

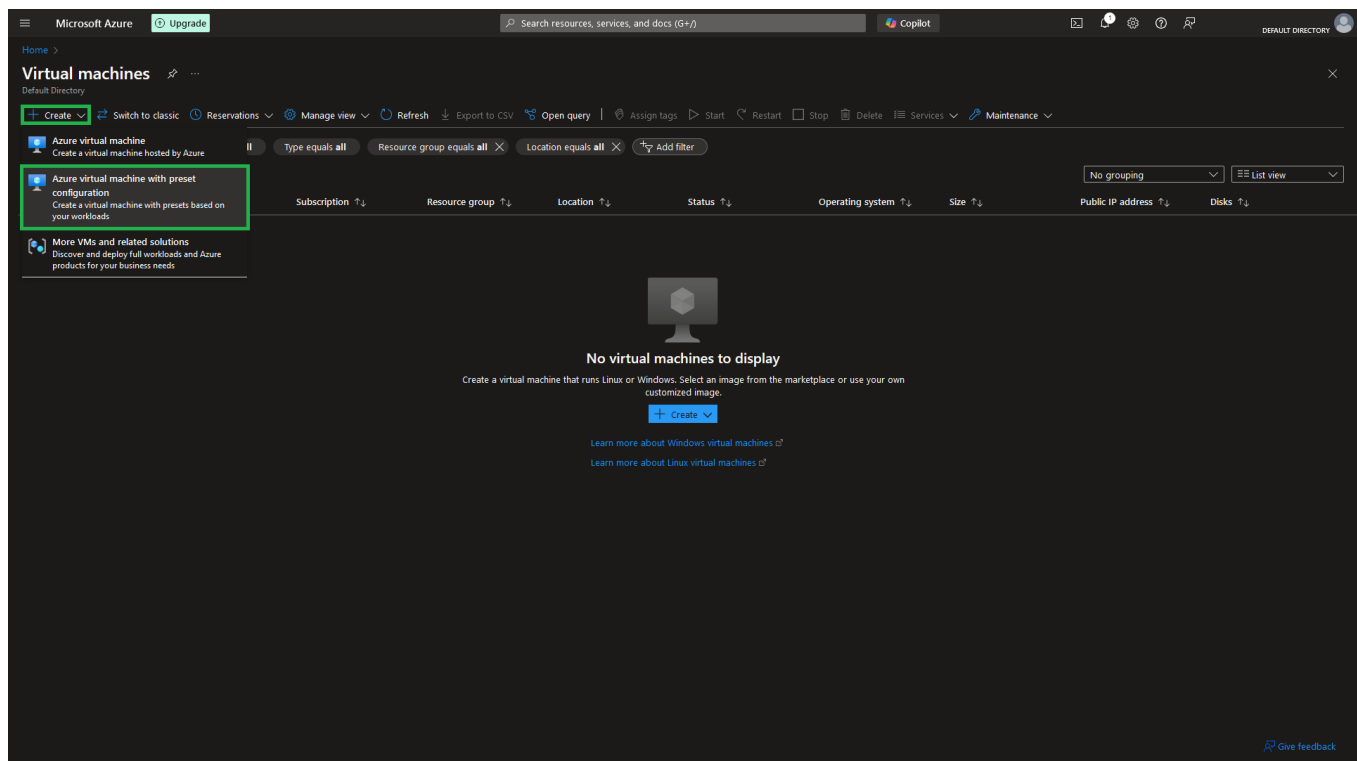
Azure security project solution PART 1:

Creating a honeypot VM

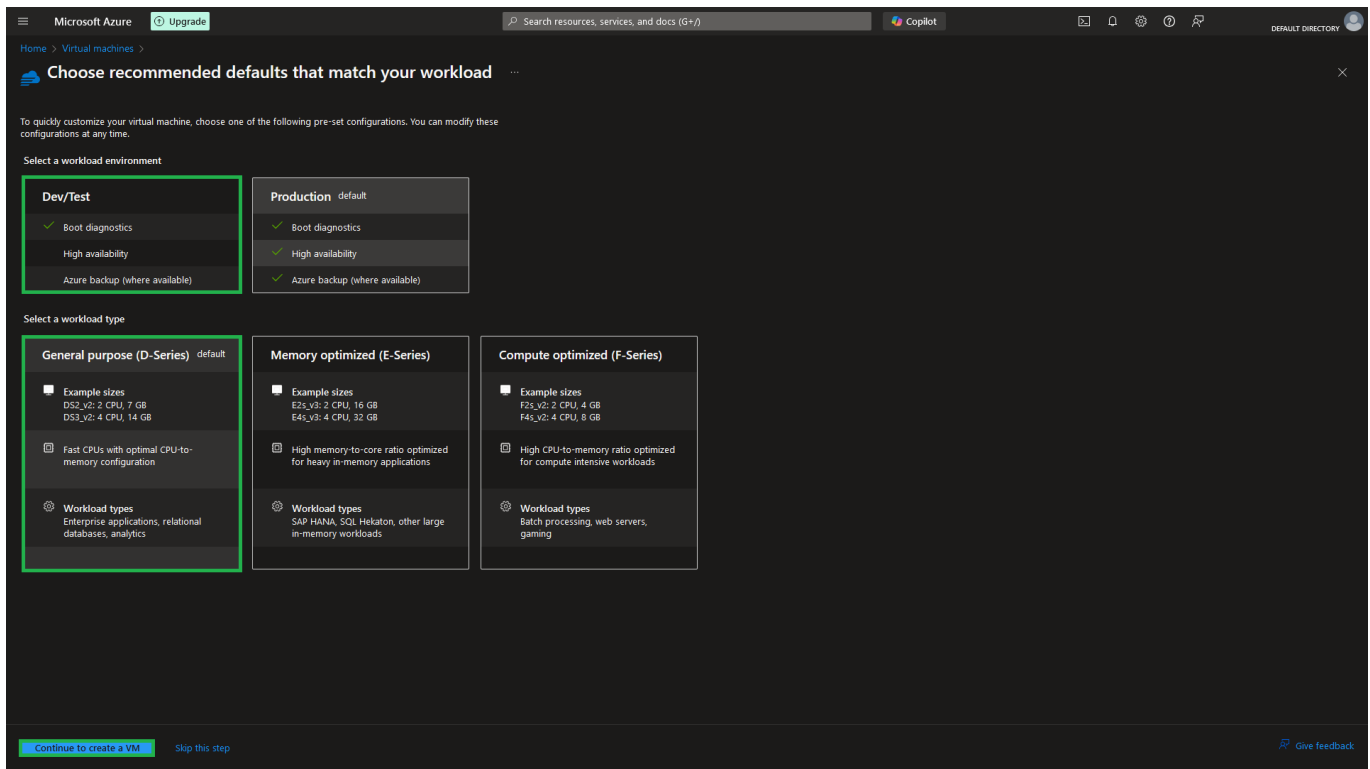
In this project we will build our own security operations center by utilizing Microsoft Sentinel to deploy a Security Information and Event Management (SIEM) solution that monitors and generates alerts for a virtual machine – we can use it as an RDP honeypot. We will also setup a threat intelligence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

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Virtual machines > Choose recommended defaults that match your workload >

Create a virtual machine

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

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

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ (New) SIEMproject
[Create new](#)

Instance details

Virtual machine name * ⓘ SIEMprojectVM

Region * ⓘ (Europe) West Europe

Availability options ⓘ Availability zone

Zone options ⓘ
☒ Self-selected zone
Choose up to 3 availability zones, one VM per zone
☐ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Availability zone * ⓘ Zone 1
✔ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ Trusted launch virtual machines
[Configure security features](#)

Image * ⓘ Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible)
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ
☐ Arm64
☒ x64

< Previous **Next : Disks >** 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.

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

[Home](#) > [Virtual machines](#) > [Choose recommended defaults that match your workload](#)

Create a virtual machine

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 Hibernation to enable this feature. [Learn more](#)

Administrator account

Username

VMadmin

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

RDP (3389)

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.

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

[Home](#) > [Virtual machines](#) > [Choose recommended defaults that match your workload](#)

Create a virtual machine

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

Validation passed

Price

1 X Standard D4s v3
by Microsoft
[Terms of use](#) [Privacy policy](#)

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

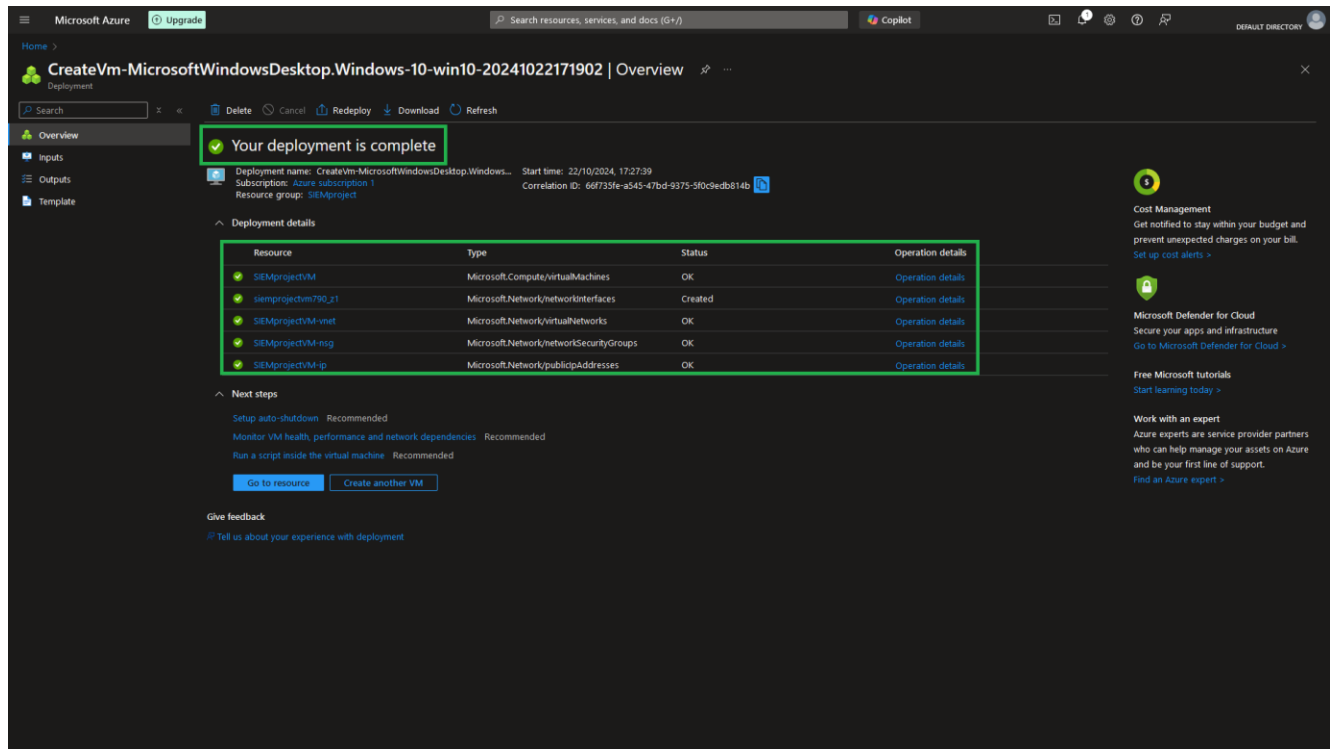
Create

< Previous

Next >

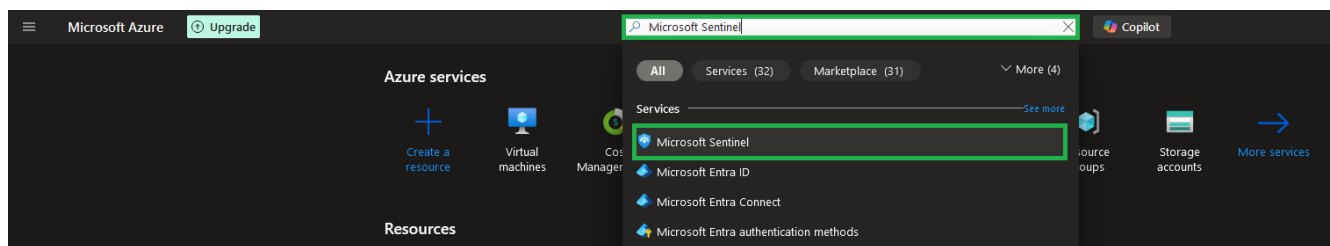
Create

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

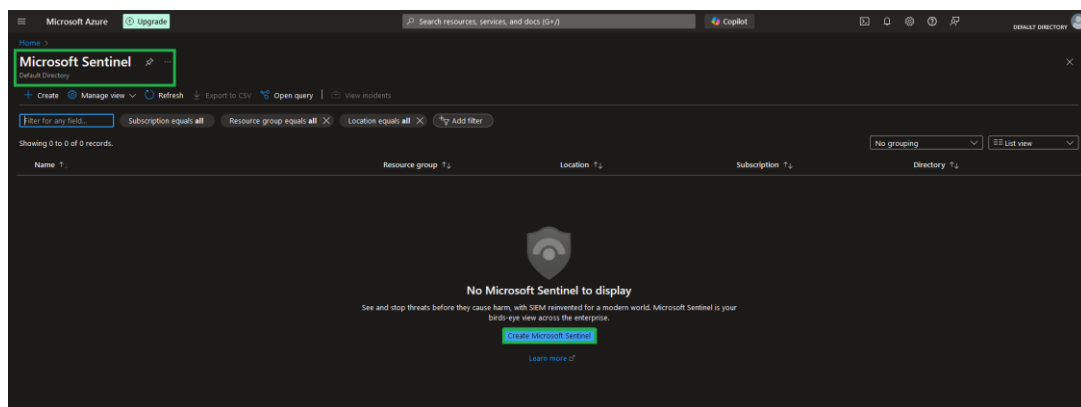


Task 2: Create a Log Analytics workspace and activate Microsoft Sentinel

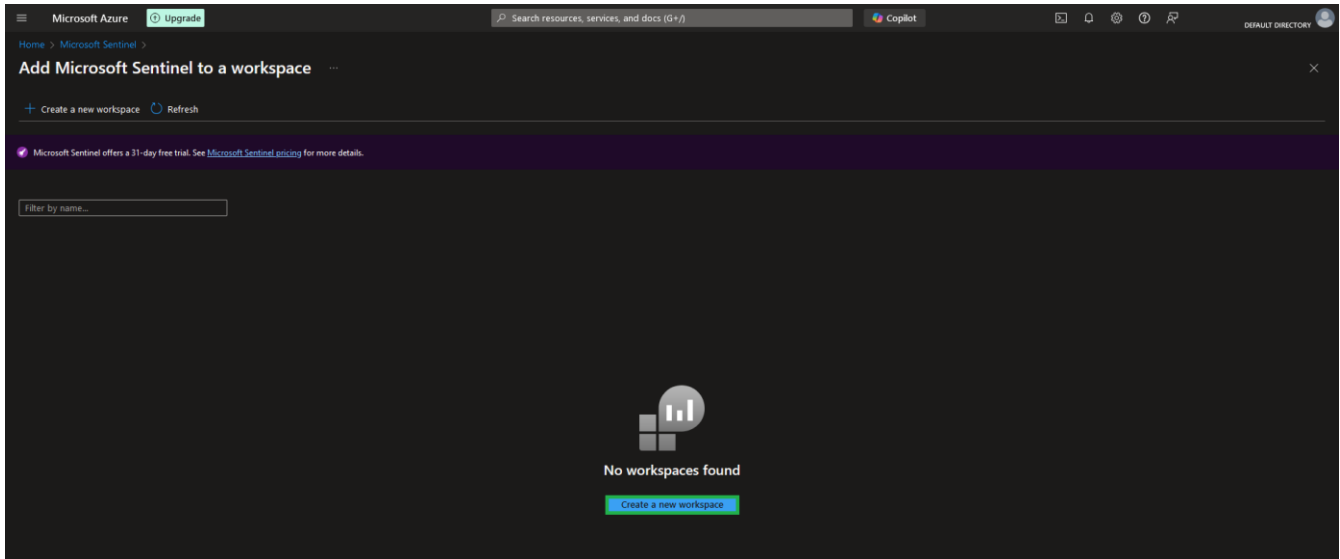
1. Once that is done, we go back to the Azure Portal and type in "Microsoft Sentinel" into the search box.



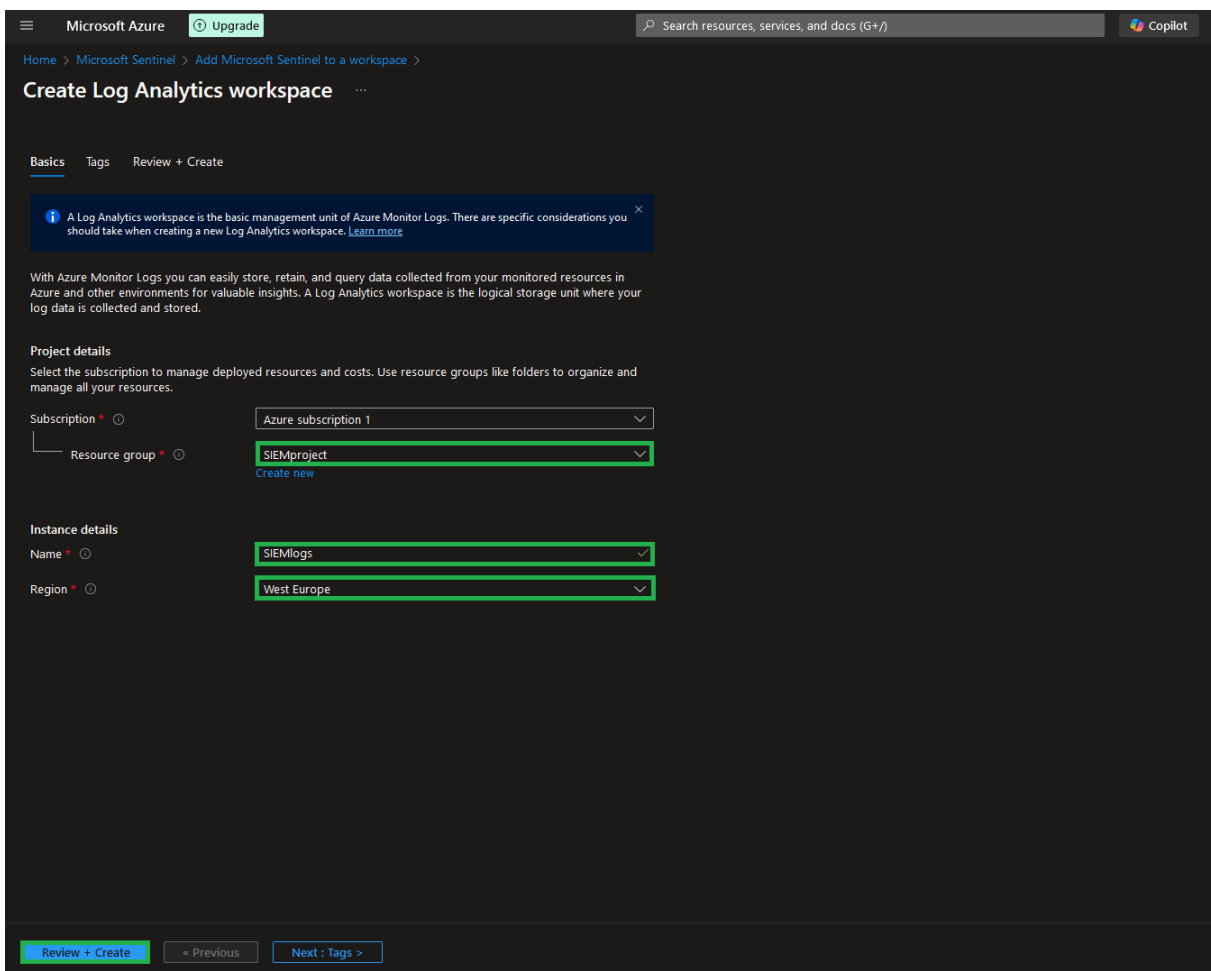
2. On the **Microsoft Sentinel** page, we simply click on **Create Microsoft Sentinel**.



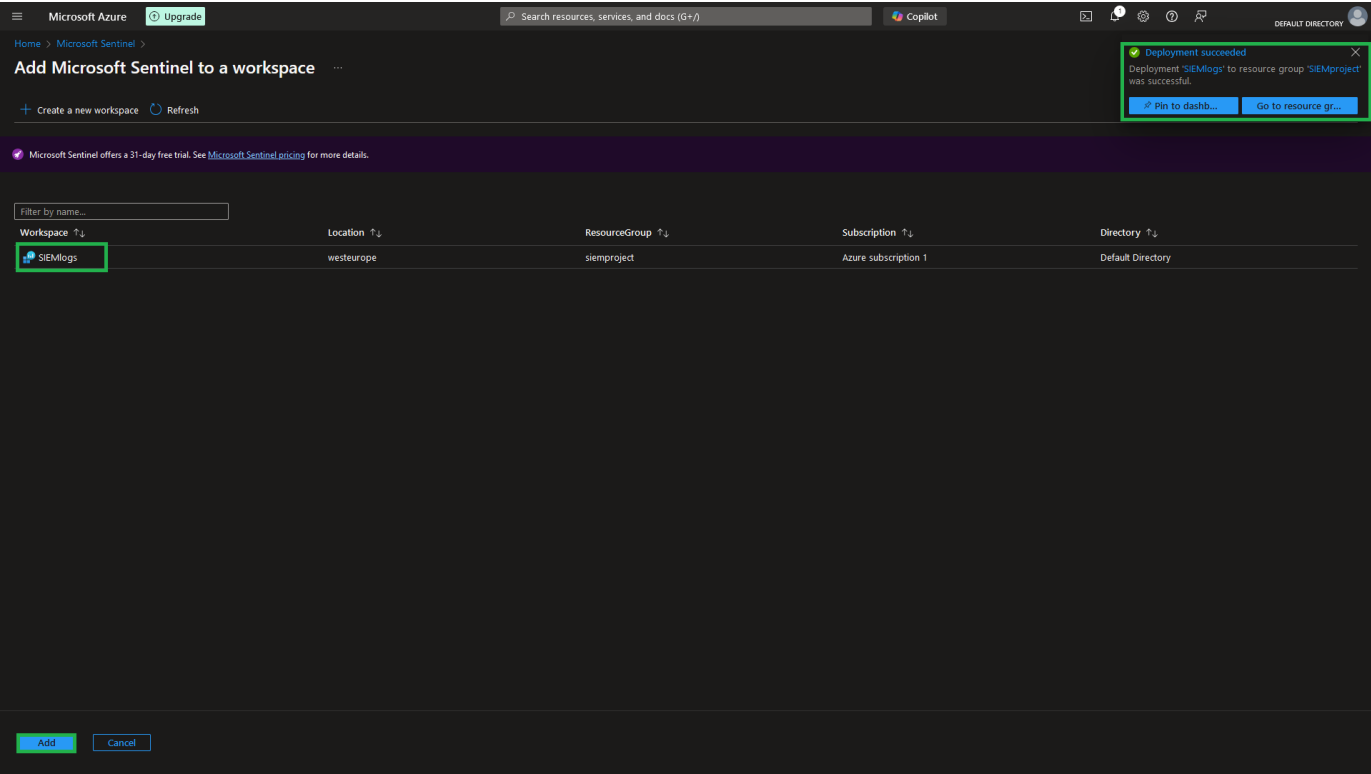
3. We can then either add Sentinel to an existing Log Analytics workspace or create a new one. Here we have no existing workspaces, so we click on the **Create a workspace** button.



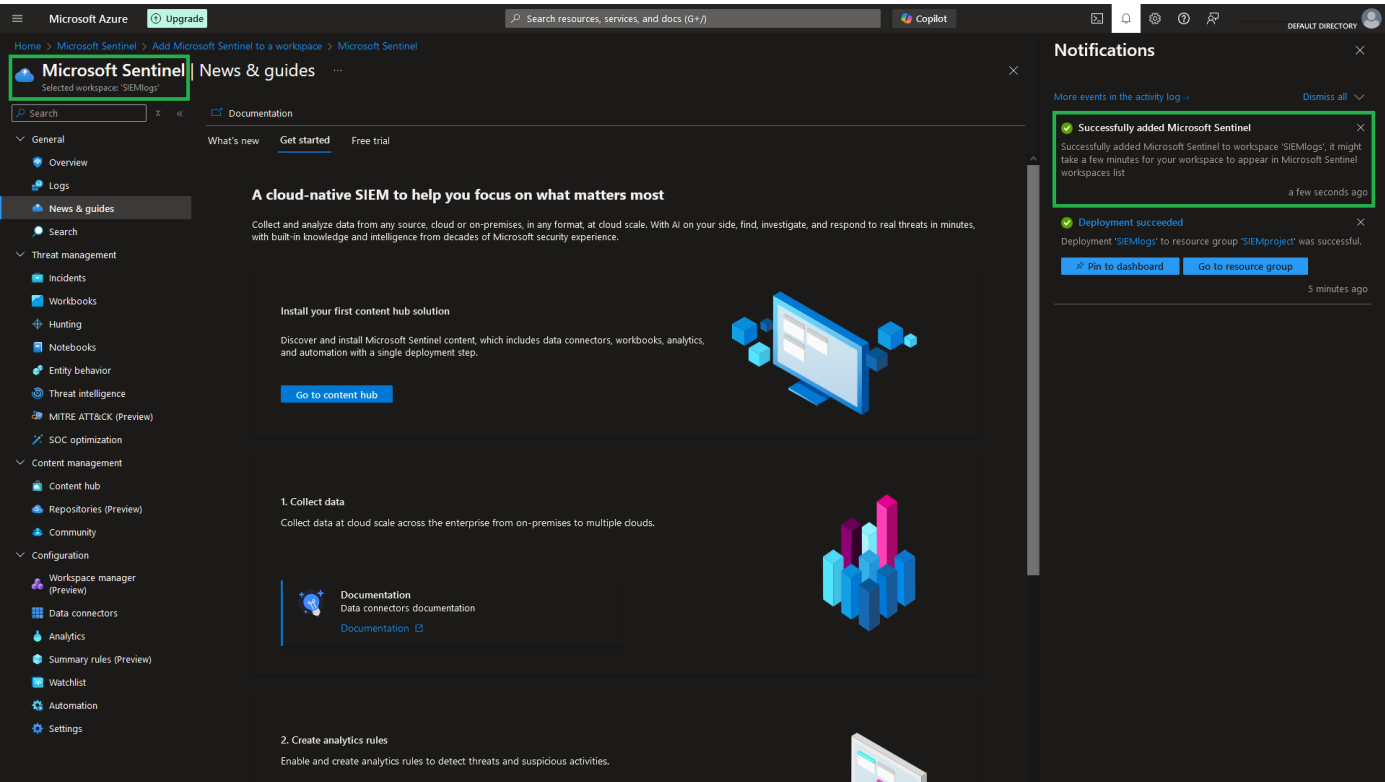
4. On the **Create Log Analytics workspace** page, we make sure that we have selected the same resource group as the resources that we want to monitor – in this case, the **SIEMproject** resource group where our VM is. We also make sure that we are deploying it the same region, in my case **West Europe**. 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.

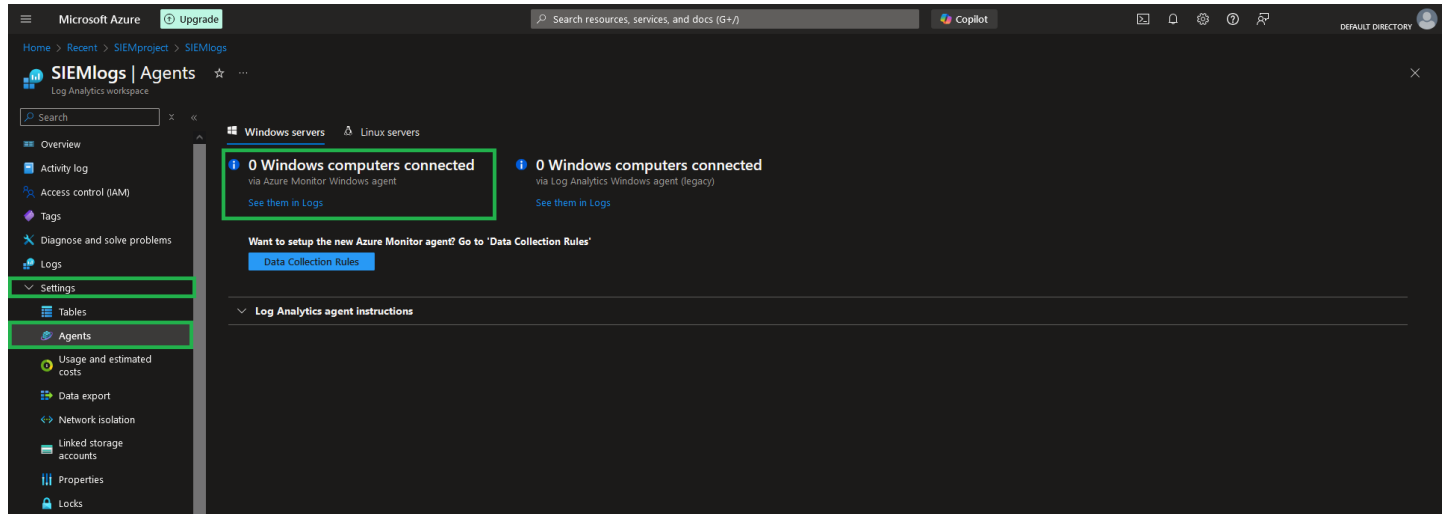


6. We now wait for the confirmation that Microsoft Sentinel has been activated.

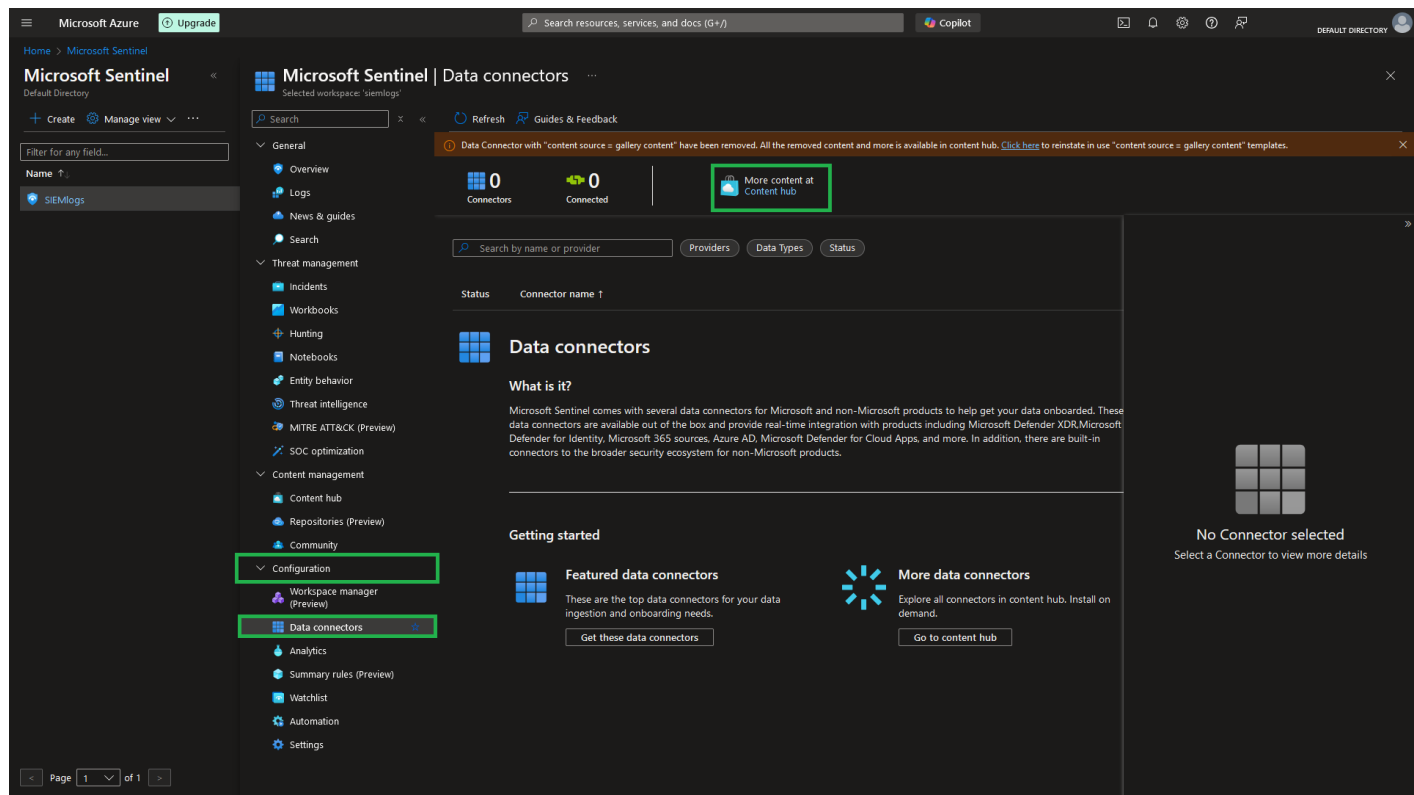


Task 3: Setting up a Data Connector and creating a data collection rule

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 **SEMlogs** 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.



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**.



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**.

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | DEFAULT DIRECTORY

Home > Microsoft Sentinel | Data connectors >

Content hub

Refresh | Install/Update | Delete | SIEM Migration | Guides & Feedback

367 Solutions | 303 Standalone contents | 0 Installed | 0 Updates

Azure Monitor Agent | Status: All | Content type: Data connector (359) | Support: All | Provider: All | Category: All | Content sources: All

Content title	Status	Content source	Provider	Support	Category	Content type
Cisco ASA	Not installed	Solution	Cisco	Microsoft	Security - Automation (SOAR)	Analytics rule (2) Data connector (2) +2
Common Event Format	Not installed	Solution	Microsoft	Microsoft	IT Operations	Data connector (2) Workbook
CyberArk Privilege Access Manage...	Not installed	Solution	Cyberark	Cyberark	Identity	Data connector (2) Workbook
Fortinet FortiWeb Cloud WAF-as-a-S...	Not installed	Solution	Microsoft	Microsoft	Security - Automation (SOAR)	Analytics rule Data connector (2) +4
Ridge Security RidgeBot	Not installed	Solution	RidgeSecurity	RidgeSecurity	Security - Vulnerability Management	Analytics rule (7) Data connector +3
Syslog	Not installed	Solution	Microsoft	Microsoft	IT Operations	Analytics rule (7) Data connector (2) +3
Windows Firewall	Not installed	Solution	Microsoft	Microsoft	Security - Network	Data connector (2) Workbook
Windows Forwarded Events	Not installed	Solution	Microsoft	Microsoft	IT Operations	Analytics rule (2) Data connector
Windows Security Events	Not installed	Solution	Microsoft	Microsoft	Security - Threat Protection	Analytics rule (20) Data connector (2) +2
Windows Server DNS	Not installed	Solution	Microsoft	Microsoft	Networking	Analytics rule (5) Data connector (2) +2

< Previous | Page 1 of 1 | Next > | Showing 1 to 10 of 10 results.

Windows Security Events

Microsoft Provider | Microsoft Support | 3.0.9 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). Microsoft recommends using this Data Connector.
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

NOTE: Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

Data Connectors: 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type: Analytics rule (20), Data connector (2), Hunting query (50), Workbook (2)

Category: [Install](#) | [View details](#)

4. 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**.

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | DEFAULT DIRECTORY

Home > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'siemlogs'

Search | Refresh | Guides & Feedback

General | Overview | Logs | News & guides | Search

Threat management | Incidents | Workbooks | Hunting | Notebooks | Entity behavior | Threat intelligence | MITRE ATT&CK (Preview) | SOC optimization

Content management | Content hub | Repositories (Preview) | Community

Configuration | Workspace manager (Preview) | **Data connectors** | Analytics | Summary rules (Preview) | Watchlist | Automation | Settings

2 Connectors | 0 Connected | More content at Content hub

Search by name or provider | Providers: Microsoft | Data Types: SecurityEvents | Status: Not connected (2)

Status	Connector name
Not connected	Security Events via Legacy Agent Microsoft
Not connected	Windows Security Events via AMA Microsoft

Windows Security Events via AMA

Disconnected Status | Microsoft Provider | Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received: --

Content source: Windows Security Events | Version: 1.0.0

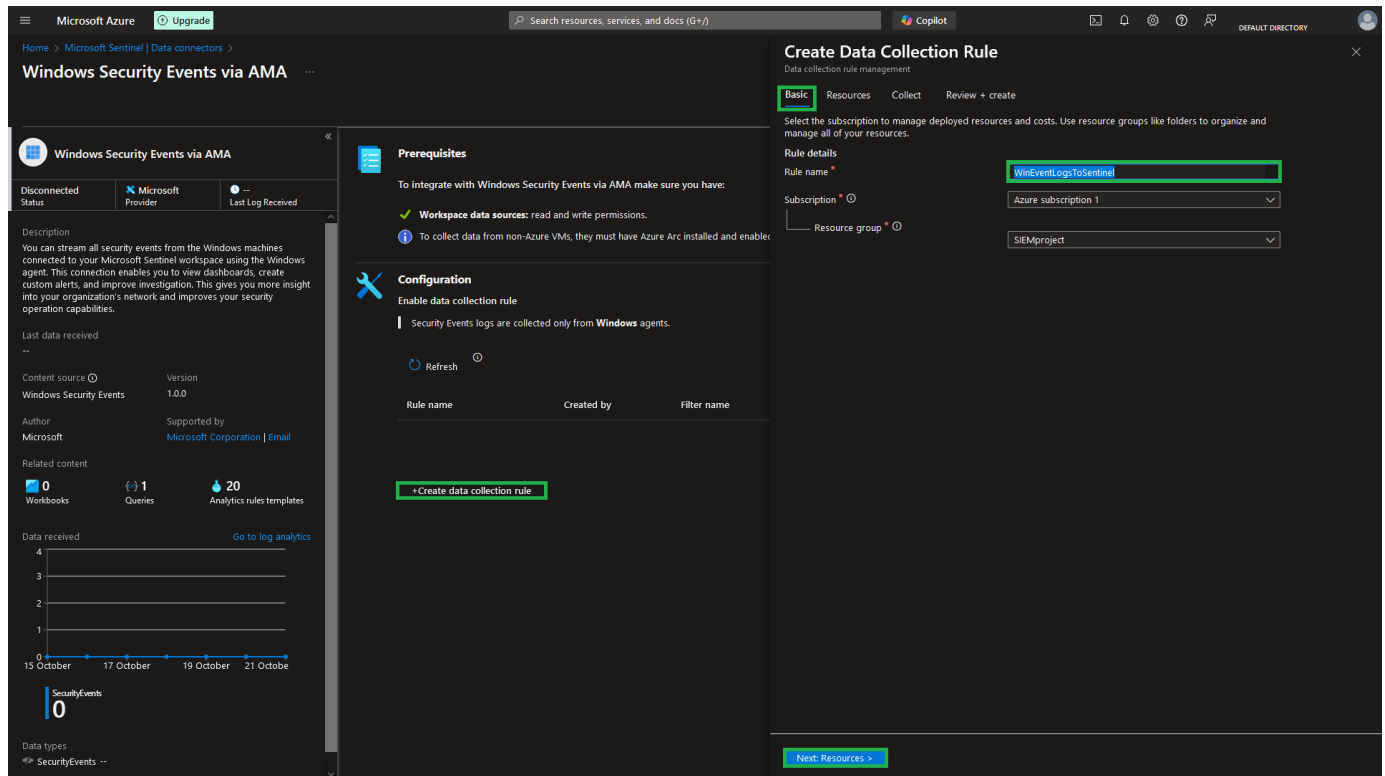
Author: Microsoft | Supported by: Microsoft Corporation | Email

Related content: 0 Workbooks, 1 Queries, 20 Analytics rules templates

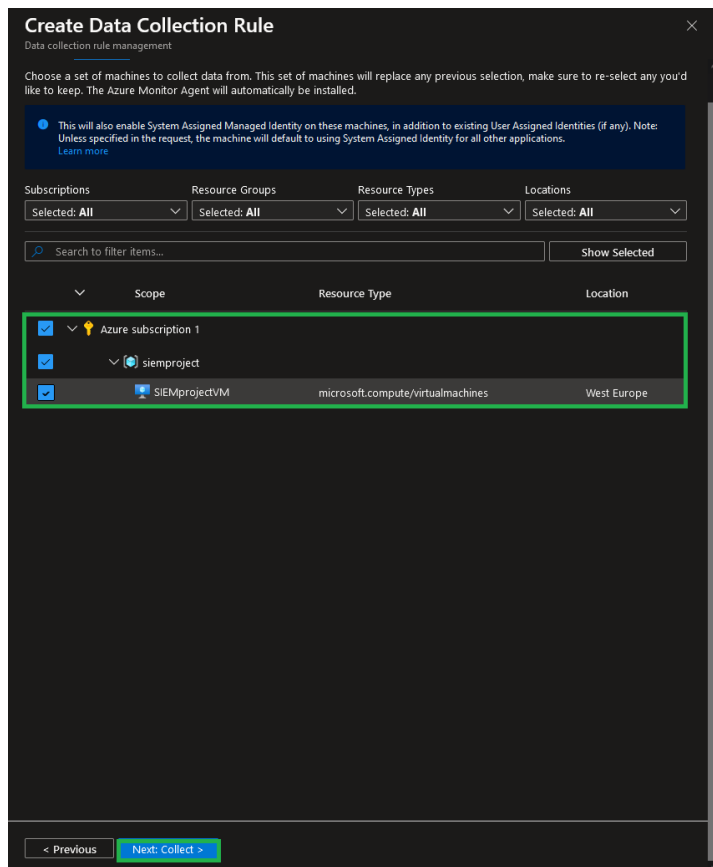
Data received: [Go to log analytics](#)

[Open connector page](#)

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**.



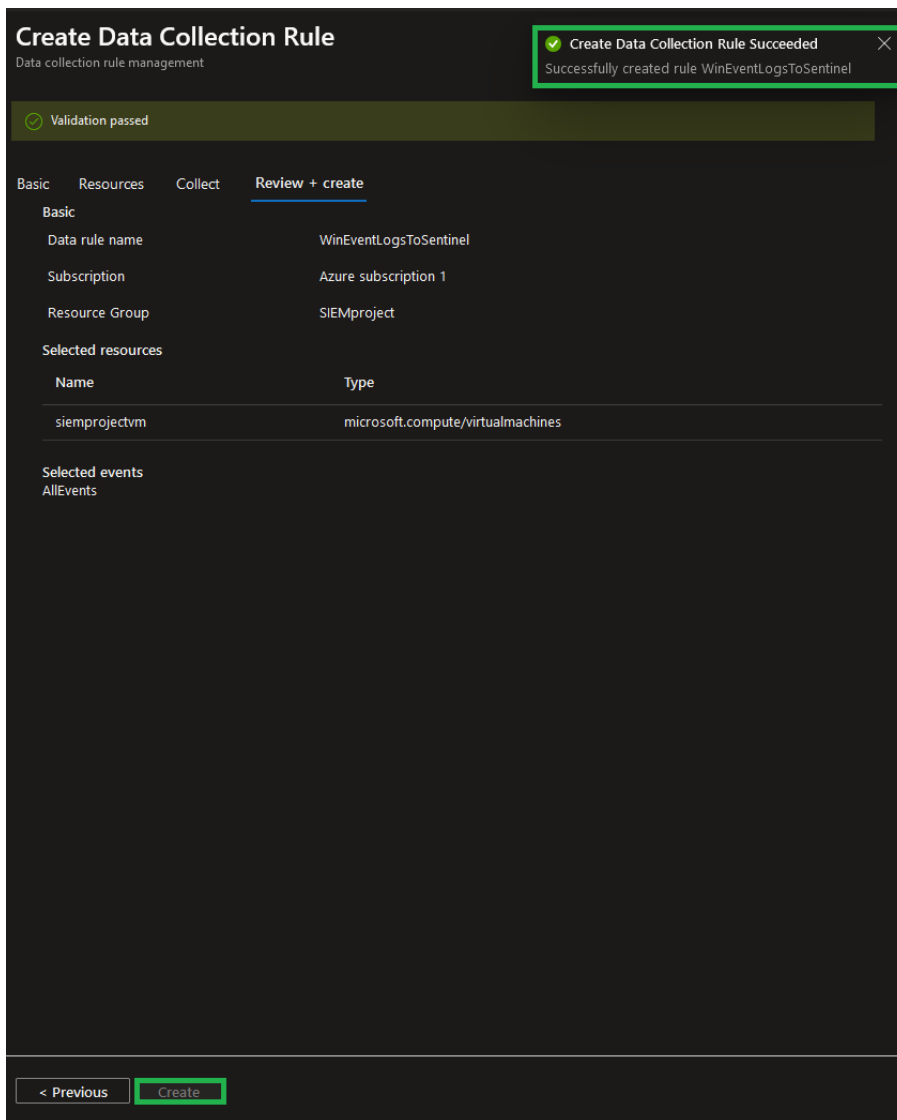
6. On the **Resources** tab, we select the subscription, resource group, and VM we wish to include and click on **Next: Collect**.



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

The screenshot shows a dark-themed dialog box titled "Create Data Collection Rule" with a close button (X) in the top right corner. Below the title is the subtitle "Data collection rule management". A horizontal tab bar at the top contains four tabs: "Basic", "Resources", "Collect" (which is selected and underlined), and "Review + create". Below the tabs, the text "Select which events to stream. ⓘ" is displayed. There are four radio button options: "All Security Events" (which is selected and highlighted with a red rectangle), "Common", "Minimal", and "Custom". At the bottom of the dialog, there are two buttons: "< Previous" and "Next: Review + create >" (which is highlighted with a red rectangle).

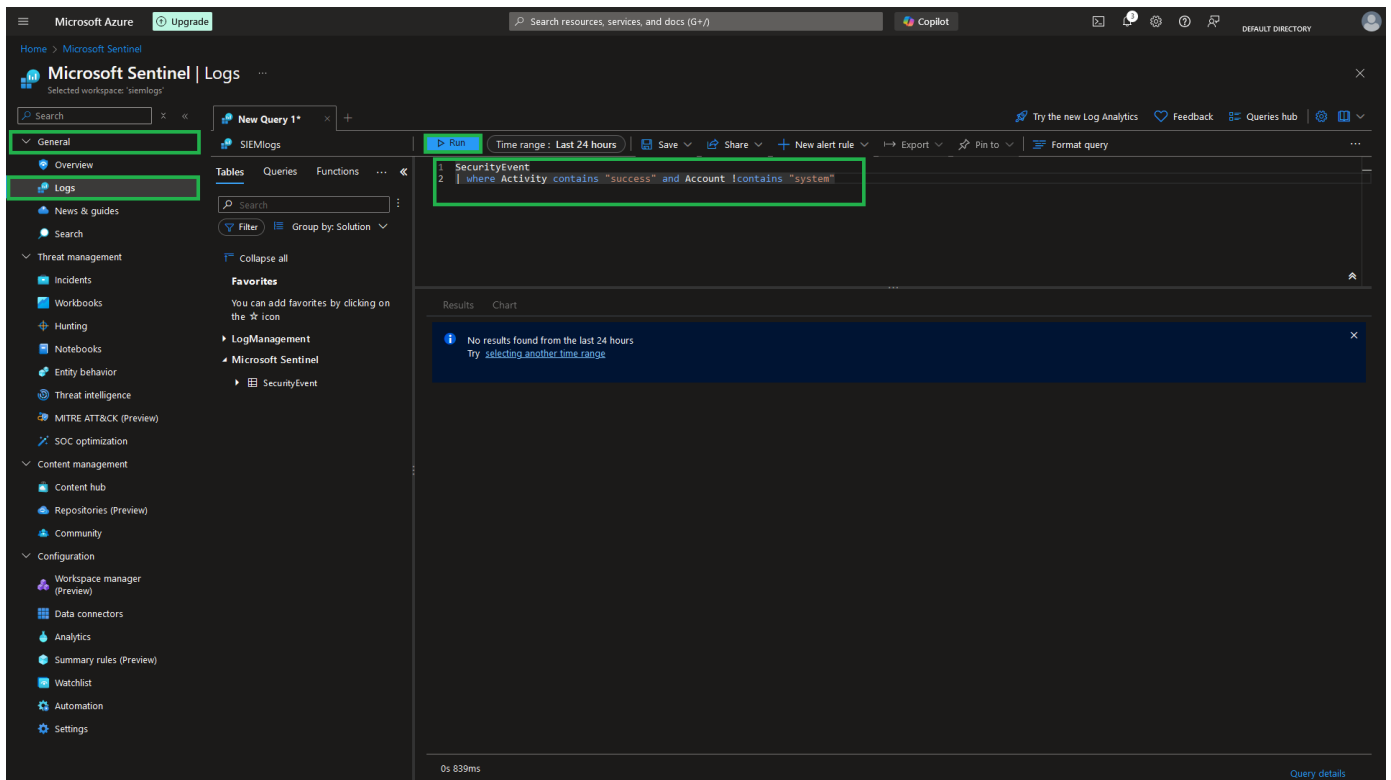
8. We then click on **Create** once more to finalize the process.



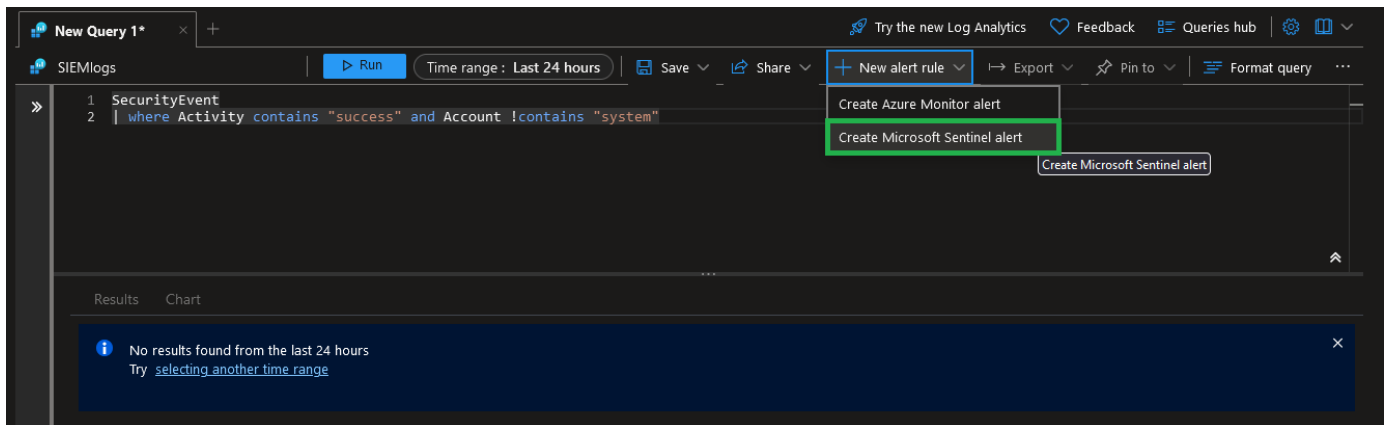
Task 4: Creating a Microsoft Sentinel scheduled rule and generating an incident

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"



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



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.

Microsoft Azure Upgrade

Home > Microsoft Sentinel | Logs >

Analytics rule wizard - Create a new Scheduled rule

General Set rule logic Incident settings Automated response Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *
Successful Local Sign Ins

Description
An administrator sign in has occurred on the Virtual Machine.

Severity
Medium

MITRE ATT&CK
Initial Access

Status
☒ Enabled

Next: Set rule logic >

- 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**.

Alert threshold

Generate alert when number of query results *

Is greater than 0

Event grouping

Configure how rule query results are grouped into alerts

☒ Group all events into a single alert

☐ Trigger an alert for each event

Suppression

Stop running query after alert is generated ⓘ

☐ Off

< Previous Next: Incident settings >

- 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**.

Analytics rule wizard - Create a new Scheduled rule

Validation passed.

General Set rule logic Incident settings Automated response **Review + create**

MITRE ATT&CK Initial Access

Severity Medium

Status Enabled

Analytics rule settings

Rule query SecurityEvent | where Activity contains "success" and Account !contains "system"

Rule frequency Run query every 5 minutes

Rule period Last 5 minutes data

Rule start time Automatic

Rule threshold Trigger alert if query returns more than 0 results

Event grouping Group all events into a single alert

Suppression Not configured

Entity mapping Not configured

Custom details Not configured

Alert details Not configured

Incident settings

Create incidents from this rule Enabled

Alert grouping Disabled

Automated response

Automation rules Not configured

< Previous 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.

Microsoft Azure Upgrade Search resources, services, and docs (0+)

Microsoft Sentinel Analytics

Selected workspace: Sentinel

Search

General Overview Logs News & guides Search Threat management Incidents Workbooks Hunting Notebooks Entity behavior Threat intelligence MITRE ATT&CK (Preview) SOC optimization Content management Content hub Repositories (Preview) Community Configuration Workspace manager (Preview) Data connectors Analytics Summary rules (Preview) Watchlist Automation Settings

2 Active rules More content at Content hub

Rules by severity High (1) Medium (1) Low (0) Informational (0)

Active rules Rule templates Anomalies

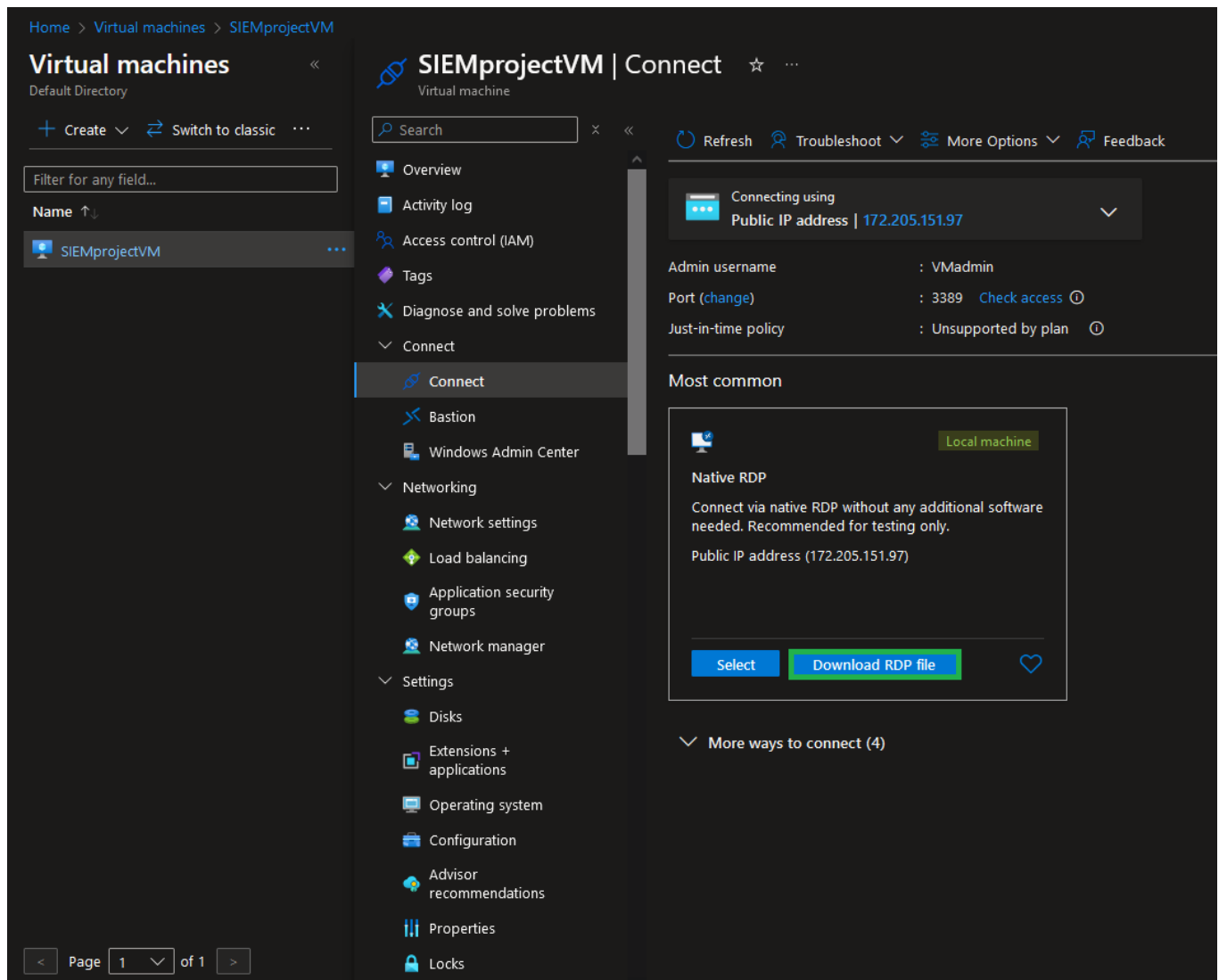
Search by ID, name, tactic or technique Add filter

Severity	Name	Rule L...	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Medium	Successful Loca...	Sd	Enabled	Initial Access			Custom Content	22/10/2024, 21...
High	Advanced Mult...	Fat	Enabled	Collection *11			Gallery Content	22/10/2024, 18...

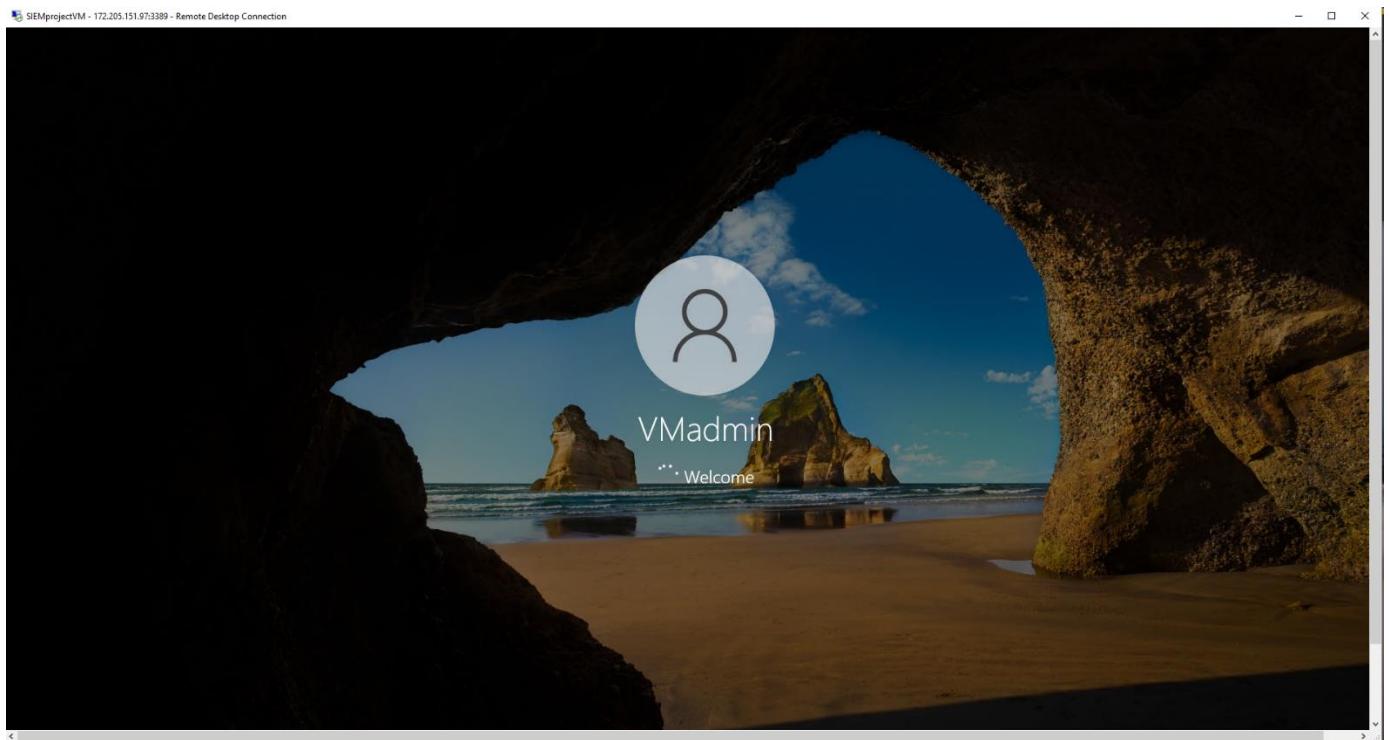
No analytics rules selected
Select an analytics rule to view more details

Previous Page 1 of 1 Next Showing 1 to 2 of 2 results

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**.



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

Successful Local Sign Ins
Incident number 2

Description
An administrator sign in has occurred on the Virtual Machine.

Alert product names
• Microsoft Sentinel

Evidence
3 Events, 1 Alerts, 0 Bookmarks

Last update time
22/10/24, 22:37

Creation time
22/10/24, 22:37

Entities (0)
-

Tactics and techniques
Initial Access (0)

Incident workbook
Incident Overview

Analytics rule
Successful Local Sign Ins

Tags
-

The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alerts. [Learn more](#)

[View full details](#) [Actions](#)

We can now use this VM as an RDP honeypot.

Azure security project solution PART 2:

Creating a threat intelligence feed using MISP

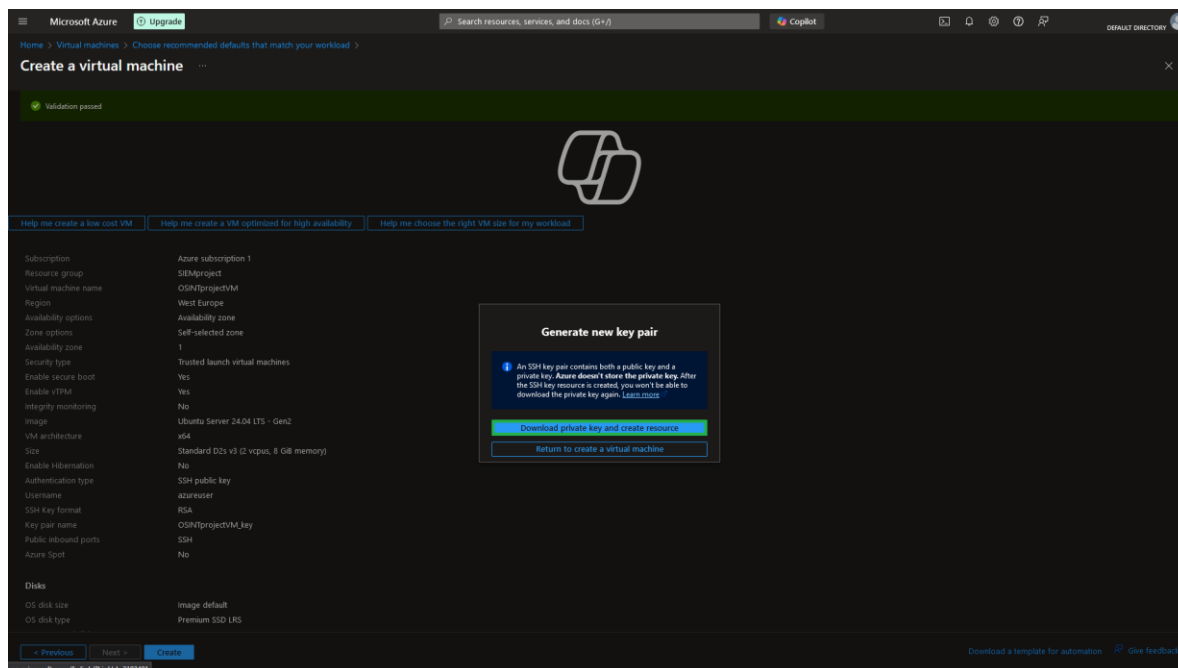
We will now setup a custom OSINT data feed to our Sentinel instance. Microsoft does have its own threat intelligence instance, but for this project we will be using the MISP open-source threat intelligence platform.

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

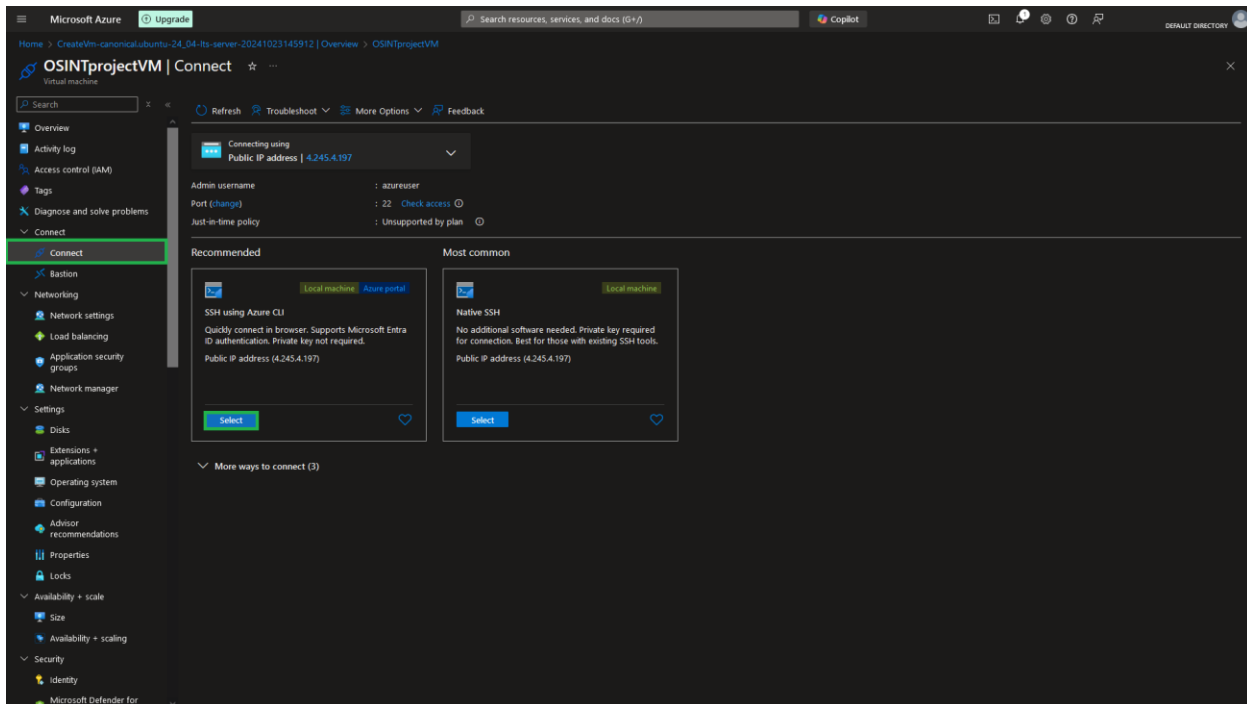
1. We begin by creating another preset virtual machine with these specifications. The rest can be leave at their default values.

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

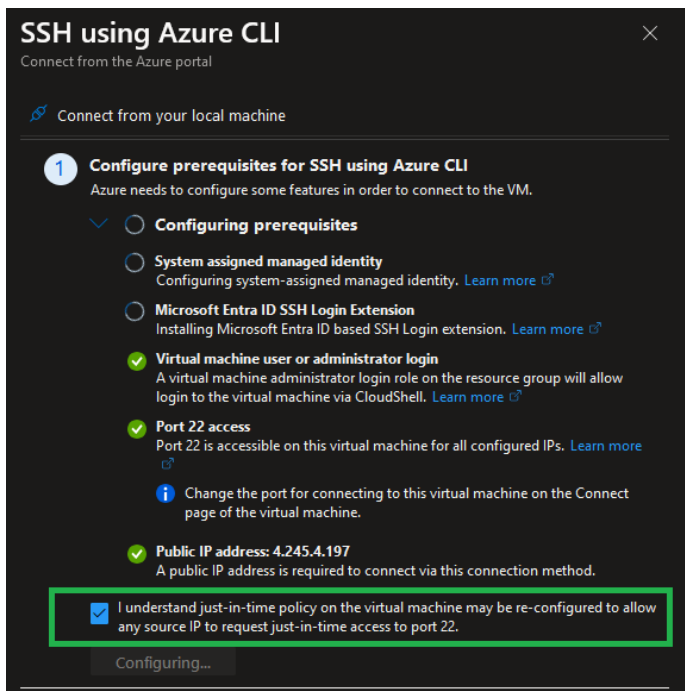
2. We then click on **Download private key and create resource** when prompted.



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.



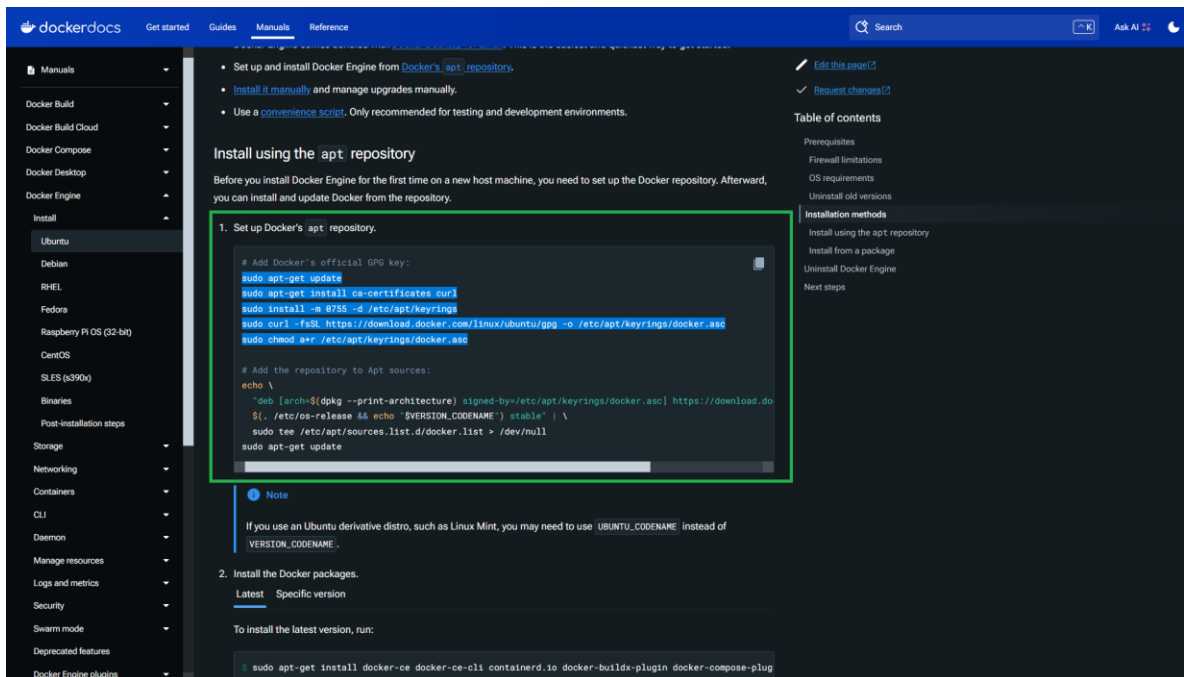
5. When the shell opens, we will be prompted to confirm we would like to continue connecting and input “yes”.

```
Switch to PowerShell Restart Manage files New session Editor Web preview Settings Help
Connecting terminal...
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

sibill [ ~ ]$ az ssh vm --resource-group SIEMproject --vm-name OSINTprojectVM --subscription 1c231d77-b506-4287-925c-aba83bffa6fb
OpenSSH 8.9p1, OpenSSL 1.1.1.k 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:jVt1c3//XLioTW2N0hbVY8Uoce5xHnQilPAsJ/kDhUs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

6. 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.



7. 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
```

8. 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 7EA0A9C3F273FCD8
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 7EA0A9C3F273FCD8
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-get(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*.

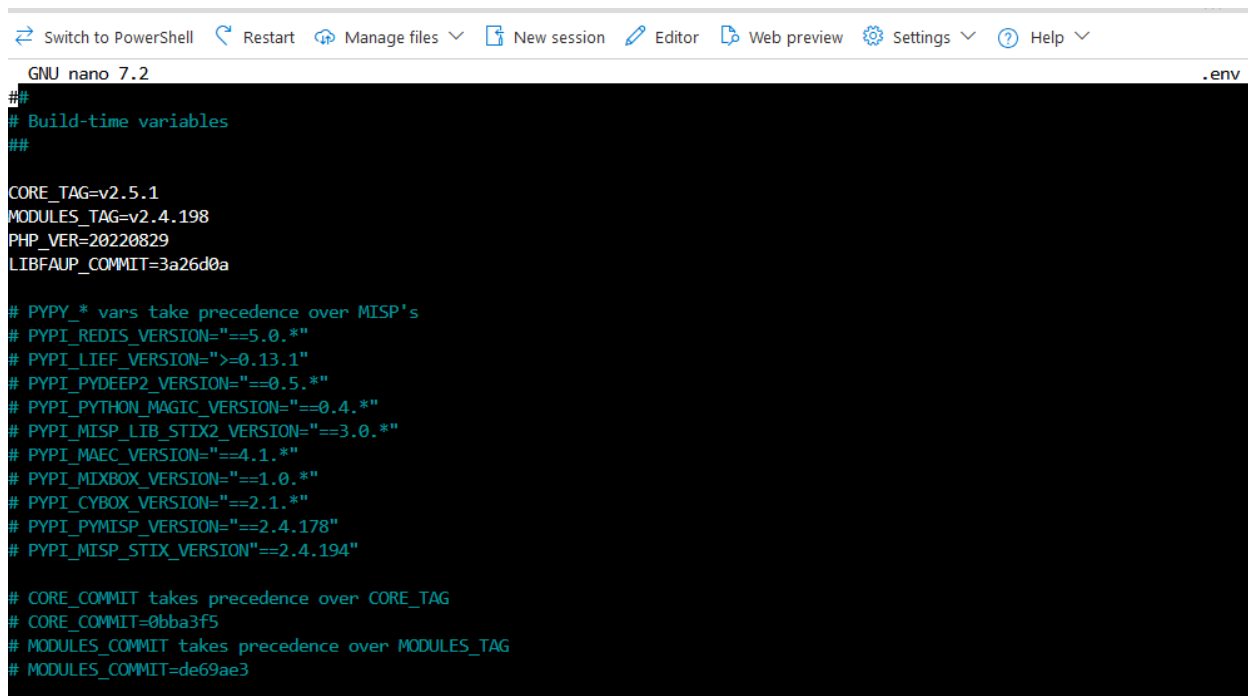
```
$ dir
misp-docker
$
```

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.



The screenshot shows a terminal window with the nano 7.2 editor open. The editor displays the contents of the *.env* file, which includes build-time variables and precedence rules. The variables are defined as follows:

```
##
# 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_MAEK_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.

```
Switch to PowerShell Restart Manage files New session Editor Web preview Settings Help
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://4.245.4.191
# 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
misp[0000] The "PROXY_METHOD" variable is not set. Defaulting to a blank string.
misp[0000] The "PROXY_USER" variable is not set. Defaulting to a blank string.
misp[0000] The "PROXY_PASSWORD" variable is not set. Defaulting to a blank string.
misp[0000] The "REDIRECT" variable is not set. Defaulting to a blank string.
misp[0000] The "SMTP_FQDN" variable is not set. Defaulting to a blank string.
misp[0000] The "PHP_SESSION_COOKIE_DOMAIN" variable is not set. Defaulting to a blank string.
misp[0000] The "HSTS_MAX_AGE" variable is not set. Defaulting to a blank string.
misp[0000] The "X_FRAME_OPTIONS" variable is not set. Defaulting to a blank string.
misp[0000] The "CONTENT_SECURITY_POLICY" variable is not set. Defaulting to a blank string.
misp[0000] The "CORE_COMMIT" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_REDIS_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_LTEF_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_PWDREP2_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_PYTHON_MAGIC_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_MISP_LTB_STD2_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_PMAC_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_PMDR_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_CYRUS_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_PMMISP_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "PVP1_MISP_STIX_VERSION" variable is not set. Defaulting to a blank string.
misp[0000] The "MODULES_COMMIT" variable is not set. Defaulting to a blank string.
misp[0000] /root/.misp-docker/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Pulling 5/5
✓ redis Pulled 62.5s
✓ misp-modules Pulled 97.0s
✓ mail Pulled 39.2s
✓ db Pulled 62.4s
✓ misp-core Pulled 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...`

```
Switch to PowerShell Restart Manage files New session Editor Web preview Settings Help
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.
misp-core-1 INIT | Configure PHP ...
misp-core-1 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
misp-core-1 2024-10-23 14:08:35,230 WARN stopped: php-fpm (exit status 143)
misp-core-1 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
misp-core-1 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*.

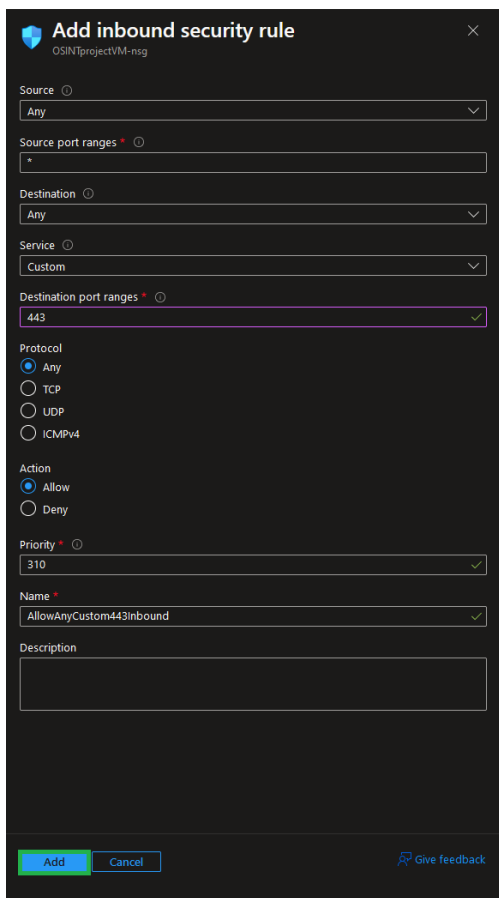
```
^Z[1] + Stopped
$ sudo docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                               NAMES
eo771b57dbc   ghcr.io/misp/misp-docker/misp-core:latest "/entrypoint.sh"        7 minutes ago Up 7 minutes (unhealthy) 0.0.0.0:80->80/tcp, :::80->80/tcp, 0.0.0.0:443->443/tcp, :::443->443/tcp misp-docker-misp-core-1
1d702851d7fc   ghcr.io/misp/misp-docker/misp-modules:latest "/usr/local/bin/misp.."  7 minutes ago Up 7 minutes (unhealthy) 0.0.0.0:80->80/tcp, :::80->80/tcp, 0.0.0.0:443->443/tcp, :::443->443/tcp misp-docker-misp-modules-1
e267c9d1212e   1xdotai/sntp                        "/bin/entrypoint.sh .."  7 minutes ago Up 7 minutes (healthy) 25/tcp misp-docker-mail-1
d49d1e47436a   valley/vallkey:7.2                 "docker-entrypoint.s.."  7 minutes ago Up 7 minutes (healthy) 6379/tcp misp-docker-redis-1
6d793207f8d7   mariadb:10.11                      "docker-entrypoint.s.."  7 minutes ago Up 7 minutes (healthy) 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 the 'OSINTProjectVM' virtual machine. The 'Network settings' page is open, displaying the 'Rules' section. A new inbound port rule is being created, with the name '0.0.0.0:443->443/tcp' highlighted in green. The rule is configured for TCP protocol, allowing traffic from any source to any destination. The 'Create port rule' button is also highlighted in green.

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	VirtualNetwork	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

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



The screenshot shows the 'Add inbound security rule' dialog box in Windows Firewall. The configuration is as follows:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Service:** Custom
- Destination port ranges:** 443
- Protocol:** Any (selected)
- Action:** Allow (selected)
- Priority:** 310
- Name:** AllowAnyCustom443inbound
- Description:** (empty text box)

At the bottom, there are 'Add' and 'Cancel' buttons, and a 'Give feedback' link.

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.



Login

Email

Password

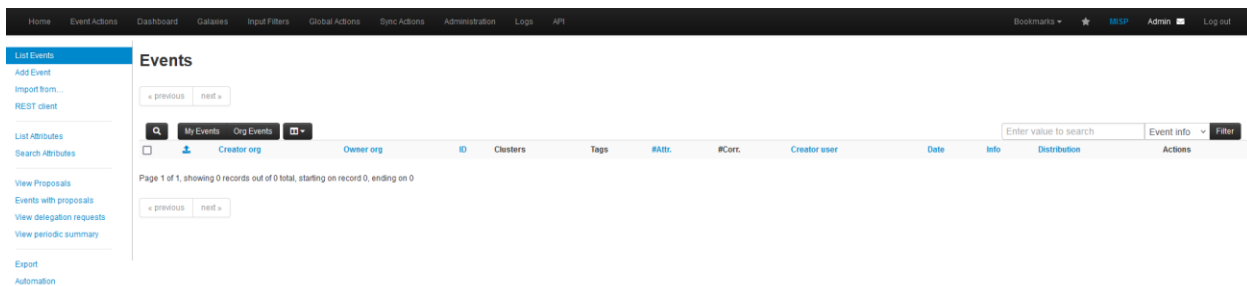
Download: [Server PDF public key](#)

Powered by MISP - 2024-10-22 14:36:13

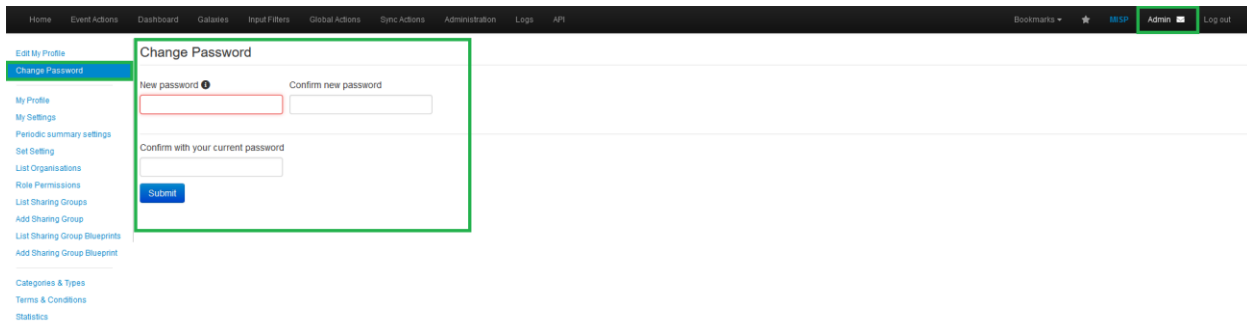
16. We log in using the following credentials:

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

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

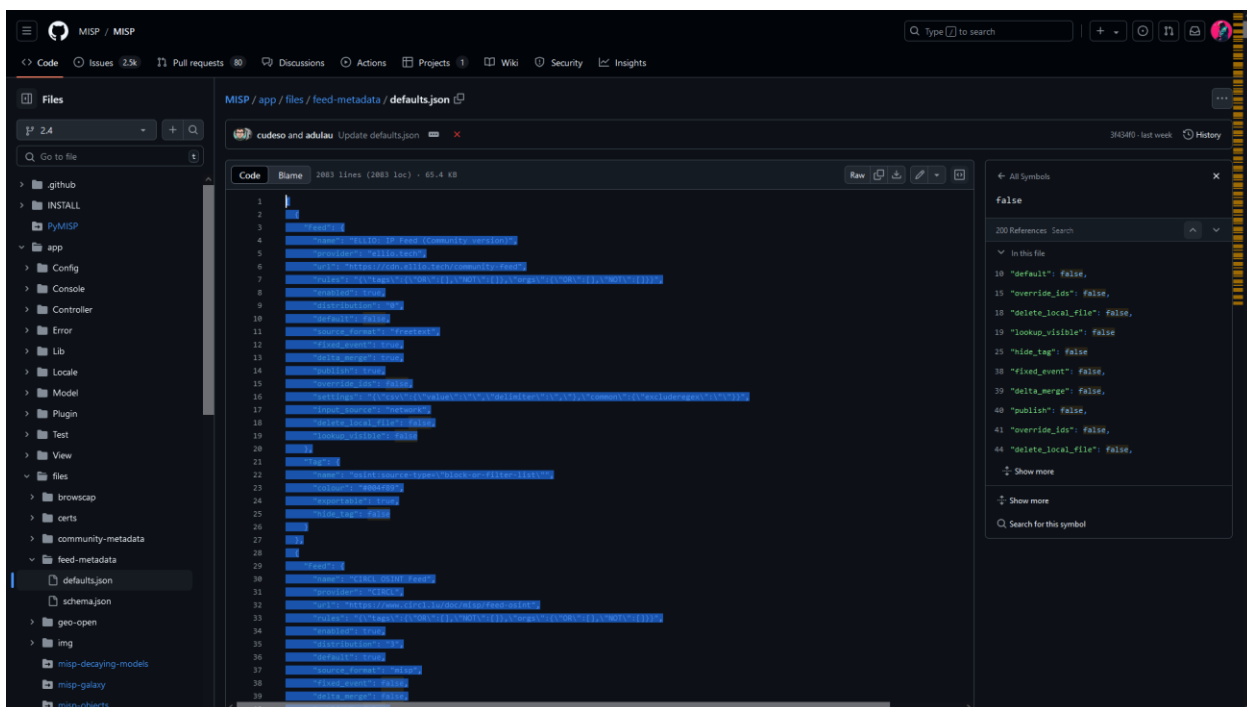


18. Since this is a public-facing server, it is highly recommended to change our admin password. This is done by clicking on **Admin** at the top-right, then going to **Change Password** and selecting new password.

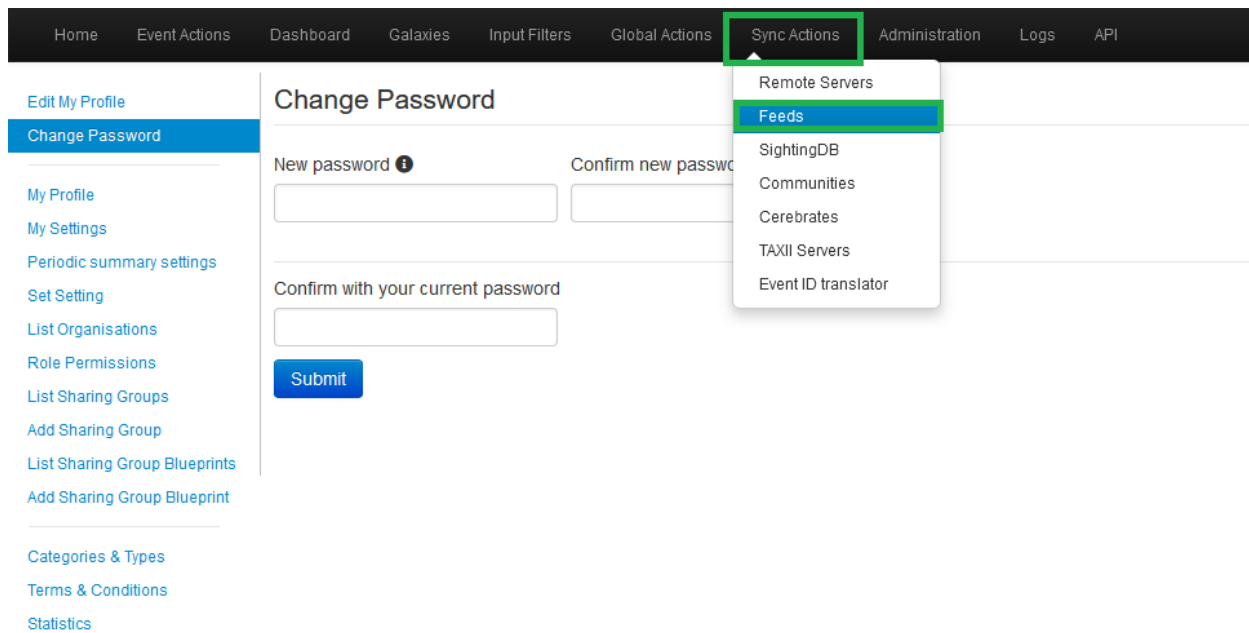


19. We now have to enable the OSINT feeds. To do this, we first go to www.misp-project.org/feeds/ or directly from GitHub at <https://github.com/MISP/MISP/blob/2.4/app/files/feed-metadata/defaults.json>.

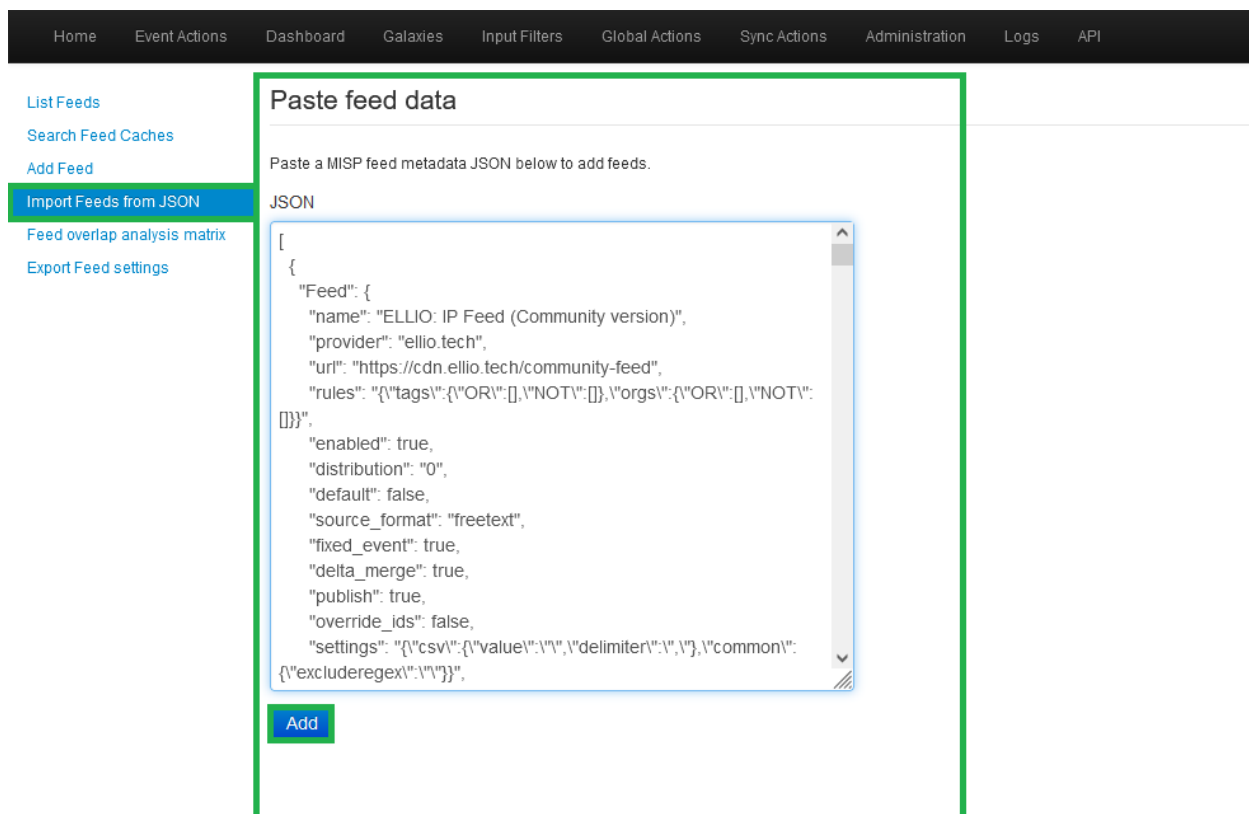
20. We copy the contents of the JSON file.



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



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

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

Scheduled Tasks
Event Block Rules

Blocklists Event
Manage Event Blocklists

Blocklists Organisation
Manage Org Blocklists

Blocklists Sightings
Manage Sighting Blocklists

Jobs

Purge job entries: **Completed** **All**

« previous 1 2 3 4 5 next »

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	6f5a87e-1c72-4975-920c-90a62302d0fe	email	publish_alert_email	Event 1	Mails sent	ADMIN	Completed	Completed
84	2024-10-23 15:12:53	2024-10-23 15:12:53	66ca234-4873-480e-a8c5-1f6852e37449	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	8093de9-b5fa-432e-ba82-91af04379110	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-46c1-4679-8685-35e0a4d709f	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	5daea96-64e6-459e-b31c-0433408a1ad	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	623ab80d-a1e7-4200-9a84-c80b79d5328	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	ea36d34-3676-40c3-df65-b5303e4a202	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	e8f1ae9e-79a3-485f-8a6b-7e09f5ae123	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	c45d9156-5005-401e-a4d7-48770249858e	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	cd88eeb-309f-4866-bacd-99931385a0b	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	15502e4-42a0-43ab-b0ca-983a7e1f8ce	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	d20e8a0e-3a27-4a00-041a-3c76cd5deb0b	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	dd6c3012-ea84-42de-98a9-60d6087d57d	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	0221ec02-194e-4dda-bca7-629407a85351	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	b349f05-2605-4a8b-8111-41a6ca49c039	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	8f94da88-a91b-419f-9305-188dbf59959	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	cd584a0-38b5-4c96-90fa-1bc12d1c073e	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	fa761f8f-8347-4321-b420-ectd8ed8a23	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	b79e418d-43d2-4647-a113-997872064c1	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	ad2be161-4114-4193-d293-d95597d30c8	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

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests
View periodic summary

Export
Automation

Events

« previous 1 2 3 next »

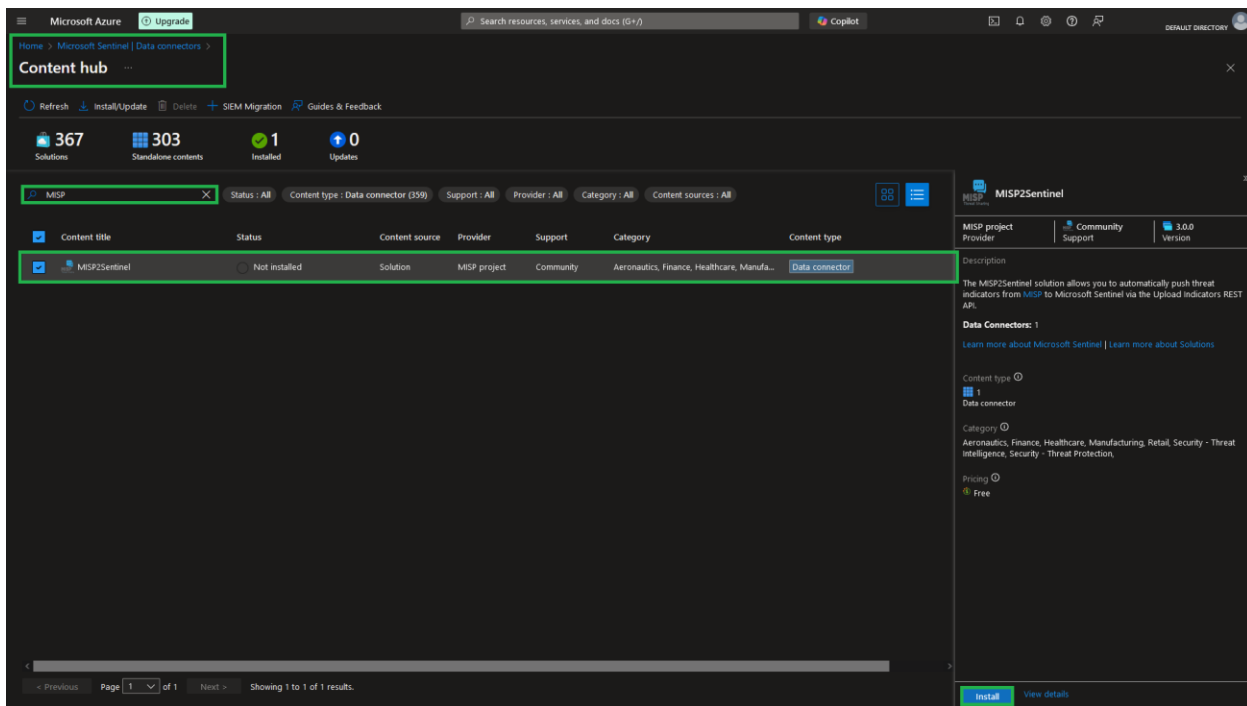
Q	My Events	Org Events	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
☐	☒	☐	7 117			1		admin@admin.test	2024-10-23	Feedo IP Blocklist feed	Organisation	
☒	☒	☐	7 3		osint:source-type="block-or-filter-list"	9970	3	admin@admin.test	2024-10-23	ELLIO IP Feed (Community version) feed	Organisation	
☐	☒	☐	7 68			5600	2	admin@admin.test	2024-10-23	pop3gprogs feed	Organisation	
☐	☒	☐	7 36		osint:source-type="block-or-filter-list"	1731		admin@admin.test	2024-10-23	diamondfor_panels feed	Organisation	
☒	☒	☐	7 33		osint:source-type="block-or-filter-list"	2		admin@admin.test	2024-10-23	ip-block-list - snort.org feed	Organisation	
☐	☒	☐	7 2		osint:source-type="block-or-filter-list"	2119	4	admin@admin.test	2024-10-23	Tor exit nodes feed	Organisation	
☐	☒	☐	7 7			8700	4	admin@admin.test	2024-10-23	Tor ALL nodes feed	Organisation	
☐	☒	☐	7 4		osint:source-type="block-or-filter-list"	604	1	admin@admin.test	2024-10-23	blockrules of rules.emergingthreats.net feed	Organisation	
☒	☒	☐	7 21		tpc:white	13		admin@admin.test	2015-12-01	LOWBOW - FireEye	All	
☒	☒	☐	7 15		tpc:white	79		admin@admin.test	2015-09-15	In Pursuit of Optical Fibers and Troop Intel: Targeted Attack Distributes PlugX in Russia	All	
☒	☒	☐	7 8		tpc:white	8		admin@admin.test	2015-11-16	WitchCoven: Exploiting Web Analytics to Ensnare Victims	All	
☒	☒	☐	7 31		tpc:white	16		admin@admin.test	2015-06-14	New Sofacy Attacks Against US Government Agency	All	
☒	☒	☐	7 25		tpc:white	8		admin@admin.test	2021-09-11	Maldoc Cybersecurity in the EU Common Security and Defense Policy	All	
☐	☒	☐	7 12		tpc:white	66		admin@admin.test	2016-04-21	Looking Into a Cyber-Attack Facilitator in the Netherlands	All	
☒	☒	☐	7 36		tpc:white	36		admin@admin.test	2015-10-16	Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites - Citizen Lab	All	
☐	☒	☐	7 20		tpc:white	133	1	admin@admin.test	2015-12-08	Pacifrat: Seven Years of a South American Threat Actor	All	
☒	☒	☐	7 122		tpc:white	10		admin@admin.test	2017-07-24	Real News, Fake Flash: Mac OS X Users Targeted	All	
☒	☒	☐	7 121		tpc:white	5		admin@admin.test	2017-07-06	New KCONI Campaign References North Korean Missile Capabilities	All	
☒	☒	☐	7 120		tpc:white	4		admin@admin.test	2017-06-22	Following the Trail of BlackTech36™s Cyber Espionage Campaigns	All	
☒	☒	☐	7 119		tpc:white	13		admin@admin.test	2017-06-16	Monkee Discovers Phishingbot Exploiting Infected Machines as Control Servers; Releases Free Tool to Detect, Disable Trojan	All	
☒	☒	☐	7 118		tpc:white	15		admin@admin.test	2017-06-12	Industroyer: Biggest threat to industrial control systems since Stuxnet	All	
☒	☒	☐	7 116		tpc:white	74		admin@admin.test	2017-05-26	TrickBotK™s bag of tricks	All	

Download: Server PGP public key

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

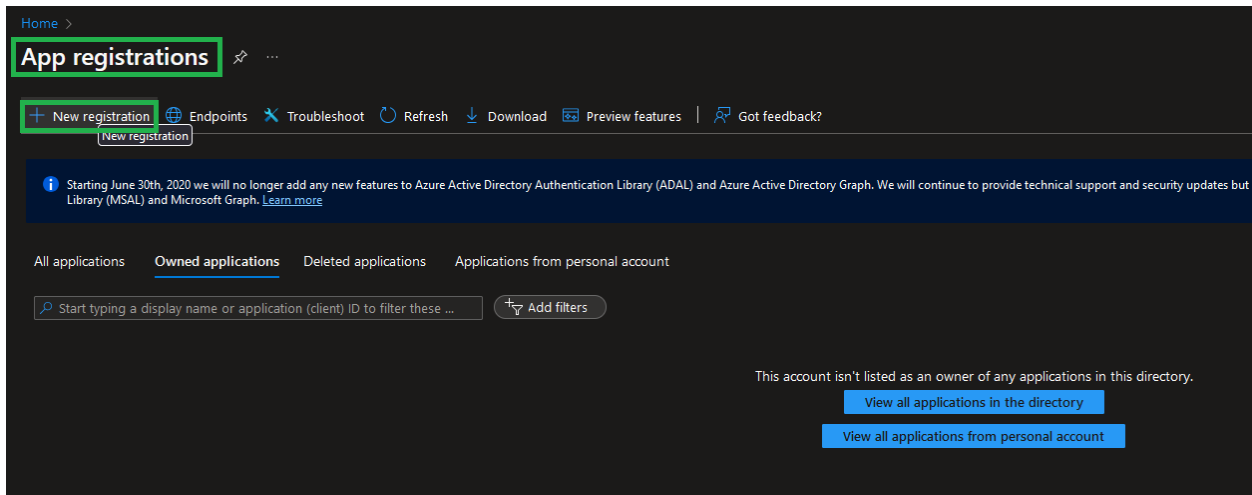
Task 7: Connecting our MISP data feed to Microsoft Sentinel

1. 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**.



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

- 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**.



- 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 [Register](#) you agree to the Microsoft Platform Policies.

[Register](#)

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

Home > App registrations >

MispToSentinelApp

Search ✕ << Delete Endpoints Preview features

Overview

Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets

Essentials

Display name : [MispToSentinelApp](#)

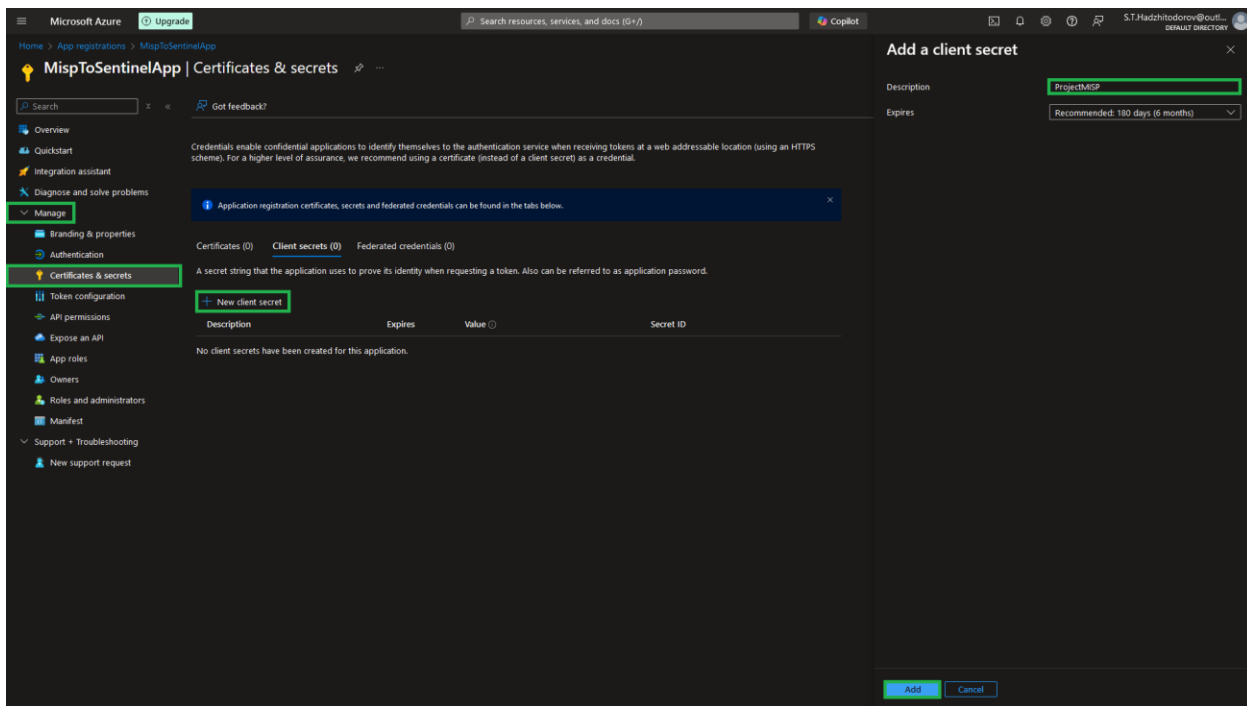
Application (client) ID : 94640c5a-036a-49f4-b700-e9e37ab4f196

Object ID : b31398ff-af0d-4904-bd3d-5122f0ea52b3

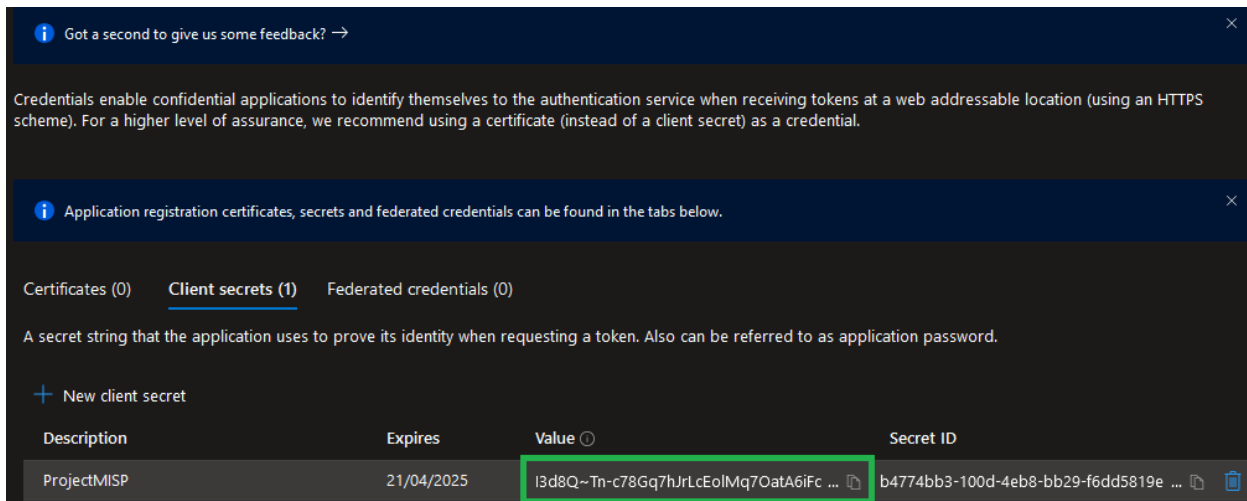
Directory (tenant) ID : 1714a8fd-e656-4185-8c3d-06e3b4b615ba

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

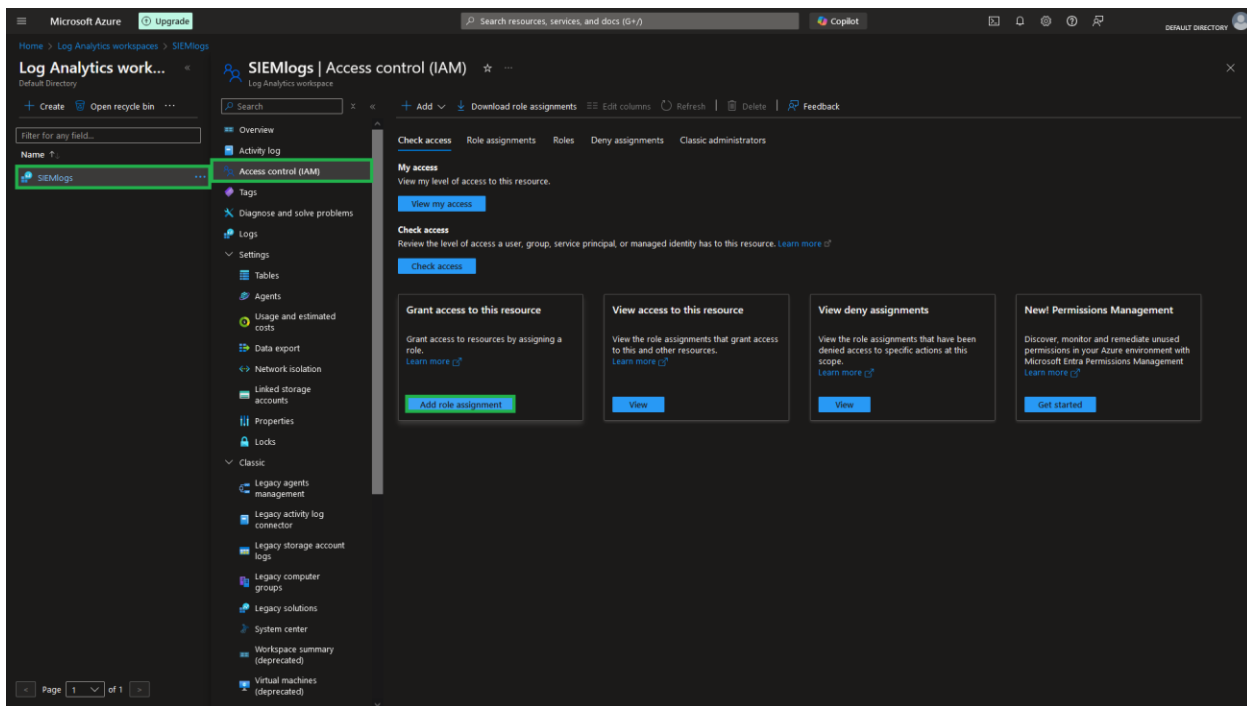
5. We then go to the **Certificates & secrets** page under the *Manage* blade, select **New client secret**, name it, and click on **Add**. We can leave the default expiry time.



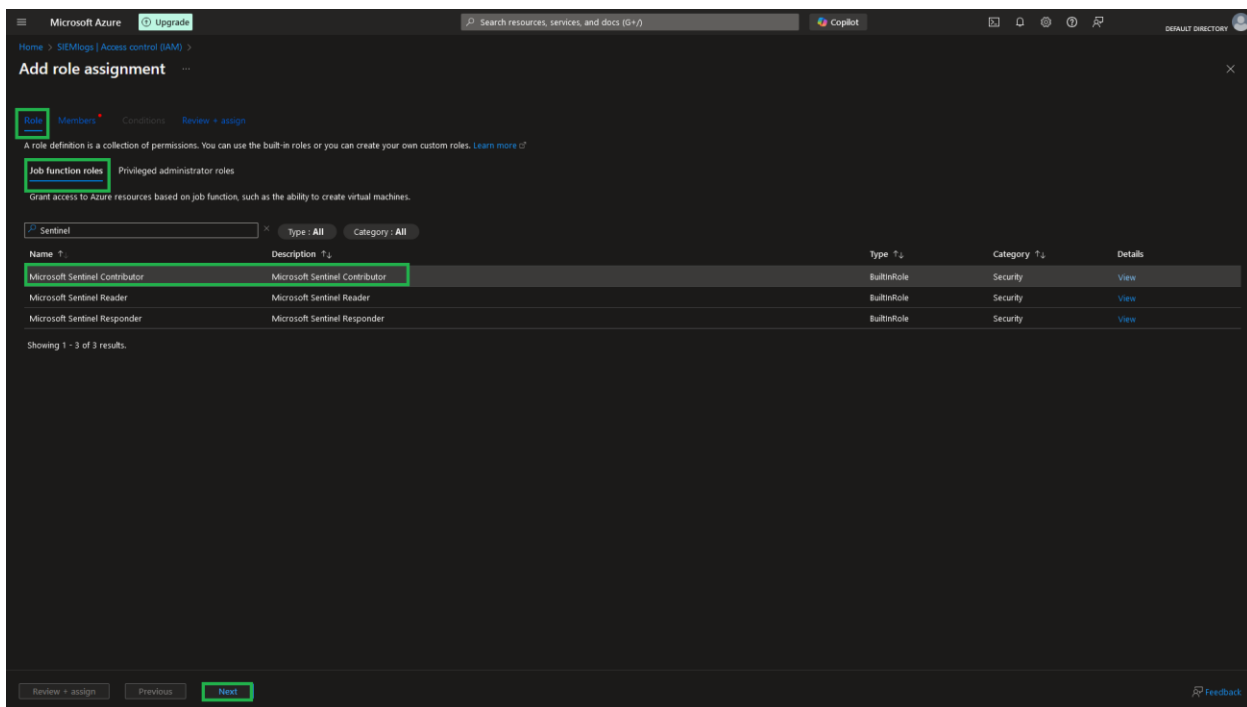
6. Now that it is created, we make sure to copy our secret's value, as it **will not be shown again**.



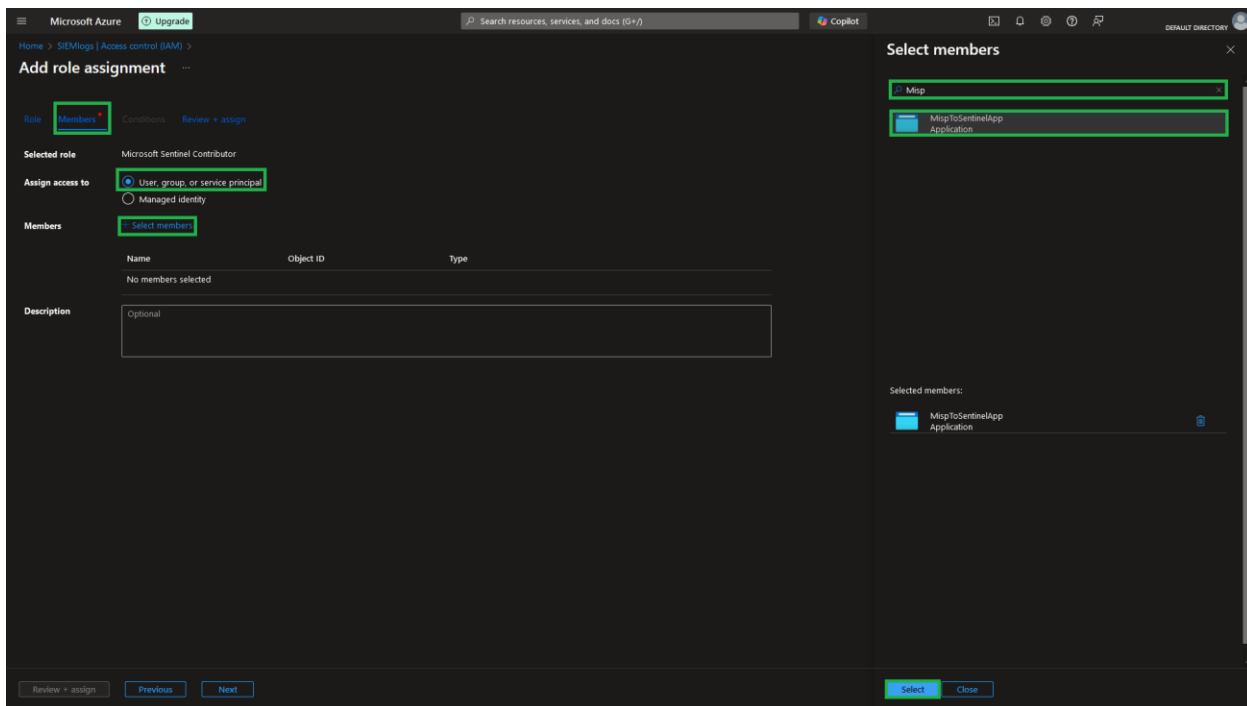
7. Now we need to add the Sentinel Contributor role to the app. We do this by going into the Log Analytics workspace our Sentinel instance is in, in this case **SIEMlogs**, navigating to the **Access control (IAM)** page, and clicking on **Add role assignment**.



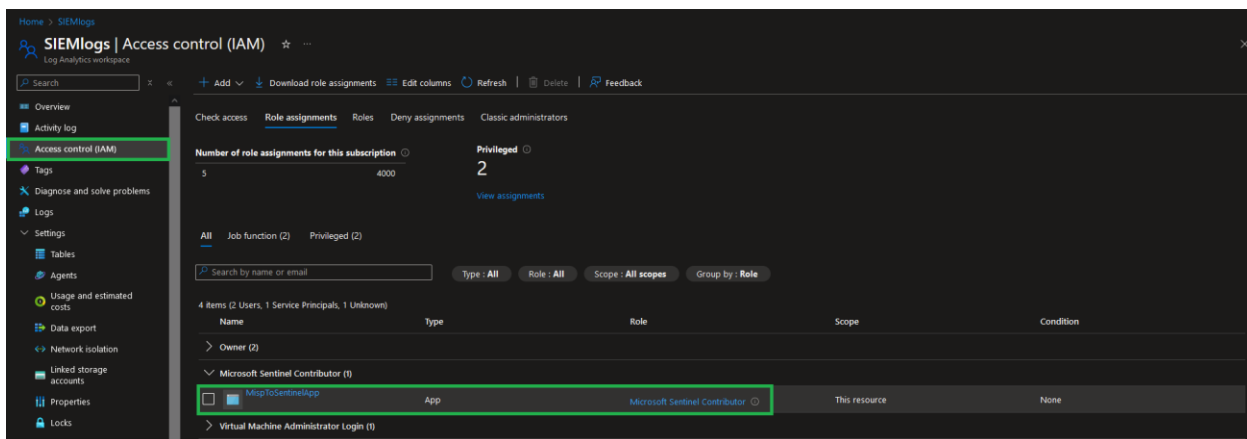
8. We now search for the Microsoft Sentinel Contributor role on the **Role** tab, select it, and click **Next**.



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.

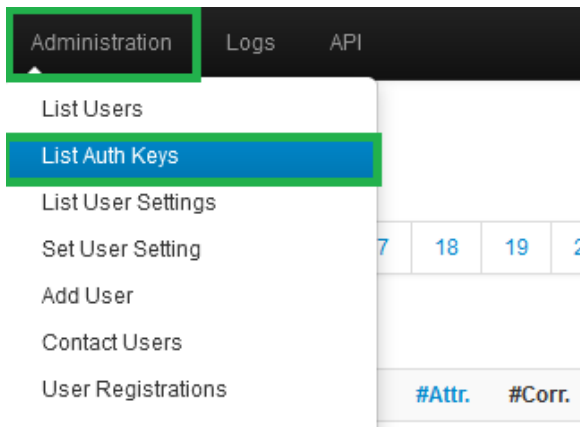


10. We then click on **Review + assign** and it should now show up on the **Access control (IAM)** page of the Log Analytics workspace.

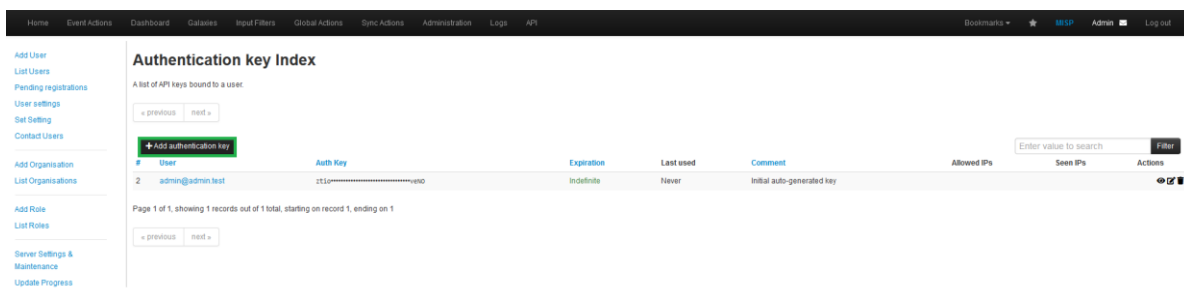


11. We need to create a MISP API Key. To do this, we go back to our MISP instance, hover over **Administration**, and click on **List Auth Keys**.

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

admin@admin.test

Comment

Allowed IPs

Expiration (keep empty for indefinite)

YYYY-MM-DD

☐ 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**.

Auth key created

Please make sure that you note down the auth key below, this is the only time the auth key is shown in plain text, so make sure you save it. If you lose the key, simply remove the entry and generate a new one.

MISP will use the first and the last 4 characters for identification purposes.

dSDK1Znk5wjay8vEoPPM6LbNTtCG1RJccwSq1bsT

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**.

Microsoft Azure

Search resources, services, and docs (Ctrl+K)

Function App

Create

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Filter for any field...

Subscription equals all

Resource group equals all

Location equals all

Add filter

No grouping

List view

Showing 0 to 0 of 0 records.

Name

Status

Location

Pricing Tier

App Service Plan

Subscription

App Type

No function apps match your filters

Try changing or clearing your filters.

Create Function app

Clear filters

Learn more about App Service

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

Create Function App

Select a hosting option

These options determine how your app scales, resources available per instance, and pricing. [Learn more about Functions hosting options.](#)

Hosting plans	Consumption	Flex Consumption	Functions Premium	App Service	Container Apps environment
Scale to zero	✓	✓	-	-	✓
Scale behavior	Event-driven	Fast event-driven	Event-driven	Metrics based	Event-driven with KEDA
Virtual networking	-	✓	✓	✓	✓
Dedicated compute and prevent cold start	-	Optional with Always Ready	Minimum of 1 instance required	Minimum of 1 instance required	Optional with minimum replicas
Max scale out (instances)	200	1000	100	40-60	300

Select

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 * ⓘ Azure subscription 1 ✓

Resource Group * ⓘ SIEMproject ✓
[Create new](#)

Instance Details

Function App name * MISP2Sentinel ✓
azurewebsites.net

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

Runtime stack * Python ✓

Version * 3.11 ✓

Region * West Europe ✓

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) * ⓘ (New) ASP-SIEMproject-92d3 ✓
[Create new](#)

Pricing plan Premium V3 P1V3 (195 minimum ACU/vCPU, 8 GB memory, 2 vCPU) ✓
[Explore pricing plans](#)

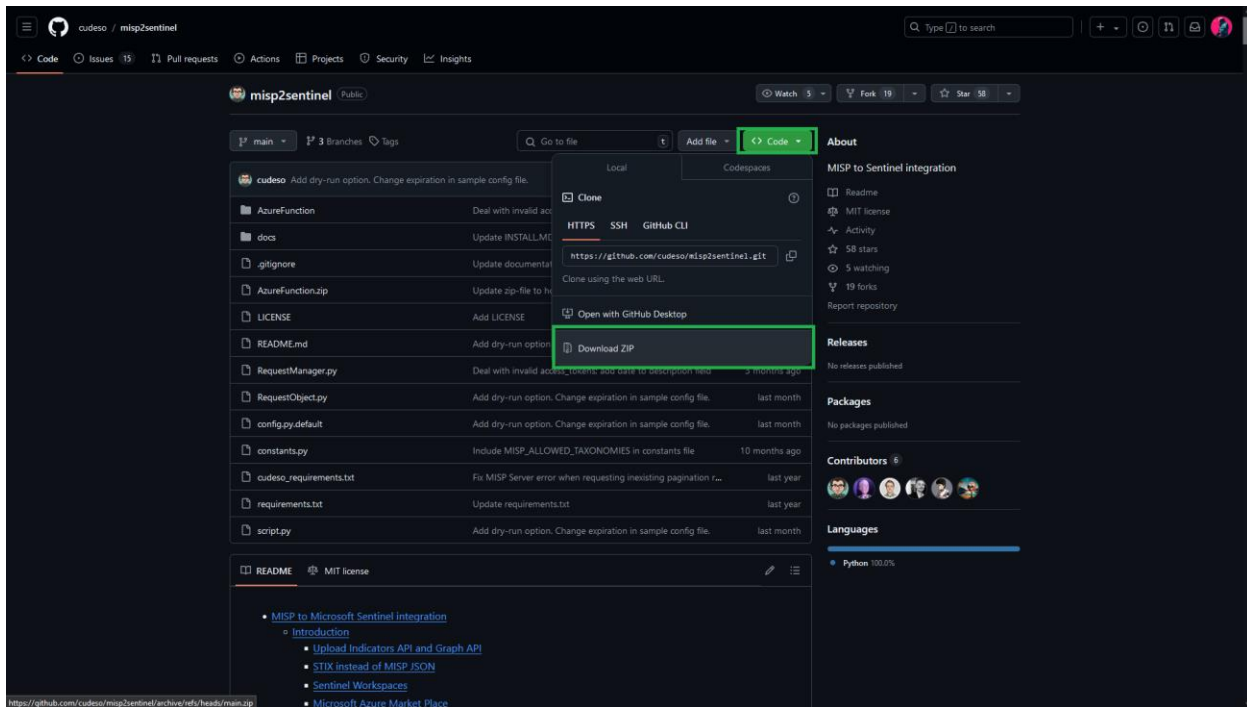
Zone redundancy

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](#) ⓘ

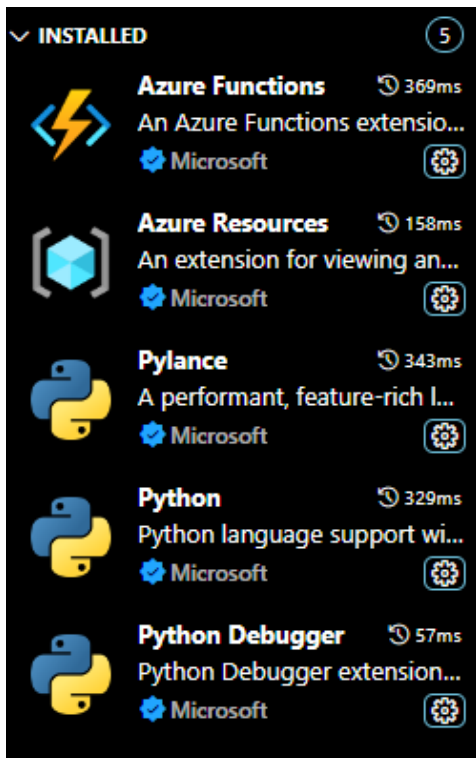
Zone redundancy ☐ **Enabled:** Your App Service plan and the apps in it will be zone redundant. The minimum App Service plan instance count will be three. ☒ **Disabled:** Your App Service Plan and the apps in it will not be zone redundant. The minimum App Service plan instance count will be one.

[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 MISP2Sentinel.config as config
3 from collections import defaultdict
4 from MISP2Sentinel.RequestManager import RequestManager
5 from MISP2Sentinel.RequestObject import RequestObject, RequestObject_Event, RequestObject_Indicator
6 from MISP2Sentinel.constants import *
7 import sys
8 from functools import reduce
9 import os
10 import datetime
11 from datetime import datetime, timedelta, timezone
12 import logging
13 import azure.functions as func
14 import requests
15 import json
16 from misp_stix_converter import MISPToSTIX2IParser
17 from stix2.base import STIXSONEncoder
18
19 if config.misp_verifycert is False:
20     import urllib3
21     urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
22
23
24 def _get_misp_events_stix():
25     logging.info("Using the following values for MISP API call: domain: {config.misp_domain}, misp_api_key: {config.misp_key[:5]} + '*' + '*' + '*' + '*' + '*'...")
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 "limit" 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 = MISPToSTIX2IParser()
45                     parser.parse_misp_event(event)
46                     stix_objects = parser.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)

```

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

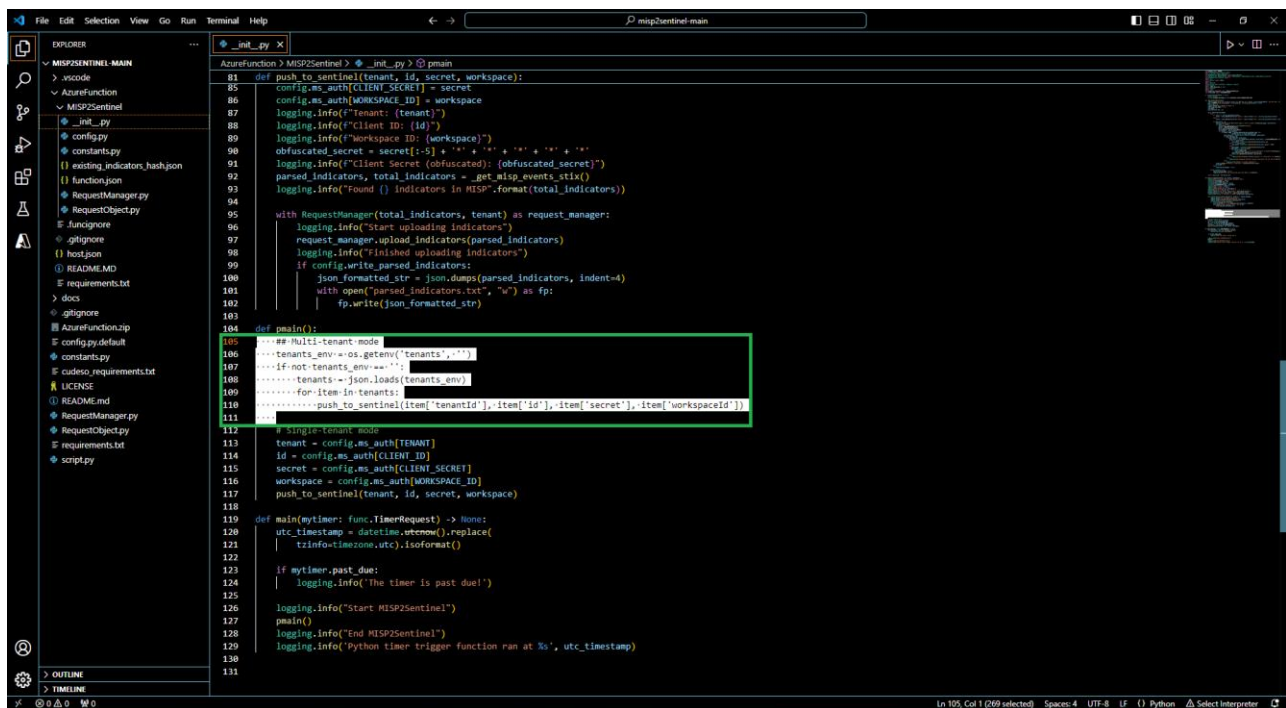
I. We go to the **config.py** file and change 'MISP-Key' to 'mispkey'.

```

34 # Log in with the virtual machines managed identity
35 credential = DefaultAzureCredential()
36 client = SecretClient(vault_url=KVURI, credential=credential)
37
38 # Retrieve values from KV (client secret, MISP-key most importantly)
39 retrieved_mispkey = client.get_secret('MISP-Key')
40 retrieved_clientsecret = client.get_secret('ClientSecret')
41
42 # Set values with
43 mispkey = retrieved_mispkey.value
44 ms_auth['client_secret'] = retrieved_clientsecret.value
45
46 elif:
47     print('key_vault_name env variable not set, falling back to env variable for config values....')
48     mispkey= os.getenv('mispkey')
49
50 #####
51 # Microsoft Section #
52 #####
53 ms_max_indicators_request = 100 # Throttle max: 100 indicators per request
54 ms_max_requests_minute = 100 # Throttle max: 100 requests per minute
55 ms_useragent = "MISP-1.0"
56 ms_target_product = "Azure Sentinel" # targetProduct
57 ms_api_version = "2022-07-01" # Upload Indicators API version
58
59 # Graph API only settings
60 ms_passiveonly = False # passiveOnly
61 ms_action = "alert" # action
62
63 #####
64 # MISP Section #
65 #####
66
67 # MISP API settings
68 misp_key = mispkey
69 misp_domain = mispurl

```

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.

Functions

Metrics

Properties

Notifications (0)

{ }

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
client_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.

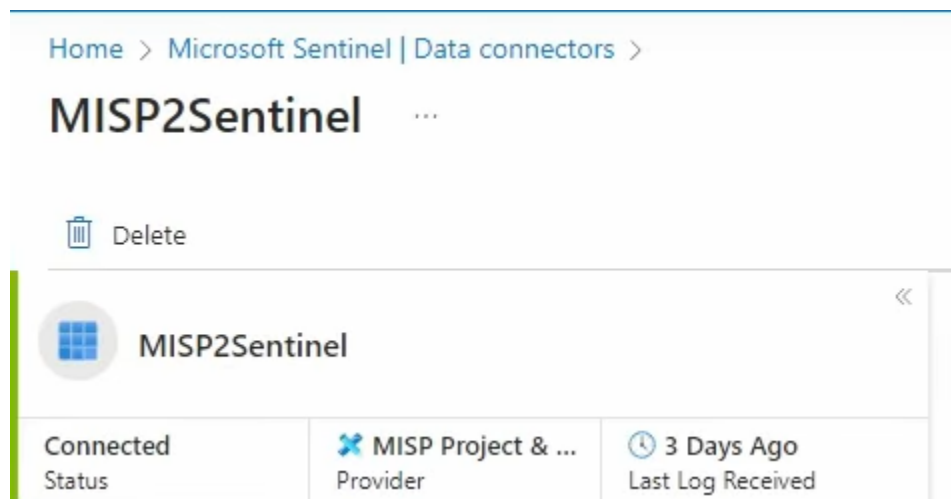
25. We then click **Appy**

The screenshot shows the 'App settings' tab of a configuration interface. It contains a table with two columns: 'Name' and 'Value'. The 'timerTriggerSchedule' variable is highlighted in the table. Below the table, there are two buttons: 'Apply' and 'Discard'. The 'Apply' button is circled in green.

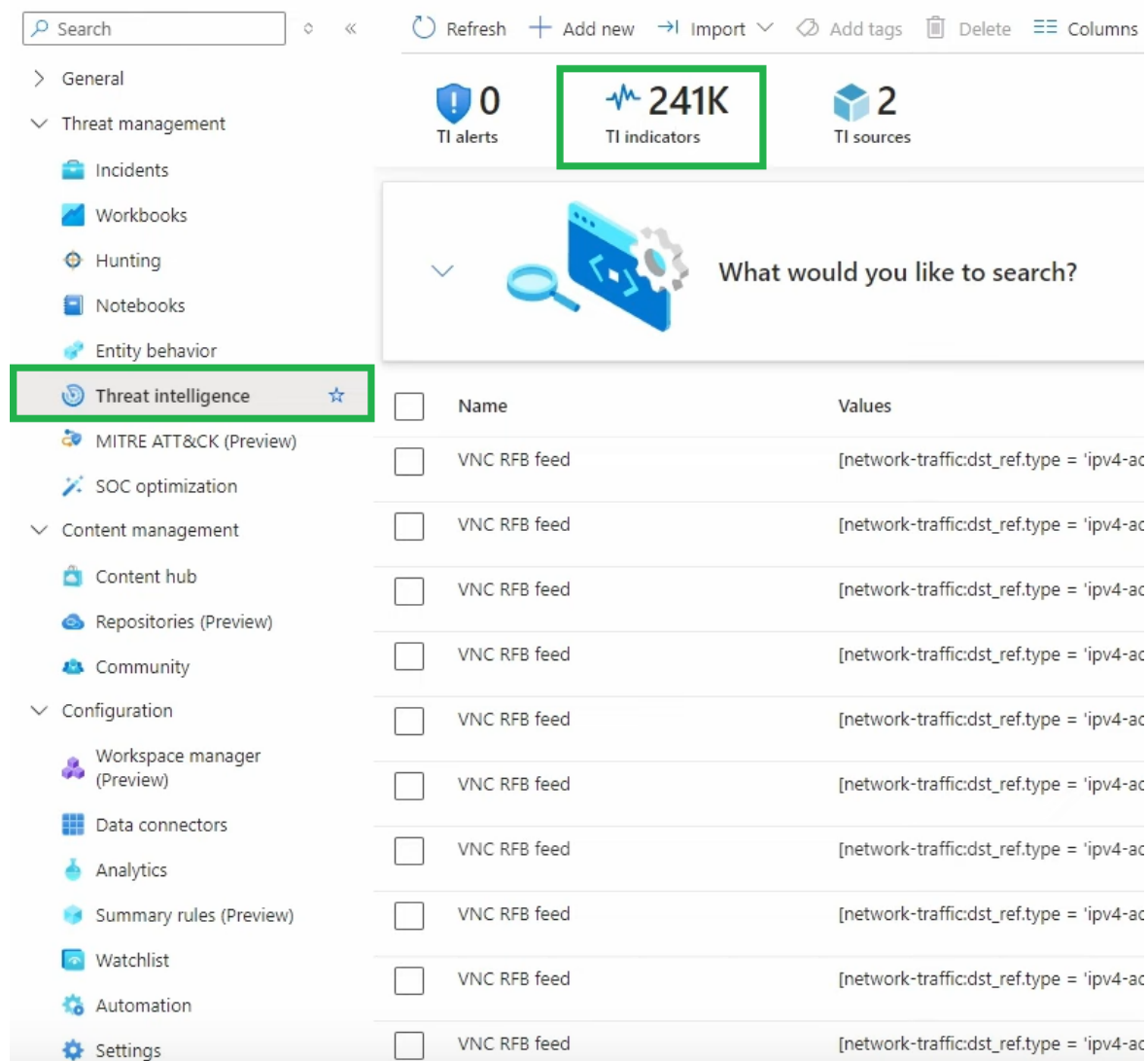
Name	Value
APPLICATIONINSIGHTS_CONNECTION_STRING	Show value
AzureWebJobsStorage	Show value
BUILD_FLAGS	Show value
client_id	Show value
client_secret	Show value
ENABLE_ORYX_BUILD	Show value
FUNCTIONS_EXTENSION_VERSION	Show value
FUNCTIONS_WORKER_RUNTIME	Show value
mispkey	Show value
mispurl	Show value
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 Connecator should change to **Connected**.



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

