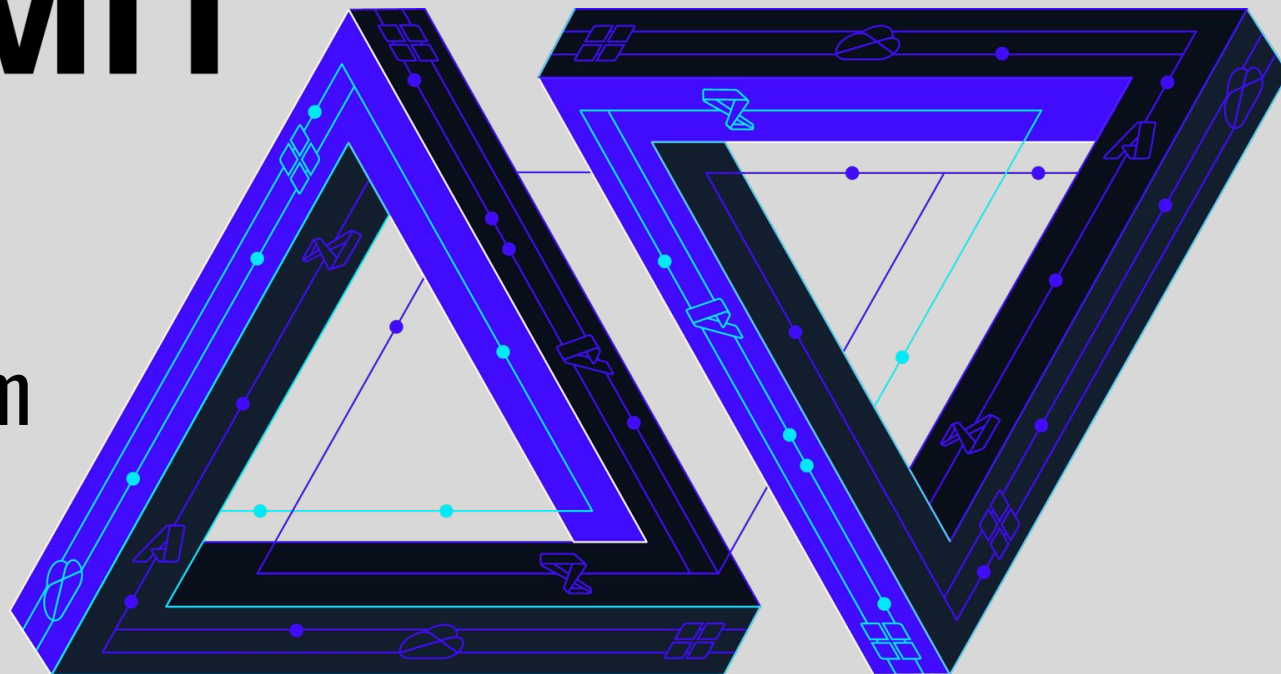


MS TECH SUMMIT

Ochrona wielu tenantów z użyciem
Azure Sentinel i Azure Lighthouse

Konrad Sagała
Cloud Security Architect, Alior Bank

 www.mstechsummit.pl



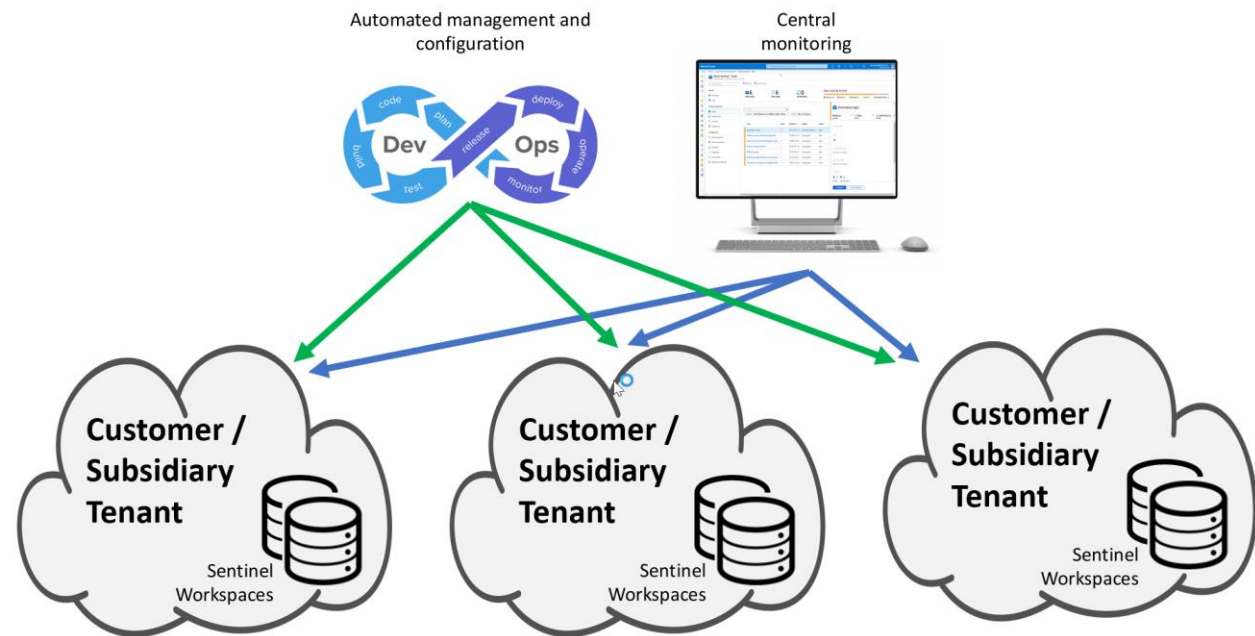
- Cloud Security Architect - Azure
- Microsoft Certified Trainer
- Microsoft MVP since 2007 – M365 Apps & Services
- Twitter - [@sagus](https://twitter.com/sagus)
- LinkedIn - [@konradsagala](https://www.linkedin.com/in/konradsagala)
- Github - <https://github.com/ksagala>
- Blog – <https://pepugmaster.blogspot.com>
- Hobby - Śpiew, Taniec, Podróże



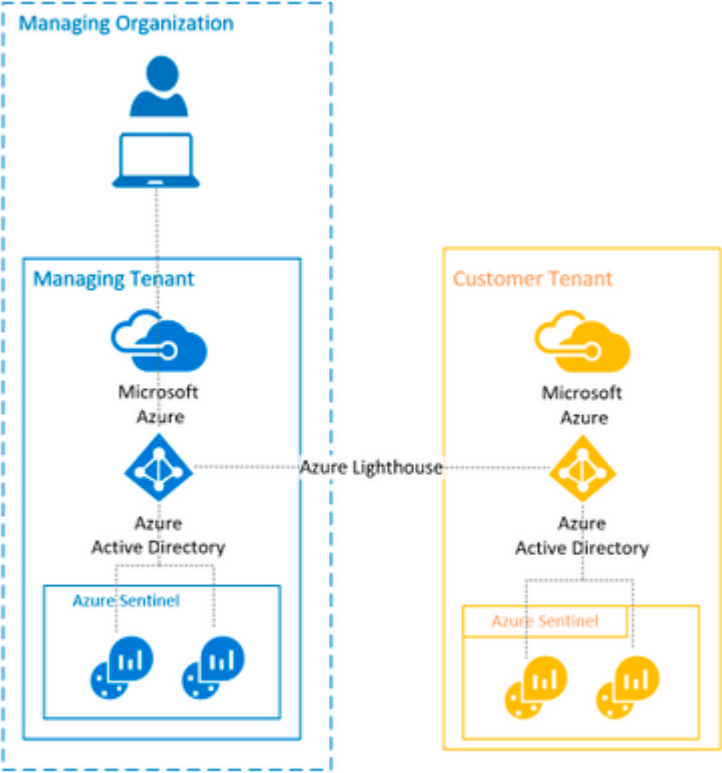
- Scenariusze
- Azure Lighthouse
- Wykorzystanie
- Workspace manager (preview)

Dlaczego niektórym firmom nie wystarczy jeden workspace Sentinel?

- Dostęp właścicieli danych do konkretnych zasobów (resource RBAC)
- Firma globalna, podział na global SOC i regionalne SOC,
- Compliance (konieczność przechowywania danych w danym kraju/regionie)
- Rozdzielność kosztów między działami
- Wiele tenantów Azure AD
- MSSP i różni klienci
- CI/CD

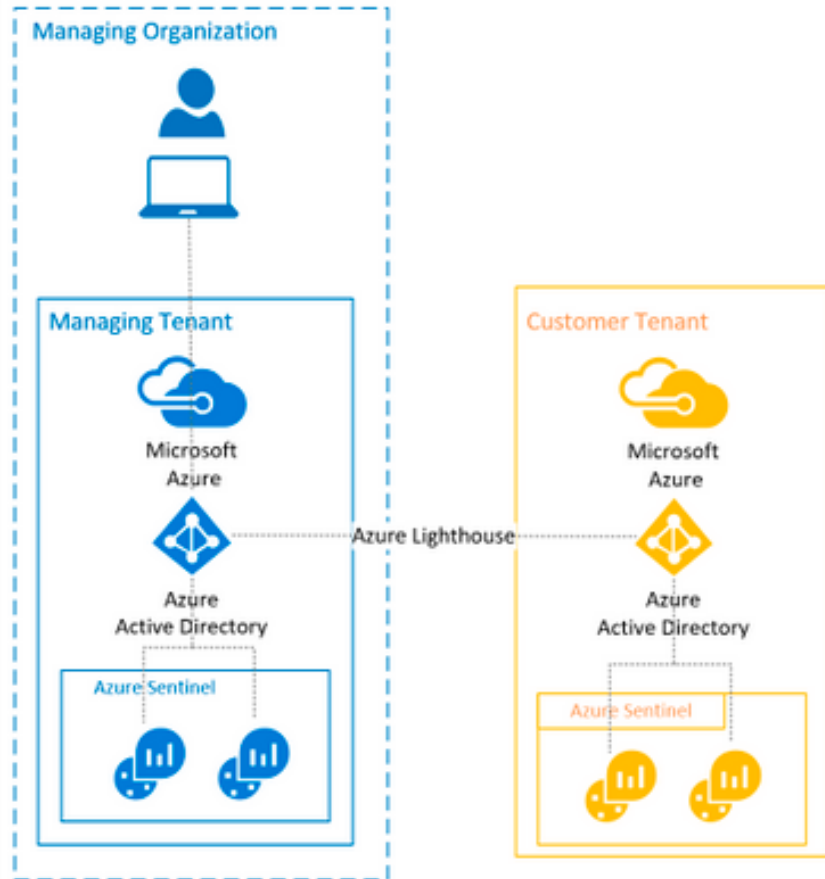


Azure Lighthouse



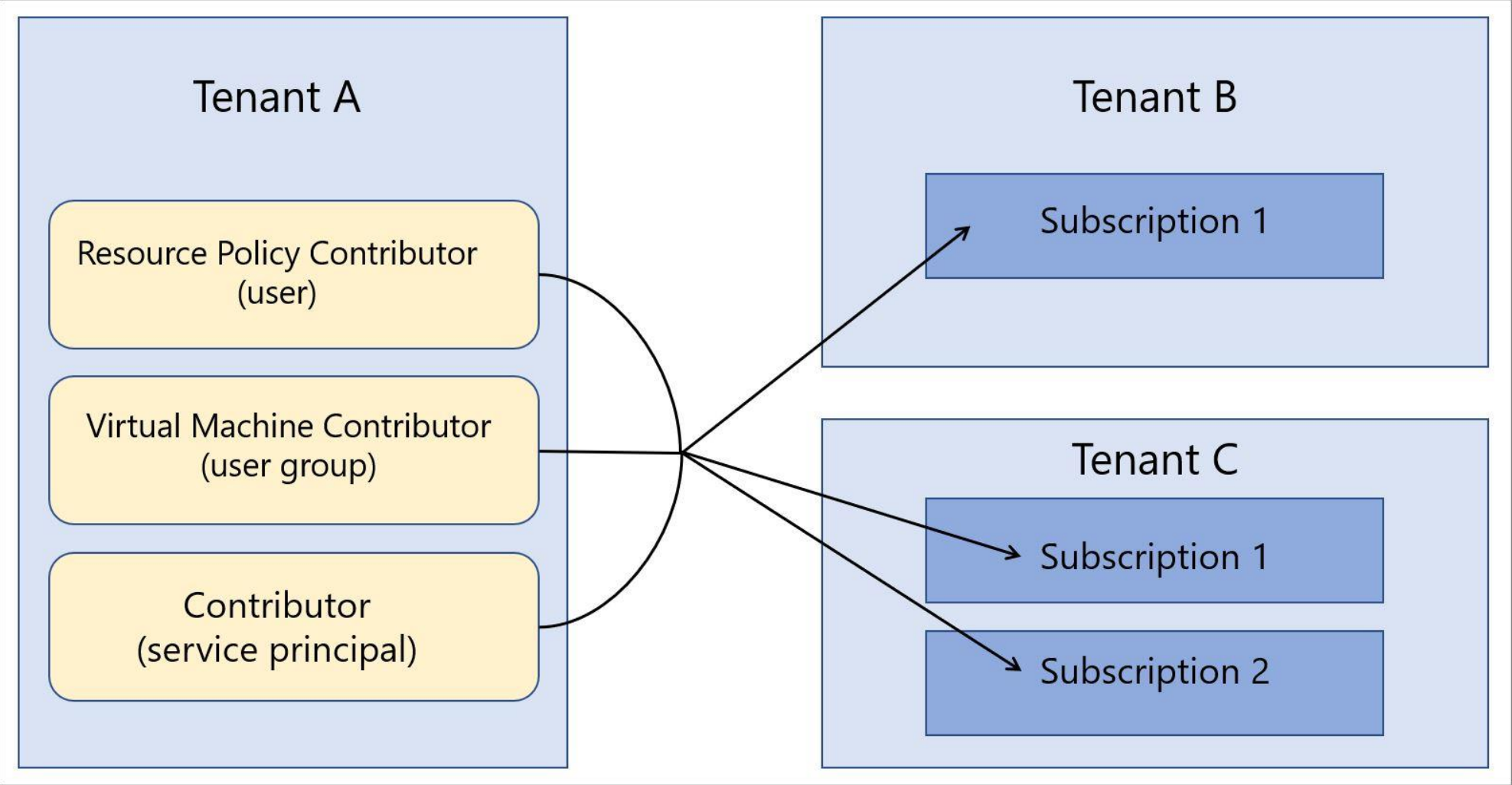
Lighthouse Architecture Diagram

AZURE LIGHTHOUSE



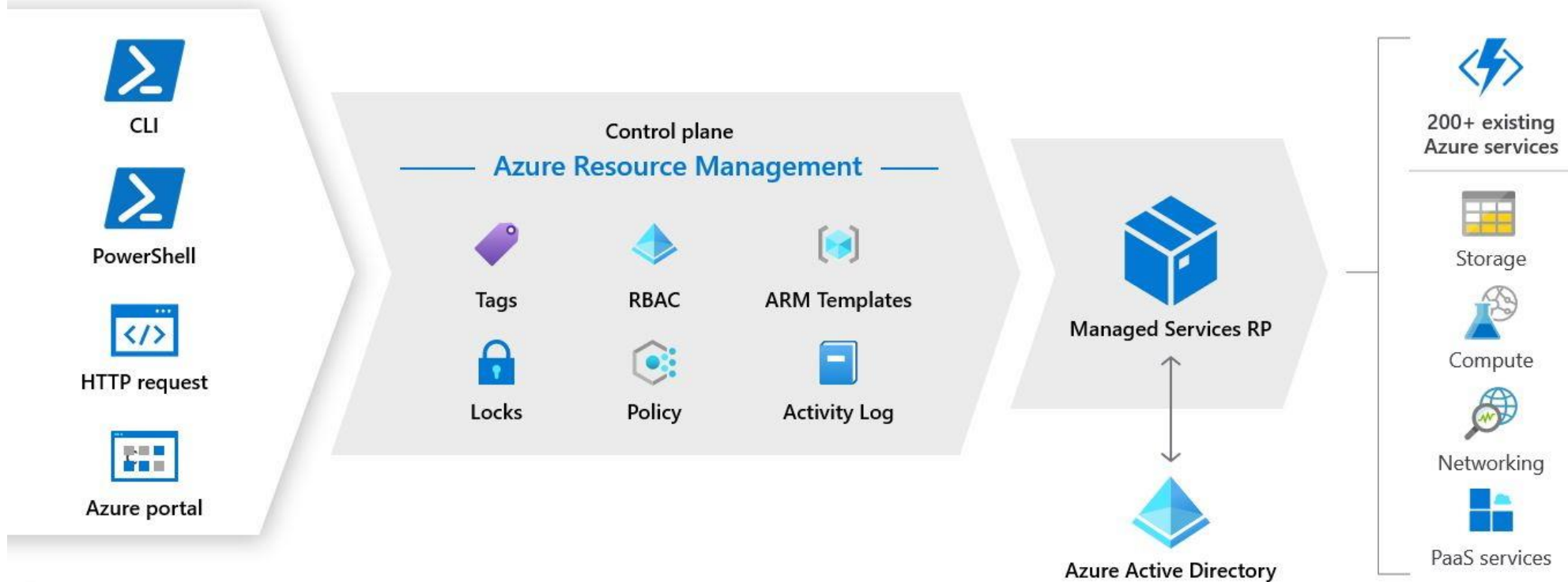
Lighthouse Architecture Diagram

- Brak dodatkowych kosztów
 - Zarządza zasobami w różnych regionach
 - Łatwy do wdrożenia poprzez szablon ARM
 - Obsługuje większość domyślnych ról Azure
- [Tenants, users, and roles in Azure Lighthouse scenarios](#)



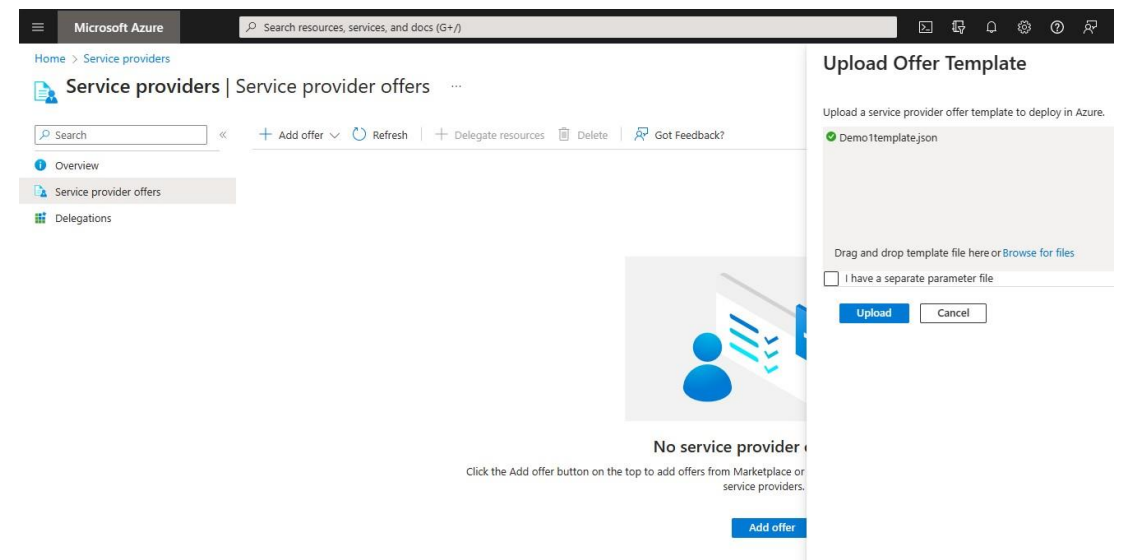
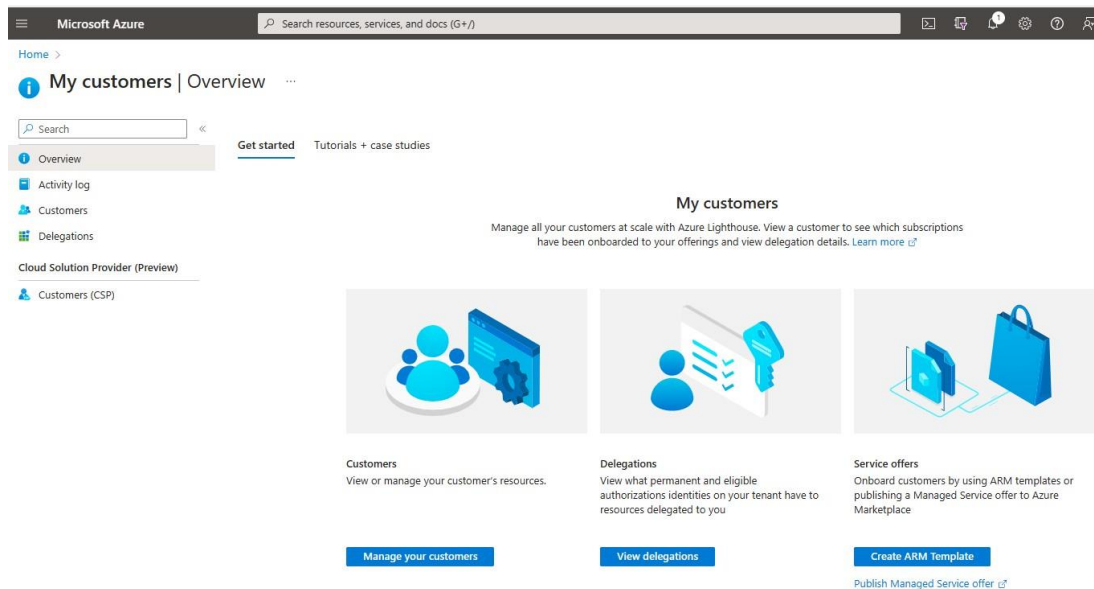
Azure delegated resource management creates logical (control plane) access to customer's environment for the service provider

- 1 Service provider initiates action on customer resource
- 2 Azure Resource Manager validates the request and calls Managed Service Resource Provider (RP)
- 3 Managed Service RP provides precise RBAC access
- 4 Service provider completes action on customer resource



Konfiguracja Lighthouse:

1. Z szablonu ARM ręcznie
<https://github.com/Azure/Azure-Lighthouse-samples/>
2. Z portalu Azure, korzystając z kreatora
[Onboard a customer to Azure Lighthouse - Azure Lighthouse](#)



3. Wdrożenie szablonu ARM z CLI/Powershell/Portalu

1. Widok wielu obszarów (max 100 workspaces)

[Home](#) >

Microsoft Sentinel

PEPUG

Create

Manage view

Refresh

Export to CSV

Open query

View incidents

Filter for any field...

Subscription equals 2 of 6 selected

Resource group equals all



Location equals all

Add filter

Run the 'View incidents' command(s) on the selected resource(s)

Showing 1 to 2 of 2 records.

No grouping

<input checked="" type="checkbox"/> Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Directory 1
<input checked="" type="checkbox"/>  ksgoms	oms-rsc	West Europe	Visual Studio Premium with MSDN	KSG MVP V
<input checked="" type="checkbox"/>  pepug-law	law-mct	West Europe	Platformy MSDN	PEPUG

2. Wykorzystanie KQL – alerty, tropienie, etc.

union
workspace("/subscriptions/<subld>/resourcegroups/<RGName>/providers/microsoft.OperationallInsights/workspaces/<wName1>").SecurityEvent,
workspace("/subscriptions/<subld>/resourcegroups/<RGName>/providers/microsoft.OperationallInsights/workspaces/<wName2>").SecurityEvent
Zapisujemy to jako funkcję unionSecuirtyEvent i można już pracować na zagregowanych zdarzeniach:
unionSecurityEvent | where ...

WYKORZYSTANIE - ROZBUDOWA WORKBOOKA

Home > Microsoft Sentinel | Workbooks >

Azure AD Sign-in logs - All workspaces

pepug-law

Done Editing Open Settings Edit Refresh Alerts Link Code Smile ? Help

Sign-in Analysis

2 Editing parameters item: parameters - 1

Settings Advanced Settings Style </> Advanced Editor

Style
Add Parameter Pills

Required?	Parameter name	Display name
<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Apps	
<input checked="" type="checkbox"/>	UserNamePrefix	UserNamePrefix
<input checked="" type="checkbox"/>	Users	UserName
<input checked="" type="checkbox"/>	Category	
<input checked="" type="checkbox"/>	Workspace	Workspace

TimeRange: Last 30 days Apps: All UserNamePrefix: All UserName: All

Done Editing Cancel Add Move Clone Remove

Edit Parameter

pepug-law

Save Revert changes Cancel ? Help

Settings Advanced Settings

Parameter name * Workspace

Display name Workspace

Parameter type Resource picker

Required? ☒

Allow multiple selections ☒

Limit multiple selections ☐

Delimiter ,

Quote with '

Explanation What is this parameter used for?

Hide parameter in reading mode ☐

Get data from Workbook Resources Query JSON Owner Resource

Subscriptions Azure Resource Graph Query

Query (change)

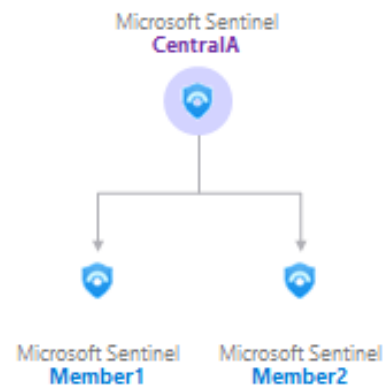
Run Query All Subscriptions Samples

```
resources | where type =~ 'Microsoft.operationsmanagement/solutions' | where name contains 'SecurityInsights' | project id = tostring(properties.workspaceResourceId)
```

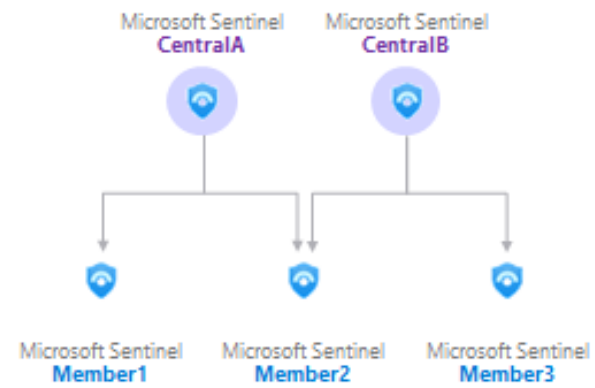
```
resources | where type =~ 'Microsoft.operationsmanagement/solutions' | where name contains 'SecurityInsights' | project id = tostring(properties.workspaceResourceId)
```

Possible Workspace Manager Architectures

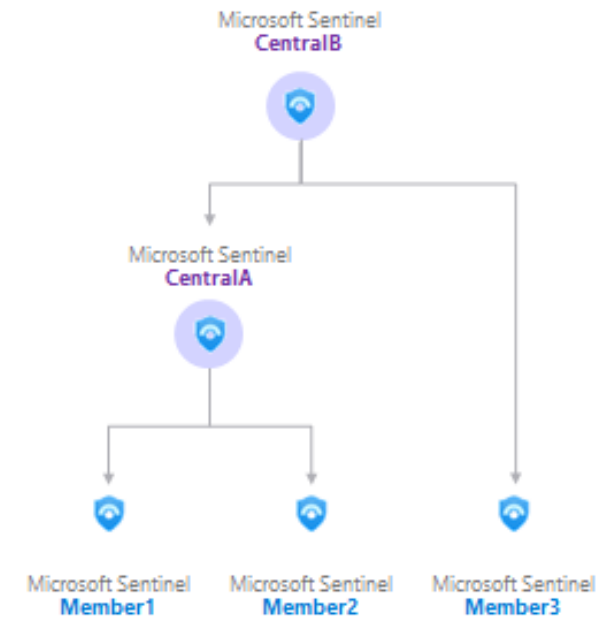
Simple / Direct-Link



Co-Management



N-Tier



WORKSPACE MANAGER (PREVIEW)

Możemy synchronizować z nadrzędnego workspace:

- Analytics rules
- Automation rules (excluding Playbooks)
- Parsers, Saved Searches and Functions
- Hunting and Livestream queries
- Workbooks

Ograniczenia (mogą ulec zmianie):

- Playbooks attributed or attached to analytics and automation rules aren't currently supported.
- Workbooks stored in bring-your-own-storage aren't currently supported.
- Workspace manager only manages content items published from the central workspace. It doesn't manage content created locally from member workspace(s).
- Currently, deleting content residing in member workspace(s) centrally via workspace manager isn't supported.

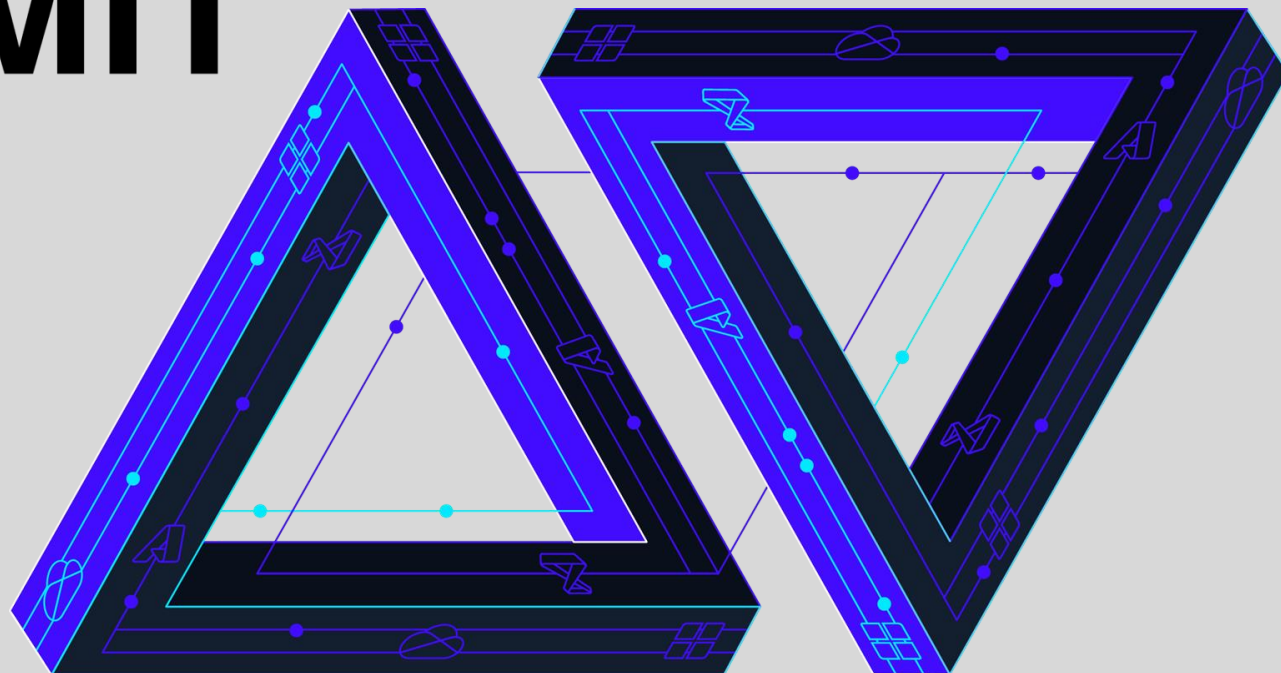


MS TECH SUMMIT

ORGANIZATOR:

AcademicPartners
FUNDACJA

Dziękujemy za uwagę
Zapraszamy do zadawania pytań
oraz **oceny wystąpienia**
pod nagraniem.



www.mstechsummit.pl
