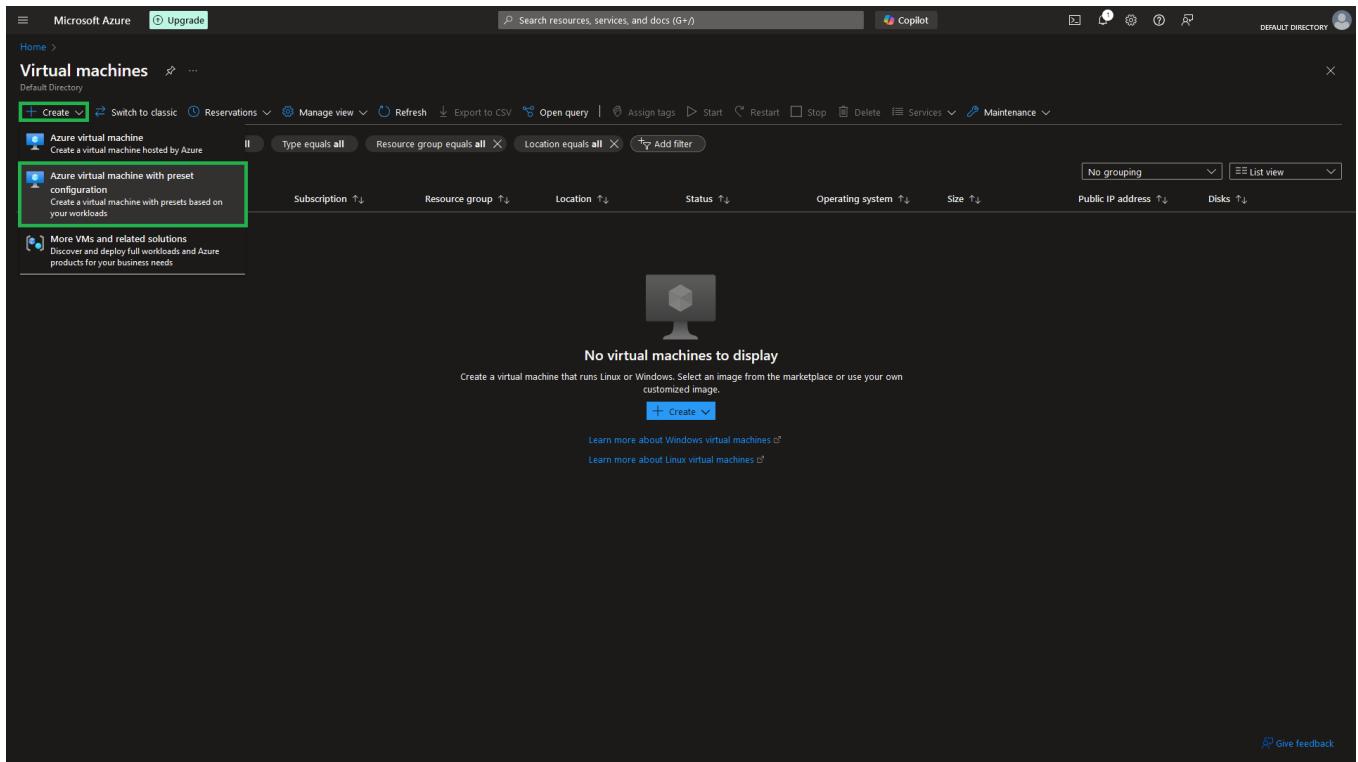


Azure security project solution PART 1: *Creating a honeypot VM*

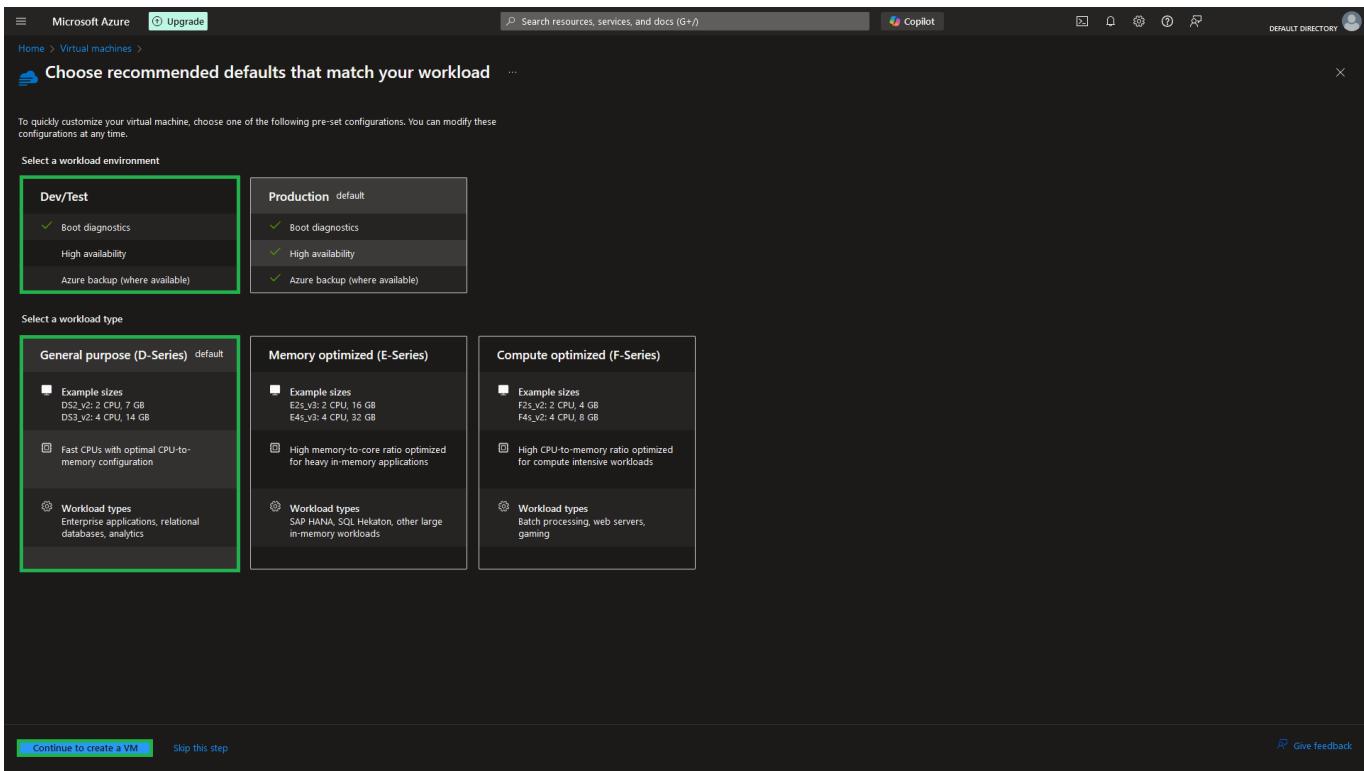
In this project we will build our own security operations center by utilizing Microsoft Sentinel to deploy a Security Information and Event Management (SIEM) solution that monitors and generates alerts for a virtual machine – we can use it as an RDP honeypot. We will also setup a threat intelligence feed that sends information about common and newly discovered indicators of compromise (IoCs) to the SIEM.

Task 1: Create a resource group and a Virtual Machine

1. After we have logged in to the Azure Portal, we begin by going to the **Virtual Machines** page, selecting **Create**, and clicking on **Azure virtual machine with preset**.



2. We then choose to the a **Dev/Test** under *Select a workload environment* and **General purpose (D-Series)** under *Select a workload type*.



3. On the next page, on the **Basics** tab, we create the following configuration:

| Field | Value |
|----------------------|---|
| Subscription | Our current subscription. |
| Resource group | Create a new resource group called SIEMproject by clicking on Create new in the Resource group section. |
| Virtual machine name | Enter a unique VM name, such as SIEMprojectVM . |
| Region | Select the with the least latency and highest availability closest to you. |
| Availability options | Select Availability zone . |
| Availability zone | Select Zones 1 . |
| Image | Select Windows 10 Pro |

The screenshot shows the Microsoft Azure 'Create a virtual machine' wizard. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', and a 'Copilot' icon. Below the navigation is a breadcrumb trail: 'Home > Virtual machines > Choose recommended defaults that match your workload > Create a virtual machine'. A warning message at the top says: '⚠️ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.' To the right is a large blue 'Create' button with a white cloud icon.

Below the warning, there are three tabs: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability' (which is selected), and 'Help me choose the right VM size for my workload'. The main configuration area starts with 'Subscription *' set to 'Azure subscription 1' and 'Resource group *' set to '(New) SIEMproject' (with a red box around it). Under 'Instance details', the 'Virtual machine name' is 'SIEMprojectVM', 'Region' is '(Europe) West Europe', and 'Availability options' is 'Availability zone'. The 'Zone options' section shows 'Self-selected zone' is selected (radio button is checked). Under 'Availability zone *', 'Zone 1' is selected. A note says: 'You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more'. The 'Security type' dropdown is set to 'Trusted launch virtual machines'. Under 'Image *', 'Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible)' is selected. The 'VM architecture' dropdown shows 'x64' is selected. At the bottom, there are buttons for '< Previous', 'Next : Disks >' (highlighted in green), and 'Review + create'.

4. We scroll down to create our admin account **username** and **password** and allow **RDP port 3389**.

Note: RDP events are the most easily generated security events which is why they are ideal to quickly test if our SIEM solution is successfully generating alerts. In a production environment, it is best to use **Microsoft Defender for Cloud's just-in-time (JIT) access** for VMs for maximum security.

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

D-series is recommended for general purpose workloads.

Enable Hibernation

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. [Learn more](#)

Administrator account

Username * ✓

Password * ✓

Confirm password * ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports None Allow selected ports

Select inbound ports * ✓

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Licensing

< Previous Next : Disks > Review + create

5. We can leave all other tabs to their default values and go straight to the **Review + create** tab where we click on **Create** to deploy the resource.

Validation passed

Price

1 X Standard D4s v3 by Microsoft Subscription credits apply
0.2400 USD/hr Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

| | |
|----------------------|------------------------------|
| Subscription | Azure subscription 1 |
| Resource group | (new) SIEMproject |
| Virtual machine name | SIEMprojectVM |
| Region | West Europe |
| Availability options | Availability zone |
| Zone options | Self-selected zone |
| Availability zone | <input type="radio"/> Create |

< Previous Next > **Create**

6. We now wait for notification that our deployment is complete.

The screenshot shows the Microsoft Azure portal with the search bar at the top containing "CreateVm-MicrosoftWindowsDesktop.Windows-10-win10-20241022171902". Below the search bar, the "Overview" tab is selected. A prominent green box highlights the message "Your deployment is complete". Deployment details are listed in a table:

| Resource | Type | Status | Operation details |
|---------------------|---|---------|-----------------------------------|
| SIEMprojectvM | Microsoft.Compute/virtualMachines | OK | Operation details |
| siemprojectvm790_x1 | Microsoft.Network/networkInterfaces | Created | Operation details |
| SIEMprojectVM-vnet | Microsoft.Network/virtualNetworks | OK | Operation details |
| SIEMprojectVM-nsg | Microsoft.Network/networkSecurityGroups | OK | Operation details |
| SIEMprojectVM-ip | Microsoft.Network/publicIPAddresses | OK | Operation details |

Below the table, there are "Next steps" recommendations: "Setup auto-shutdown Recommended", "Monitor VM health, performance and network dependencies Recommended", and "Run a script inside the virtual machine Recommended". At the bottom, there are two buttons: "Go to resource" and "Create another VM". To the right of the main content, there are promotional cards for "Cost Management", "Microsoft Defender for Cloud", and "Free Microsoft tutorials".

Task 2: Create a Log Analytics workspace and activate Microsoft Sentinel

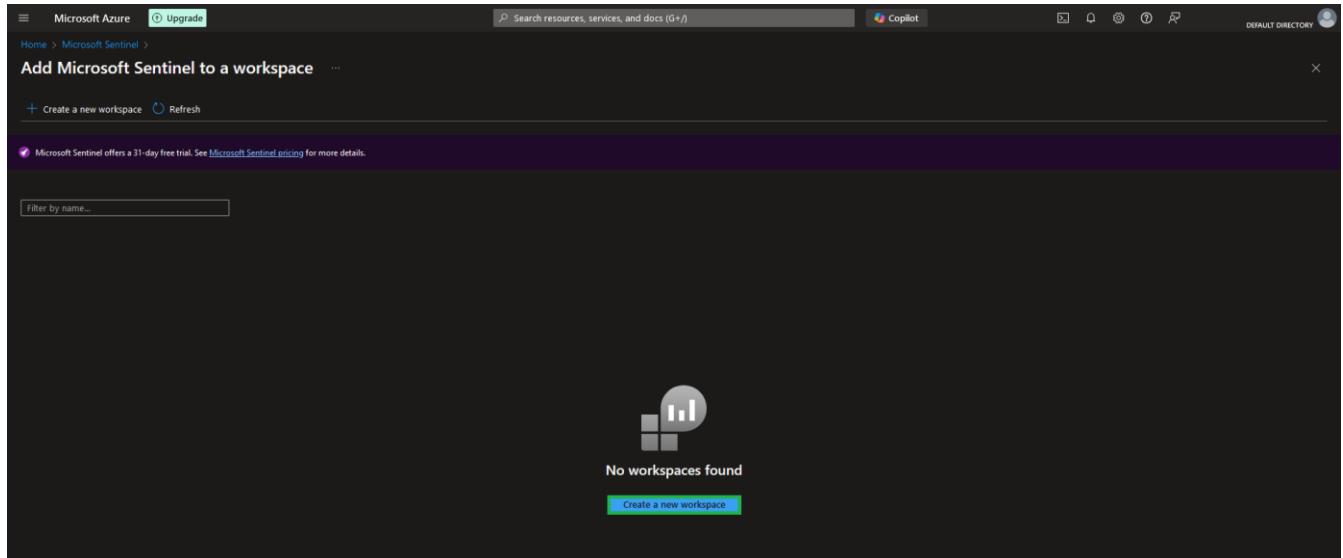
- Once that is done, we go back to the Azure Portal and type in “Microsoft Sentinel” into the search box.

The screenshot shows the Microsoft Azure portal search results for "Microsoft Sentinel". The search bar at the top contains "Microsoft Sentinel". Below the search bar, the "Azure services" section is visible, along with a "Resources" section. The search results show a list of services, with "Microsoft Sentinel" highlighted by a green box. Other listed services include "Virtual machines", "Cosmos DB", "Microsoft Entra ID", "Microsoft Entra Connect", and "Microsoft Entra authentication methods". To the right, there are buttons for "Storage accounts" and "More services".

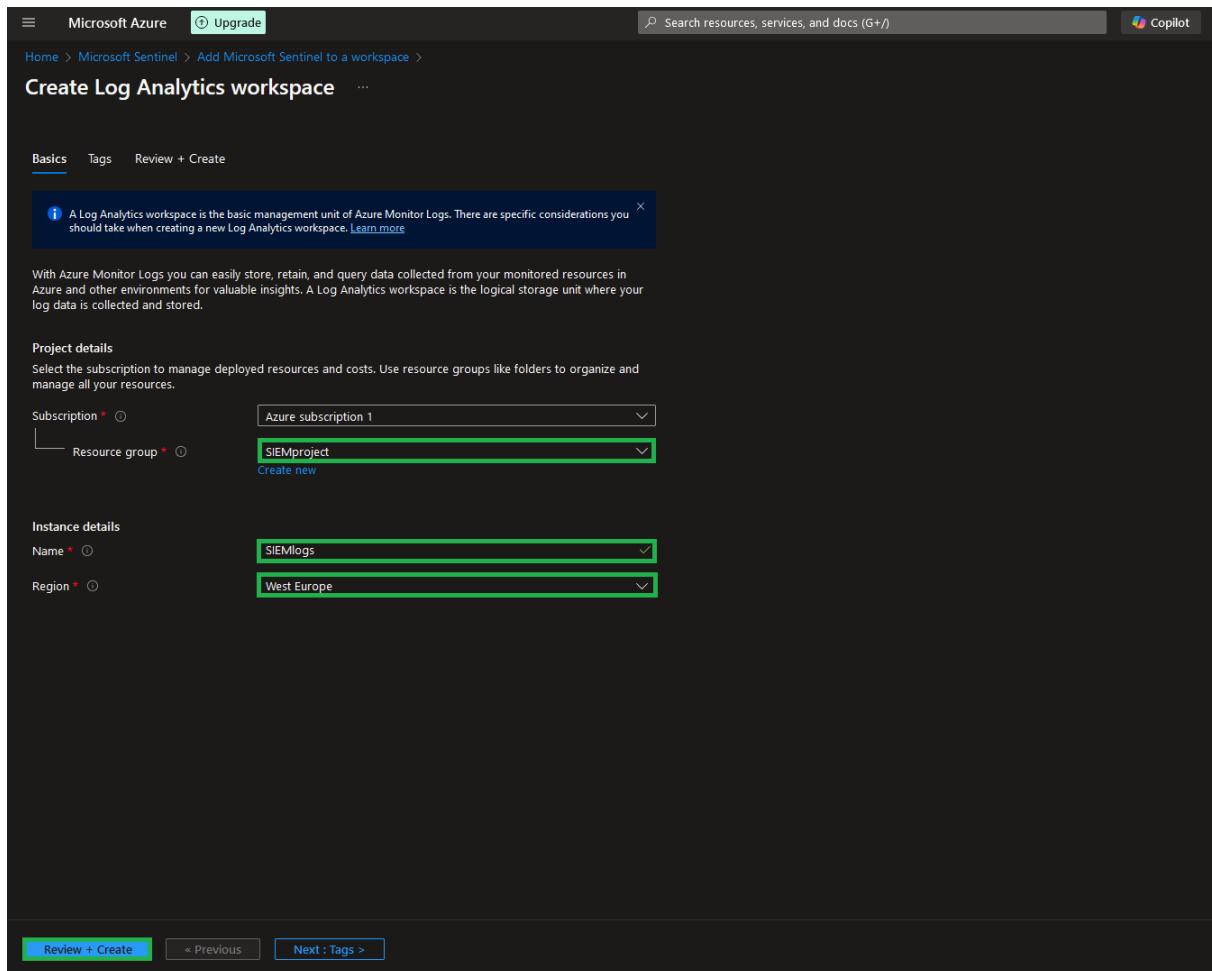
- On the Microsoft Sentinel page, we simply click on **Create Microsoft Sentinel**.

The screenshot shows the Microsoft Azure portal Microsoft Sentinel page. The search bar at the top contains "Microsoft Sentinel". The main content area displays a message: "No Microsoft Sentinel to display. See and stop threats before they cause harm, with SEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise." Below this message are two buttons: "Create Microsoft Sentinel" and "Learn more".

3. We can then either add Sentinel to an existing Log Analytics workspace or create a new one. Here we have no existing workspaces, so we click on the **Create a workspace** button.



4. On the **Create Log Analytics workspace** page, we make sure that we have selected the same resource group as the resources that we want to monitor – in this case, the **SIEMproject** resource group where our VM is. We also make sure that we are deploying it the same region, in my case **West Europe**. Finally, we name our workspace, select Review + create, and click **Create** after we've reviewed our configuration.

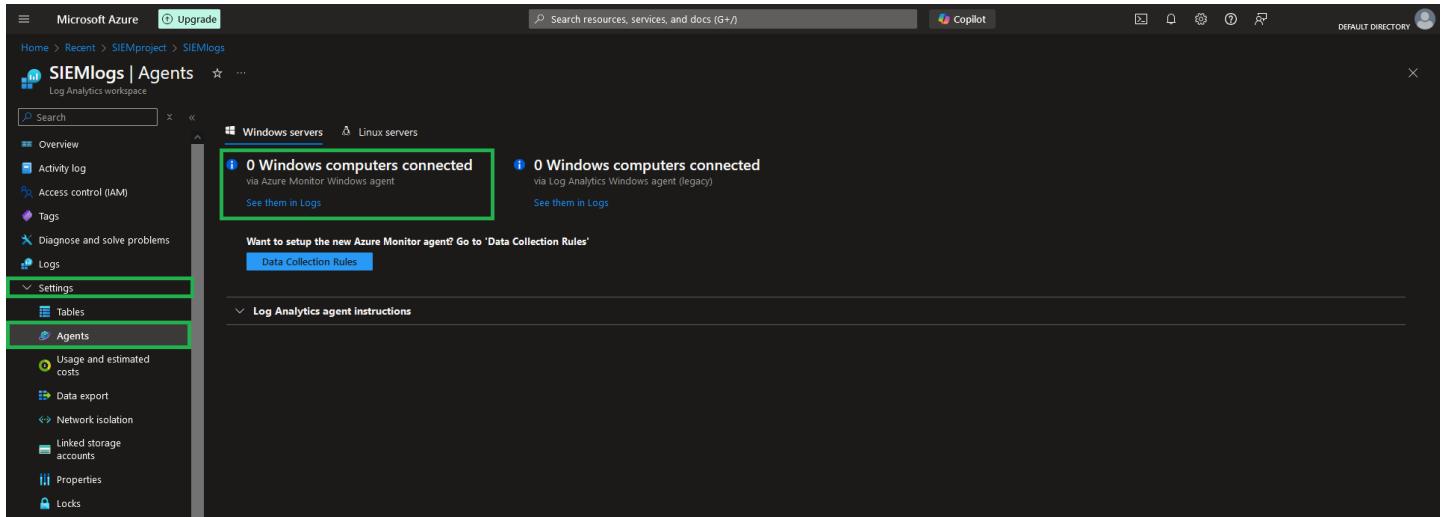


5. Once we are notified that our Log Analytics workspace is created, we click on the **Add** button to add Microsoft Sentinel to the workspace.

6. We now wait for the confirmation that Microsoft Sentinel has been activated.

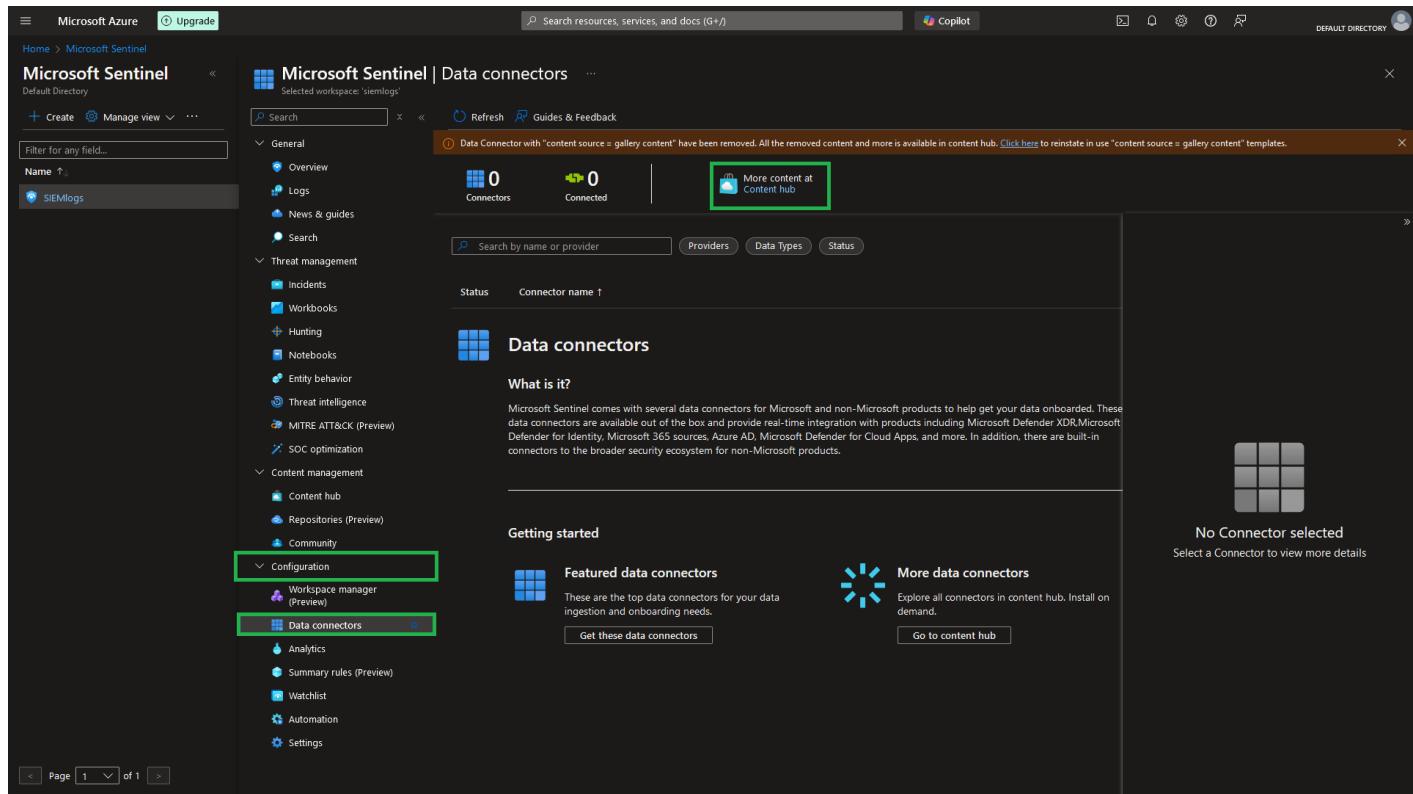
Task 3: Setting up a Data Connector and creating a data collection rule

1. We now need to add our virtual machine to the Log Analytics workspace so that its event logs can be ingested by Microsoft Sentinel. If we go back to the **SIEMlogs** Log Analytics workspace page and go to **Agents** under the *Settings* blade, we will see that we have 0 Windows computers connected to the workspace.



The screenshot shows the Microsoft Azure Log Analytics workspace titled 'SIEMlogs'. In the left sidebar, the 'Agents' section is highlighted with a green box. The main content area shows two status boxes: one for 'Azure Monitor Windows agent' and another for 'Log Analytics Windows agent (legacy)', both indicating 0 connected computers. A button labeled 'Data Collection Rules' is visible below the first status box.

2. To remedy this, we have to set up a **Data connector**. This is done by going to the **Microsoft Sentinel** page, clicking on **Data connectors** under the *Configurations* blade, and going to the **Content hub**.



The screenshot shows the Microsoft Sentinel 'Data connectors' page. The 'Content hub' section is highlighted with a green box. The main area displays '0 Connectors' and '0 Connected'. A message at the top states: 'Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" template.' Below this, there's a search bar and a 'More content at Content hub' button. The 'Data connectors' section includes a 'What is it?' summary and a 'Getting started' section with 'Featured data connectors' and 'More data connectors' options.

3. On the Content hub page, we input “Azure Monitor Agent” into the search box, select **Windows Security Events** from the results and click on **Install**.

The screenshot shows the Microsoft Azure Content hub interface. At the top, there are summary counts: 367 Solutions, 303 Standalone contents, 0 Installed, and 0 Updates. A search bar and Copilot button are also present. Below the summary, a search bar filters results for "Azure Monitor Agent". The main table lists various connectors, including "Windows Security Events" which is highlighted with a green border. The right panel provides detailed information about the "Windows Security Events" connector, including its provider (Microsoft), support (Microsoft Support), and version (3.0.9). It also includes a note about the connector's functionality and compatibility.

- Two data connectors should now show up on the Data connectors page. We select the **Windows Security Events via AMA** connector and click on **Open connector page**.

The screenshot shows the Microsoft Sentinel Data connectors page. The left sidebar navigation includes General, Threat management, Content management, Configuration, and Data connectors (which is currently selected). The main area displays a list of connectors, with "Windows Security Events via AMA" highlighted with a green border. The right panel provides detailed information about the "Windows Security Events via AMA" connector, including its status (Disconnected), provider (Microsoft), and last log received. It also includes sections for Last data received, Content source, Author, Related content, and a chart showing data received over time.

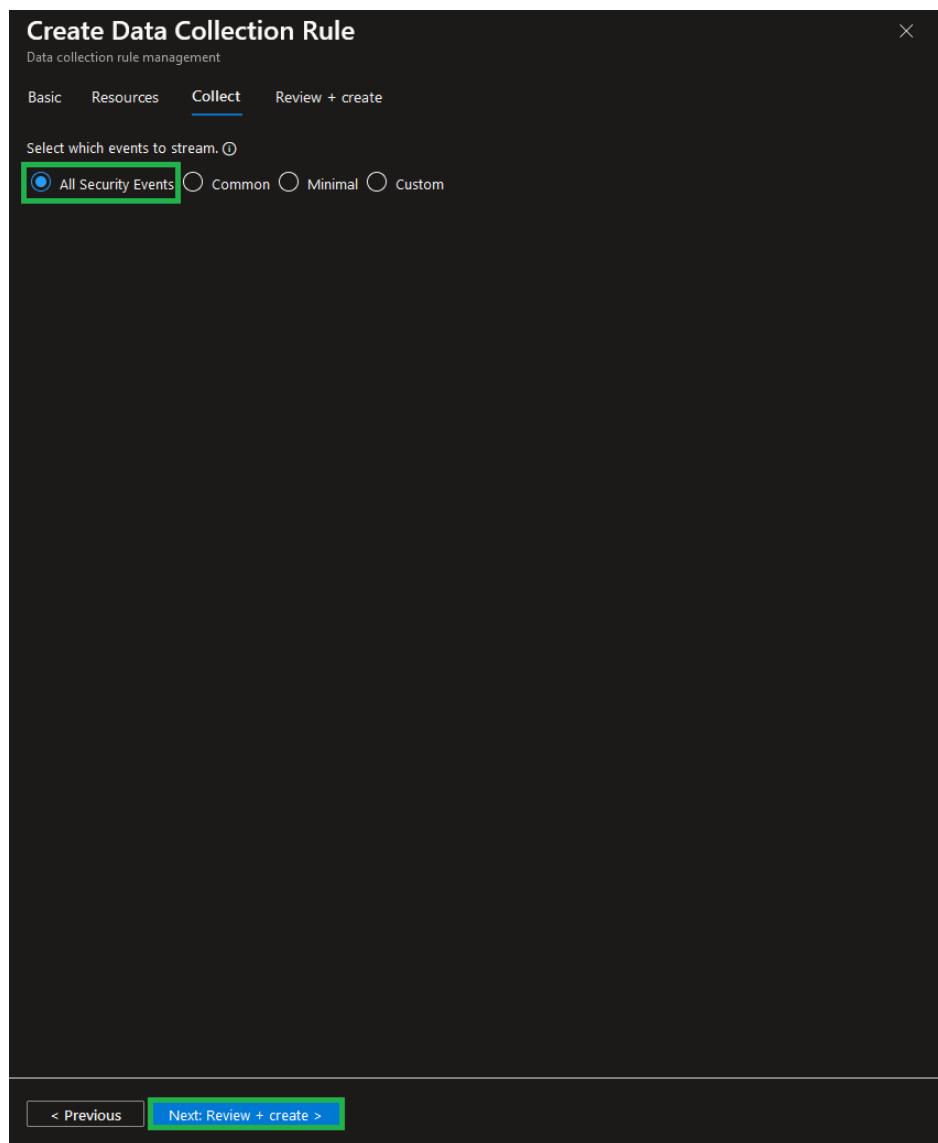
5. Once on the connector page, we click on **+Create data collection rule** and input a **Rule name** on the **Basic** tab like, for example, **WinEventLogsToSentinel**. We then click on **Next: Resources**.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Windows Security Events via AMA' connector page is displayed, showing details like 'Disconnected Status', 'Microsoft Provider', and 'Last Log Received'. It also includes a 'Description' section about streaming security events from Windows machines. On the right, the 'Create Data Collection Rule' wizard is open, specifically the 'Basic' tab. The 'Rule name' field is set to 'WinEventLogsToSentinel'. The 'Subscription' dropdown shows 'Azure subscription 1' and the 'Resource group' dropdown shows 'SIEMproject'. A green box highlights the 'Rule name' field. At the bottom right of the wizard, the 'Next: Resources >' button is visible.

6. On the **Resources** tab, we select the subscription, resource group, and VM we wish to include and click on **Next: Collect**.

The screenshot shows the 'Create Data Collection Rule' wizard on the 'Resources' tab. It lists the selected resources under 'Scope': 'Selected: All' for Subscriptions, Resource Groups, Resource Types, and Locations. Below this, a tree view shows 'Azure subscription 1' expanded, revealing 'siemproject' and 'SIEMprojectVM'. The 'SIEMprojectVM' node is highlighted with a green box. At the bottom, the '< Previous' and 'Next: Collect >' buttons are visible.

7. On the **Collect** tab we select the **All Security Events** radio button and click on **Next: Review + create**.



8. We then click on **Create** once more to finalize the process.

Create Data Collection Rule

Data collection rule management

Validation passed

Basic Resources Collect **Review + create**

Basic

Data rule name: WinEventLogsToSentinel

Subscription: Azure subscription 1

Resource Group: SIEMproject

Selected resources

| Name | Type |
|---------------|-----------------------------------|
| siemprojectvm | microsoft.compute/virtualmachines |

Selected events

AllEvents

< Previous **Create**

A green box highlights the "Create" button at the bottom.

Task 4: Creating a Microsoft Sentinel scheduled rule and generating an incident

1. We now want to go back to the Microsoft Sentinel page and create a rule that checks for successful sign ins via RDP. To do this, we select **Logs** under the *General* blade. We type in the following query and hit **Run**:

```
SecurityEvent  
| where Activity contains "success" and Account !contains "system"
```

The screenshot shows the Microsoft Sentinel Logs interface. On the left, there's a navigation sidebar with sections like General, Threat management, Content management, and Configuration. The 'Logs' section is currently selected. In the main area, there's a search bar and a 'New Query 1*' button. Below it, a query editor window displays the following LogSearch query:

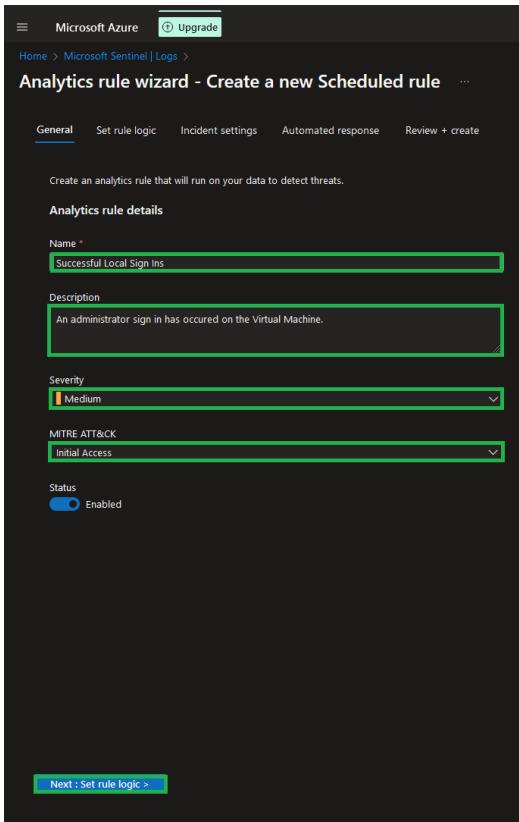
```
1 SecurityEvent  
2 | where Activity contains "success" and Account !contains "system"
```

The results pane below shows a message: "No results found from the last 24 hours. Try selecting another time range".

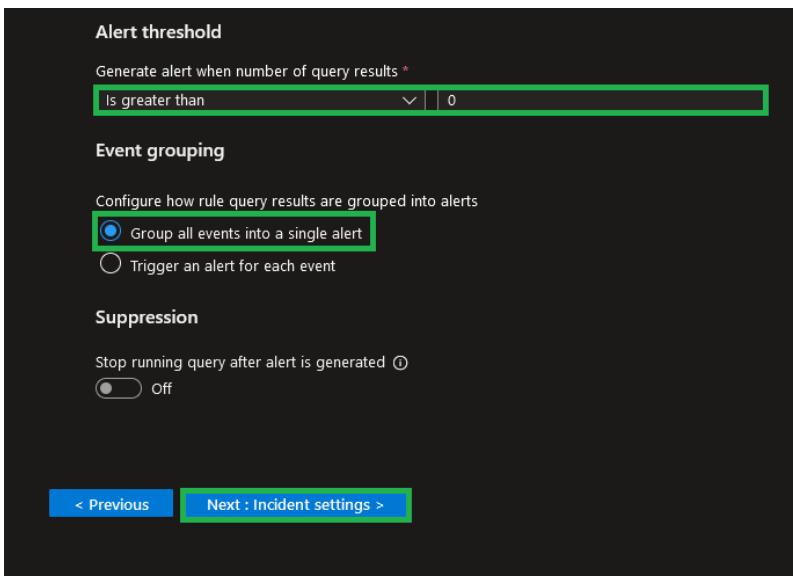
2. We then click on New alert rule and select Create Microsoft Sentinel Alert.

The screenshot shows the same Microsoft Sentinel Logs interface as before, but with a focus on the 'New alert rule' dropdown menu. This menu has two options: 'Create Azure Monitor alert' and 'Create Microsoft Sentinel alert'. The 'Create Microsoft Sentinel alert' option is highlighted with a green box.

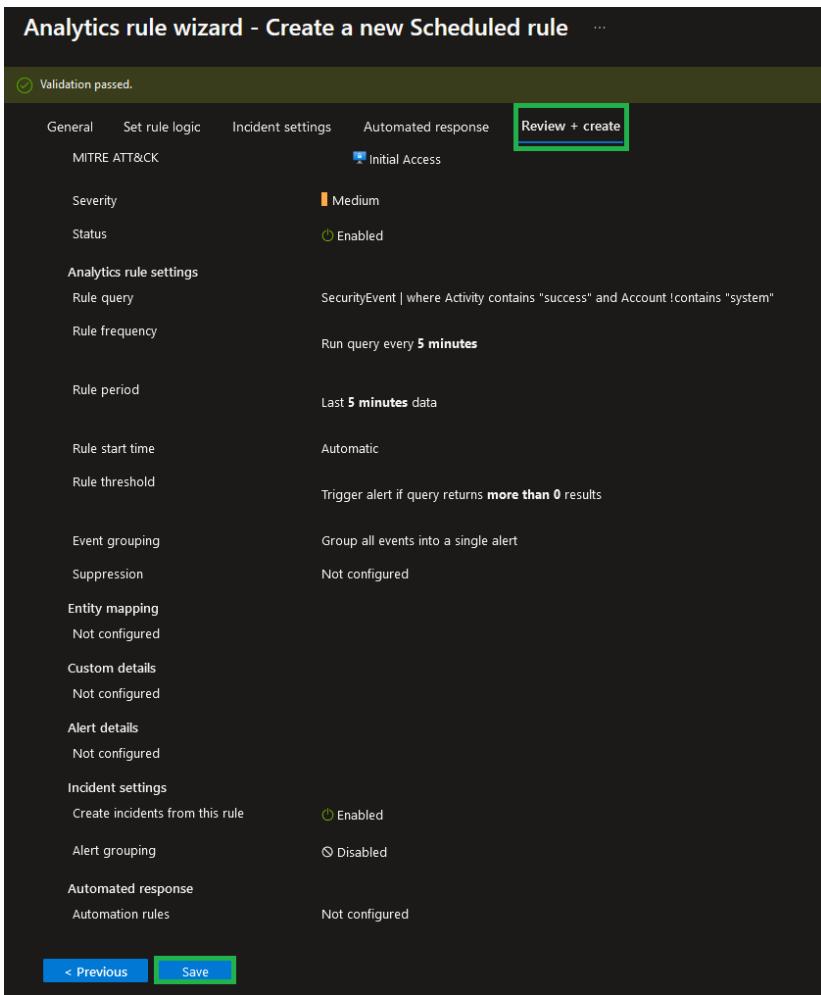
3. The General tab of the Create a new Scheduled rule page, we name our rule, choose the severity level of the event, and select Initial Access under MITRE ATT&CK. We then move on to the Set rule logic tab.



4. There, we set the **Alert threshold** to **Is greater than 0**, select the **Group all events into a single alert** radio button under **Event grouping**, and click on **Next: Incident settings**.



5. We leave the defaults on the **Incident settings** tab and the **Automated response** tab and go to the **Review + create** tab where we click on **Save**.



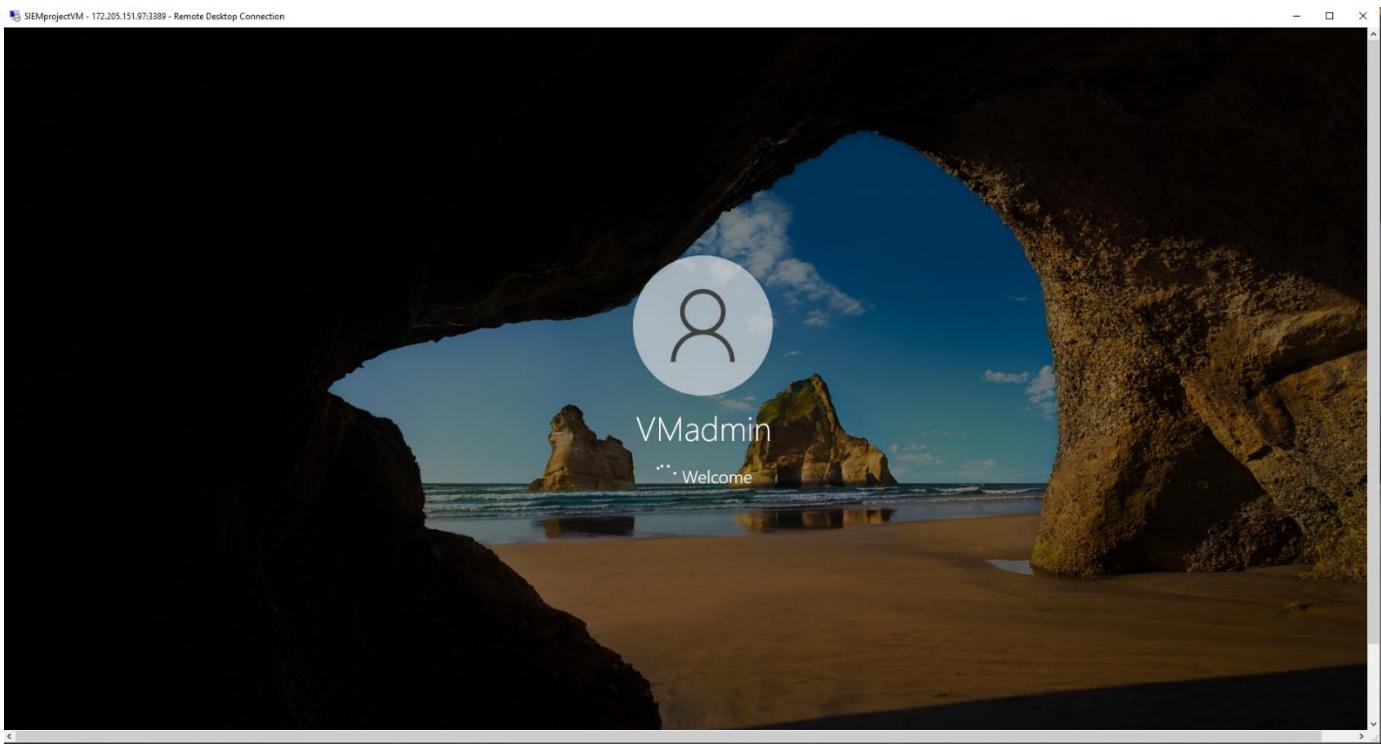
6. If we go back to the **Microsoft Sentinel** page and select **Analytics** under the *Configuration* blade, we can now see our newly created alert rule on the **Active rules** tab. Logging into our VM via RDP should trigger it.

| Severity | Name | Status | Tactics | Techniques | Sub techniques | Source name | Last modified |
|----------|---------------------------|---------|----------------|------------|----------------|-----------------|-------------------|
| Medium | Successful Local Logon | Enabled | Initial Access | | | Custom Content | 22/10/2024, 21:15 |
| High | Advanced Multi-step Logon | Enabled | Collection +11 | | | Gallery Content | 22/10/2024, 18:15 |

7. To test it, we go to our VM's page, go into the select **Connect** under the *Connect* blade, and click on **Download RDP file**.

The screenshot shows the Azure portal interface for a virtual machine named 'SIEMprojectVM'. The left sidebar lists various management options like 'Create', 'Switch to classic', and 'Connect'. Under 'Connect', the 'Native RDP' option is selected, indicated by a blue bar. This section displays the public IP address (172.205.151.97) and port (3389). Below this, there are buttons for 'Select' and 'Download RDP file', with the 'Download RDP file' button highlighted in green. Other connection methods listed include 'Bastion', 'Windows Admin Center', and 'More ways to connect (4)'.

8. We log in to the VM with our credentials.



9. We then go the **Incidents** (or **Overview**) page of Microsoft Sentinel to view our generated alert. It should look like this:

| Severity | Incident number | Title | Alerts | Incident provider n... | Alert product name |
|----------|-----------------|-------------------------|--------|------------------------|--------------------|
| Medium | 2 | Successful Local Sig... | 1 | Azure Sentinel | Microsoft Sentinel |
| Medium | 1 | Successful Local Sig... | 1 | Azure Sentinel | Microsoft Sentinel |

We can now use this VM as an RDP honeypot.

Azure security project solution PART 2: *Creating a threat intelligence feed using MISP*

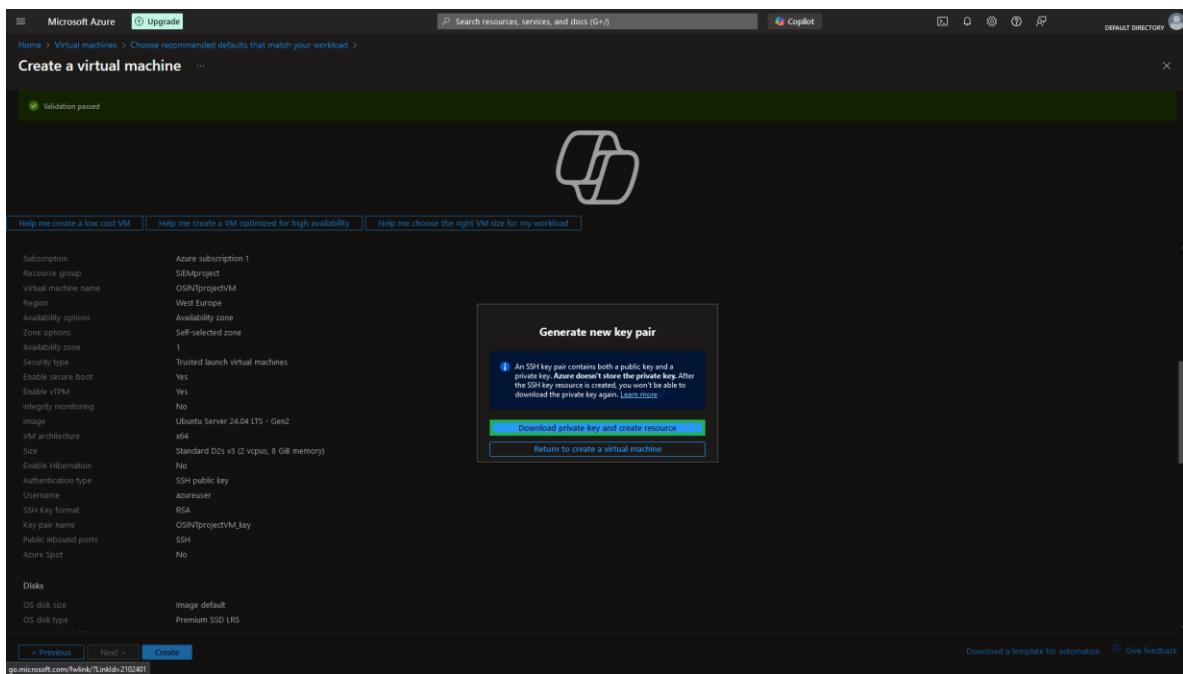
We will now setup a custom OSINT data feed to our Sentinel instance. Microsoft does have its own threat intelligence instance, but for this project we will be using the MISP open-source threat intelligence platform.

Task 5: Creating an Ubuntu server VM and setting up Docker

1. We begin by creating another preset virtual machine with these specifications. The rest can be leave at their default values.

| Field | Value |
|----------------------|---|
| Subscription | Our current subscription. |
| Resource group | SIEMproject |
| Virtual machine name | Enter a unique VM name, such as OSINTprojectVM . |
| Region | Select the same region as previous resources |
| Availability options | Select Availability zone . |
| Availability zone | Select Zones 1 . |
| Image | Select Ubuntu Server 24.04 LTS - x64 Gen2 |
| Size | Select Standard_D2s_v3 - 2 vcpus, 8GiB memory |

2. We then click on **Download private key and create resource** when prompted.



3. We then click on **Go to resource**, navigate to the **Connect** page, and click **Select** under the SSH using Azure CLI connection method.

4. We then tick the checkbox beside “**I understand just-in-time policy on the virtual machine may be re-configured...**” in the wizard to continue.

5. When the shell opens, we will be prompted to confirm we would like to continue connecting and input “yes”.

```
sibil [ ~ ]$ az ssh vm --resource-group SIEMproject --vm-name OSINTprojectVM --subscription 1c231d77-b506-4287-925c-aba83bffa6fb
OpenSSH_8.9p1, OpenSSL 1.1.1k FIPS 25 Mar 2021
The authenticity of host '4.245.4.197 (4.245.4.197)' can't be established.
ED25519 key fingerprint is SHA256:jVtIc3//XLoIWNohbVV8Uoce5xhNQjIPAsJ/kDhUs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

- We now go to the webpage docs.docker.com/engine/install/ubuntu/, scroll down to the **Install using the apt repository** section and follow the steps there.

Ubuntu

Install using the apt repository

Before you install Docker Engine for the first time on a new host machine, you need to set up the Docker repository. Afterward, you can install and update Docker from the repository.

- Set up Docker's apt repository.


```
# Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc

# Add the repository to Apt sources:
echo 'deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu $(/etc/os-release && echo "$VERSION_CODENAME") stable' | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```
- Install the Docker packages.

Latest Specific version

To install the latest version, run:

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

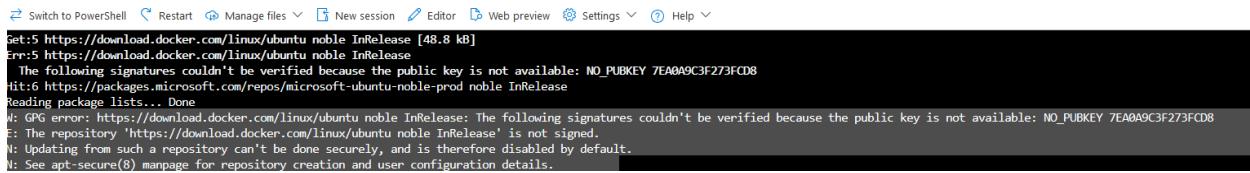
- We first add Docker's official GPG key:

```
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
```

- We then add the repository to apt sources:

```
echo |
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/ubuntu |
$(/etc/os-release && echo "$VERSION_CODENAME") stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

Note: in my case here I got the following error:



```
Switch to PowerShell  Restart  Manage files  New session  Editor  Web preview  Settings  Help
Get:5 https://download.docker.com/linux/ubuntu noble InRelease [48.8 kB]
Err:5 https://download.docker.com/linux/ubuntu noble InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7EA0A9C3F273FCDB
Hit:6 https://packages.microsoft.com/repos/microsoft-ubuntu-noble-prod noble InRelease
Reading package lists... Done
W: GPG error: https://download.docker.com/linux/ubuntu noble InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7EA0A9C3F273FCDB
E: The repository 'https://download.docker.com/linux/ubuntu noble InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
```

I fixed this in the following way:

- I. Update the GPG Key for Docker's Repository:** We need to download and add the correct public key for the Docker repository manually. We run the following commands:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
```

This command fetches the GPG key and stores it in /usr/share/keyrings/docker-archive-keyring.gpg.

- II. Update the Docker Repository List:** Now that we have the key, we update the Docker repository entry to use the GPG key we just added. We create or update the following repository file:

```
echo \
```

```
"deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]
https://download.docker.com/linux/ubuntu \
```

```
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

This ensures that the correct key is used when installing Docker.

- III. Update Package Index and Install Docker:** Now, we update our package list and install Docker:

```
sudo apt-get update
```

```
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

9. We can now continue with our installation of the docker packages:

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

Note: input Y



```
$ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  docker-ce-rootless-extras libltdl7 libslirp0 pigz slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-buildx-plugin docker-ce docker-ce-cli docker-ce-rootless-extras docker-compose-plugin libltdl7 libslirp0 pigz slirp4netns
0 upgraded, 10 newly installed, 0 to remove and 1 not upgraded.
Need to get 123 MB of archives.
After this operation, 442 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

10. If no errors are present, the response should look like this:

```
Running kernel seems to be up-to-date.  
No services need to be restarted.  
No containers need to be restarted.  
No user sessions are running outdated binaries.  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
$ █
```

11. We now run the hello-world image to verify that the installation is successful:

```
sudo docker run hello-world
```

```
$ sudo docker run hello-world  
Unable to find image 'hello-world:latest' locally  
latest: Pulling from library/hello-world  
c1ec31eb5944: Pull complete  
Digest: sha256:d211f485f2dd1dee407a80973c8f129f00d54604d2c90732e8e320e5038a0348  
Status: Downloaded newer image for hello-world:latest  
  
Hello from Docker!  
This message shows that your installation appears to be working correctly.  
  
To generate this message, Docker took the following steps:  
1. The Docker client contacted the Docker daemon.  
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.  
   (amd64)  
3. The Docker daemon created a new container from that image which runs the  
   executable that produces the output you are currently reading.  
4. The Docker daemon streamed that output to the Docker client, which sent it  
   to your terminal.  
  
To try something more ambitious, you can run an Ubuntu container with:  
$ docker run -it ubuntu bash  
  
Share images, automate workflows, and more with a free Docker ID:  
https://hub.docker.com/  
  
For more examples and ideas, visit:  
https://docs.docker.com/get-started/  
$ █
```

Task 6: Setting up MISP

1. We can now get the MISP docker image from this URL: github.com/MISP/misp-docker:

```
git clone https://github.com/MISP/misp-docker
```

```
$ git clone https://github.com/MISP/misp-docker  
Cloning into 'misp-docker'...  
remote: Enumerating objects: 2080, done.  
remote: Counting objects: 100% (467/467), done.  
remote: Compressing objects: 100% (159/159), done.  
remote: Total 2080 (delta 409), reused 327 (delta 305), pack-reused 1613 (from 1)  
Receiving objects: 100% (2080/2080), 454.23 KiB | 8.26 MiB/s, done.  
Resolving deltas: 100% (1121/1121), done.  
$ █
```

2. We can check whether the image is in the directory by typing *dir*.

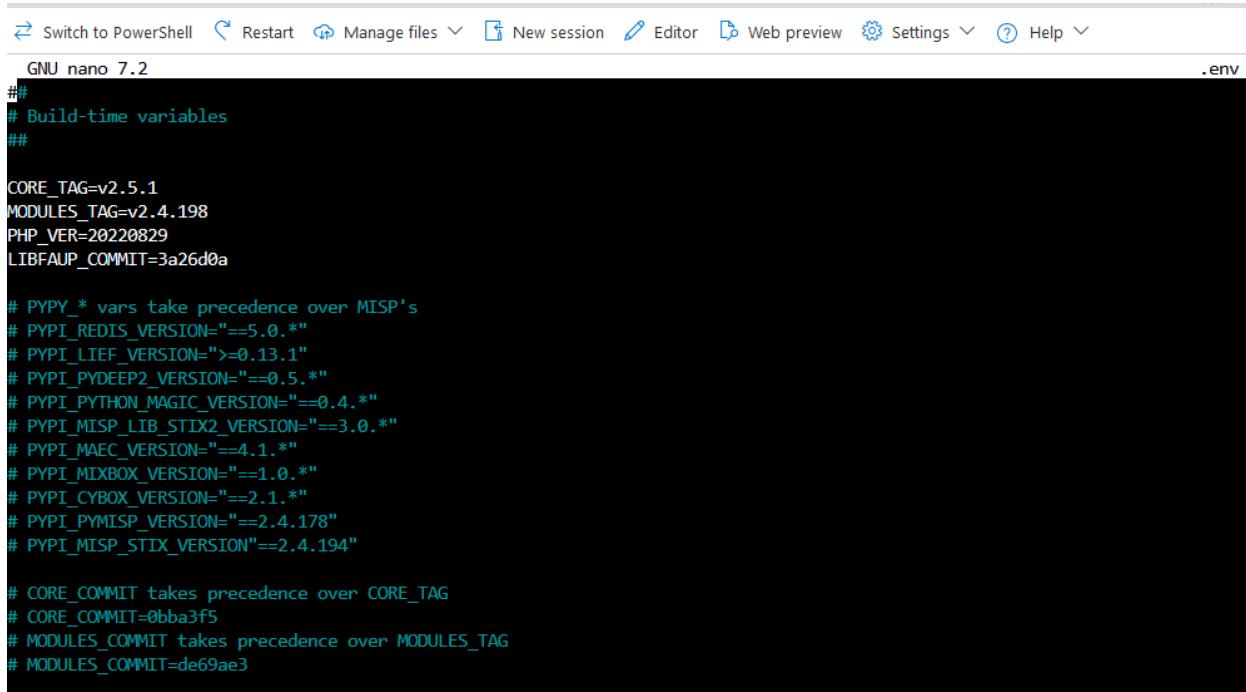
```
$ dir  
misp-docker  
$
```

3. The next step is to navigate to the misp-docker directory using the *cd* command.
4. We then use the *dir* command once more to confirm we changed directories.
5. And finally we copy the *template.env* file with the following command to create a new *.env* file:

```
cp template.env .env
```

```
$ cd misp-docker  
$ dir  
LICENSE README.md core docker-bake.hcl docker-compose.yml experimental modules template.env  
$ cp template.env .env  
$
```

6. We have to now edit the new file using nano by typing in *nano .env* which should open up the editing software.



```
GNU nano 7.2 .env  
##  
# Build-time variables  
##  
  
CORE_TAG=v2.5.1  
MODULES_TAG=v2.4.198  
PHP_VER=20220829  
LIBFAUP_COMMIT=3a26d0a  
  
# Pypy_* vars take precedence over MISP's  
# PYPI_REDIS_VERSION=="5.0.*"  
# PYPI_LIEF_VERSION">=0.13.1"  
# PYPI_PYDEEP2_VERSION=="0.5.*"  
# PYPI_PYTHON_MAGIC_VERSION=="0.4.*"  
# PYPI_MISP_LIB_STIX2_VERSION=="3.0.*"  
# PYPI_MAEC_VERSION=="4.1.*"  
# PYPI_MIXBOX_VERSION=="1.0.*"  
# PYPI_CYBOX_VERSION=="2.1.*"  
# PYPI_PYMISP_VERSION=="2.4.178"  
# PYPI_MISP_STIX_VERSION=="2.4.194"  
  
# CORE_COMMIT takes precedence over CORE_TAG  
# CORE_COMMIT=0bba3f5  
# MODULES_COMMIT takes precedence over MODULES_TAG  
# MODULES_COMMIT=de69ae3
```

7. We scroll down to *BASE_URL* and input our VM's public IP address.

GNU nano 7.2 .env *

```
# Email/username for user #1, defaults to MISP's default (admin@admin.test)
ADMIN_EMAIL=
# name of org #1, default to MISP's default (ORGNAME)
ADMIN_ORG=
# defaults to an automatically generated one
ADMIN_KEY=
# defaults to MISP's default (admin)
ADMIN_PASSWORD=
# defaults to 'passphrase'
GPG_PASSPHRASE=
# defaults to 1 (the admin user)
CRON_USER_ID=
# defaults to 'https://localhost'
BASE_URL=https://4.245.4.197
# store settings in db except those that must stay in config.php. true/false, defaults to false
ENABLE_DB_SETTINGS=
# encryption key. defaults to empty string
ENCRYPTION_KEY=
# enable background updates. defaults to false
ENABLE_BACKGROUND_UPDATES=

# defines the FQDN of the mail sub-system (defaults to 'mail')
# SMTP_FQDN=
```

8. We then input **Ctrl+X** to Exit and will be prompted to save our changes. We confirm with **Y** and then Press **Enter** on the *File name to Write: .env* prompt.
9. The next step is to input *sudo docker compose pull* if to use pre-built images. Once completed, it should look like this:

Switch to PowerShell Restart Manage files New session Editor Web preview Settings Help

```
[root@4.245.4.197 ~]# sudo docker compose pull
[+] Pulling redis (misp-redis:latest)...
redis: Pulling from misp-redis
latest: Downloading [progress] 0B / 62.5M
redis: 62.5M / 62.5M (100%) 97.0s
[+] Pulling misp-modules (misp-modules:latest)...
misp-modules: Pulling from misp-modules
latest: Downloading [progress] 0B / 39.2M
misp-modules: 39.2M / 39.2M (100%) 62.4s
[+] Pulling db (misp-db:latest)...
db: Pulling from misp-db
latest: Downloading [progress] 0B / 121.1M
db: 121.1M / 121.1M (100%) 121.1s
```

10. We then run the command *sudo docker compose up* to spin up the docker container. Successful completion should end with *INIT / Done...*

```
misp-core-1 | MISP | Set Up AAD ...
misp-core-1 | ... Entra (AzureAD) authentication disabled
misp-core-1 | MISP | Set Up Session ...
misp-core-1 | ... Session configured
misp-core-1 | MISP | Set Up Proxy ...
misp-core-1 | ... Proxy disabled
misp-core-1 | MISP | Mark instance live
misp-core-1 | Set live status to True in Redis.
misp-core-1 | Set live status in PHP config file.
misp-core-1 | MISP is now live. Users can now log in.
INIT | Configure PHP ...
2024-10-23 14:08:35,229 INFO waiting for php-fpm to stop
misp-core-1 | Entrypoint FPM caught SIGTERM signal!
misp-core-1 | Killing process 38
2024-10-23 14:08:35,230 WARN stopped: php-fpm (exit status 143)
2024-10-23 14:08:35,240 INFO spawned: 'php-fpm' with pid 3679
misp-core-1 | Configure PHP | Change PHP values ...
misp-core-1 | Configure PHP | Setting 'memory_limit = 2048M'
misp-core-1 | Configure PHP | Setting 'max_execution_time = 300'
misp-core-1 | Configure PHP | Setting 'upload_max_filesize = 50M'
misp-core-1 | Configure PHP | Setting 'post_max_size = 50M'
misp-core-1 | Configure PHP | Setting 'max_input_time = 300'
misp-core-1 | Configure PHP | Setting 'session.save_path = 'tcp://redis:6379?auth=redispASSWORD'
misp-core-1 | Configure PHP | Starting PHP FPM
2024-10-23 14:08:36,306 INFO success: php-fpm entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
misp-core-1 | php-fpm: stopped
misp-core-1 | php-fpm: started
misp-core-1 | INIT | Done ...
```

Note: Ctrl+Z might be necessary to exit the process after *INIT / Done...* is displayed.

11. To make sure that everything succeeded we can check the status of the container with *sudo docker ps*.

```
*[1] + Stopped      sudo docker compose up
$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
ee7741bd7dbc        ghcrl.io/misp/misp-docker/misp-core:latest   "/entrypoint.sh"    7 minutes ago     Up 7 minutes (unhealthy)   0.0.0.0:80->80/tcp, ::1:80->80/tcp, 0.0.0.0:443->443/tcp, ::1:443->443/tcp   misp-docker-misp-core-1
1d702851dfcc        ghcrl.io/misp/misp-docker/misp-modules:latest  "/usr/local/bin/misp_...
e2e7c9d1212e        ixodtai/smtp                                "/bin/entrypoint.sh..." 7 minutes ago     Up 7 minutes          25/tcp               misp-docker-misp-modules-1
d49d1a47436a        valkey/valkey:7.2                            "/docker-entrypoint.s...
6d759207fd77        mariadb:10.11                               "/docker-entrypoint.s... 7 minutes ago     Up 7 minutes (healthy)   6379/tcp            misp-docker-mail-1
                                         3306/tcp            misp-docker-redis-1
                                         3306/tcp            misp-docker-db-1
$
```

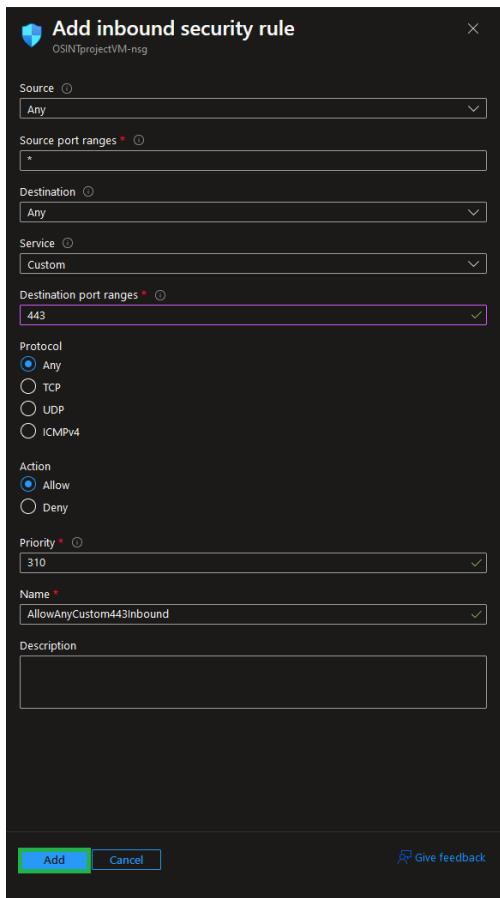
12. We now go the **Network settings** page under the *Networking* blade of the Ubuntu VM. We need to create an inbound port rule for Port 443.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'OSINTProjectVM'. The 'Networking' blade is active. In the 'Inbound port rules' section, a new rule is being added. The 'Create port rule' dropdown menu is open, with 'Inbound port rule' selected. The table below lists four existing inbound port rules, each with columns for Port, Protocol, Source, Destination, and Action. The new rule will be added below these.

| Port | Protocol | Source | Destination | Action |
|-------|----------|-------------------|----------------|--------|
| 300 | TCP | Any | Any | Allow |
| 65000 | TCP | Any | VirtualNetwork | Allow |
| 65001 | TCP | AzureLoadBalancer | Any | Allow |
| 65500 | TCP | Any | Any | Deny |

```
*[1] + Stopped      sudo docker compose up
$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS               NAMES
ee7741bd7dbc        ghcrl.io/misp/misp-docker/misp-core:latest   "/entrypoint.sh"    7 minutes ago     Up 7 minutes (unhealthy)   0.0.0.0:80->80/tcp, ::1:80->80/tcp, 0.0.0.0:443->443/tcp, ::1:443->443/tcp   misp-docker-misp-core-1
1d702851dfcc        ghcrl.io/misp/misp-docker/misp-modules:latest  "/usr/local/bin/misp_...
e2e7c9d1212e        ixodtai/smtp                                "/bin/entrypoint.sh..." 7 minutes ago     Up 7 minutes          25/tcp               misp-docker-misp-modules-1
d49d1a47436a        valkey/valkey:7.2                            "/docker-entrypoint.s...
6d759207fd77        mariadb:10.11                               "/docker-entrypoint.s... 7 minutes ago     Up 7 minutes (healthy)   6379/tcp            misp-docker-mail-1
                                         3306/tcp            misp-docker-redis-1
                                         3306/tcp            misp-docker-db-1
$
```

13. We input the following configuration and select **Add**:



14. We then paste our VM's public IP address into a browser and bypass the warning that the page is unsafe (we need to add a signed certificate to fix this).

Note: this should now work for any VM we have, such as the honeypot VM from PART 1.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **4.245.4.197**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

4.245.4.197 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

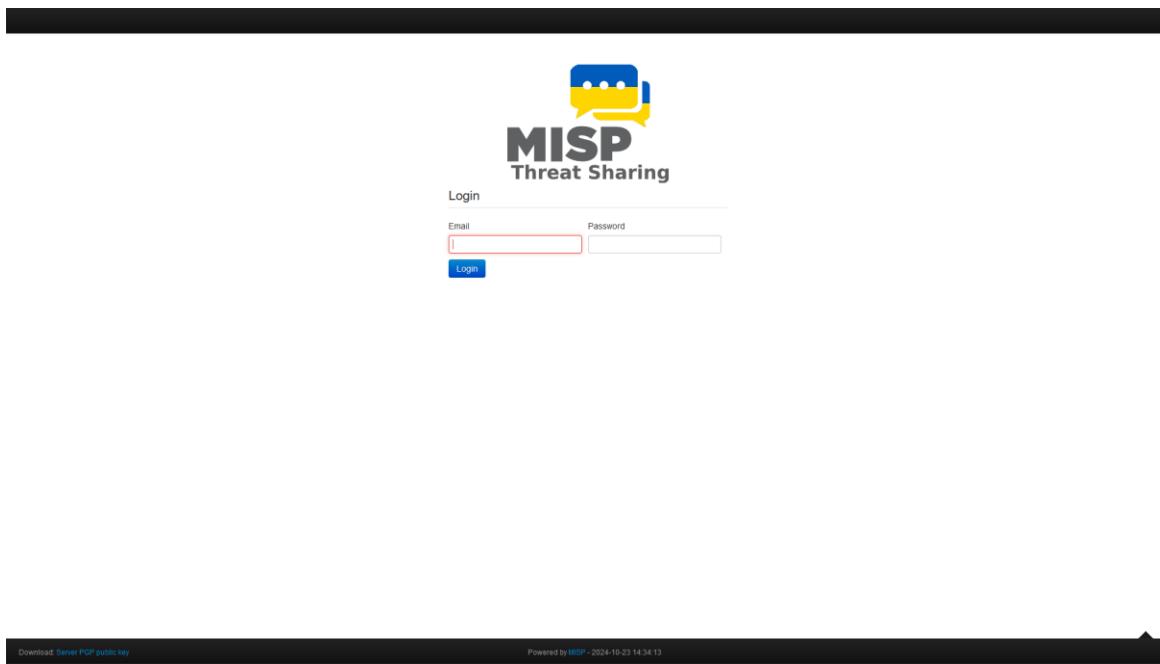
Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

[View Certificate](#)

[Go Back \(Recommended\)](#)

[Accept the Risk and Continue](#)

15. The MISP instance is now running.



16. We log in using the following credentials:

- User: admin@admin.test
- Password: admin

17. Now we should have access to our MISP Instance.

18. Since this is a public-facing server, it is highly recommended to change our admin password. This is done by clickin on **Admin** at the top-right, then going to **Change Password** and selecting new password.

19. We now have to enable the OSINT feeds. To do this, we first go to www.misp-project.org/feeds/ or directly from GitHub at <https://github.com/MISP/MISP/blob/2.4/app/files/feed-metadata/defaults.json>.

20. We copy the contents of the JSON file.

```

{
  "default": false,
  "override_ids": false,
  "delete_local_file": false,
  "lookup_visible": false,
  "hide_tag": false,
  "fixed_event": false,
  "delta_merge": false,
  "publish": false,
  "override_ids": false,
  "delete_local_file": false
}

```

21. We then go back to the MISP instance, go to **Synch Actions**, and select **Feeds**.

[Edit My Profile](#)

Change Password

- [My Profile](#)
- [My Settings](#)
- [Periodic summary settings](#)
- [Set Setting](#)
- [List Organisations](#)
- [Role Permissions](#)
- [List Sharing Groups](#)
- [Add Sharing Group](#)
- [List Sharing Group Blueprints](#)
- [Add Sharing Group Blueprint](#)

[Categories & Types](#)

[Terms & Conditions](#)

[Statistics](#)

[Sync Actions](#)
[Remote Servers](#)
Feeds
[SightingDB](#)
[Communities](#)
[Cerebrates](#)
[TAXII Servers](#)
[Event ID translator](#)

22. We go to the **Import Feeds from JSON** menu, paste the code we copied from GitHub and click on **Add**.

[Home](#)
[Event Actions](#)
[Dashboard](#)
[Galaxies](#)
[Input Filters](#)
[Global Actions](#)
[Sync Actions](#)
[Administration](#)
[Logs](#)
[API](#)

[List Feeds](#)

[Search Feed Caches](#)

[Add Feed](#)

Import Feeds from JSON

[Feed overlap analysis matrix](#)

[Export Feed settings](#)

Paste feed data

Paste a MISP feed metadata JSON below to add feeds.

JSON

```
[{"Feed": {"name": "ELLIO: IP Feed (Community version)", "provider": "ellio.tech", "url": "https://cdn.ellio.tech/community-feed", "rules": "[\"tags\":[\"OR\":[], \"NOT\[]], \"orgs\":[\"OR\":[], \"NOT\[]]}", "enabled": true, "distribution": "0", "default": false, "source_format": "freetext", "fixed_event": true, "delta_merge": true, "publish": true, "override_ids": false, "settings": {"\"csv\": {\"value\": \"\", \"delimiter\": \",\", \"common\": [\"excluderegex\"]}}}
```

Add

23. We now need to enable them, which is done by selecting the checkbox next to **ID** on the Feeds page that we will be automatically redirected to and clicking on **Enable selected**. We have to do this for all 5 pages individually.

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks ★ MISP Admin Log out

82 new feeds added.

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Load default feed metadata Cache all feeds Cache freezed/CSV feeds Cache MISP feeds Fetch and store all feed data

| ID | Enabled | Caching | Name | Format | Provider | Org | Source | URL | Headers | Target | Publish | Delta | Override | Distrib |
|----|-------------------------------------|---------|---|----------|--|---------|---|-----|------------------|--------|---------|-------|----------|---------|
| 1 | <input checked="" type="checkbox"/> | x | CIRCL OSINT Feed | misp | CIRCL | network | https://www.circl.lu/doc/misp/feed-osint | | Feed not enabled | x | x | x | All com | |
| 2 | <input checked="" type="checkbox"/> | x | The Botrij.eu Data | misp | Botrij.eu | network | https://www.botrij.eu/datafeed-osint | | Feed not enabled | x | x | x | All com | |
| 3 | <input checked="" type="checkbox"/> | x | ELIO: IP Feed (Community version) | freetext | elliot.tech | network | https://cdn.elliot.tech/community-feed | | Feed not enabled | ✓ | ✓ | x | Your org | |
| 4 | <input checked="" type="checkbox"/> | x | blockrules of rules.emergingthreats.net | csv | rules.emergingthreats.net | network | https://rules.emergingthreats.net/blockrules/compromised-ips.txt | | Feed not enabled | x | ✓ | x | Your org | |
| 5 | <input checked="" type="checkbox"/> | x | Tor exit nodes | csv | TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL nodes" feed. | network | https://www.dan.me.uk/torlist/?exit | | Feed not enabled | x | ✓ | x | Your org | |
| 6 | <input checked="" type="checkbox"/> | x | Tor ALL nodes | csv | TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed. | network | https://www.dan.me.uk/torlist/ | | Feed not enabled | x | ✓ | x | Your org | |
| 7 | <input checked="" type="checkbox"/> | x | cybercrime-tracker.net - all | freetext | cybercrime-tracker.net | network | https://cybercrime-tracker.net/all.php | | Feed not enabled | x | ✓ | x | Your org | |
| 8 | <input checked="" type="checkbox"/> | x | Phishank online valid phishing | csv | Phishank | network | https://data.phishank.com/data/online-valid.csv | | Feed not enabled | x | ✓ | x | Your org | |
| 9 | <input checked="" type="checkbox"/> | x | ip-block-list - snort.org | freetext | https://snort.org | network | https://snort.org/downloads/ip-block-list | | Feed not enabled | ✓ | ✓ | x | Your org | |
| 10 | <input checked="" type="checkbox"/> | x | diamondfor_panels | freetext | pan-unit42 | network | https://githubusercontent.com/pan-unit42/ocs/master/diamondfor_panels.txt | | Feed not enabled | ✓ | ✓ | x | Your org | |
| 11 | <input checked="" type="checkbox"/> | x | pop3/gropers | csv | home.nusig.no | network | https://home.nusig.no/~petef/pop3/gropers.txt | | Feed not enabled | ✓ | ✓ | x | Your org | |
| 12 | <input checked="" type="checkbox"/> | x | Feodo IP Blocklist | csv | abuse.ch | network | https://feodotracker.abuse.ch/downloads/ipblocklist.csv | | Feed not enabled | x | x | x | Your org | |
| 13 | <input checked="" type="checkbox"/> | x | OpenPhish url list | freetext | openphish.com | network | https://openphish.com/feed.txt | | Feed not enabled | x | ✓ | x | Your org | |

Download: Server PGP public key

Powered by MISP 2.5.1 - 2024-10-23 15:02:55

24. All feeds should now have checkmarks. We then click on **Fetch and store all feed data**.

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks ★ MISP Admin Log out

4 feeds enabled.

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Load default feed metadata Cache all feeds Cache freezed/CSV feeds Cache MISP feeds Fetch and store all feed data

| ID | Enabled | Caching | Name | Format | Provider | Org | Source | URL | Headers | Target | Publish | Delta | Override | Distrib |
|----|-------------------------------------|---------|---|----------|--|---------|---|-----|----------------|--------|---------|-------|----------|---------|
| 1 | <input checked="" type="checkbox"/> | x | CIRCL OSINT Feed | misp | CIRCL | network | https://www.circl.lu/doc/misp/feed-osint | | x | x | x | | All comm | |
| 2 | <input checked="" type="checkbox"/> | x | The Botrij.eu Data | misp | Botrij.eu | network | https://www.botrij.eu/datafeed-osint | | x | x | x | | All comm | |
| 3 | <input checked="" type="checkbox"/> | x | ELIO: IP Feed (Community version) | freetext | elliot.tech | network | https://cdn.elliot.tech/community-feed | | New feed event | ✓ | ✓ | x | Your org | |
| 4 | <input checked="" type="checkbox"/> | x | blockrules of rules.emergingthreats.net | csv | rules.emergingthreats.net | network | https://rules.emergingthreats.net/blockrules/compromised-ips.txt | | New feed event | x | ✓ | x | Your org | |
| 5 | <input checked="" type="checkbox"/> | x | Tor exit nodes | csv | TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL nodes" feed. | network | https://www.dan.me.uk/torlist/?exit | | New feed event | x | ✓ | x | Your org | |
| 6 | <input checked="" type="checkbox"/> | x | Tor ALL nodes | csv | TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed. | network | https://www.dan.me.uk/torlist/ | | New feed event | x | ✓ | x | Your org | |
| 7 | <input checked="" type="checkbox"/> | x | cybercrime-tracker.net - all | freetext | cybercrime-tracker.net | network | https://cybercrime-tracker.net/all.php | | New feed event | x | ✓ | x | Your org | |
| 8 | <input checked="" type="checkbox"/> | x | Phishank online valid phishing | csv | Phishank | network | https://data.phishank.com/data/online-valid.csv | | New feed event | x | ✓ | x | Your org | |
| 9 | <input checked="" type="checkbox"/> | x | ip-block-list - snort.org | freetext | https://snort.org | network | https://snort.org/downloads/ip-block-list | | New feed event | ✓ | ✓ | x | Your org | |
| 10 | <input checked="" type="checkbox"/> | x | diamondfor_panels | freetext | pan-unit42 | network | https://githubusercontent.com/pan-unit42/ocs/master/diamondfor_panels.txt | | New feed event | ✓ | ✓ | x | Your org | |
| 11 | <input checked="" type="checkbox"/> | x | pop3/gropers | csv | home.nusig.no | network | https://home.nusig.no/~petef/pop3/gropers.txt | | New feed event | ✓ | ✓ | x | Your org | |
| 12 | <input checked="" type="checkbox"/> | x | Feodo IP Blocklist | csv | abuse.ch | network | https://feodotracker.abuse.ch/downloads/ipblocklist.csv | | New feed event | x | x | x | Your org | |
| 13 | <input checked="" type="checkbox"/> | x | OpenPhish url list | freetext | openphish.com | network | https://openphish.com/feed.txt | | New feed event | x | ✓ | x | Your org | |

Download: Server PGP public key

Powered by MISP 2.5.1 - 2024-10-23 15:08:29

<https://4.245.4.197/feeds/fetchFromAllFeeds>

Note: Synch status of the new feeds can be checked by hovering over the **Administration** and selecting **Jobs**.

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks ★ MISP Admin Log out

Add User List Users Pending registrations User settings Set Setting Contact Users

Add Organisation List Organisations

Add Role List Roles

Server Settings & Maintenance Update Progress

Jobs

Purge job entries: Completed All

| ID | Date created | Date modified | Process ID | Worker | Job type | Input | Message | Organisation name | Status | Progress |
|----|---------------------|---------------------|--------------------------------------|---------|---------------------|----------|---------------------------|-------------------|-----------|-----------|
| 85 | 2024-10-23 15:12:53 | 2024-10-23 15:12:54 | 6f5af7a-1c72-4975-920c-90e52302dc6e | email | publish_alert_email | Event: 1 | Mails sent. | ADMIN | Completed | Completed |
| 84 | 2024-10-23 15:12:53 | 2024-10-23 15:12:53 | 66ca2434-4873-480e-a9cd-1fb852e37449 | default | fetch_feed | Feed: 84 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 83 | 2024-10-23 15:12:53 | 2024-10-23 15:12:53 | 16093d9d-bf5a-432e-5aa2-91af437910 | default | fetch_feed | Feed: 83 | Starting fetch from Feed | ADMIN | Waiting | Waiting |
| 82 | 2024-10-23 15:12:53 | 2024-10-23 15:12:53 | 316e50ec-45c1-4879-8685-5e6e6044d70f | default | fetch_feed | Feed: 82 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 81 | 2024-10-23 15:12:53 | 2024-10-23 15:12:53 | 5daea909-6468-455e-b31c-04334809a1ad | default | fetch_feed | Feed: 81 | Starting fetch from Feed | ADMIN | Waiting | Waiting |
| 80 | 2024-10-23 15:12:53 | 2024-10-23 15:12:53 | 823ab9b0-a1e7-4200-8a84-040fb7935320 | default | fetch_feed | Feed: 80 | Starting fetch from Feed | ADMIN | Waiting | Waiting |
| 79 | 2024-10-23 15:12:53 | 2024-10-23 15:12:53 | a363634-3679-403-8f86-b5383e4a9202 | default | fetch_feed | Feed: 79 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 78 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | e91aa9e9-78e3-45f5-8eb-7edbf5aeed123 | default | fetch_feed | Feed: 78 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 77 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | c459156-4005-4e47-487702498598 | default | fetch_feed | Feed: 77 | Starting fetch from Feed | ADMIN | Waiting | Waiting |
| 76 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | c0a85eeb-309f-4086-aad-99931385e6fb | default | fetch_feed | Feed: 76 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 75 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | 15502de4-620e-424b-983a-983a7effceca | default | fetch_feed | Feed: 75 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 74 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | 020e8a0e-3e27-4a0d-841a-3c785d5d0e00 | default | fetch_feed | Feed: 74 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 73 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | ddcc3b12-e894-422e-8845-8d050987bd77 | default | fetch_feed | Feed: 73 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 72 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | 0221ecb2-104e-4dd9-bca7-82947ab5351 | default | fetch_feed | Feed: 72 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 71 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | b349095-2685-4885-8111-4146ca9c939 | default | fetch_feed | Feed: 71 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 70 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | f094d998-9919-4199-9305-188dbd999559 | default | fetch_feed | Feed: 70 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 69 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | dc584db-3805-4c98-99fa-1bc1281d073e | default | fetch_feed | Feed: 69 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 68 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | fa7611b8-3347-4321-42d0-ecfd8e6b023 | default | fetch_feed | Feed: 68 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 67 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | 8764e18d-4302-8447-a113-9787b2054c1 | default | fetch_feed | Feed: 67 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |
| 66 | 2024-10-23 15:12:52 | 2024-10-23 15:12:52 | ad22e161-4193-b293-d95957d036c8 | default | fetch_feed | Feed: 66 | Starting fetch from Feed. | ADMIN | Waiting | Waiting |

Page 1 of 5, showing 20 records out of 85 total, starting on record 1, ending on 20

« previous 1 2 3 4 5 next »

Download Server PGP public key

Powered by MISP 2.5.1 - 2024-10-23 15:13:02

25. We can also see how our **Home** page is now being populated by feeds. We can click on the ID of any of them to see more detailed information such as indicators etc.

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks ★ MISP Admin Log out

Events

My Events Org Events □

| ID | Creator org | Owner org | Custers | Tags | #Att. | #Corr. | Creator user | Date | Info | Enter value to search | Event info | Filter |
|-------|-------------|-----------|---------|-----------|-------|--------|------------------|------------|---|-----------------------|--------------|--------|
| 7 117 | | | | | 1 | 3 | admin@admin.test | 2024-10-23 | Feed: IP Blocklist feed | | Organisation | Filter |
| 7 3 | | | | | 9976 | 2 | admin@admin.test | 2024-10-23 | ELIO: IP Feed (Community version) feed | | Organisation | Filter |
| 7 68 | | | | | 5600 | 2 | admin@admin.test | 2024-10-23 | pg3gropers feed | | Organisation | Filter |
| 7 36 | | | | | 1731 | 2 | admin@admin.test | 2024-10-23 | diamondfox_panels feed | | Organisation | Filter |
| 7 33 | | | | | 2 | 2 | admin@admin.test | 2024-10-23 | ip-block-lst - snort.org feed | | Organisation | Filter |
| 7 2 | | | | | 2119 | 4 | admin@admin.test | 2024-10-23 | Tor exit nodes feed | | Organisation | Filter |
| 7 7 | | | | | 8700 | 4 | admin@admin.test | 2024-10-23 | Tor ALL nodes feed | | Organisation | Filter |
| 7 4 | | | | | 604 | 1 | admin@admin.test | 2024-10-23 | blotches of rules.emergingthreats.net feed | | Organisation | Filter |
| 7 21 | CUDESO | | | | 13 | 1 | admin@admin.test | 2015-12-07 | LOWBOW - FireEye | All | Filter | |
| 7 15 | CUDESO | | | | 79 | 1 | admin@admin.test | 2015-09-15 | In Pursuit of Optical Fibers and Trop Intel: Targeted Attack Distributes PlugX in Russia | All | Filter | |
| 7 8 | CUDESO | | | | 8 | 1 | admin@admin.test | 2015-11-16 | WitchCover Exploiting Web Analytics to Ensnare Victims | All | Filter | |
| 7 81 | CUDESO | | | | 16 | 1 | admin@admin.test | 2016-06-14 | New Sofacy Attacks Against US Government Agency | All | Filter | |
| 7 25 | CUDESO | | | Malware Q | 8 | 1 | admin@admin.test | 2021-09-11 | Maldec Cybersecurity in the EU Common Security and Defense Policy | All | Filter | |
| 7 72 | CUDESO | | | | 66 | 1 | admin@admin.test | 2016-04-21 | Looking Into a Cyber-Attack Facilitator in the Netherlands | All | Filter | |
| 7 18 | CUDESO | | | | 36 | 1 | admin@admin.test | 2015-10-16 | Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites - Citizen Lab | All | Filter | |
| 7 20 | CUDESO | | | | 133 | 1 | admin@admin.test | 2015-12-20 | Pacifrat: Seven Years of a South American Threat Actor | All | Filter | |
| 7 122 | CUDESO | | | | 10 | 1 | admin@admin.test | 2017-07-24 | Real News: Fake Flash: Mac OS X Users Targeted | All | Filter | |
| 7 121 | CUDESO | | | | 5 | 1 | admin@admin.test | 2017-07-24 | New KONG! Campaign References North Korean Missile Capabilities | All | Filter | |
| 7 120 | CUDESO | | | | 4 | 1 | admin@admin.test | 2017-06-16 | Following the Trail of BlackTechné™: Cyber Espionage Campaigns | All | Filter | |
| 7 119 | CUDESO | | | | 13 | 1 | admin@admin.test | 2017-06-16 | McAfee Discovers Pinksheepbot Exploiting Infected Machines as Control Servers; Releases Free Tool to Detect, Disable Trojan | All | Filter | |
| 7 118 | CUDESO | | | | 15 | 1 | admin@admin.test | 2017-05-12 | Industroyer: Biggest threat to industrial control systems since Stuxnet | All | Filter | |
| 7 116 | CUDESO | | | | 74 | 1 | admin@admin.test | 2017-05-26 | TroxBot™: A bag of tricks | All | Filter | |

Download Server PGP public key

Powered by MISP 2.5.1 - 2024-10-23 15:15:13

Task 7: Connecting our MISP data feed to Microsoft Sentinel

- We once again go to the **Content Hub** from the **Data connectors** menu in Microsoft Sentinel and download the **MISP2Sentinel** preconfigured data connector and click **Install**.

The screenshot shows the Microsoft Azure Content hub interface. At the top, there are statistics: 367 Solutions, 303 Standalone contents, 1 Installed, and 0 Updates. A search bar at the top right says "Search resources, services, and docs (G+)." Below the stats, a search bar has "MSP" typed into it. To its right are filters for Status (All), Content type (Data connector (359)), Support (All), Provider (All), Category (All), and Content sources (All). On the left, there's a sidebar with "Content title" and a checkbox for "MISP2Sentinel". The main table lists one item: "MISP2Sentinel" by "MISP project" (Community) under "Aeronautics, Finance, Healthcare, Manufa...". The "Content type" column shows "Data connector". To the right of the table is a detailed view for "MISP2Sentinel". It includes sections for "MISP project", "Provider" (Community), "Support" (3.0.0), "Description" (which states "The MISP2Sentinel solution allows you to automatically push threat indicators from MISP to Microsoft Sentinel via the Upload Indicators REST API."), "Data Connectors" (1), and "Category" (Aeronautics, Finance, Healthcare, Manufacturing, Retail, Security - Threat Intelligence, Security - Threat Protection). It also shows "Pricing" (Free). At the bottom right of the detailed view is a blue "Install" button.

Note: We will now be following setup instructions from github.com/cudeyo/misp2sentinel.

2. To use our new connector, we will set up the Upload Indicators API. We begin by registering a new application to our Azure tenant by going to the **App registrations** page using the main search bar and **selecting New registration**.

The screenshot shows the "App registrations" page in the Azure portal. At the top, there's a header with "Home >" and a green box around "App registrations". Below the header is a navigation bar with "New registration" (highlighted in green), "Endpoints", "Troubleshoot", "Refresh", "Download", "Preview features", and "Got feedback?". A note below the navigation bar says: "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but Library (MSAL) and Microsoft Graph. [Learn more](#)". The main content area has tabs: "All applications" (gray), "Owned applications" (blue, highlighted), "Deleted applications", and "Applications from personal account". Below the tabs is a search bar with "Start typing a display name or application (client) ID to filter these ..." and a "Add filters" button. A message at the top says "This account isn't listed as an owner of any applications in this directory." with two buttons: "View all applications in the directory" and "View all applications from personal account".

3. We name our app and click on **Register**.

Home > App registrations >

Register an application

* Name
The user-facing display name for this application (this can be changed later).

MispToSentinelApp

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, [I agree to the Microsoft Platform Policies](#) [View details](#)

[Register](#)

4. We take note of our *Application (client) ID*, *Object ID*, and *Directory (tenant) ID*.

Home > App registrations >

MispToSentinelApp

Search X ⌂ Delete Endpoints Preview features

Overview Quickstart Integration assistant Diagnose and solve problems

Manage Branding & properties Authentication Certificates & secrets

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

| | |
|-------------------------|--|
| Display name | : MispToSentinelApp |
| Application (client) ID | : 94640c5a-036a-49f4-b700-e9e37ab4f196 |
| Object ID | : b31398ff-af0d-4904-bd3d-5122f0ea52b3 |
| Directory (tenant) ID | : 1714a8fd-e656-4185-8c3d-06e3b4b615ba |

Supported account types : [My organization only](#)

5. We then go to the **Certificates & secrets** page under the *Manage* blade, select **New client secret**, name it, and click on **Add**. We can leave the default expiry time.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation options like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Certificates & secrets (which is selected and highlighted with a green box), Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area is titled 'MisToSentinelApp | Certificates & secrets'. It contains a message about credentials and a table for managing client secrets. The table has columns for Description, Expires, Value (which is currently empty), and Secret ID. A 'New client secret' button is visible. A modal window titled 'Add a client secret' is open, showing fields for Description (set to 'ProjectMISP'), Expires (set to 'Recommended: 180 days (6 months)'), and Value (which is also empty). At the bottom of the modal are 'Add' and 'Cancel' buttons.

6. Now that it is created, we make sure to copy our secret's value, as it **will not be shown again**.

This screenshot shows the 'Certificates & secrets' section of the Azure portal. It displays a message about credentials and a table of client secrets. The table has columns for Description, Expires, Value (which is populated with a long secret key), and Secret ID. The 'Value' column for the 'ProjectMISP' entry is highlighted with a green box. The 'Description' column for the same entry is also highlighted with a green box.

7. Now we need to add the Sentinel Contributor role to the app. We do this by going into the Log Analytics workspace our Sentinel instance is in, in this case **SIEMlogs**, navigating to the **Access control (IAM)** page, and clicking on **Add role assignment**.

Microsoft Azure

Log Analytics workspaces > SIEMlogs

SIEMlogs | Access control (IAM)

Check access Role assignments Roles Deny assignments Classic administrators

My access

Check access

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Check access

Grant access to this resource

Grant access to resources by assigning a role. Learn more

Add role assignment

View access to this resource

View the role assignments that grant access to this and other resources. Learn more

View

View deny assignments

View the role assignments that have been denied access to specific actions at this scope. Learn more

View

New! Permissions Management

Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Extra Permissions Management. Learn more

Get started

8. We now search for the Microsoft Sentinel Contributor role on the **Role** tab, select it, and click **Next**.

Microsoft Azure

Home > SIEMlogs | Access control (IAM) >

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Job function roles Privileged administrator roles

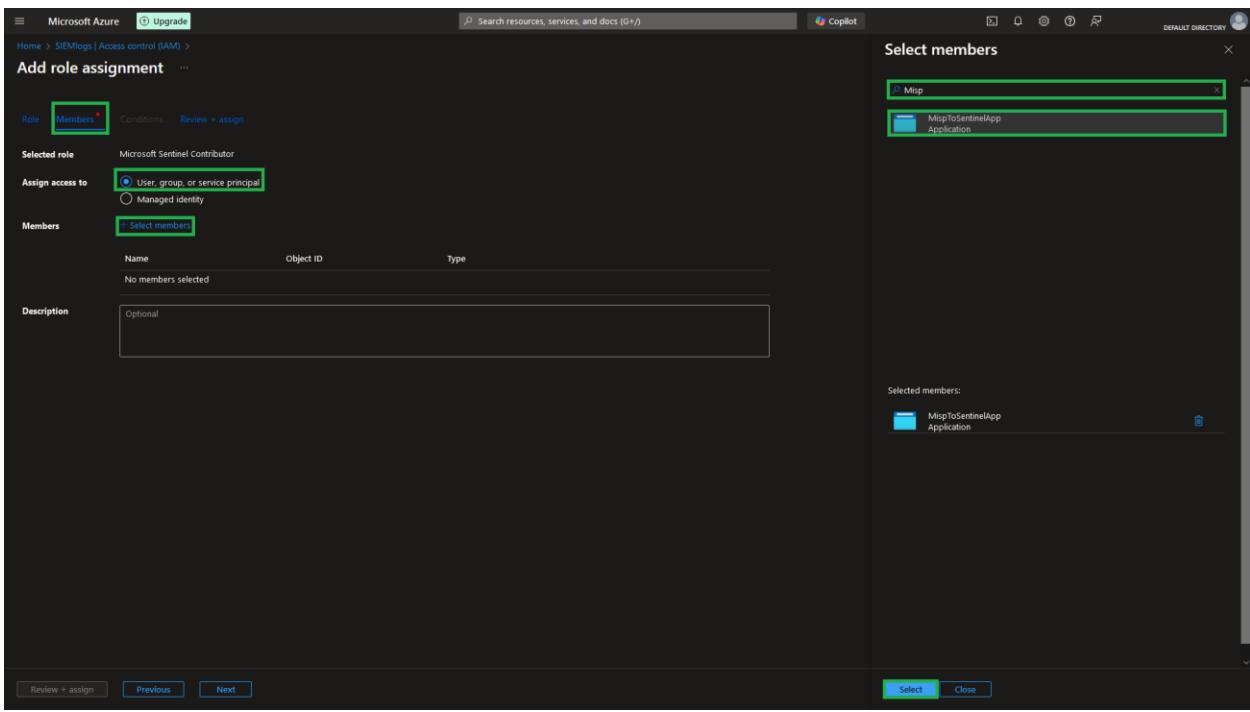
Sentinel Type: All Category: All

| Name | Description | Type | Category | Details |
|--------------------------------|--------------------------------|-------------|----------|---------|
| Microsoft Sentinel Contributor | Microsoft Sentinel Contributor | BuiltInRole | Security | View |
| Microsoft Sentinel Reader | Microsoft Sentinel Reader | BuiltInRole | Security | View |
| Microsoft Sentinel Responder | Microsoft Sentinel Responder | BuiltInRole | Security | View |

Showing 1 - 3 of 3 results.

Review + assign Previous Next Feedback

9. On the **Members** tab, we leave the **User, group, or service principal** radio button selected, click on **Select members**, search for the name of our app, select it, and click on the **Select** button.



10. We then click on **Review + assign** and it should now show up on the **Access control (IAM)** page of the Log Analytics workspace.

| Name | Type | Role | Scope | Condition |
|---|------|--------------------------------|---------------|-----------|
| Owner (2) | | | | |
| Microsoft Sentinel Contributor (1) | App | Microsoft Sentinel Contributor | This resource | None |
| MisptoSentinelApp | App | Microsoft Sentinel Contributor | This resource | None |
| Virtual Machine Administrator Login (1) | | | | |

11. We need to create a MISP API Key. To do this, we go back to our MISP instance, hover over **Administration**, and click on **List Auth Keys**.

Afterwards, this API key should ideally be stored in an Azure Key Vault, but for the sake of brevity we will not be doing this for this project.

12. On the **Authentication key index** page, we click on **+Add authentication key**.

13. On the **Add auth key** page, we have the ability to secure our key by creating an IP Allow list and setting an expiration date, but we will leave it blank for this project and click on **Submit**.

Add auth key

Auth keys are used for API access. A user can have more than one authkey, so if you would like to use separate keys per tool that queries MISP, add additional keys. Use the comment field to make identifying your keys easier.

User

Comment

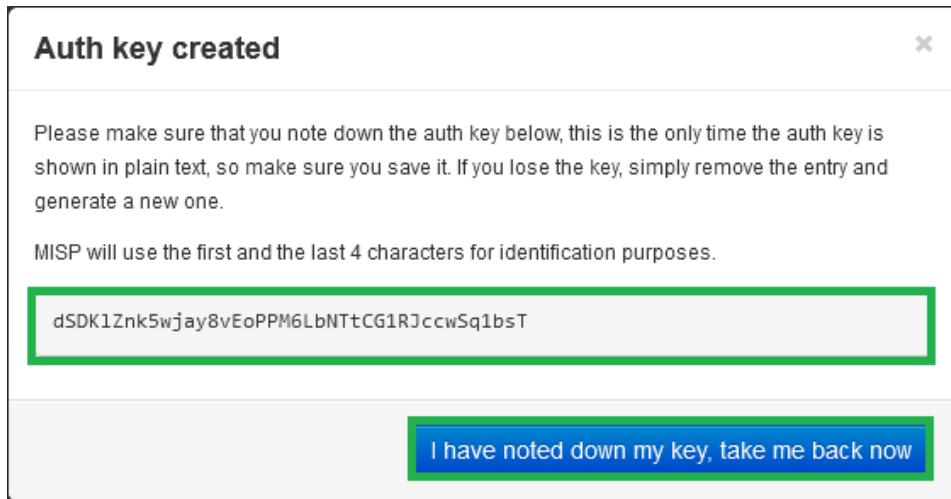
Allowed IPs

Expiration (keep empty for indefinite)

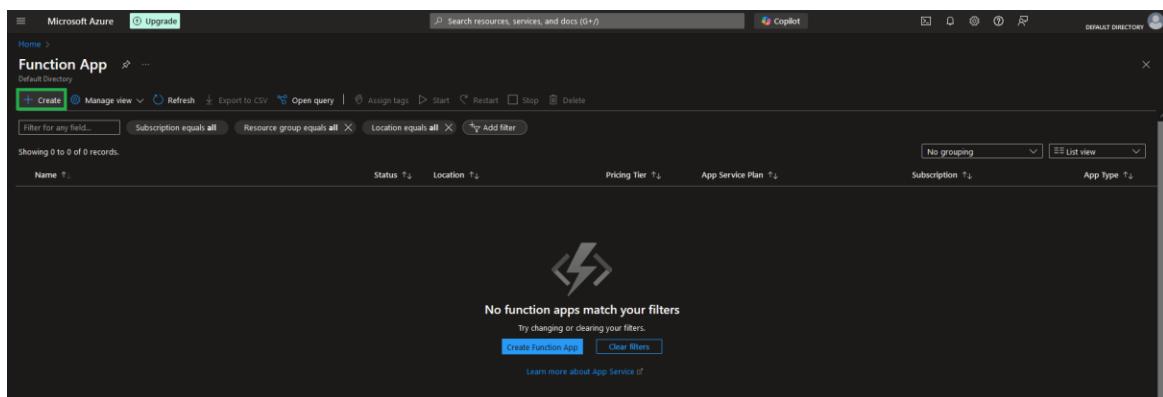
Read only (it will unset all permissions. This should not be used for sync users)

Submit **Cancel**

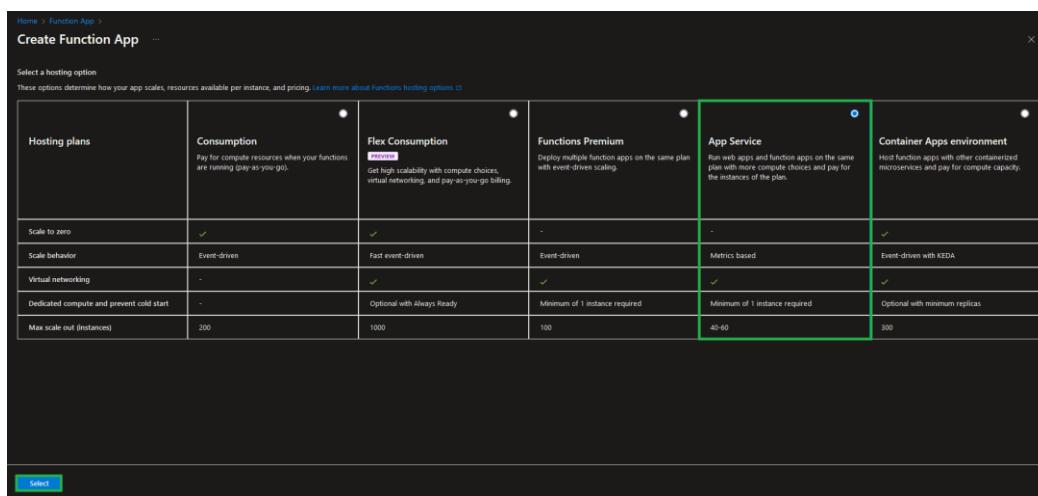
14. We take a note of our key, as it will not be shown in full again later and click on **I have noted down my key, take me back now**.



15. We now go back to the Azure Portal and create a Function app. We go to the **Function app** page through the search bar and click on **Create**.



16. We then select the **App Service** hosting option.



17. We select the following configuration on the **Basics** tab and click on **Review + create**:

| Field | Value |
|-------------------|---|
| Subscription | Our current subscription. |
| Resource group | SIEMproject |
| Function App name | Enter a unique name, such as MISP2Sentinel . |
| Region | Select the same region as previous resources |
| Runtime stack | Python |
| Availability zone | 3.11 (Any Python 3) |
| Size | Premium V3 P1V3 (Can be left default) |

Home >

Create Function App (App Service) ...

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource Group * ⓘ [Create new](#)

Instance Details

Function App name * [.azurewebsites.net](#)

Do you want to deploy code or container image? * Code Container Image

Runtime stack *

Version *

Region *

i Not finding your App Service Plan? Try a different region or select your App Service Environment.

Operating System * Linux Windows

Environment details

Linux Plan (West Europe) * ⓘ [Create new](#)

Pricing plan [Explore pricing plans](#)

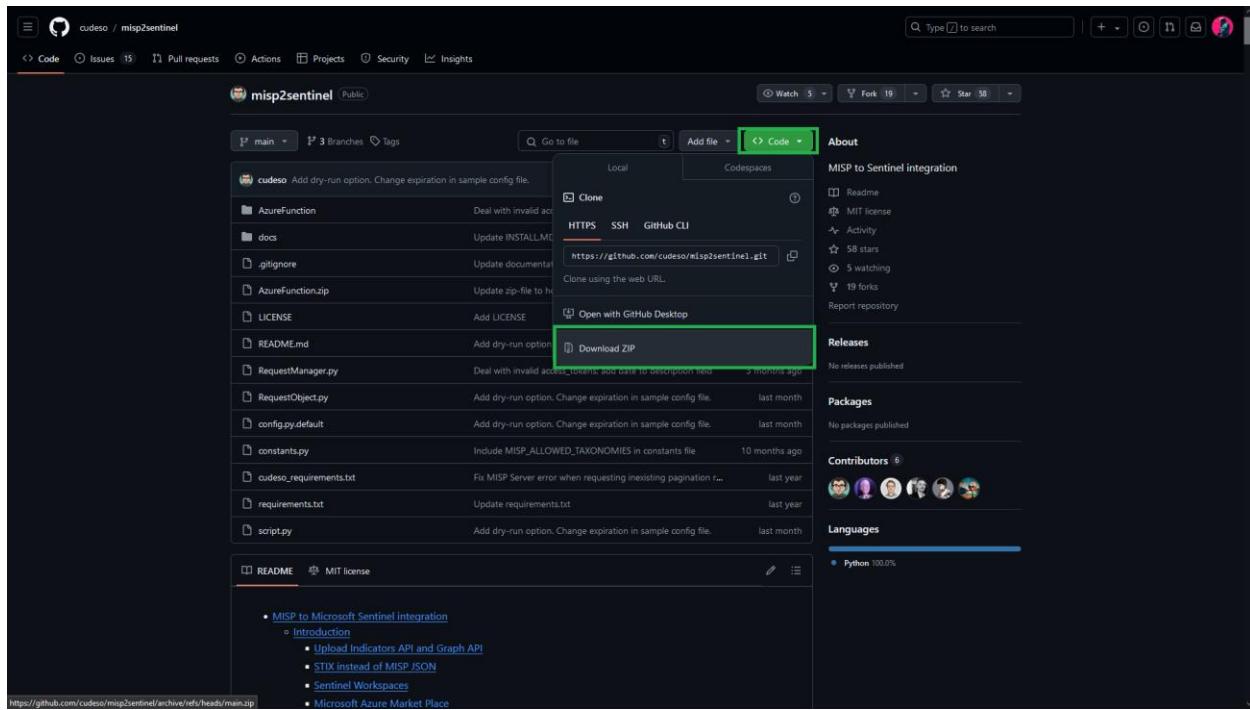
Zone redundancy

An App Service plan can be deployed as a zone redundant service in the regions that support it. This is a deployment time only decision. You can't make an App Service plan zone redundant after it has been deployed [Learn more ↗](#)

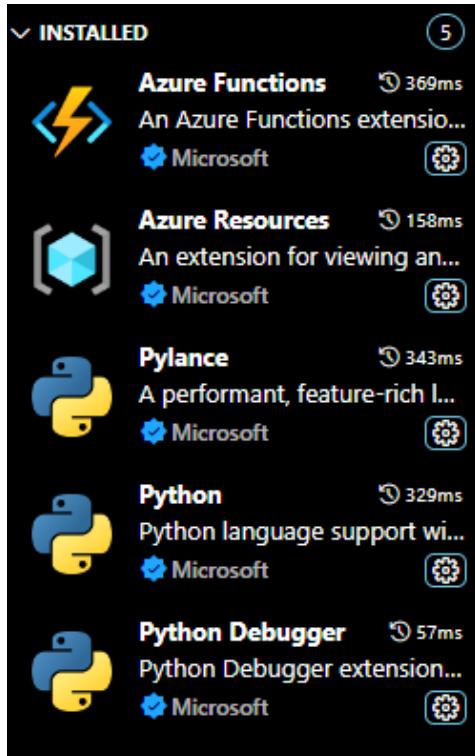
Zone redundancy **Enabled:** Your App Service plan and the apps in it will be zone redundant. The minimum App Service plan instance count will be three. **Disabled:** Your App Service Plan and the apps in it will not be zone redundant. The minimum App Service plan instance count will be one.

[Review + create](#) [< Previous](#) [Next : Networking >](#)

18. We now go to github.com/cudeso/misp2sentinel, click on **Code**, and then the **Download ZIP** option.



Note: We need to have Visual Studio Code and the Python, Pylance, Python Debugger, Azure Resources, and Azure Functions extensions installed for the following steps.



19. We extract the .zip file and open the extracted folder with Microsoft Visual Studio Code. We select the Azure icon, click on **Sign in to Azure..**, and choose **Allow** when prompted.

```

1  from pymisp import PyMISP
2  import MISPSentinel.config as config
3  from MISPSentinel import RequestManager
4  from MISPSentinel.RequestObject import RequestObject, RequestObject_Event, RequestObject_Indicator
5  from MISPSentinel.constants import *
6  import sys
7  from functools import reduce
8  import os
9  import datetime
10 from pytz import timezone, timedelta, timezone
11 import requests
12 import json
13 import azure.functions as func
14 import requests
15 import json
16 from misp_stix_converter import MISPToSTIX2Parser
17 from stix2.base import STIXJSONEncoder
18
19 if config.misp_verifycert is False:
20     import urllib
21     import urllib3
22     urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
23
24 def _get_misp_events_stix():
25     logging.info("Using the following values for MISP API call: domain: %s, misp API key: %s" % (config.misp_domain, config.misp_key))
26     misp = PyMISP(config.misp_domain, config.misp_key, config.misp_verifycert, False)
27     result_set = []
28     logging.debug("Query MISP for events...")
29     remaining_misp_pages = True
30     misp_page = 1
31     misp_indicator_ids = []
32
33     while remaining_misp_pages:
34         try:
35             if "list" in config.misp_event_filters:
36                 result = misp.search(controller='events', return_format='json', **config.misp_event_filters)
37             else:
38                 result = misp.search(controller='events', return_format='json', **config.misp_event_filters, limit=config.misp_event_limit_per_page, page=misp_page)
39
40             if len(result) > 0:
41                 logging.info("Received MISP events page {} with {} events".format(misp_page, len(result)))
42                 for event in result:
43                     misp_event = RequestObject_Event(event["Event"])
44                     parser = MISPToSTIX2Parser()
45                     parser.parse_misp_event(misp_event)
46                     stix_objects = parser.get_stix_objects()
47                     for element in stix_objects:
48                         if element.type in UPLOAD_INDICATOR_API_ACCEPTED_TYPES and \
49                             element.id not in misp_indicator_ids:
50                             misp_indicator = RequestObject_Indicator(element, misp_event)
51
52
53     credential = DefaultAzureCredential()
54     client = SecretClient(vault_url=VAULT, credential=credential)
55
56     # Retrieve values from KV (client_secret, MISP-key most importantly)
57     retrieved_mispkey = client.get_secret('MISP-Key')
58     retrieved_clientsecret = client.get_secret('ClientSecret')
59
60     # Set values with
61     mispkey = retrieved_mispkey.value
62     ms_auth['client_secret'] = retrieved_clientsecret.value
63
64     else:
65         print('key.vault_name env variable not set, falling back to env variable for config values...')
66         mispkey = os.getenv('mispkey')
67
68     #####
69     # Microsoft Section #
70     #####
71
72     # Graph API only settings
73     ms_max_indicators_request = 100    # Throttle max: 100 indicators per request
74     ms_max_requests_minute = 100      # Throttle max: 100 requests per minute
75     ms_username = 'MISP-1.0'
76
77     config.target_product = 'Azure Sentinel' # Target Product
78     ms_api_version = '2022-07-01'        # Upload Indicators API Version
79
80     #####
81     # MISP API settings
82     ms_key = mispkey
83     ms_domain = misurl

```

20. We no go back into the Python scripts as there are two changes we need to make to the code.

I. We go to the config.py file and change 'MISP-Key' to 'mispkey'.

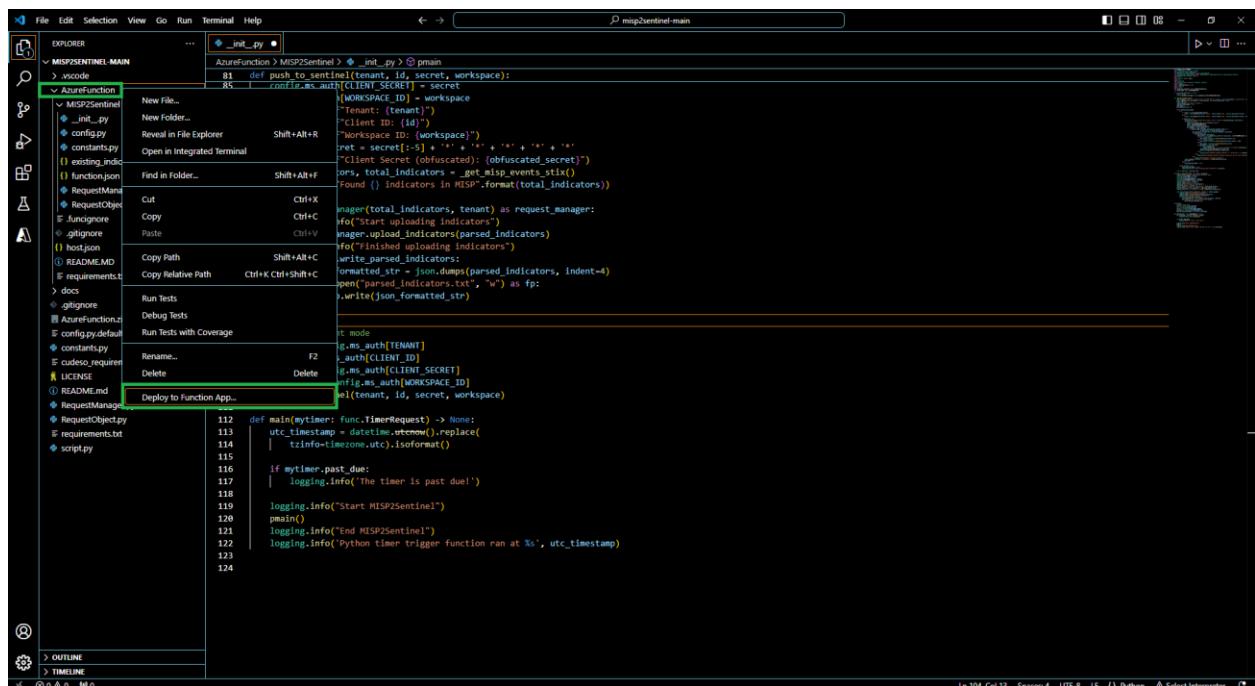
```

1  # Log in with the virtual machines managed identity
2  credential = DefaultAzureCredential()
3  client = SecretClient(vault_url=VAULT, credential=credential)
4
5  # Retrieve values from KV (client_secret, MISP-key most importantly)
6  retrieved_mispkey = client.get_secret('MISP-Key')
7  retrieved_clientsecret = client.get_secret('ClientSecret')
8
9  # Set values with
10 mispkey = retrieved_mispkey.value
11 ms_auth['client_secret'] = retrieved_clientsecret.value
12
13 else:
14     print('key.vault_name env variable not set, falling back to env variable for config values...')
15     mispkey = os.getenv('mispkey')
16
17 #####
18 # Microsoft Section #
19 #####
20
21 # Graph API only settings
22 ms_max_indicators_request = 100    # Throttle max: 100 indicators per request
23 ms_max_requests_minute = 100      # Throttle max: 100 requests per minute
24 ms_username = 'MISP-1.0'
25
26 config.target_product = 'Azure Sentinel' # Target Product
27 ms_api_version = '2022-07-01'        # Upload Indicators API Version
28
29 #####
30 # MISP API settings
31 ms_key = mispkey
32 ms_domain = misurl

```

II. We then go to the _init_.py file and delete the code block under the ## Multi-tenant mode comment.

III. We then right-click on **AzureFunction** and select **Deploy to Function App**.



21. The function should now be visible under the **Functions** tab on the **Overview** page.

{ } Set up local environment Refresh

Filter by name...

| Name | Trigger |
|---------------|---------|
| MISP2Sentinel | Timer |

22. We then go to **Environment variables** under the *Settings* blade and click on **Add** on the **App settings** tab.

| Name | Value |
|---------------------------------------|----------------------------|
| APPLICATIONINSIGHTS_CONNECTION_STRING | Show value |
| AzureWebJobsStorage | Show value |
| BUILD_FLAGS | Show value |
| ENABLE_ORYX_BUILD | Show value |
| FUNCTIONS_EXTENSION_VERSION | Show value |
| FUNCTIONS_WORKER_RUNTIME | Show value |
| SCM_DO_BUILD_DURING_DEPLOYMENT | Show value |
| XDG_CACHE_HOME | Show value |

23. We create the following variables that are expected in our MISP2Sentinel python code:

```

6  mispkey = ''
7  mispurl=os.getenv('mispurl')
8
9  local_mode=os.getenv('local_mode', 'False')
10 keyVaultName=os.getenv('key_vault_name', '')
11
12 tenant_id=os.getenv('tenant_id', '')
13 workspace_id=os.getenv('workspace_id', '')
14 client_id=os.getenv('client_id', '')
15 client_secret=os.getenv('client_secret', '')
16
17 # MS API settings
18 ms_auth = [
19     'tenant': tenant_id,
20     'client_id': client_id,
21     'client_secret': client_secret,
22     'scope': 'https://management.azure.com/.default',
23     'graph_api': False,
24     'workspace_id': workspace_id
25 ]

```

tenant_id
client_id
clinet_secret

They can be found on the app registration page we made earlier.

workspace_id

It can be found on the **Overview** page of the workspace our Sentinel instance is in.

mispkey

The key we generated on the **Authentication key index** page of our MISP instance.

mispurl

The public IP address of our Ubuntu server, can be found on our VMs **Connect** page.

24. We also need to add a *timerTriggerSchedule* variable with a value of:

0 */2 * * *

This is so that the function can run every 2 hours.

25. We then click **Appy**

| App settings | | Connection strings |
|---------------------------------------|-------|--------------------|
| Name | Value | |
| APPLICATIONINSIGHTS_CONNECTION_STRING | | Show value |
| AzureWebJobsStorage | | Show value |
| BUILD_FLAGS | | Show value |
| client_id | | Show value |
| client_secret | | Show value |
| ENABLE_ORYX_BUILD | | Show value |
| FUNCTIONS_EXTENSION_VERSION | | Show value |
| FUNCTIONS_WORKER_RUNTIME | | Show value |
| mispkey | | Show value |
| mispurl | | Show value |
| SCM_DO_BUILD_DURING_DEPLOYMENT | | Show value |
| tenant_id | | Show value |
| workspace_id | | Show value |
| XDG_CACHE_HOME | | Show value |

Apply **Discard**

26. Once we run the Function App, it should take a couple of hours for it to update in Sentinel. If we are successful, the status of our MISP2Sentinel Connector should change to **Connected**.

| MISP2Sentinel | |
|---|--|
|  Delete | ... |
|  MISP2Sentinel | « |
| Connected Status |  MISP Project & ... Provider |
| |  3 Days Ago Last Log Received |

27. We should also now have our new threat intelligence indicators available.

28. We should also now have threat intelligence indicators available as a table that we could use to create alerts in Sentinel

Tables Queries Functions ... <

Search :
Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the icon

- ▶ LogManagement
- ◀ Microsoft Sentinel
 - ▶ SecurityEvent
 - ▶ ThreatIntelligenceIndicator
- ▶ Security and Audit