CERT-EU Security Guidance (Technical)

Configuring Microsoft 365 for Splunk and Remote monitoring

CERT-EU Team
ver. **2.2.0-beta**
07-11-2022

Contents

1 What is `azap.sh`?

The purpose of the `azap.sh` script is to allow Constituents to grant access to CERT-EU in a scripted way to the needed Azure Security APIs in the various Tenants used, in the scope of CERT-EU's Log Monitoring service.

2 Running `azap.sh`

2.1 Prerequisites

2.1.1 Setting the SAS token environment variable

Running the `azap.sh` script requires to set the environment variable `AZURE_STORAGE_SAS_TOKEN` as shown in the instructions below. This may be *rotated regularly* and may include CERT-EU Constituents *IP ranges* so that only requests originating from these addresses are accepted.

The current value of the `AZURE_STORAGE_SAS_TOKEN` environment variable is distributed with the release and should be treated as *confidential*. If you do not have access or cannot have access at present, you can request it from CERT-EU's Engineering Team via services@cert.europa.eu.

Note that the SAS token has the following form:

```
export AZURE_STORAGE_SAS_TOKEN="sr=https://azap<...>.queue.core.windows.net/credentials&spr=htt
  ps&sv=<...>&si=azap-client-queue-policy&sig=<>...>"
```

Please set the `AZURE_STORAGE_SAS_TOKEN` environment variable now.

2.1.2 Creating and accessing an Azure Cloud Shell

The `azap.sh` script will be executed in an Azure Cloud Shell. Please create it and select the `bash` mode when prompted. You can refer to the following documentation on how to create a Cloud Shell: https://learn.microsoft.com/en-us/azure/cloud-shell/quickstart

Please note that the Cloud Shell does not need to be created in the same Tenant that will be the target of `azap.sh`. You can create a Cloud Shell in a separate, administrative Tenant if needed.

2.2 Providing consent and running the script

- Have your Tenant ID available.
- Open an Azure Cloud Shell and choose the `bash` variant of the Cloud Shell.
- Upload to the Cloud Shell the `azap.sh` script.
- Ensure that you have set the `AZURE_STORAGE_SAS_TOKEN` environment variable as described above.
- Set the `AZAP_TENANT_ID` environment variable to the ID of the Tenant that you wish to configure for CERT-EU Log Monitoring service:

```
export AZAP_TENANT_ID=<TENANT_ID>
```

- If the Tenant to be configured is not the same where the Azure Cloud Shell is running and where you are already authenticated, login to that Tenant:

```
az login --allow-no-subscriptions --tenant <TENANT_ID>
```

- Run the following command in a terminal to give consent, allow the script to run and configure the relevant Tenant for CERT-EU:

```
chmod +x azap.sh
./azap.sh
```

Please close the terminal after copying the secret. The secret will persist on the filesystem until `azap.sh` is run again.

2.3 Removing consent

At any time, you can remove your consent to CERT-EU's access in the configured Tenant. The `azap.sh` script creates an Azure AD application and service principal. One can remove consent at any time by deleting this Azure Active Directory App from the Tenant, and the `azap.sh` script generates a convenient script to perform this operation. To use it, please run:

```
/tmp/azap/cleanup-certeu-azap-for-splunk-and-remote-monitoring.sh
```

Please note that deleting this App from the Azure Tenant will also prevent CERT-EU from monitoring the cloud logs of that Tenant.

2.4 Rotating of credentials

All credentials generated by `azap.sh` expire after 12 months. One can replace the credentials at any time and frequency by re-executing `azap.sh` as presented above.

PLEASE NOTE:

- `azap.sh` is updated frequently. Please make sure that you always ask for, or download, the latest version.
- Every time the `azap.sh` runs, the credentials are regenerated and former ones deleted. One should thus be prepared to update all Cloud TAs used in the Splunk infrastructure shortly after `azap.sh` has generated new credentials. Failing this, the Splunk TAs will be denied access by the various Microsoft Azure APIs and no cloud logs will be fetched.

3 Scope and context

3.1 Technical steps

The following steps will be taken by `azap.sh`:

- Create an App registration in the target Azure AD Tenant.
- Grants permissions to that App that allow read access to the Microsoft Security Graph API and other Azure APIs, listed below, as needed by CERT-EU's Log Monitoring service.
- Sends specific credentials (one secret) to CERT-EU over an Azure Storage Queue identified by a SAS Token. These credentials will be used in a central CERT-EU application which will pull alerts from the Graph Security API into the CERT-EU incident response platform.
- Outputs another set of credentials (one secret) to the Azure Cloud Shell filesystem. These credentials are dedicated to the Splunk platform Applications used in the scope of CERT-EU's Log Monitoring service. These credentials should be used to configure the various Splunk Technolgy Add-ons (TAs) used and advised by CERT-EU's Engineering team.

For more information about the context, use and configuration of these TAs, please refer to CERT-EU Log Monitoring with Splunk configuration guides, the latest revision of which is always available in our Unified Portal. For any question, please do not hesitate to contact services@cert.europa.eu.

3.2 List of Azure APIs

The script sets access permissions to the following APIs:

- Microsoft Graph: `00000003-0000-0000-c000-000000000000` (https://graph.microsoft.com)
- Windows Defender ATP API: `fc780465-2017-40d4-a0c5-307022471b92` (https://api.securitycenter.microsoft.com)
- Microsoft Defender for Cloud Apps / Cloud Apps Security: `05a65629-4c1b-48c1-a78b-804c4abdd4af`
- Office 365 Exchange Online: `00000002-0000-0ff1-ce00-000000000000`
- Office 365 Management API: `c5393580-f805-4401-95e8-94b7a6ef2fc2`

3.2.1 Write permissions

Only one **Write** permissions is granted `ThreatIndicators.ReadWrite.OwnedBy` that allows us to upload ThreatIntelligence data to Sentinel and Defender.

3.3 Administrative actions performed by the script

The script performs the following actions in the destination Tenant:

3.3.1 Add member to Azure AD role

- Makes the Azure AD App a Global Reader in the Tenant.

3.3.2 Grants Permissions and Admin Consent

The permissions can be examined by reading the source code of azap.sh. They are also provided in the following screenshot:

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (9)				
AuditLog.Read.All	Application	Read all audit log data	Yes	Granted for EC_CERT-EU...
Directory.Read.All	Application	Read directory data	Yes	Granted for EC_CERT-EU...
Policy.Read.All	Application	Read your organization's policies	Yes	Granted for EC_CERT-EU...
Reports.Read.All	Application	Read all usage reports	Yes	Granted for EC_CERT-EU...
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	Granted for EC_CERT-EU...
ServiceHealth.Read.All	Application	Read service health	Yes	Granted for EC_CERT-EU...
ServiceMessage.Read.All	Application	Read service messages	Yes	Granted for EC_CERT-EU...
ThreatIndicators.ReadWrite.Own	Application	Manage threat indicators this app creates or owns	Yes	Granted for EC_CERT-EU...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for EC_CERT-EU...
Office 365 Exchange Online (1)				
ReportingWebService.Read.All	Application	ReportingWebService.Read.All	Yes	Granted for EC_CERT-EU...
Office 365 Management APIs (2)				
ActivityFeed.Read	Application	Read activity data for your organization	Yes	Granted for EC_CERT-EU...
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes	Granted for EC_CERT-EU...
WindowsDefenderATP (1)				
Alert.Read.All	Application	Read all alerts	Yes	Granted for EC_CERT-EU...

Figure 1: app-permissions

3.4 Test

After updating the username and password in the various Splunk Apps, please check the last log received for each Cloud App in Splunk in order to confirm that everything is working well with the new secret. Please contact CERT-EU if you wish that we cross-check.

3.5 Errors and warnings

Indicates your tenant may not have Licenses for O365:

```
-------------- Check API is present: 'Office 365 Exchange Online' with id:
  00000002-0000-0ff1-ce00-000000000000
ERROR: Resource '00000002-0000-0ff1-ce00-000000000000' does not exist or one of its queried
  reference-property objects are not present.
-------------- Check API is present: 'Office 365 Management APIs' with id:
  c5393580-f805-4401-95e8-94b7a6ef2fc2
ERROR: Resource 'c5393580-f805-4401-95e8-94b7a6ef2fc2' does not exist or one of its queried
  reference-property objects are not present.
WARNING: Missing API so will not add permission ActivityFeed.Read
WARNING: Missing API so will not add permission ActivityFeed.ReadDlp
WARNING: Missing API so will not add permission ReportingWebService.Read.All
```

Indicates that azap has already been run in this Tenant::

```
WARNING: Found an existing application instance: (id) a22e91fb-86ae-4876-878d-ed4f3f60894d. We
  will patch it.
```

Indicates the permission is already present:

```
-------------- Assign 'Global Reader' to 8bd9d5a9-e70e-4118-b2d8-82e2a872e434
ERROR: Bad Request({"error":{"code":"Request_BadRequest","message":"A conflicting object with
  one or more of the specified property values is present in the
  directory.","innerError":{"date":"2022-10-28T09:34:39","request-
  id":"894d429e-b09b-462b-a6aa-08bc768225c9","client-request-
  id":"894d429e-b09b-462b-a6aa-08bc768225c9"}}})
```

4 Lighthouse for Incident Response in Azure

> According to Microsoft "Azure Lighthouse offers service providers a single control plane to view and manage Azure across all their customers with higher automation, scale, and enhanced governance. With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust management tooling built into the Azure platform. This offering can also benefit enterprise IT organisations managing resources across multiple tenants." - Microsoft

Please run the following script in your account to grant CERT-EU permissions for *incident response*.

- You may find Azure CloudShell convenient for running the script. If you prefer, the script is very simple and you can copy and paste the instructions directly into a shell.

Lighthouse works on a per subscription basis, which means Lighthouse has to be set up in each of your Azure subscriptions. The following will set up Lighthouse in all the subscriptions returned by `az account list`.

To see details of subscriptions use:

```
./deploy-lighthouse-to-allow-certeu-access.sh --list
```

To set up Lighthouse for all subscriptions:

```
./deploy-lighthouse-to-allow-certeu-access.sh --all
```

Alternatively, you can set it up per subscription as follows:

```
chmod u+x
./deploy-lighthouse-to-allow-certeu-access.sh <subscription name>
```

4.1 Roles granted to CERT-EU

These roles are based on those granted to Digit S2 - SecOps/CSIRC for **Commission and the Executive Agencies** subscriptions: Security Reader, Log Analytics Reader and Reader.

- Security Reader
- Log Analytics Reader
- Microsoft Sentinel Reader is a more restricted permission than (Reader).

4.2 View permissions

Sign into the Azure Portal and search for Service providers | Delegations.

One can retrieve this information from the Azure CLI:

```
$ az managedservices definition list
$ az managedservices assignment list
```

CERT-EU can view consenting constituents by signing into the Azure Portal under My customers | Customers.

5 Manual task

5.1 Threat Intelligence

> Microsoft Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Microsoft Sentinel from your Threat Intelligence Platform (TIP), ...

To ensure that ThreatIntelligence is loaded into Sentinel add the **Threat Intelligent Platforms (Preview)** *connector*. On the Azure Portal, search for Microsoft Sentinel then look for **Data connectors** under the **Configuration** section on the left hand panel.

Each Microsoft Sentinel instance has a *Log Analytics Workspace*. The *connector* loads threat intelligence into the *Log Analytics* ** ThreatIntelligenceIndicator** table. One can query this table while **Threat Hunting**.

To enable auditing of the **ThreatIntelligenceIndicator** table. From the Azure Portal search for each *Log Analytics Workspace*. On the left panel click on **Diagnostic Settings** under the **Monitoring** section. Choose **Add diagnostic setting** then **Audit** and **Send to Log Analytics workspace**.

TLP Definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER information only with members of their own organisation.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
WHITE	Disclosure is not limited.	TLP:WHITE information may be distributed freely.