CERT STAR

Bring Your Own Threat Intelligence Feeds

GLOBAL
CYBER SECURITY
CENTER

Microsoft

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Contents

Bring Your Own Threat Intelligence Feeds

Abstract and learning objectives

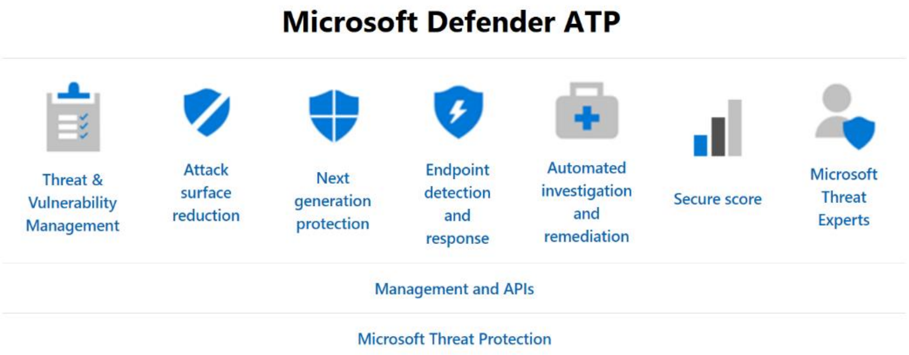
Understand how to push 3rd party threat feeds into Microsoft Cloud Services: Microsoft Defender ATP and Azure Sentinel

Overview

In this lab, attendees will deploy Microsoft Defender Advanced Threat Protection and Azure Sentinel focusing on how to integrate 3rd party threat feeds.

Microsoft Defender Advanced Threat Protection is a platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. MDATP uses the following combination of technologies enabled by Microsoft's cloud:

- **Endpoint behavioral sensors**
- **Cloud Security Analytics**
- **Threat Intelligence**


Microsoft Defender ATP
Threat & Vulnerability Management
Attack surface reduction
Next generation protection
Endpoint detection and response
Automated investigation and remediation
Secure score
Microsoft Threat Experts
Management and APIs
Microsoft Threat Protection

Azure Sentinel is Microsoft's cloud-native **SIEM** — *Security Information Event Management* — and **SOAR** — *Security Orchestration Automated Response* — that provides intelligent security analytics. It can easily collect data from all cloud and/or on-premises assets: Office 365, Azure resources, and other clouds. The core capabilities are:

1. **Collect** data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
2. **Detect** previously undetected threats, and minimize false positives using Microsoft's analytics and threat intelligence.

3. **Investigate** threats with artificial intelligence, and hunt for suspicious activities at scale.
4. **Respond** to incidents rapidly with built-in orchestration and automation of common tasks.

Azure Sentinel displays a number of connectors for Microsoft solutions. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use common event format, Syslog or REST-API to connect your data sources with Azure Sentinel as well.

If you are interested in understanding built-in connector availability and configuration, the updated list and documentation is here.

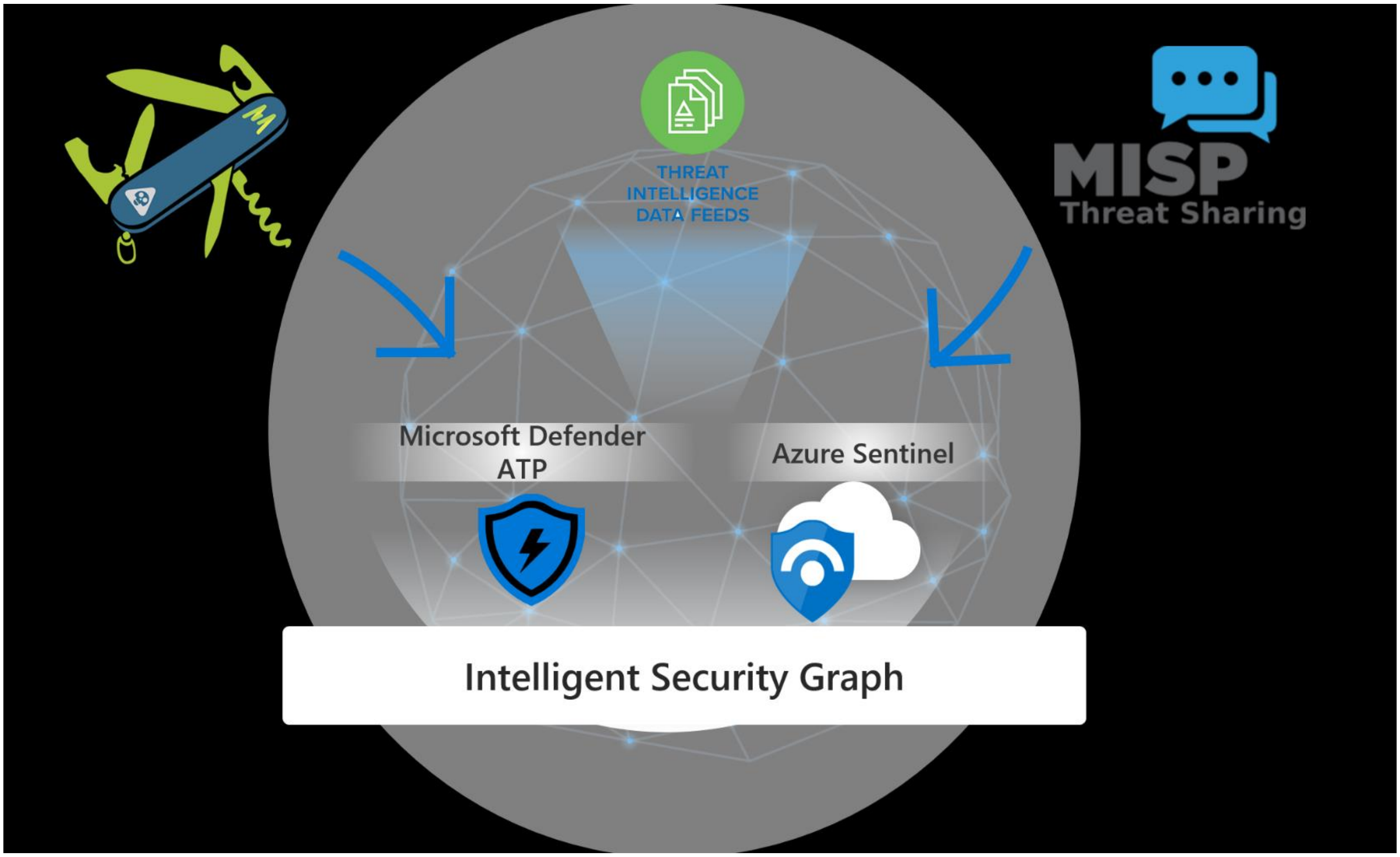
MISP - Malware Information Sharing Platform - is an Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing –

It's a threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organizations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organizations or people.

MineMeld, by **Palo Alto Networks**, is an open source Threat Intelligence processing framework. MineMeld can be used to collect, aggregate and filter indicators from a variety of sources and make them available for consumption to peers or to the Palo Alto Networks security platforms.

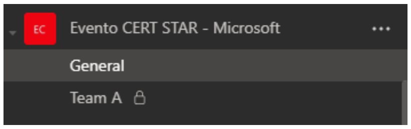
MineMeld can be used to aggregate multiple threat intelligence feeds and extend to your Windows Defender ATP tenant. Windows Defender ATP can ingest: IPv4 addresses, File hashes, URLs, Domains and FQDNs

Solution architecture



Credentials

Note Team**X** means Team**A** or Team**B**, it depends on members assignment. Please notice Microsoft Teams channel you are part of.



Means TeamA@certstarmicrosoftlab.it – TeamA – teama

Resource	Username	Password	Description
Microsoft Cloud Services	TeamX@certstarmicrosoftlab.it	M10d6nj! (needs reset at first sign-in)	portal.azure.com, Microsoft Defender ATP, Azure Sentinel
MineMeld	TeamX	M10d6nj!	
MISP	TeamX@certstarmicrosoftlab.it	M10d6nj!M10d6nj!	
Server MISP (ssh)	teamx	M10d6nj!	

Lab Requirements

In this lab scenario, attendees will be provided an overview of the Microsoft Defender ATP and Azure Sentinel. Requirements are as follows based on the solution diagram previously shown.

1. Join the Microsoft Teams Channel
2. Credentials
3. SSH client

Exercise 1: Microsoft Defender ATP – Threat Intelligence Platform integration

This exercise will lead you through setting up TIP (Threat Intelligence Platform) integration using MineMeld.

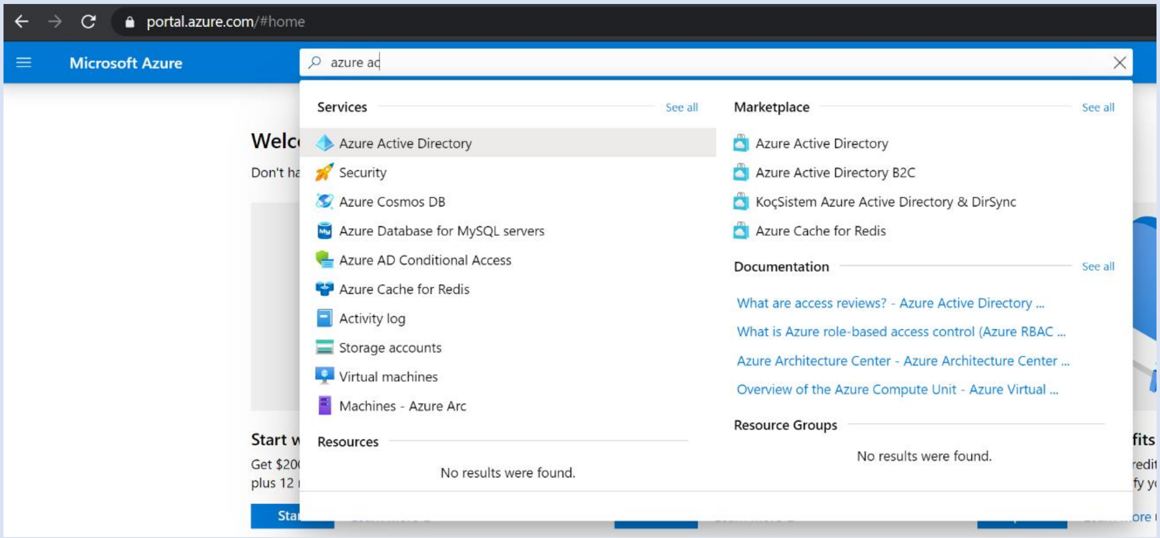
In order to connect MineMeld to Microsoft Defender ATP, the main tasks are the following:

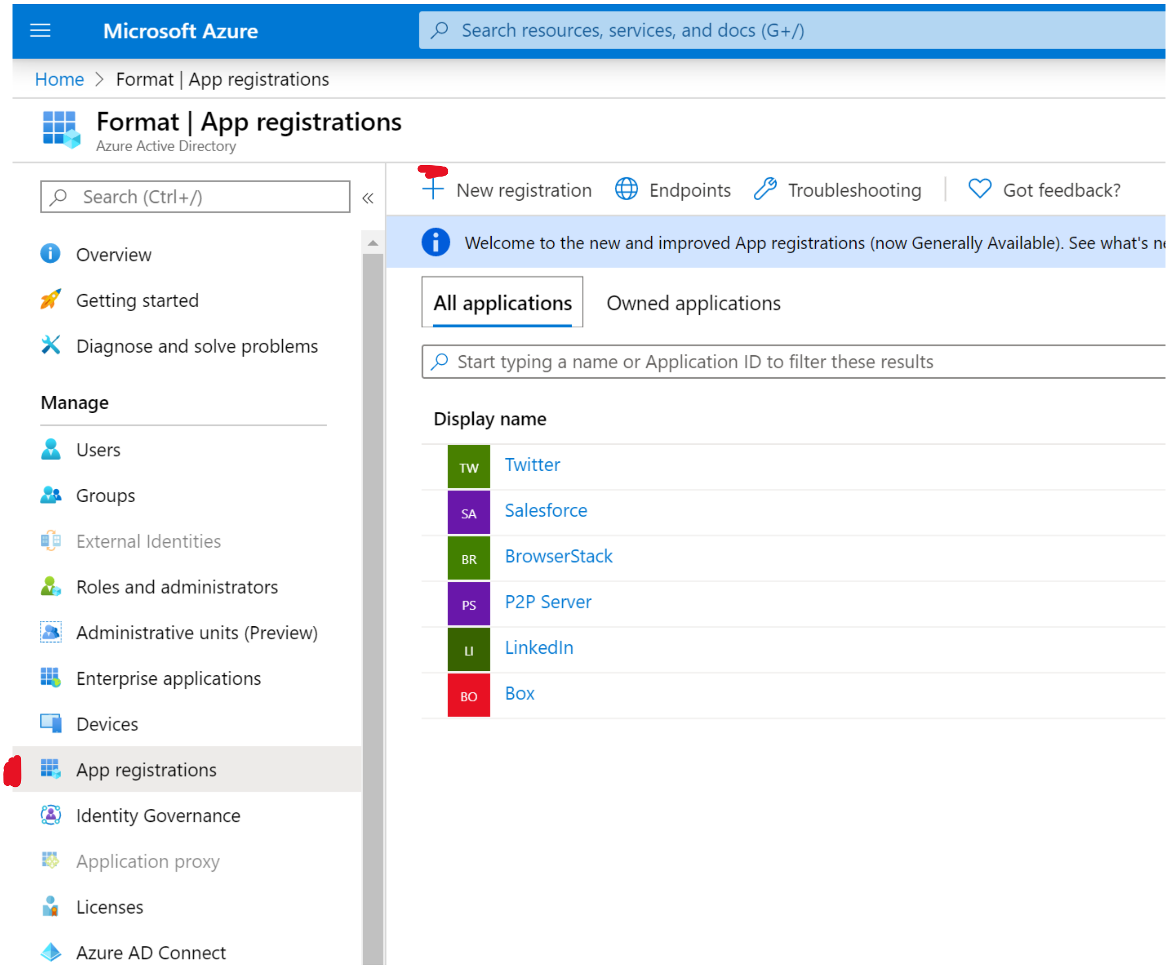
1. Create custom Azure Active Directory application
2. Install MineMeld — MDATP extension
3. Configure MDATP extension

All detailed steps are fully described here: https://live.paloaltonetworks.com/t5/MineMeld-Articles/How-to-configure-MineMeld-to-send-Indicators-to-Microsoft/ta-p/244121

Let's start with Task n.1:

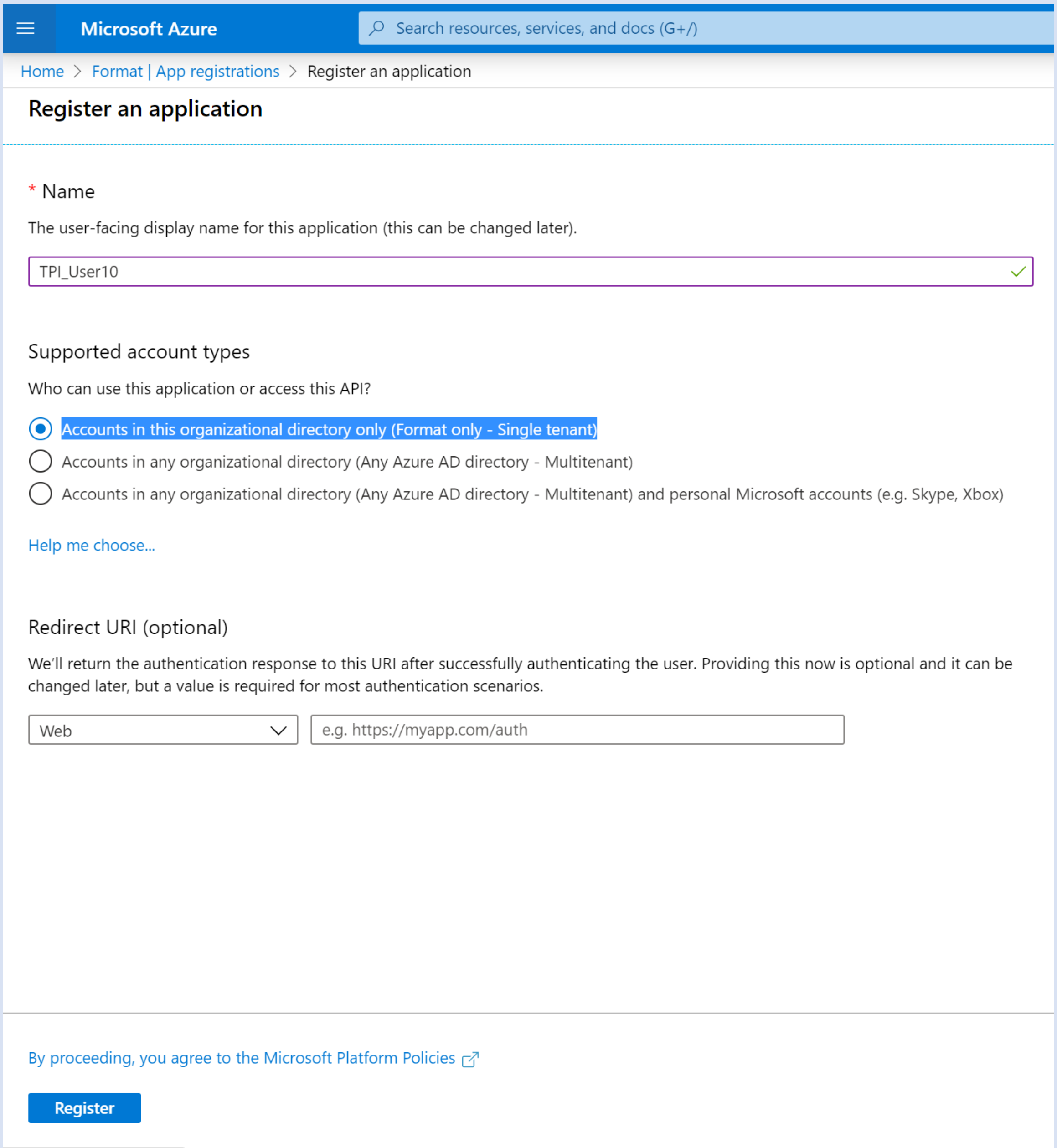
Task 1: Create Azure Active Directory app registration

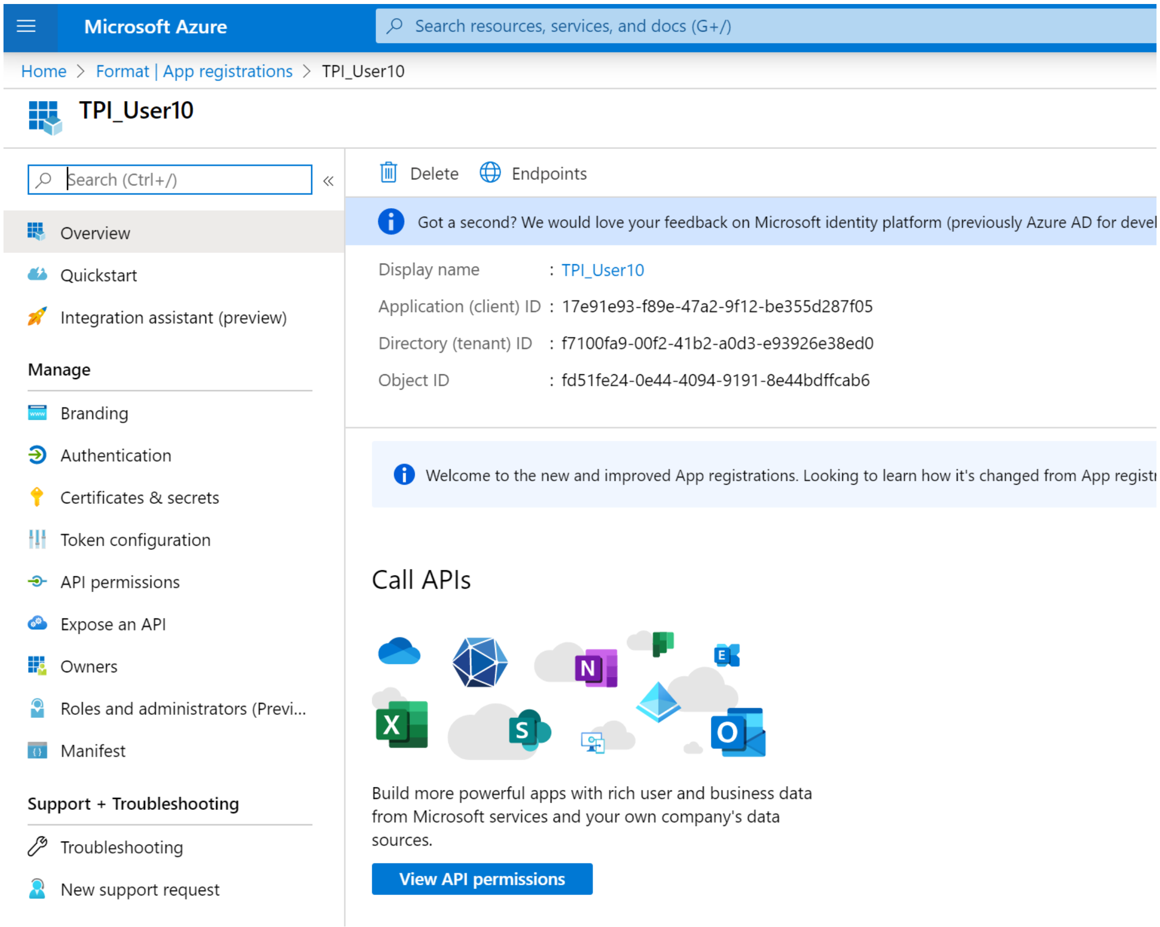
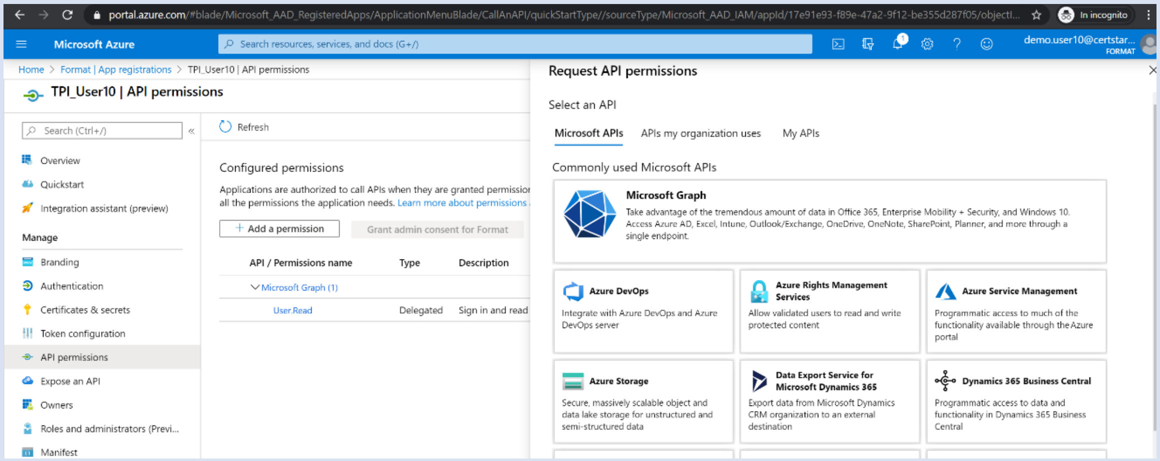
Step	Action
1.	Login on https://portal.azure.com with credentials provided
2.	Search for Azure Active Directory service  portal.azure.com/#home Microsoft Azure azure ad Services See all Azure Active Directory Security Azure Cosmos DB Azure Database for MySQL servers Azure AD Conditional Access Azure Cache for Redis Activity log Storage accounts Virtual machines Machines - Azure Arc Resources No results were found. Marketplace See all Azure Active Directory Azure Active Directory B2C KoçSistem Azure Active Directory & DirSync Azure Cache for Redis Documentation See all What are access reviews? - Azure Active Directory ... What is Azure role-based access control (Azure RBAC ... Azure Architecture Center - Azure Architecture Center ... Overview of the Azure Compute Unit - Azure Virtual ... Resource Groups No results were found.

Step	Action
3.	Create new app registration. Azure AD → App Registration → + New Registration 

Welcome to the new and improved App registrations (now Generally Available). See what's n

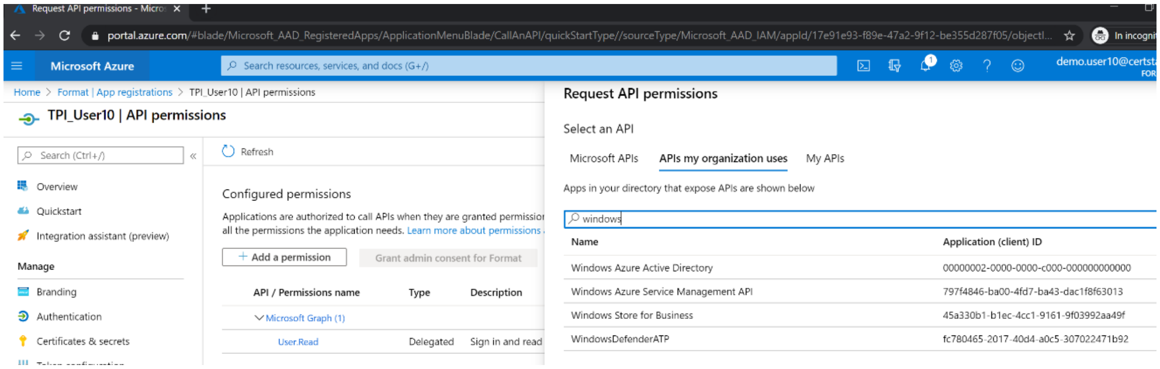
Display name
TW Twitter
SA Salesforce
BR BrowserStack
PS P2P Server
LI LinkedIn
BO Box

Step	Action
4.	Insert Name: TPI_UserX, select "Accounts in this organizational directory only (Format only - Single tenant)" and click Register  Microsoft Azure Search resources, services, and docs (G+/) Home > Format | App registrations > Register an application **Register an application** * Name The user-facing display name for this application (this can be changed later). TPI_User10 Supported account types Who can use this application or access this API? ● Accounts in this organizational directory only (Format only - Single tenant) ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) 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. Web e.g. https://myapp.com/auth By proceeding, you agree to the Microsoft Platform Policies Register

Step	Action
5.	take note of Application ID and Tenant ID  Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for devel Display name : TPI_User10 Application (client) ID : 17e91e93-f89e-47a2-9f12-be355d287f05 Directory (tenant) ID : f7100fa9-00f2-41b2-a0d3-e93926e38ed0 Object ID : fd51fe24-0e44-4094-9191-8e44bdffcab6 Welcome to the new and improved App registrations. Looking to learn how it's changed from App registr Call APIs Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. Microsoft Azure Search resources, services, and docs (G+/) Home > Format | App registrations > TPI_User10 TPI_User10 Search (Ctrl+/) Delete Endpoints Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators (Previ... Manifest Support + Troubleshooting Troubleshooting New support request View API permissions
6.	Inside Azure AD app just created → API Permissions → +Add a permission and select “APIs my organization uses”  portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be355d287f05/objectI... Configured permissions Applications are authorized to call APIs when they are granted permissio all the permissions the application needs. Learn more about permissions API / Permissions name | Type | Description Microsoft Graph (1) User.Read | Delegated | Sign in and read Request API permissions Select an API Microsoft APIs | APIs my organization uses | My APIs Commonly used Microsoft APIs Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint. Azure DevOps: Integrate with Azure DevOps and Azure DevOps server Azure Rights Management Services: Allow validated users to read and write protected content Azure Service Management: Programmatic access to much of the functionality available through the Azure portal Azure Storage: Secure, massively scalable object and data lake storage for unstructured and semi-structured data Data Export Service for Microsoft Dynamics 365: Export data from Microsoft Dynamics CRM organization to an external destination Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central In incognito Microsoft Azure Search resources, services, and docs (G+/) demo.user10@certstar... FORMAT Home > Format | App registrations > TPI_User10 | API permissions TPI_User10 | API permissions Search (Ctrl+/) Refresh Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators (Previ... Manifest + Add a permission Grant admin consent for Format

Step **Action**

7. Search anc click on "WindowsDefenderATP"



Request API permissions - Micro

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be355d287f05/objectI...

In incogni
Microsoft Azure
Search resources, services, and docs (G+/)
demo.user10@certst
FOR
Home > Format | App registrations > TPI_User10 | API permissions
TPI_User10 | API permissions
Search (Ctrl+/)
Overview
Quickstart
Integration assistant (preview)
Manage
Branding
Authentication
Certificates & secrets
Token configuration
Refresh
+ Add a permission
Grant admin consent for Format

Configured permissions

Applications are authorized to call APIs when they are granted permissio all the permissions the application needs. Learn more about permissions

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read

Request API permissions

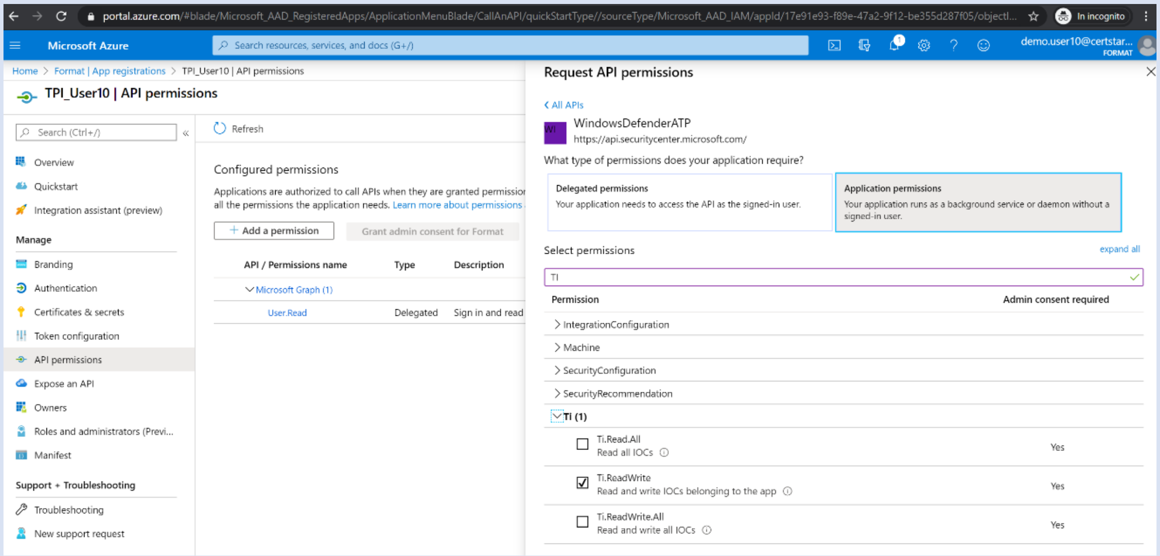
Select an API

Apps in your directory that expose APIs are shown below

windows

Name	Application (client) ID
Windows Azure Active Directory	00000002-0000-0000-c000-000000000000
Windows Azure Service Management API	797f4846-ba00-4fd7-ba43-dac1f8f63013
Windows Store for Business	45a330b1-b1ec-4cc1-9161-9f03992aa49f
WindowsDefenderATP	fc780465-2017-40d4-a0c5-307022471b92

8. Click on Application Permissions → search and Select "Ti.ReadWrite - Read and write IOCs belonging to the app". That means application will use MDATP API to read and write IoCs. → Click on add permissions



portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be355d287f05/objectI...

Configured permissions

Applications are authorized to call APIs when they are granted permissio all the permissions the application needs. Learn more about permissions

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read

Request API permissions

< All APIs

WindowsDefenderATP
https://api.securitycenter.microsoft.com/

What type of permissions does your application require?

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

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

Select permissions

TI

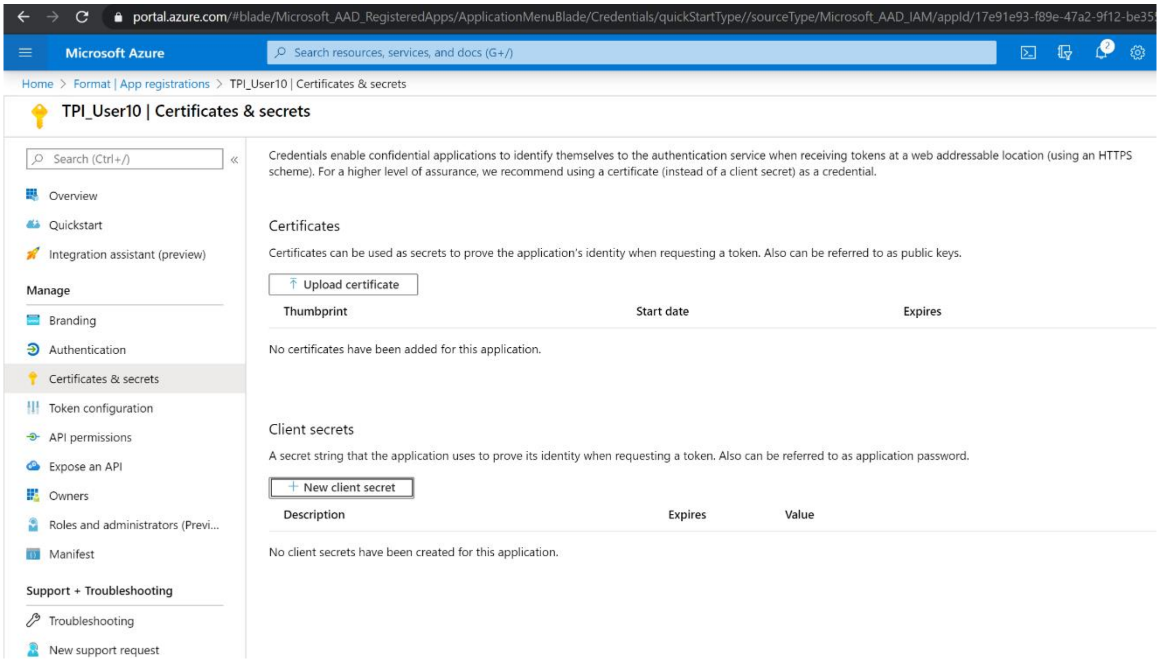
Permission	Admin consent required
> IntegrationConfiguration	
> Machine	
> SecurityConfiguration	
> SecurityRecommendation	
Ti (1)	
☐ Ti.Read.All Read all IOCs	Yes
☑ Ti.ReadWrite Read and write IOCs belonging to the app	Yes
☐ Ti.ReadWrite.All Read and write all IOCs	Yes

9. You will receive a notification on top saying: "You are editing permission(s) to your application, users will have to consent even if they've already done so previously."

That means Global Admin consent is required.

10. Please send a message on General Teams channel with your Team Name asking for consent.

Tutors will apply Consent to you App Registration remotely upon your request. Please note that this step is mandatory and necessary to proceed further.

Step	Action
11.	Create a new client secret in "Certificate" & Secrets" 

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Credentials/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be35

Home > Format | App registrations > TPI_User10 | Certificates & secrets

TPI_User10 | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

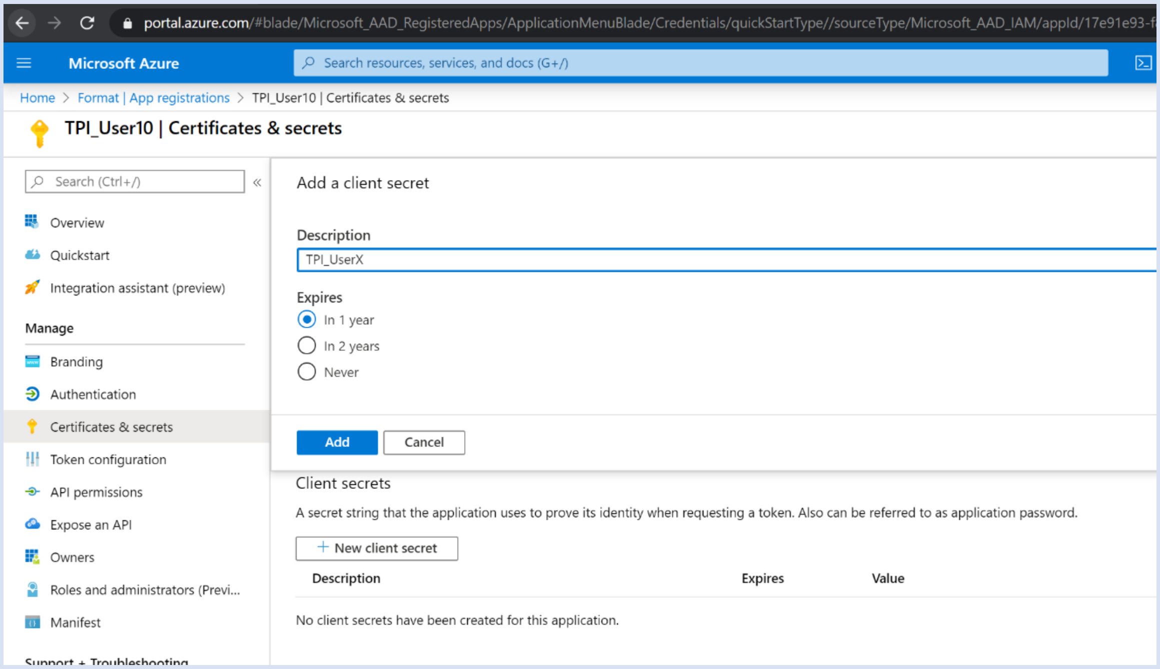
No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

12.	Click "+ New client secret" → Add Description "TPI_UserX", Select 1 year and click Add 

portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Credentials/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f

Home > Format | App registrations > TPI_User10 | Certificates & secrets

TPI_User10 | Certificates & secrets

Add a client secret

Description: TPI_UserX

Expires
● In 1 year
○ In 2 years
○ Never

Client secrets

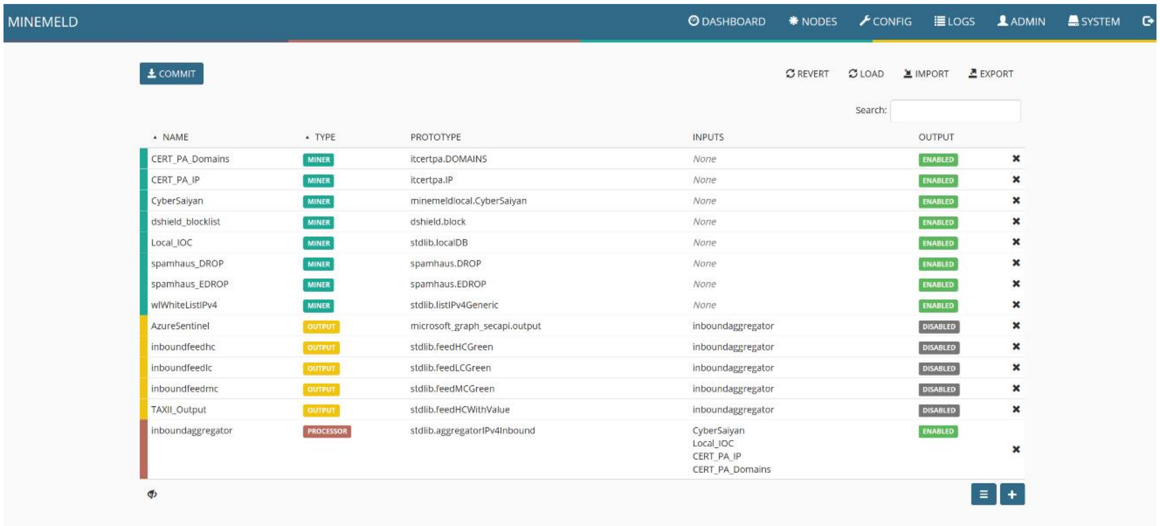
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

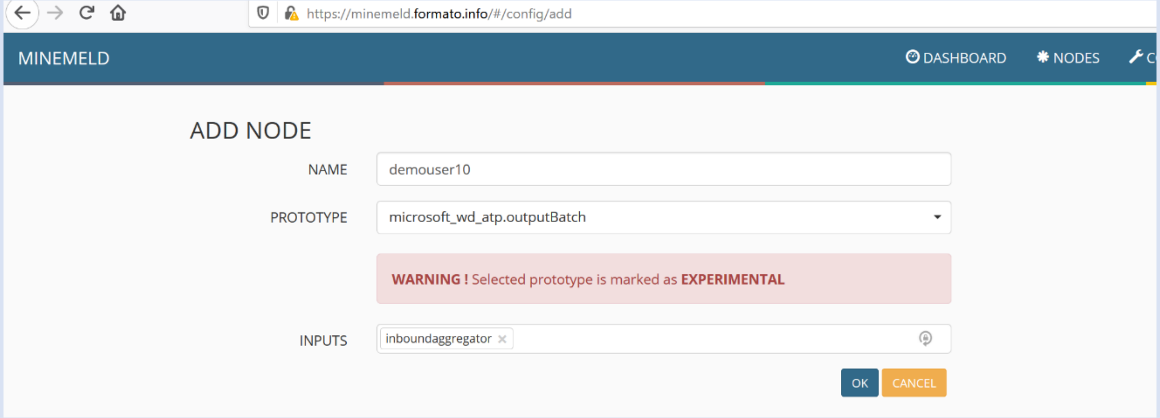
Description	Expires	Value

No client secrets have been created for this application.

13.	Copy the new client secret Value on your text editor.

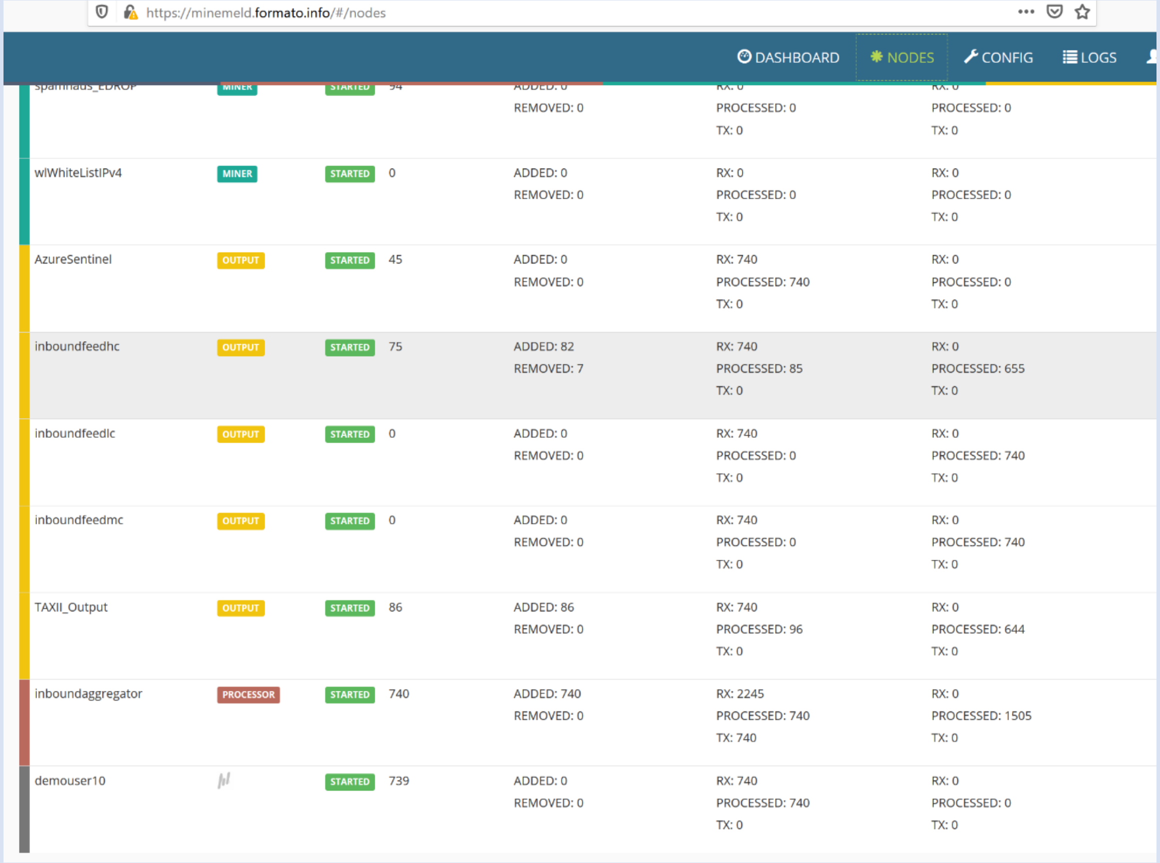
Task 2: Connect MineMeld to Microsoft Defender ATP

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td>Login on https://minemeld.formato.info with credentials provided</td></tr>
<tr><td>2.</td><td>Descrizione Miners, ecc</td></tr>
<tr><td>3.</td><td>Configure Miners to aggregate Threat Indicators.
Click Config → click on “Eye” icon on the left down hand side of the screen , a + button will appear → Click on it


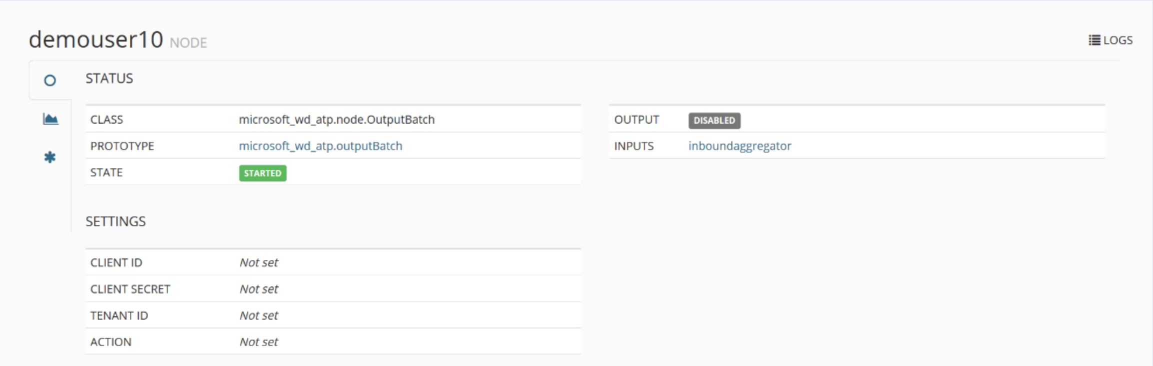
<table>
<tr><th>NAME</th><th>TYPE</th><th>PROTOTYPE</th><th>INPUTS</th><th>OUTPUT</th><th></th></tr>
<tr><td>CERT_PA_Domains</td><td>MINER</td><td>itcertpa.DOMAINS</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>CERT_PA_IP</td><td>MINER</td><td>itcertpa.IP</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>CyberSaiyan</td><td>MINER</td><td>minemeldlocal.CyberSaiyan</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>dshield_blocklist</td><td>MINER</td><td>dshield.block</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>Local_IOC</td><td>MINER</td><td>stdlib.localDB</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>spamhaus_DROP</td><td>MINER</td><td>spamhaus.DROP</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>spamhaus_EDROP</td><td>MINER</td><td>spamhaus.EDROP</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>wlWhiteListIPv4</td><td>MINER</td><td>stdlib.listIPv4Generic</td><td>None</td><td>ENABLED</td><td>✖</td></tr>
<tr><td>AzureSentinel</td><td>OUTPUT</td><td>microsoft_graph_secapi.output</td><td>inboundaggregator</td><td>DISABLED</td><td>✖</td></tr>
<tr><td>inboundfeedhc</td><td>OUTPUT</td><td>stdlib.feedHCGreen</td><td>inboundaggregator</td><td>DISABLED</td><td>✖</td></tr>
<tr><td>inboundfeedlc</td><td>OUTPUT</td><td>stdlib.feedLCGreen</td><td>inboundaggregator</td><td>DISABLED</td><td>✖</td></tr>
<tr><td>inboundfeedmc</td><td>OUTPUT</td><td>stdlib.feedMCGreen</td><td>inboundaggregator</td><td>DISABLED</td><td>✖</td></tr>
<tr><td>TAXII_Output</td><td>OUTPUT</td><td>stdlib.feedHCWithValue</td><td>inboundaggregator</td><td>DISABLED</td><td>✖</td></tr>
<tr><td>inboundaggregator</td><td>PROCESSOR</td><td>stdlib.aggregatorIPv4Inbound</td><td>CyberSaiyan
Local_IOC
CERT_PA_IP
CERT_PA_Domains</td><td>ENABLED</td><td>✖</td></tr>
</table>
</td></tr>
<tr><td>4.</td><td>Name “demouserX” → Prototype “microsoft_wd_adtp.outputBatch” (don’t worry about the alert)→ Inputs “inboundaggregator” → click OK


https://minemeld.formato.info/#/config/add
ADD NODE
NAME demouser10
PROTOTYPE microsoft_wd_atp.outputBatch
WARNING ! Selected prototype is marked as EXPERIMENTAL
INPUTS inboundaggregator ×</td></tr>
<tr><td>5.</td><td>Click “Commit” and wait for COMPLETE services restart.</td></tr>
</table>

6. Edit MDATP node properties in "Nodes" → click on the node just created, scroll to "Settings" section and provide: CLIENT ID (Azure AD Application ID), CLIENT SECRET: (Client Secret), TENANT ID (Azure AD Identifier)



spamhaus_EDROP	MINER	STARTED	94	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
wlWhiteListIPv4	MINER	STARTED	0	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
AzureSentinel	OUTPUT	STARTED	45	ADDED: 0 REMOVED: 0	RX: 740 PROCESSED: 740 TX: 0	RX: 0 PROCESSED: 0 TX: 0
inboundfeedhc	OUTPUT	STARTED	75	ADDED: 82 REMOVED: 7	RX: 740 PROCESSED: 85 TX: 0	RX: 0 PROCESSED: 655 TX: 0
inboundfeedlc	OUTPUT	STARTED	0	ADDED: 0 REMOVED: 0	RX: 740 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 740 TX: 0
inboundfeedmc	OUTPUT	STARTED	0	ADDED: 0 REMOVED: 0	RX: 740 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 740 TX: 0
TAXII_Output	OUTPUT	STARTED	86	ADDED: 86 REMOVED: 0	RX: 740 PROCESSED: 96 TX: 0	RX: 0 PROCESSED: 644 TX: 0
inboundaggregator	PROCESSOR	STARTED	740	ADDED: 740 REMOVED: 0	RX: 2245 PROCESSED: 740 TX: 740	RX: 0 PROCESSED: 1505 TX: 0
demouser10		STARTED	739	ADDED: 0 REMOVED: 0	RX: 740 PROCESSED: 740 TX: 0	RX: 0 PROCESSED: 0 TX: 0



demouser10 NODE

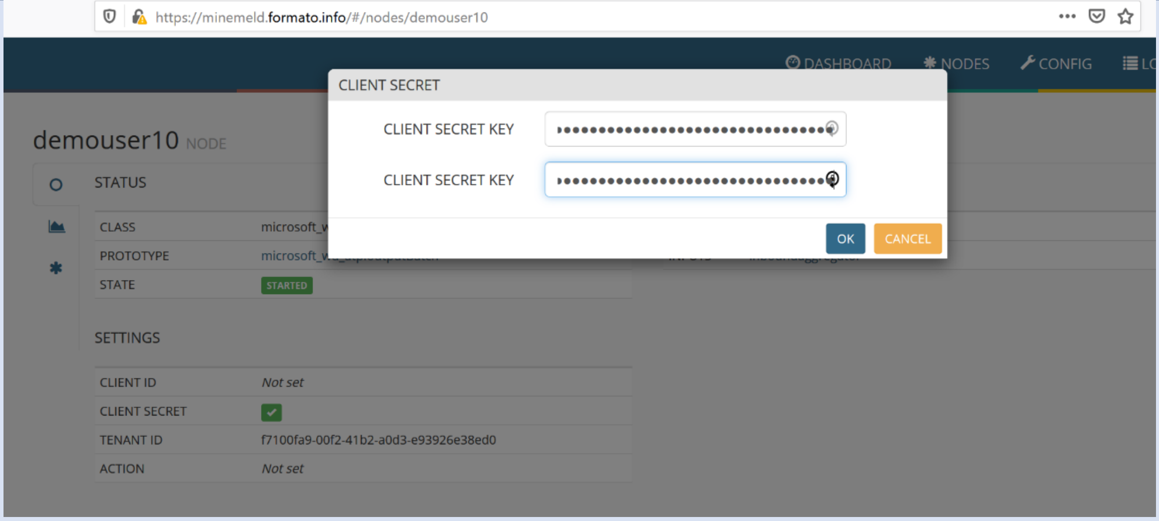
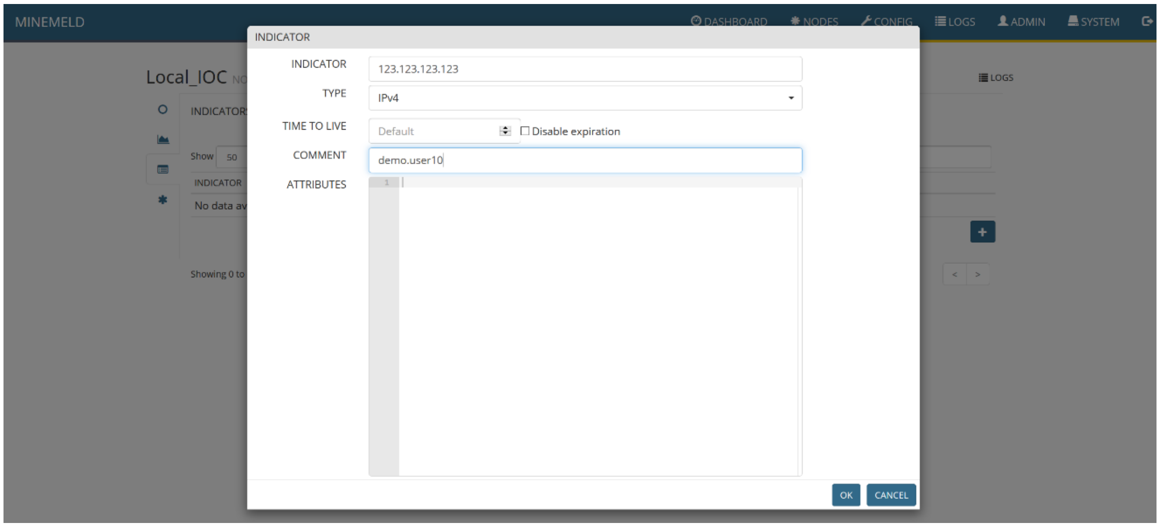
STATUS

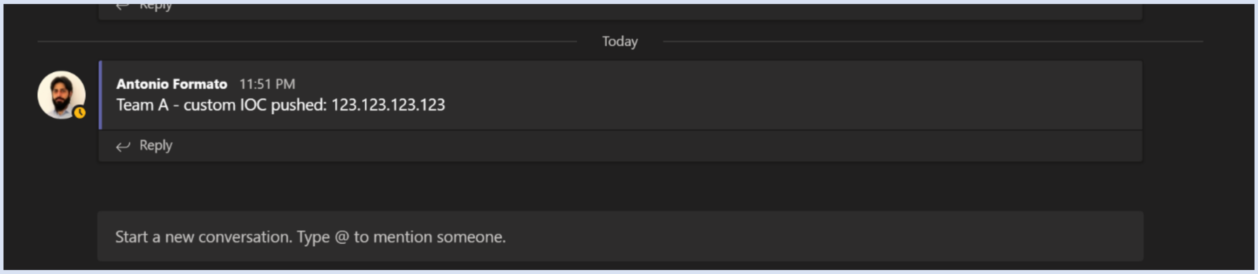
CLASS	microsoft_wd_atp.node.OutputBatch
PROTOTYPE	microsoft_wd_atp.outputBatch
STATE	STARTED

OUTPUT	DISABLED
INPUTS	inboundaggregator

SETTINGS

CLIENT ID	*Not set*
CLIENT SECRET	*Not set*
TENANT ID	*Not set*
ACTION	*Not set*

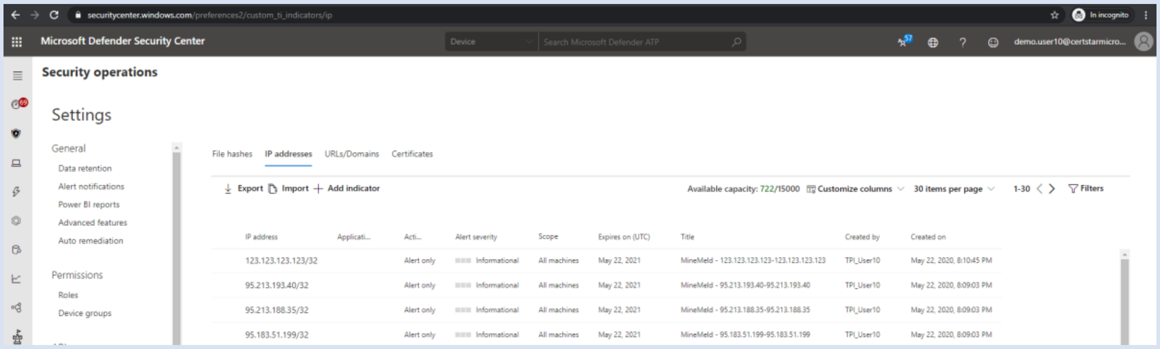
Step	Action
	 https://minemeld.formato.info/#/nodes/demouser10 CLIENT SECRET CLIENT SECRET KEY •••••••••••••••••••••••••••••••• CLIENT SECRET KEY •••••••••••••••••••••••••••••••• OK CANCEL demouser10 NODE STATUS CLASS microsoft_v PROTOTYPE microsoft_v STATE STARTED SETTINGS CLIENT ID *Not set* CLIENT SECRET ✓ TENANT ID f7100fa9-00f2-41b2-a0d3-e93926e38ed0 ACTION *Not set*
7.	Insert TeamX's indicators. Note: MineMeld do not push duplicated indicators. In order to see your own IOC implement below procedure. **MineMeld → Node → Local IOC –> select 3rd tab on the left "Indicators" and click on + Add Indicator** Insert you indicator i.e. 123.123.123.123 → Type IPv4 → Comment insert your account name "demo.userX". Click OK Comment: TeamX (it could be useful for troubleshooting purpose if needed)  INDICATOR INDICATOR 123.123.123.123 TYPE IPv4 TIME TO LIVE Default ☐ Disable expiration COMMENT demo.user10 ATTRIBUTES OK CANCEL

Step	Action
8.	Please chat custom IOC pushed to General MS Teams channel chat 

Today

Antonio Formato 11:51 PM
Team A - custom IOC pushed: 123.123.123.123

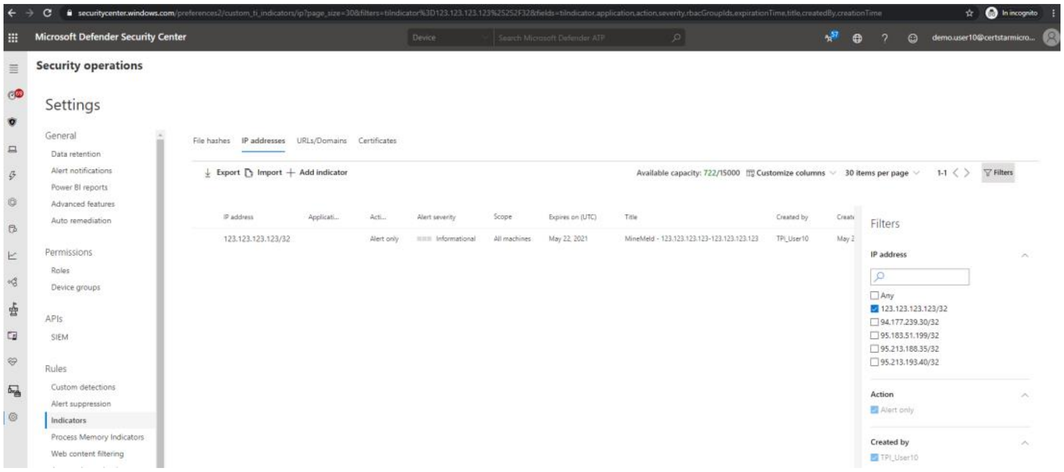
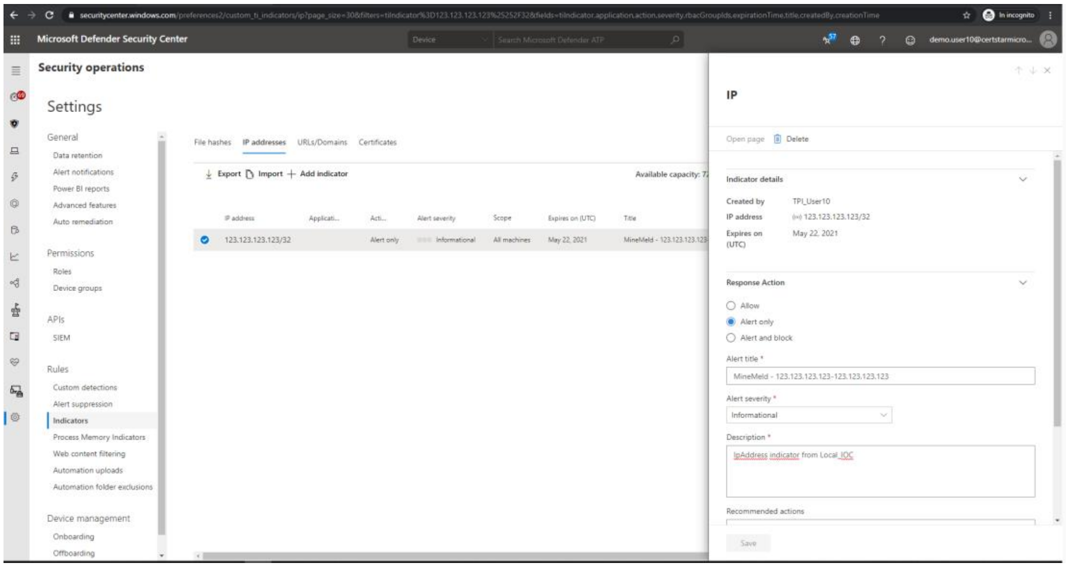
Task 3: Use Data on MDATP

Step	Action
1.	Login on https://securitycenter.windows.com with credentials provided
2.	Open the hamburger menu and expand "Settings" →In "Rules" section click on "Indicators" → IP Addresses  Notice "Created by" field. You can Filter on this fied to see your IoCs

securitycenter.windows.com/preferences2/custom_ti_indicators/ip

Available capacity: 722/15000

IP address	Applicati...	Acti...	Alert severity	Scope	Expires on (UTC)	Title	Created by	Created on
123.123.123.123/32		Alert only	Informational	All machines	May 22, 2021	MineMeld - 123.123.123.123-123.123.123.123	TPI_User10	May 22, 2020, 8:10:45 PM
95.213.193.40/32		Alert only	Informational	All machines	May 22, 2021	MineMeld - 95.213.193.40-95.213.193.40	TPI_User10	May 22, 2020, 8:09:03 PM
95.213.188.35/32		Alert only	Informational	All machines	May 22, 2021	MineMeld - 95.213.188.35-95.213.188.35	TPI_User10	May 22, 2020, 8:09:03 PM
95.183.51.199/32		Alert only	Informational	All machines	May 22, 2021	MineMeld - 95.183.51.199-95.183.51.199	TPI_User10	May 22, 2020, 8:09:03 PM

Step	Action
3.	Click on Filter and search for you custom IOC  securitycenter.windows.com/preferences2/custom_ti_indicators/ip?page_size=30&filters=tiIndicator%3D123.123.123.123%25252F32&fields=tiIndicator,application,action,severity,rbacGroupIds,expirationTime,title,createdBy,creationTime Available capacity: 722/15000 IP address: 123.123.123.123/32 · Acti...: Alert only · Alert severity: Informational · Scope: All machines · Expires on (UTC): May 22, 2021 · Title: MineMeld - 123.123.123.123-123.123.123.123 · Created by: TPI_User10 Filters IP address □ Any ☑ 123.123.123.123/32 □ 94.177.239.30/32 □ 95.183.51.199/32 □ 95.213.188.35/32 □ 95.213.193.40/32 Action ☑ Alert only Created by ☑ TPI_User10  IP Indicator details Created by: TPI_User10 IP address: 123.123.123.123/32 Expires on (UTC): May 22, 2021 Response Action ○ Allow ● Alert only ○ Alert and block Alert title *: MineMeld - 123.123.123.123-123.123.123.123 Alert severity *: Informational Description *: IpAddress indicator from Local_IOC Recommended actions

Exercise 2: Azure Sentinel – MISP integration

This exercise will lead you through setting up MISP Integration.

Azure Sentinel lets you import the threat indicators your organization is using, which can enhance your security analysts' ability to detect and prioritize known threats. Several features from Azure Sentinel then become available or are enhanced:

- **Analytics** includes a set of scheduled rule templates you can enable to generate alerts and incidents based on matches of log events from your threat indicators.
- **Workbooks** provide summarized information about the threat indicators imported into Azure Sentinel and any alerts generated from analytics rules that match your threat indicators.
- **Hunting** queries allow security investigators to use threat indicators within the context of common hunting scenarios.
- **Notebooks** can use threat indicators when you investigate anomalies and hunt for malicious behaviors.

You can stream threat indicators to Azure Sentinel by using one of the integrated threat intelligence platform (TIP) products listed in the next section, connecting to TAXII servers, or by using direct integration with the Microsoft Graph Security tiIndicators API.

Integrated threat intelligence platform products

- MISP Open Source Threat Intelligence Platform

For a sample script that provides clients with MISP instances to migrate threat indicators to the Microsoft Graph Security API, see the MISP to Microsoft Graph Security Script.

- Anomali ThreatStream

To download ThreatStream Integrator and Extensions, and the instructions for connecting ThreatStream intelligence to the Microsoft Graph Security API, see the ThreatStream downloads page.

- Palo Alto Networks MineMeld

For guided instructions, see Sending IOCs to the Microsoft Graph Security API using MineMeld.

- ThreatConnect Platform

For information, see ThreatConnect Integrations and look for Microsoft Graph Security API on the page.

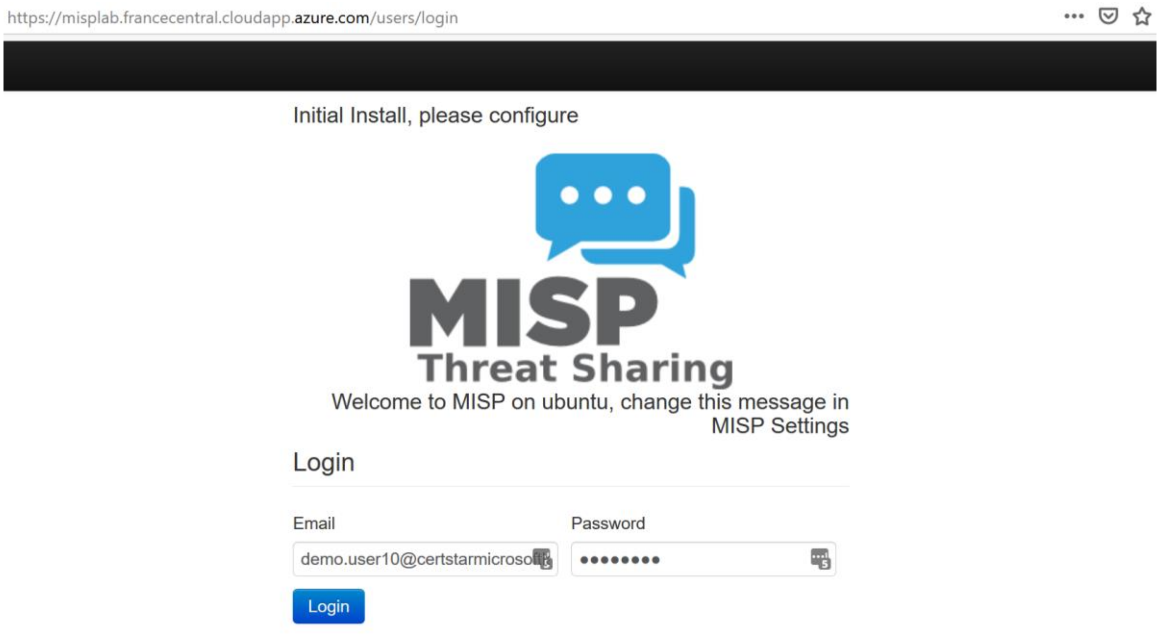
In order to connect MineMeld to Microsoft Defender ATP, the main steps are:

1. Add feed to the MISP server
2. Install MineMeld — MDATP extension
3. Configure MDATP extension

Task 1: Adding feed to the MISP server

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1.</td><td>

Login on https://misplab.francecentral.cloudapp.azure.com with credentials provided M10d6nj!M10d6nj!



https://misplab.francecentral.cloudapp.azure.com/users/login
Initial Install, please configure
MISP
Threat Sharing
Login
Login

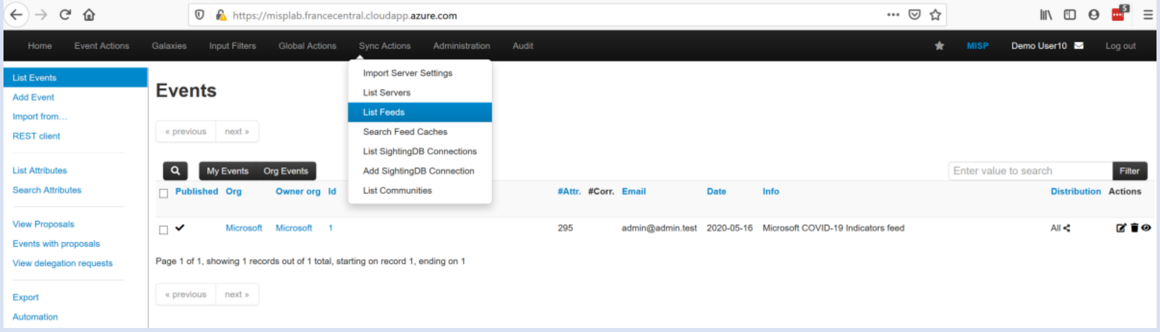
Welcome to MISP on ubuntu, change this message in MISP Settings

Email: demo.user10@certstarmicroso

Password: ●●●●●●●●●

</td></tr>
<tr><td>2.</td><td>

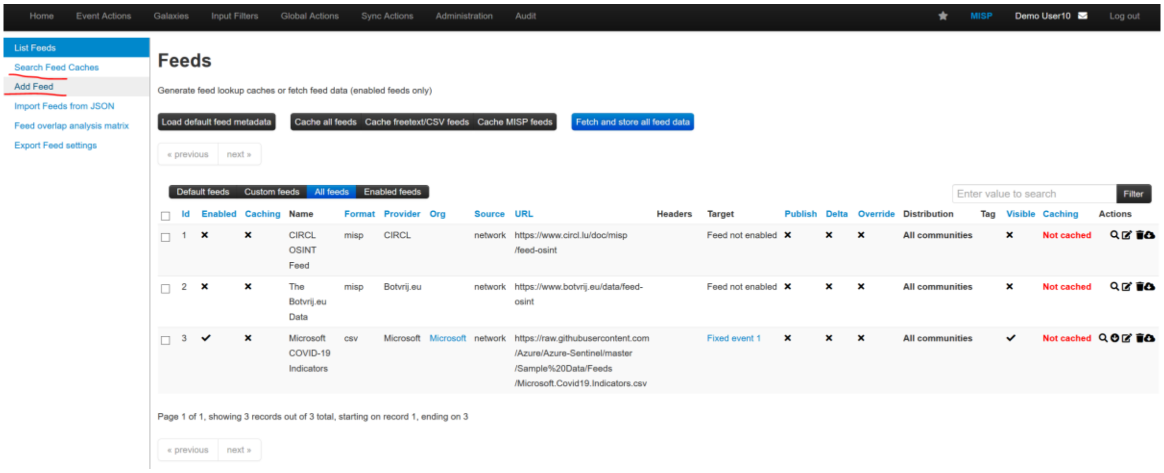
The next step is to add the Microsoft feed to the MISP server. Click on “Sync Actions” pn the top menu → “List Feeds”



□	Published	Org	Owner org	Id	#Attr.	#Corr.	Email	Date	Info	Distribution	Actions
□	✓	Microsoft	Microsoft	1	295		admin@admin.test	2020-05-16	Microsoft COVID-19 Indicators feed	All	

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

</td></tr>
</table>

Step	Action
3.	Click on “Add feeds” 

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit ★ MISP Demo User10 ✉ Log out

List Feeds
Search Feed Caches
Add Feed
Import Feeds from JSON
Feed overlap analysis matrix
Export Feed settings

Feeds

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

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

« previous next »

Default feeds | Custom feeds | All feeds | Enabled feeds

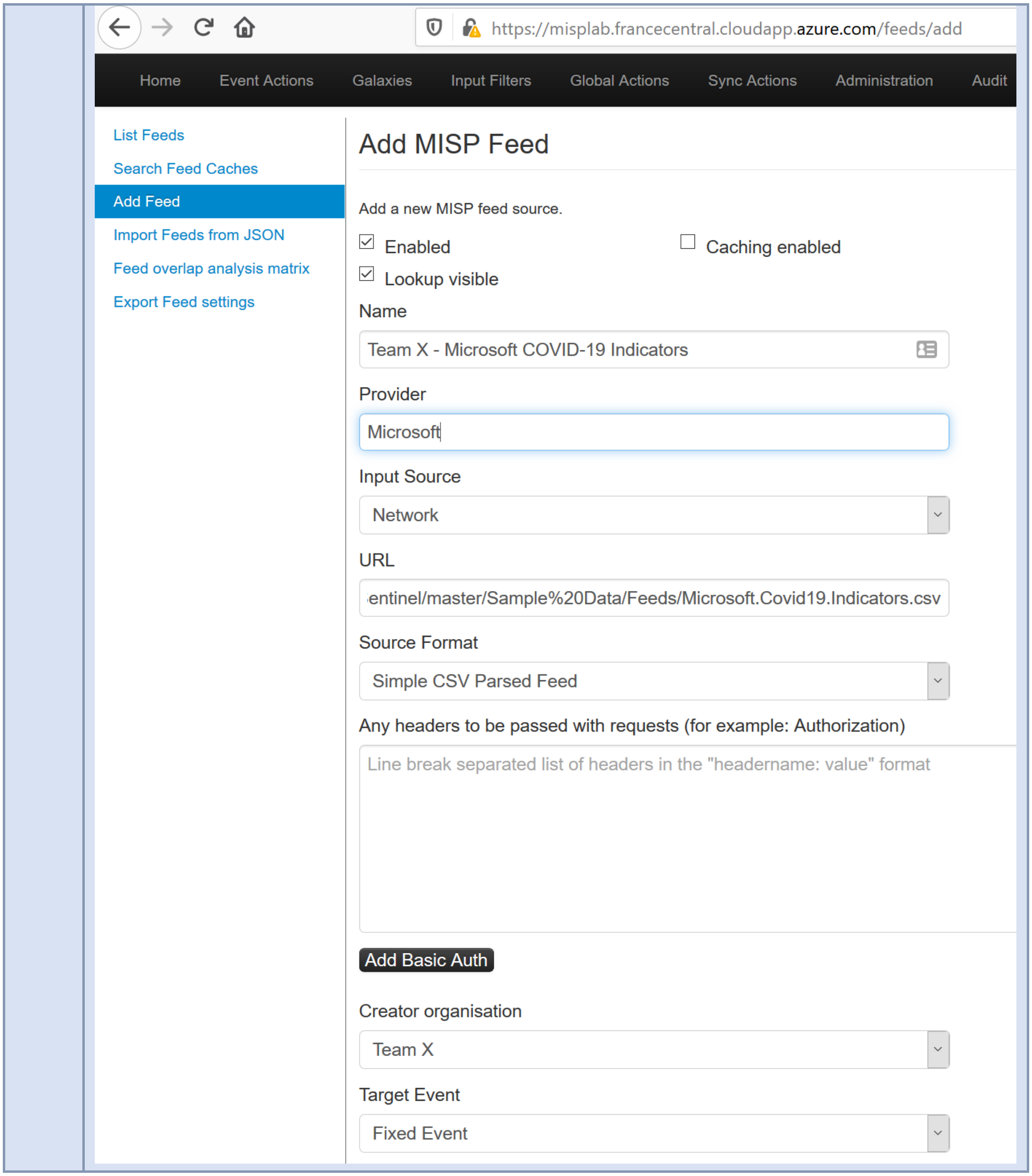
Enter value to search | Filter

□	Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions
□	1	✗	✗	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cached	
□	2	✗	✗	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cached	
□	3	✓	✗	Microsoft COVID-19 Indicators	csv	Microsoft	Microsoft	network	https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Microsoft.Covid19.Indicators.csv		Fixed event 1	✗	✗	✗	All communities		✓	Not cached	

Page 1 of 1, showing 3 records out of 3 total, starting on record 1, ending on 3

« previous next »

4.	• Enter the address of Microsoft's COVID-19 feed: https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Microsoft.Covid19.Indicators.csv • Select "Enabled" • Name: "Team X - Microsoft COVID-19 Indicators" → X is your team's ID (letter) • Provider = Microsoft • Input Source = Network • Source Format = Simple CSV Parsed Feed • Creator Organisation, select Team X → X is your team's ID (letter) • Set the 'Value field(s) in the CSV' to 2 • Select "Auto Publish" • Distribution = Your organisation only • Add



Add MISP Feed

Add a new MISP feed source.

☑ Enabled ☐ Caching enabled

☑ Lookup visible

Name: Team X - Microsoft COVID-19 Indicators

Provider: Microsoft

Input Source: Network

URL: entinel/master/Sample%20Data/Feeds/Microsoft.Covid19.Indicators.csv

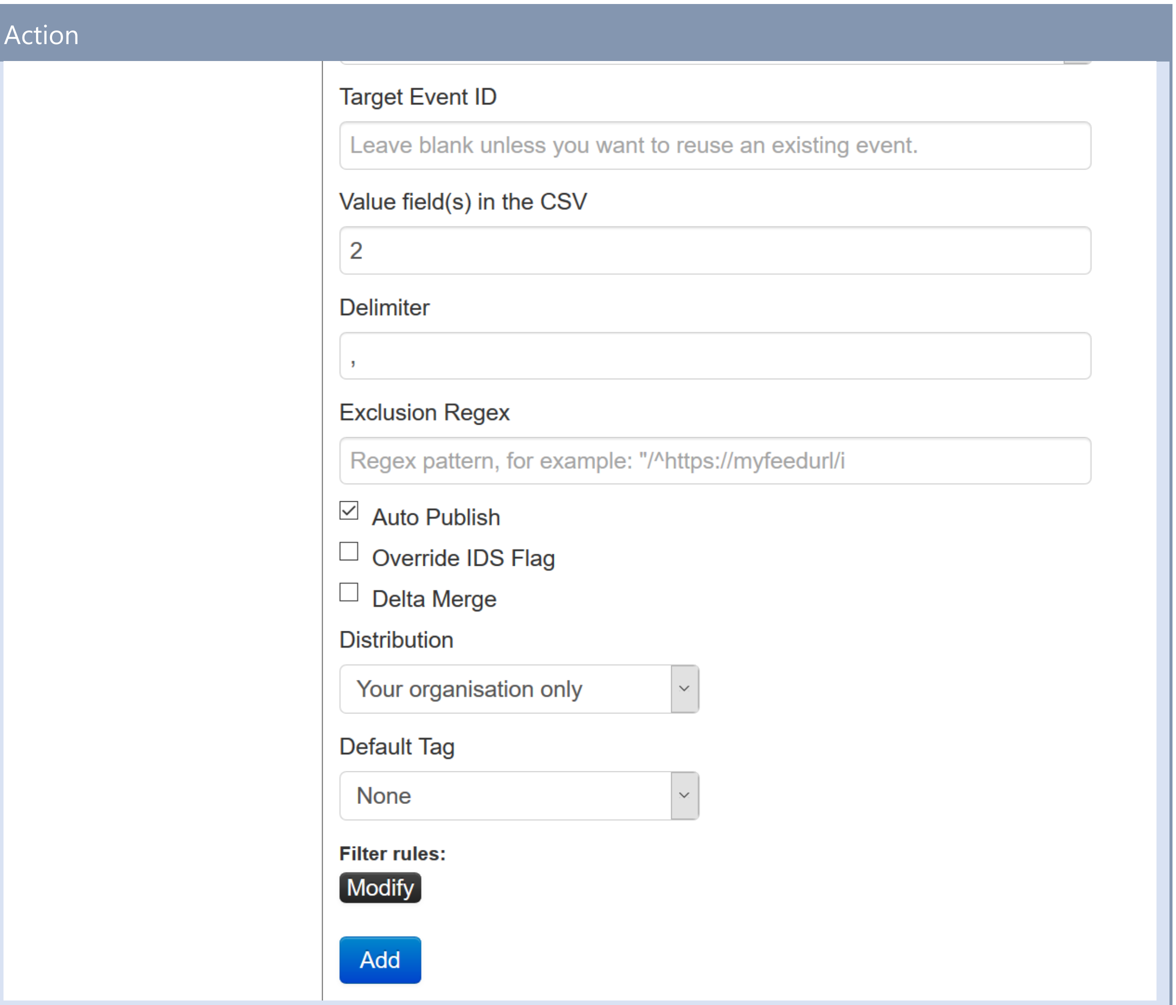
Source Format: Simple CSV Parsed Feed

Any headers to be passed with requests (for example: Authorization)

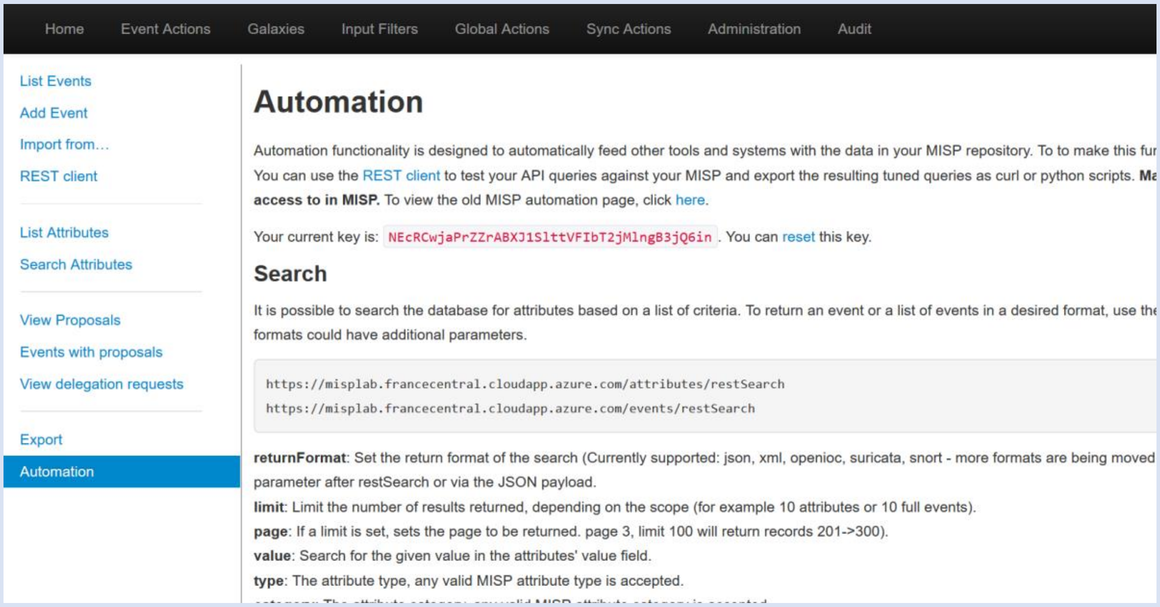
Line break separated list of headers in the "headername: value" format

Creator organisation: Team X

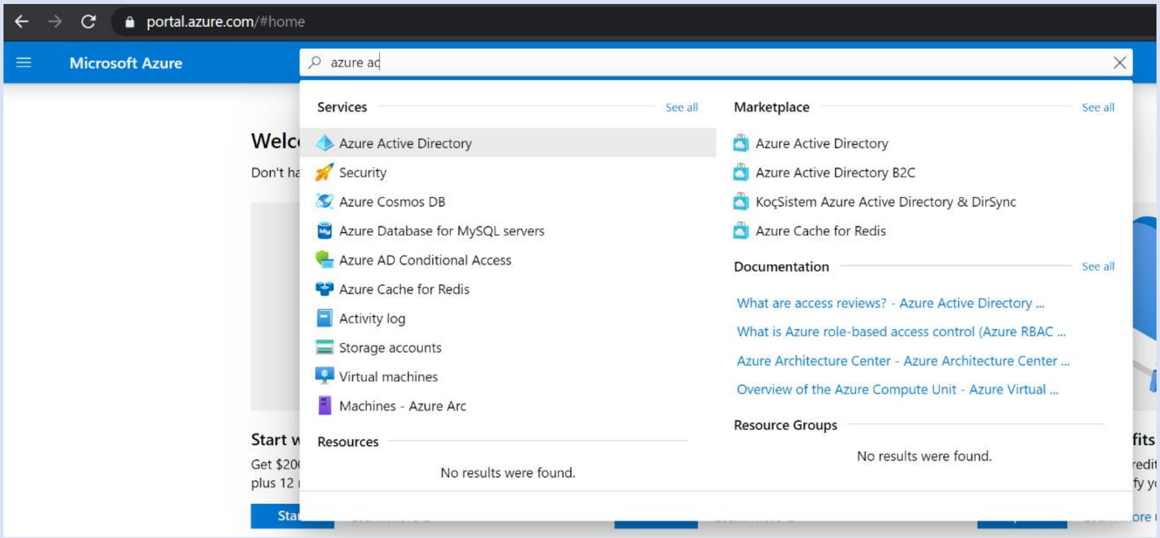
Target Event: Fixed Event

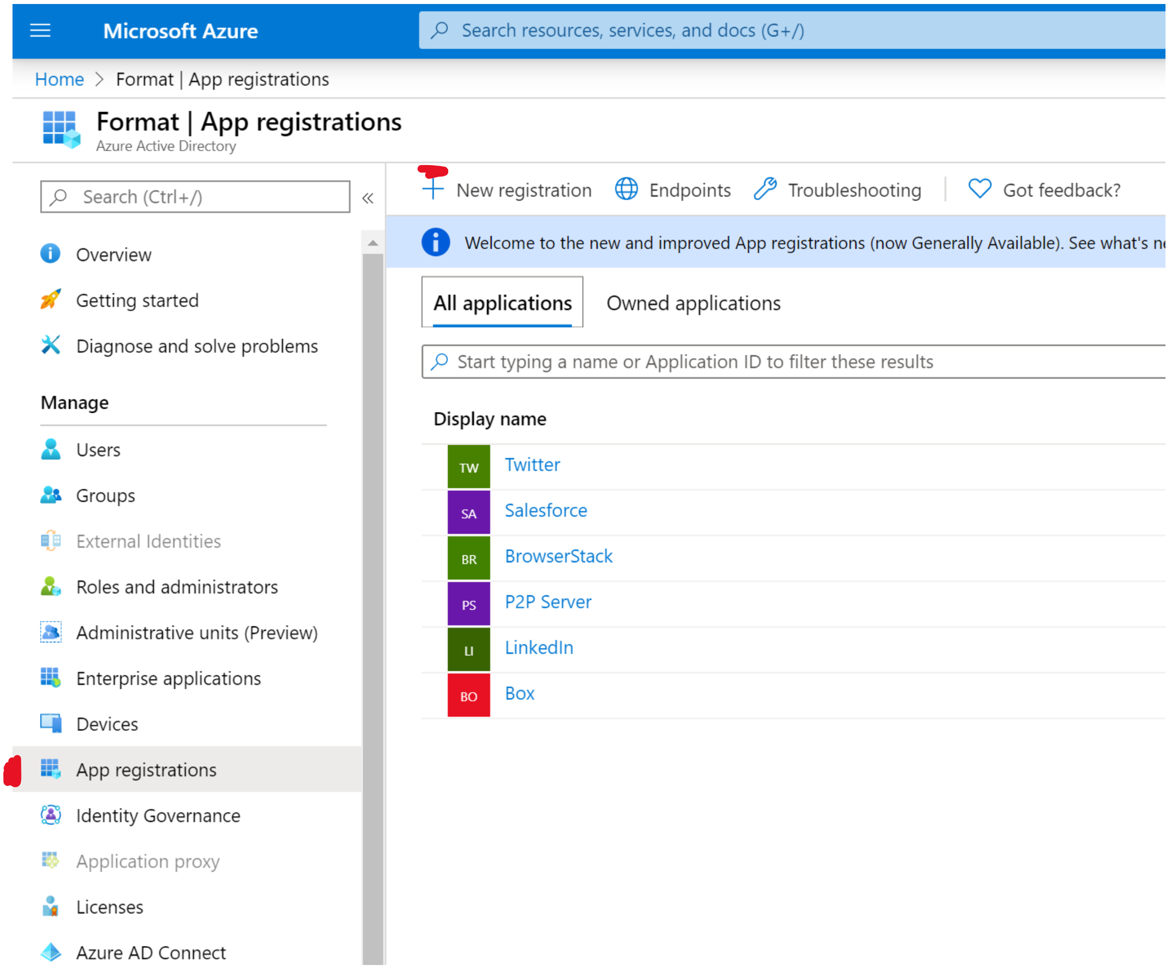
Step	Action
	 Target Event ID Leave blank unless you want to reuse an existing event. Value field(s) in the CSV 2 Delimiter , Exclusion Regex Regex pattern, for example: "/^https://myfeedurl/i ☑ Auto Publish ☐ Override IDS Flag ☐ Delta Merge Distribution Your organisation only Default Tag None **Filter rules:** Modify Add There are several other 3rd party feeds you may also want to enable and have available in your Sentinel workspace. Each of these will need to be enabled separately.
5.	The next step is to ensure that the feed is automatically updated. In the 'Scheduled Tasks' section of the Administration menu on the top set the fetch_feeds task frequency to 1h.

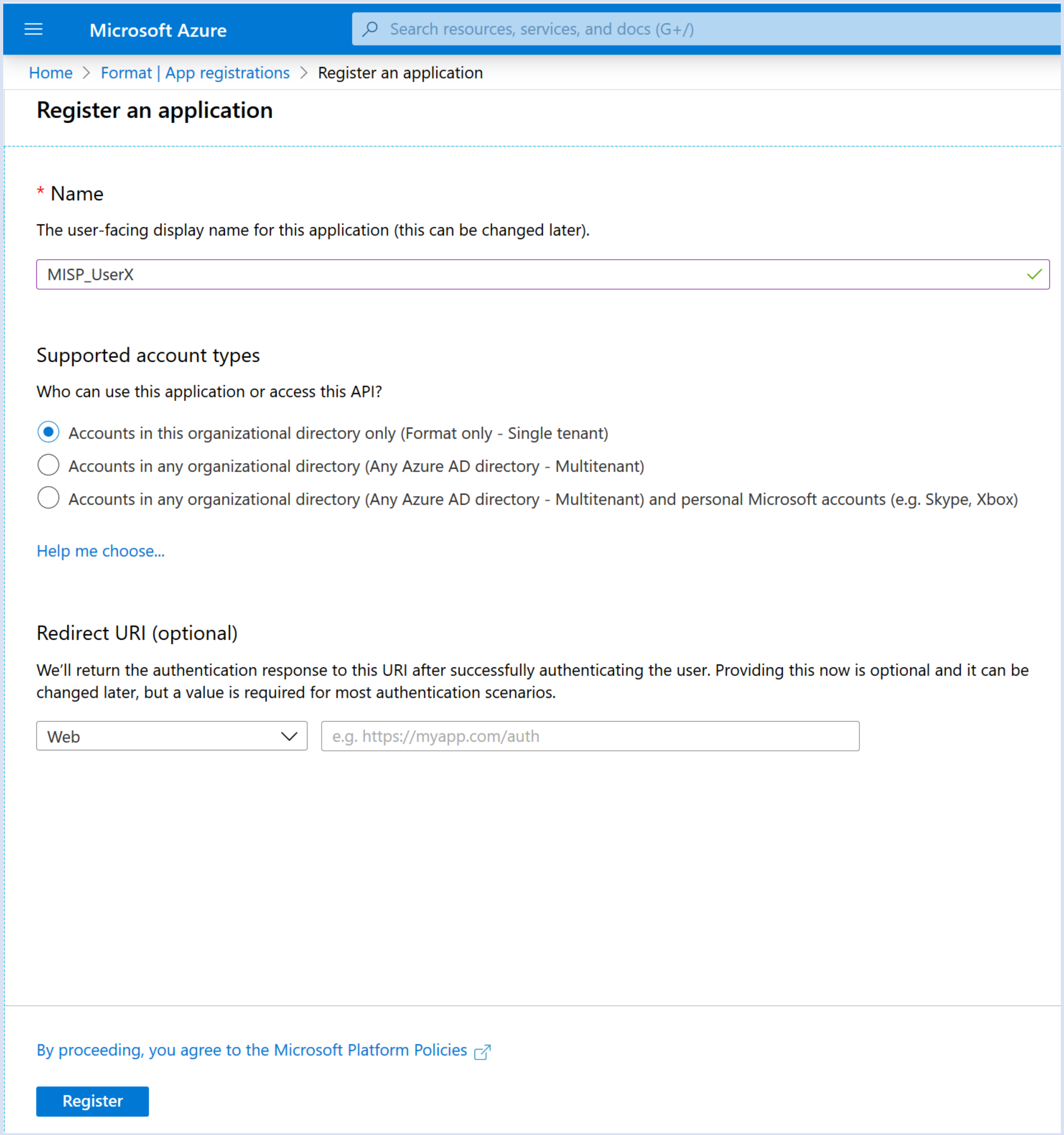
Step	Action

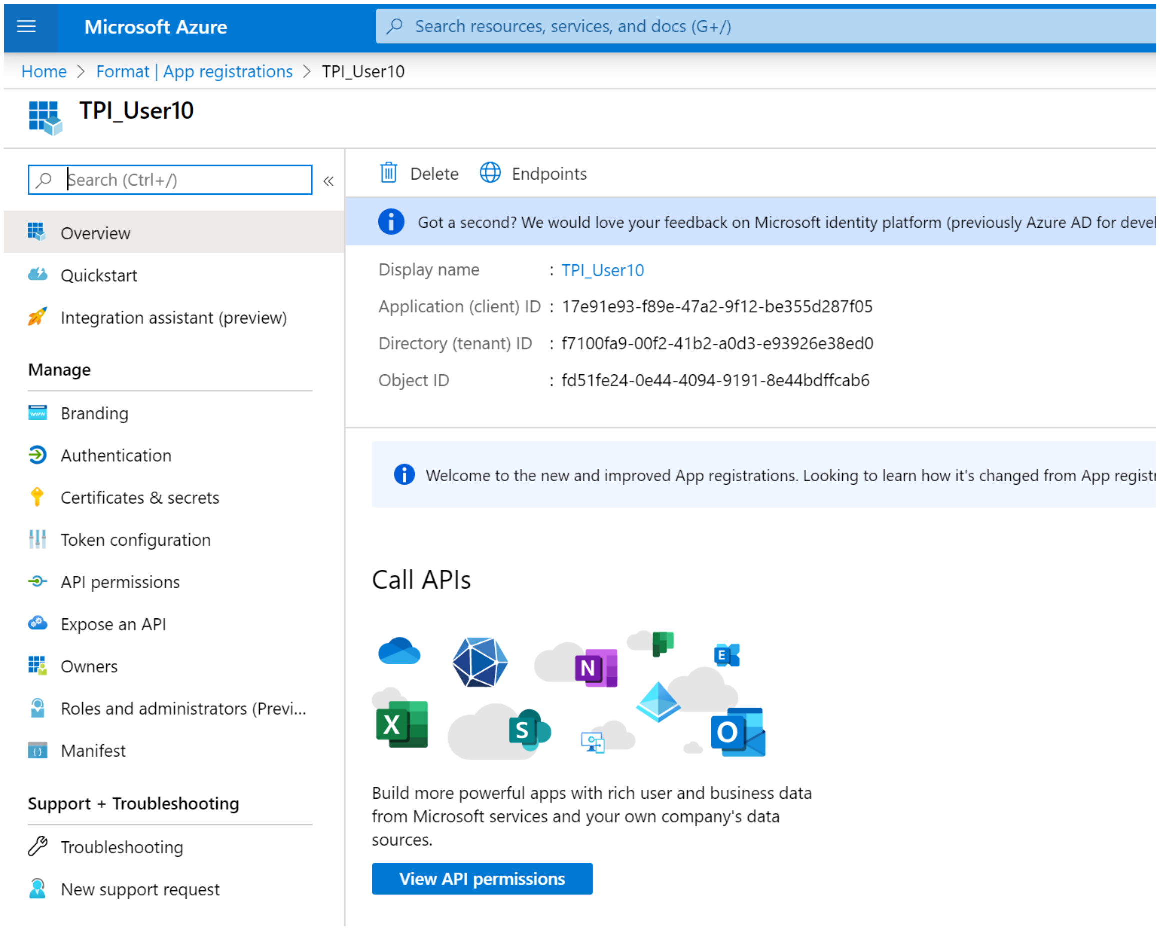
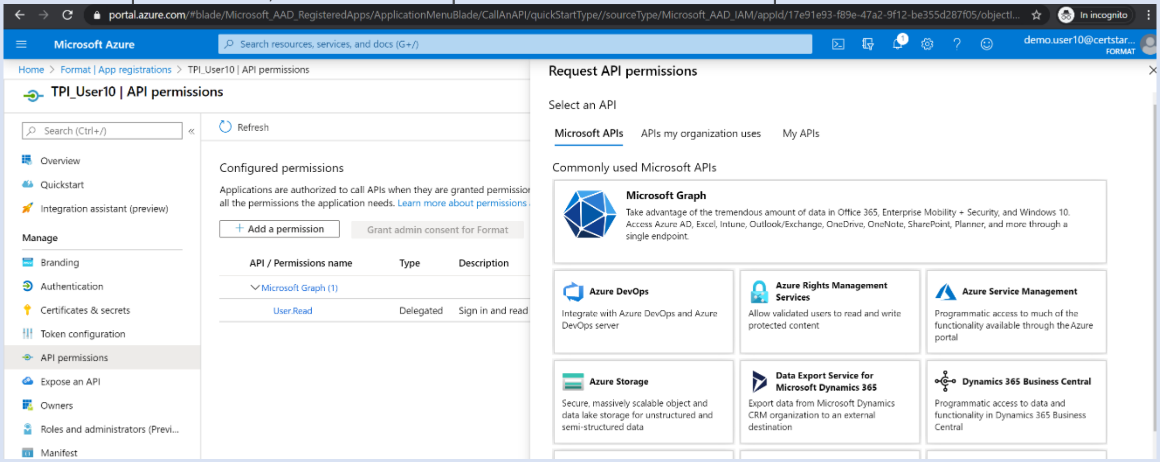
6.	Retrieve your MISP auth key.
	Within the MISP web interface click 'Event Actions' on the menu bar then select 'Automation'. Your MISP auth key will be listed on the screen, note this down for entry into the script later.
	
	 Home
	Event Actions
	Galaxies
	Input Filters
	Global Actions
	Sync Actions
	Administration
	Audit
	List Events
	Add Event
	Import from…
	REST client
	List Attributes
	Search Attributes
	View Proposals
	Events with proposals
	View delegation requests
	Export
	Automation
	Automation
	Automation functionality is designed to automatically feed other tools and systems with the data in your MISP repository. To to make this fur
	You can use the REST client to test your API queries against your MISP and export the resulting tuned queries as curl or python scripts. **Ma** **access to in MISP.** To view the old MISP automation page, click here.
	Your current key is: `NEcRCwjaPrZZrABXJ1SlttVFIbT2jMlngB3jQ6in`. You can reset this key.
	Search
	It is possible to search the database for attributes based on a list of criteria. To return an event or a list of events in a desired format, use the
	formats could have additional parameters.
	`https://misplab.francecentral.cloudapp.azure.com/attributes/restSearch`
	`https://misplab.francecentral.cloudapp.azure.com/events/restSearch`
	returnFormat: Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are being moved
	parameter after restSearch or via the JSON payload.
	limit: Limit the number of results returned, depending on the scope (for example 10 attributes or 10 full events).
	page: If a limit is set, sets the page to be returned. page 3, limit 100 will return records 201->300).
	value: Search for the given value in the attributes' value field.
	type: The attribute type, any valid MISP attribute type is accepted.
	MISP Auth Key is the red string.

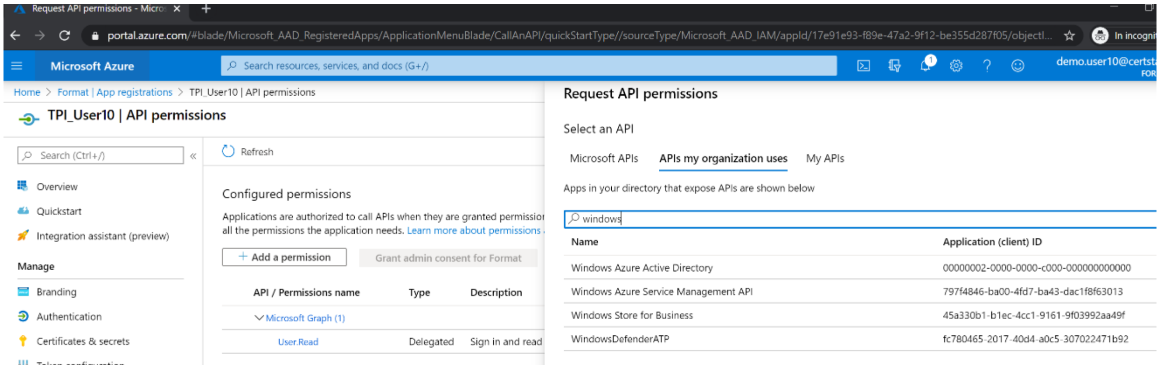
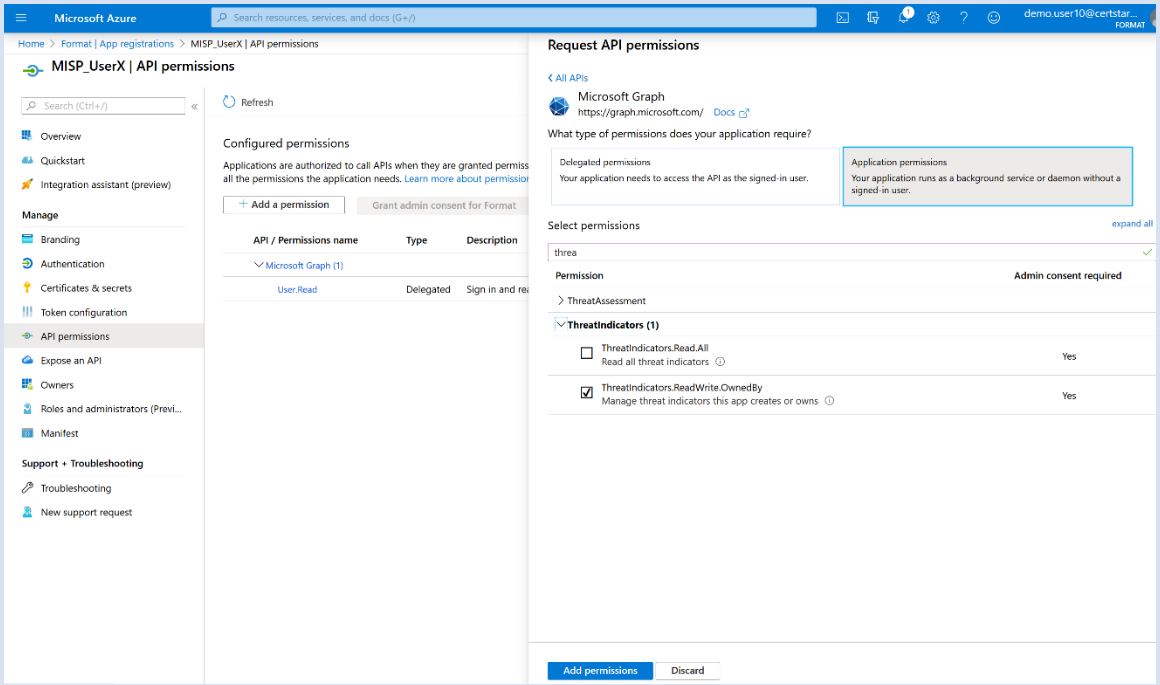
Task 2: Create an App Registration with the required permissions

Step	Action
1.	Login on https://portal.azure.com with credentials provided
2.	Search for Azure Active Directory service  portal.azure.com/#home Microsoft Azure azure ad Services See all Azure Active Directory Security Azure Cosmos DB Azure Database for MySQL servers Azure AD Conditional Access Azure Cache for Redis Activity log Storage accounts Virtual machines Machines - Azure Arc Resources No results were found. Marketplace See all Azure Active Directory Azure Active Directory B2C KoçSistem Azure Active Directory & DirSync Azure Cache for Redis Documentation See all What are access reviews? - Azure Active Directory ... What is Azure role-based access control (Azure RBAC ... Azure Architecture Center - Azure Architecture Center ... Overview of the Azure Compute Unit - Azure Virtual ... Resource Groups No results were found. Welc Don't ha Start w Get $200 plus 12 Sta

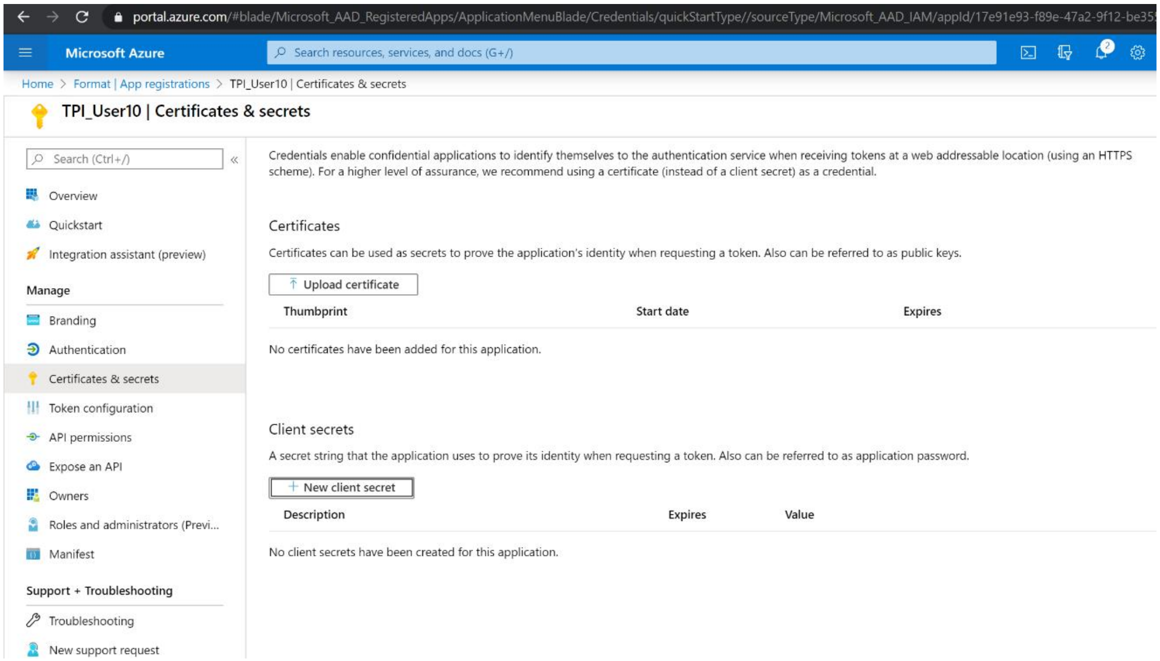
Step	Action
3.	Create new app registration. Azure AD → App Registration → + New Registration 

Step	Action
4.	Insert Name: “**MISP_UserX**”, select “Accounts in this organizational directory only (Format only - Single tenant)” and click Register  Microsoft Azure Search resources, services, and docs (G+/) Home > Format | App registrations > Register an application Register an application * Name The user-facing display name for this application (this can be changed later). MISP_UserX ✓ Supported account types Who can use this application or access this API? ● Accounts in this organizational directory only (Format only - Single tenant) ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) 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. Web e.g. https://myapp.com/auth By proceeding, you agree to the Microsoft Platform Policies Register

Step	Action
5.	take note of Application ID and Tenant ID  Home > Format | App registrations > TPI_User10 TPI_User10 Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for devel Display name : TPI_User10 Application (client) ID : 17e91e93-f89e-47a2-9f12-be355d287f05 Directory (tenant) ID : f7100fa9-00f2-41b2-a0d3-e93926e38ed0 Object ID : fd51fe24-0e44-4094-9191-8e44bdffcab6 Welcome to the new and improved App registrations. Looking to learn how it's changed from App registr Call APIs Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources. Microsoft Azure Search resources, services, and docs (G+/) Search (Ctrl+/) Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators (Previ... Manifest Support + Troubleshooting Troubleshooting New support request Delete Endpoints View API permissions
6.	Under API permissions, choose Add a permission > Microsoft Graph.  portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be355d287f05/objectI... demo.user10@certstar... FORMAT Home > Format | App registrations > TPI_User10 | API permissions TPI_User10 | API permissions Configured permissions Applications are authorized to call APIs when they are granted permissio all the permissions the application needs. Learn more about permissions API / Permissions name — Type — Description Microsoft Graph (1) User.Read — Delegated — Sign in and read Request API permissions Select an API Commonly used Microsoft APIs Microsoft Graph: Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint. Azure DevOps: Integrate with Azure DevOps and Azure DevOps server Azure Rights Management Services: Allow validated users to read and write protected content Azure Service Management: Programmatic access to much of the functionality available through the Azure portal Azure Storage: Secure, massively scalable object and data lake storage for unstructured and semi-structured data Data Export Service for Microsoft Dynamics 365: Export data from Microsoft Dynamics CRM organization to an external destination Dynamics 365 Business Central: Programmatic access to data and functionality in Dynamics 365 Business Central In incognito Microsoft Azure Search resources, services, and docs (G+/) Search (Ctrl+/) Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators (Previ... Manifest Refresh + Add a permission Grant admin consent for Format Microsoft APIs APIs my organization uses My APIs

Step	Action
7.	Search anc click on "WindowsDefenderATP"  Request API permissions - Micro portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be355d287f05/objectI... In incogni Microsoft Azure Search resources, services, and docs (G+/) demo.user10@certst... Home > Format | App registrations > TPI_User10 | API permissions TPI_User10 | API permissions Search (Ctrl+/) Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Refresh Configured permissions Applications are authorized to call APIs when they are granted permissio... all the permissions the application needs. Learn more about permissions + Add a permission Grant admin consent for Format API / Permissions name Type Description Microsoft Graph (1) User.Read Delegated Sign in and read Request API permissions Select an API Microsoft APIs APIs my organization uses My APIs Apps in your directory that expose APIs are shown below windows Name | Application (client) ID Windows Azure Active Directory | 00000002-0000-0000-c000-000000000000 Windows Azure Service Management API | 797f4846-ba00-4fd7-ba43-dac1f8f63013 Windows Store for Business | 45a330b1-b1ec-4cc1-9161-9f03992aa49f WindowsDefenderATP | fc780465-2017-40d4-a0c5-307022471b92
8.	Under Application Permissions, add ThreatIndicators.ReadWrite.OwnedBy.  Microsoft Azure Search resources, services, and docs (G+/) demo.user10@certstar... FORMAT Home > Format | App registrations > MISP_UserX | API permissions MISP_UserX | API permissions Search (Ctrl+/) Overview Quickstart Integration assistant (preview) Manage Branding Authentication Certificates & secrets Token configuration API permissions Expose an API Owners Roles and administrators (Previ... Manifest Support + Troubleshooting Troubleshooting New support request Refresh Configured permissions Applications are authorized to call APIs when they are granted permiss... all the permissions the application needs. Learn more about permission + Add a permission Grant admin consent for Format API / Permissions name Type Description Microsoft Graph (1) User.Read Delegated Sign in and rea Request API permissions < All APIs Microsoft Graph https://graph.microsoft.com/ Docs What type of permissions does your application require? Delegated permissions Your application needs to access the API as the signed-in user. Application permissions Your application runs as a background service or daemon without a signed-in user. Select permissions expand all threa Permission | Admin consent required > ThreatAssessment ThreatIndicators (1) □ ThreatIndicators.Read.All — Read all threat indicators | Yes ☑ ThreatIndicators.ReadWrite.OwnedBy — Manage threat indicators this app creates or owns | Yes Add permissions Discard
9.	Note message: "You are editing permission(s) to your application, users will have to consent even if they've already done so previously." That means Global Admin consent is required
10	Send message on General Teams channel with your Team Name asking for consent. Tutors will apply Consent to you App Registration

Step	Action
11	Create a new client secret in “Certificate” & Secrets”



portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Credentials/quickStartType//sourceType/Microsoft_AAD_IAM/appId/17e91e93-f89e-47a2-9f12-be35

TPI_User10 | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

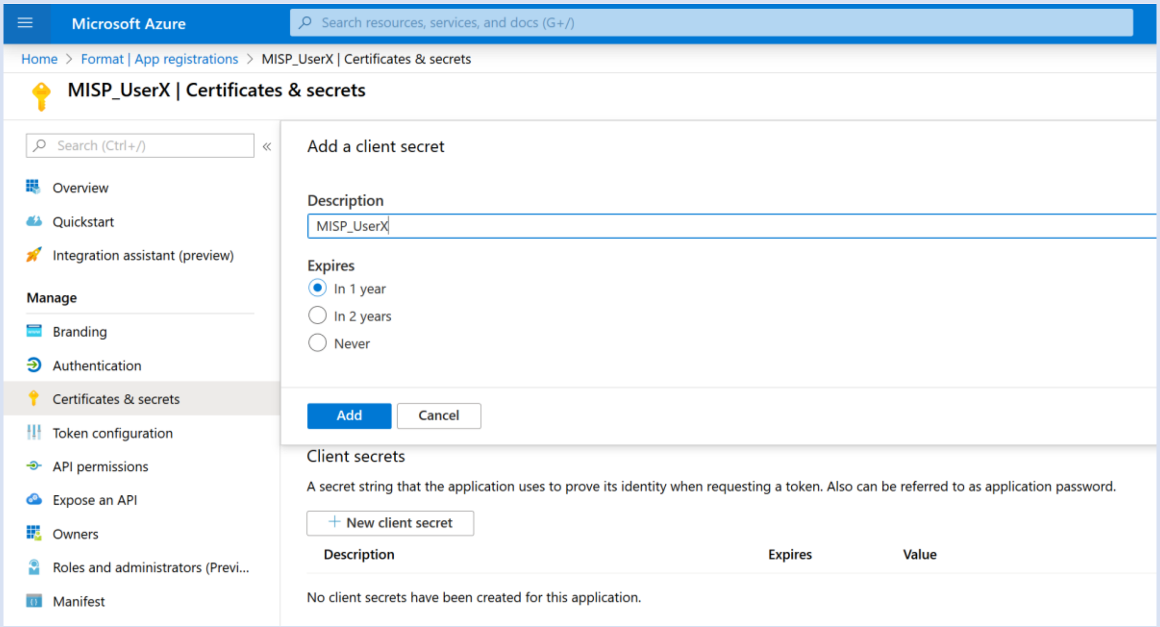
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

Step	Action
12	Click “+ New client secret” → Add Description “MISP_UserX”, Select 1 year and click Add



MISP_UserX | Certificates & secrets

Add a client secret

Description: MISP_UserX

Expires

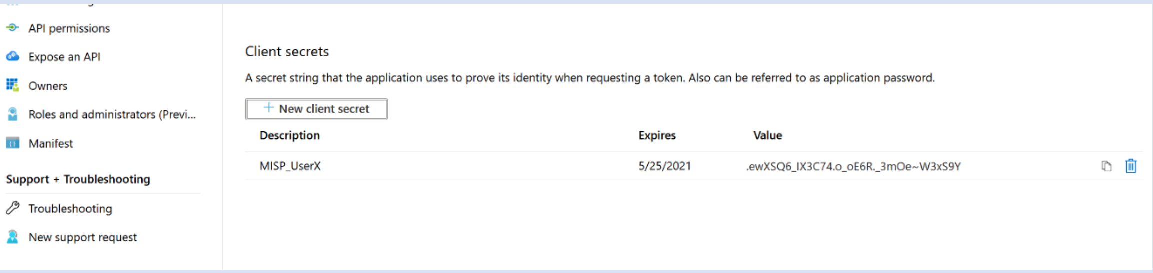
- ● In 1 year
- ○ In 2 years
- ○ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
MISP_UserX	5/25/2021	.ewXSQ6_IX3C74.o_oE6R._3mOe~W3xS9Y

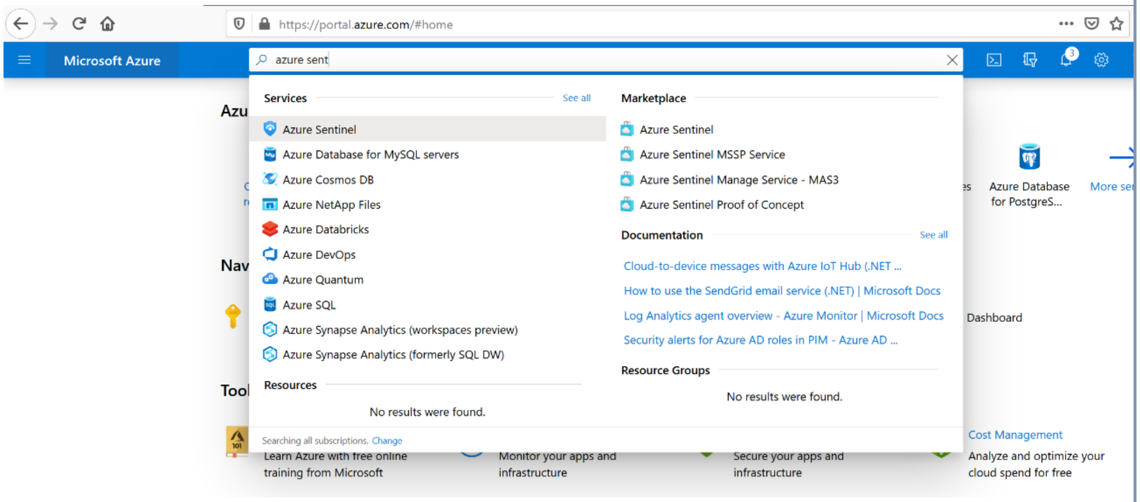
Step	Action
13	Copy Value on your text editor.

Task 3: Enable Azure Sentinel Connector

Step	Action

1. Login on https://portal.azure.com with credentials provided and open your Azure Sentinel Workspace.

- https://portal.azure.com
- Search for “Azure Sentinel”



https://portal.azure.com/#home

Microsoft Azure

azure sent

Services See all

- Azure Sentinel
- Azure Database for MySQL servers
- Azure Cosmos DB
- Azure NetApp Files
- Azure Databricks
- Azure DevOps
- Azure Quantum
- Azure SQL
- Azure Synapse Analytics (workspaces preview)
- Azure Synapse Analytics (formerly SQL DW)

Resources

No results were found.

Searching all subscriptions. Change

Marketplace

- Azure Sentinel
- Azure Sentinel MSSP Service
- Azure Sentinel Manage Service - MAS3
- Azure Sentinel Proof of Concept

Documentation See all

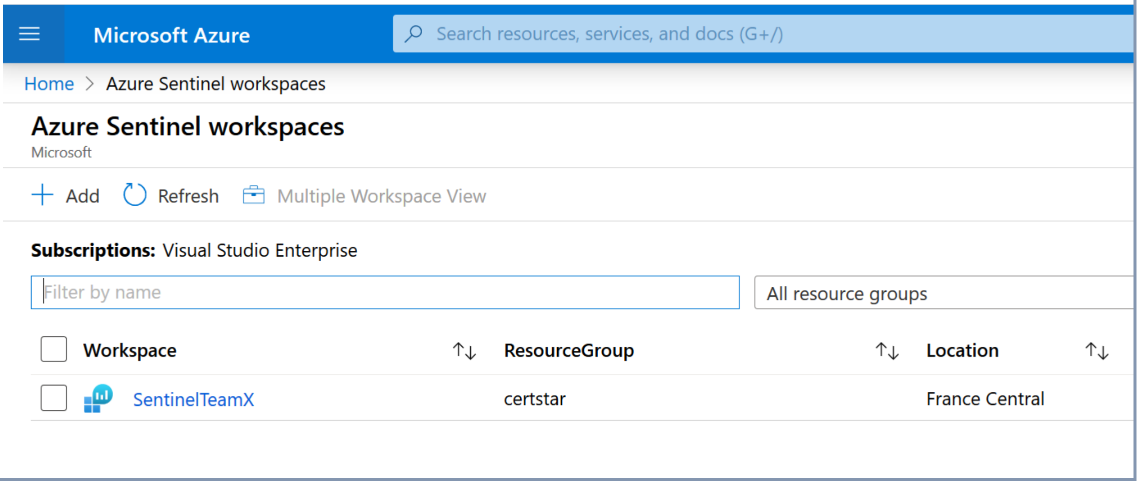
- Cloud-to-device messages with Azure IoT Hub (.NET ...
- How to use the SendGrid email service (.NET) | Microsoft Docs
- Log Analytics agent overview - Azure Monitor | Microsoft Docs
- Security alerts for Azure AD roles in PIM - Azure AD ...

Resource Groups

No results were found.

Azu
Nav
Tool
Azure Database for PostgreS...
More ser
Dashboard
Cost Management
Learn Azure with free online training from Microsoft
Monitor your apps and infrastructure
Secure your apps and infrastructure
Analyze and optimize your cloud spend for free

-
- Select your workspace → SentinelTeamX



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Azure Sentinel workspaces

Azure Sentinel workspaces

Microsoft

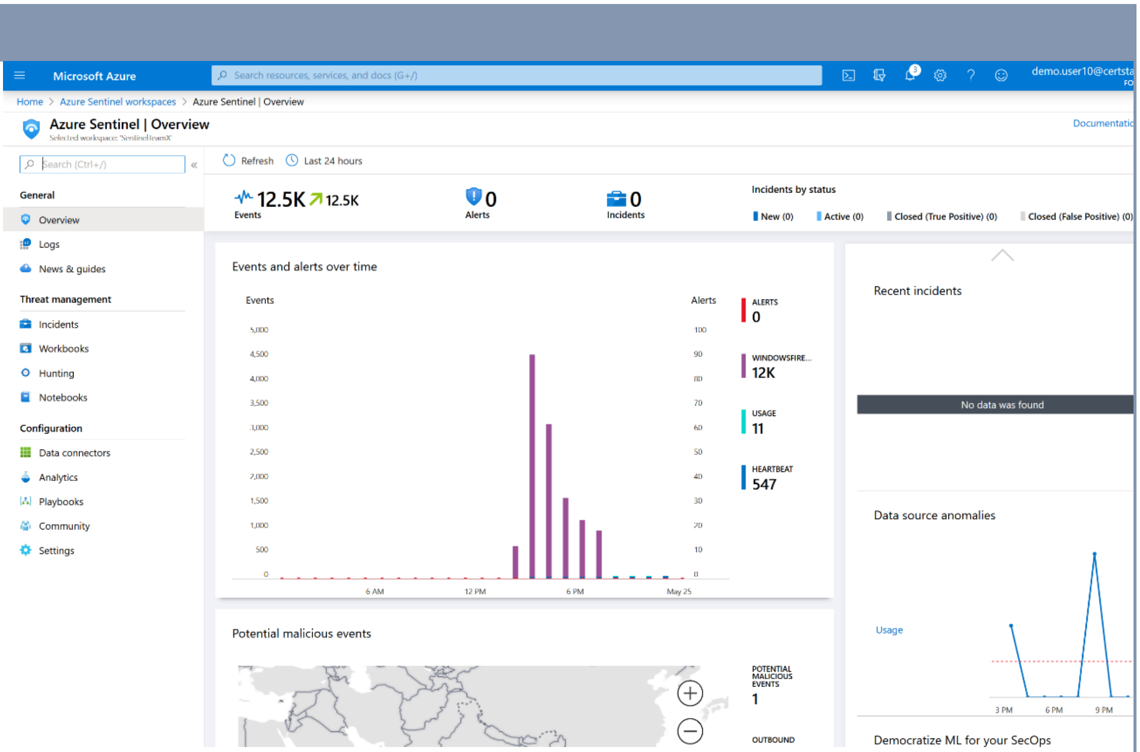
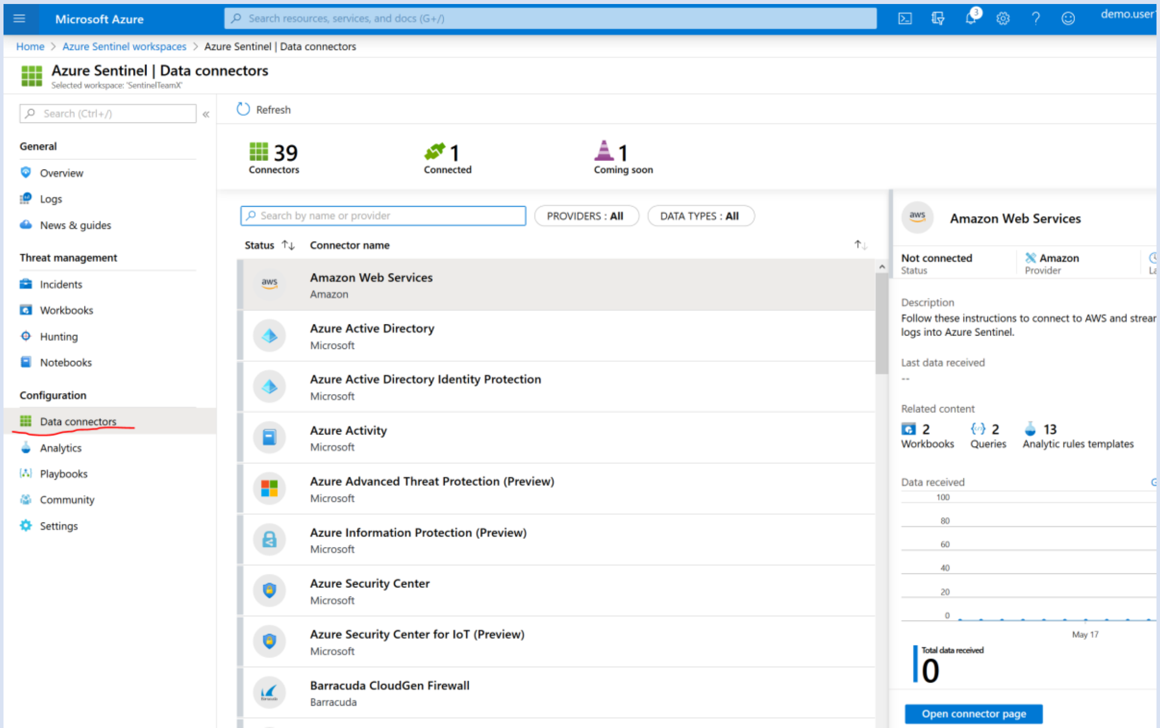
Subscriptions: Visual Studio Enterprise

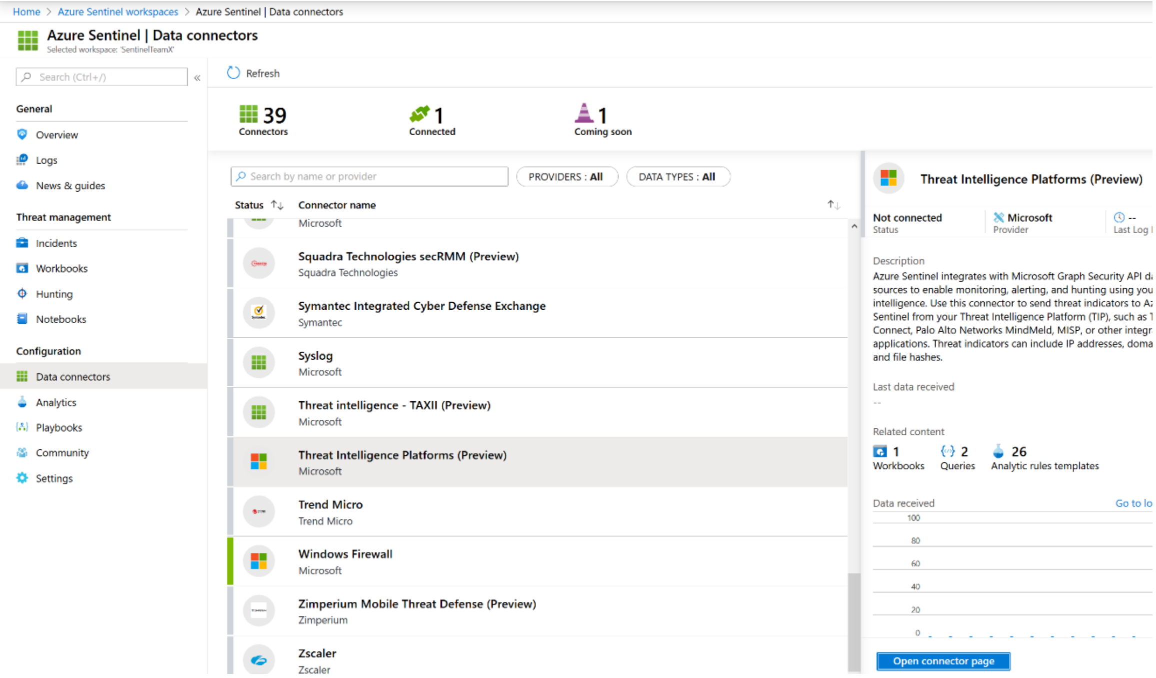
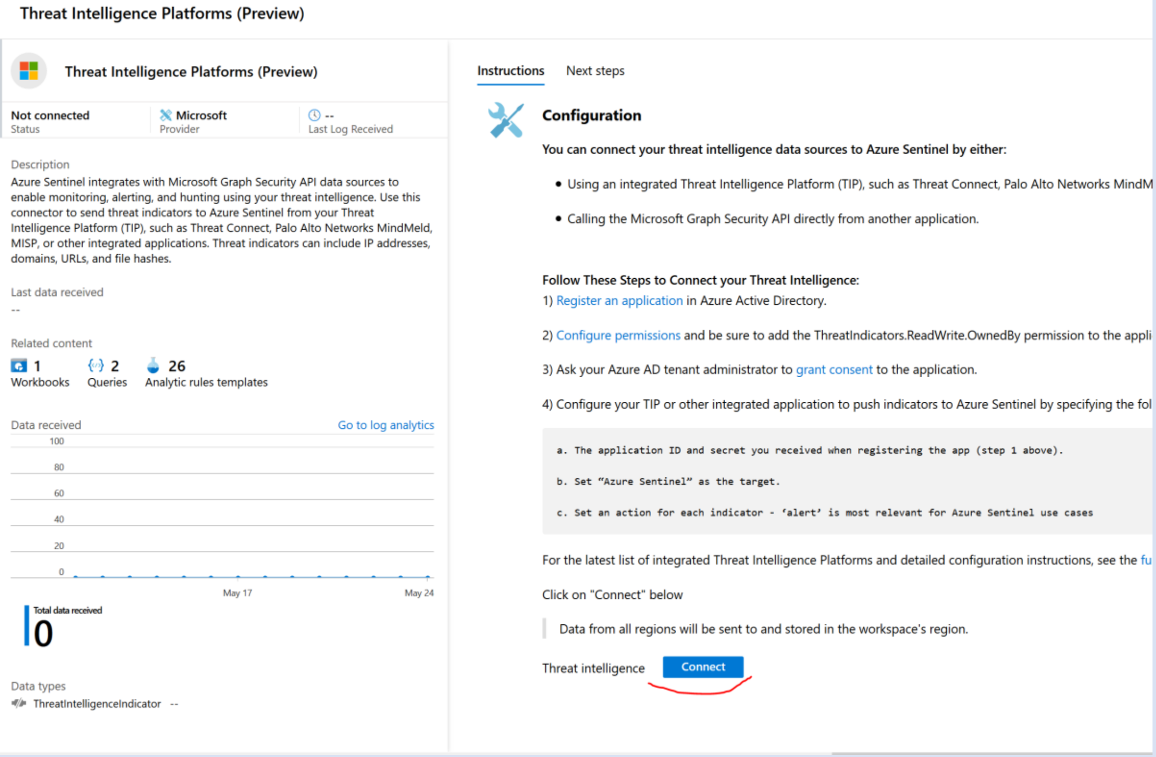
Filter by name

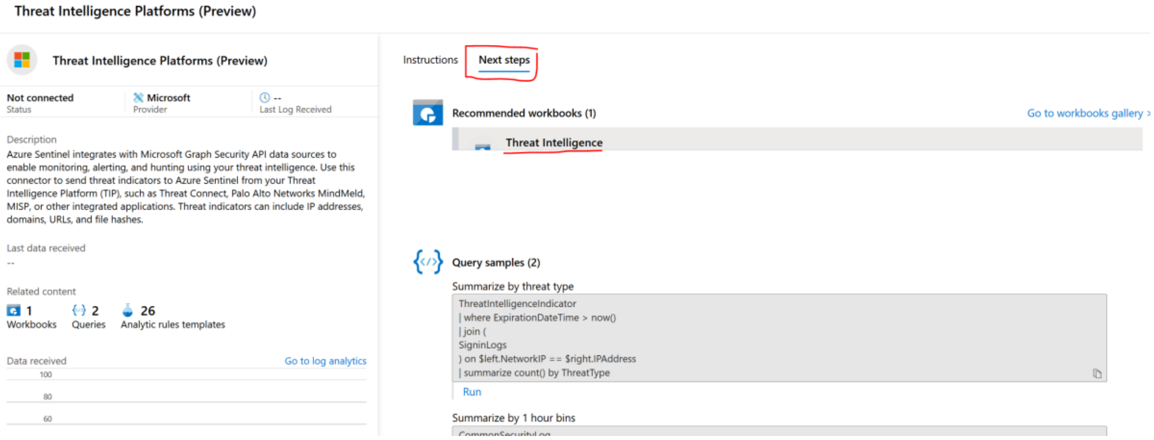
All resource groups

□	Workspace ↑↓	ResourceGroup ↑↓	Location ↑↓
□	SentinelTeamX	certstar	France Central

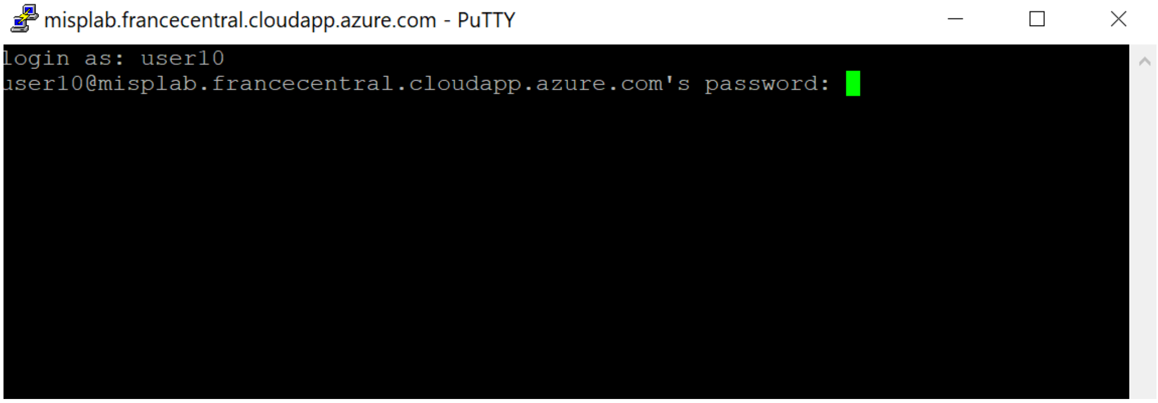
-

Step	Action
	 •
2.	Click on Data Connector 

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>3.</td><td>click ‘Data connectors’ and then look for the ‘Threat Intelligence Platforms’ connection. Open the connector

Home > Azure Sentinel workspaces > Azure Sentinel | Data connectors
Azure Sentinel | Data connectors
Selected workspace: 'SentinelTeamX'
Refresh
39 Connectors · 1 Connected · 1 Coming soon
PROVIDERS : All · DATA TYPES : All
Status · Connector name
Microsoft
Squadra Technologies secRMM (Preview) — Squadra Technologies
Symantec Integrated Cyber Defense Exchange — Symantec
Syslog — Microsoft
Threat intelligence - TAXII (Preview) — Microsoft
Threat Intelligence Platforms (Preview) — Microsoft
Trend Micro — Trend Micro
Windows Firewall — Microsoft
Zimperium Mobile Threat Defense (Preview) — Zimperium
Zscaler — Zscaler
Threat Intelligence Platforms (Preview)
Not connected Status · Microsoft Provider · -- Last Log I
Description
Azure Sentinel integrates with Microsoft Graph Security API da sources to enable monitoring, alerting, and hunting using you intelligence. Use this connector to send threat indicators to Az Sentinel from your Threat Intelligence Platform (TIP), such as T Connect, Palo Alto Networks MindMeld, MISP, or other integr applications. Threat indicators can include IP addresses, doma and file hashes.
Last data received
--
Related content
1 Workbooks · 2 Queries · 26 Analytic rules templates
Data received · Go to lo
</td></tr>
<tr><td>4.</td><td>Click “Connect”

Threat Intelligence Platforms (Preview)
Threat Intelligence Platforms (Preview)
Not connected Status · Microsoft Provider · -- Last Log Received
Description
Azure Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Azure Sentinel from your Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. Threat indicators can include IP addresses, domains, URLs, and file hashes.
Last data received
--
Related content
1 Workbooks · 2 Queries · 26 Analytic rules templates
Data received · Go to log analytics
Total data received 0
Data types
ThreatIntelligenceIndicator --
Configuration
You can connect your threat intelligence data sources to Azure Sentinel by either:
• Using an integrated Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindM
• Calling the Microsoft Graph Security API directly from another application.
Follow These Steps to Connect your Threat Intelligence:
1) Register an application in Azure Active Directory.
2) Configure permissions and be sure to add the ThreatIndicators.ReadWrite.OwnedBy permission to the appli
3) Ask your Azure AD tenant administrator to grant consent to the application.
4) Configure your TIP or other integrated application to push indicators to Azure Sentinel by specifying the fol
a. The application ID and secret you received when registering the app (step 1 above).
b. Set “Azure Sentinel” as the target.
c. Set an action for each indicator - ‘alert’ is most relevant for Azure Sentinel use cases
For the latest list of integrated Threat Intelligence Platforms and detailed configuration instructions, see the fu
Click on "Connect" below
Data from all regions will be sent to and stored in the workspace's region.
Threat intelligence · Connect
</td></tr>
</table>

Step	Action
5.	Click “Next Steps” →“Threat Intelligence” under Recommended workbooks  Threat Intelligence Platforms (Preview) Threat Intelligence Platforms (Preview) Not connected Status · Microsoft Provider · -- Last Log Received Description Azure Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Azure Sentinel from your Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. Threat indicators can include IP addresses, domains, URLs, and file hashes. Last data received -- Related content 1 Workbooks · 2 Queries · 26 Analytic rules templates Data received · Go to log analytics 100 80 60 Instructions · Next steps Recommended workbooks (1) · Go to workbooks gallery › Threat Intelligence Query samples (2) Summarize by threat type ThreatIntelligenceIndicator | where ExpirationDateTime > now() | join (SigninLogs) on $left.NetworkIP == $right.IPAddress | summarize count() by ThreatType Run Summarize by 1 hour bins CommonSecurityLog
6.	
7.	

Task 4: Setup the script

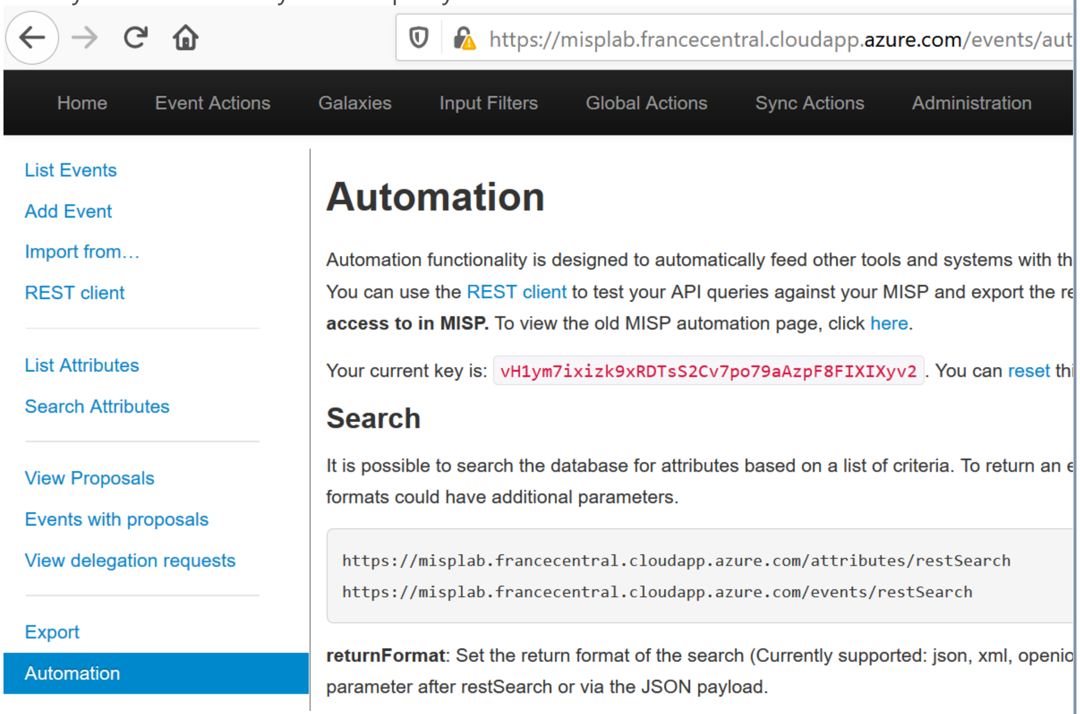
Step	Action
1.	Using putty (or your preferred SSH client) logon to: **misplab.francecentral.cloudapp.azure.com** using credential provided  misplab.francecentral.cloudapp.azure.com - PuTTY login as: user10 user10@misplab.francecentral.cloudapp.azure.com's password:

Step	Action
2.	Enter the following commands. These will create an environment for the script to run, download it from GitHub, install the necessary prerequisites and open the configuration file.

```
sudo apt-get install python3-venv
python3 -m venv mispToSentinel
cd mispToSentinel
source bin/activate
git clone https://github.com/microsoftgraph/security-api-solutions
cd security-api-solutions/Samples/MISP/
pip install -r requirements.txt
nano config.py
```

Step	Action
3.	There are a few options that need to be changed in the configuration file:

- Under the graph_auth key enter the details from the AAD App Registration earlier.
- Set the '<targetProduct>' to be 'Azure Sentinel'.
- I added a # comment at the start of each line in the misp_event_filters section to effectively disable any filtering, all data from the MISP server will be available in Sentinel.
- Set '<action>' to 'alert'.
- Enter you MISP auth key in '<misp key>→ MISP GUI →Event Action →Automation



Automation

Automation functionality is designed to automatically feed other tools and systems with th
You can use the REST client to test your API queries against your MISP and export the re
access to in MISP. To view the old MISP automation page, click here.

Your current key is: `vH1ym7ixizk9xRDTsS2Cv7po79aAzpF8FIXIXyv2`. You can reset thi

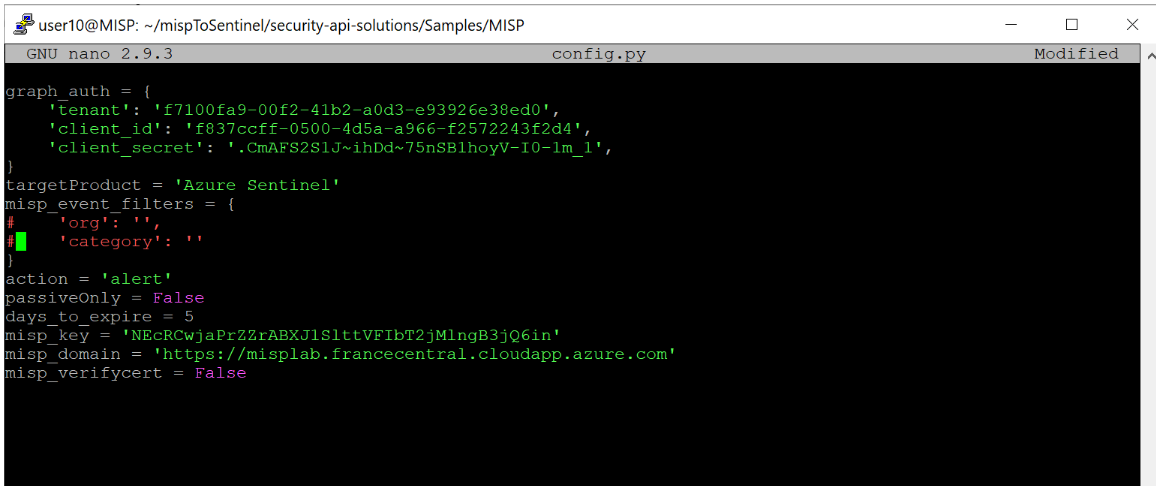
Search

It is possible to search the database for attributes based on a list of criteria. To return an e
formats could have additional parameters.

```
https://misplab.francecentral.cloudapp.azure.com/attributes/restSearch
https://misplab.francecentral.cloudapp.azure.com/events/restSearch
```

returnFormat: Set the return format of the search (Currently supported: json, xml, openio
parameter after restSearch or via the JSON payload.

-
- Enter MISP URL in '<misp url>= https://misplab.francecentral.cloudapp.azure.com'.
- Finally set the lifetime for this data, I would recommend 30-60 days depending on your use case.

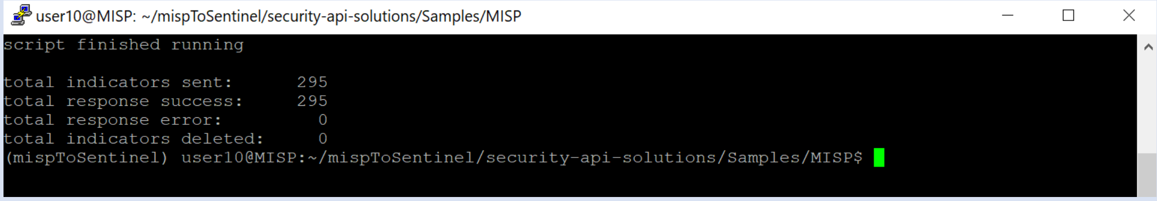

user10@MISP: ~/mispToSentinel/security-api-solutions/Samples/MISP

```
  GNU nano 2.9.3                              config.py                              Modified

graph_auth = {
    'tenant': 'f7100fa9-00f2-41b2-a0d3-e93926e38ed0',
    'client_id': 'f837ccff-0500-4d5a-a966-f2572243f2d4',
    'client_secret': '.CmAFS2S1J~ihDd~75nSB1hoyV-I0-1m_1',
}
targetProduct = 'Azure Sentinel'
misp_event_filters = {
#     'org': '',
#     'category': ''
}
action = 'alert'
passiveOnly = False
days_to_expire = 5
misp_key = 'NEcRCwjaPrZZrABXJ1SlttVFIbT2jMlngB3jQ6in'
misp_domain = 'https://misplab.francecentral.cloudapp.azure.com'
misp_verifycert = False
```

Ctrl + X → Yes

Step	Action

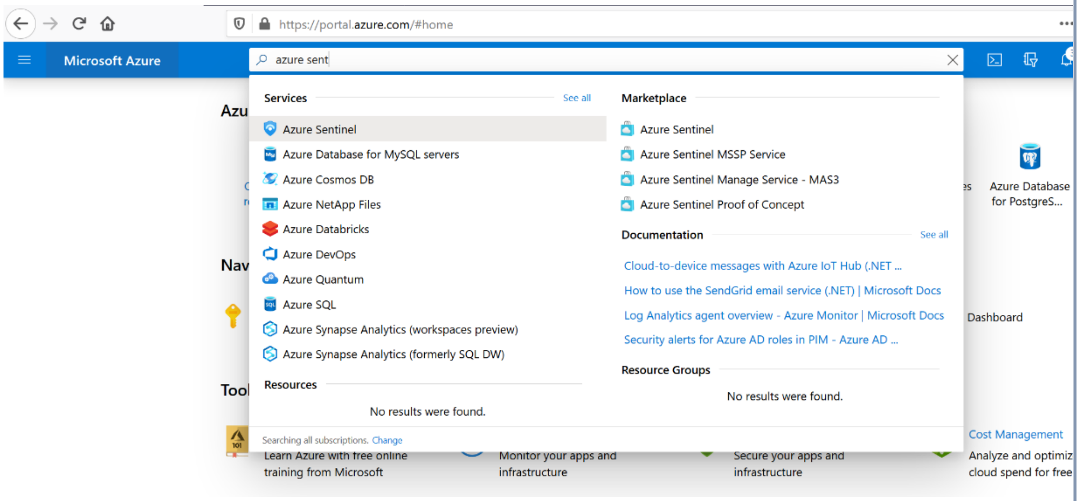
4.	You can now run the script to pull data from the MISP instance and push into your Sentinel workspace.
	`python script.py`
	
	user10@MISP: ~/mispToSentinel/security-api-solutions/Samples/MISP
	`script finished running`
	`total indicators sent:      295`
	`total response success:     295`
	`total response error:         0`
	`total indicators deleted:      0`
	`(mispToSentinel) user10@MISP:~/mispToSentinel/security-api-solutions/Samples/MISP$`

Task 5: Use the data

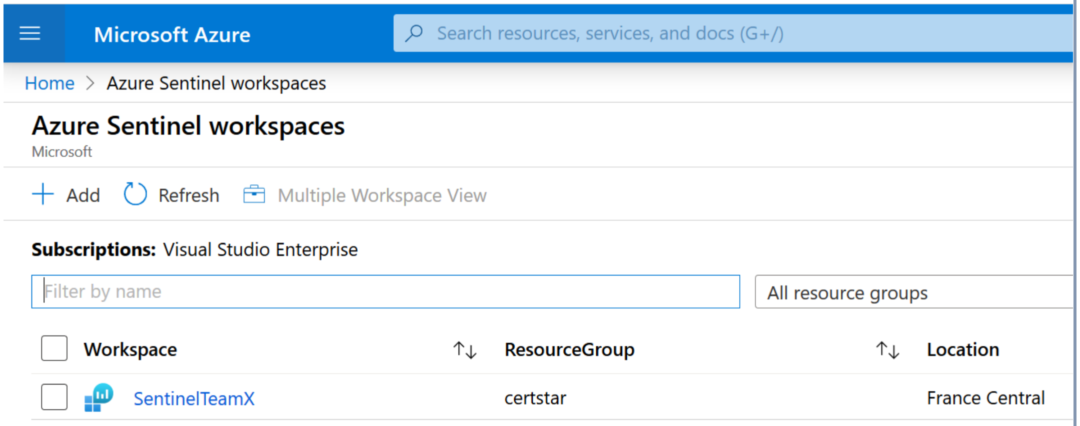
Step	Action
1.	Login on https://portal.azure.com with credentials provided and open your Azure Sentinel Workspace.
2.	After a few minutes you should be able to query the ThreatIntelligenceIndicator table in your Sentinel workspace. Click on "Logs" section and type search:

Step 1:

- https://portal.azure.com
- Search for "Azure Sentinel"


https://portal.azure.com/#home
Microsoft Azure
azure sent
Services
See all
Azure Sentinel
Azure Database for MySQL servers
Azure Cosmos DB
Azure NetApp Files
Azure Databricks
Azure DevOps
Azure Quantum
Azure SQL
Azure Synapse Analytics (workspaces preview)
Azure Synapse Analytics (formerly SQL DW)
Resources
No results were found.
Searching all subscriptions. Change
Marketplace
Azure Sentinel
Azure Sentinel MSSP Service
Azure Sentinel Manage Service - MAS3
Azure Sentinel Proof of Concept
Documentation
See all
Cloud-to-device messages with Azure IoT Hub (.NET ...
How to use the SendGrid email service (.NET) | Microsoft Docs
Log Analytics agent overview - Azure Monitor | Microsoft Docs
Security alerts for Azure AD roles in PIM - Azure AD ...
Resource Groups
No results were found.
Azure Database for PostgreS...
Dashboard
Cost Management
Analyze and optimiz cloud spend for free
Learn Azure with free online training from Microsoft
Monitor your apps and infrastructure
Secure your apps and infrastructure

- Select your workspace → SentinelTeamX


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Sentinel workspaces
Azure Sentinel workspaces
Microsoft
+ Add
Refresh
Multiple Workspace View
Filter by name
All resource groups

Subscriptions: Visual Studio Enterprise

□ Workspace	ResourceGroup	Location
□ SentinelTeamX	certstar	France Central

Step 2:

```
ThreatIntelligenceIndicator
| count
```

.

Authors

The following authors contributed to the creation of this deliverable.

Antonio Formato Antonio.Formato@Microsoft.com	Technical Specialist Security & Compliance	https://www.linkedin.com/in/antonioformato/
Rebecca Travasi Rebecca.Travasi@microsoft.com	Technical Specialist Security & Compliance	https://www.linkedin.com/in/rebeccatravasi/

References

- https://techcommunity.microsoft.com/t5/azure-sentinel/integrating-open-source-threat-feeds-with-misp-and-sentinel/ba-p/1350371#
- https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence
- https://github.com/format81/CERTStarLAB
- https://github.com/microsoftgraph/security-api-solutions/tree/master/Samples/MISP
- https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Microsoft.Covid19.Indicators.csv
- https://www.microsoft.com/security/blog/2020/05/14/open-sourcing-covid-threat-intelligence/
- https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld
- https://live.paloaltonetworks.com/t5/minemeld/ct-p/MineMeld
- https://github.com/PaloAltoNetworks/minemeld/wiki
- https://www.misp-project.org/
- https://github.com/MISP/MISP