Opensource ICT Solutions

ZABBIX MEETUP

Monitoring Office 365 defender and other Azure cloud resources

- Microphones are muted
- Ask your questions in Q&A, not in the chat

Whoami

Brian van Baekel

Zabbix trainer / Consultant

Opensource ICT Solutions

Your Zabbix partner in:

- The Netherlands
- United Kingdom
- United States

How it began

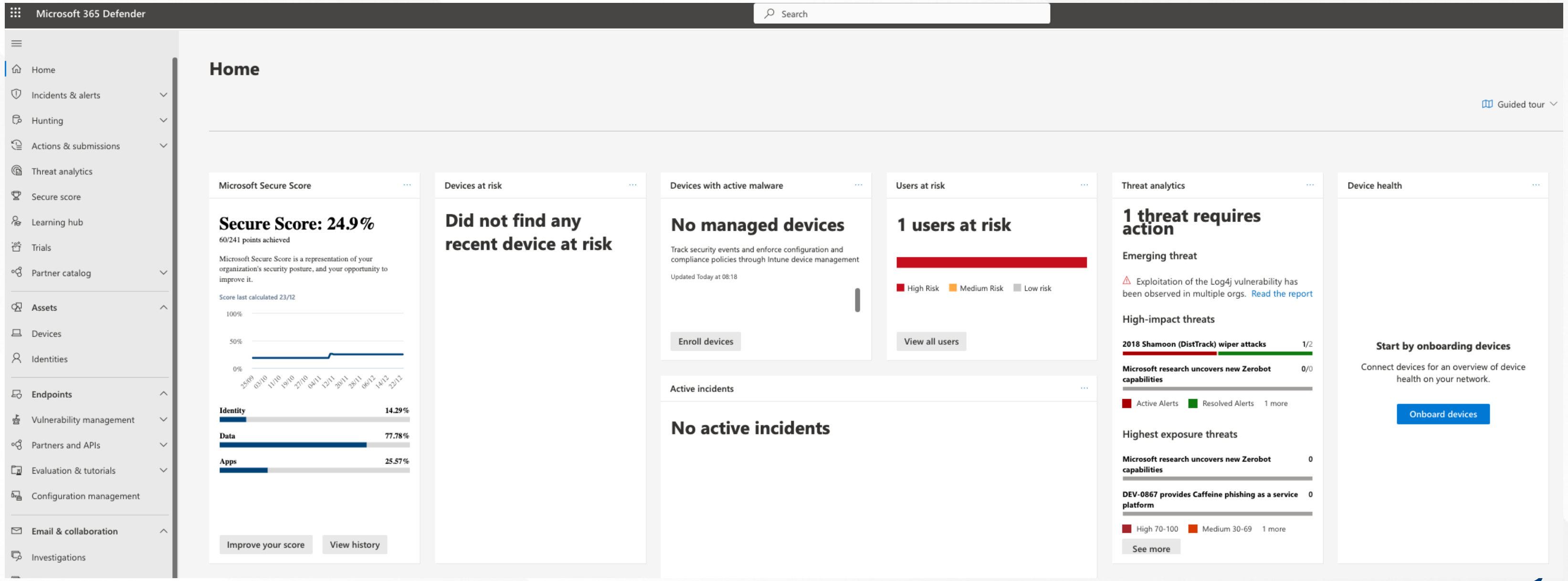
- Customer request
  - Somewhat greenfield
  - Full azure shop
  - Windows shop
- Requirements
  - Quick overview via dashboards
  - Monitoring Azure Defender
  - Monitoring of Cisco Meraki
- Time of implementation: December 2022

Requirements

- Dashboards: No problem at all
- Azure Defender open incidents + risky users: Should be possible, but it’s not out of the box. Challenge!
- Cisco Meraki: Thanks to ZBXNEXT-6844 this was no problem anymore.

What is defender?

“Microsoft 365 Defender is a unified pre- and post-breach enterprise defence suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.”



Home

Microsoft Secure Score

Secure Score: 24.9%

60/241 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 23/12

Identity	14.29%
Data	77.78%
Apps	25.57%

Devices at risk

Did not find any recent device at risk

Devices with active malware

No managed devices

Track security events and enforce configuration and compliance policies through Intune device management

Updated Today at 08:18

Users at risk

1 users at risk

Active incidents

No active incidents

Threat analytics

1 threat requires action

Emerging threat

⚠ Exploitation of the Log4j vulnerability has been observed in multiple orgs. Read the report

High-impact threats

2018 Shamoon (DistTrack) wiper attacks	1/2
Microsoft research uncovers new Zerobot capabilities	0/0

Highest exposure threats

Microsoft research uncovers new Zerobot capabilities	0
DEV-0867 provides Caffeine phishing as a service platform	0

Device health

Start by onboarding devices

Connect devices for an overview of device health on your network.

Talking to Azure via Zabbix

- During research we figured out defender is accessible via an Azure AD application
- After the application is created, a token needs to be generated
- Token will be used to talk to the API.

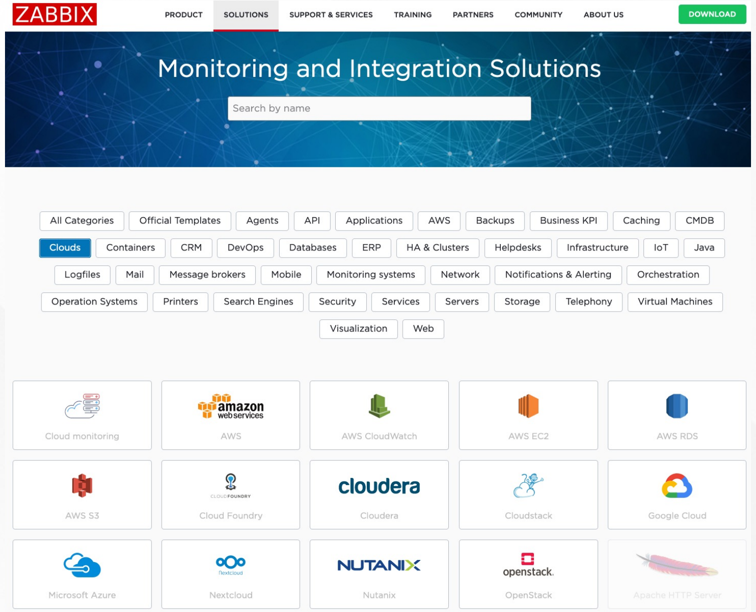
- So far, so good. API queries are doable!

Reusing Zabbix templates

- Zabbix created a template to monitor VMs in Azure.
- This is done via a script item, which means JavaScript

- Script is getting the oauth token, and performing all calls to get those VM statistics.

- Hmmmmm.....!



Workflow

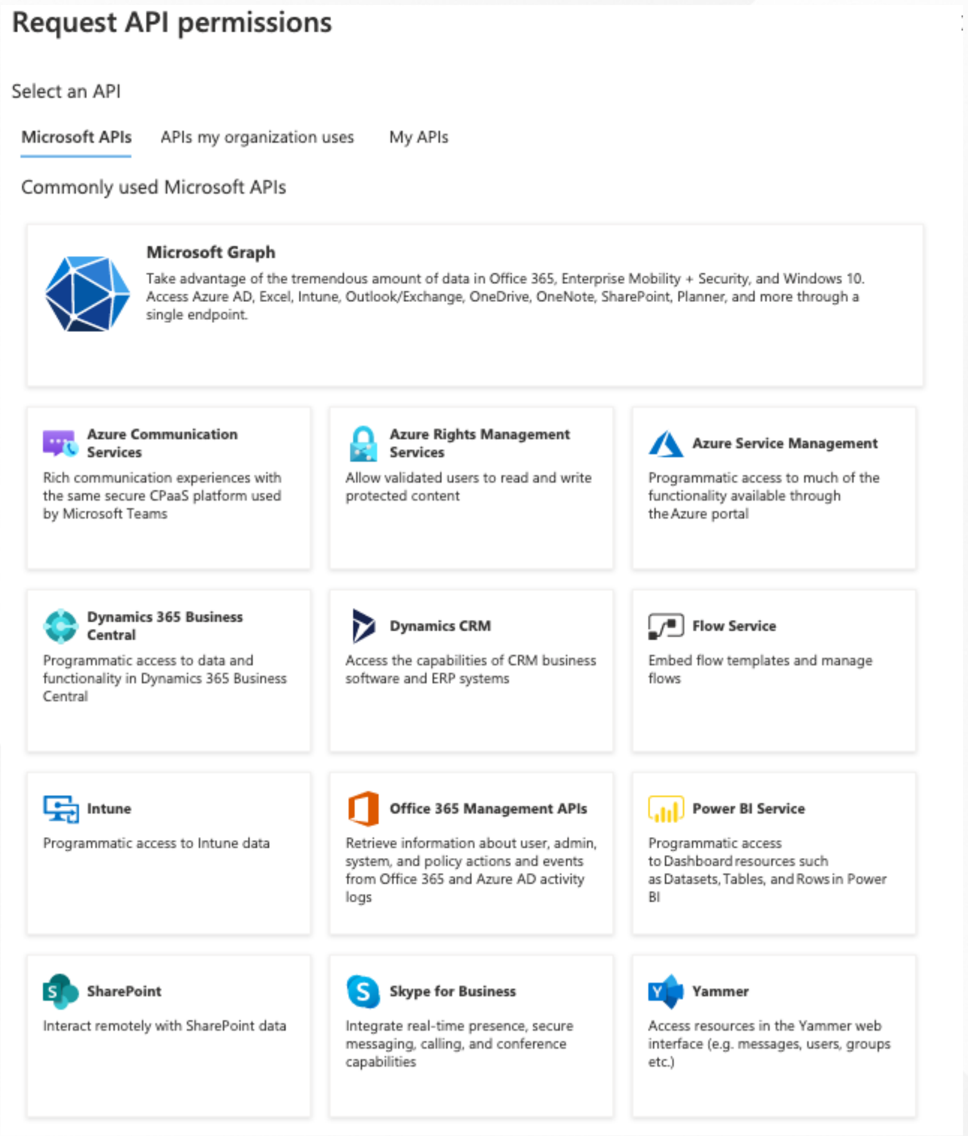
- Prepare Azure environment (application in Azure AD, RBAC rules etc)
- Strip the script
- Change URLs to talk to different API endpoints
- Profit!

1 Prepare Azure – app registration

- Login to Azure
- Go to “App registrations” and create a new registration
- Assign the correct permissions to this app registration
  - Of course, it depends on the goal; which things to monitor etc.
- Create a Client secret (Certificates – Secrets) -> Client Secrets

- Note down the following info:
  - App ID
  - Azure Password
  - Tenant ID

- List of Default Microsoft APIs



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

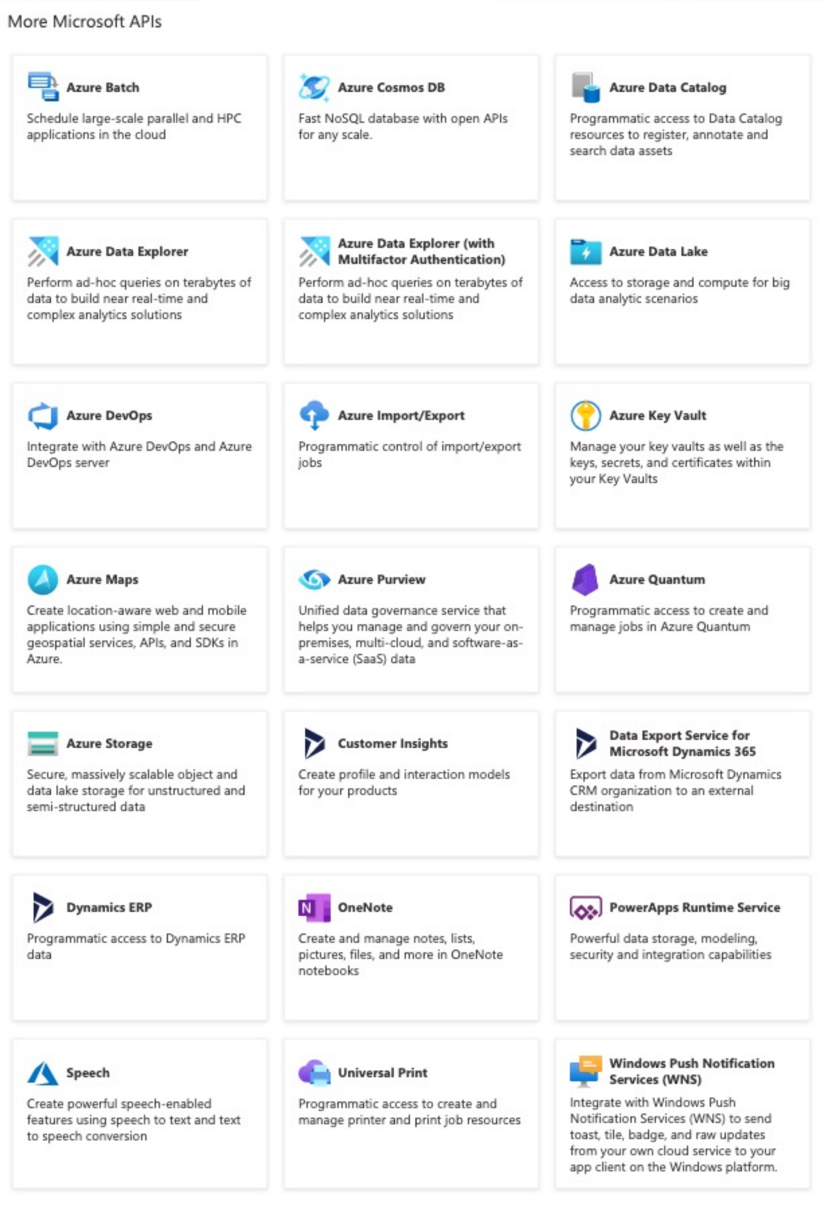
Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

SharePoint
Interact remotely with SharePoint data

Skype for Business
Integrate real-time presence, secure messaging, calling, and conference capabilities

Yammer
Access resources in the Yammer web interface (e.g. messages, users, groups etc.)

- List of Default Microsoft APIs



More Microsoft APIs

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Cosmos DB
Fast NoSQL database with open APIs for any scale.

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Explorer (with Multifactor Authentication)
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Maps
Create location-aware web and mobile applications using simple and secure geospatial services, APIs, and SDKs in Azure.

Azure Purview
Unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data

Azure Quantum
Programmatic access to create and manage jobs in Azure Quantum

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics ERP
Programmatic access to Dynamics ERP data

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

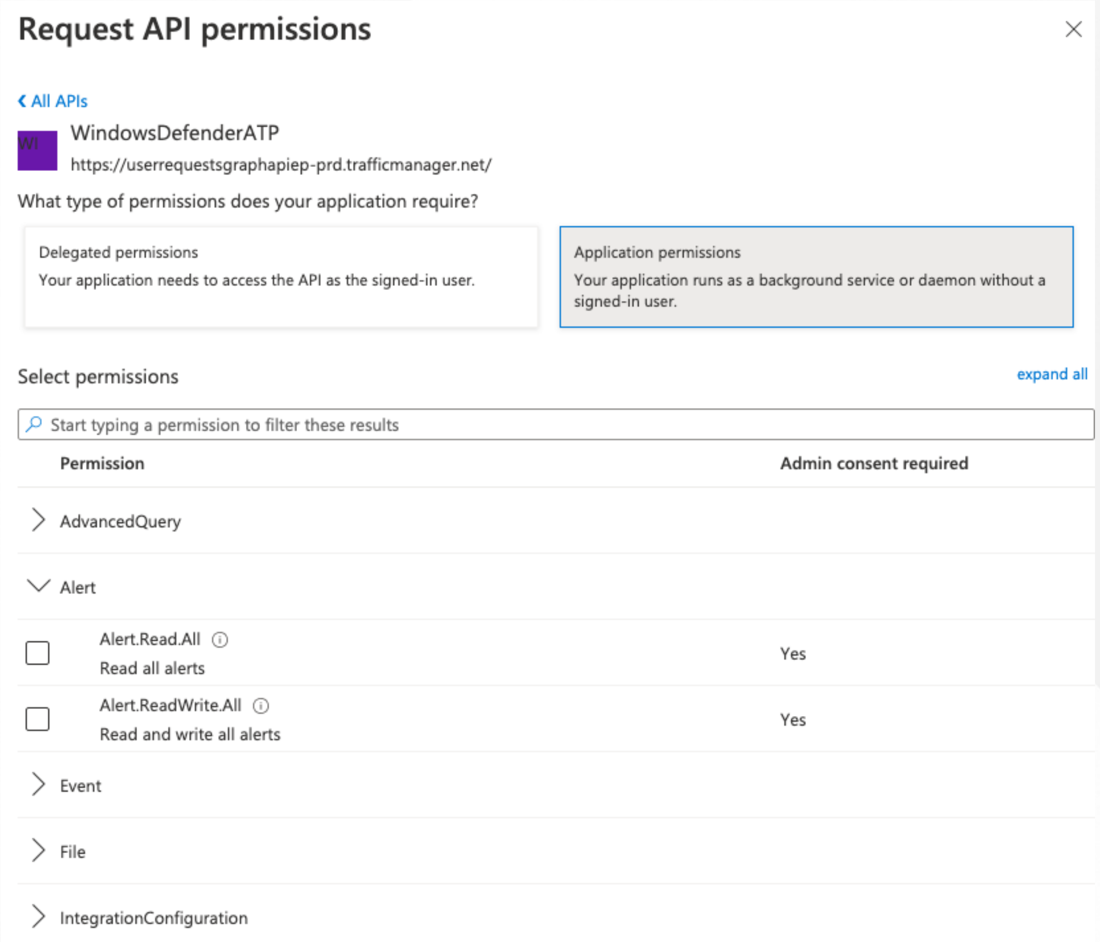
PowerApps Runtime Service
Powerful data storage, modeling, security and integration capabilities

Speech
Create powerful speech-enabled features using speech to text and text to speech conversion

Universal Print
Programmatic access to create and manage printer and print job resources

Windows Push Notification Services (WNS)
Integrate with Windows Push Notification Services (WNS) to send toast, tile, badge, and raw updates from your own cloud service to your app client on the Windows platform.

- In “APIs my organization uses” there is a WindowsDefenderATP method, which is really useful…



Request API permissions

< All APIs

WI WindowsDefenderATP
https://userrequestsgraphapiep-prd.trafficmanager.net/

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

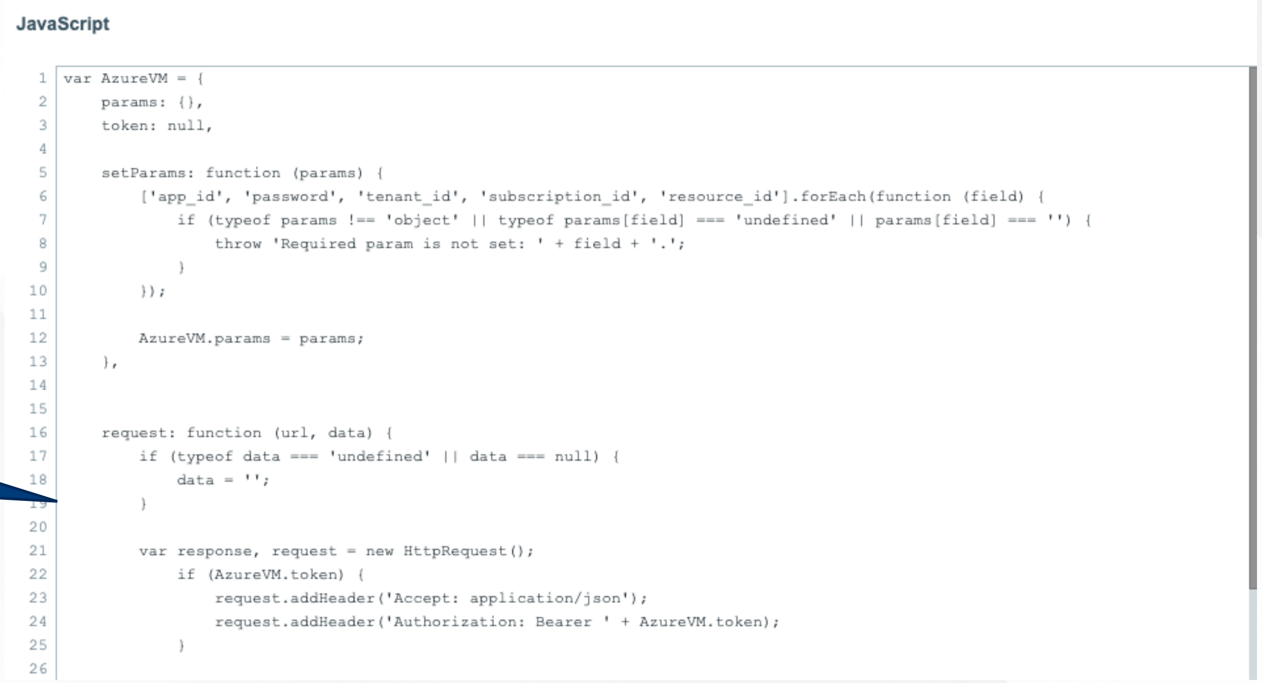
Start typing a permission to filter these results

	Permission	Admin consent required
>	AdvancedQuery	
∨	Alert	
□	Alert.Read.All ⓘ Read all alerts	Yes
□	Alert.ReadWrite.All ⓘ Read and write all alerts	Yes
>	Event	
>	File	
>	IntegrationConfiguration	

2 Edit the Script, or write your own…

- In Zabbix, there is a templates named “Azure virtual machine by HTTP”
- In this template there are 52 items:
  - 1 Script type item
  - 51 Dependent type items
- In the script type item, there is a JavaScript that is logging in to Azure and gathering all information. This information is pushed into the Dependent items, and parsed over there.

- We took this script, and stripped all parts that are not needed for us, as we do not need VM metrics or such
- What was left was basically the authentication part, and structure to make a call to Azure



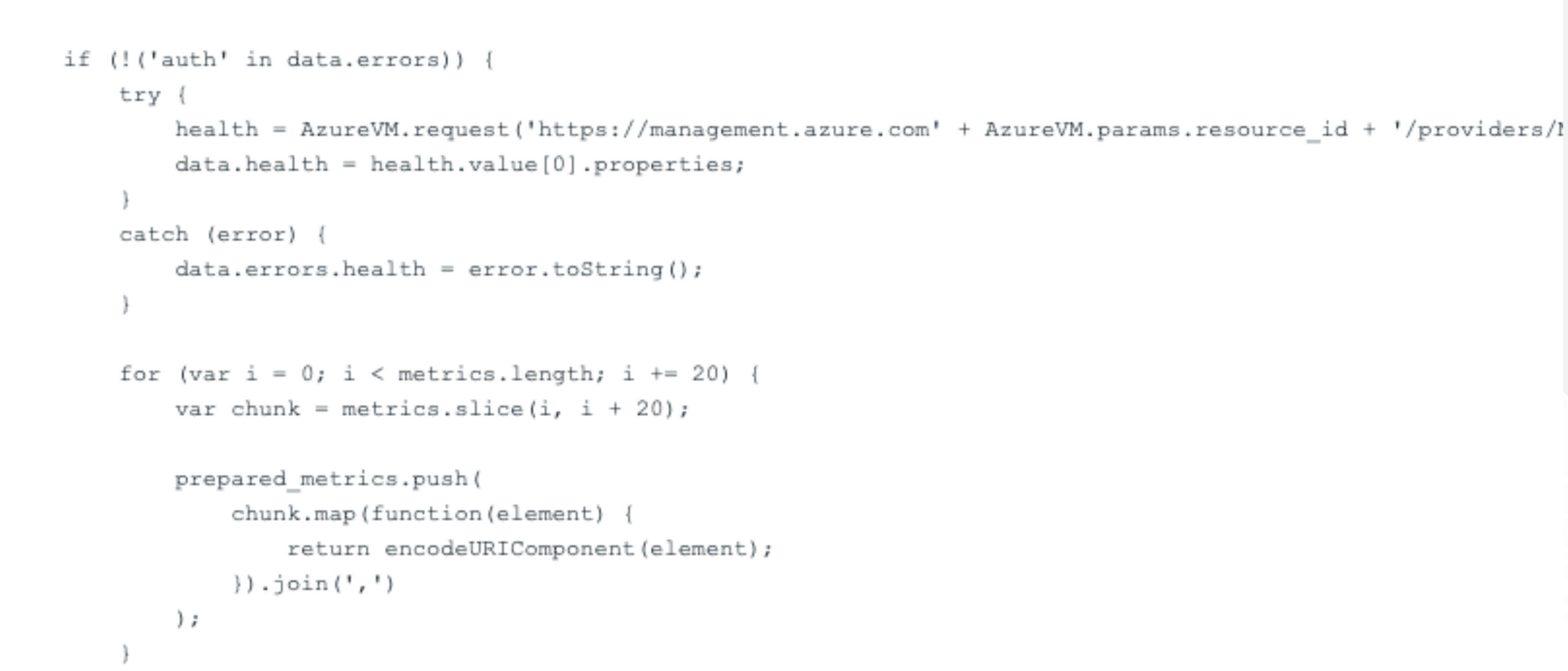
JavaScript

```javascript
var AzureVM = {
    params: {},
    token: null,

    setParams: function (params) {
        ['app_id', 'password', 'tenant_id', 'subscription_id', 'resource_id'].forEach(function (field) {
            if (typeof params !== 'object' || typeof params[field] === 'undefined' || params[field] === '') {
                throw 'Required param is not set: ' + field + '.';
            }
        });

        AzureVM.params = params;
    },


    request: function (url, data) {
        if (typeof data === 'undefined' || data === null) {
            data = '';
        }

        var response, request = new HttpRequest();
            if (AzureVM.token) {
                request.addHeader('Accept: application/json');
                request.addHeader('Authorization: Bearer ' + AzureVM.token);
            }

```

Just an example!

- Once the authentication succeeded, it is time to make the call to the API endpoint in Azure.

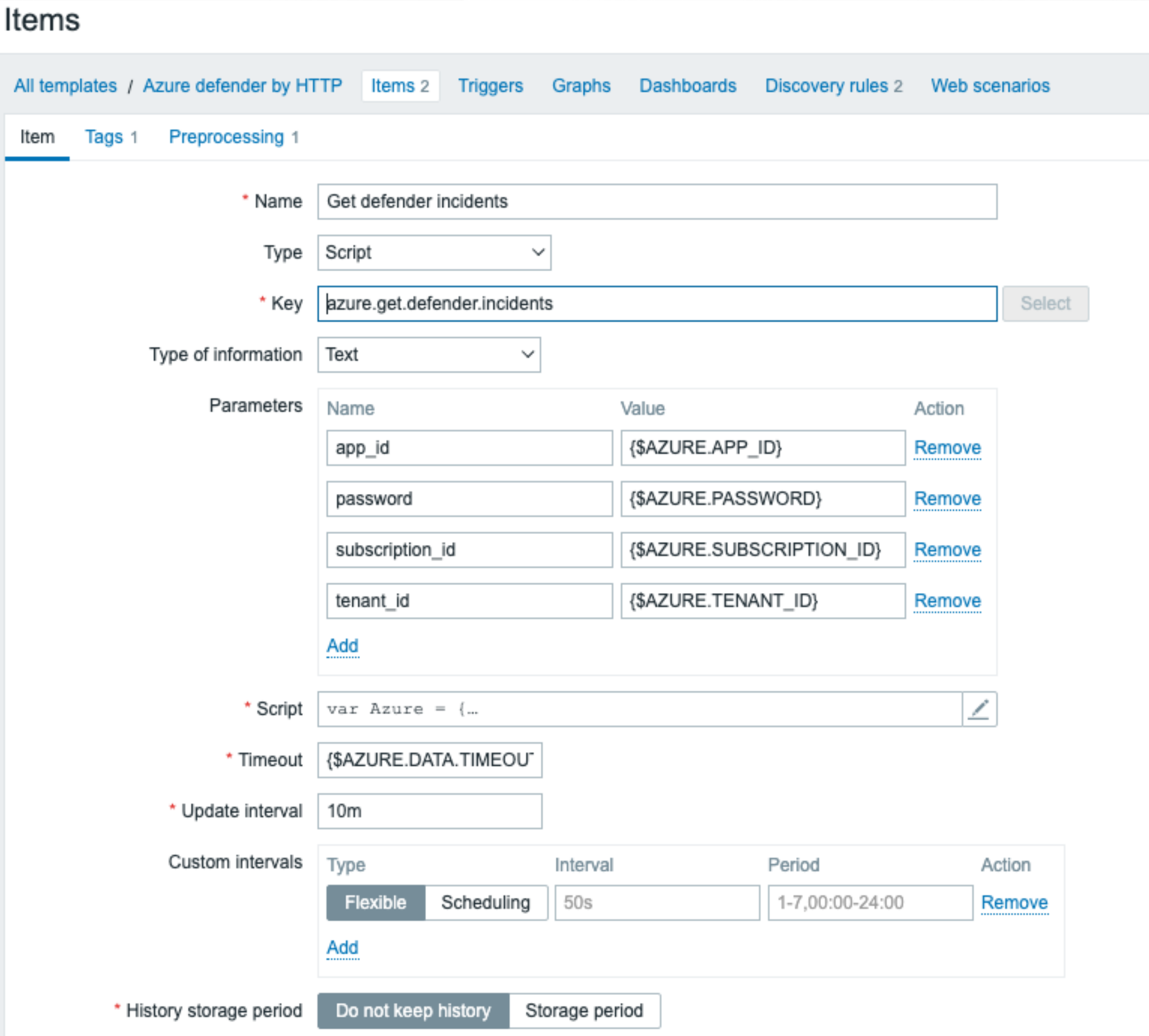
- Original snippet:



```
if (!('auth' in data.errors)) {
    try {
        health = AzureVM.request('https://management.azure.com' + AzureVM.params.resource_id + '/providers/M
        data.health = health.value[0].properties;
    }
    catch (error) {
        data.errors.health = error.toString();
    }

    for (var i = 0; i < metrics.length; i += 20) {
        var chunk = metrics.slice(i, i + 20);

        prepared_metrics.push(
            chunk.map(function(element) {
                return encodeURIComponent(element);
            }).join(',')
        );
    }
```

Testing

- Time to test!



Items

All templates / Azure defender by HTTP | Items 2 | Triggers | Graphs | Dashboards | Discovery rules 2 | Web scenarios

Item | Tags 1 | Preprocessing 1

* Name: Get defender incidents

Type: Script

* Key: azure.get.defender.incidents [Select]

Type of information: Text

Parameters

Name	Value	Action
app_id	{$AZURE.APP_ID}	Remove
password	{$AZURE.PASSWORD}	Remove
subscription_id	{$AZURE.SUBSCRIPTION_ID}	Remove
tenant_id	{$AZURE.TENANT_ID}	Remove

Add

* Script: `var Azure = {…`

* Timeout: {$AZURE.DATA.TIMEOU`

* Update interval: 10m

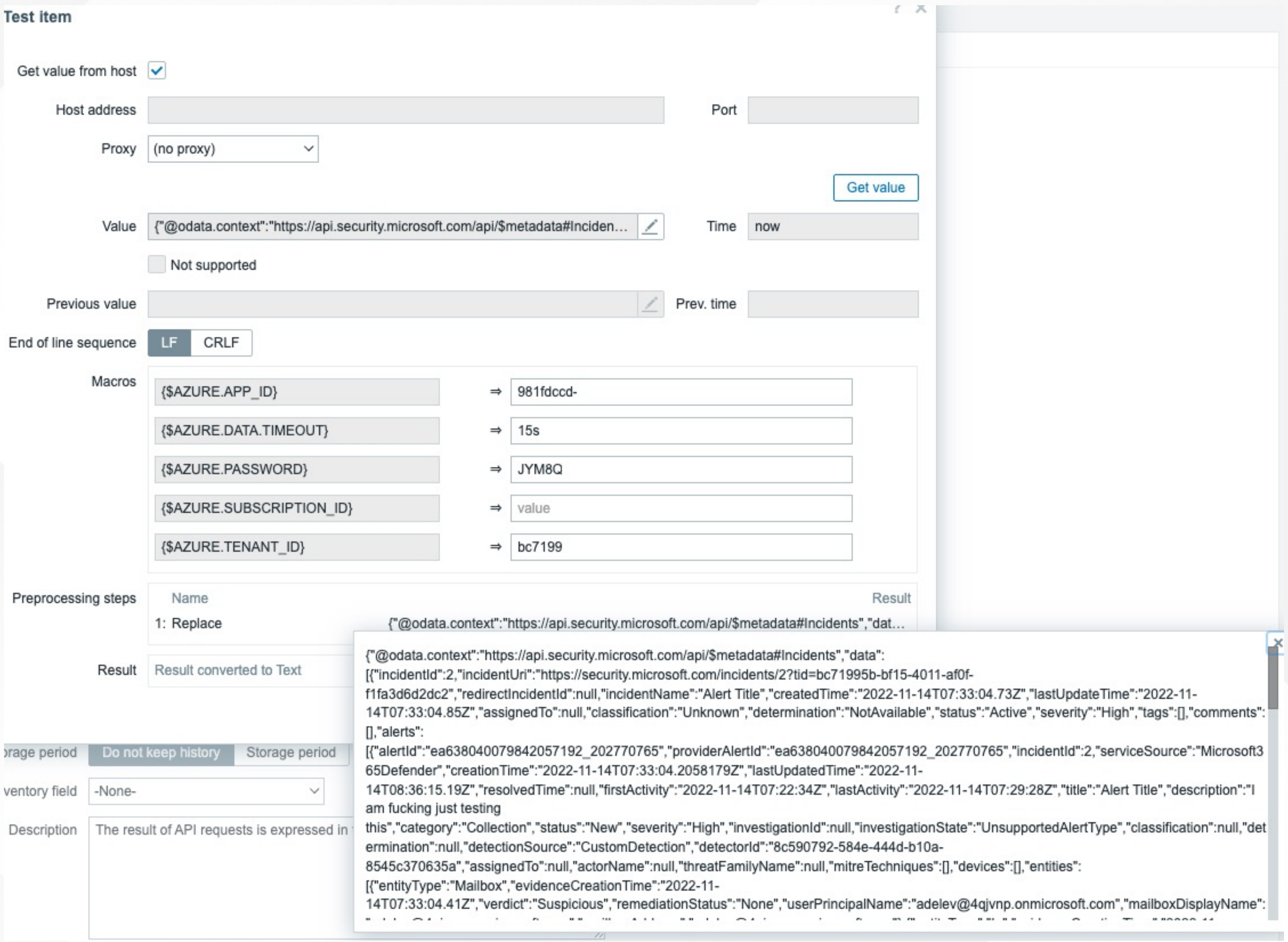
Custom intervals

Type	Interval	Period	Action
Flexible / Scheduling	50s	1-7,00:00-24:00	Remove

Add

* History storage period: Do not keep history | Storage period

- Great success!
- There are threats returned, in JSON format.



Test item

Get value from host ☑

Host address

Port

Proxy (no proxy)

Value {"@odata.context":"https://api.security.microsoft.com/api/$metadata#Inciden…

Time now

□ Not supported

Previous value

Prev. time

End of line sequence LF CRLF

Macros

{$AZURE.APP_ID}	⇒	981fdccd-
{$AZURE.DATA.TIMEOUT}	⇒	15s
{$AZURE.PASSWORD}	⇒	JYM8Q
{$AZURE.SUBSCRIPTION_ID}	⇒	value
{$AZURE.TENANT_ID}	⇒	bc7199

Preprocessing steps

Name	Result
1: Replace	{"@odata.context":"https://api.security.microsoft.com/api/$metadata#Incidents","dat…

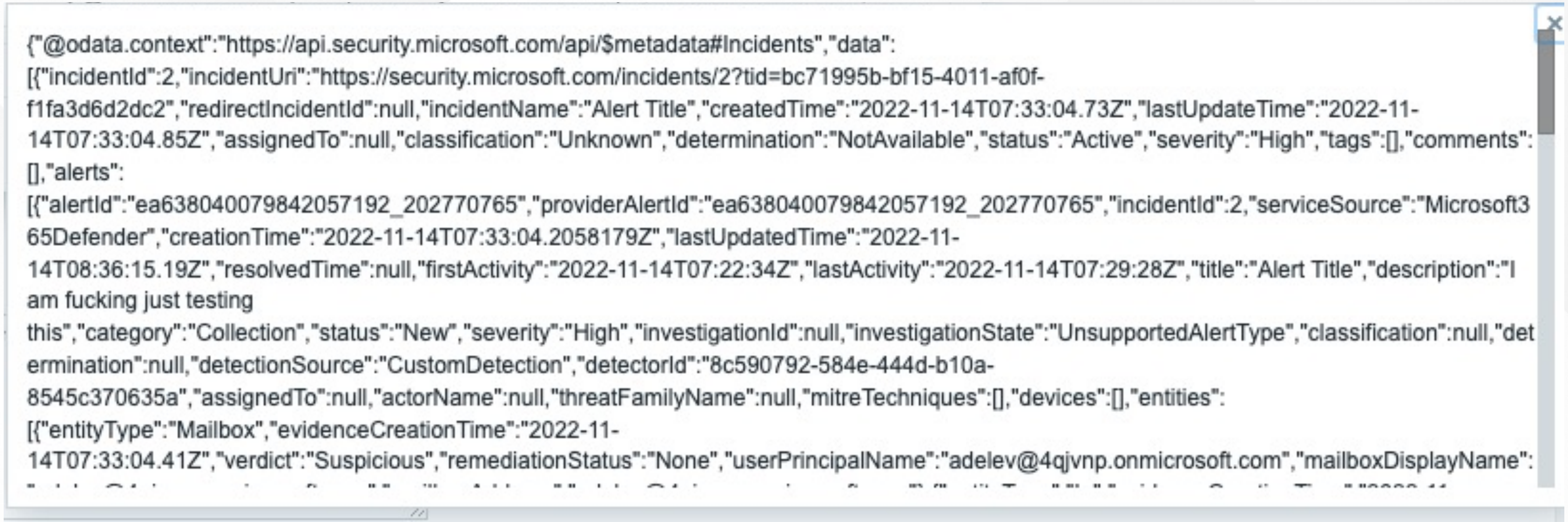
Result Result converted to Text

rage period Do not keep history Storage period

ventory field -None-

Description The result of API requests is expressed in

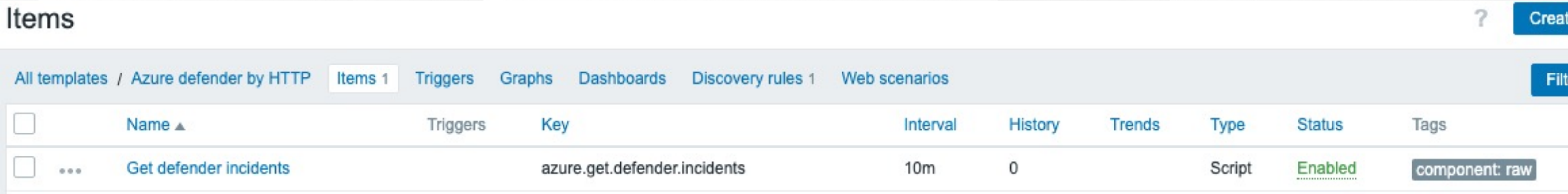
```
{"@odata.context":"https://api.security.microsoft.com/api/$metadata#Incidents","data":
[{"incidentId":2,"incidentUri":"https://security.microsoft.com/incidents/2?tid=bc71995b-bf15-4011-af0f-
f1fa3d6d2dc2","redirectIncidentId":null,"incidentName":"Alert Title","createdTime":"2022-11-14T07:33:04.73Z","lastUpdateTime":"2022-11-
14T07:33:04.85Z","assignedTo":null,"classification":"Unknown","determination":"NotAvailable","status":"Active","severity":"High","tags":[],"comments":
[],"alerts":
[{"alertId":"ea638040079842057192_202770765","providerAlertId":"ea638040079842057192_202770765","incidentId":2,"serviceSource":"Microsoft3
65Defender","creationTime":"2022-11-14T07:33:04.2058179Z","lastUpdatedTime":"2022-11-
14T08:36:15.19Z","resolvedTime":null,"firstActivity":"2022-11-14T07:22:34Z","lastActivity":"2022-11-14T07:29:28Z","title":"Alert Title","description":"I
am fucking just testing
this","category":"Collection","status":"New","severity":"High","investigationId":null,"investigationState":"UnsupportedAlertType","classification":null,"det
ermination":null,"detectionSource":"CustomDetection","detectorId":"8c590792-584e-444d-b10a-
8545c370635a","assignedTo":null,"actorName":null,"threatFamilyName":null,"mitreTechniques":[],"devices":[],"entities":
[{"entityType":"Mailbox","evidenceCreationTime":"2022-11-
14T07:33:04.41Z","verdict":"Suspicious","remediationStatus":"None","userPrincipalName":"adelev@4qjvnp.onmicrosoft.com","mailboxDisplayName":
```



```
{"@odata.context":"https://api.security.microsoft.com/api/$metadata#Incidents","data":
[{"incidentId":2,"incidentUri":"https://security.microsoft.com/incidents/2?tid=bc71995b-bf15-4011-af0f-
f1fa3d6d2dc2","redirectIncidentId":null,"incidentName":"Alert Title","createdTime":"2022-11-14T07:33:04.73Z","lastUpdateTime":"2022-11-
14T07:33:04.85Z","assignedTo":null,"classification":"Unknown","determination":"NotAvailable","status":"Active","severity":"High","tags":[],"comments":
[],"alerts":
[{"alertId":"ea638040079842057192_202770765","providerAlertId":"ea638040079842057192_202770765","incidentId":2,"serviceSource":"Microsoft3
65Defender","creationTime":"2022-11-14T07:33:04.2058179Z","lastUpdatedTime":"2022-11-
14T08:36:15.19Z","resolvedTime":null,"firstActivity":"2022-11-14T07:22:34Z","lastActivity":"2022-11-14T07:29:28Z","title":"Alert Title","description":"I
am fucking just testing
this","category":"Collection","status":"New","severity":"High","investigationId":null,"investigationState":"UnsupportedAlertType","classification":null,"det
ermination":null,"detectionSource":"CustomDetection","detectorId":"8c590792-584e-444d-b10a-
8545c370635a","assignedTo":null,"actorName":null,"threatFamilyName":null,"mitreTechniques":[],"devices":[],"entities":
[{"entityType":"Mailbox","evidenceCreationTime":"2022-11-
14T07:33:04.41Z","verdict":"Suspicious","remediationStatus":"None","userPrincipalName":"adelev@4qjvnp.onmicrosoft.com","mailboxDisplayName":
```

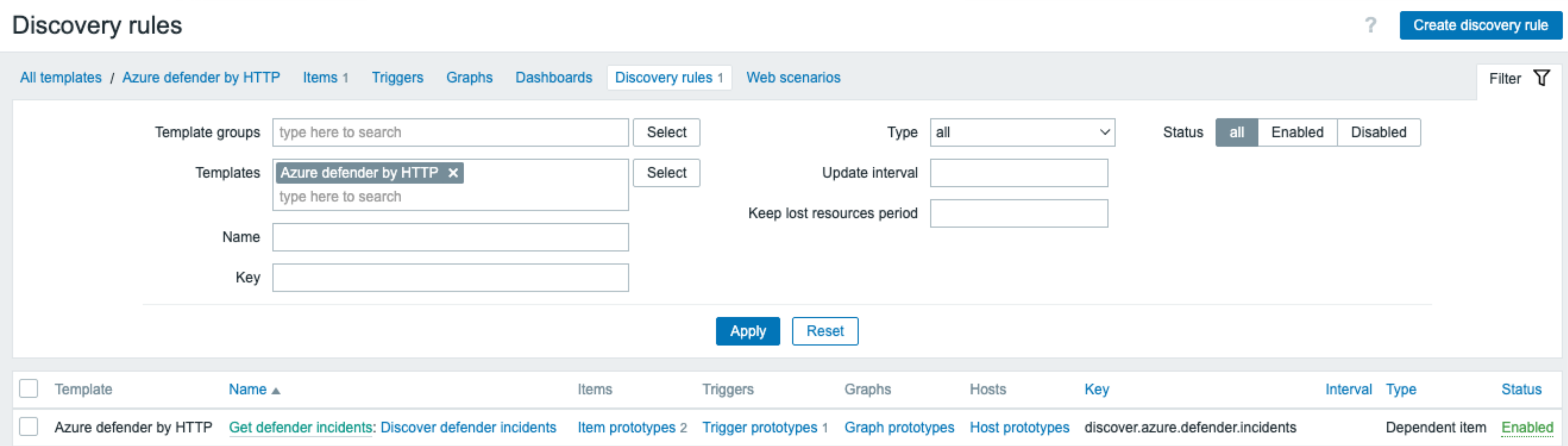
- Phew! Hard part is done. Data comes into Zabbix.

- Time to parse it.
- ”Master” item is already in place, and as there can be multiple incidents, a dependent LLD rule should give enough flexibility.
  - In the LLD rule we create item prototypes to get the incidents
  - In the LLD rule we create trigger prototypes to get the problems



Items

□		Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
□	•••	Get defender incidents		azure.get.defender.incidents	10m	0		Script	Enabled	component: raw



Discovery rules

Template groups: type here to search

Templates: Azure defender by HTTP ✕ type here to search

Name:

Key:

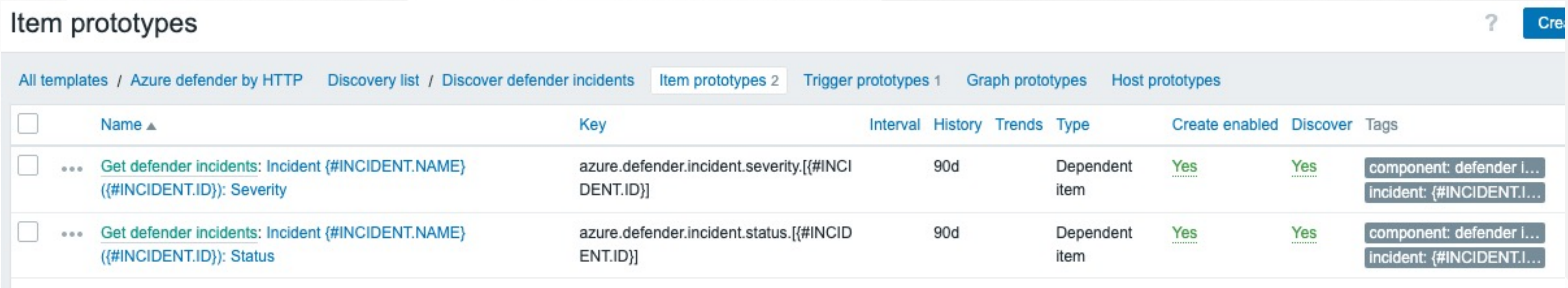
Type: all

Update interval:

Keep lost resources period:

Status: [✓ all] Enabled Disabled

☐	Template	Name ▲	Items	Triggers	Graphs	Hosts	Key	Interval	Type	Status
☐	Azure defender by HTTP	Get defender incidents: Discover defender incidents	Item prototypes 2	Trigger prototypes 1	Graph prototypes	Host prototypes	discover.azure.defender.incidents		Dependent item	Enabled



Item prototypes

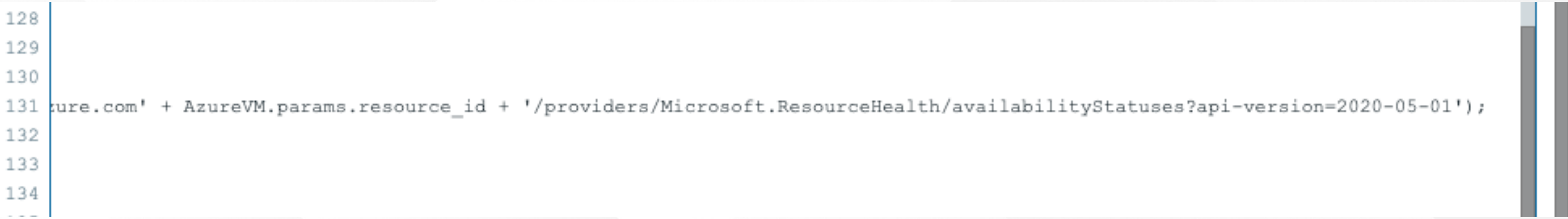
All templates / Azure defender by HTTP   Discovery list / Discover defender incidents   Item prototypes 2   Trigger prototypes 1   Graph prototypes   Host prototypes

□		Name ▲	Key	Interval	History	Trends	Type	Create enabled	Discover	Tags
□	•••	Get defender incidents: Incident {#INCIDENT.NAME} ({#INCIDENT.ID}): Severity	azure.defender.incident.severity.[{#INCIDENT.ID}]		90d		Dependent item	Yes	Yes	component: defender i... incident: {#INCIDENT.I...
□	•••	Get defender incidents: Incident {#INCIDENT.NAME} ({#INCIDENT.ID}): Status	azure.defender.incident.status.[{#INCIDENT.ID}]		90d		Dependent item	Yes	Yes	component: defender i... incident: {#INCIDENT.I...

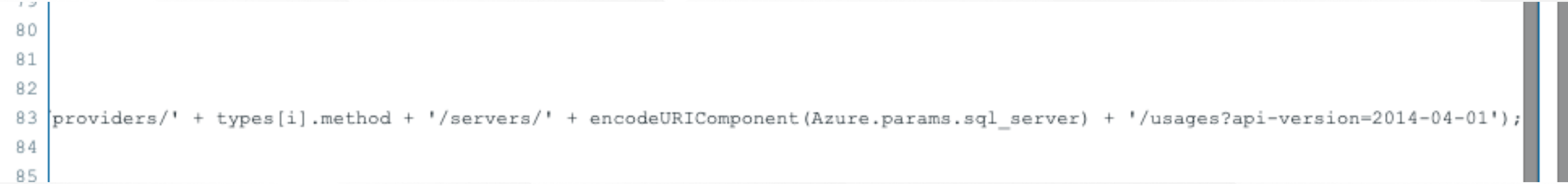
Ok. Whats next?

- Now that this requirement was fulfilled, let’s get out the risky users.
  - Risky user: “The investigation priority score is a score Defender for Cloud Apps gives to each user to let you know how risky a user is relative to other users in your organization.”

- Actually, that is the same workflow, just a different endpoint, and of course a different response.

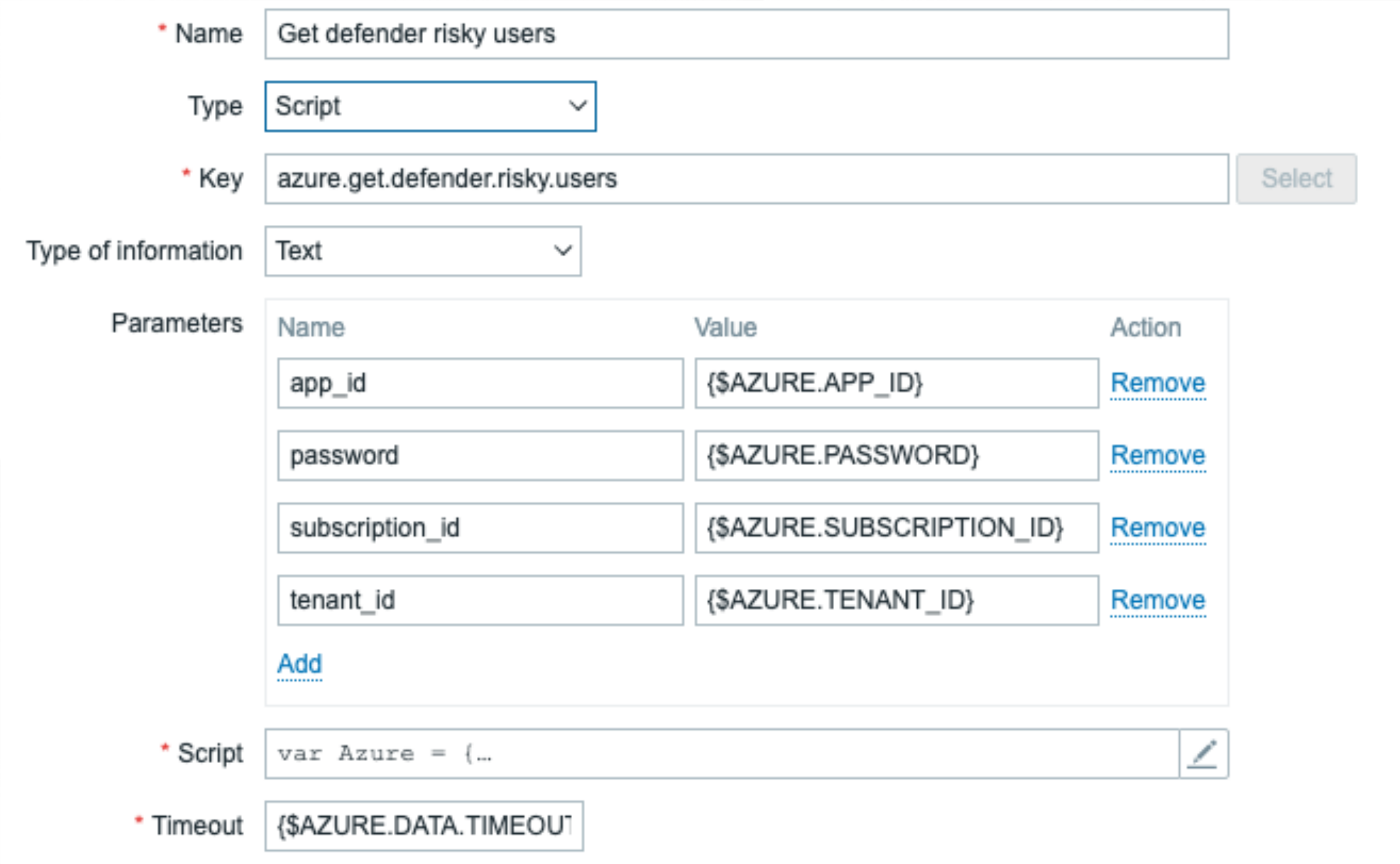


```



ure.com' + AzureVM.params.resource_id + '/providers/Microsoft.ResourceHealth/availabilityStatuses?api-version=2020-05-01');



```



```



providers/' + types[i].method + '/servers/' + encodeURIComponent(Azure.params.sql_server) + '/usages?api-version=2014-04-01');


```

- Master item



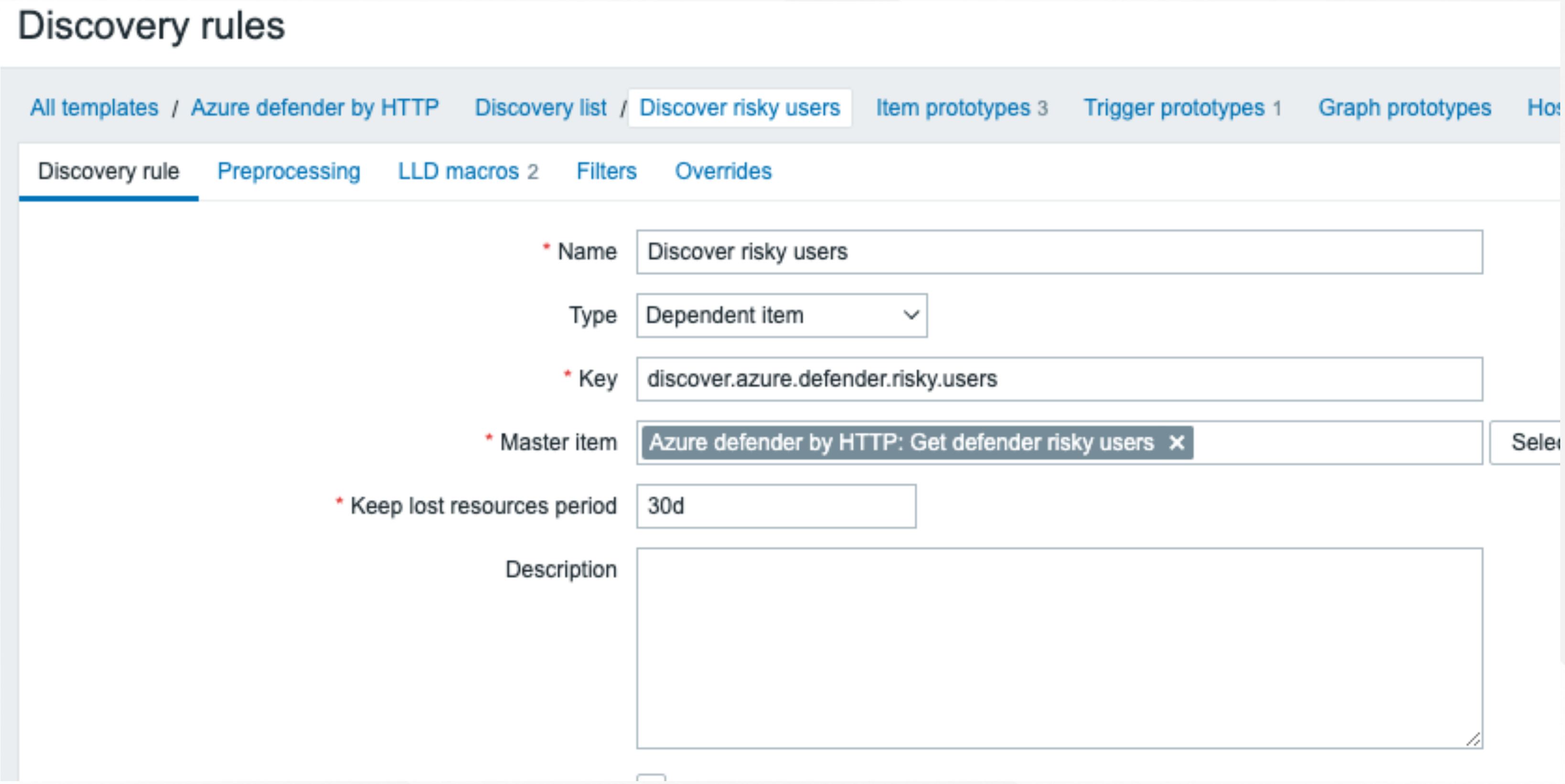
* Name	Get defender risky users
Type	Script
* Key	azure.get.defender.risky.users
Type of information	Text

Parameters

Name	Value	Action
app_id	{$AZURE.APP_ID}	Remove
password	{$AZURE.PASSWORD}	Remove
subscription_id	{$AZURE.SUBSCRIPTION_ID}	Remove
tenant_id	{$AZURE.TENANT_ID}	Remove

* Script	var Azure = {…
* Timeout	{$AZURE.DATA.TIMEOUT

- Dependent LLD rule



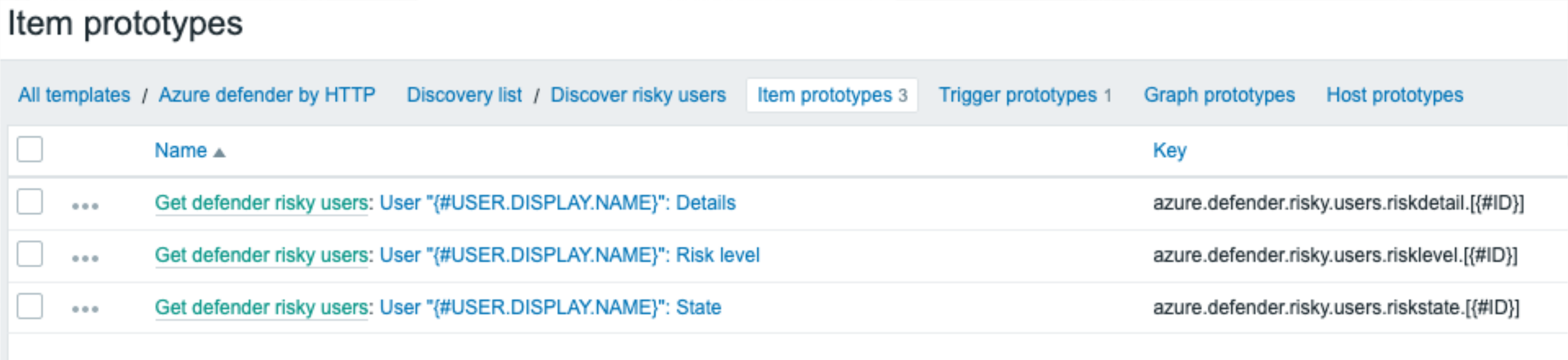
Discovery rules

All templates / Azure defender by HTTP Discovery list / Discover risky users Item prototypes 3 Trigger prototypes 1 Graph prototypes Hos

Discovery rule Preprocessing LLD macros 2 Filters Overrides

* Name	Discover risky users
Type	Dependent item
* Key	discover.azure.defender.risky.users
* Master item	Azure defender by HTTP: Get defender risky users ✕
* Keep lost resources period	30d
Description	

- Some item prototypes

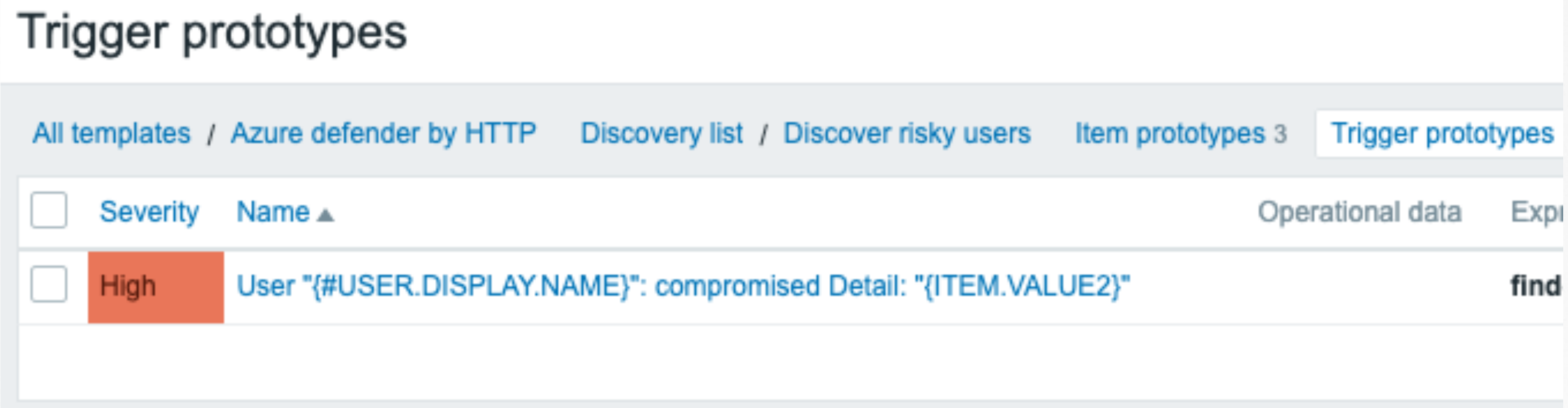


Item prototypes

All templates / Azure defender by HTTP Discovery list / Discover risky users Item prototypes 3 Trigger prototypes 1 Graph prototypes Host prototypes

□		Name ▲	Key
□	•••	Get defender risky users: User "{#USER.DISPLAY.NAME}": Details	azure.defender.risky.users.riskdetail.[{#ID}]
□	•••	Get defender risky users: User "{#USER.DISPLAY.NAME}": Risk level	azure.defender.risky.users.risklevel.[{#ID}]
□	•••	Get defender risky users: User "{#USER.DISPLAY.NAME}": State	azure.defender.risky.users.riskstate.[{#ID}]

- Trigger prototype



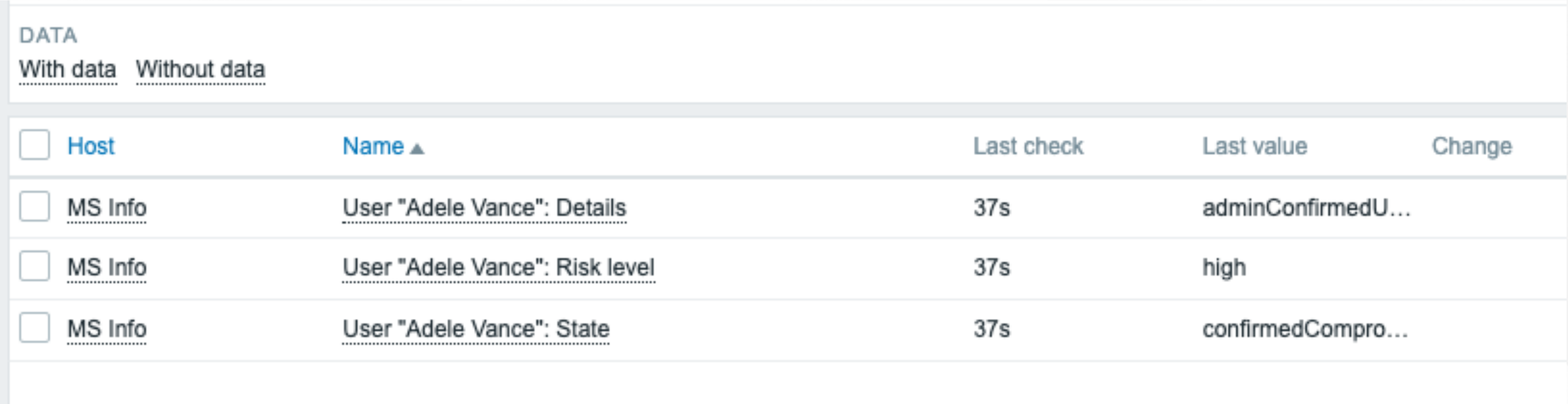
Trigger prototypes

All templates / Azure defender by HTTP Discovery list / Discover risky users Item prototypes 3 Trigger prototypes

□	Severity	Name ▲	Operational data	Expr
□	High	User "{#USER.DISPLAY.NAME}": compromised Detail: "{ITEM.VALUE2}"		find

Oh oh……

- CRAP! We need to fix something….

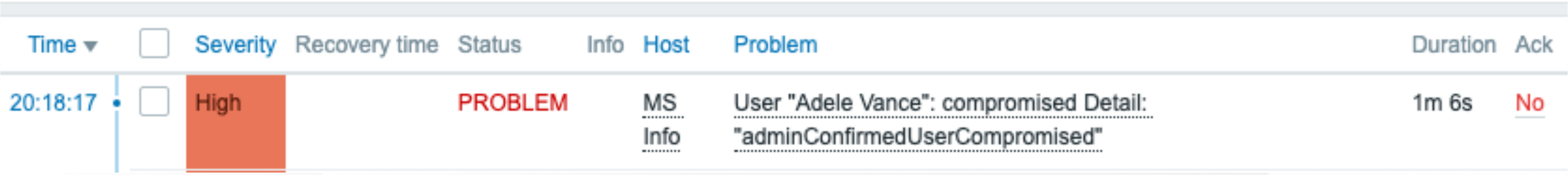


DATA

With data Without data

☐	Host	Name ▲	Last check	Last value	Change
☐	MS Info	User "Adele Vance": Details	37s	adminConfirmedU…	
☐	MS Info	User "Adele Vance": Risk level	37s	high	
☐	MS Info	User "Adele Vance": State	37s	confirmedCompro…	

But atleast Zabbix alerted us



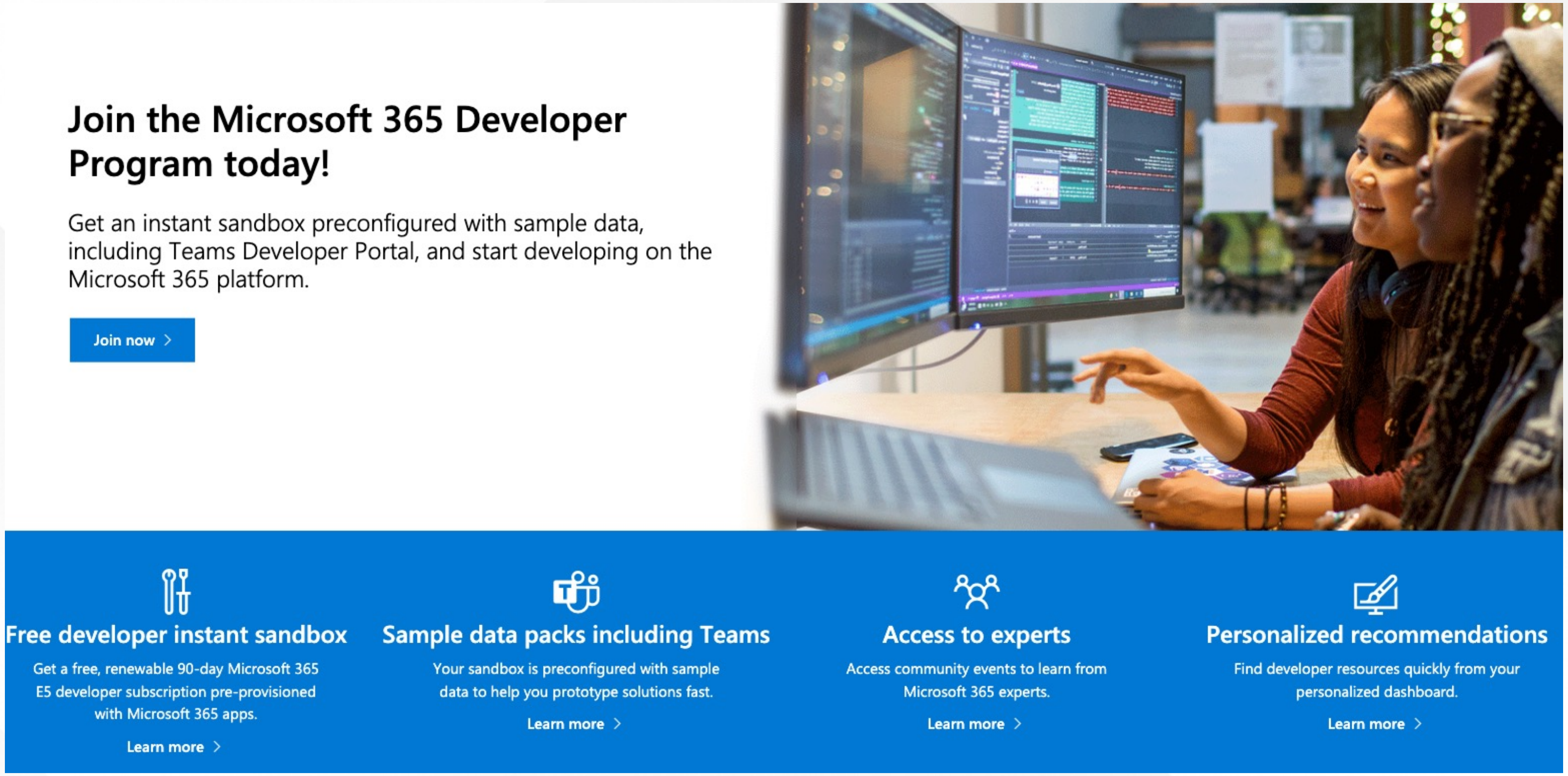
Time ▾	☐	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack
20:18:17 •	☐	High		PROBLEM		MS Info	User "Adele Vance": compromised Detail: "adminConfirmedUserCompromised"	1m 6s	No

- Wait a minute…. That gives us a TON of other options! – remember those API methods mentioned a few slides ago? 😆

- Monitoring email threats
- Monitoring licenses(available, consumed)
- Monitoring locked out users
- Monitoring mailbox size
- Etc, etc etc.

- Please take note of the O365 developer program:

https://developer.microsoft.com/en-us/microsoft-365/dev-program



Join the Microsoft 365 Developer Program today!

Get an instant sandbox preconfigured with sample data, including Teams Developer Portal, and start developing on the Microsoft 365 platform.

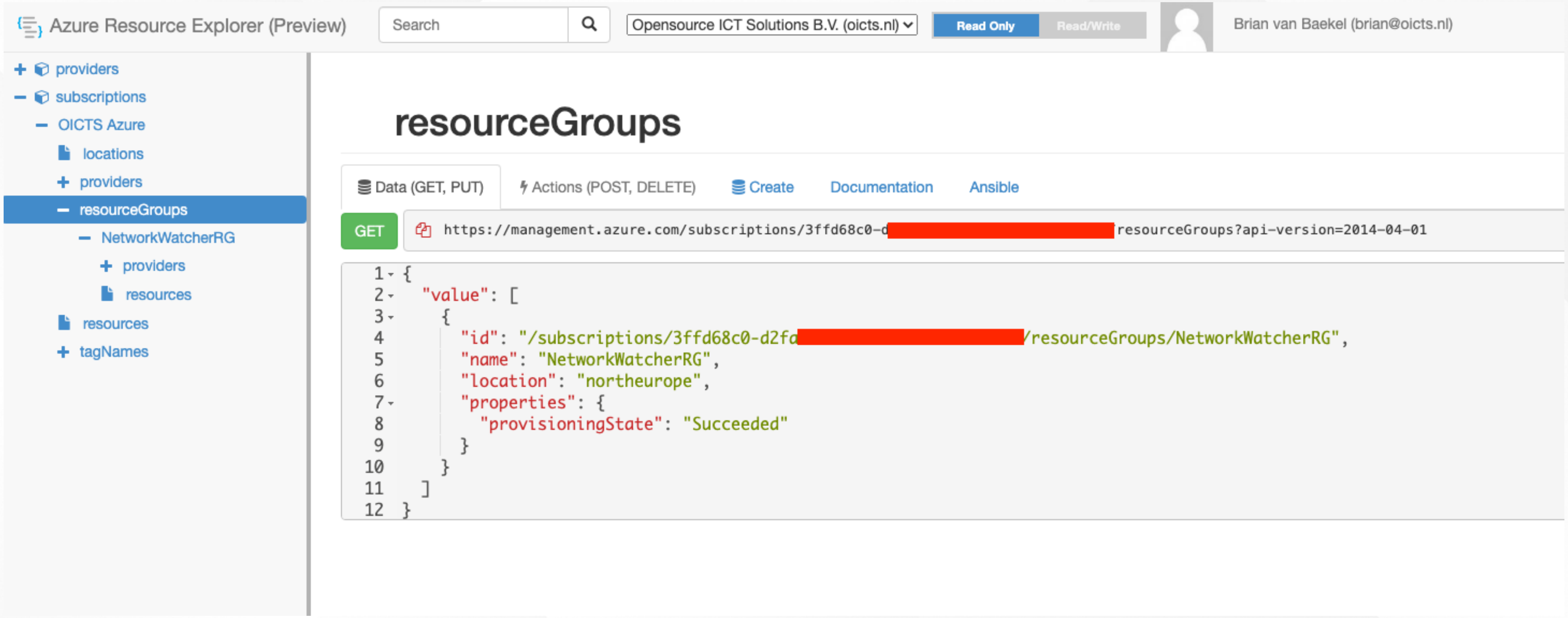
Free developer instant sandbox
Get a free, renewable 90-day Microsoft 365 E5 developer subscription pre-provisioned with Microsoft 365 apps.

Sample data packs including Teams
Your sandbox is preconfigured with sample data to help you prototype solutions fast.

Access to experts
Access community events to learn from Microsoft 365 experts.

Personalized recommendations
Find developer resources quickly from your personalized dashboard.

- Resources.azure.com



resourceGroups

```
https://management.azure.com/subscriptions/3ffd68c0-d[redacted]resourceGroups?api-version=2014-04-01
```

```
{
  "value": [
    {
      "id": "/subscriptions/3ffd68c0-d2fa[redacted]/resourceGroups/NetworkWatcherRG",
      "name": "NetworkWatcherRG",
      "location": "northeurope",
      "properties": {
        "provisioningState": "Succeeded"
      }
    }
  ]
}
```

Contact

Opensource ICT Solutions LTD
5-7 Cranwood Street
London EC1V 9EE
United Kingdom
T. +44 (0) 20 4551 1827
E. info@oicts.co.uk
W. https://oicts.co.uk

Opensource ICT Solutions B.V.
Agriport 38D
1775TB Middenmeer
The Netherlands
T. +31 (0) 72 743 65 83
E. info@oicts.nl
W. https://oicts.nl

Opensource ICT Solutions LLC
251 Little Falls Drive
Wilmington, DE 19808
United States
T. +1 (929) 377 1253
E. info@oicts.com
W. https://oicts.com