

yellow arrow

# Beheer meerdere Sentinel omgevingen met Azure Lighthouse



18-06-2024



Tom Rolvers

# Wie ben ik?

## Tom Rolvers

Werkzaam bij yellow arrow

Vrijetijd

- Customer Connection Program
- Wielrennen
- Hack the Box & TryHackMe
- Community avonden



Geen phishing



Github: awt-tom

Blog: <https://azurewithtom.com>

Linkedin: <https://linkedin.com/in/tomrolvers>

# Inhoudsopgave

**1** Wat is Azure Lighthouse

**2** Implementatie overzicht

**3** Groepen structuur

**4** JSON Template

**5** Workspace Manager

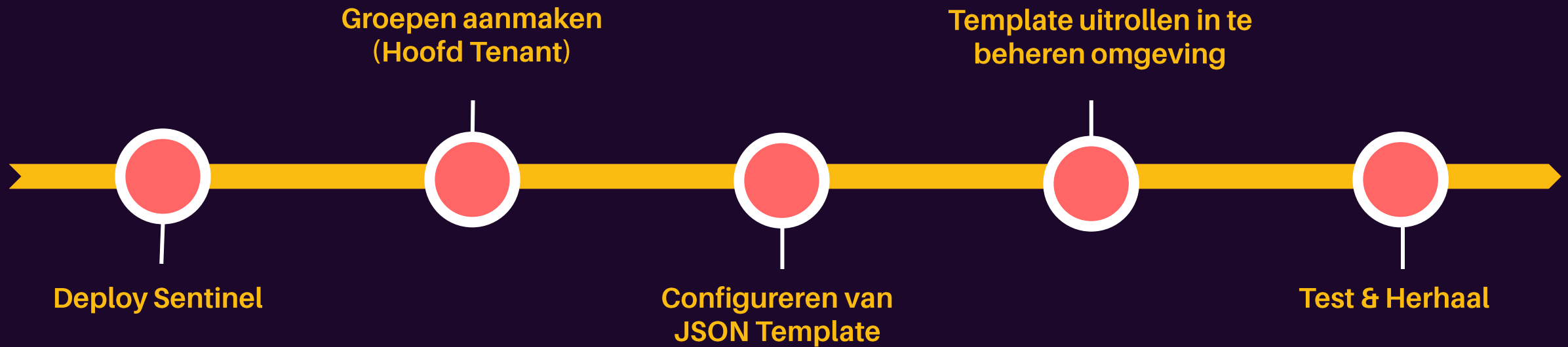
**6** Extra mogelijkheden & Hulpmiddel



# Wat is Azure Lighthouse?

- Gecentraliseerd beheer
- Meer grip op toegangsbeheer
- Overzicht over andere tenants
- Unified logs

# Implementatie overzicht



# Groepen structuur

Role	Permissions
Microsoft Sentinel Reader	Can view data, incidents, workbooks, and other Microsoft Sentinel Resources.
Microsoft Sentinel Responder	Can manage incidents (assign, dismiss, change) in addition to permissions for Microsoft Sentinel Reader.
Microsoft Sentinel Contributor	Can install and update solutions from content hub, create and edit resources (workbooks, analytics rules, etc.), in addition to permissions for Microsoft Sentinel Responder.
Microsoft Sentinel Playbook Operator	Can list, view, and manually run playbooks.
Microsoft Sentinel Automation Contributor	Allows Microsoft Sentinel to add playbooks to automation rules. Not meant for user accounts.



# Groepen structuur


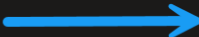
Role	Role ID
Microsoft Sentinel Reader	8d289c81-5878-46d4-8554-54e1e3d8b5cb
Microsoft Sentinel Responder	3e150937-b8fe-4cfb-8069-0eaf05ecd056
Microsoft Sentinel Contributor	ab8e14d6-4a74-4a29-9ba8-549422addade
Microsoft Sentinel Playbook Operator	51d6186e-6489-4900-b93f-92e23144cca5
Microsoft Sentinel Automation Contributor	f4c81013-99ee-4d62-a7ee-b3f1f648599a

# Groepen structuur

Role	Group name
Microsoft Sentinel Reader	Azure with Tom - Level 1 SOC
Microsoft Sentinel Responder	Azure with Tom - Level 2 SOC
Microsoft Sentinel Contributor	Azure with Tom - Sentinel Contributor
Microsoft Sentinel Playbook Operator	Azure with Tom - Playbook Operator
Microsoft Sentinel Automation Contributor	Azure with Tom - Automation Contributor



# Groepen structuur

<input type="checkbox"/>	Name ↑↓		Object Id	Group type	Membership type
<input type="checkbox"/>	 Lighthouse test group		cdf535a3-5aa9-4c42-8e76-3d7476947add	Security	Assigned

# JSON Template

mspOfferName:

Type: String

Description: Unique name for your offer.

DefaultValue: Replace  
NAMEOFYOUROFFER with your specific  
offer name.

```
</> JSON
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTempl
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "mspOfferName": {
6       "type": "string",
7       "metadata": {
8         "description": "Specify a unique name for your offer"
9       },
10      "defaultValue": "NAMEOFYOUROFFER"
11    },
12    "mspOfferDescription": {
13      "type": "string",
14      "metadata": {
15        "description": "Name of the Managed Service Provider offering"
16      },
17      "defaultValue": "Delegated Subscription access for the use of Microsoft Sentinel"
18    }
19  },
20  "variables": {
21    "mspRegistrationName": "[guid(parameters('mspOfferName'))]",
22    "mspAssignmentName": "[guid(parameters('mspOfferName'))]",
23    "managedByTenantId": "YOURTENANTID",
24    "authorizations": [
25      {
26        "principalId": "GROUPOBJECTID",
27        "roleDefinitionId": "8d289c81-5878-46d4-8554-54e1e3d8b5cb",
28        "principalIdDisplayName": "AzurewithTom - 1e lijn SOC"
29      }
30    ]
31  }
32 }
```

# JSON Template

mspOfferDescription:

Type: String

Description: Name of the Managed Service Provider offering.

DefaultValue: Default is set to: Delegated Subscription access for the use of Microsoft Sentinel. Modify as needed.

```
</> JSON
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTemp1
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "mspOfferName": {
6       "type": "string",
7       "metadata": {
8         "description": "Specify a unique name for your offer"
9       },
10      "defaultValue": "NAMEOFOUROFFER"
11    },
12    "mspOfferDescription": {
13      "type": "string",
14      "metadata": {
15        "description": "Name of the Managed Service Provider offering"
16      },
17      "defaultValue": "Delegated Subscription access for the use of Microsoft Sentinel"
18    }
19  },
20  "variables": {
21    "mspRegistrationName": "[guid(parameters('mspOfferName'))]",
22    "mspAssignmentName": "[guid(parameters('mspOfferName'))]",
23    "managedByTenantId": "YOURTENANTID",
24    "authorizations": [
25      {
26        "principalId": "GROUPOBJECTID",
27        "roleDefinitionId": "8d289c81-5878-46d4-8554-54e1e3d8b5cb",
28        "principalIdDisplayName": "AzurewithTom - 1e lijn SOC"
29      }
30    ]
31  }
32 }
```

# JSON Template

Automatically generated GUIDs based on mspOfferName. No change needed.

```
</> JSON
1  {
2    "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTempl
3    "contentVersion": "1.0.0.0",
4    "parameters": {
5      "mspOfferName": {
6        "type": "string",
7        "metadata": {
8          "description": "Specify a unique name for your offer"
9        },
10       "defaultValue": "NAMEOFYOUROFFER"
11     },
12     "mspOfferDescription": {
13       "type": "string",
14       "metadata": {
15         "description": "Name of the Managed Service Provider offering"
16       },
17       "defaultValue": "Delegated Subscription access for the use of Microsoft Sentinel"
18     },
19   },
20   "variables": {
21     "mspRegistrationName": "[guid(parameters('mspOfferName'))]",
22     "mspAssignmentName": "[guid(parameters('mspOfferName'))]",
23     "managedByTenantId": "YOURTENANTID",
24     "authorizations": [
25       {
26         "principalId": "GROUPOBJECTID",
27         "roleDefinitionId": "8d289c81-5878-46d4-8554-54e1e3d8b5cb",
28         "principalIdDisplayName": "AzurewithTom - 1e lijn SOC"
29       },
30     ]
31   }
32 }
```

# JSON Template

Replace YOURTENANTID with your specific Azure Tenant ID.

```
</> JSON
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTempl
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "mspOfferName": {
6       "type": "string",
7       "metadata": {
8         "description": "Specify a unique name for your offer"
9       },
10      "defaultValue": "NAMEOFYOUROFFER"
11    },
12    "mspOfferDescription": {
13      "type": "string",
14      "metadata": {
15        "description": "Name of the Managed Service Provider offering"
16      },
17      "defaultValue": "Delegated Subscription access for the use of Microsoft Sentinel"
18    }
19  },
20  "variables": {
21    "mspRegistrationName": "[guid(parameters('mspOfferName'))]",
22    "mspAssignmentName": "[guid(parameters('mspOfferName'))]",
23    "managedByTenantId": "YOURTENANTID",
24    "authorizations": [
25      {
26        "principalId": "GROUPOBJECTID",
27        "roleDefinitionId": "8d289c81-5878-46d4-8554-54e1e3d8b5cb",
28        "principalIdDisplayName": "AzurewithTom - 1e lijn SOC"
29      },

```

# JSON Template

Principal ID: Your group object ID

Role Definition ID: ID based on the role you want to use

Principal ID Display name: Name of the group

```
</> JSON
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTempl
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "mspOfferName": {
6       "type": "string",
7       "metadata": {
8         "description": "Specify a unique name for your offer"
9       },
10      "defaultValue": "NAMEOFOUROFFER"
11    },
12    "mspOfferDescription": {
13      "type": "string",
14      "metadata": {
15        "description": "Name of the Managed Service Provider offering"
16      },
17      "defaultValue": "Delegated Subscription access for the use of Microsoft Sentinel"
18    }
19  },
20  "variables": {
21    "mspRegistrationName": "[guid(parameters('mspOfferName'))]",
22    "mspAssignmentName": "[guid(parameters('mspOfferName'))]",
23    "managedByTenantId": "YOURTENANTID",
24    "authorizations": [
25      {
26        "principalId": "GROUPOBJECTID",
27        "roleDefinitionId": "8d289c81-5878-46d4-8554-54e1e3d8b5cb",
28        "principalIdDisplayName": "AzurewithTom - 1e lijn SOC"
29      },
30    ]
31  }
32 }
```

# JSON template

Ga naar [portal.azure.com](https://portal.azure.com)  
en voeg een resource toe  
(Custom Deployment)

## Custom deployment ...

Deploy from a custom template

### Select a template

Basics

Review + create

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. [Learn more about template deployment](#) ↗



Build your own template in the editor

### Common templates



Create a Linux virtual machine



Create a Windows virtual machine



Create a web app



Create a SQL database



Azure landing zone

### Start with a quickstart template or template spec

Template source ⓘ



Quickstart template



Template spec

Quickstart template (disclaimer) ⓘ



# JSON Template

Voeg de template die  
zojuist gemaakt is toe.

### Edit template

Edit your Azure Resource Manager template

+ Add resource   ↑ Quickstart template   ↑ Load file   ↓ Download

<<

Parameters (2)

Variables (4)

Resources (2)

[variables('mspRegistrationName')]  
(Microsoft.ManagedServices/regis

[variables('mspAssignmentName')]  
(Microsoft.ManagedServices/regis

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "mspOfferName": {
6       "defaultValue": "AzurewithTom-Managed-SOC",
7       "type": "String",
8       "metadata": {
9         "description": "Specify a unique name for your offer"
10      }
11   },
12   "mspOfferDescription": {
13     "defaultValue": "Delegated Microsoft Sentinel access for AzurewithTom",
14     "type": "String",
15     "metadata": {
16       "description": "Name of the Managed Service Provider offering"
17     }
18   }
19 },
20 "variables": {
21   "mspRegistrationName": "[guid(parameters('mspOfferName'))]",
22   "mspAssignmentName": "[guid(parameters('mspOfferName'))]",
23   "managedByTenantId": "621xx765-b123-456d-a5af-3b65555xx69x7",
24   "authorizations": [
25     {
26       "principalId": "41fb71e8-668d-4bee-9bac-564da1465003",
27       "roleDefinitionId": "8d289c81-5878-46d4-8554-54e1e3d8b5cb",
28       "principalIdDisplayName": "Azure with Tom - Level 1 SOC"
29     },
30     {
31       "principalId": "6864ad7c-cfb4-4d6c-a3e1-210155035563",
32       "roleDefinitionId": "3e150937-b8fe-4cfb-8069-0eaf05ecd056",
33       "principalIdDisplayName": "Azure with Tom - Level 2 SOC"
34     }
35   ]
36 }
```

Save


Discard

# JSON Template

Controleer de gegevens inclusief de  
gewenste regio.

## Custom deployment

Deploy from a custom template



 New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →


Select a template

**Basics**


Review + create

### Template

 Customized template   
2 resources

 Edit template

 Edit parameters

 Visualize

### Project details

Deploying templates at subscription scope enables scenarios like applying policies and assigning roles at the subscription level. Subscription scope deployments are also used for creating resource groups and deploying resources in it. You can change the deployment scope by updating the schema in the template.

Subscription \* ⓘ

Azure with Tom – MPN

### Instance details

Region \* ⓘ

West Europe

Msp Offer Name ⓘ

AzurewithTom-Managed-SOC

Msp Offer Description ⓘ

Delegated Microsoft Sentinel access for AzurewithTom

Previous

Next

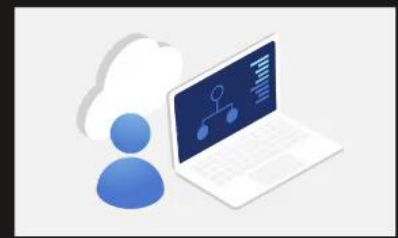
Review + create



Home >

## Grow your business with Azure Lighthouse

Businesses and service providers can easily work together on Azure. Service providers offer their expertise to efficiently manage multiple customer environments. Businesses can let experts manage their Azure infrastructure and services so they can focus on their core business. [Learn more](#)



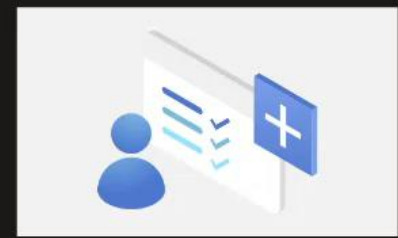
**Manage customers at scale**  
See which customers have been onboarded to your offerings and view delegated resources. [Learn more](#)

Manage your customers



**Ask for Azure Lighthouse.**  
Explore expert service providers who can manage your resources. [Learn more](#)

View AppSource Partners



**Control service provider access**  
Assign eligible authorizations that use Azure AD Privileged Identity Management to temporarily elevate access on a Just In Time basis. [Learn more](#)

View service provider offers

# Resource Provider

- Microsoft.OperationalInsights
- Microsoft.SecurityInsights

Azure with Tom Test Lab – MPN | Resource providers

Subscription

Search

3 Register Unregister Refresh Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Events

Cost Management

Cost analysis

Cost alerts

Budgets

Advisor recommendations

Billing

Invoices

External services

Payment methods

Partner information

Settings

Programmatic deployment

Resource groups

Resources

Preview features

Usage + quotas

Policies

Management certificates

My permissions

Resource providers 1

Deployments

Deployment stacks

Properties

Resource locks

Help

Support + Troubleshooting

Search

oper

Provider ↑	Status
<input type="radio"/> Microsoft.IoTOperations	NotRegistered
<input type="radio"/> Microsoft.IoTOperationsDataProcessor	NotRegistered
<input type="radio"/> Microsoft.IoTOperationsMQ	NotRegistered
<input type="radio"/> Microsoft.IoTOperationsOrchestrator	NotRegistered
<input checked="" type="radio"/> Microsoft.OperationalInsights	Registered
<input checked="" type="radio"/> Microsoft.OperationsManagement	Registered
<input type="radio"/> Microsoft.OperatorVoicemail	NotRegistered

# < In vijf stappen naar

Het beheer van meerdere  
Sentinel workspaces >



## > Deploy Sentinel

Deploy Sentinel op jouw manier.  
Zorg dat deze het zelfde werkt  
voor je SOC Analysten.



Recycle Bin



Search for apps, settings, and documents

Pinned

All apps >



Edge



Word



Excel



PowerPoint



Settings



OneNote



File Explorer



Recommended



Outlook (new)  
Recently added



Dev Home  
Recently added



Darth Vader

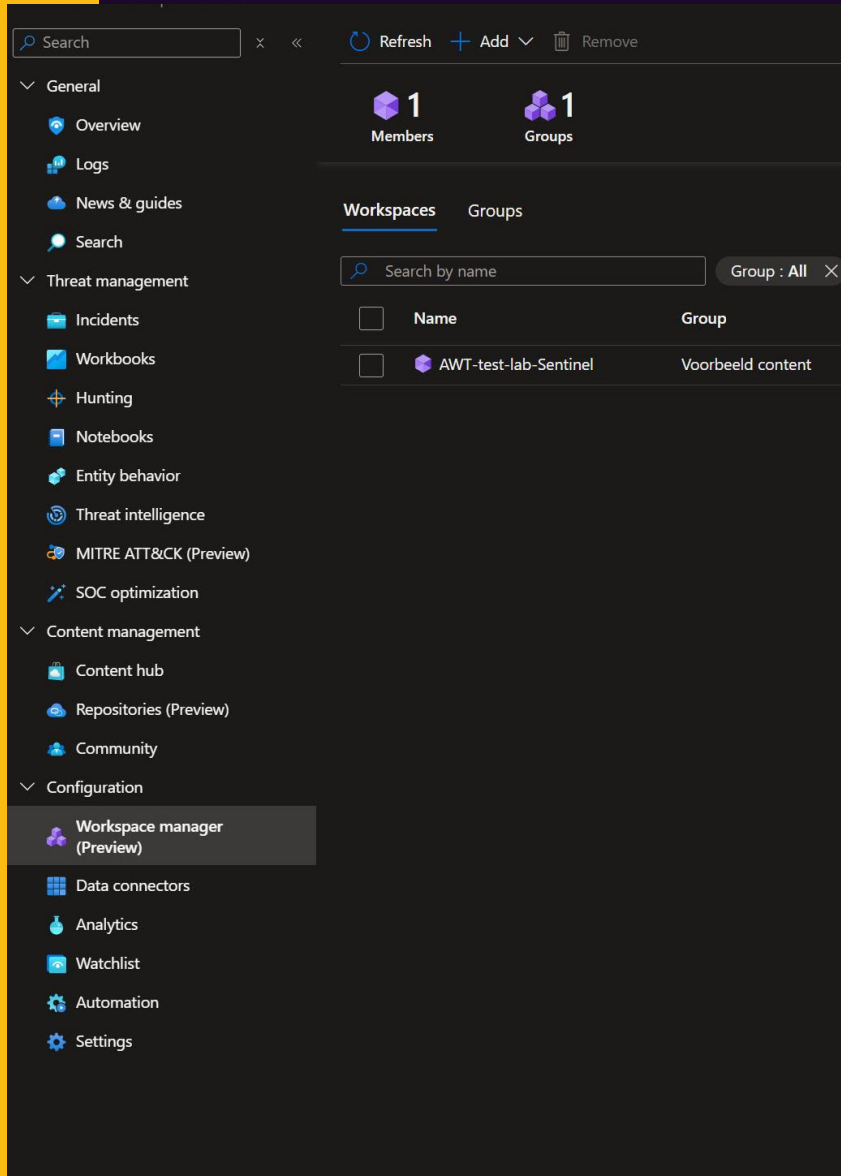


Search



# De Workspace Manager

- Gecentraliseerd beheer vanaf hoofd workspace
  - Meer grip op content
  - Makkelijk publiceren
- 
- (Max.Content: 200 items Workspace x Content)
  - Voorbeeld: 10 Sentinel workspaces met 20 Analytic Rules komt neer op 200.





# ◀ DEMO Video ▶

Home > Microsoft Sentinel

Microsoft Sentinel

Azure with Tom (azurewithtom.com)

+ Create ⚙️ Manage view ⌵ ⋮

Filter for any field...

Name ↑

AWT-SOC

AWT-test-lab-Sentinel

Microsoft Sentinel | Workspace manager (Preview) ⋮

Selected workspace: 'awt\_soc'

Search x ⌵ Refresh + Add ⌵ Remove

General

Overview (Preview)

Logs

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Watchlist

Automation

Settings

0 Members 0 Groups

Workspaces Groups

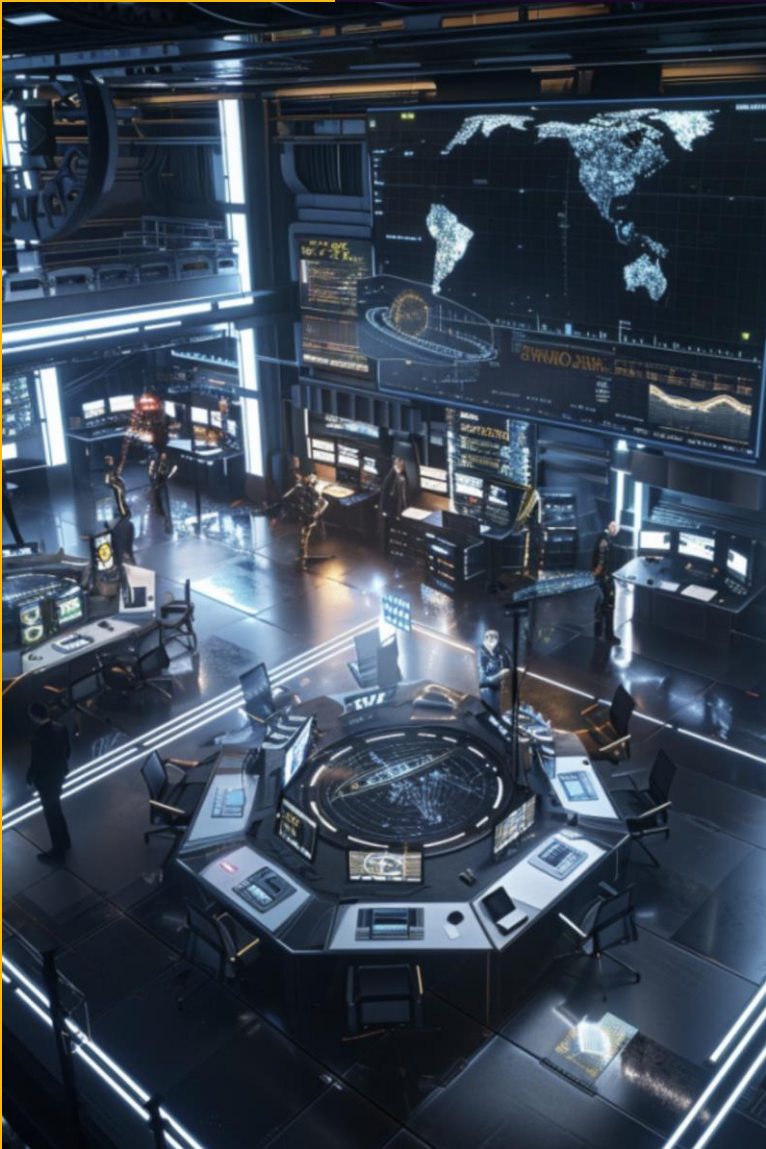
Search by name Group : All x Directory : All x Location : All x Resource group : All x Subscription : All x

Name	Group	Directory	Location
------	-------	-----------	----------

No workspaces found

Add workspaces

# Extra mogelijkheden



Voeg XDR overzicht  
toe



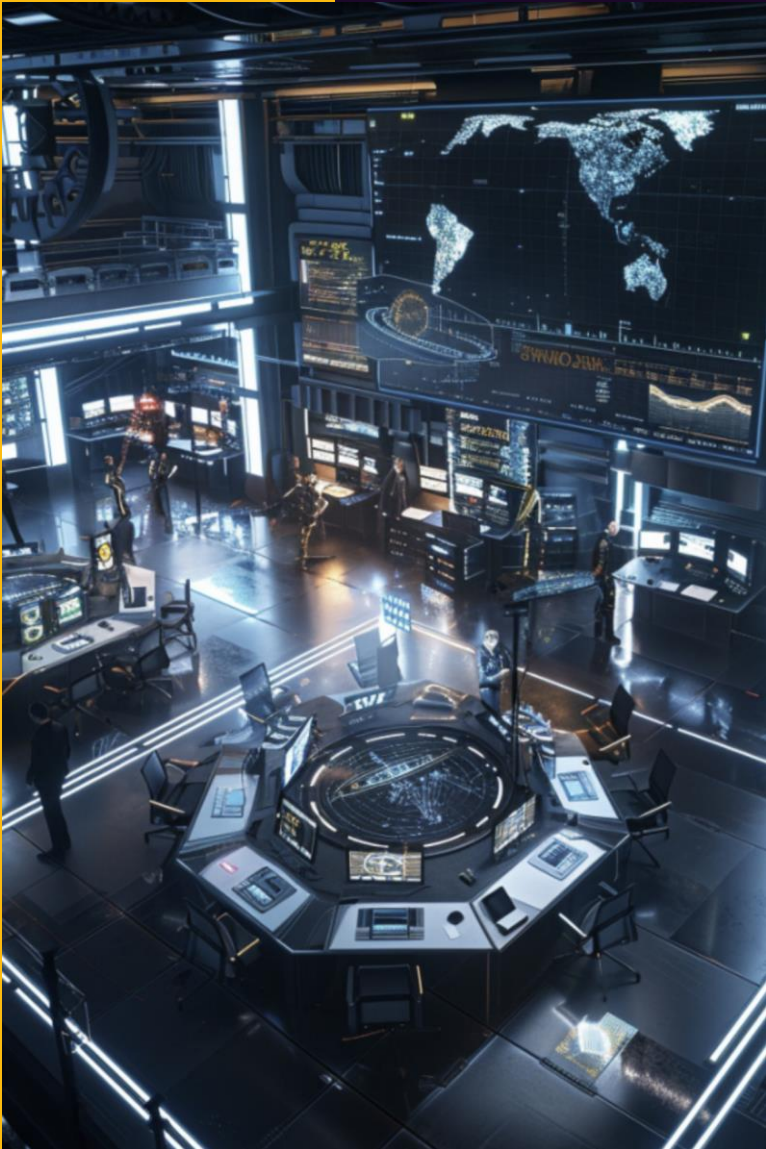
Sentinel test  
omgeving



Leeromgeving



# Extra mogelijkheden



Voeg XDR  
overzicht toe

- › Advanced Hunting
- › Bi-Directioneel
- › Samen nog krachtiger



Sentinel test  
omgeving



Leeromgeving

# Extra mogelijkheden



Voeg XDR overzicht  
toe



Sentinel test  
omgeving

- › Testen van regels
- › Testen van Playbooks
- › Dummy data



Leeromgeving

# Extra mogelijkheden



Voeg XDR overzicht  
toe



Sentinel test  
omgeving



## Leeromgeving

- › Fouten maken mag
- › Je hebt de tijd
- › Het leren van triage uitvoeren



# Mass-YAML-to-JSON



Haalt de up-to-date Microsoft Analytic rules van Github



Convert van YAML naar JSON in bulk



Klaar voor import in Sentinel via Github of Azure Devops





Product

Solutions

Open Source

Enterprise

Pricing

Search or jump to...

awt-tom / mass-yaml-to-json

Public

Notifications

Fork 0

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

main

1 Branch

0 Tags

Go to file

Code

awt-tom

Change on readme

fe18ec · 3 days ago

4 Commits

LICENSE

Initial commit

3 days ago

Mass-YAML-to-JSON.ps1

Add files via upload

3 days ago

README.md

Change on readme

3 days ago

README

MIT license

Convert-YamlToJson.ps1 Script Documentation

Why this script

Throughout the years I have learned alot from the Security community and love to give something back to the community!

When using Microsoft Sentinel you want your detections to be crisp. This can be done by creating your own analytic rules or use other methodes. But when you want to start out and have no clue, it can be quite a hussle to get started with enabling all the rules, keep them up to date.

I can see that many organizations leveled up and done this all through pipelines where others are finding their way on how to start. With this script I hope I can encourage many more people to start automate their Sentinel Analytic rule management and being able to import many more detection rules in order to find incidents within their environments.

About

This PowerShell script automates the process of downloading YAML analytic rule files from the Azure Sentinel GitHub repository, converting them to JSON format, and saving them locally in their original folder structure.

Readme

MIT license

Activity

0 stars

1 watching

0 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

PowerShell 100.0%

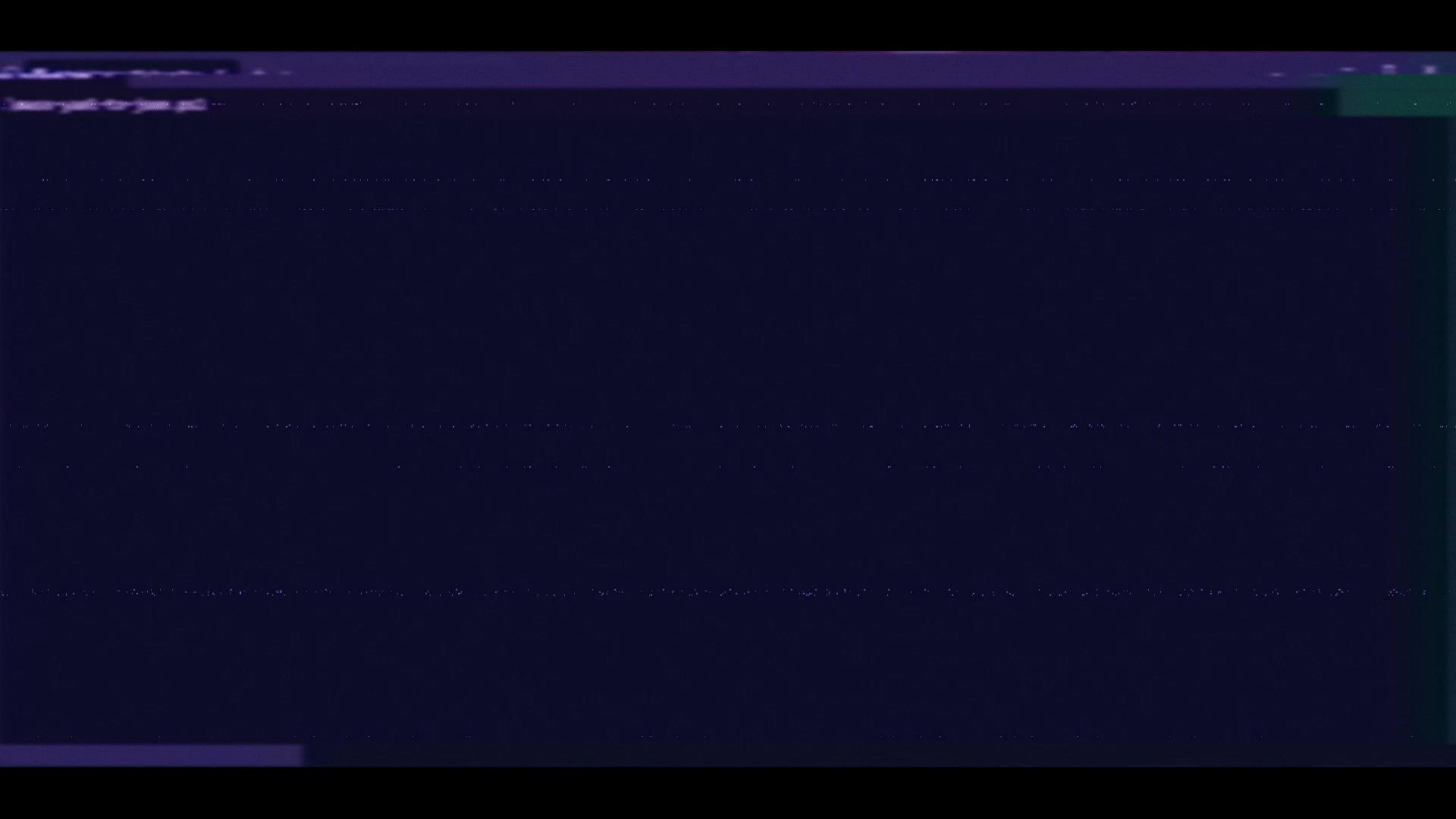
BOS - DAL

In 3 hours

Search

Search

# ◀ DEMO Video ▶



# Tijd voor vragen

**Dooooooooor naar de pubquiz!**