SOAR

Tim Groothuis
Raoul van der Voort

AGENDA

SOAR: organisatie/SOC perspectief

-> SOAR waarom

-> Waar brengt SOAR ons naartoe?

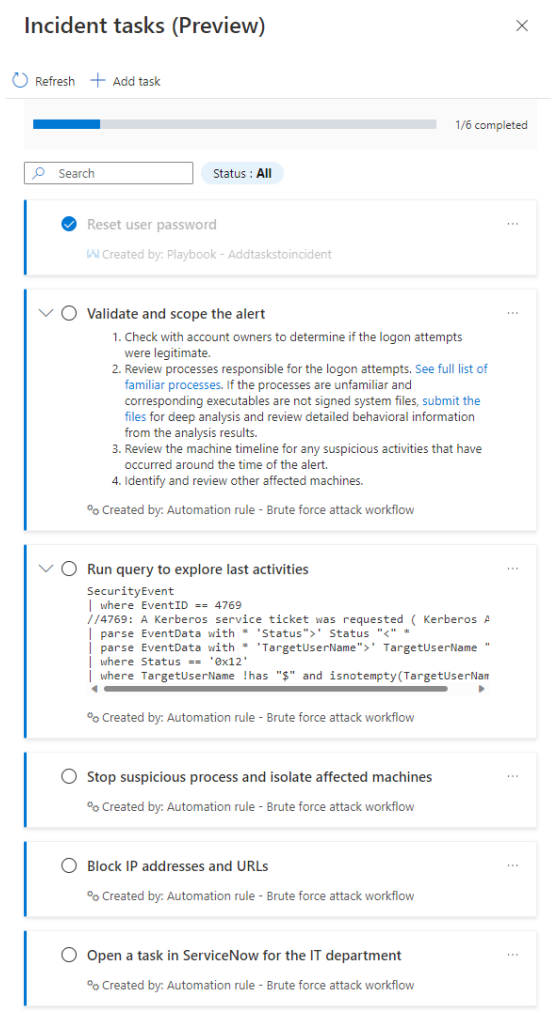
-> Hoe beginnen?

SOAR: Engineer perspectief

-> Wat hebben we nodig om te starten?

-> Playbook development do’s/dont’s

-> Playbook deepdive



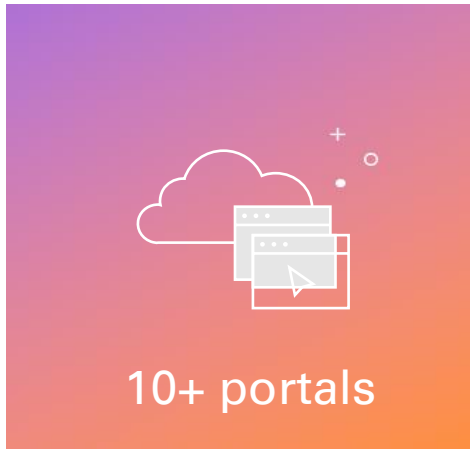
Wie zijn wij?

Raoul van der Voort

Tim Groothuis

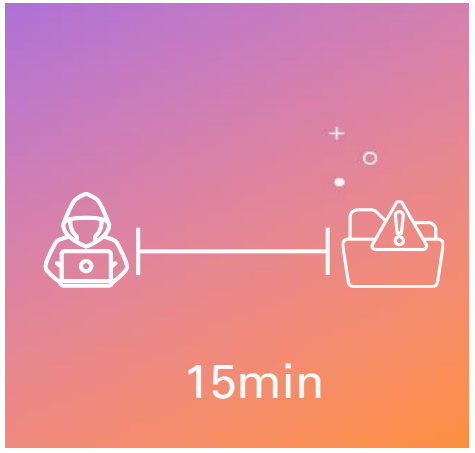
Waarom SOAR? SOC perspectief

Alerts/Incidenten



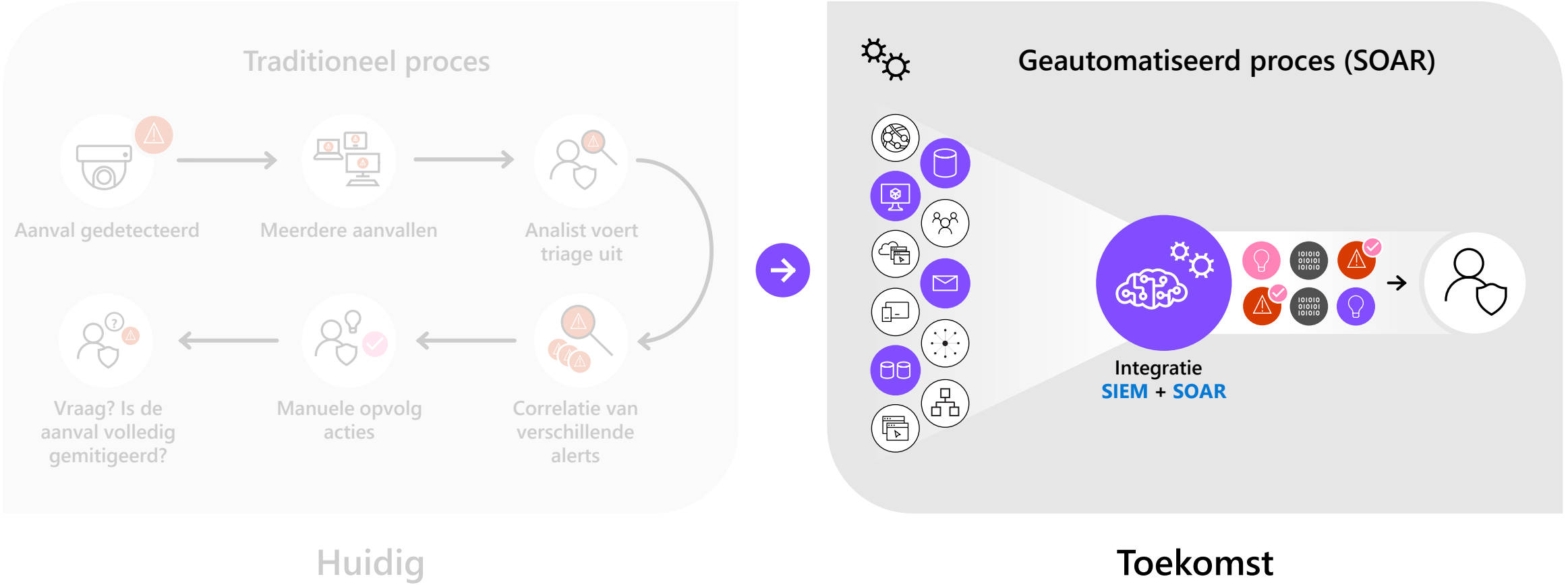
Security portals

“het complete Plaatje”

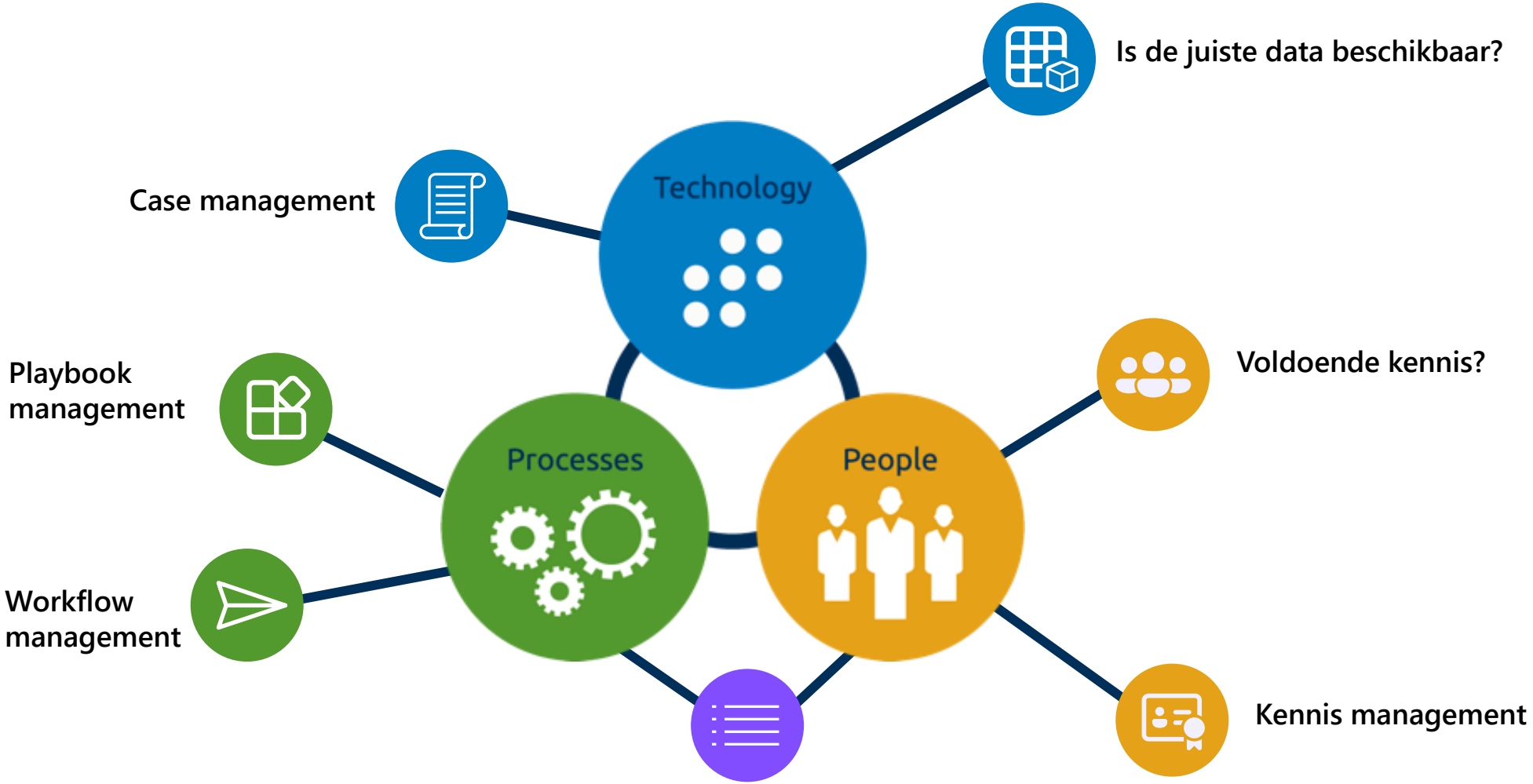


Entry > Breach

Waar brengt SOAR ons naartoe?



Maar….niet alles is technologie!



Hoe beginnen? Welke voorwaarden moeten vooraf duidelijk zijn?

1

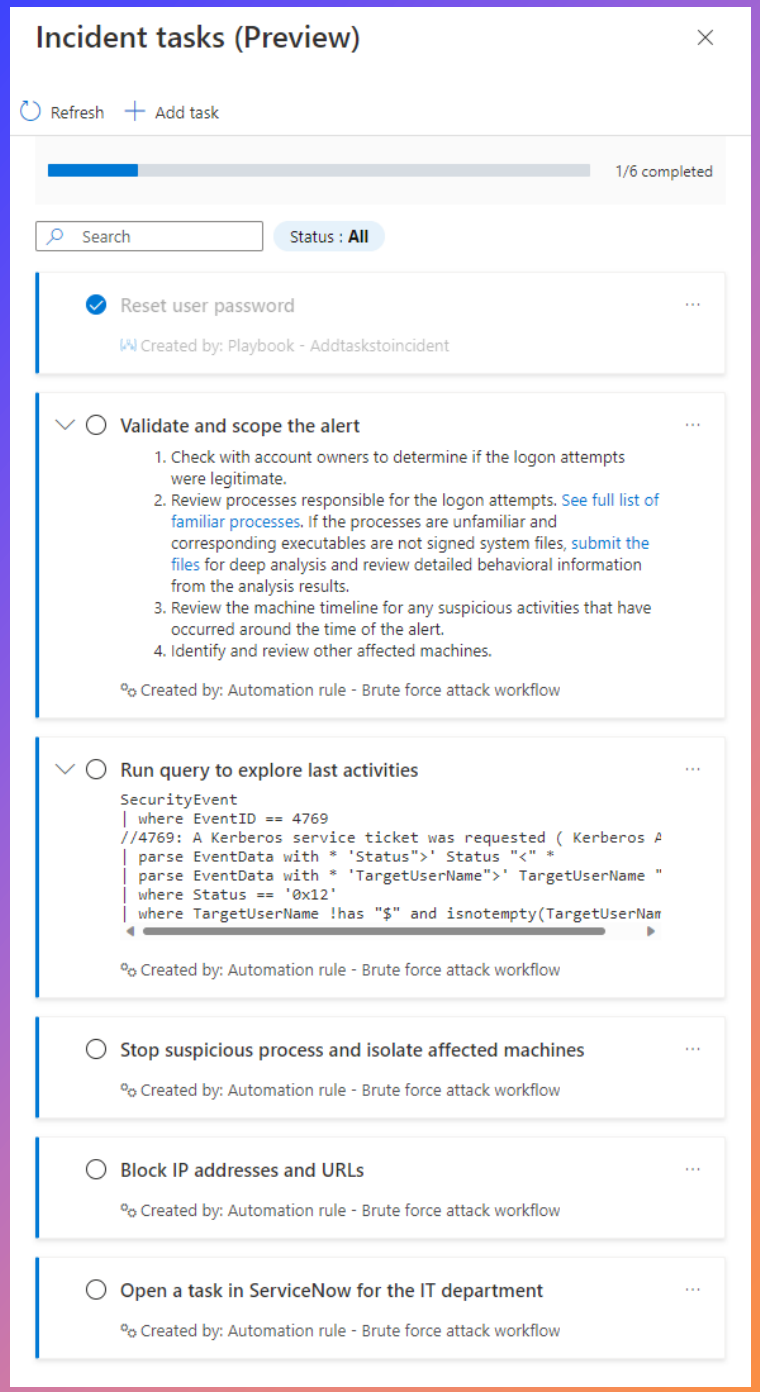
Incident response “context”

- Zijn bestaande detectie regels beschreven?
- Is het proces van uitlopen incidenten (incident response) duidelijk beschreven (inclusief opvolg acties)?
- Welke alerts/incidenten hebben een hoog risico als het gaat om “response” tijd?
- Welke Alert/Incidenten zorgen voor de langste doorlooptijd?

2

Incident response “doel”

- **Alert enrichment:** incident informatie verrijken/aanreiken
- **Alert mitigatie:** welke opvolg acties zijn er nodig? (sentinel tasks)
- **Automated alert enrichment:** geautomatiseerd een alert “verrijken” met context informatie
- **Automated reponse:** volledig geautomatiseerd incident response proces



Wat brengt de toekomst [½]?

- Zelfde aantal mensen, meer alerts afhandelen
- Minder “specifieke” kennis, meer geavanceerde response acties
- Engineer en Analist dichter bij elkaar

ZIJN JULLIE ENTHOUSIAST? ☺

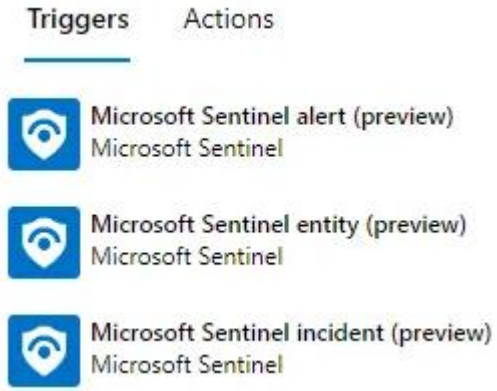
Hoe begin je?

Wat hebben we nodig om te starten?

- Automation Rule
  - Koppelt Sentinel aan de Logic App
- Playbook
  - Een Logic App met de daadwerkelijke logica

Waar beginnen we?

1. Definieër je process
   - Optimaliseren → automatiseren
2. Kies je architectuur
   - Generic of single-use-case
3. Verzamel de benodigde rechten
   - Azure RBAC, Entra ID, API permissions
4. Bouw je Playbook
5. Monitor je Playbook



Playbook Architectuur

Playbook identiteiten

Azure = Zero trust

Playbook identiteiten (pro’s)

User Account

- ✓ Makkelijkste om te gebruiken
- ✓ Rechten staan vrijwel altijd direct goed

App Registration

- ✓ Makkelijk cross tenant
- ✓ Makkelijk interactief te gebruiken tijdens ontwikkeling

Managed identity

- ✓ Geen credential management
- ✓ Finetune toegang per Playbook

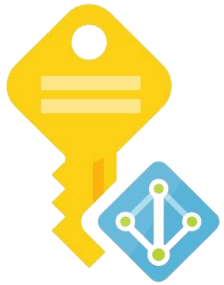
Playbook identiteiten (con’s)

User Account

- Lastig als iemand weggaat
- Veranderingen in assignments breken playbooks

App Registration

- Credential managent



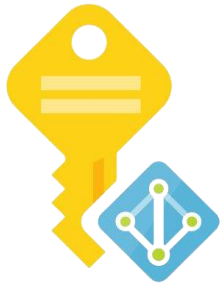
Managed identity

- Niet altijd ondersteunt
- Wildgroei aan assignments

Playbook identiteiten

User Account

App Registration



Managed identity

Rechten & Permissies

Entra ID

Azure RBAC

Entra Roles

Microsoft Graph, Defender, etc.

API Permissies

Rechten & Permissies

Microsoft Graph (6)		
Application.ReadWrite.OwnedBy	Application	Manage apps that this app creates or owns
Device.Read.All	Application	Read all devices
SecurityAlert.Read.All	Application	Read all security alerts
SecurityEvents.Read.All	Application	Read your organization's security events
SecurityIncident.Read.All	Application	Read all security incidents
User.Read.All	Application	Read all users' full profiles
WindowsDefenderATP (5)		
AdvancedQuery.Read.All	Application	Run advanced queries
Alert.Read.All	Application	Read all alerts
Machine.Read.All	Application	Read all machine profiles
Score.Read.All	Application	Read Threat and Vulnerability Management
Vulnerability.Read.All	Application	Read Threat and Vulnerability Management

Microsoft Graph

API Permissies

Rechten & Permissies

Entra ID

Azure RBAC

Entra Roles

Microsoft Graph

API Permissies

Requires Admin Rights

Rechten & Permissies

- API Permissies via PowerShell

```powershell
### Declaring variables related to the Microsoft Graph API
$GraphAppId = "00000003-0000-0000-c000-000000000000" # Can be found inside Enterprise applications when disabling filters"
$GraphServicePrincipal = Get-MgServicePrincipal -filter "appId eq '$GraphAppId'"

### The Approle names that our Application Registration needs on the Graph API
$PermissionName1 = "User.Read.All"
$PermissionName2 = "Device.Read.All"
$PermissionName3 = "SecurityAlert.Read.All"
$PermissionName4 = "SecurityIncident.Read.All"
$PermissionName5 = "SecurityEvents.Read.All"
$PermissionName6 = "Application.ReadWrite.OwnedBy"

# Granting Admin Consent on each role
$AppRole1 = $GraphServicePrincipal.Approles | Where-Object {$_.Value -eq $PermissionName1}
$params = @{
    PrincipalId = $ApplicationServicePrincipal.Id
    ResourceId = $GraphServicePrincipal.Id
    AppRoleId = $AppRole1.Id
}
New-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $ApplicationServicePrincipal.Id -BodyParameter $params
```

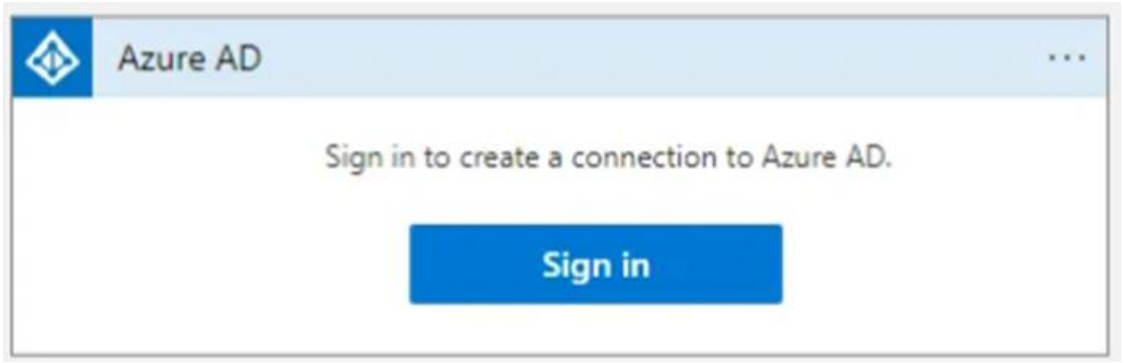
Playbook Development

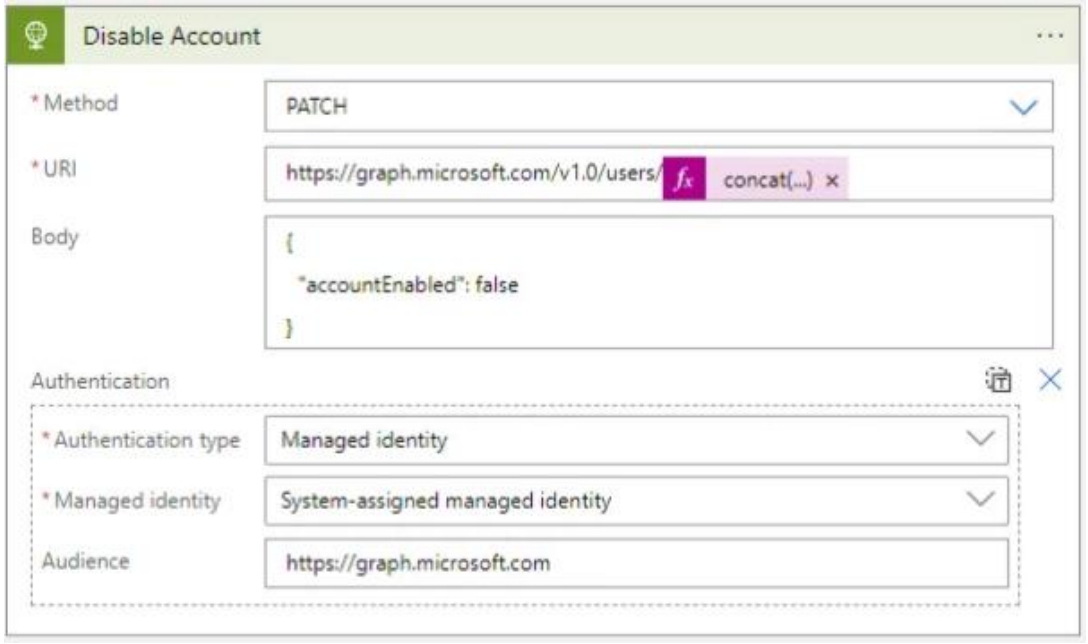
Welke connector?

Managed Connectors

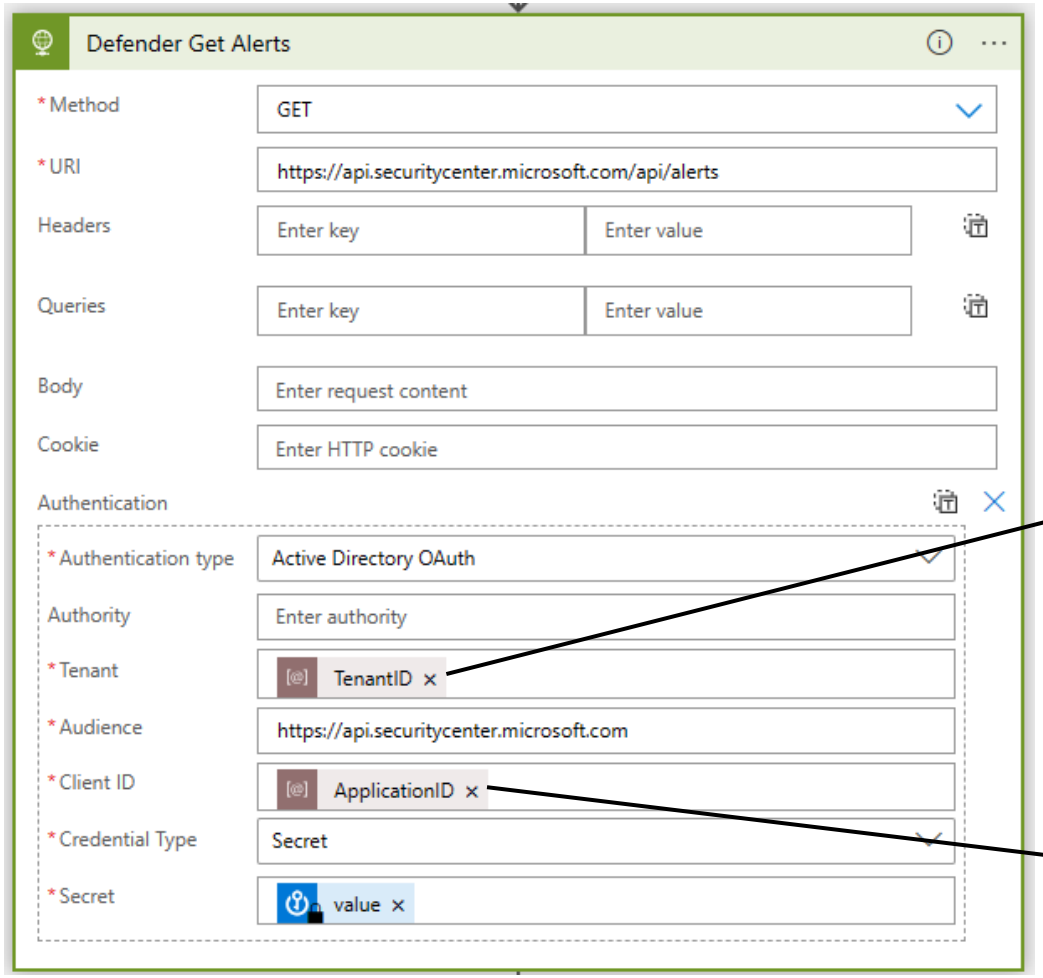
HTTP Calls

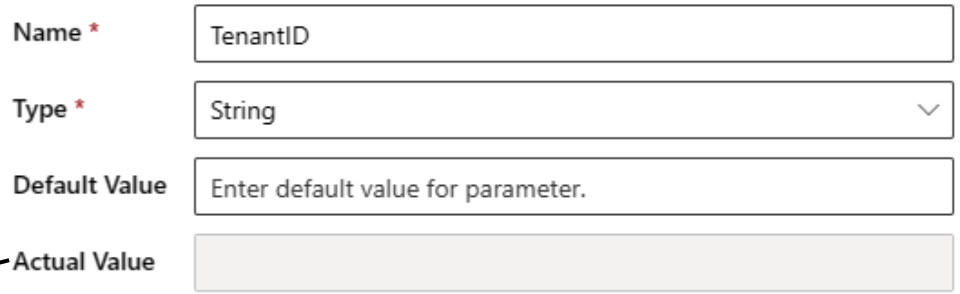
Welke connector?

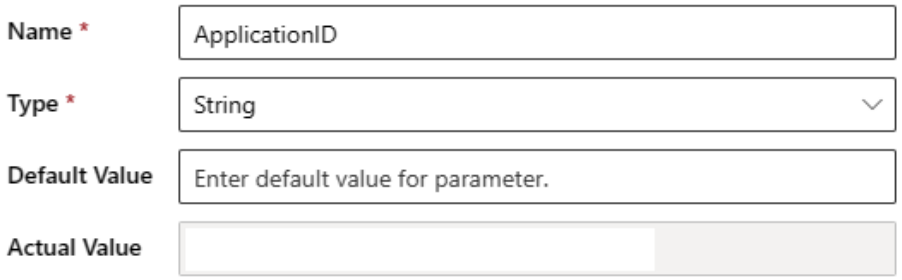




Waarom parameters?







Van ARM naar Parameter?

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "SecretName": {
            "type": "String"
        }
    },
```

Als Parameter in de ARM template

```
"parameters": {
    "SecretName": {
        "Value": "[parameters('SecretName')]"
    }
```

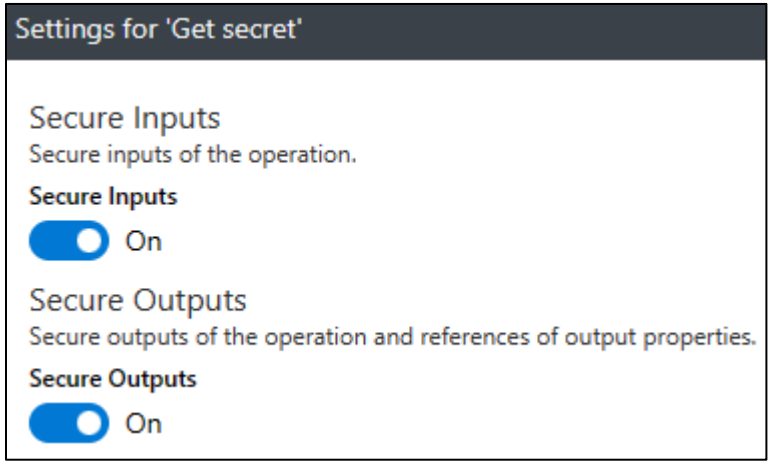
Als ARM expressie in de “Parameters” sectie van de Logic App

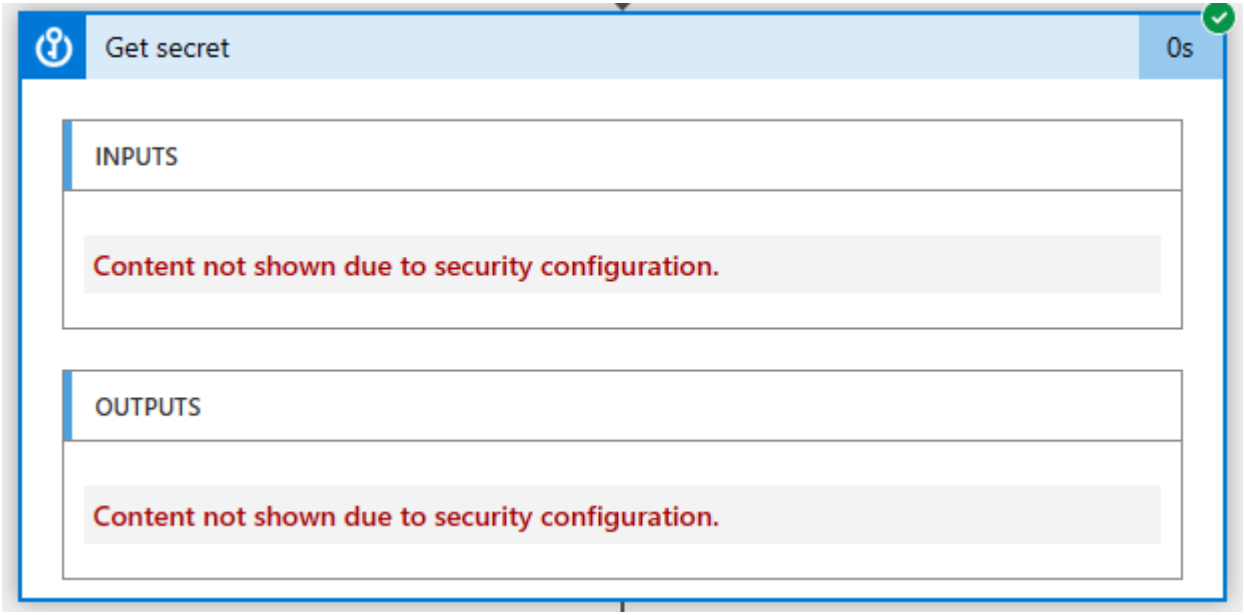
```
"definition": {
    "$schema": "https://schema.management.azure.com/providers/Microsoft.Logic/schemas/2016-06-01/workflowdefinition.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "SecretName": {
            "type": "String"
        }
```

Laad de Parameter van de Logic App in de Logic App Definition

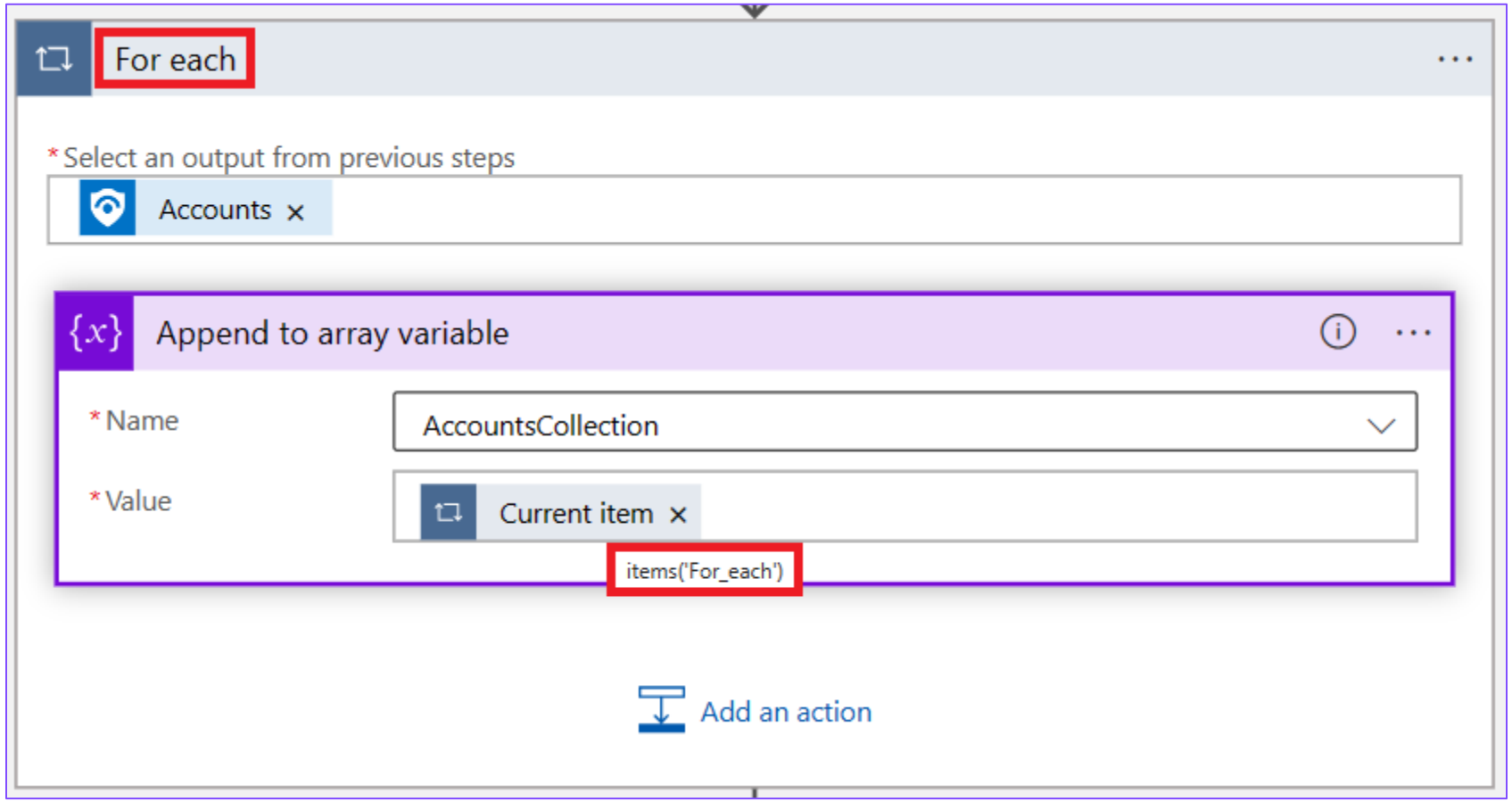
Hoe bescherm je gevoelige info?

Hoe bescherm je gevoelige info?

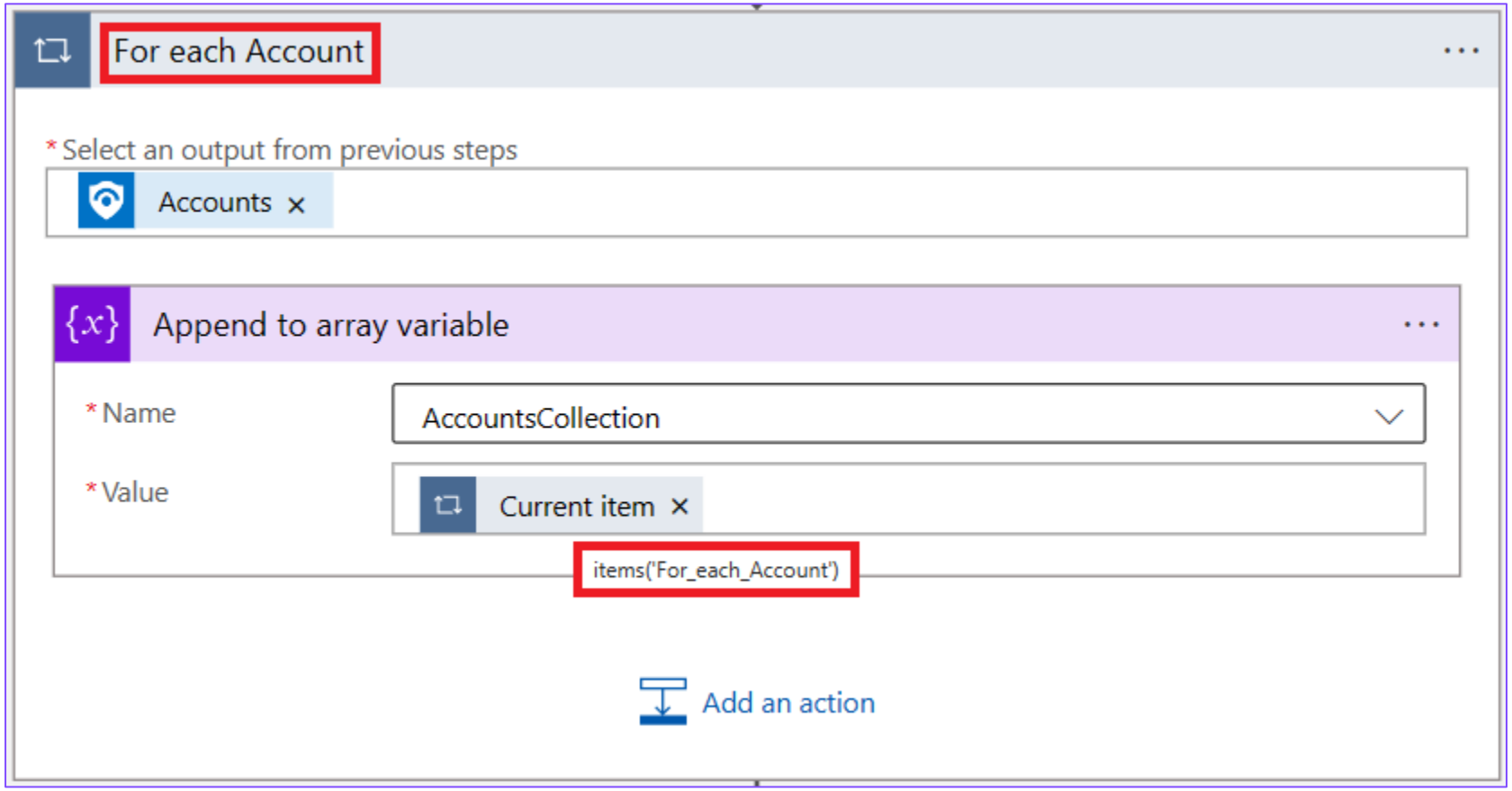




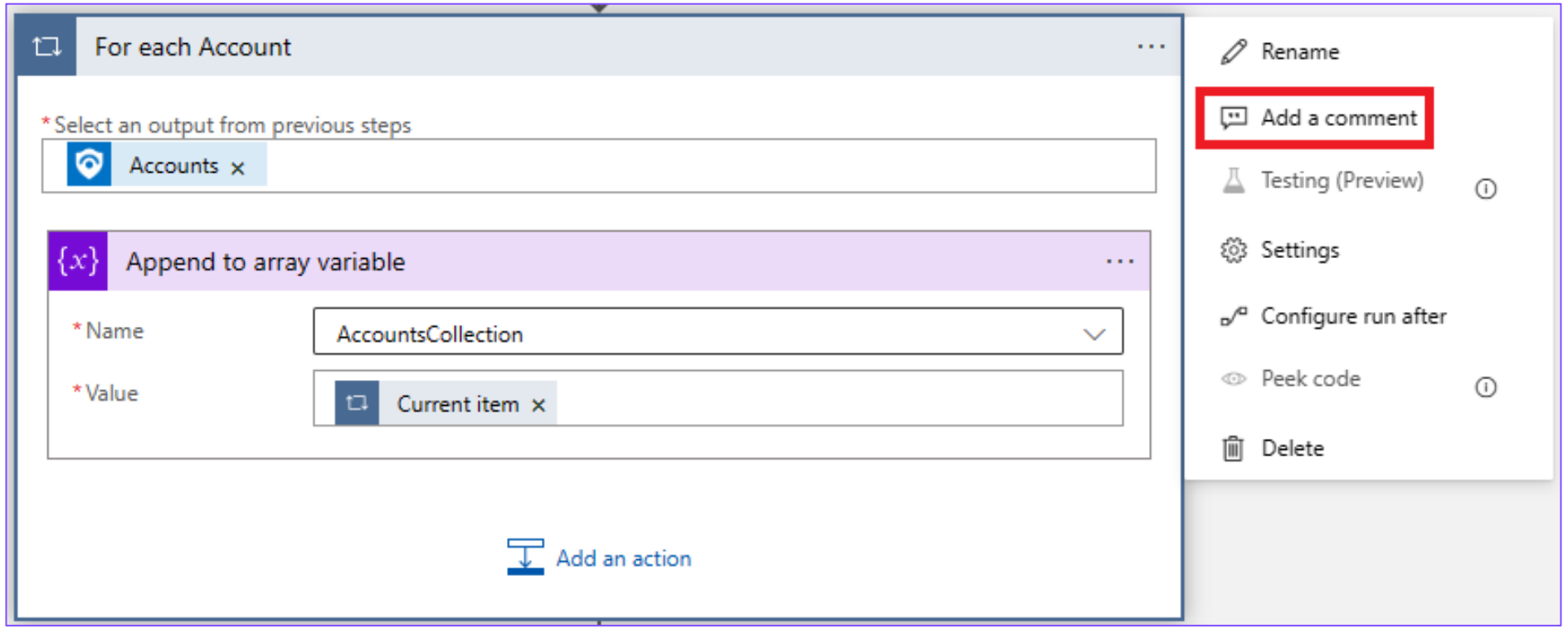
Hoe kan je code leesbaar houden?



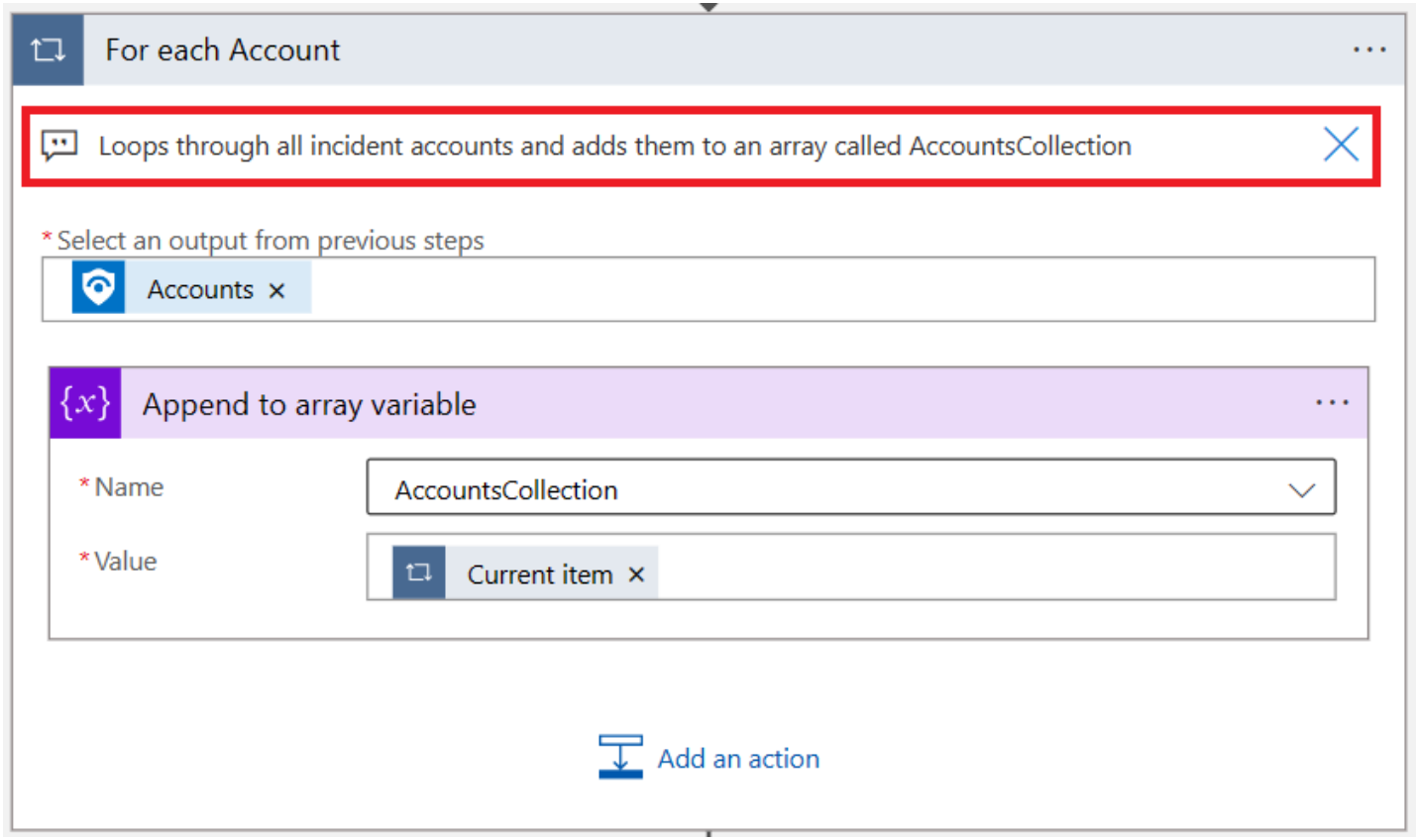
Hoe kan je code leesbaar houden?



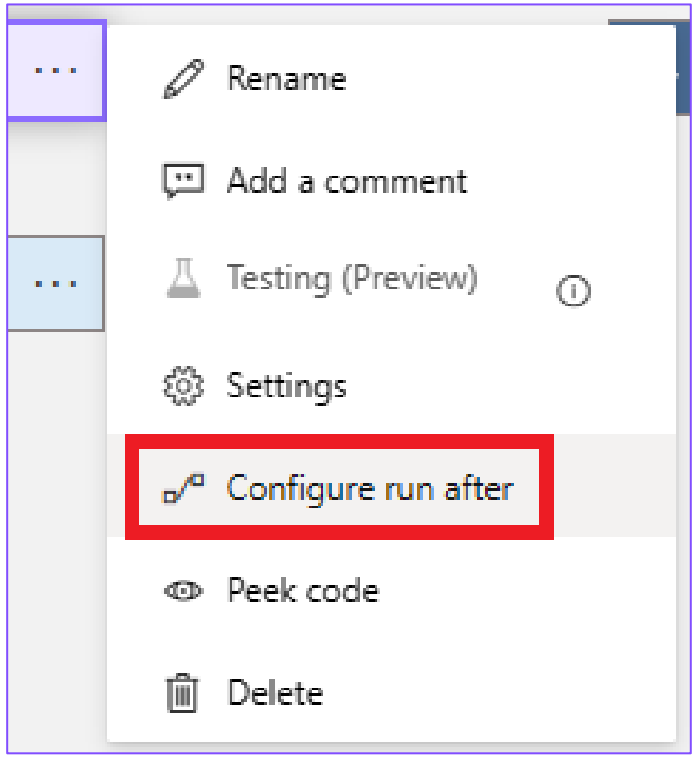
Hoe kan je code leesbaar houden?



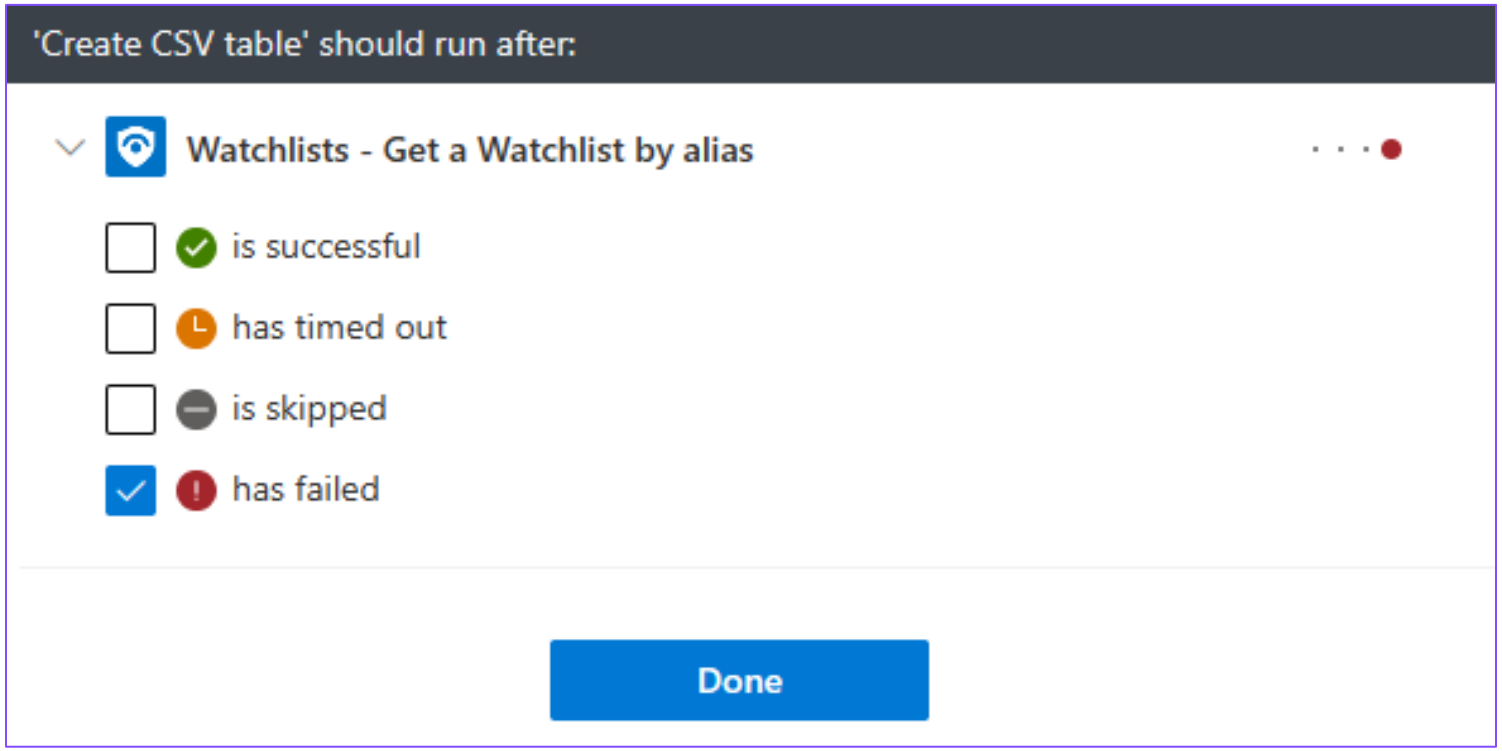
Hoe kan je code leesbaar houden?



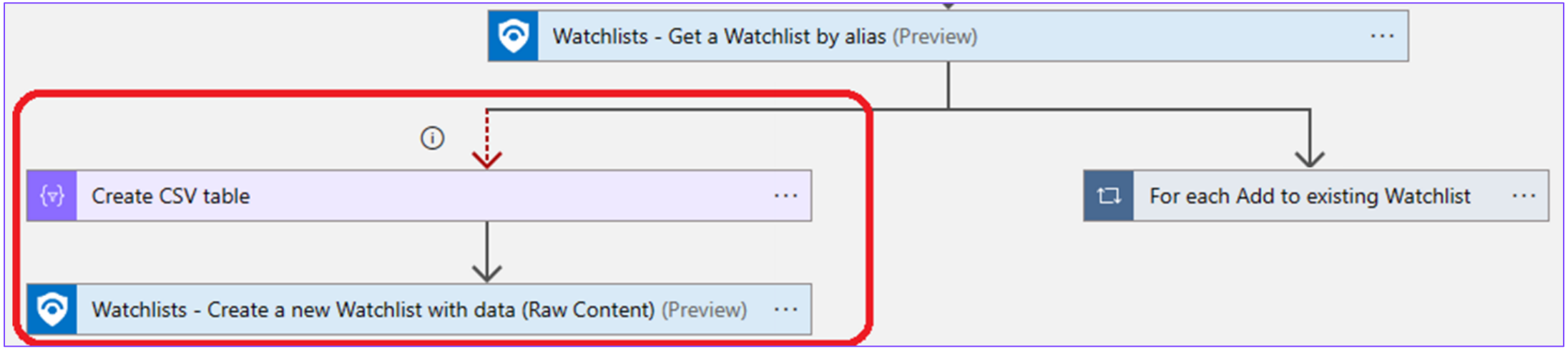
Hoe voorkom ik errors?



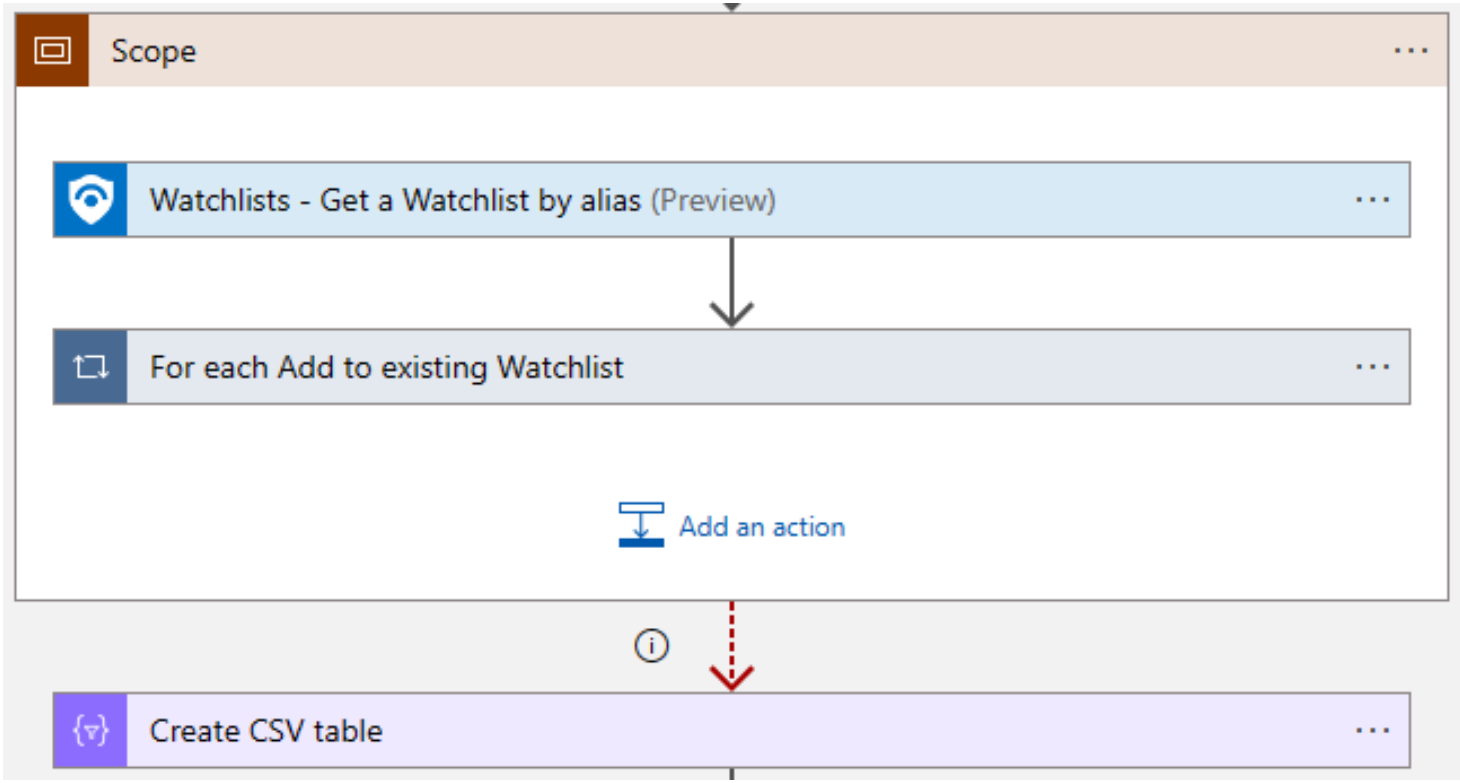
Hoe voorkom ik errors?



Hoe voorkom ik errors?



Hoe voorkom ik errors?

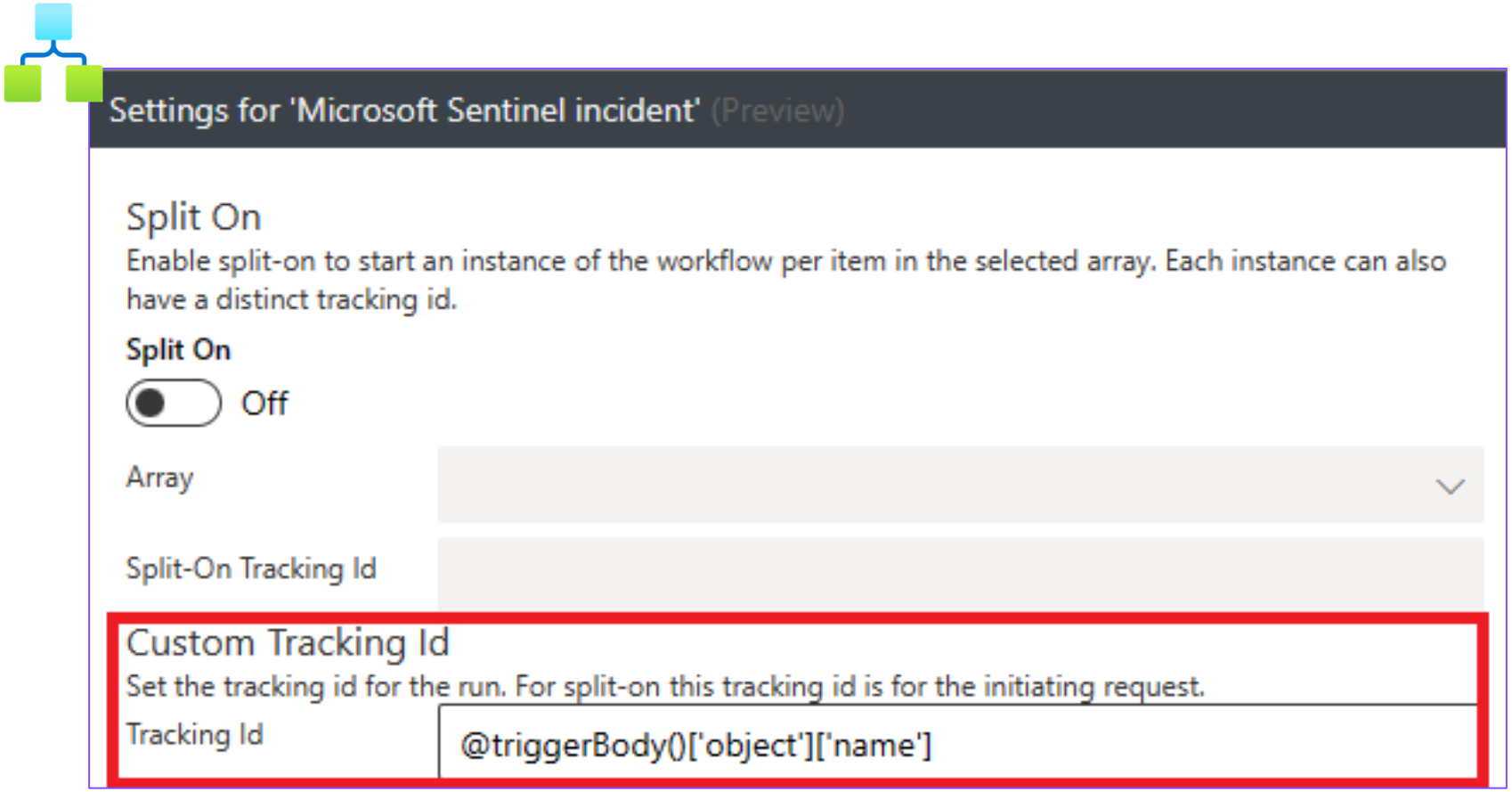


Hoe controleer ik mijn SOAR?

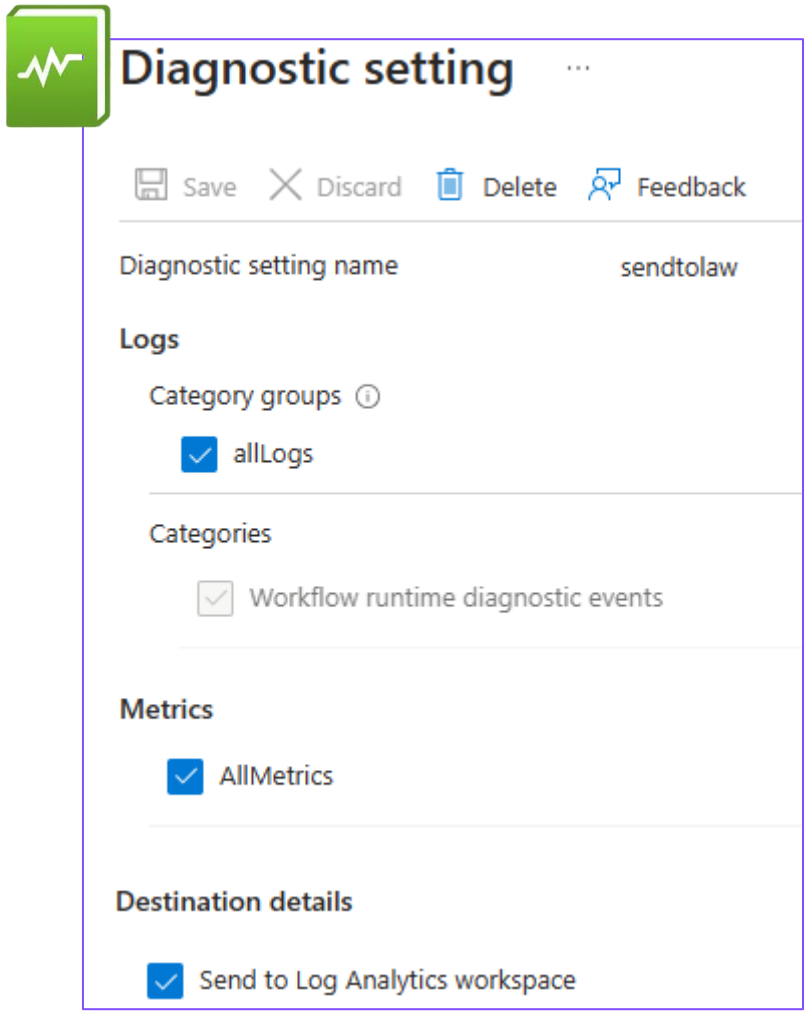
Hoe controleer ik mijn SOAR?


```
"body": {
    "eventUniqueId": "26695135-a746-4f64-992e-6550a9f373ab",
    "objectSchemaType": "Incident",
    "objectEventType": "Update",
    "workspaceInfo": {
        "SubscriptionId":                                    ,
        "ResourceGroupName": "rsg-soar-test",
        "WorkspaceName": "test-law"
    },
    "workspaceId": "                                         ",
    "object": {
        "id": "
        "name": "2ed5c665-7af0-41c4-a20f-b45c9bb890da"
        "etag": "\"8500bb0f-0000-0d00-0000-65494cf10000\"",
        "type": "Microsoft.SecurityInsights/Incidents",
        "properties": {
            "title": "Tim-Testing-Bruteforce",
            "description": "A testing rule running on testing data to create a fake brute force incident with a entity mapped",
            "severity": "Low",
            "status": "New",
            "owner": {
                "objectId": null,
                "email": null,
                "assignedTo": null,
                "userPrincipalName": null
            },
```

Hoe controleer ik mijn SOAR?



Hoe controleer ik mijn SOAR?



Hoe controleer ik mijn SOAR?

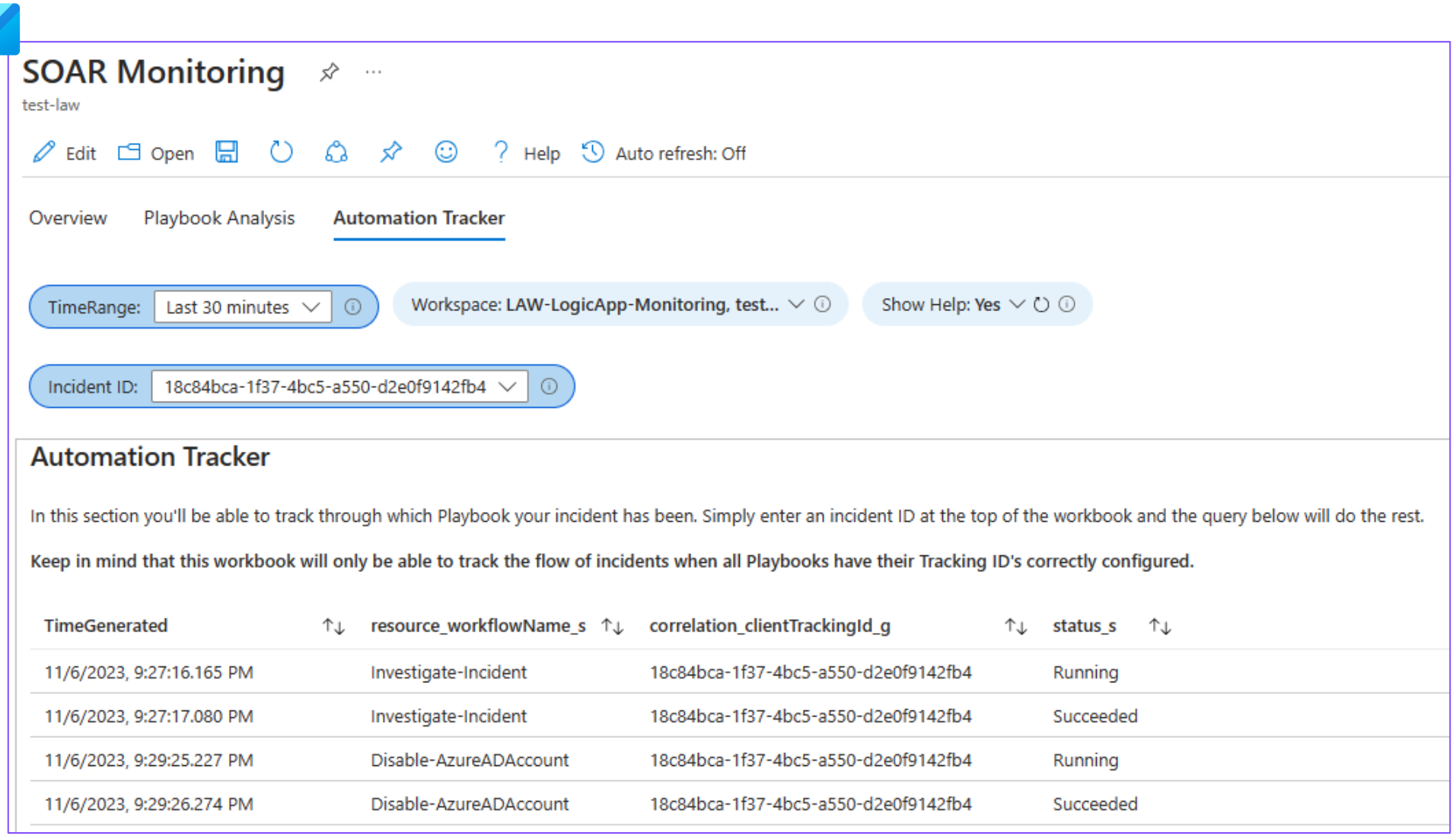
```
1  AzureDiagnostics
2  | where ResourceProvider == "MICROSOFT.LOGIC"
3  | where ResourceType == "WORKFLOWS/RUNS"
4  | where correlation_clientTrackingId_g == "2ed5c665-7af0-41c4-a20f-b45c9bb890da"
5  | project TimeGenerated, resource_workflowName_s, correlation_clientTrackingId_g, status_s
```

...

Results | Chart

TimeGenerated [UTC]	resource_workflowName_s	correlation_clientTrackingId_g	status_s
11/6/2023, 8:32:51.072 PM	Disable-AzureADAccount	2ed5c665-7af0-41c4-a20f-b45c9bb890da	Succeeded
11/6/2023, 8:32:50.293 PM	Disable-AzureADAccount	2ed5c665-7af0-41c4-a20f-b45c9bb890da	Running
11/6/2023, 8:30:41.720 PM	Investigate-Incident	2ed5c665-7af0-41c4-a20f-b45c9bb890da	Succeeded
11/6/2023, 8:30:40.784 PM	Investigate-Incident	2ed5c665-7af0-41c4-a20f-b45c9bb890da	Running

Playbook Monitoring



WRAP-UP

Organisatie/SOC perspectief

Alerts/Incidenten | Securityportals | "het complete Plaatje" | Entry > Breach

+

+

1

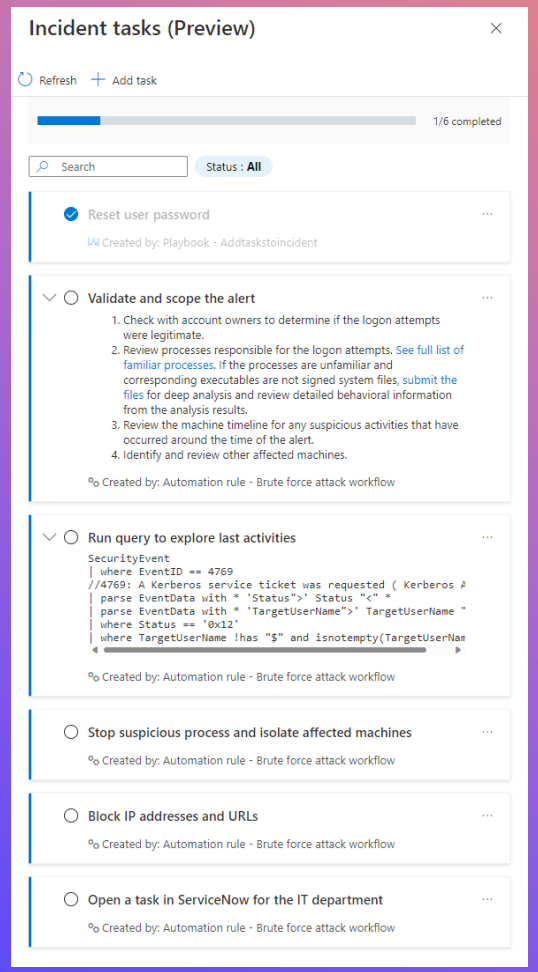
Incident response "context"

- Zijn bestaande detectie regels beschreven?
- Is het proces van uitlopen incidenten (incident response) duidelijk beschreven (inclusief opvolg acties)?
- Welke alerts/incidenten hebben een hoog risico als het gaat om "response" tijd?
- Welke Alert/Incidenten zorgen voor de langste doorlooptijd?

2

Incident response "doel"

- **Alert enrichment**: incident informatie verrijken/aanreiken
- **Alert mitigatie**: welke opvolg acties zijn er nodig? (sentinel tasks)
- **Automated alert enrichment**: geautomatiseerd een alert "verrijken" met context informatie
- **Automated reponse**: volledig geautomatiseerd incident response proces



Engineer perspectief