LTRSEC-2724

Stopping the lastest attacks with Email Threat Defense

A hand on lab covering Protection of Mail Platforms, Best Practices, and API Automation

Greg Barnes - TME
Alberto Torralba - TME

Cisco Secure Email Threat Defense Lab

Last Updated: February - 2025

IMPORTANT! This content is community-developed and is not subject to standard Cisco verification or support.

About This Lab

In this lab, you'll explore Cisco Secure Email Threat Defense (ETD), a powerful solution designed to safeguard email environments against advanced threats. Email remains one of the most common and high-risk channels for cyberattacks, with threats ranging from spam and phishing to sophisticated malware and Business Email Compromise (BEC) attacks. Cisco Secure Email Threat Defense integrates seamlessly with on-premises or cloud-based email systems, providing real-time protection through machine learning, threat intelligence, and advanced analytics.

Objectives

This hands-on lab will guide you through key features of ETD:
Setting up and Connection to MS365: Learn the simple process of setting up ETD and connecting it to Microsoft 365 environments
Policy Configuration: Learn to set up policies for detecting and mitigating various threats, including phishing attempts, malware, and spam.
Threat Intelligence: Discover how Cisco leverages AI/ML/others, to identify and block new and emerging threats in real-time.
Reporting and Analytics: Use the ETD dashboard to view threat reports and analyze trends, giving you insights into email security within your organization.
Integration and APIs: Understand how to leverage REST APIs to build powerful integration between ETD and your Security applications and/or processes.

Lab Structure
Throughout this lab, you'll configure security policies, test threat detection capabilities, and monitor and respond to malicious messages. By the end, you should have a robust understanding of how Cisco Secure Email Threat Defense can strengthen your organization's email security posture.

Let's get started on securing email communications and defending against today's most advanced email-based threats!

Table of Contents

Requirements

This lab will use cloud-based applications and solutions. It is not a requirement to install any application on your laptop, although you have the option to do so.
The requirements are:

- Laptop
- Internet connectivity
- Mobile phone to install the Cisco DUO mobile app

During this lab, we will create accounts on:

- Cisco Email Threat Defense
- Postman Cloud
- Cisco DUO
- Free Email Service (you can also use any other business email account)

About This Solution

Email Threat Defense augments native Microsoft 365 security and provides complete visibility to inbound, outbound, and internal user-to-user messages.

With Email Threat Defense customers can:

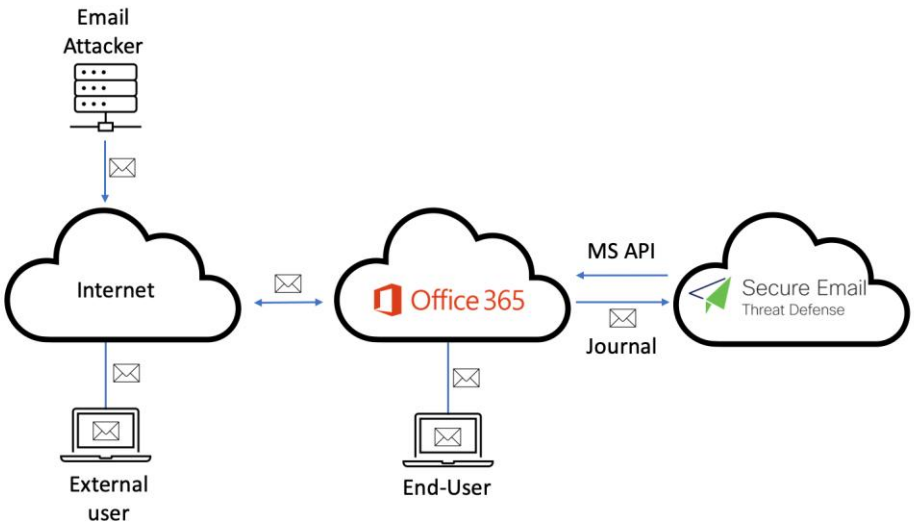
- Detect and block threats with superior threat intelligence from Cisco Talos, one of the largest threat research and efficacy teams.
- Combat advanced threats using Secure Endpoint, and Secure Malware Analytics
- Get complete visibility to inbound, outbound, and internal messages.
- Leverage fast API-driven remediation of messages with malicious content.
- Use an integrated dashboard for search, reporting, and tracking, including conversation view and message trajectory.
- Enhance Microsoft 365 security in less than 5 minutes without changing the mail flow.

For additional information about Cisco Secure Email solutions, visit https://www.cisco.com/site/us/en/products/security/secure-email/index.html.

Topology

In this diagram, we can see the different elements that we are going to use in our lab environment:

Figure 1. Lab Topology



Item Description:

Workstation 1	A workstation that allows lab attendees to access other devices in the same topology
Attacker	A Linux machine that acts as the bad actor, which sends random email messages to other users.
Exchange Online	An Exchange Online mail server provided by the proctor.
Email Threat Defense	An email security cloud account provided by the trainer.

Scenario – Integration with Email Threat Defense

Use Case

Attackers are becoming increasingly creative. To detect and prevent the latest attacks, AI/ML should complement what customers currently use for email security, such as gateways or Microsoft 365.

Objective

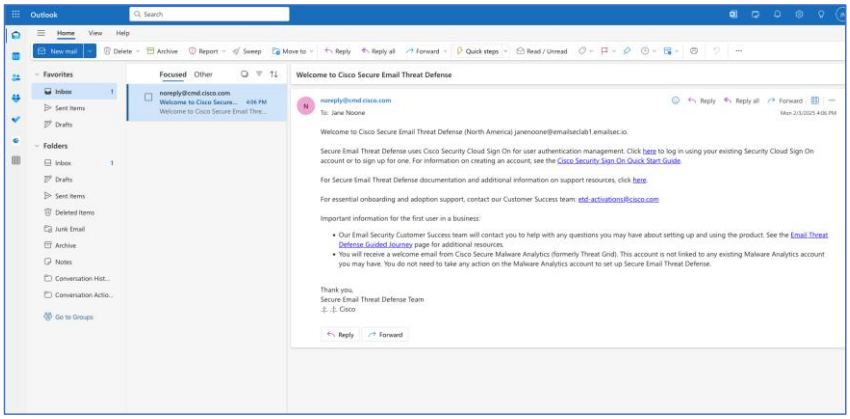
This lab goal is to deploy ETD in a Microsoft O365 environment.
For production environments, we may encounter scenarios and situations where some configurations may be different, but the chosen scenario is one of the most common for customers who want to increase security in their Microsoft O365 environment.

Task – Activate Cisco Secure Email Threat Defense account.

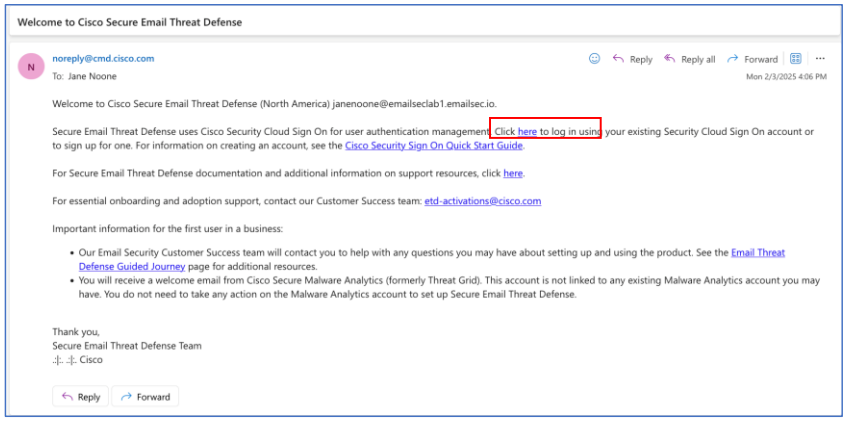
In this lab, we are going to use the ETD beta portal. This means that some steps may be different from those in a production environment.

1. Please go to O365 portal https://outlook.office.com/mail/
   For authentication credentials, please use the lab number assigned by the proctor.
   Administrator 1: janenoone@emailseclabXX.emailsec.io
   User 2: marcmarquez@emailseclabXX.emailsec.io

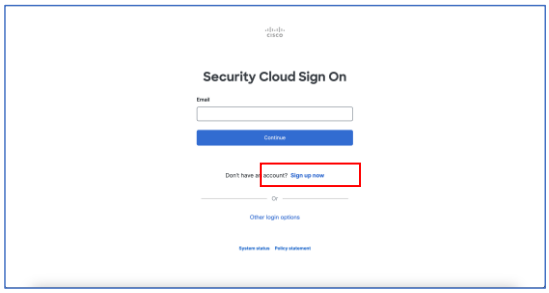
2. Open the inbox, and you will see a “Welcome to Cisco Email Threat Defense” email.



3. Click on the link inside the email (see the picture)



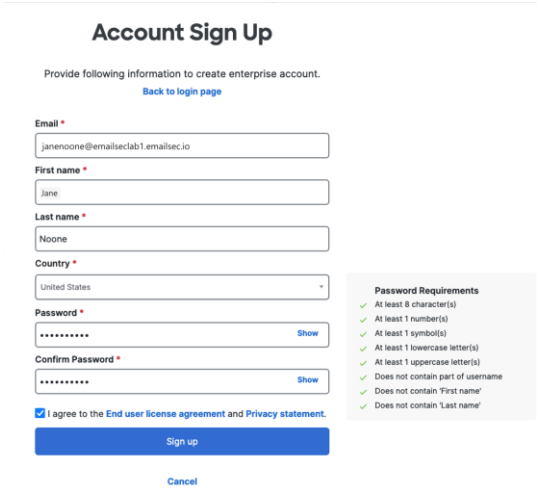
4. For the email address, please use the one you used to log in to O365. Click on ***Sign up now.***



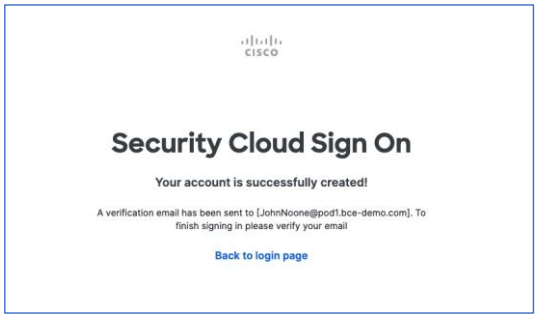
5. For the email address, please use the one given to you by your proctor, choose the correct information, check the "***I agree…***" box, and click on "***Sign up***"

Email: ***janenoone@emailseclabXX.emailsec.io*** First Name: Jane Last Name: Noone Country: United States Password:	Email: ***marcmarquez@emailseclabXX.emailsec.io*** First Name: Marc Last Name: Marquez Country: United States Password:

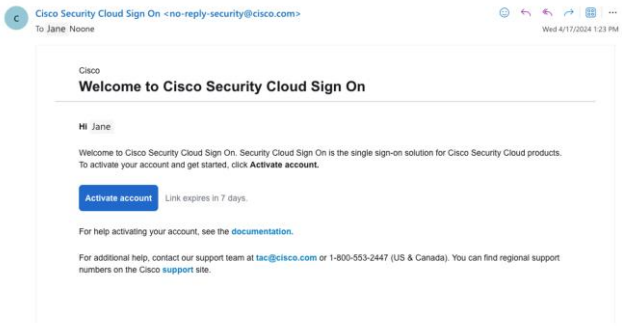
Commented [S(1]: why is this here?



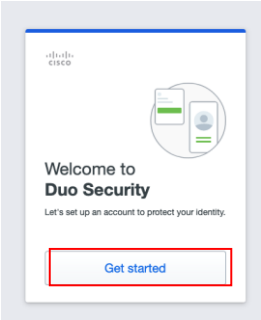
6. You should expect this screen:



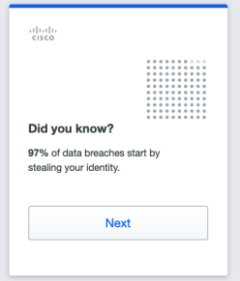
7. Go back to your administrator mailbox in O365: https://outlook.office.com/mail/
8. Open the new message and press “Activate Account.”



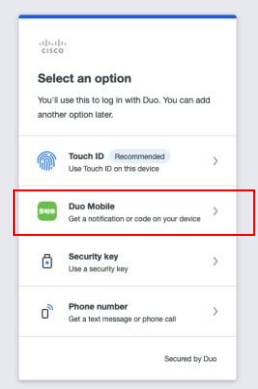
9. By default, you need to set up MFA when creating an ETD account. Press the “***Get started***” button:



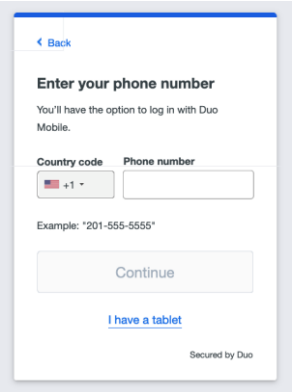
10. Click on ***Next***.



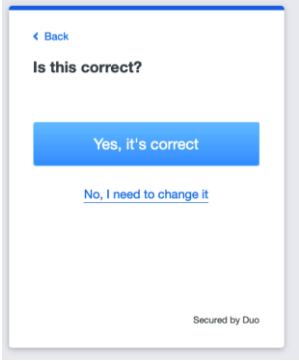
11. Press the "***Duo Mobile"*** button.



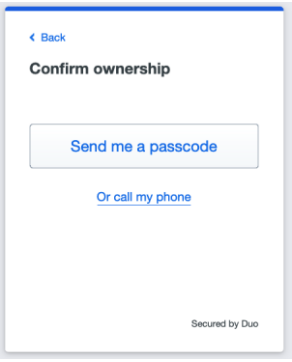
12. Introduce your phone number and press ***Continue***.



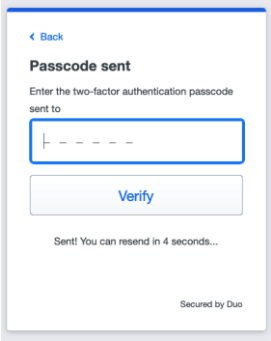
13. Verify the number and press ***Yes, it's correct.***



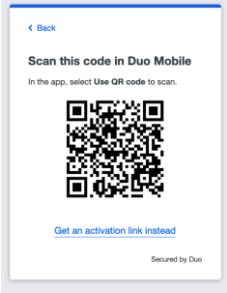
14. Now, click on "Send me a passcode" to confirm that you are the owner.



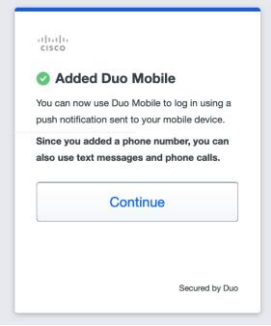
15. Introduce the code and press ***Verify***.



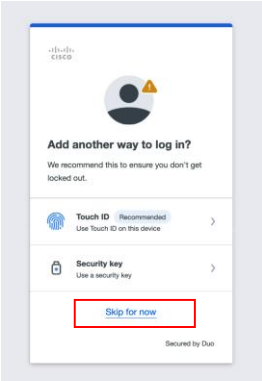
16. Open DUO or the camera to scan the QR code presented on the web page.



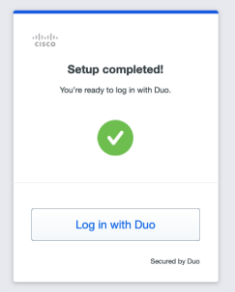
17. If you have DUO installed, you will see this image. For the ones that need to be installed, follow the steps presented in the browser.



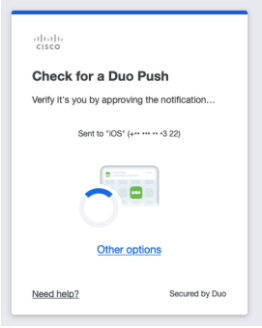
18. Press ***Continue***
19. Click on ***Skip for now***.



20. Now, you can log in with Duo MFA. Click on ***Log in with Duo***



21. Approved the push in your phone and click on ***Finish***

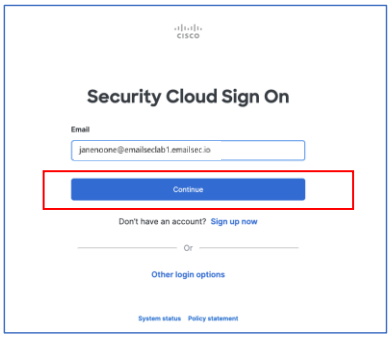


22. Please close the current window, open a new tab, and connect directly with https://beta-ui.cmd.cisco.com/login

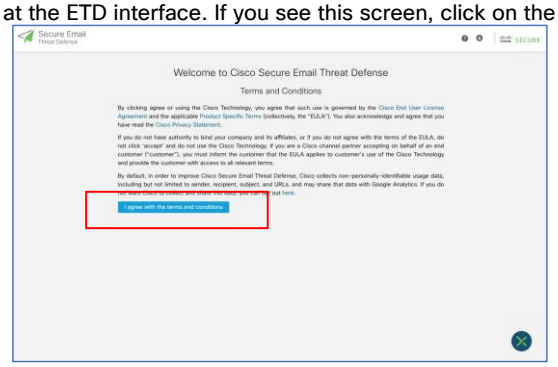
This step is required because we are using the beta environment.

This step needs to be done by one Administrator only

23. Introduce the email address provided by the proctor and used to activate the service. Click on ***Continue***.



24. You should now be at the ETD interface. If you see this screen, click on the button with "I agree.."



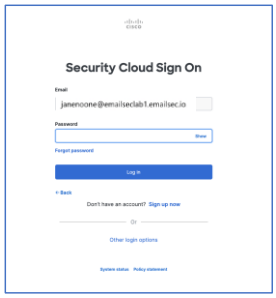
Lesson learned.

In this task, we have seen how to activate an Email Threat Defense account. This will be common for all types of deployments, although in today's lab, we will integrate it with O365.
The steps are simple and will always be executed with our client's account.

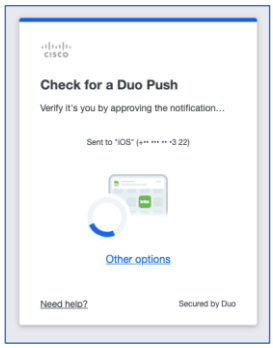
Task – Configure Email Threat Defense account.

The steps we are going to see below are not the usual steps when deploying ETD.
This is because we are using an already partially configured BETA environment.

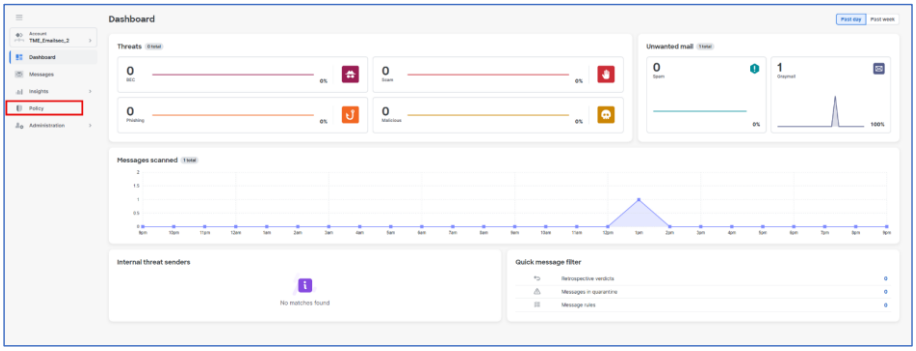
1. Log in again to the beta portal: https://beta-ui.cmd.cisco.com/login



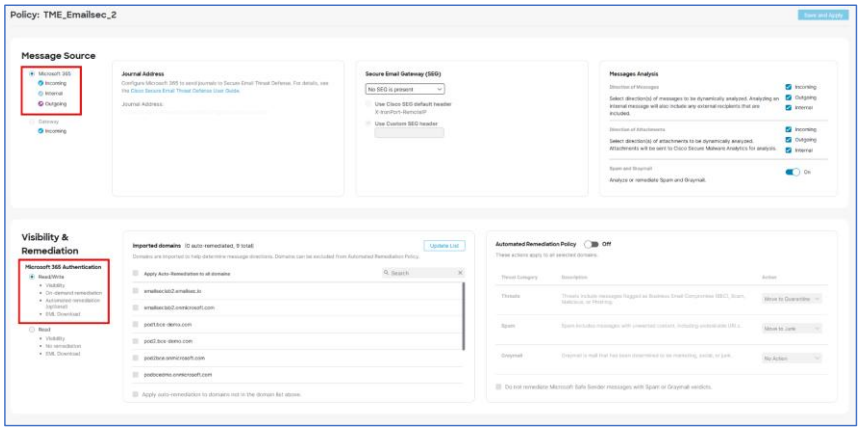
2. Accept the push from DUO on your mobile.



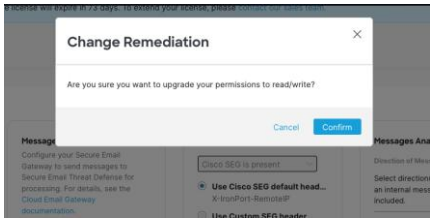
3. As we mentioned at the beginning, these are not the usual steps.
   Click on ***Policy***



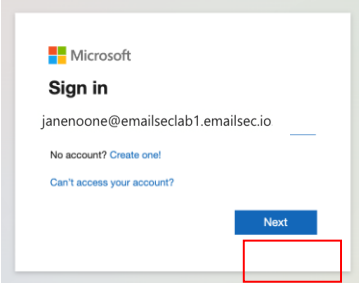
4. The Email Threat Defense account you have access to is already activated to work with a gateway with no integration with O365. We need to connect with O365 and to do this, we need to move from Gateway/No auth to Microsoft 365/Read-Write.
   Click on ***Read/Write*** and after click on ***Microsoft 365***



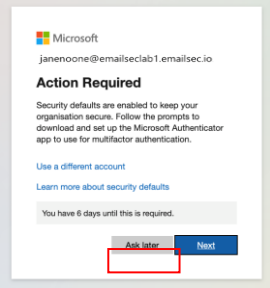
5. Click on ***Confirm***.



6. Let's start the integration with MS365. We need to use the MS365 account provided: janenoone@emailseclabXX.emailsec.io
   Click on ***Next***



7. After the password, a new window will appear, asking to move to enable MFA.
   Click on ***Ask Later***.



8. Click on ***Accept***.

Lesson learned.

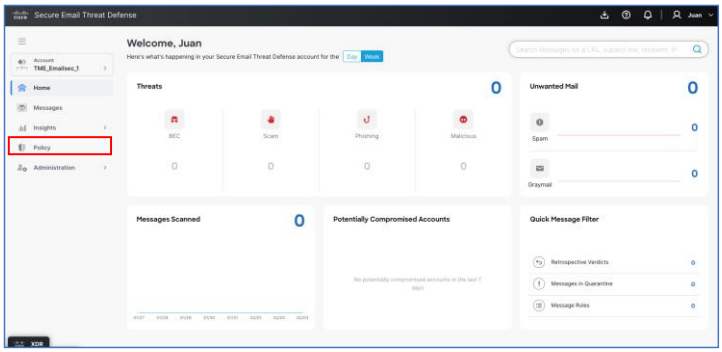
After activating Email Threat Defense, as in the first task, we made the first connection between Cisco Email Threat Defense and MS365.
This connection will still need to analyze the mail. We have activated the ability of Cisco Email Threat Defense to clean the mailboxes, in addition to having decided how we wanted to integrate it.

Configure Cisco Secure Email Threat Defense Policy

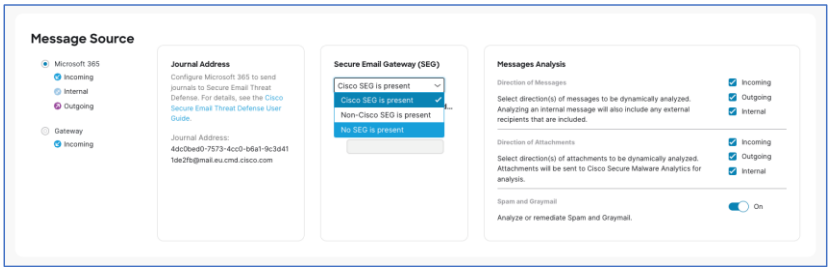
Depending on the customer scenario, we may need to adjust which features are enabled.
If the customer has a Cisco Secure Gateway (on-prem or cloud), we should leave SPAM and Graymail disabled. In this case, we will enable all the analysis modules.

If you want to learn more:
https://www.cisco.com/c/en/us/td/docs/security/email-threat-defense/user-guide/secure-email-threat-defense-user-guide/policy.html

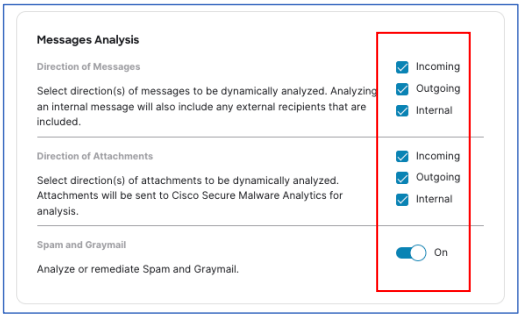
1. On the Cisco Secure Email Threat Defense console, click on ***Policy***:



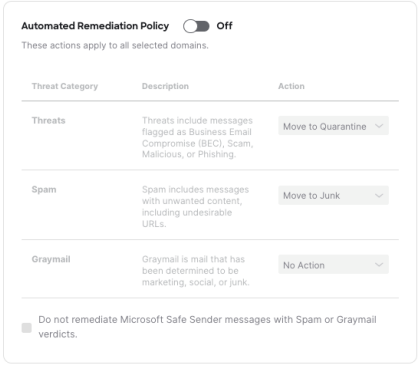
2. Select "***No SEG is present***"
   In this lab we don't have any security gateway in front of O365.



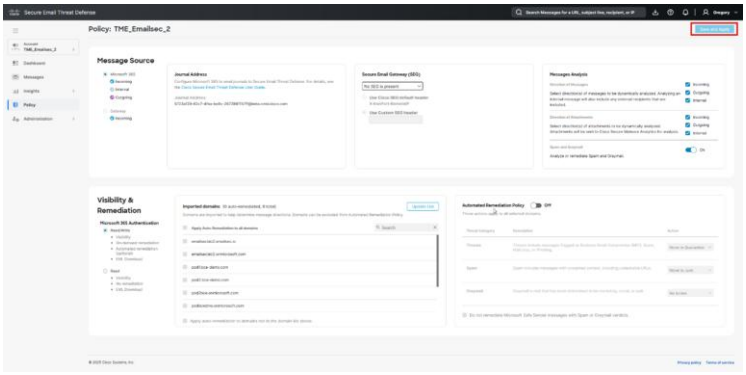
3. Enable "***Spam and Graymail***" and all the options.



4. We will keep all the Automated Remediation actions disabled. For POV/POC scenarios, you should enable this feature after a couple of weeks, because the AI/ML engines already learned from the customer mail flow.



5. Click on ***Save and Apply***.



Lesson learned.

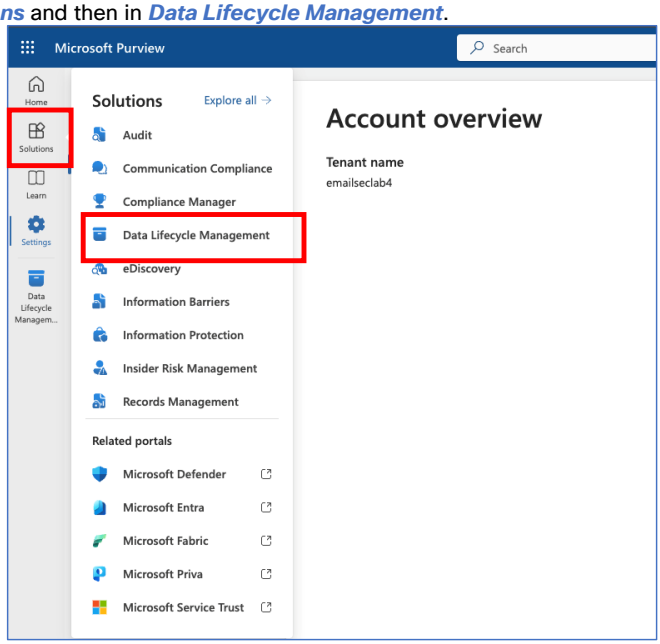
It is essential to understand this task that we have done now.
Before managing traffic, we must configure a policy in our Email Threat Defense account. If we do not do this, we may have unexpected behavior since it could be deleting emails we do not want to delete. Therefore, before carrying out the next task, we must have the policy we want to implement configured. In most cases, this will have a monitor mode configuration.

Task – Configure Exchange Online.

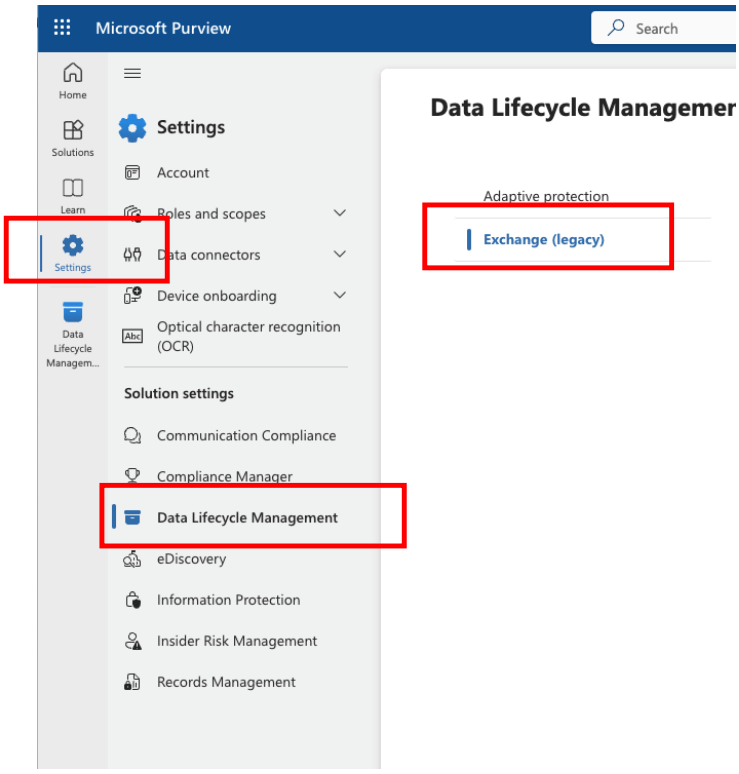
In this task, we will configure Exchange Online and review the permissions automatically configured in the previous step.

1. Now we need to go to the Purview Microsoft Admin center and configure the journaling rule.
   https://purview.microsoft.com/
   Microsoft updates the console from time to time. In this case, you can see either the legacy portal or the new Purview portal.
   The configuration presented here is for the new Purview console.

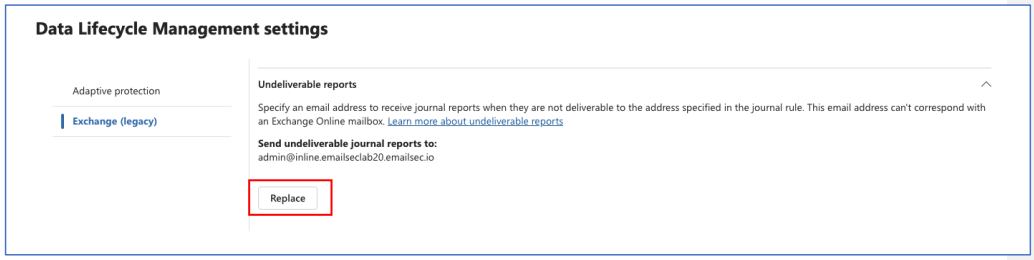
   Click on ***Solutions*** and then in ***Data Lifecycle Management***.



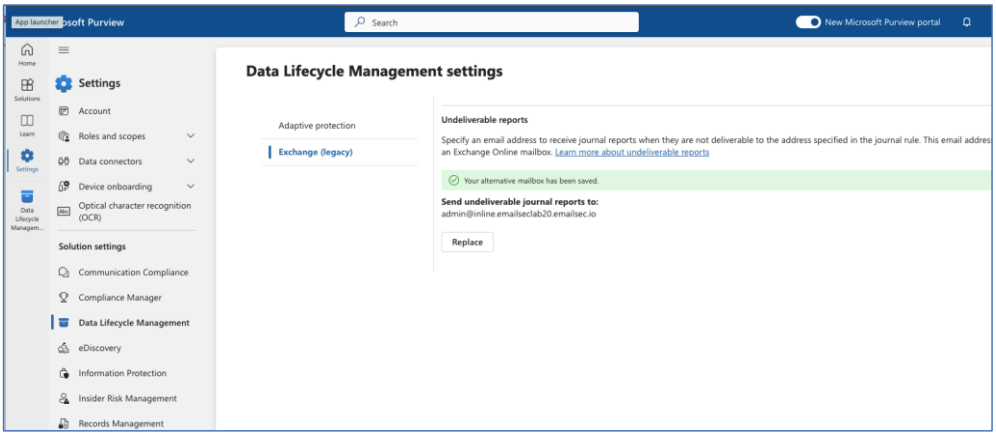
2. Click in ***Settings*** and ***Data Lifecycle management*** and then **Exchange (legacy).**



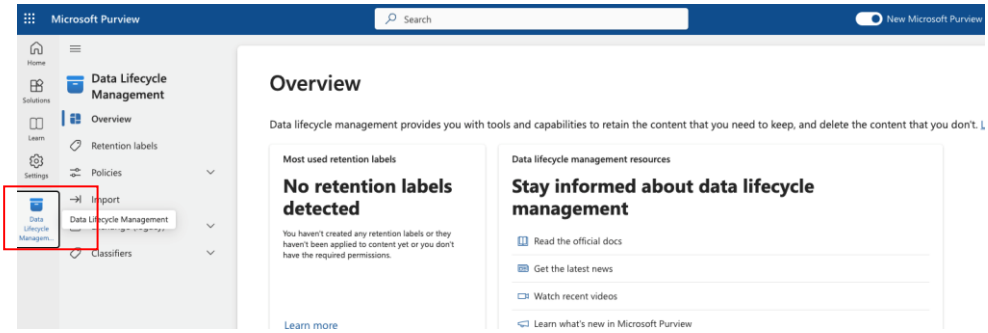
3. Click on ***Replace***. Before configuring the Journaling rule, you must indicate an email address to receive Undeliverable Reports. Please note that in a production environment, this step may already have been completed by the client.



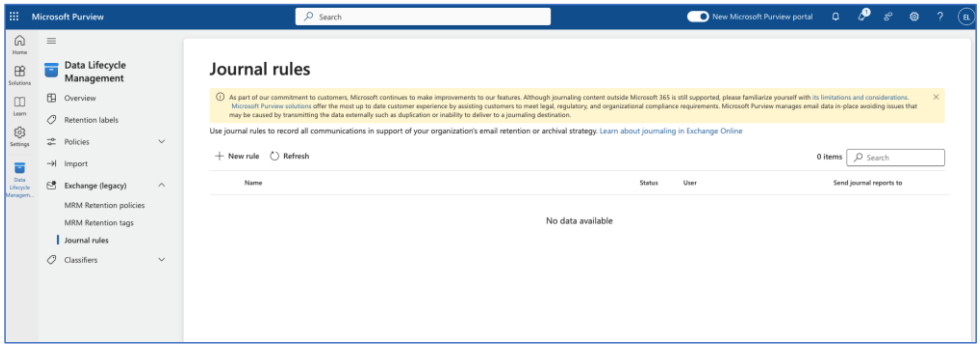
In the new Microsoft Pureview console verify the email address, if the email address is not present, please add it.
admin@inline.emailseclab20.emailsec.io



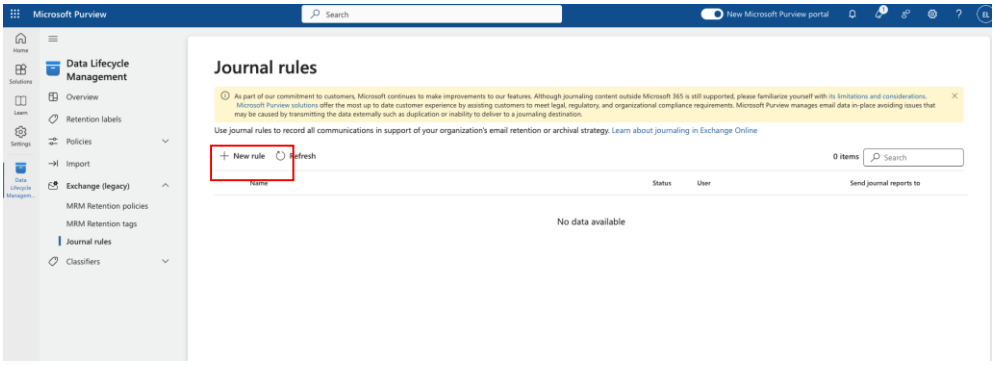
4. Click on "***Data Lifecycle management***":



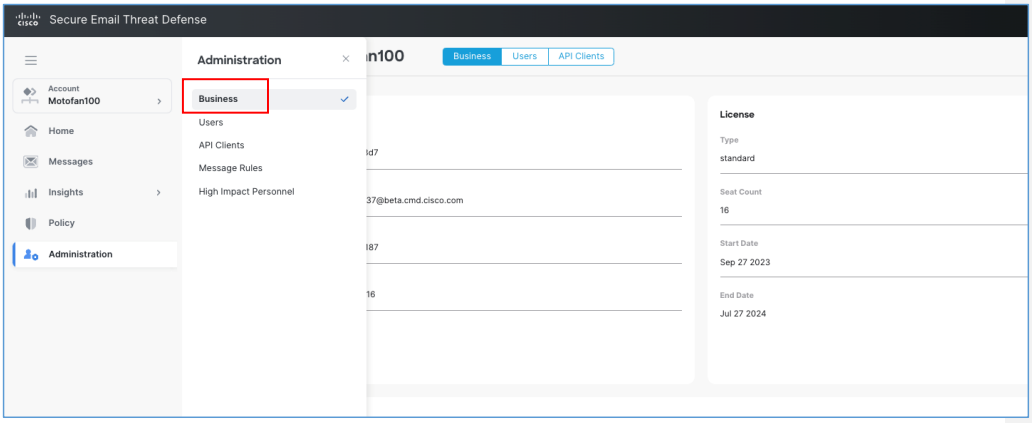
5. Click on "***Exchange Legacy***" and on "***journal Rule***s".
   If you see a rule created, please select and remove it.

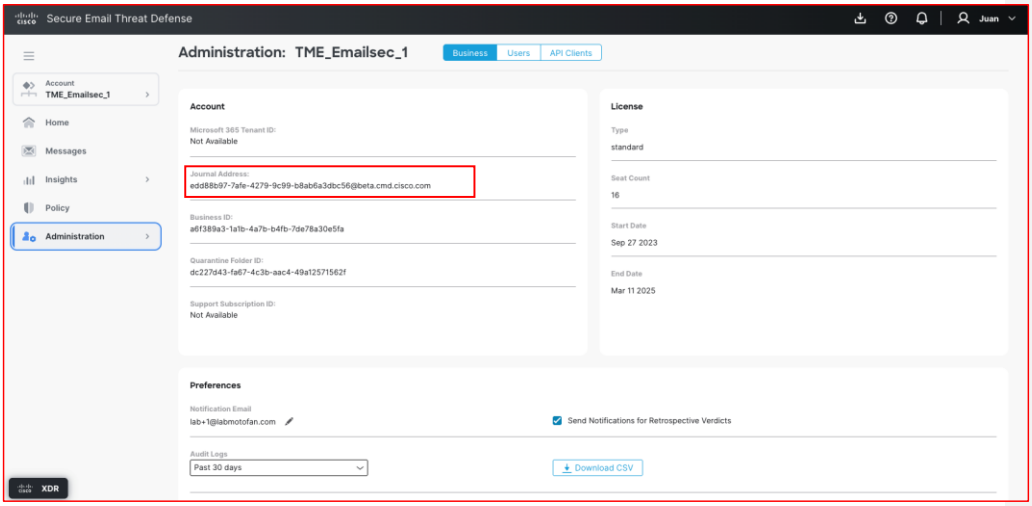


6. Click on "***New Rule***"

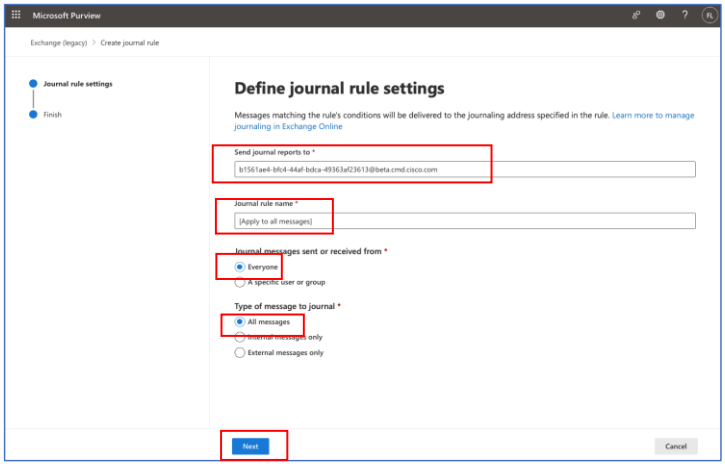


7. Before to fill the rule information, we need to get the journaling email address. Go back to Cisco Secure Email Threat Defense. Open ***Settings → Administration***
   Copy the ***Journal Address***.



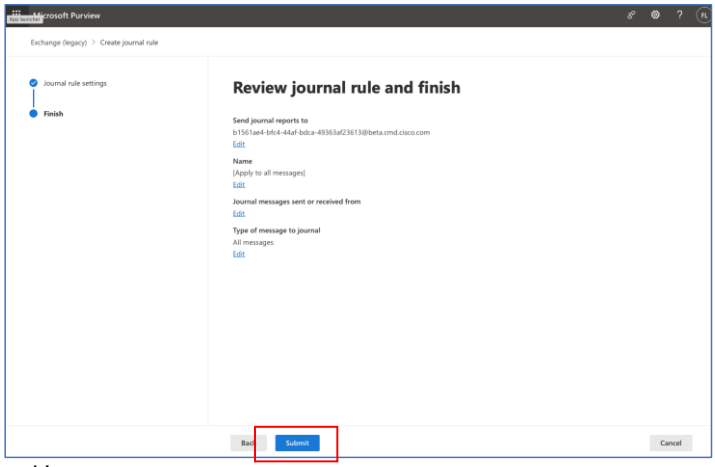


8. Now in the O365 window, fill all the data. Add a rule name, copy the journal address, and choose ***Everyone*** and "***All Messages***". (Name should be the last box to fill).
   Click on "***Next***":



9. Click on "*Submit*"

This is the most crucial step. All traffic will be sent to Email Threat Defense when you press the submit button. Since we are in a lab, we will not see anything. In a production environment, messages will be sent to ETD immediately, so we must ensure we have the correct policy settings before clicking the Submit button.



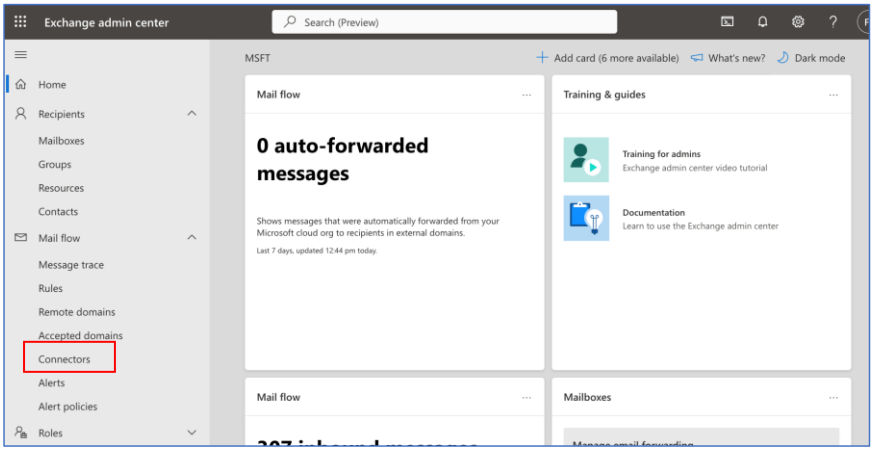
10. You should see this screen:

This concludes the ETD and Microsoft integration scenario.

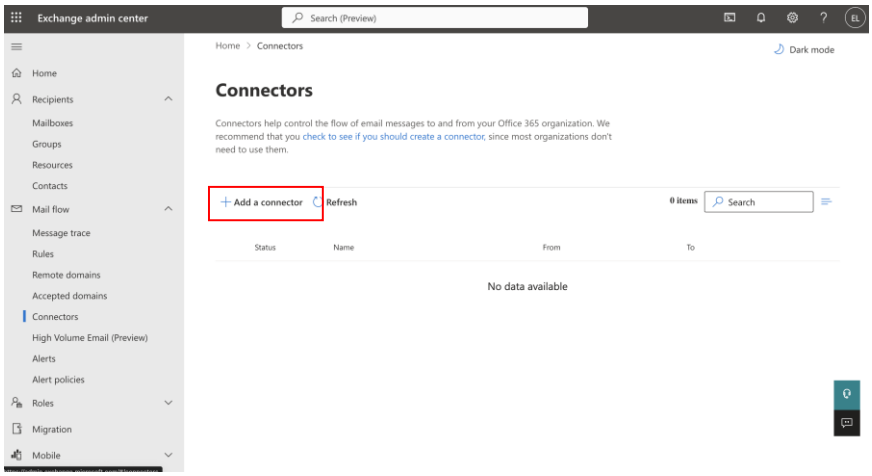
Connector in O365 for ETD traffic.

In some environments, with secure gateways, Exchange on-premises devices, etc., more connectors will be configured. If this happens, it's important that the traffic delivered to ETD goes through one of these platforms without being stopped or delayed. Creating a connector for this traffic will force O365 to send this traffic directly to ETD.

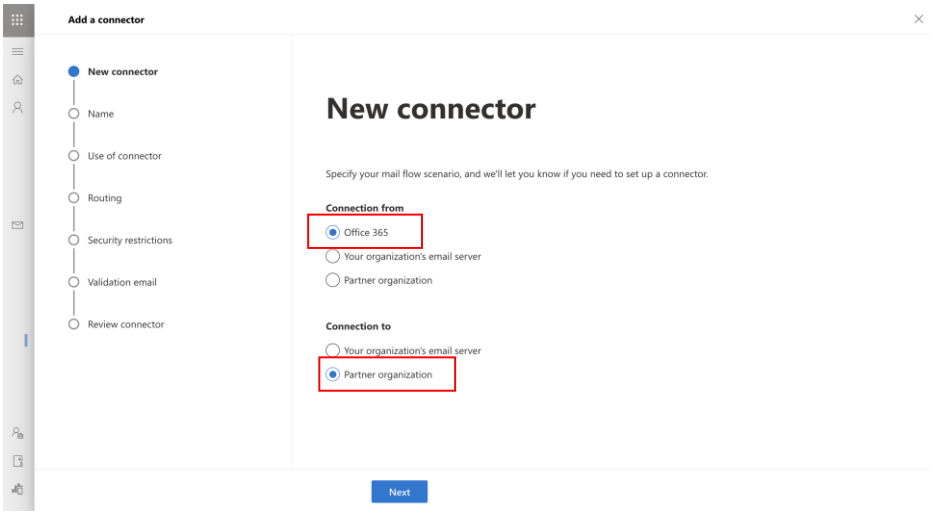
1. Open Exchange Online administration console at https://admin.exchange.microsoft.com/
2. Click on "***Mail Flow***" and "***Connectors***".



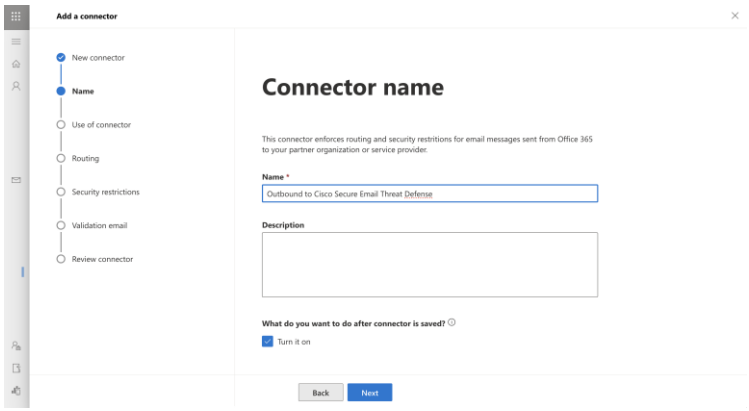
3. Click on "***Add a connector***".



4. Select Connection From "***Office 365***" and Connection to "***Partner Organization***" and click ***Next***

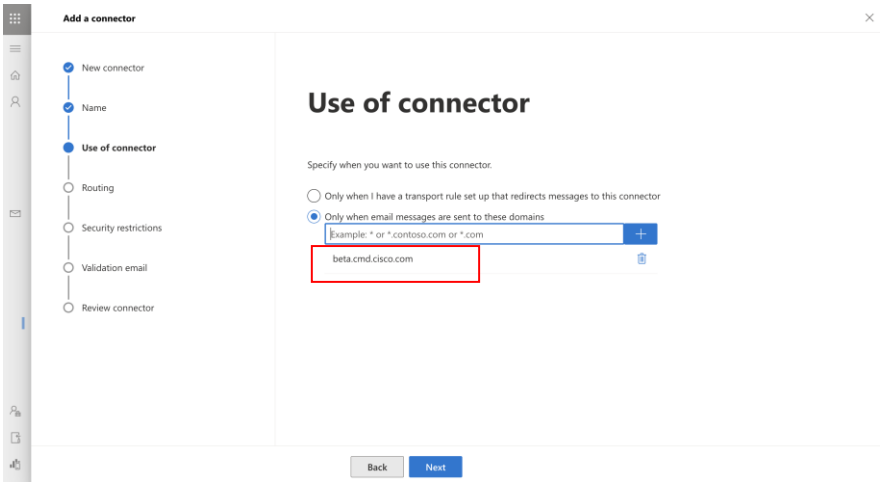


5. Write a name, in our case we can use "***Outbound to Cisco Secure Email Threat Defense***" and click ***Next***.



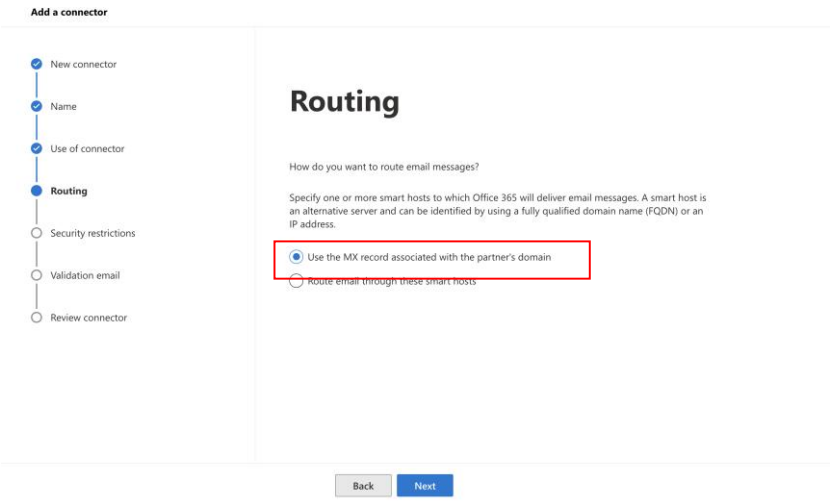
6. Write the domain that is in your journaling email address. In this lab the domain is "***beta.cmd.cisco.com***"

   Click on **+**

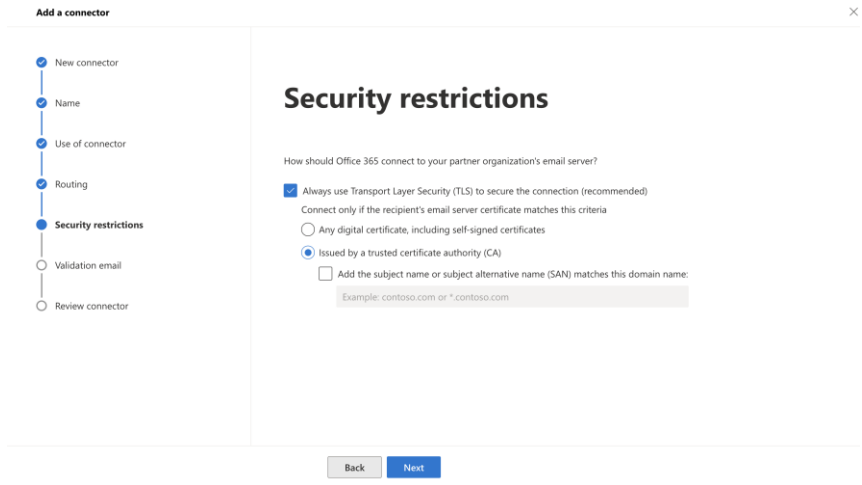


7. Click on ***Next***

8. Select "***Use the MX record associated with the partner's domain***" and click on ***Next***

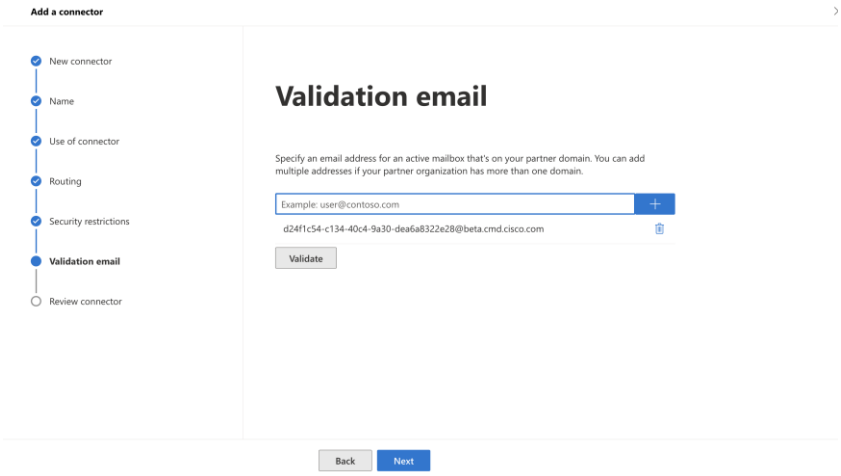


9. Select "***Always use Transport Layer Security (TLS) to secure the connection (recommended); Issued by a trusted certificate authority (CA)***" and Click on ***Next***

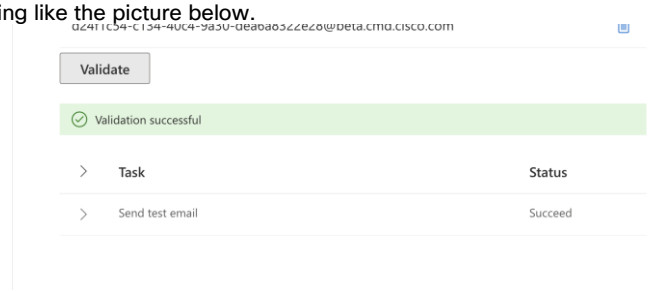


10. Copy the journaling address to validate the connector. Click on "***Validate***"

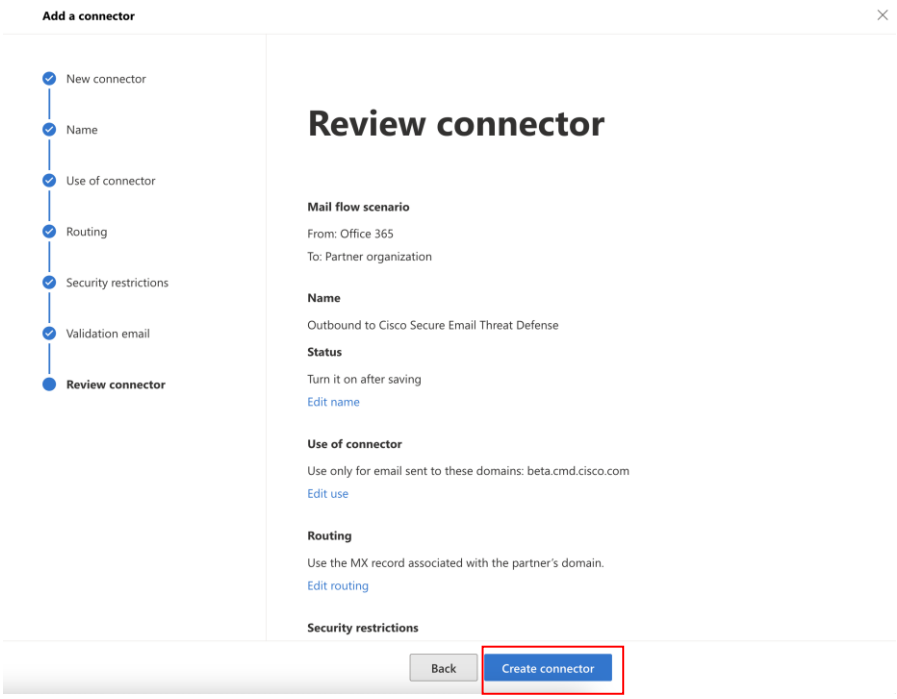
Note: The connector validation may fail if your O365 tenant is already configured with conditional mail routing using an Exchange transport rule to route outbound mail to an existing connector. While journal messages are system-privileged and are not affected by transport rules, the connector validation test email is not privileged and is affected by transport rules.



Validation process takes some time to perform and not always is successful. If everything works you will see something like the picture below.



11. Click on "***Create Connector***"



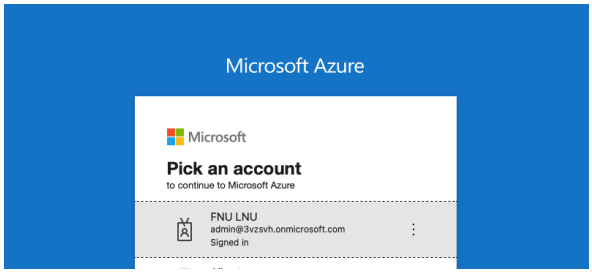
Lesson learned.

We have already finished the integration between ETD and O365 in both directions.
The next step is to verify the operation and carry out tests.

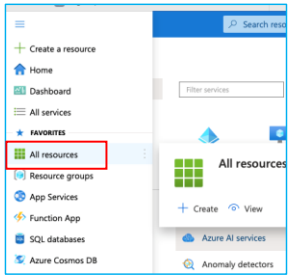
Task –Review the permissions assigned in Microsoft (optional)

Frequently, customers ask about the permissions required to integrate ETD with Microsoft to be able to use the Read-Write mode on ETD.
Let's see what Microsoft permissions are assigned to Cisco ETD.

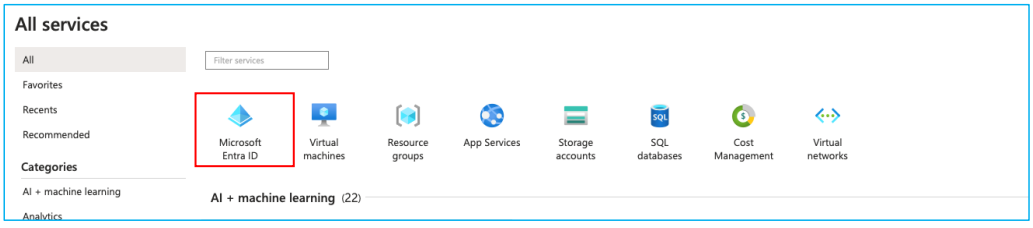
1. Open the Azure portal with the O365 account provided for this lab:
https://azure.microsoft.com/en-us/get-started/azure-portal/



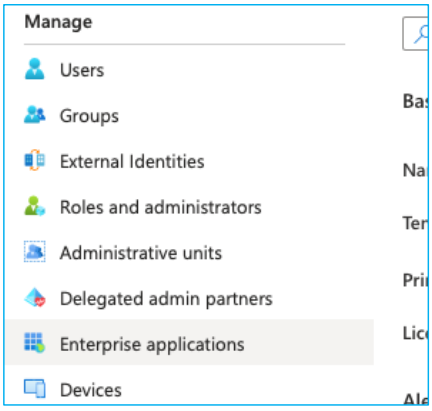
2. Click on "***All resources***"



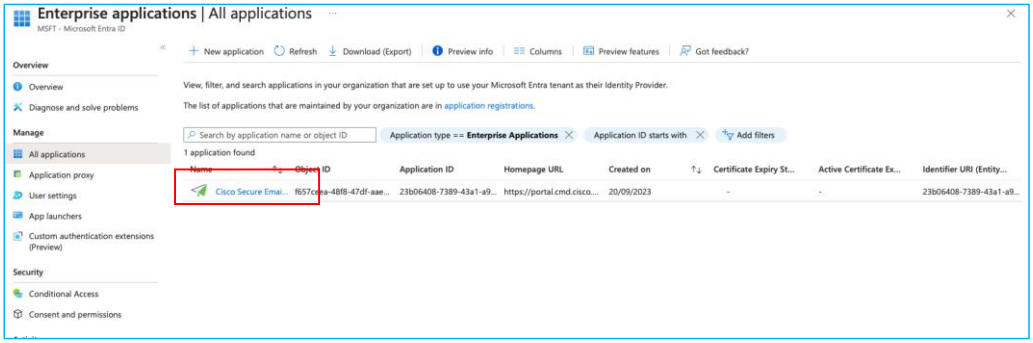
3. Click on "***Microsoft Entra ID***".



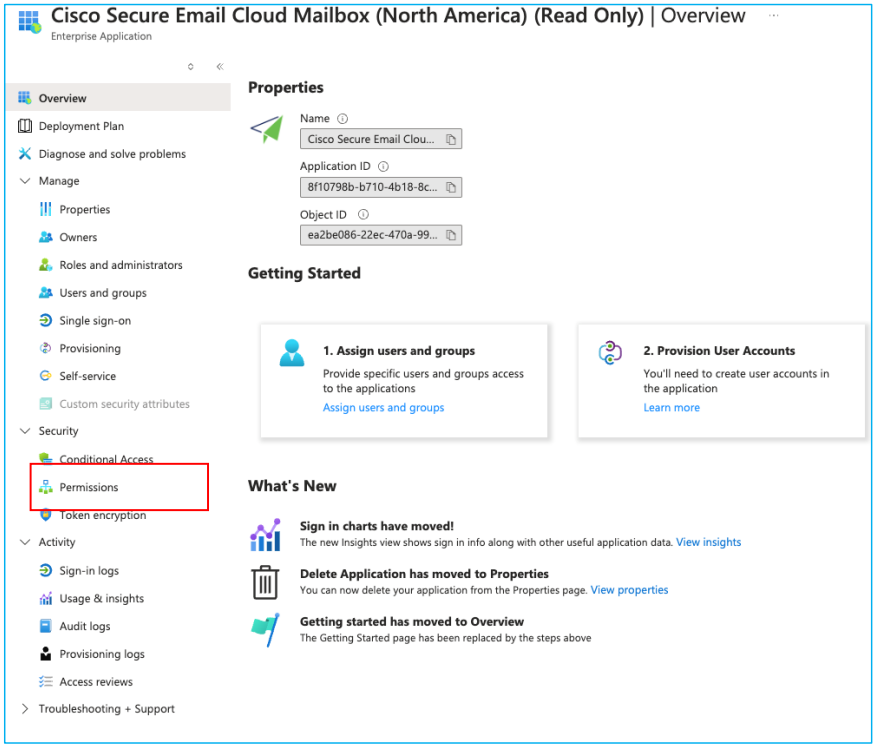
4. Click on “***Enterprise Applications”***.



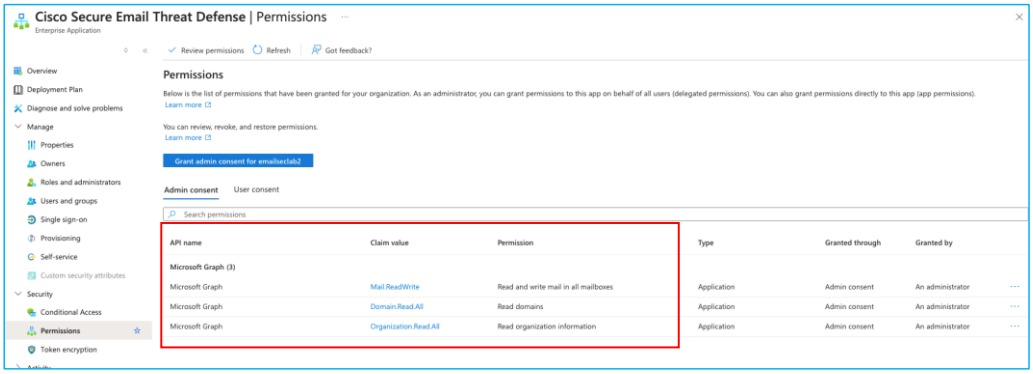
5. If the integration is correct, you will see an entry with the name “***Cisco Secure Email***...”



6. Click on Permisions



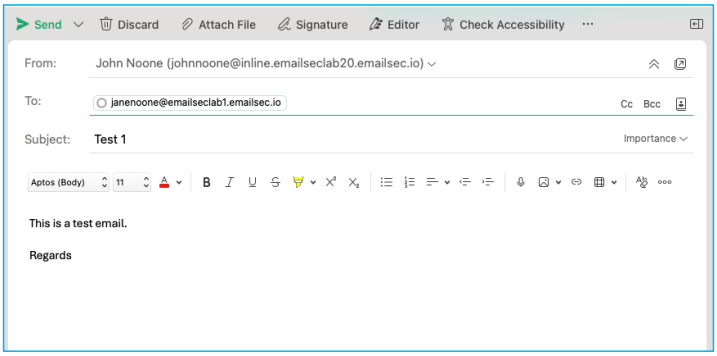
7. If you open the application, you can see the permissions assigned.



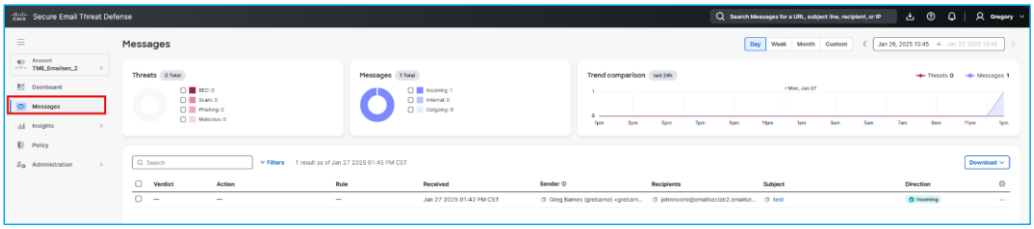
Task – Test the solution.

To continue this lab, you are going to generate email traffic. Since the account is valid, you can send emails from your own business or personal account, and you see how it appears in the ETD admin interface.
You will test all the options to verify that everything is working as expected.

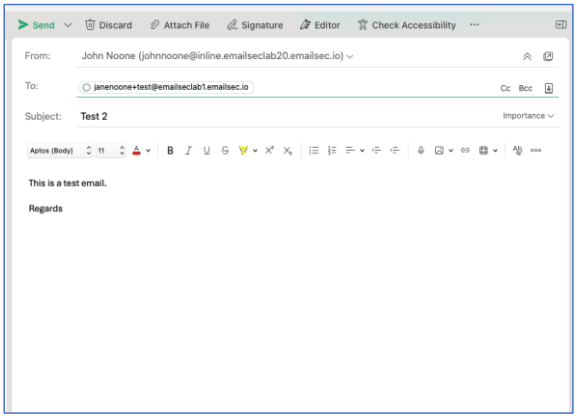
1. Open your Email client and send an email to the account created in Exchange Online. Something like janenoone@emailseclabXX.emailsec.io (Please use your admin user and pod number)



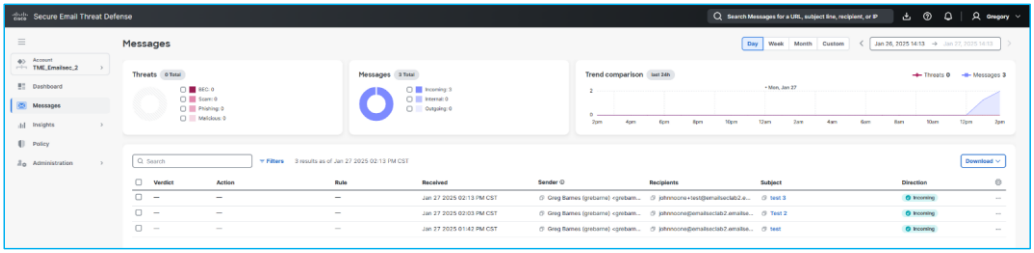
2. In the Email Threat Defense dashboard, on the ***Messages tab***, you will see information about the email you just sent:



3. Using your business or any other email account, send an email to ***janenoone+test@emailseclabXX.emailsec.io or "marcmarquez+test@emailseclabXX.emailsec.io"***. (Please use your pod number)



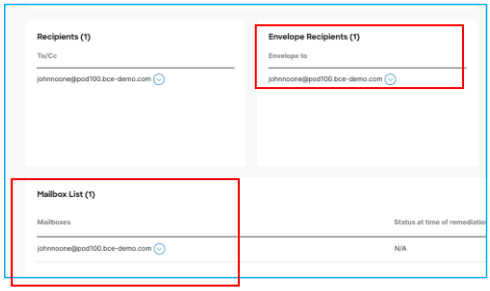
4. You should see something like this in your ETD console.

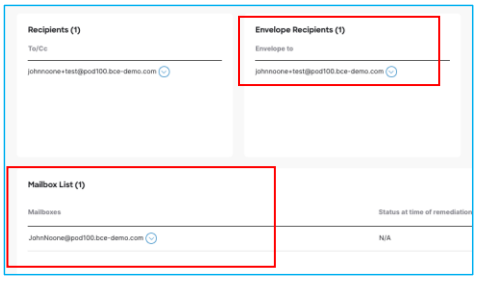


5. Open both messages and compare the “Delivered To” field.

As you can see, both messages arrived in the same mailbox. “Delivered To” means who is the destination (final Mailbox). Many times, we will see “To”, “Envelope To” and “Delivered To” totally different. This happens when email is going to a Distribution List, Alias, BCC, etc.

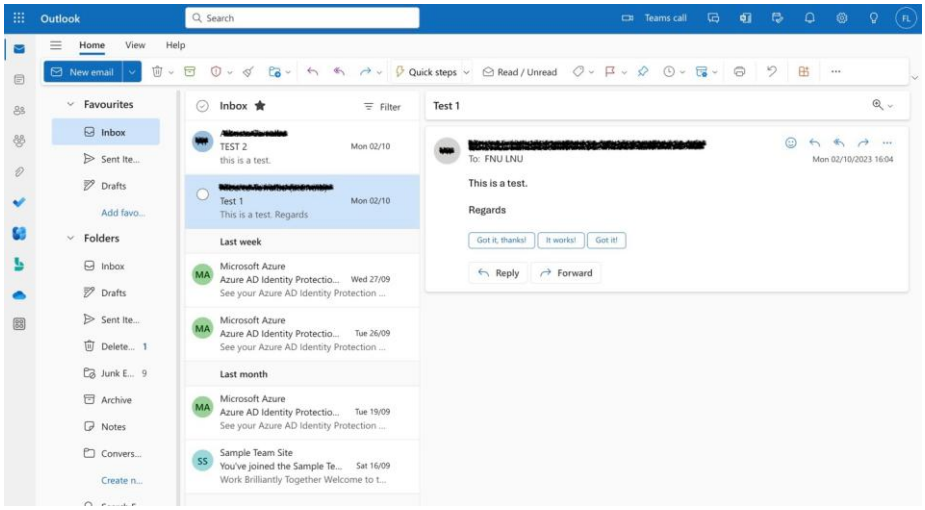
ETD allows you to understand exactly where the email was sent to and who received it.



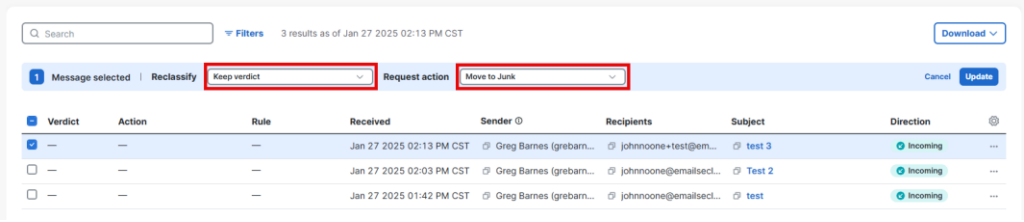


6. If you want to confirm that both messages were delivered to the same destination, please open Outlook for your O365 admin user by clicking on https://outlook.office.com/mail/

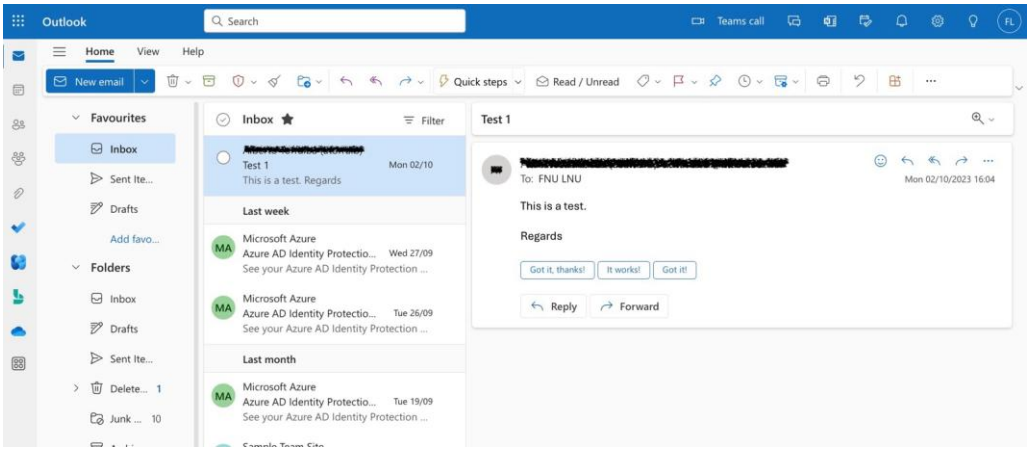
   You should have these two emails.



7. Go back to the ETD dashboard, and on the Messages tab, please select one of the messages and remove the email. Select "***Keep Verdict***" and "***Move to Junk***"
   Then click "***Update***".



8. Automatically the email should disappear from the user's inbox and appear in the junk folder. Please go back to Outlook and confirm that the message is now in the Junk folder:



This concludes this task, and you may continue to the next one.

Lesson learned.

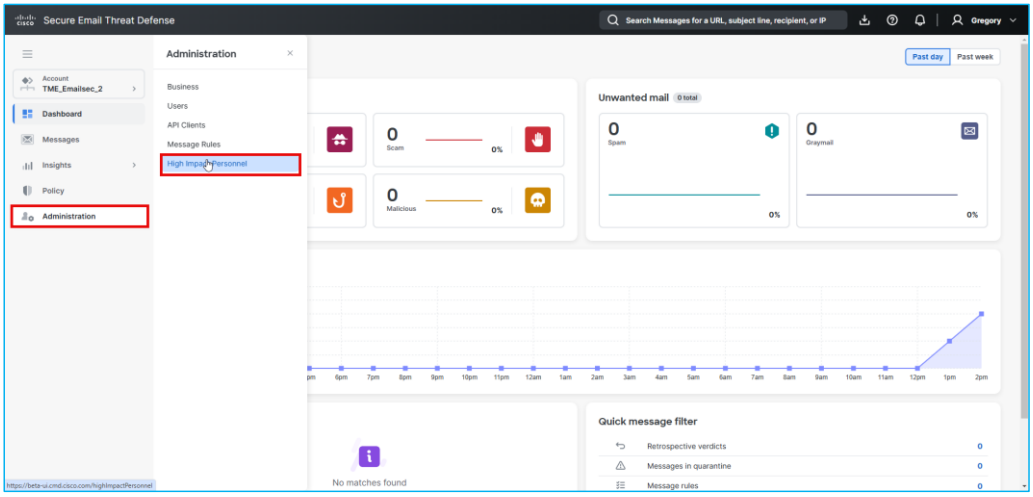
In this task, we have carried out several tests and seen how Email Threat Defense displays the information in the console.
We have also conducted a test with an alias to understand what some of the parameters appearing in the console mean.

Task - High Impact Personnel

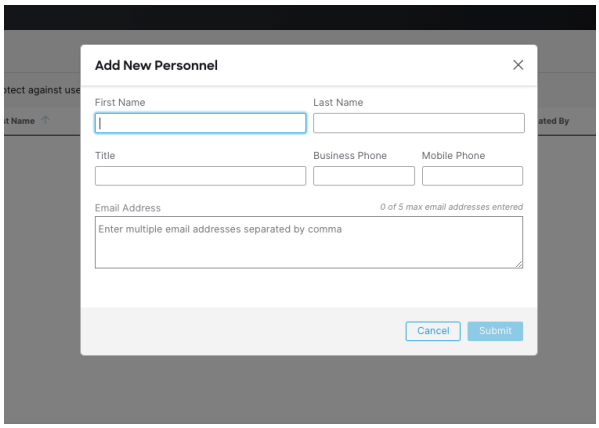
Important personnel, such as members of executive leadership teams, are at risk of being impersonated in an attempt to compromise other targets. The high-impact personnel list helps Secure Email Threat Defense defend your organization from impersonation attacks.

Admins can create a list of up to 100 people that is sent to Cisco Talos for higher scrutiny on Display Name and Sender Email Address. Deviations from the configured information for an individual will be identified as a Technique in the Verdict Details panel of convicted messages.

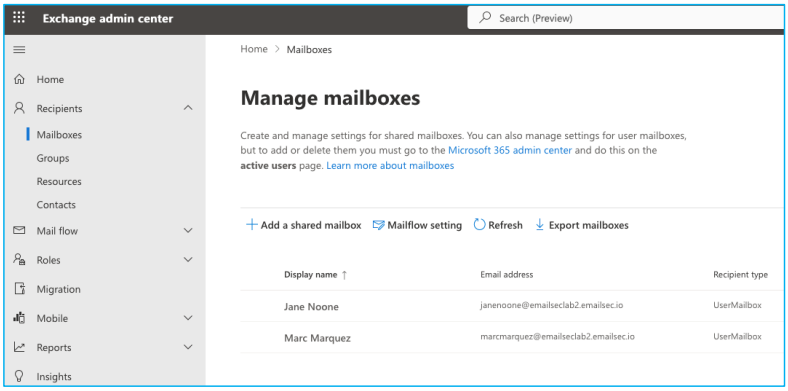
1. Open the Cisco Email Threat Defense console.
2. Click on Administration → High Impact Personnel.

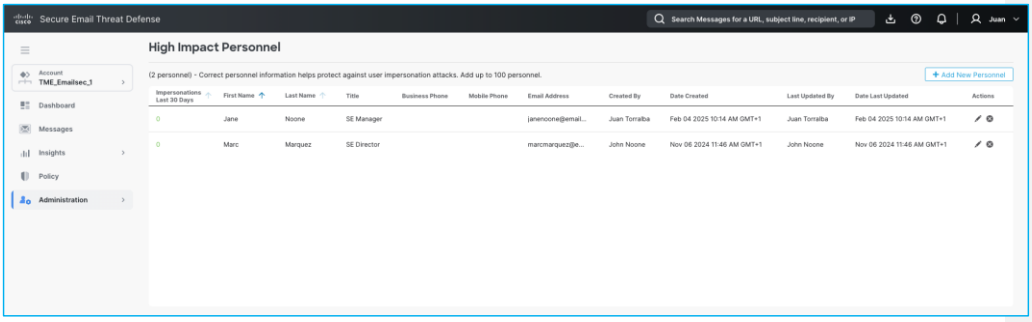


3. Click on "***Add New Personnel***"
4. We can add some names. In the list below we have the list of users created by Microsoft by default. Then you can add some of them manually in your environment. Add the users that you have in your environment. (You can see a list below)



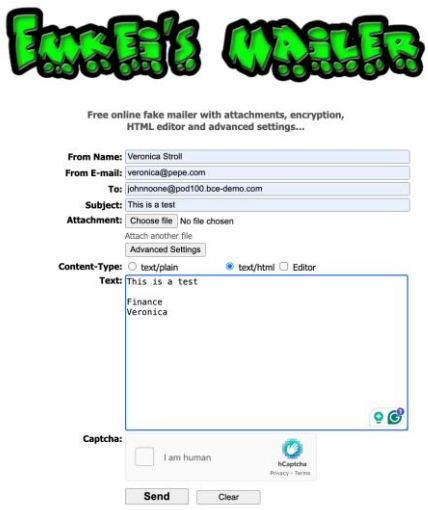
First Name	Last Name	Title	Email Address
Jane	Noone	SE Manager	janenoone@***emailseclabXX.emailsec.io***
Marc	Marquez	SE Director	MarcMarquez@***emailseclabXX.emailsec.io***



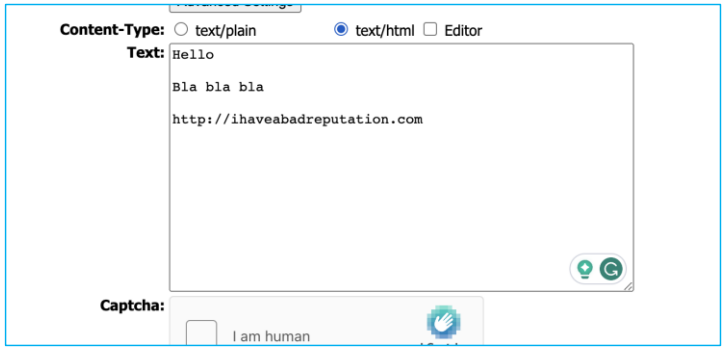


5. Open the web site: https://emkei.cz/

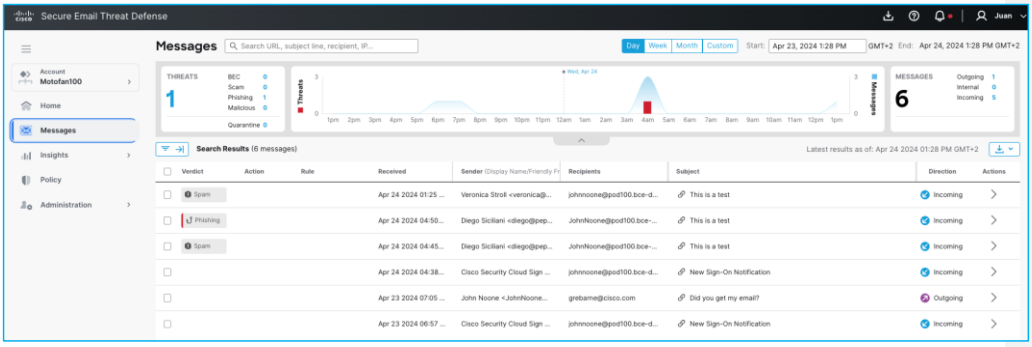
6. Fill the form with this information. (the name must be one of the ones from your list).
From Name: Veronica Stroll
From Email: Jane@pepe.com
To: janenoone@emailseclabXX.emailsec.io or MarcMarquez@emailseclabXX.emailsec.io (You must put your O365 email domain).
Content Type: text/html
Subject: This is a test
Body: Hello



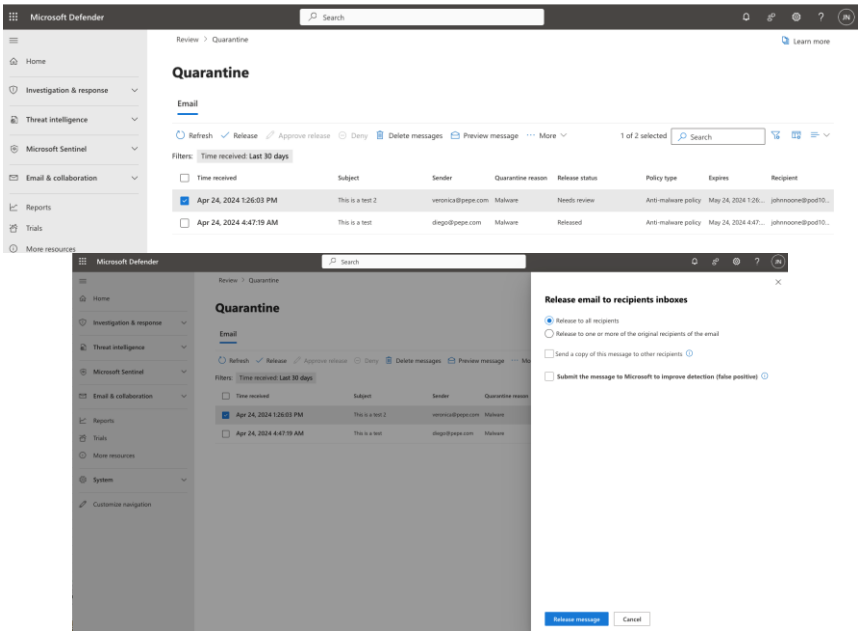
7. Repeat the same as before but change the body content adding http://ihaveabadreputation[.]com



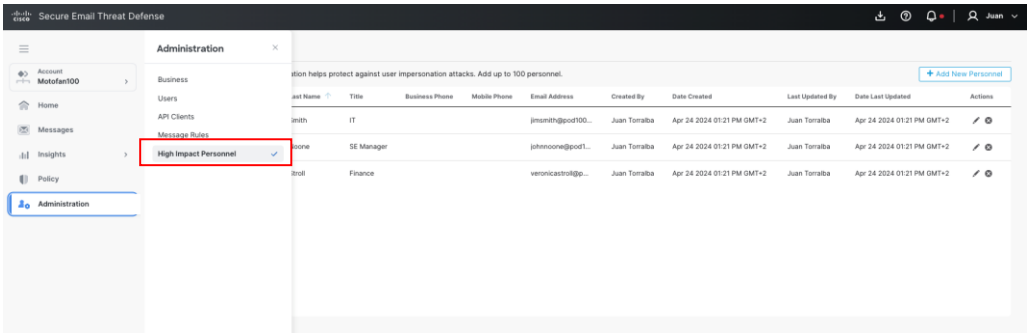
8. Review If both messages were processed by Cisco Secure Email Threat Defense.



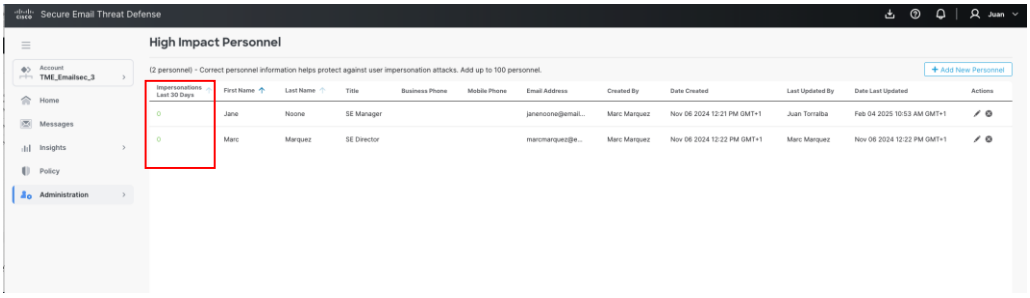
9. If you don't see a message processed by Email Threat Defense, then maybe O365 detected as malicious and quarantined it. In this case, open the O365 quarantine and release the email. Remember that Microsoft will process all the emails before Cisco Secure Email Threat Defense. https://security.microsoft.com/quarantine?viewid=Email



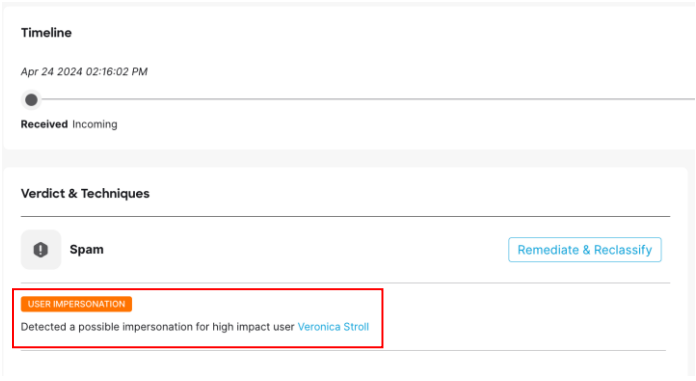
10. Go back to Cisco Secure Email Threat Defense and Open "***High Impact Personnel***".



11. You should see a number next to the name, this indicates how many HIP detections have occurred.



12. Click on Messages and expand the message detected as phishing. You should see a “User Impersonation” technique.



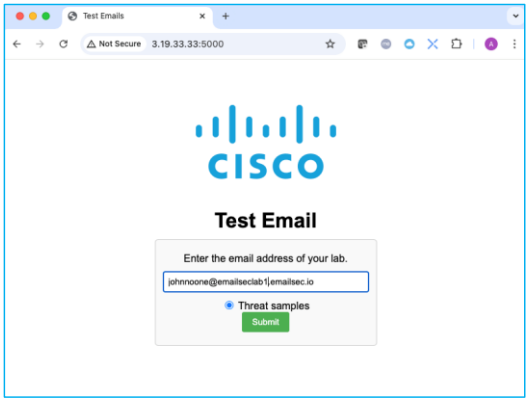
Task – “Attack” your environment.

Send Email Threats.

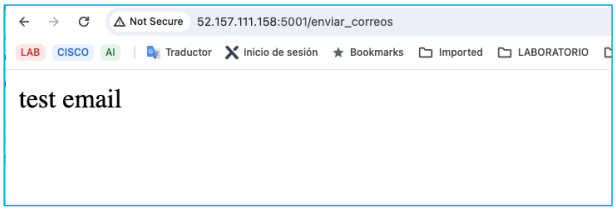
To be able to see ETD detection capabilities, threat messages must be sent to users. For this lab, we have prepared a group of threat messages (around 60) to be sent to users created within the Microsoft E5 dev account.

Use this email tool just for lab purposes. Actions are being logged.
Microsoft can block the traffic coming from these IPs, if this happens you can create traffic manually from a free account or from https://emkei.cz/.
As a malicious IOC you can use http://ihaveabadreputation[.]com

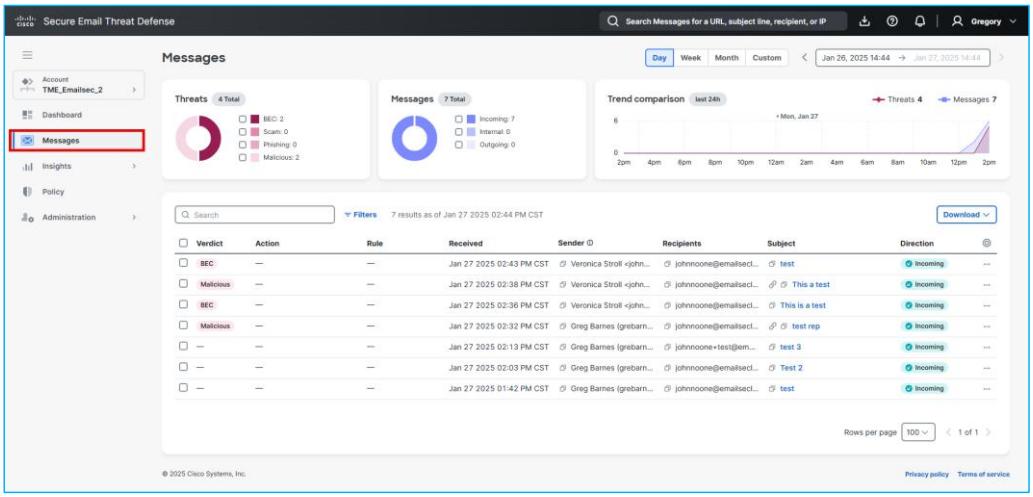
1. Connect to any of the sites below, insert your email domain, and press ***Submit.***
   http://3.19.33.33:5000/



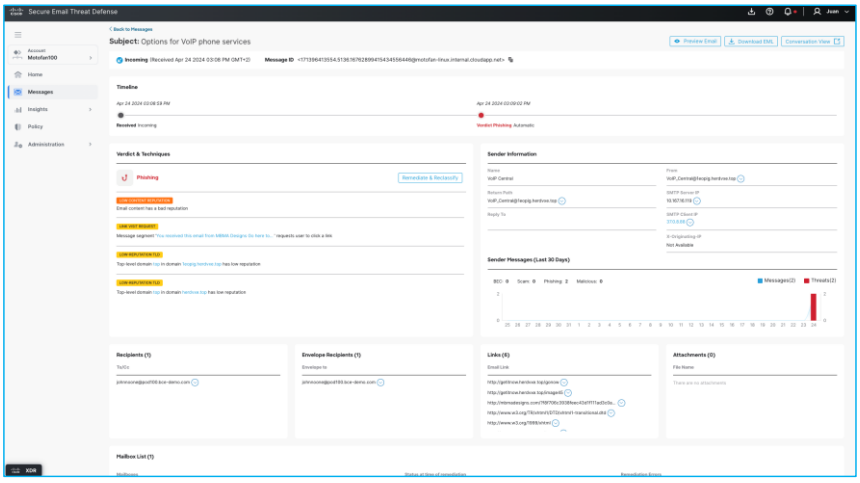
2. Wait for the “Thank you for submitting your domain:” message to be displayed on the screen. **This message may take up to 3min to show**.



3. Go back to your ETD dashboard. On the Home tab or at the Messages tab, you should be able to see threat messages in the 6 categories: BEC, Scam, Phishing, Malicious, Spam, and Graymail

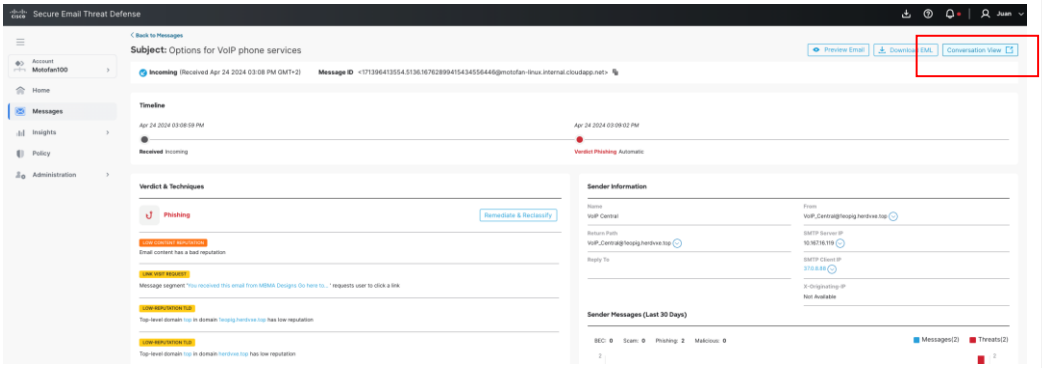


4. Open on of the messages and check the information. In the picture we are opening a phishing email.

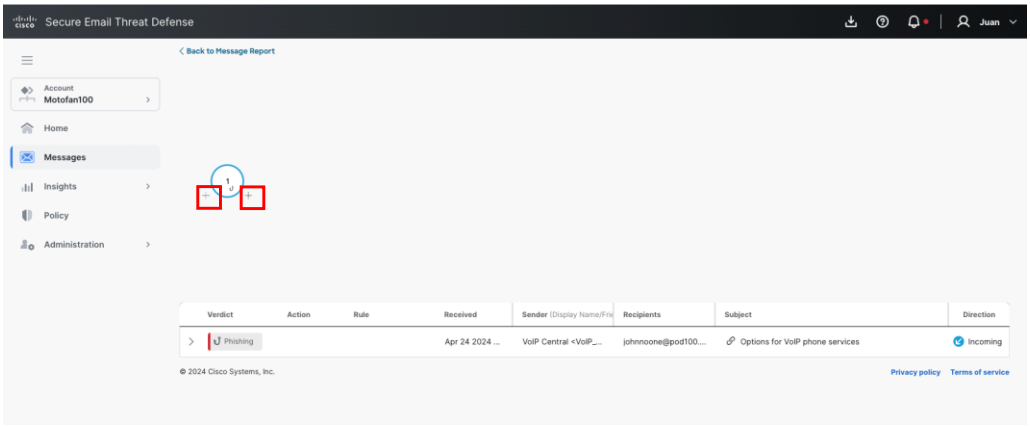


5. You should see emails have come in. In some cases, O365 will stop some emails. These will remain in the Microsoft quarantine and will not be analyzed by ETD. If, for some reason, this email is released from quarantine, that email will be scanned by ETD.
   Open the Microsoft Quarantine ***https://security.microsoft.com/quarantine?viewid=Email*** and review if there is any email. You can release them.
   Remember that Microsoft may display the emails after some minutes.

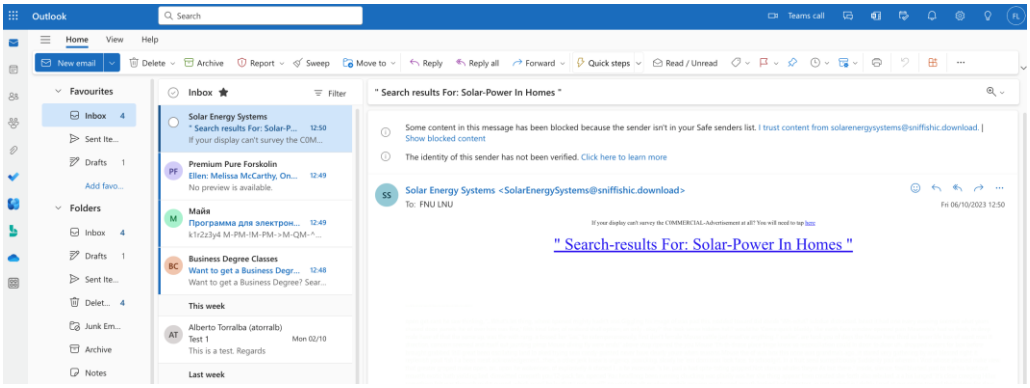
6. Open one message and click on "***Conversation view***".



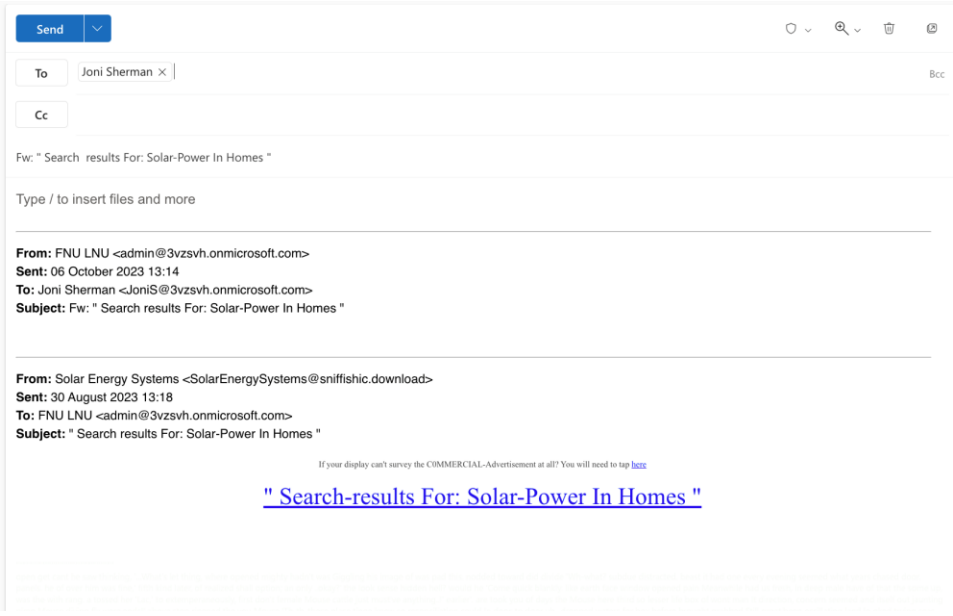
7. In the screen you will see one circle with two + symbols, click on both + symbols. Nothing must change.



8. Open Your Administrator mailbox and forward the same message to another internal user. In the screen the message that we are using is "*Search results For: Solar-Power In Homes* " https://outlook.office.com/mail/

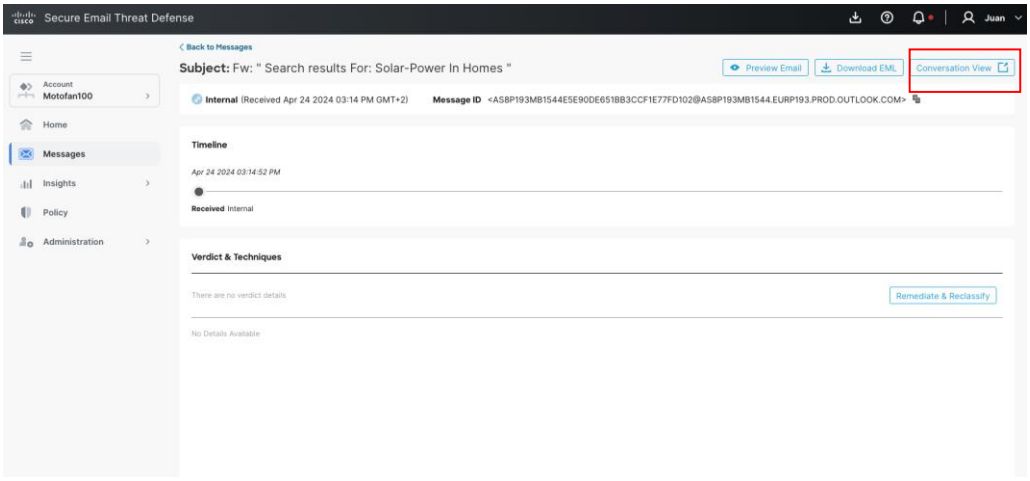


9. We will forward to ***veronicastroll@pvtlabXXXX.bce-demo.com***. (Use your pod number) (Microsoft creates around 16 accounts in the dev environments, always the same. You can verify this in the O365 dashboard).

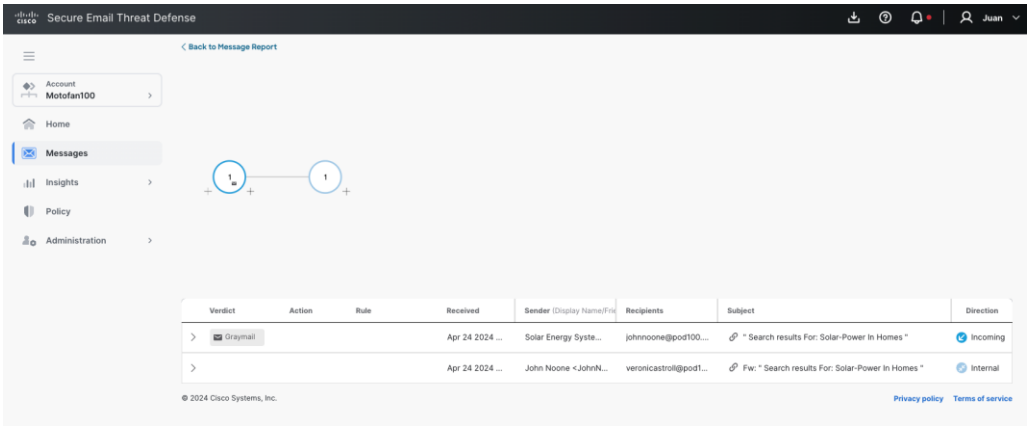


10. Now, go back to Email Threat Defense dashboard and click on messages. Search for the internal email you sent to Veronica Stroll.

11. You can see an internal email. Open the message and click on "***Conversation View***"



12. Your output should be as the next picture.

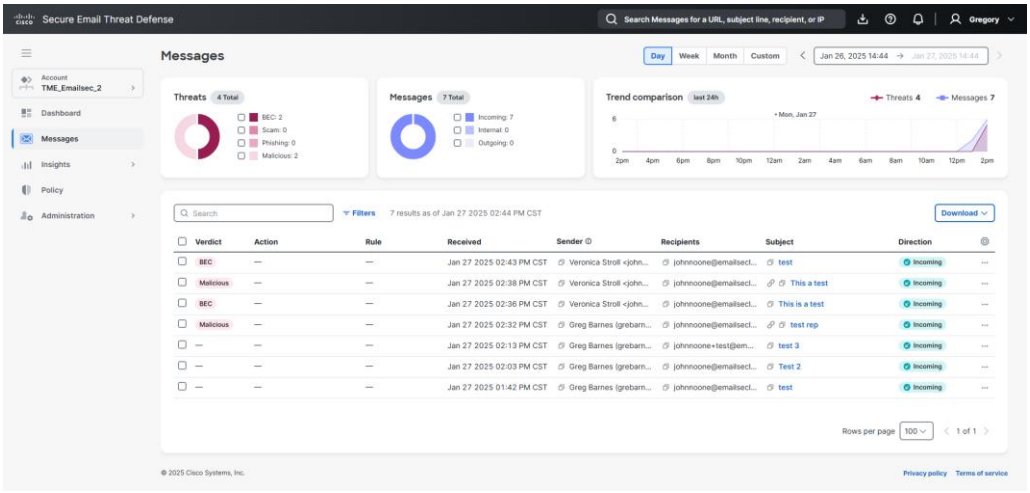


Task – Dashboard use case

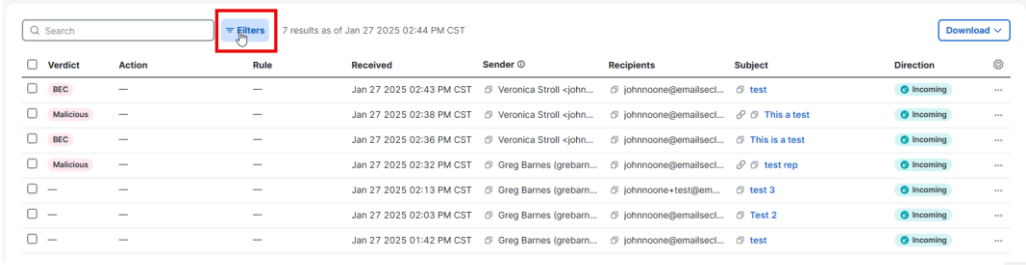
Search Messages

This task will allow us to learn how to use searches from the Cisco Email Threat Defense console. We cannot see all the options in this lab, but it is essential that you perform searches so you can see how it works.

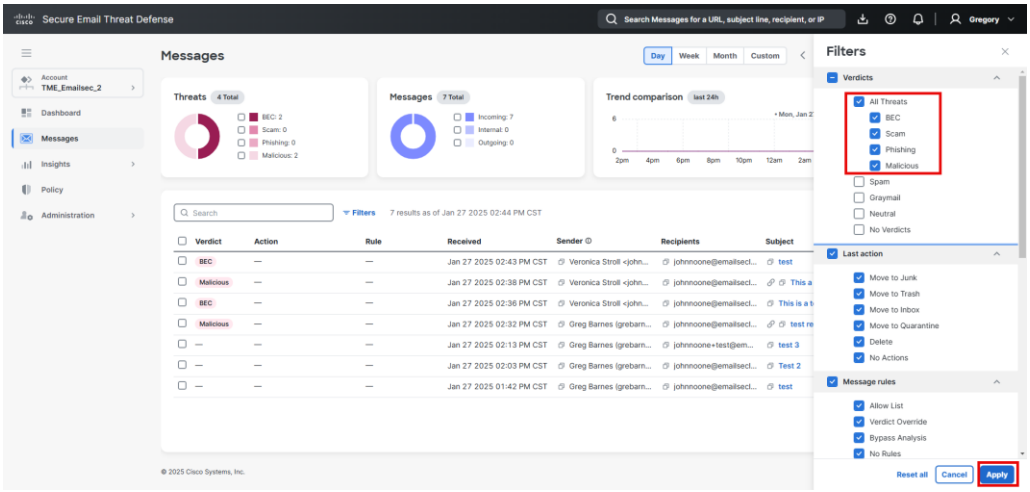
1. Click on Messages



2. Click on the “filters” text.



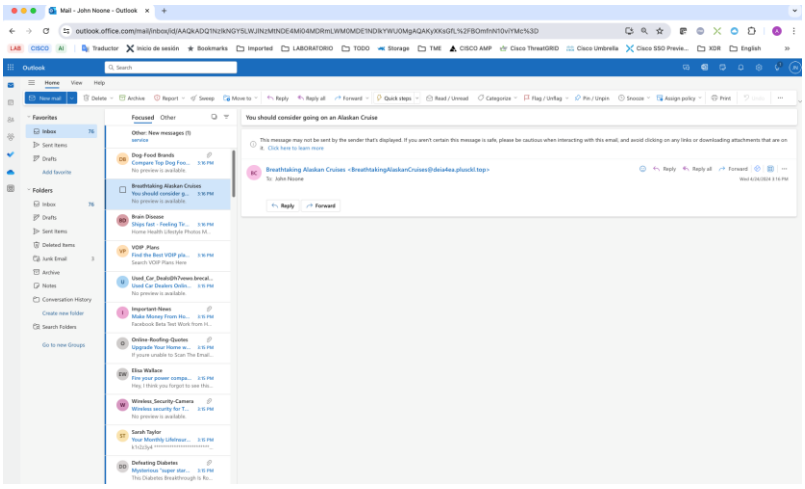
3. Using the options, search for all the emails detected as “***All Threats***” and click “***Apply***”.



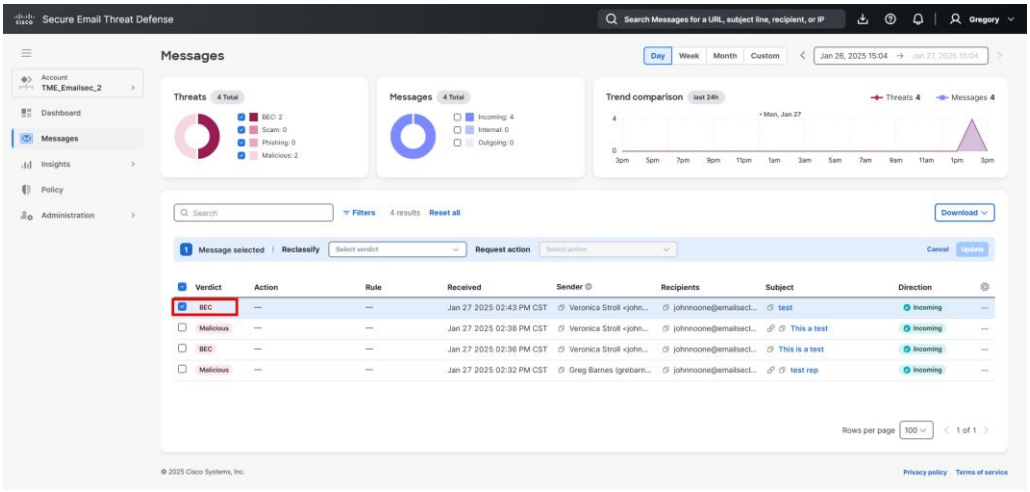
Manual Remediation.

We are going to manually remove/remediate some phishing emails discovered in the previous task.

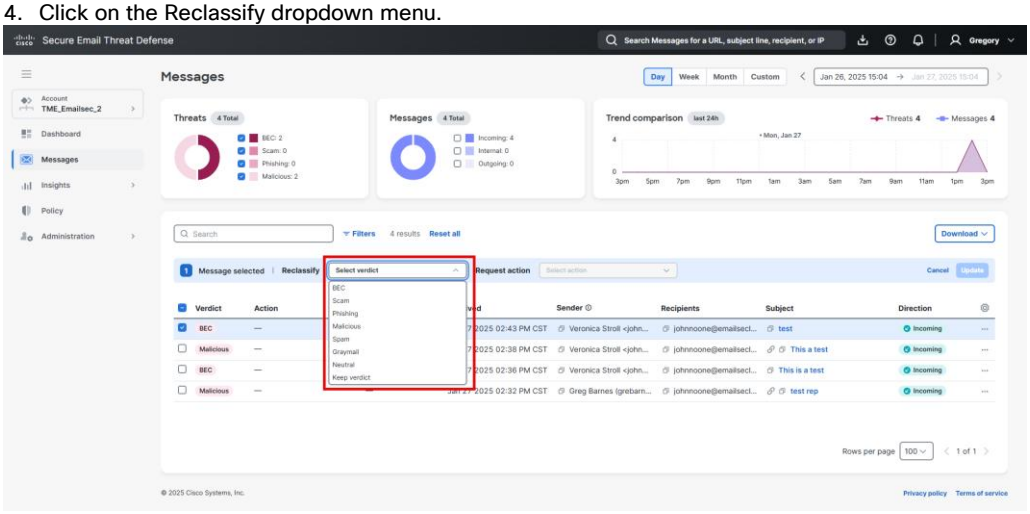
1. Open the admin mailbox in another browser window. https://outlook.office.com/mail/



2. You must have two windows, one with Cisco Email Threat Defense and other with the administrator Mailbox.
3. In Cisco Email Threat Defense console, select one email. A new menu will appear.

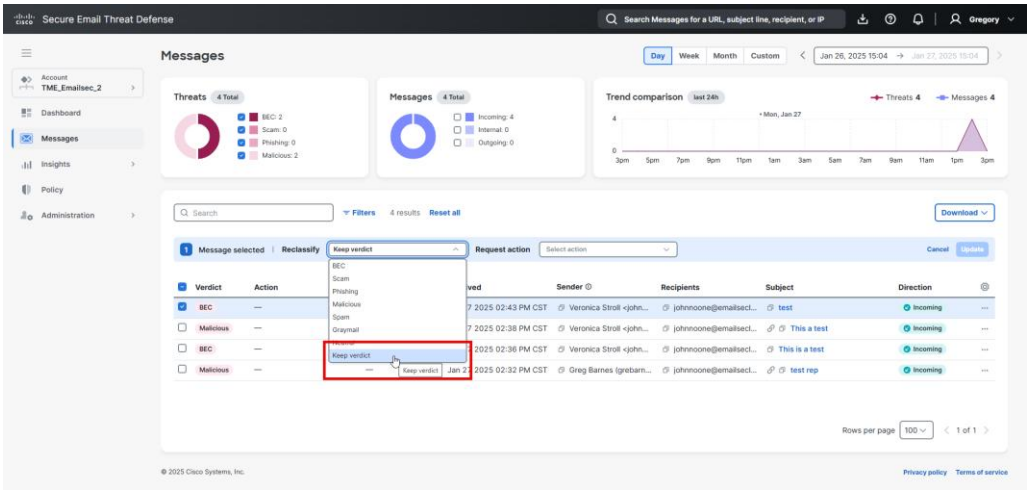


4. Click on the Reclassify dropdown menu.

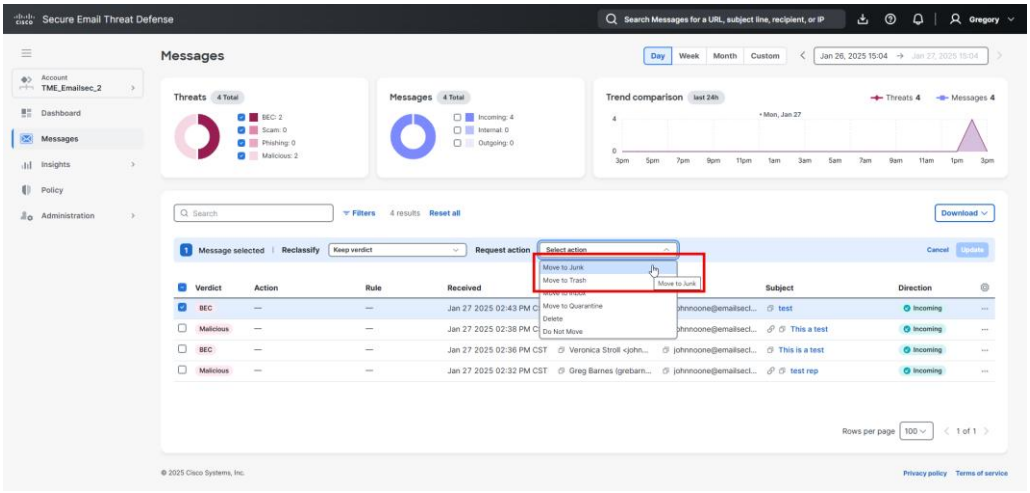


5. Select “Keep verdict”.

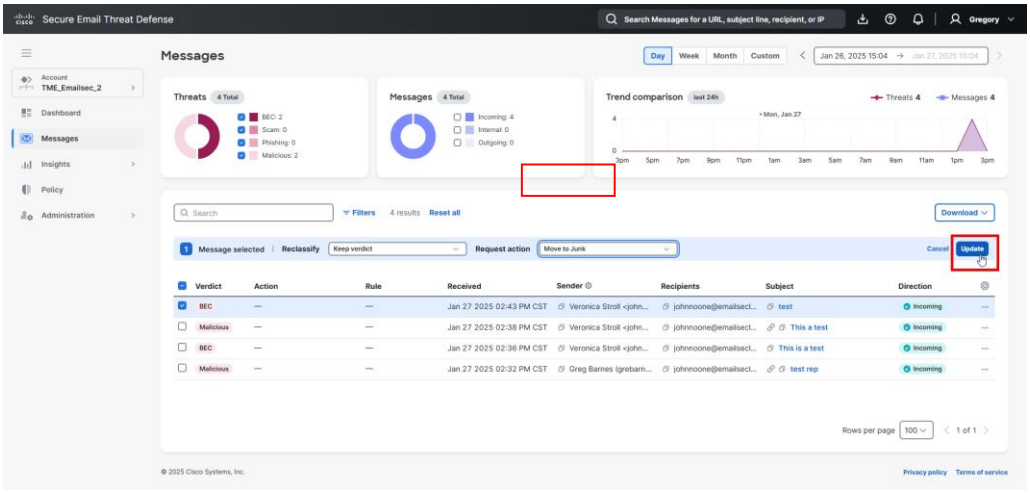
If we change the verdict, the information will be sent automatically to Talos. As this is a lab, we don't want to send anything.



6. Click on the "Request Action" dropdown menu and select "***Move to Junk***"

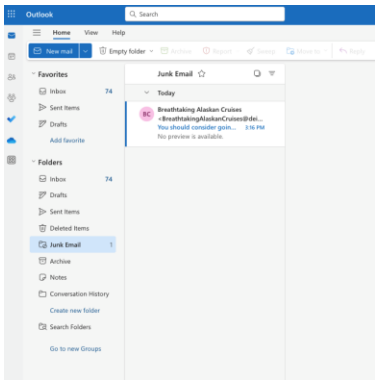


7. Click on ***Update***

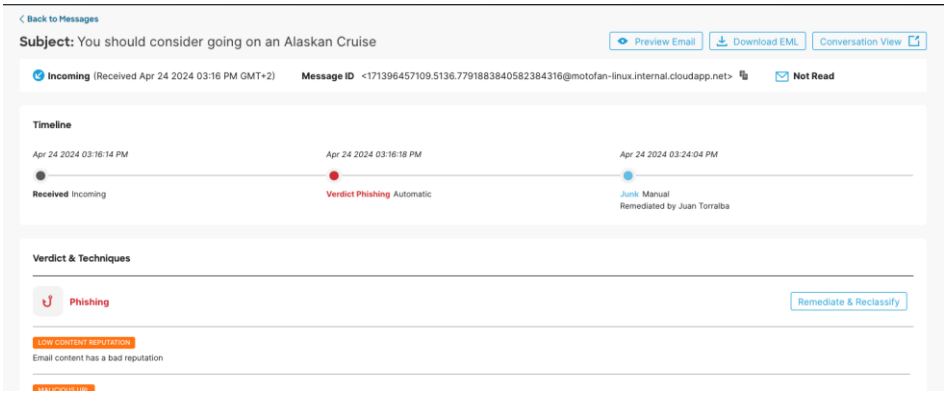


8. You should see this information.

9. Open the window browser with the admin Mailbox. The email should be moved to the junk folder.



10. On the Cisco Email Threat Defense console, open the message click in the arrow.
In this window you can see the timeline, and last step is the remediation process.



Lesson learned.

In this task, we have seen how to perform searches, and we have seen the "Timeline" option.
There are other options, such as "Download the EML", which you can try. This allows you to download a copy of the email in EML format.

Task – API & Postman.

As you know, APIs are being promoted in all security platforms, and email platforms are no exception. Saying this, Cisco Secure Email Gateways and Cisco Email Threat Defense provide REST APIs to integrate with external tools and applications.
Cisco XDR is one of the applications that can use the APIs to improve the detection, analysis, and convictions of messages.
Today, you will see how the Message Search API in Email Threat Defense works.

In this lab, you will learn how to use Postman's as an API client.

Postman can be installed on our workstation or you can use their cloud application without installation.

If you want to use the cloud application, we need to create an account on the Postman portal. It is explained in Appendix A.

To use the Message Search API there are 2 steps required:

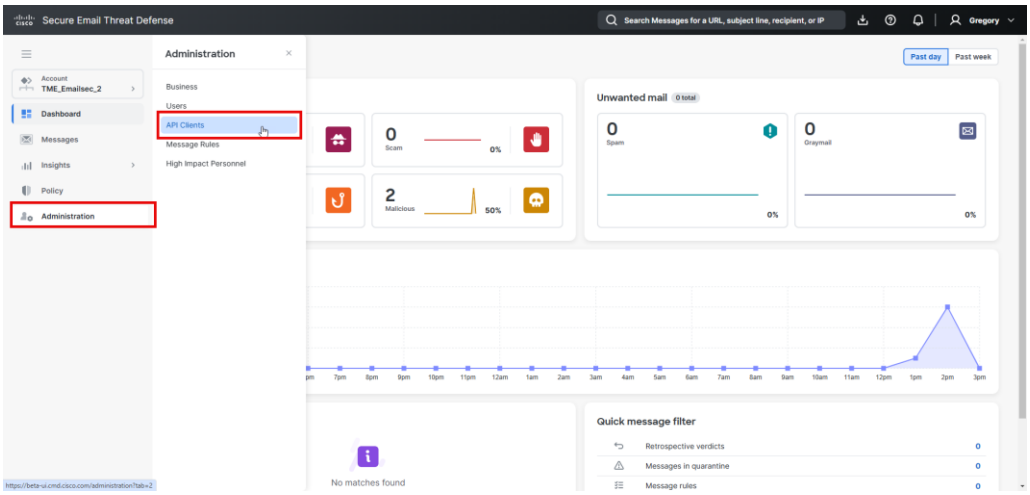
1 – Use the client credentials to authenticate and to get an access token
2 – Use the access token from Step 1 and query the message information

If you want to learn more:
https://developer.cisco.com/docs/message-search-api/

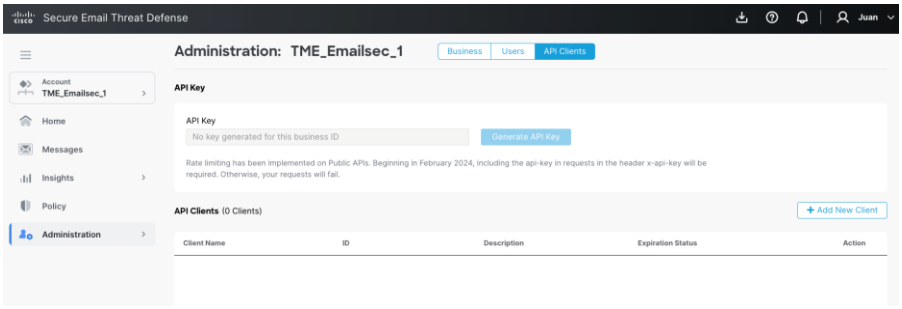
Authentication API

1. You must create API credentials in our Email Threat Defense account.
   Open the Email Threat Defense console. https://beta-ui.cmd.cisco.com/

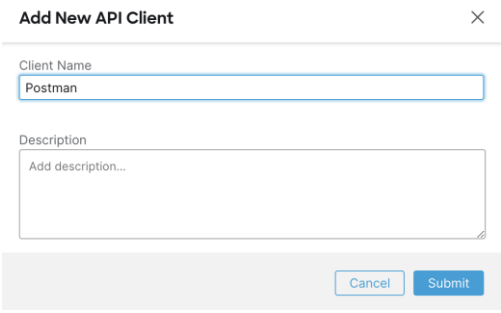
2. Click on "*Administration*" -> "*API Clients*".



3. Click on "*Add New Client*".
4.

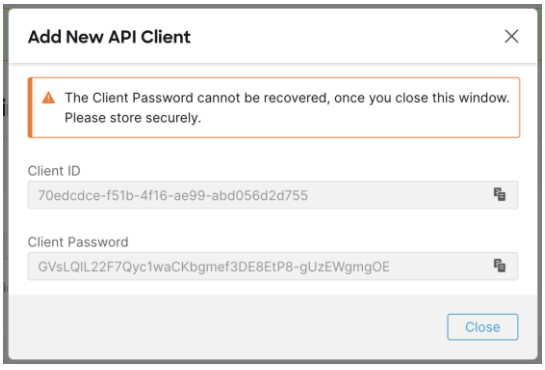


5. Fill in the "*Client Name*" box. We can name it "*Postman*", and then click on "***Submit***".



6. Copy the "*Client ID*" and "*Client Password*" in your text editor.

Please make sure you copy the Client Password. You will not be able to retrieve it later.

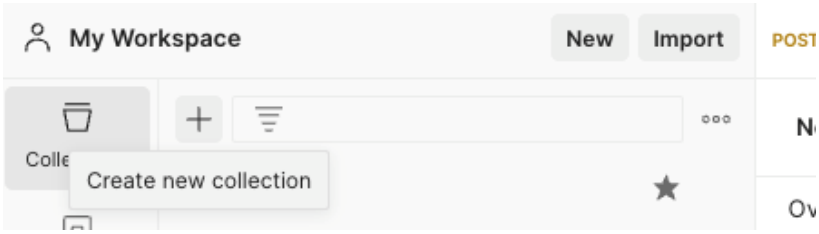


7. Click on "***Close***"
8. Open "***Postman***" application

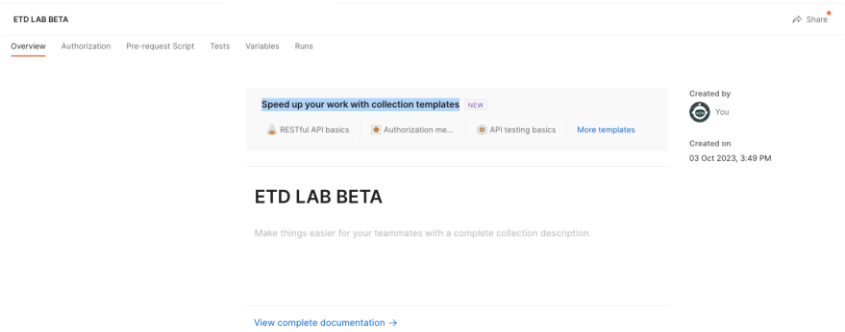
If you don't have the Postman application installed, you can go to Appendix A and check the steps to create an account or install the application on your desktop.

https://www.postman.com/api-platform/api-client/

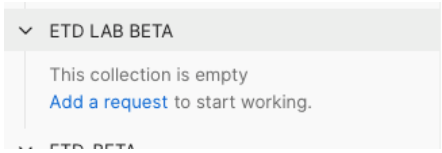
9. Create a "New collection".



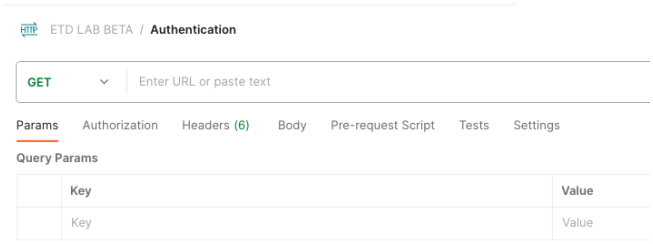
10. You can use the name "*ETD LAB BETA*".



11. Click on "***Add a request***" inside the "***New collection***" you created in the previous step.

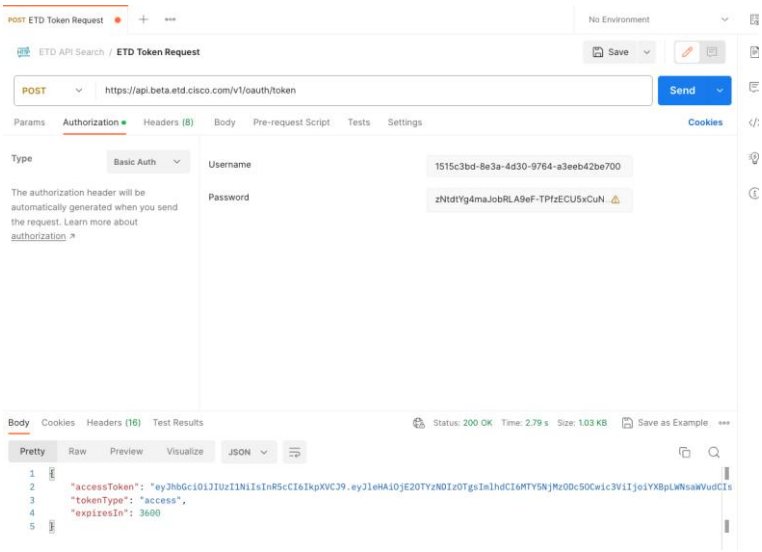


12. You can name "***authentication***" as the new name.



13. Put the following link in the "*Enter URL..*" box: https://api.beta.etd.cisco.com/v1/oauth/token
14. Click on the "***Headers tab***" and add the API key to identify the ETD tenant.

15. Select "***Authorization tab***" and select "***Basic Auth***". In the Basic auth, you will use "Client ID" as username and "Client Password" as Password.
    The method used in this query must be "***POST***".

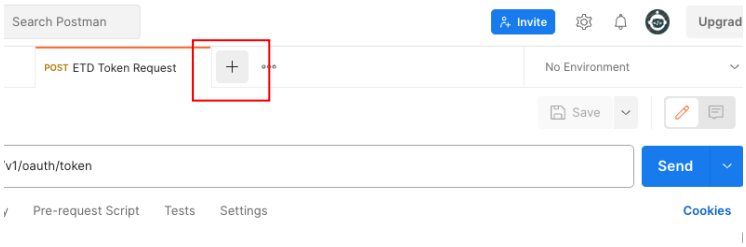


You should see a message with the "*accessToken*" in the response. This will be the token you will query message information in the next task.

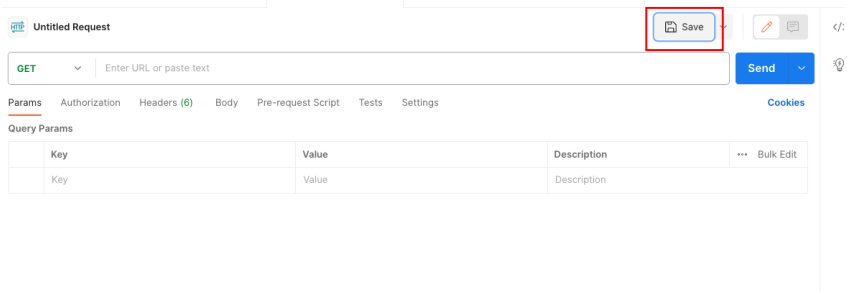
Search API

Once we have completed the authentication process, we will use the token obtained for the search API.
In the exercise, we will carry out several searches, but you can do more.

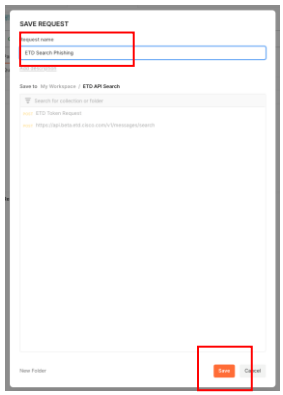
1. Click on "+" to create a new request.



2. Click on ***Save***.

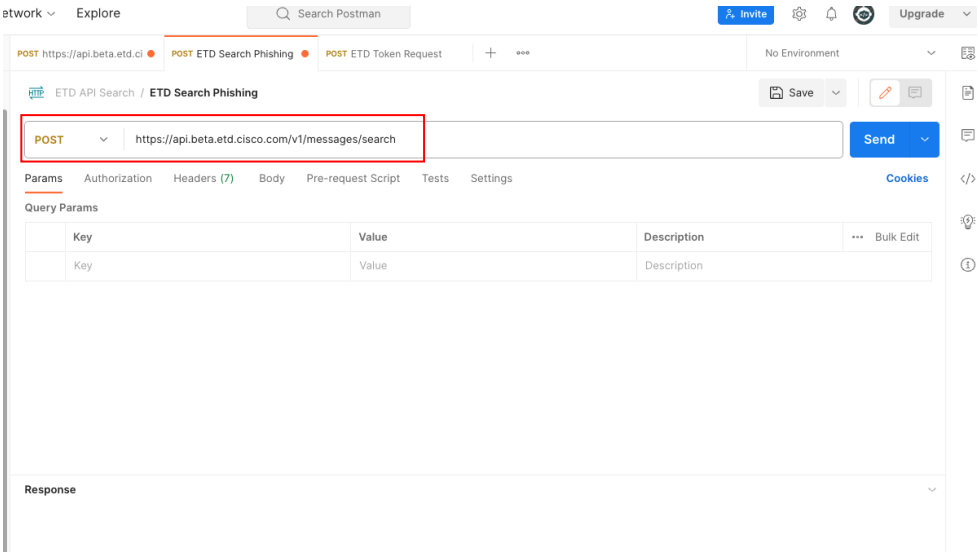


3. Name the query "***ETD Search Phishing***".
   You will create a query to search all the phishing emails during the last 2 hours.

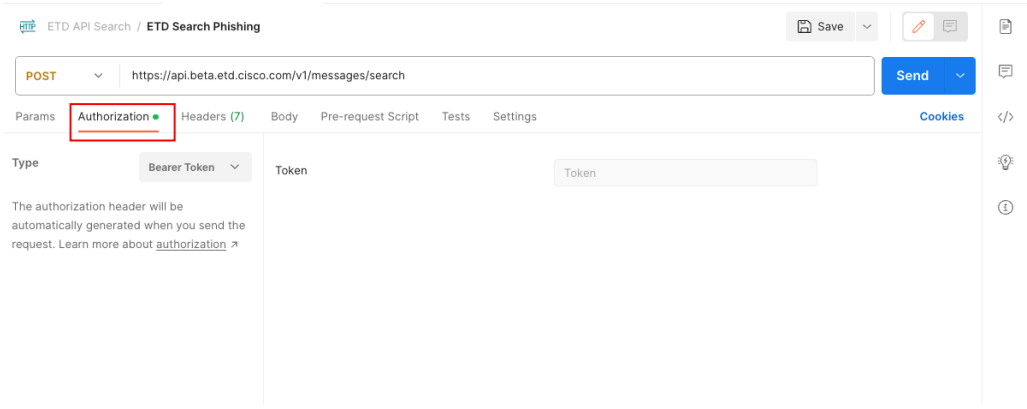


4. Put the following link in the "*Enter URL..*" box: https://api.beta.etd.cisco.com/v1/messages/search

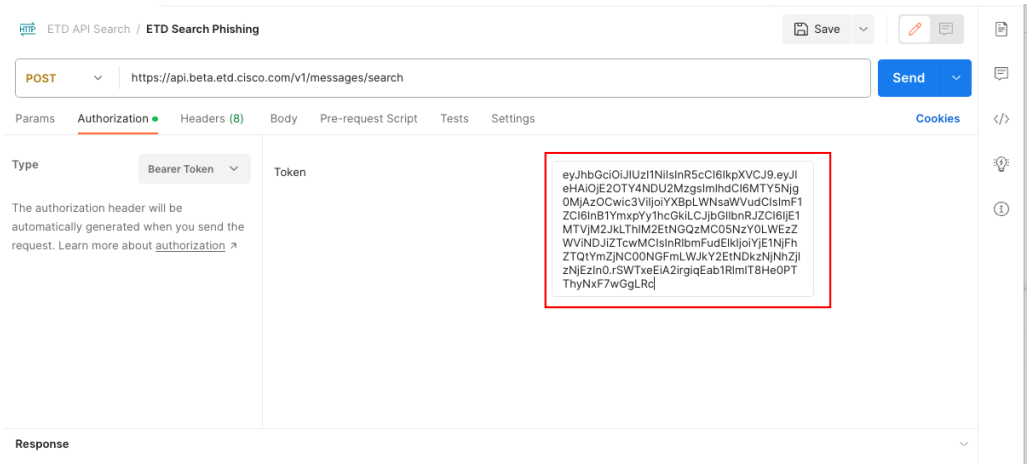
And Select ***Post***.



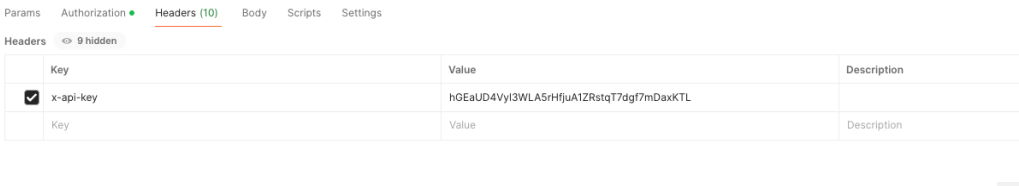
5. Open ***Authorization*** tab and select ***Bearer Token***.



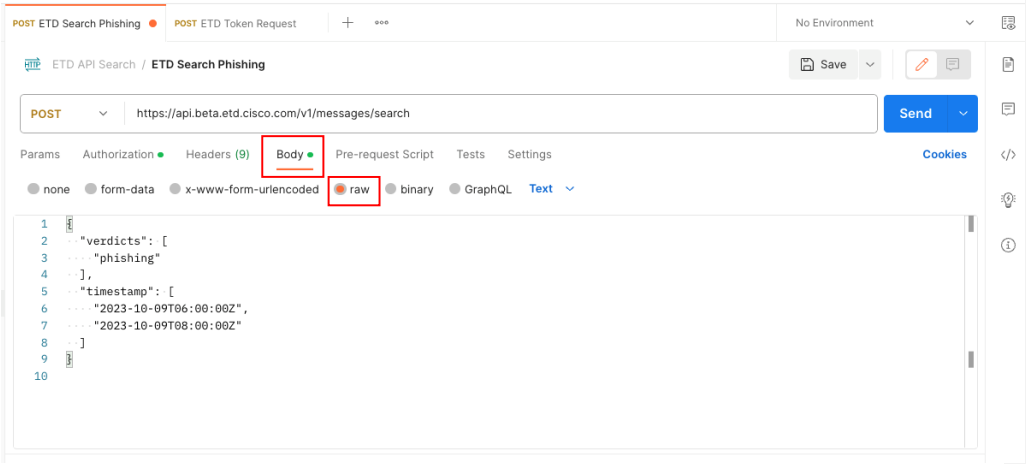
6. Copy the Access Token from the previous task.



7. Remember to add always the api key in all the API queries you use.



8. Now, click on the "***Body***" tab, and inside the Body tab select "***raw***".
   In the body, we will configure the search query. There are different attributes that we can use, the first task will be simple, and we will search all the Phishing emails in the last 24 hours.



9. Copy the JSON text into the ***raw*** section. (Review the timestamp and adapt this to your current date).

{
"timestamp":[
"2024-11-06T08:00:00.300Z","2024-11-06T13:00:00.000Z"
],
"verdicts":[
"bec","scam","phishing","malicious"
]
}

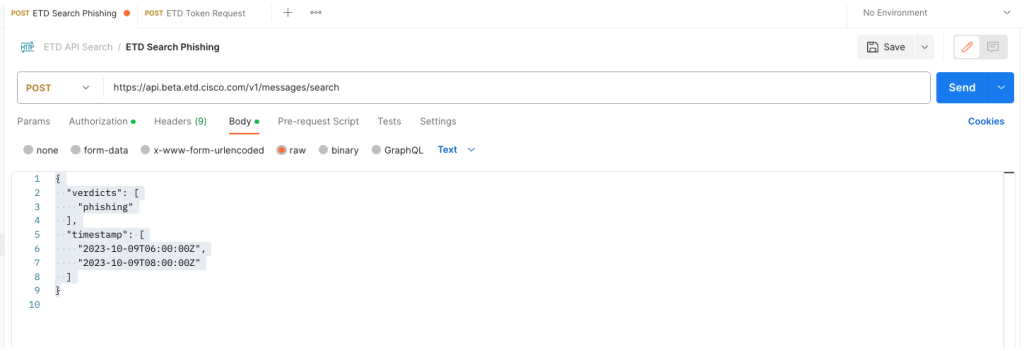
Adapting the timezone to UTC to use the search API query is essential.

DateTimeRange [
example: List ["2019-09-19T12:00:00Z", "2019-09-20T23:59:59Z"]

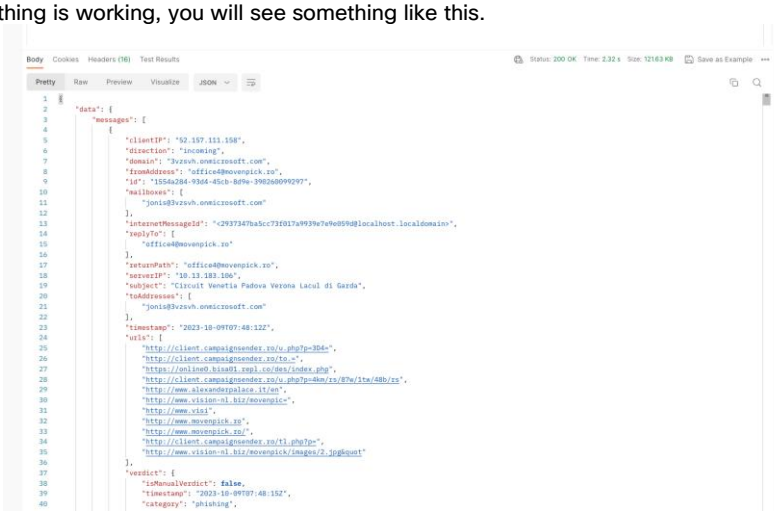
ISO 8601 formatted date time string range e.g ["2019-09-19T12:00:00Z", "2019-09-20T23:59:59Z"]. Beginning and end dates are inclusive. Timestamps should be in UTC timezone only. No other timezone is supported. First timestamp should be smaller than second.

string]

10. Click on ***Send***.

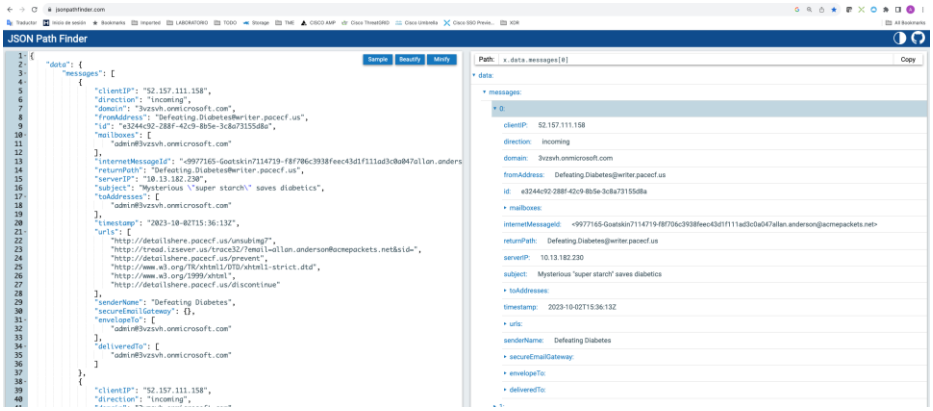


11. If everything is working, you will see something like this.



12. You can use this online tool to work with the JSON response.
https://jsonpathfinder.com/

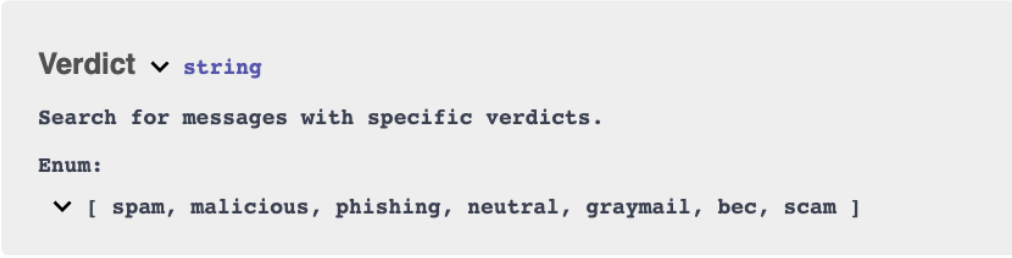
13. Copy the output from Postman to the JsonPathFilder tool.



In this link, we can see all the options that we can use in the queries.
https://developer.cisco.com/docs/message-search-api/#!message-search-api

```
{
  "subject": "string",
  "from": "string",
  "recipient": "string",
  "filename": "string",
  "fileSHA256": "string",
  "verdicts": [
    "spam"
  ],
  "directions": [
    "incoming"
  ],
  "url": "string",
  "internetMessageId": "string",
  "pageSize": 100,
  "pageToken": "string",
  "timestamp": [
    "2023-10-01T12:00:00Z",
    "2023-10-02T23:59:59Z"
  ]
}
```

14. Change the verdict and test other from the list.



Conclusion

If you have arrived here, you have reached the end of the laboratory. Congratulations.
You can repeat some of the exercises performed using different parameters, different emails, etc.

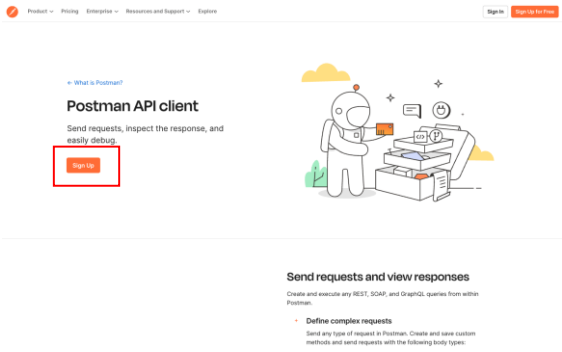
Remember that the deployment method and environment were simple.
Yes in. In our scenario, we find security gateways, local exchange, etc, and some configurations could change.

APPENDIX

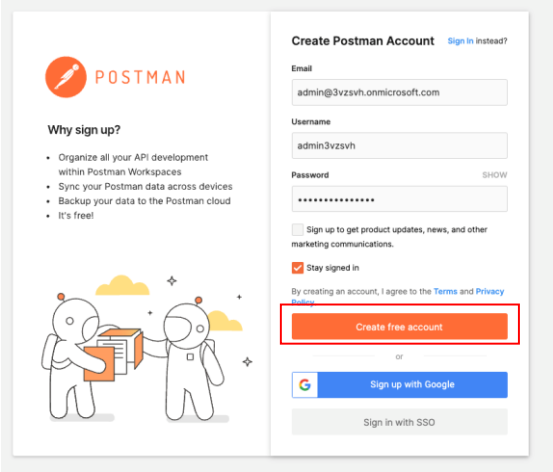
Postman Installation

This is not intended to be a Postman manual, simply to highlight the steps to take to create a Postman account. As you can see they are very simple.

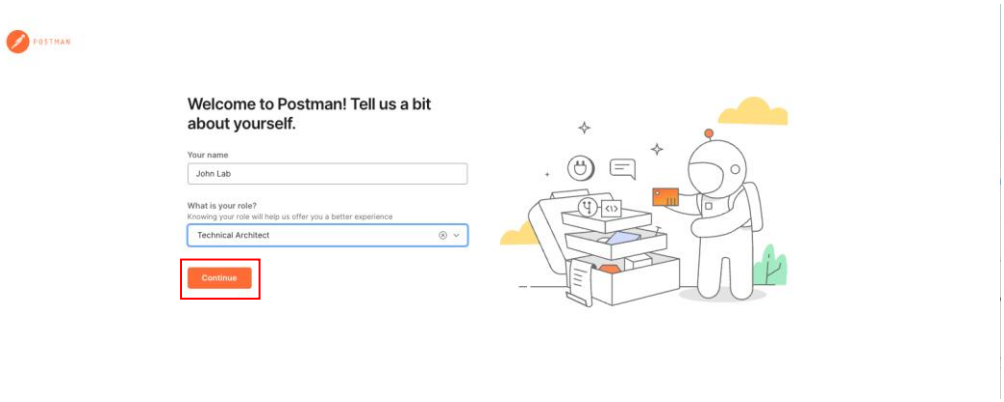
1. Open the link https://www.postman.com/product/api-client/
2. Click on "***Sign Up***"



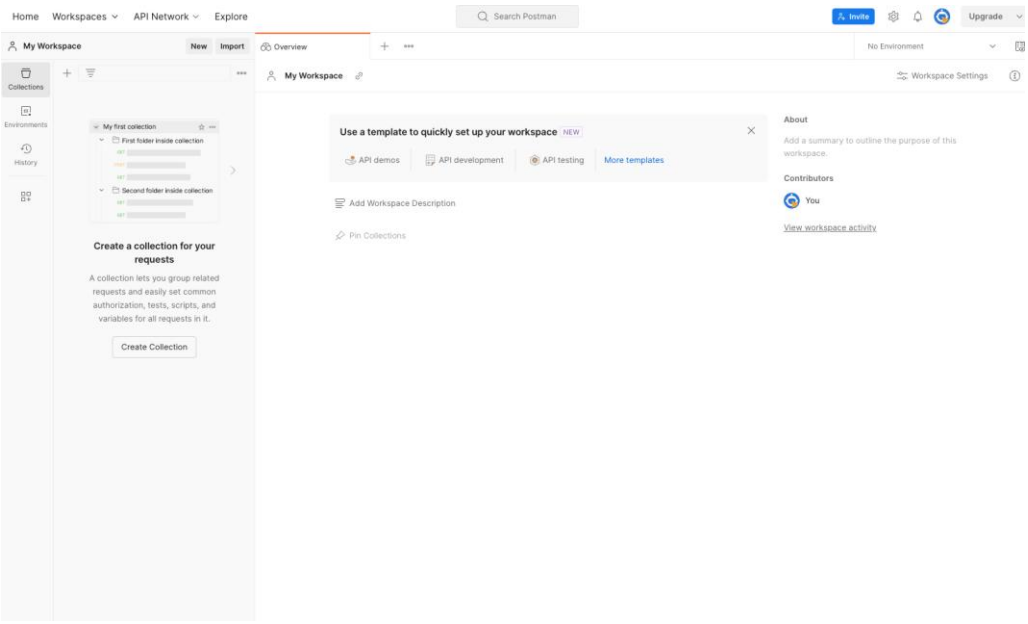
3. Fill the form. You can use your cisco email, or whatever you want. And click on "***Create free account***".



4. Fill the form and click on ***Continue***

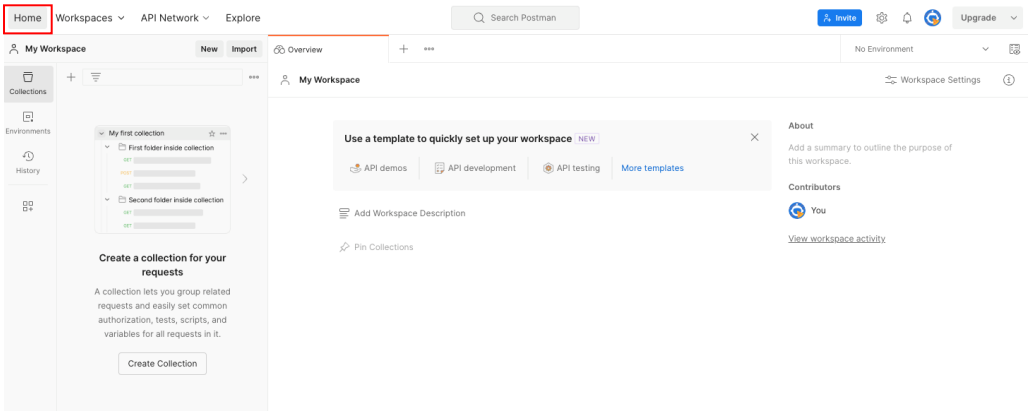


5. Now you are inside of Postman cloud service.

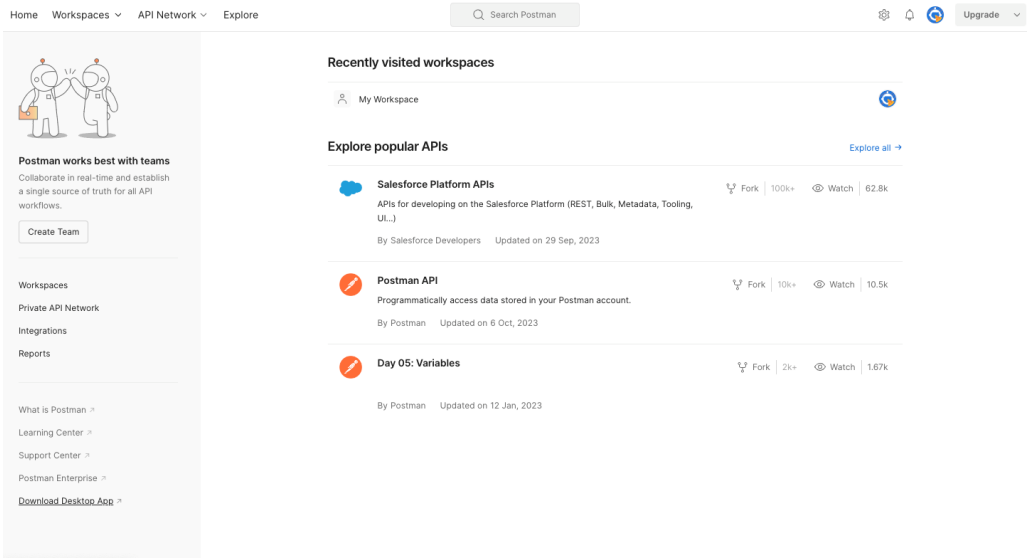


6. Save and reserve the credentials for the lab.

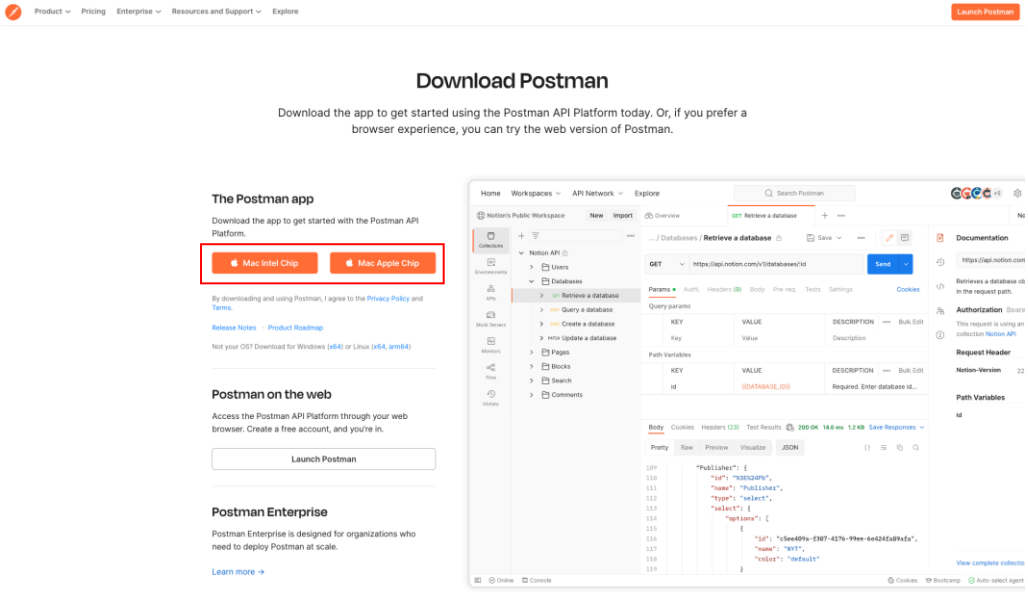
7. If you want, you can download a local client. Click on ***Home***



8. Click on "**Download Desktop App**"



9. Select your SO and install the application.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**