEER



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INS PARK

Microsoft



Peter Klapwijk

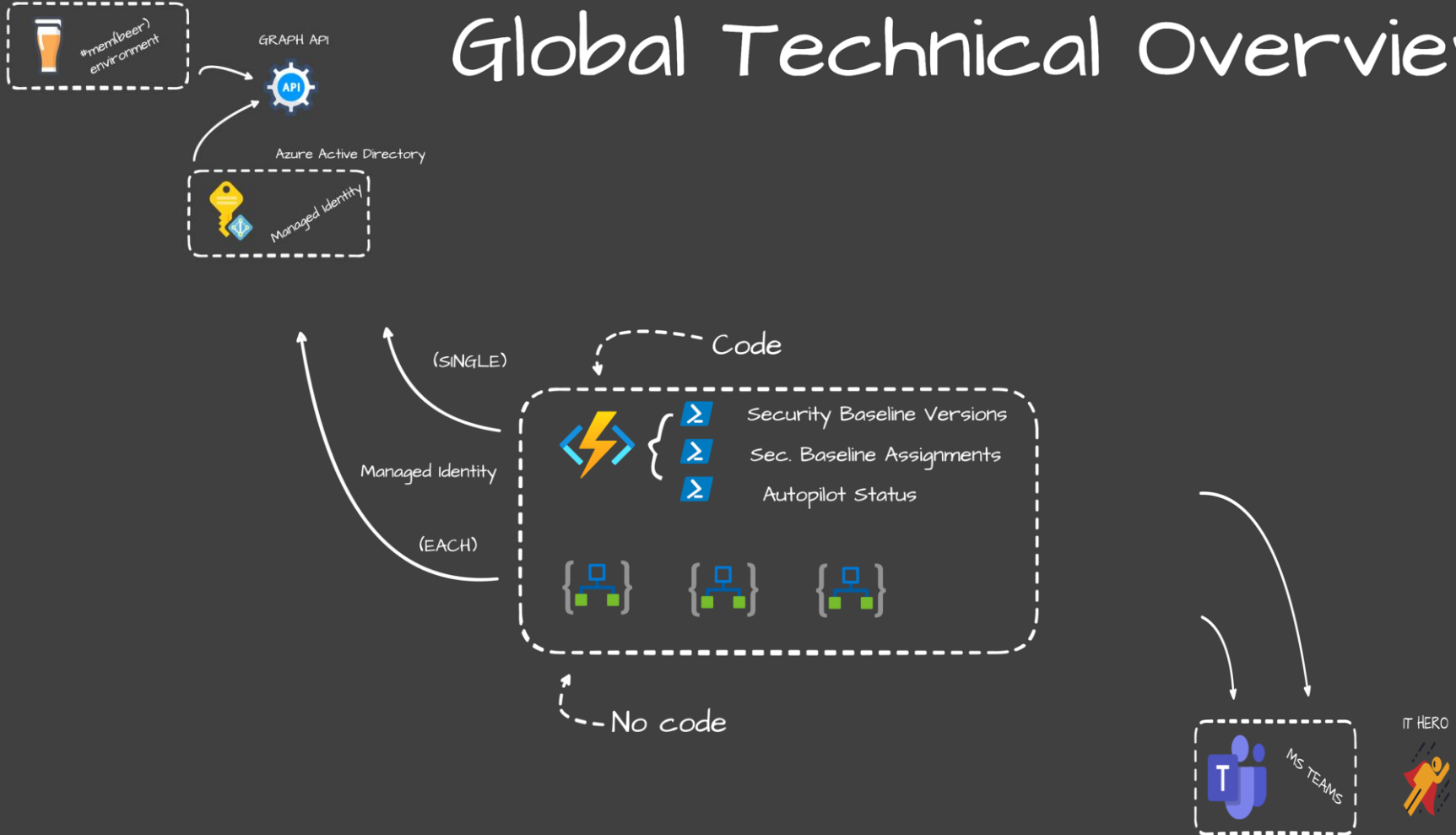
Modern Workplace engineer – NN Group

Like: Football, blogging, #MEMbeer

Award: MVP Enterprise Mobility



Global Technical Overview



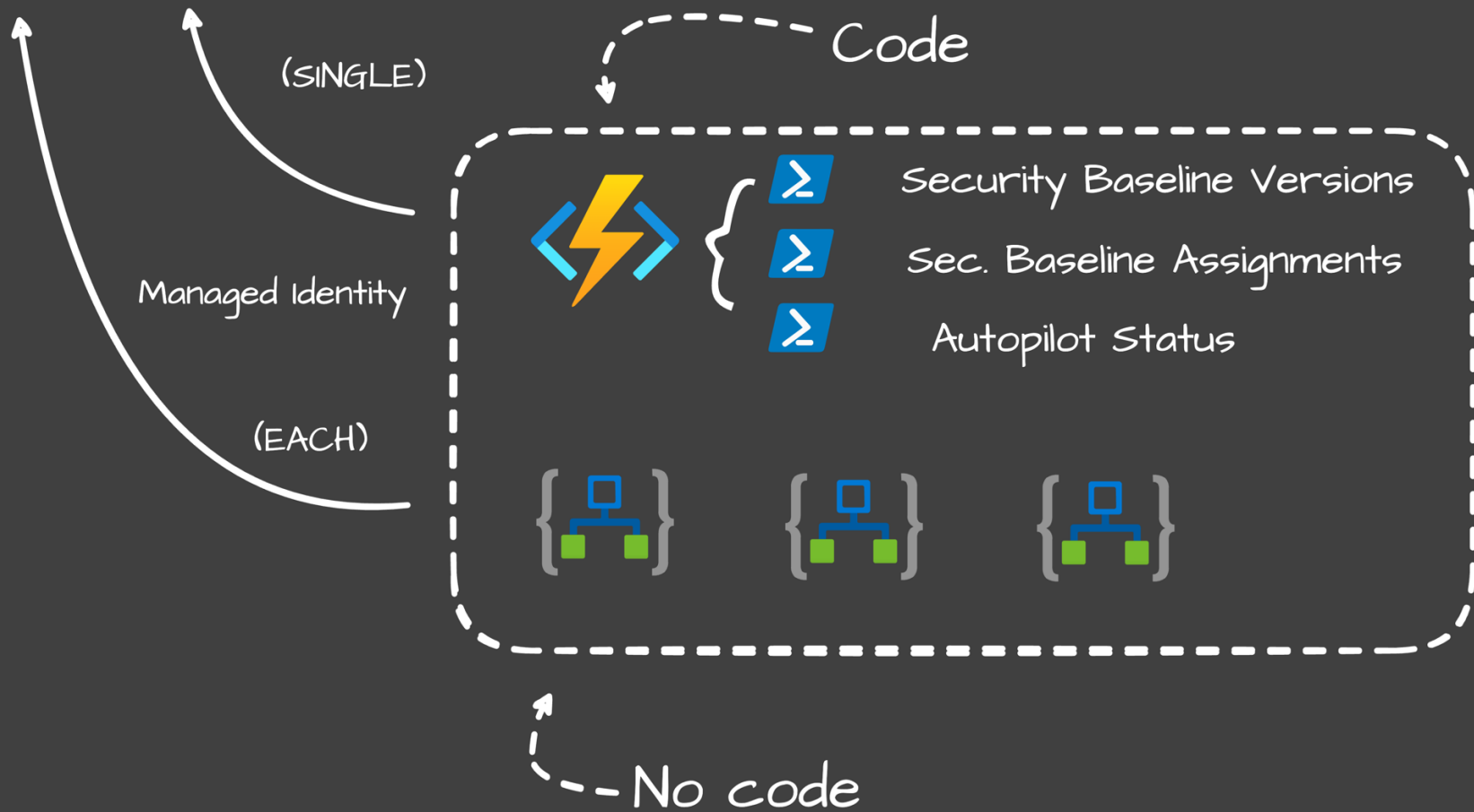


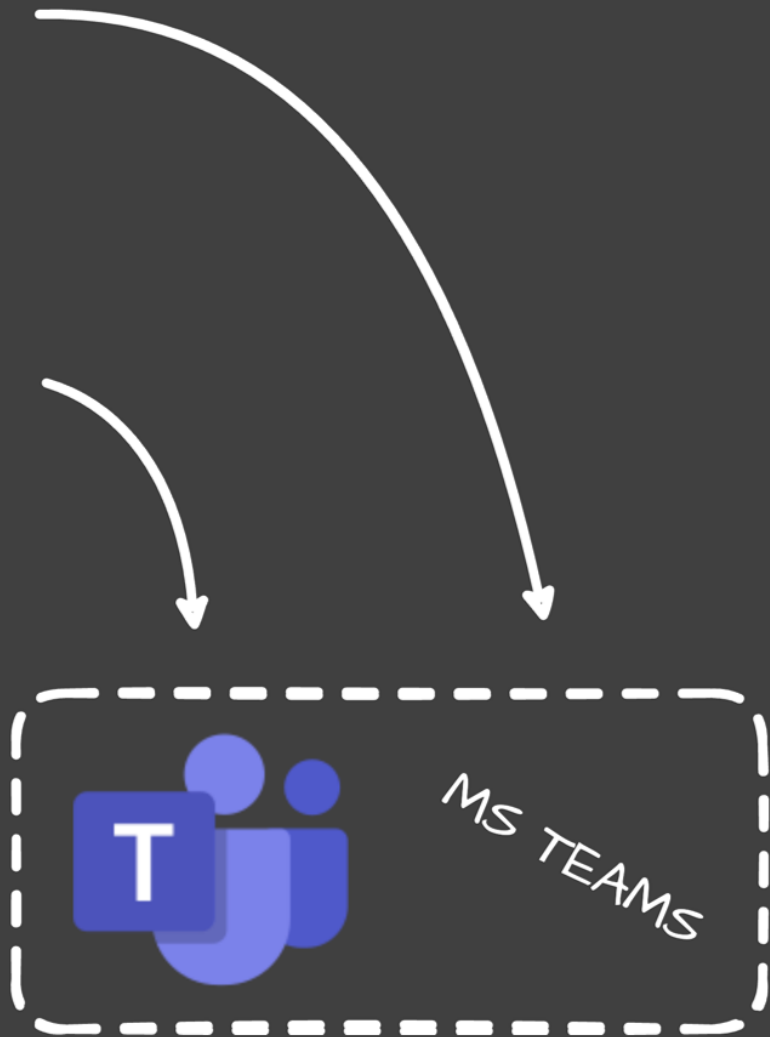
GRAPH API



Azure Active Directory



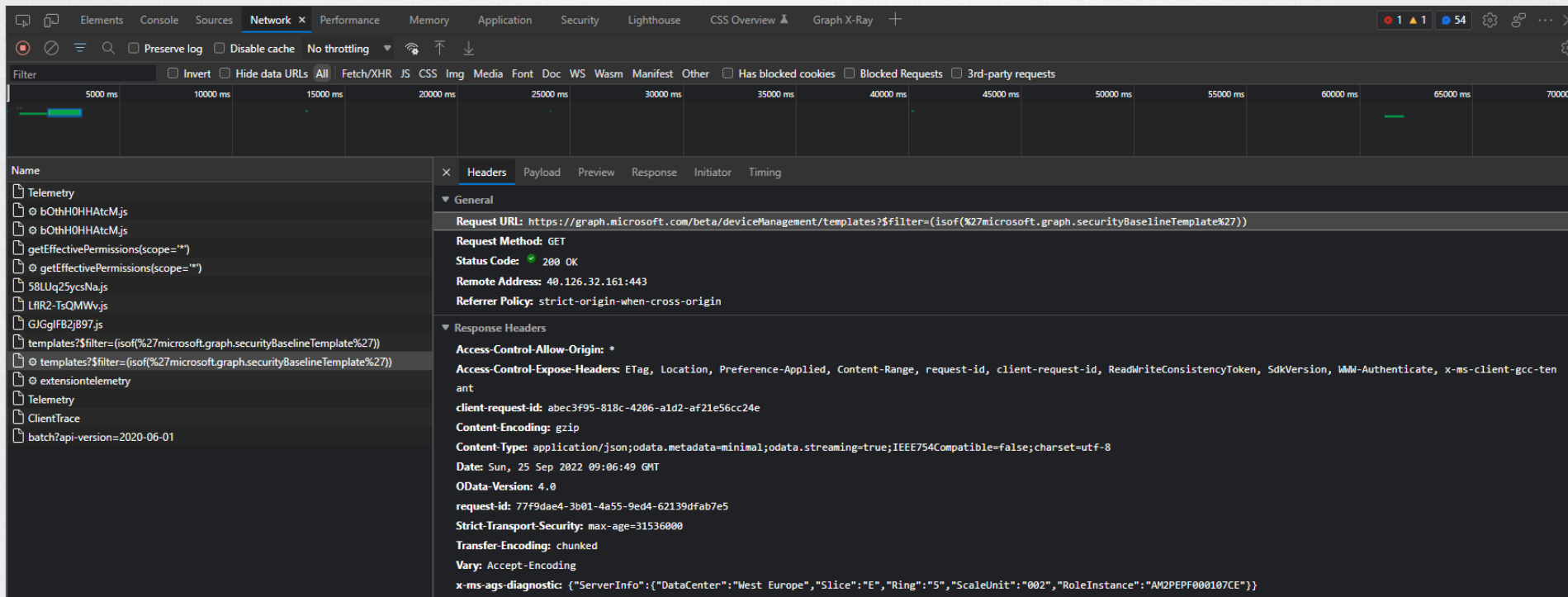




IT HERO



MICROSOFT 365



The screenshot displays the Network tab of a web browser's developer tools. The top panel shows a timeline of network requests. The selected request is a GET request to the URL: `https://graph.microsoft.com/beta/deviceManagement/templates?$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27))`. The status code is 200 OK. The response headers include `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-tenant`, `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`, and `x-ms-ags-diagnostic: {"ServerInfo":{"DataCenter":"West Europe","Slice":"E","Ring":"5","ScaleUnit":"002","RoleInstance":"AM2PEPF000107CE"}}`.

Network Tab Details:

- Name:** Telemetry, bOthH0HHAtcM.js, getEffectivePermissions(scope=""), 58LUq25ycsNaj.js, LfR2-TsQMwv.js, GJGglFB2jB97.js, templates?\$filter=(isof(%27microsoft.graph.securityBaselineTemplate%27)), ClientTrace, batch?api-version=2020-06-01
- 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-tenant`
 - `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"}}`



Headers

Payload

Preview

Response


Initiator

Timing

General

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

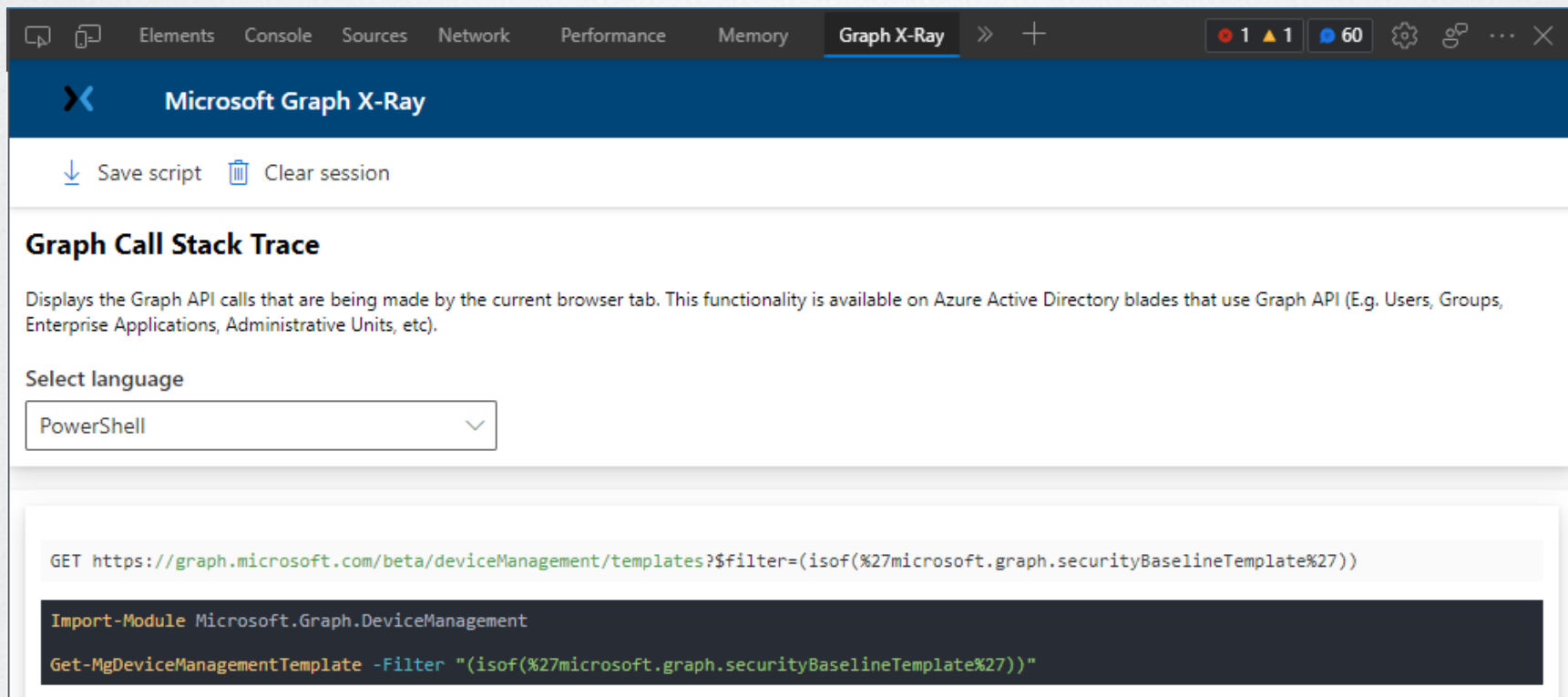
Request Method: GET

Status Code:  200 OK

Remote Address: 40.126.32.161:443

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





The image shows the Microsoft Graph X-Ray web application interface. At the top is a dark navigation bar with tabs for Elements, Console, Sources, Network, Performance, Memory, and Graph X-Ray (which is selected). To the right of the tabs are status indicators: a red circle with '1', a yellow triangle with '1', and a blue circle with '60'. Below the navigation bar is a blue header with the Microsoft Graph X-Ray logo and name. Underneath the header are two buttons: 'Save script' (with a download icon) and 'Clear session' (with a trash icon). The main content area has a section titled 'Graph Call Stack Trace' with a descriptive paragraph. Below this is a 'Select language' dropdown menu currently set to 'PowerShell'. At the bottom, there is a code block containing a REST API call and two PowerShell commands.

Microsoft Graph X-Ray

↓ Save script 🗑️ Clear session

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'))

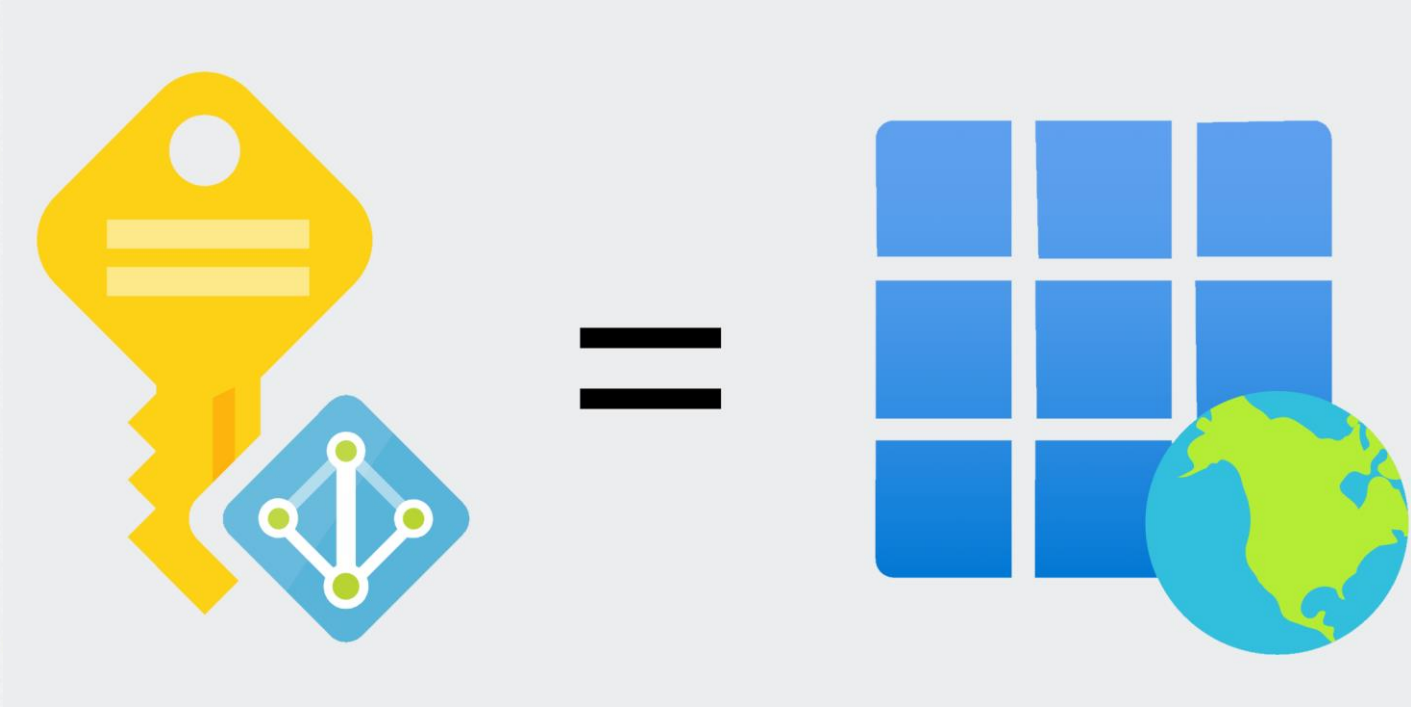
Import-Module Microsoft.Graph.DeviceManagement

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





MICROSOFT 365



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INSPARK

Microsoft

MICROSOFT 365

Home > Enterprise applications | All applications > memmonitor

memmonitor | Permissions

- Overview
- Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes (preview)

Security

- Permissions

« Refresh Review permissions Got feedback?

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.

Grant admin consent for klapwijk

Admin consent User consent

Search permissions

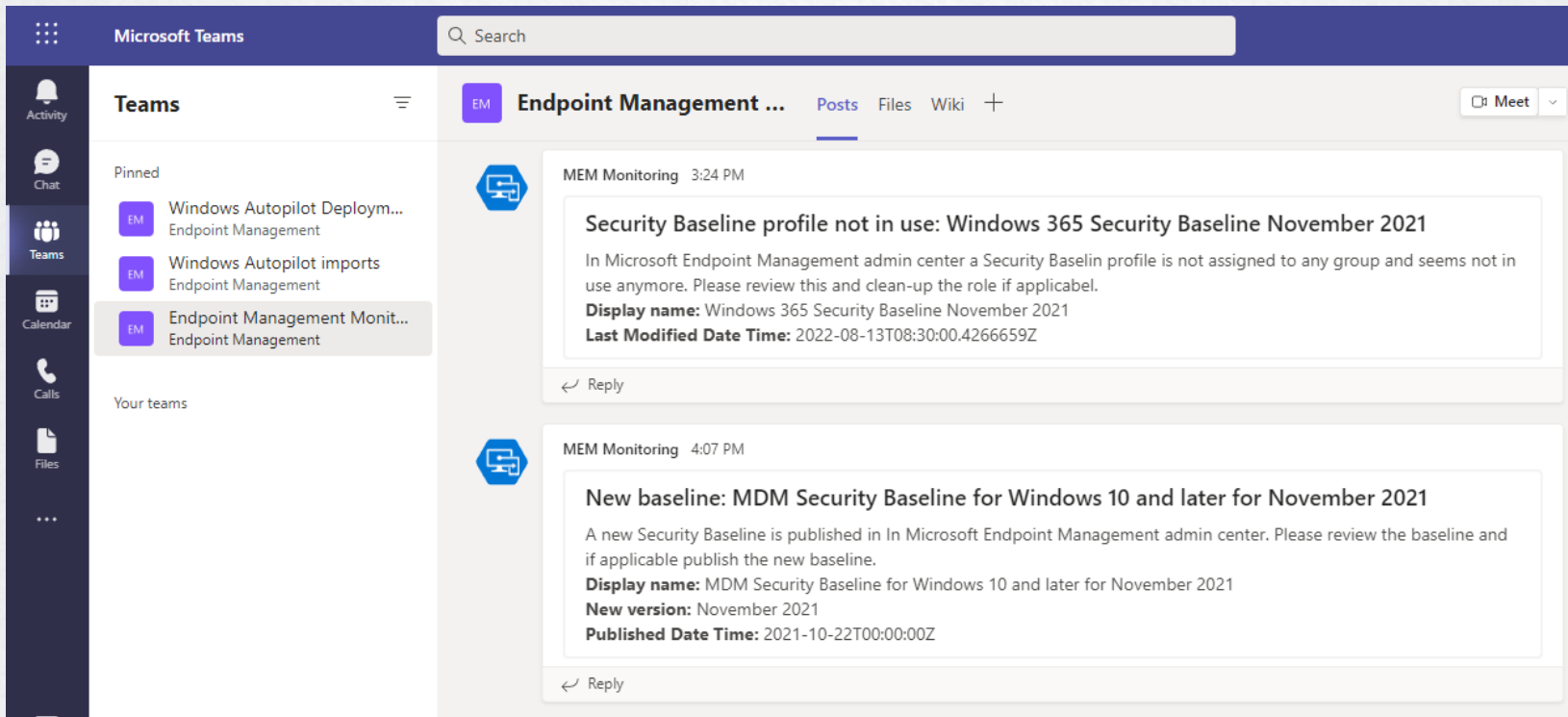
API Name	↑↓ Claim value	↑↓ Permission	↑↓ Type
Microsoft Graph			
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Read Microsoft Intune devices	Application
Microsoft Graph	DeviceManagementConfiguration.Read.All	Read Microsoft Intune device configuration and policies	Application



No code – Logic Apps



Teams notification!



The screenshot shows the Microsoft Teams interface. On the left is a navigation pane with icons for Activity, Chat, Teams, Calendar, Calls, and Files. The main area displays a list of pinned items under the 'Teams' tab, including 'Windows Autopilot Deploy...', 'Windows Autopilot imports', and 'Endpoint Management Monit...'. The right pane shows a chat conversation with a notification from 'MEM Monitoring' at 3:24 PM. The notification text reads: 'Security Baseline profile not in use: Windows 365 Security Baseline November 2021'. It includes a detailed description: '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.' and metadata: 'Display name: Windows 365 Security Baseline November 2021' and 'Last Modified Date Time: 2022-08-13T08:30:00.4266659Z'. Below the notification is a 'Reply' button. A second notification from 'MEM Monitoring' at 4:07 PM is also visible, titled 'New baseline: MDM Security Baseline for Windows 10 and later for November 2021', with details about a new security baseline being published and its version and date.

Microsoft Teams

Search

Teams

Pinned

- Windows Autopilot Deploy... Endpoint Management
- Windows Autopilot imports Endpoint Management
- Endpoint Management Monit... Endpoint Management

Your teams

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

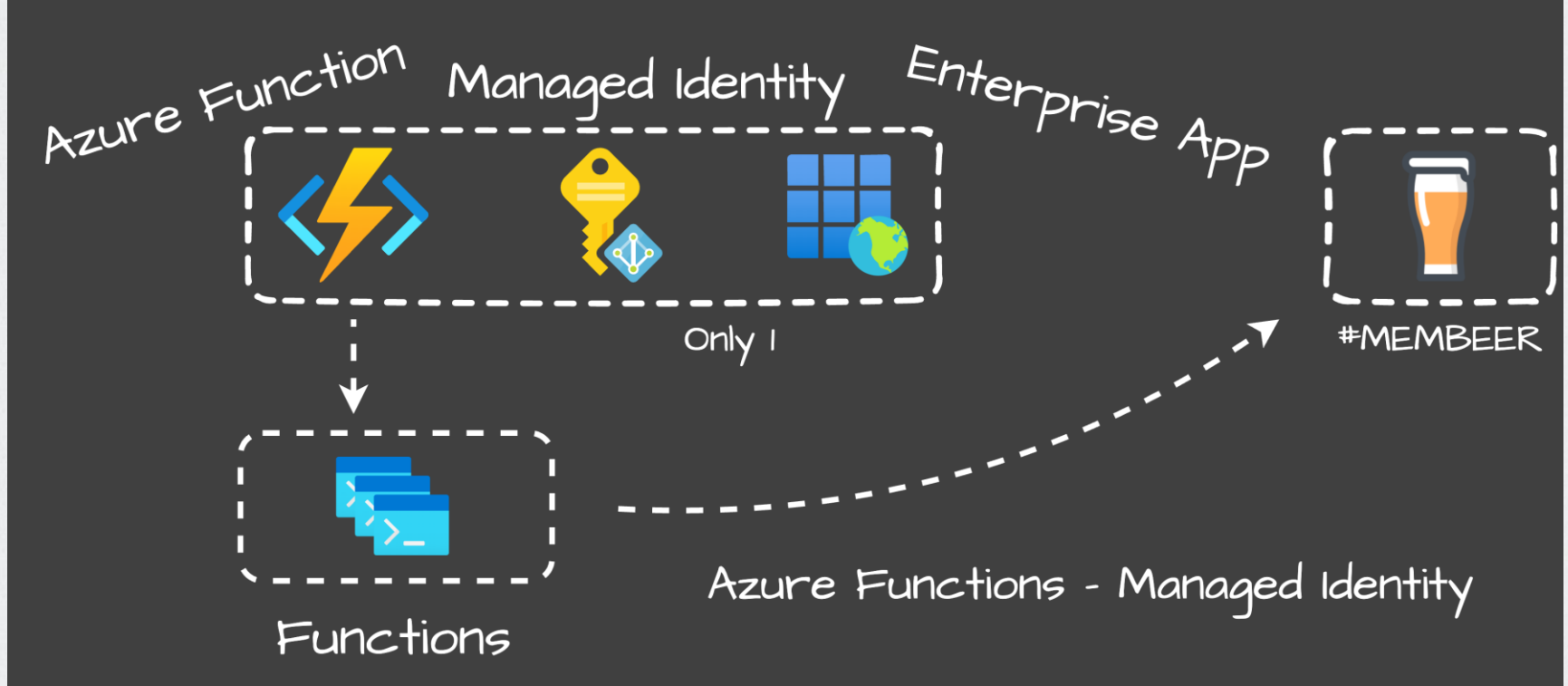
Published Date Time: 2021-10-22T00:00:00Z

Reply



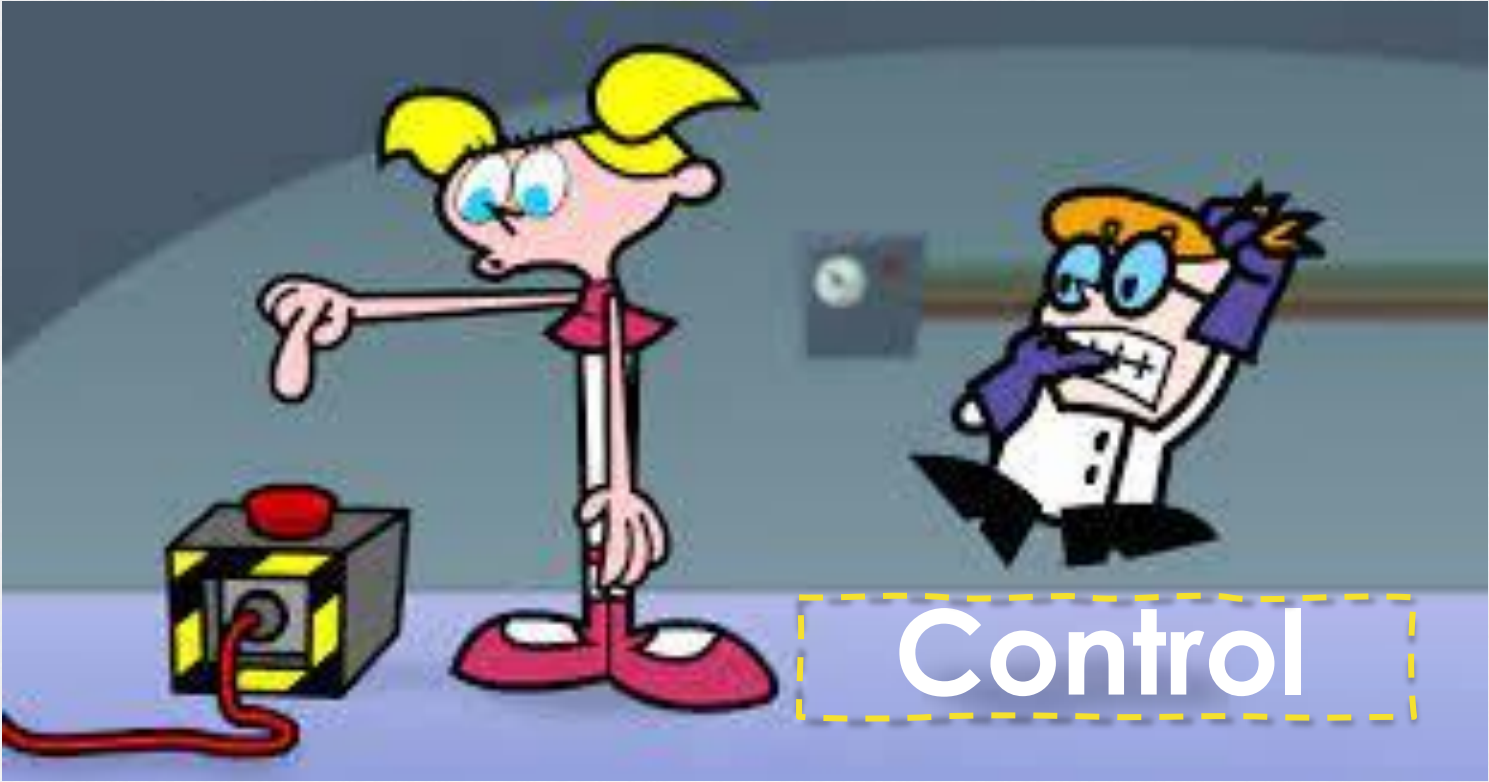
A man with a full brown beard and a gold crown with red and green jewels is shown from the chest up. He is wearing a black tuxedo jacket over a white shirt with black buttons. He has a serious, questioning expression and is holding his right hand near his chin. The background is dark. The text "Azure Functions?" is overlaid in white, sans-serif font across the center of the image.

Azure Functions?





MICROSOFT 365

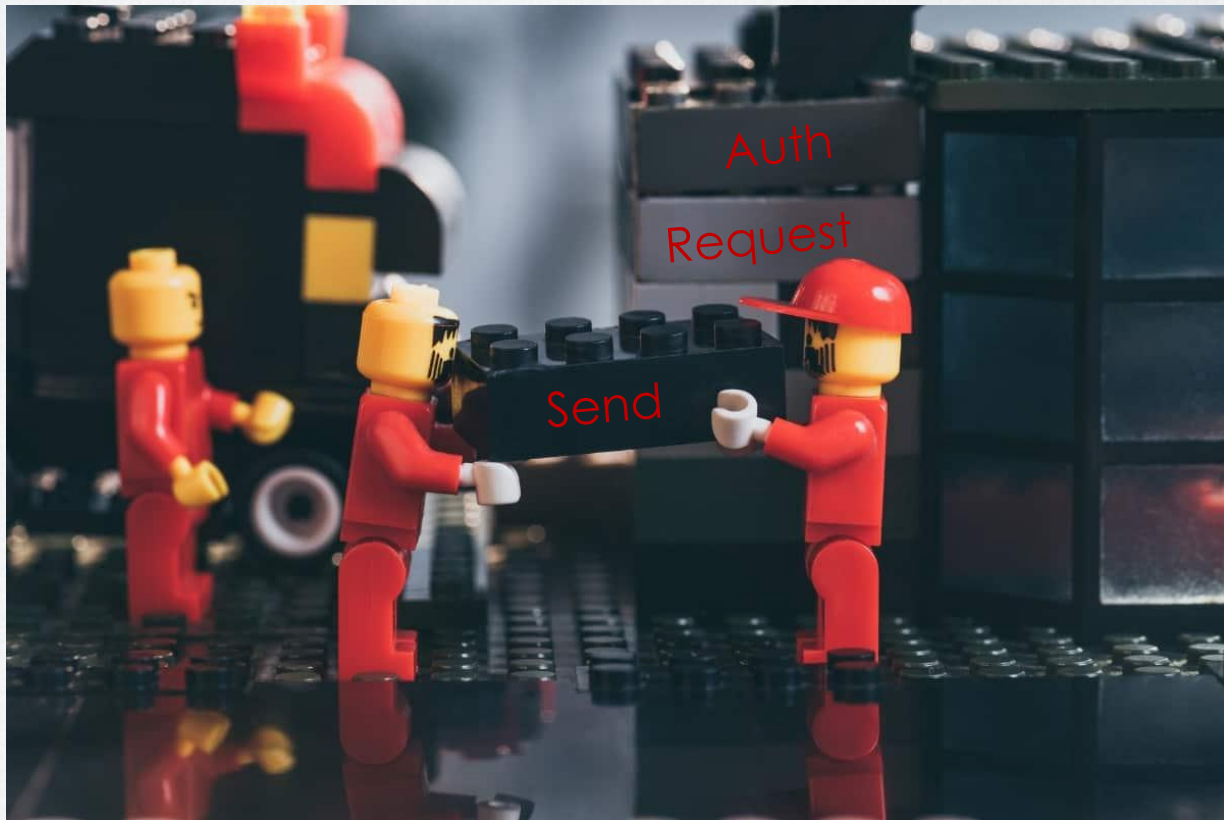




MICROSOFT 365

Efficiency

Be DRY



Delta-N
Connecting the Cloud

cegeka

ANNO

LIQUIT

INS PARK

Microsoft

membermonitor | Functions ...

Function App



Create



Refresh



Delete



Overview



Activity log



Access control (IAM)



Tags



Diagnose and solve problems



Microsoft Defender for Cloud



Events (preview)

Functions



Functions



App keys



App files



Proxies



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



Filter by name...



Name ↑↓

Trigger ↑↓



Security-BaselineVersionCheck

Timer



Security-UnAssignedBaselines

Timer



Security-BaselineVersionCheck | Code + Test ...

Function

Save Discard Refresh Test/Run Test integration Upload

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

membermonitor \ Security-BaselineVersionCheck \

run.ps1

```
11 Write-Output "PowerShell timer trigger function ran! TIME: $currentTime"
12 try {
13     ...import-module .\Modules\mem-monitor-functions.psm1
14 }
15 catch {
16     ...Write-Error "Functions module not found!"
17     ...exit;
18 }
19 try {
20     ...Get-AuthApiToken -resource $env:graphApiUrl
21 }
22 catch {
23     ...Throw "No token received, $_"
24 }
25
26 try {
27     ...Write-Information "Searching for security baselines"
28     ...$getUrl = "{0}/beta/deviceManagement/templates?$filter=(templateType%20eq%20'securityBaseline')%20or%20(templateTyp
29     ...$results = Invoke-RestMethod -URI $getUrl -Method GET -Headers $authHeader
```



MICROSOFT 365

Final words



To code



Not to code



Delta-N
Connecting the Cloud

cegeka

ANW

LIQUIT

INS PARK

Microsoft



MICROSOFT 365

Please provide feedback



Delta-N
Connecting the Cloud

 cegeka

 ANW

 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