CIS-CAT Pro Assessor: Amazon Elastic Kubernetes Extraction Guide Tip Sheet

CIS-CAT Pro Assessor

December 2023

Revision history

Revision #	Date	Changes made	Performed by	Authorized by
1.0	31.08.2023	New Tipsheet		Adi Kogan
1.1	12.12.2023	Update CyMA import process and general steps structure	Noam Hazon	Adi Kogan

Table of content

1. Tool Description....4
2. Licensing Requirements....4
3. Who Should Use the Document....4
4. Requirements & Permissions....4
5. High Level Process Flow....5
6. AWS - Creating Dedicated User & Policy....6
7. CIS-CAT Pro Configuration....14
8. AWS CLI & "Kubectl" Configuration....15
9. The Extraction Process....17
10. Open and Review Integration Results....21

1. Tool Description

CIS-CAT Pro Assessor is a Java-based tool that scans a target system's configuration settings and reports the system's compliance to the corresponding CIS Benchmark. The results generated are only presented in machine-readable format.

2. Licensing Requirements

The CIS-CAT Pro Assessor is available for download through Mastercard's resources. For the complete download and installation guide please refer to the "CIS-CAT Pro Assessor: Extraction Guide Tip Sheet".

The CIS-CAT Pro Assessor tool must be deleted once the configuration files export is completed.

3. Who Should Use the Document

This document is for "Cyber Quant CyMA" users participating in an organizational cyber risk and security assessment using Mastercard's "Cyber Quant Cyber Risk Quantification" platform. The document is also targeted at experienced IT and cyber professionals who will extract AWS Elastic Kubernetes configuration files for the "Cyber Quant CyMA" cyber risk and security assessment.

4. Requirements & Permissions

- CIS Tool Requirements:
  - Machine Requirements -
    - Linux machine
      - AWS CLI to authenticate and connect to the EKS Cluster.
    - CIS-CAT Pro Assessor requires a Java Runtime Environment (JRE) at or above version 1.8.
  - Access Requirements -

- Administrative permissions to execute the CIS-CAT Pro Assessor.
- Administrative permissions to connect to the organizational technological assets.

5. High Level Process Flow

Create a user in the AWS account that will be used to handle AWS API calls.

Create the policy to handle API calls and attack it to the new user.

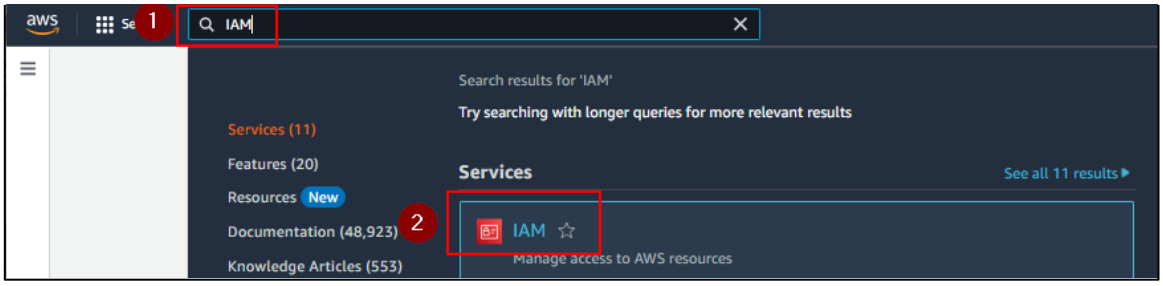
Connect the AWS CLI to the appropriate AWS EKS region and cluster to extract the information from.

Execute the CIS tool to perform the benchmark on the AWS EKS cluster and import the generated report into CyMA.

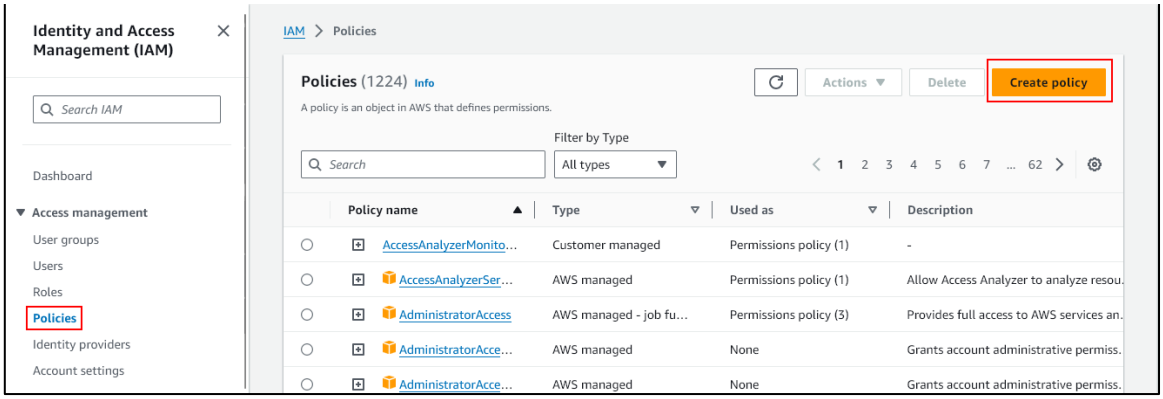
6. AWS - Creating Dedicated User & Policy

1. It is recommended to create a dedicated read-only AWS API calls user in the AWS IAM Panel. For authentication, AWS CLI must have a user or role configured (no IAM permissions are needed for the assessment itself). The user or role must be granted the **eks:DescribeCluster** permission, which is utilized for The update-kubeconfig command to target the specific cluster for assessment.

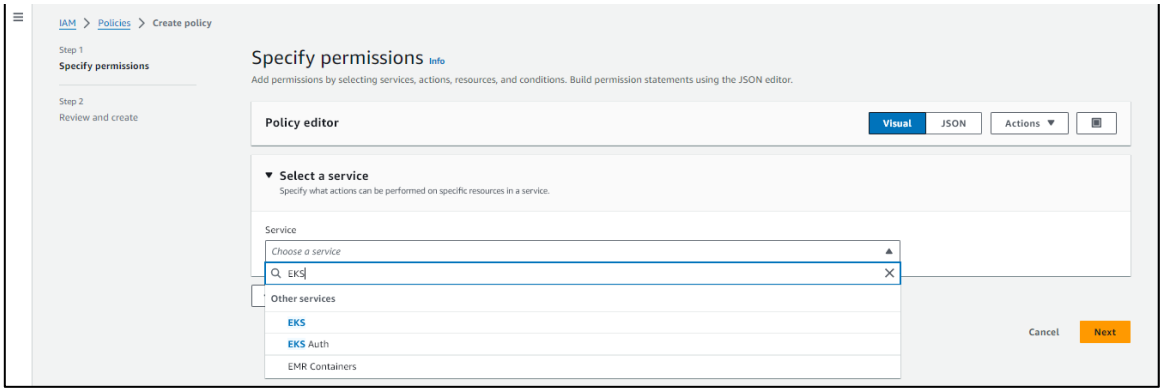
2. Search for "IAM" and click on it to navigate to the platform for users and roles management.



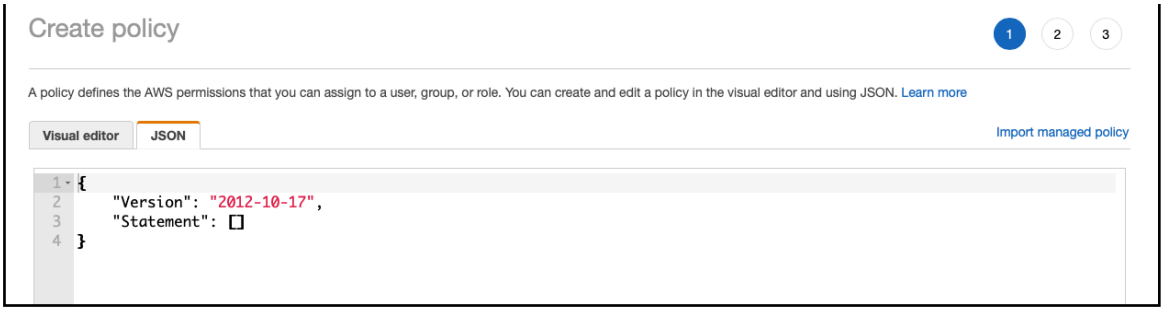
3. In the menu on the left, under the "Access management" section, click on "Policies" and then on "Create Policy".



4. Select EKS Service in the Visual editor.



5. Click on the "JSON" tab in the policy menu.



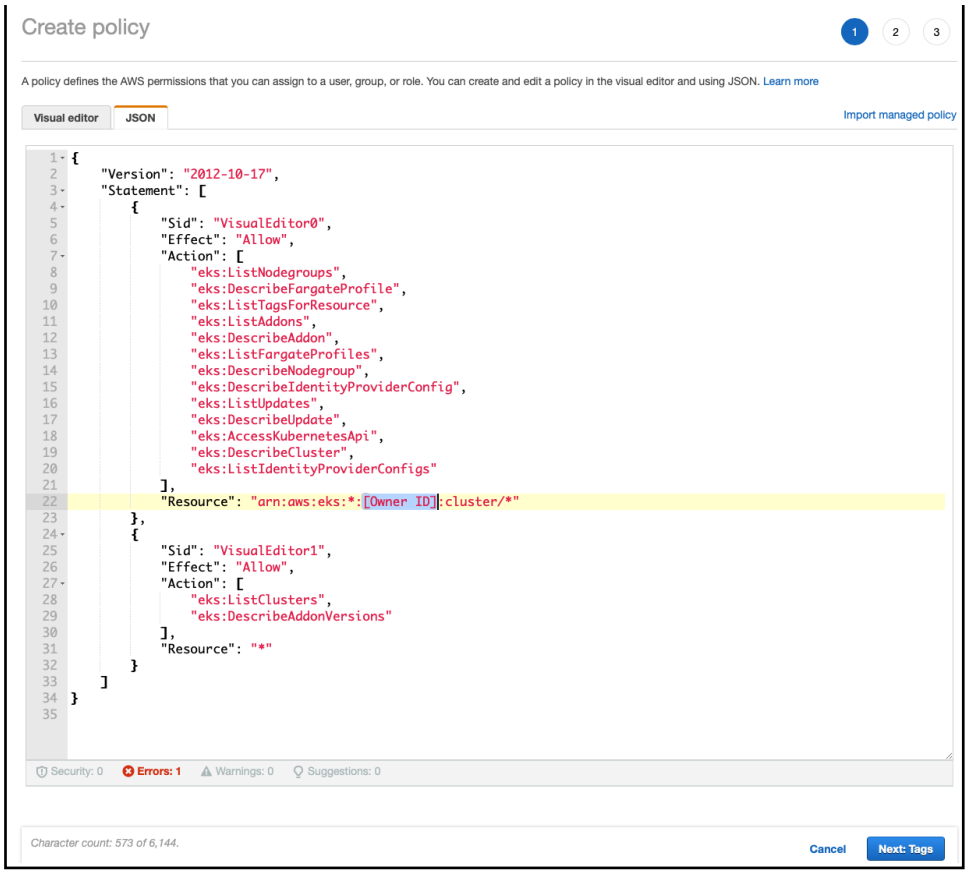
6. Run the following command in AWS CLI to extract the Owner ID

```
aws sts get-caller-identity --query Account --output text
```

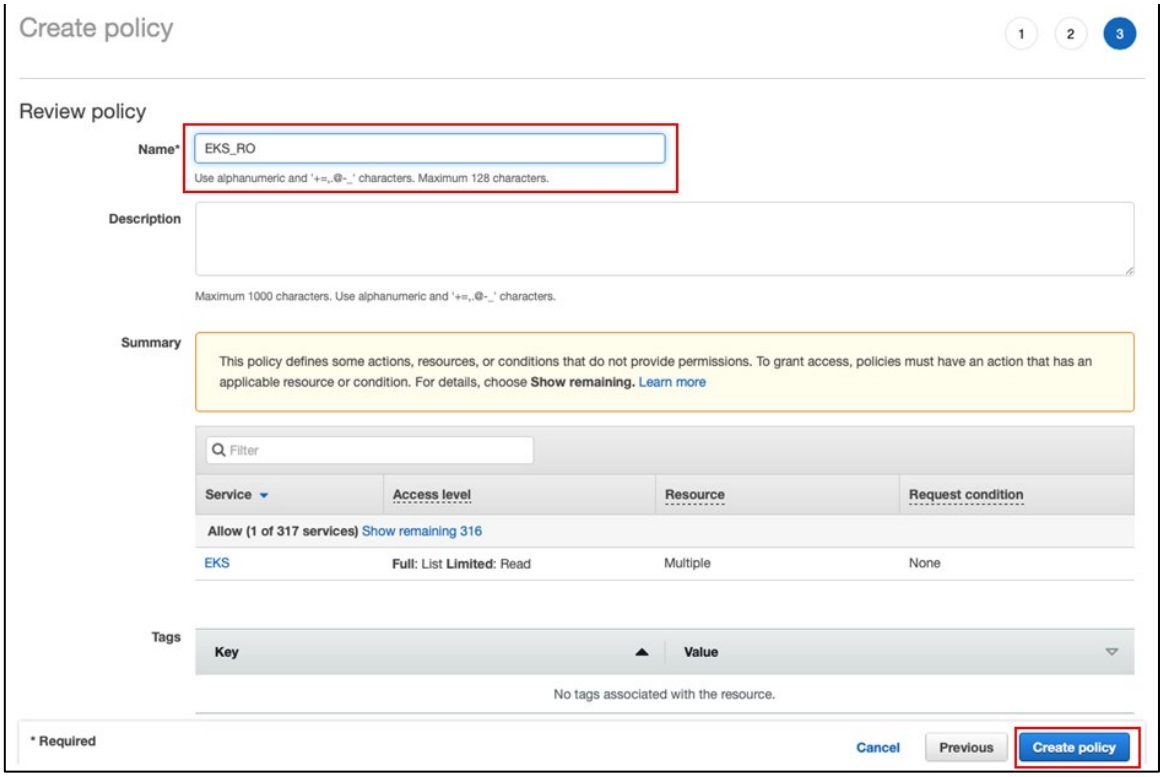
7. The text below will be placed in the content of the policy in the next step. Replace the [Owner ID] in the "Resource" section with your owner ID and copy the text.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "eks:ListNodegroups",
                "eks:DescribeFargateProfile",
                "eks:ListTagsForResource",
                "eks:ListAddons",
                "eks:DescribeAddon",
                "eks:ListFargateProfiles",
                "eks:DescribeNodegroup",
                "eks:DescribeIdentityProviderConfig",
                "eks:ListUpdates",
                "eks:DescribeUpdate",
                "eks:AccessKubernetesApi",
                "eks:DescribeCluster",
                "eks:ListIdentityProviderConfigs"
            ],
            "Resource": "arn:aws:eks:*:[Owner ID]:cluster/*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "eks:ListClusters",
                "eks:DescribeAddonVersions"
            ],
            "Resource": "*"
        }
    ]
}
```

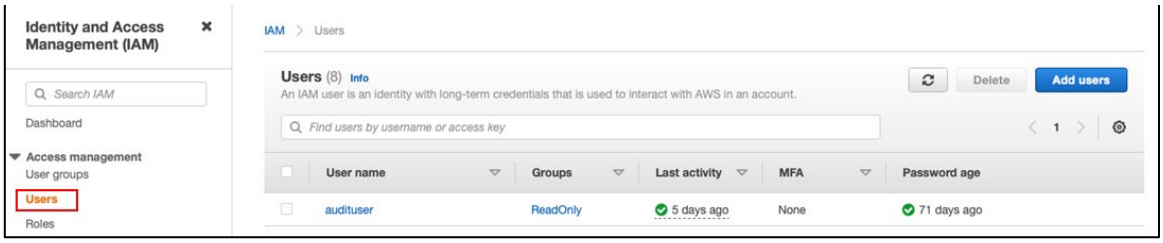
8. Paste the example text inside the JSON editor and click on “Next: Tags” until you get to the ‘Review policy” page.



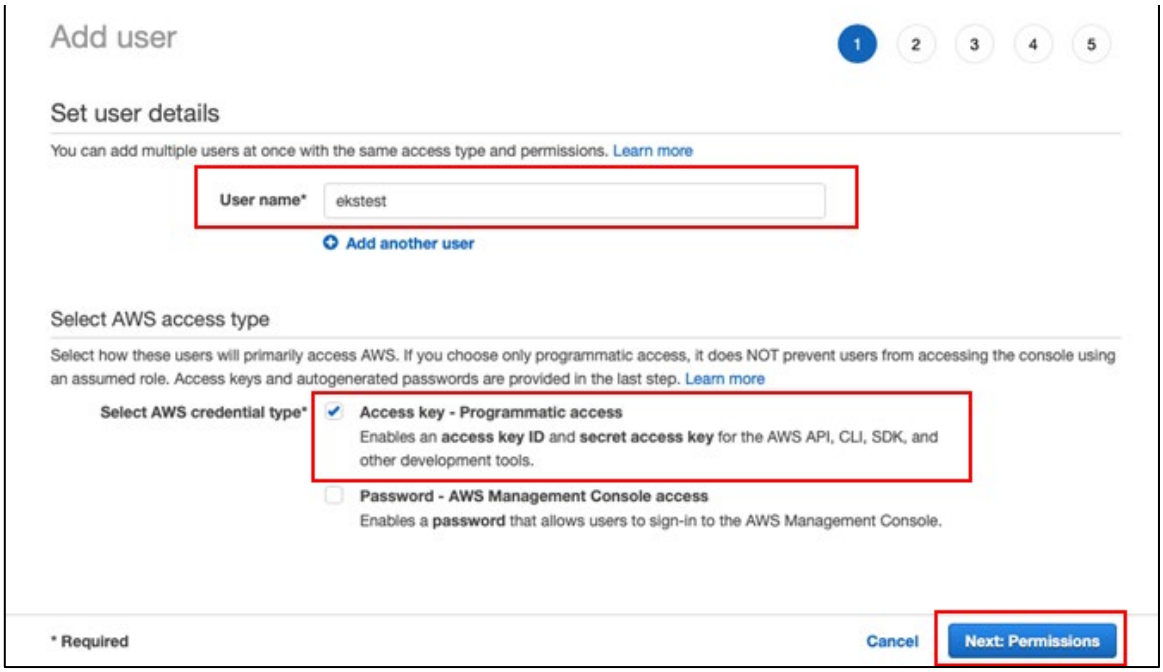
9. Enter the policy name and click on "Create policy".



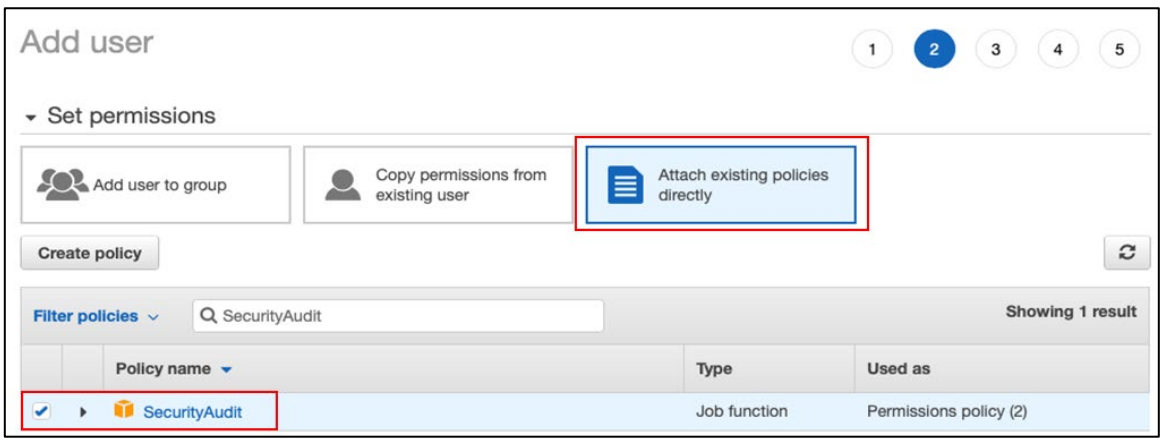
10. In the IAM management panel, select the "Users section" and click on "Add users".



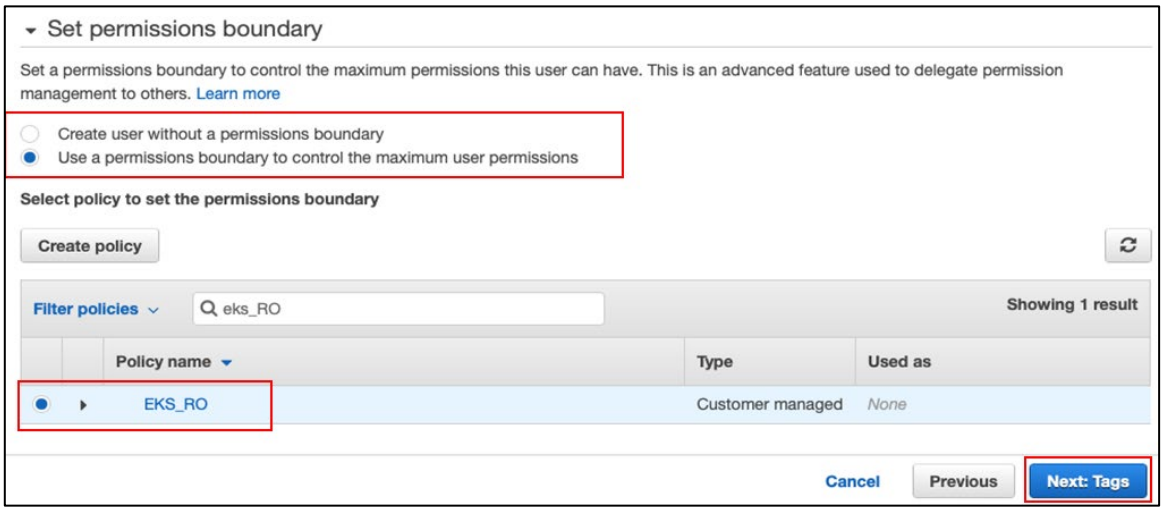
11. Type the username, select AWS credential type – Access key – Programmatic access, and click on "Next: Permissions".



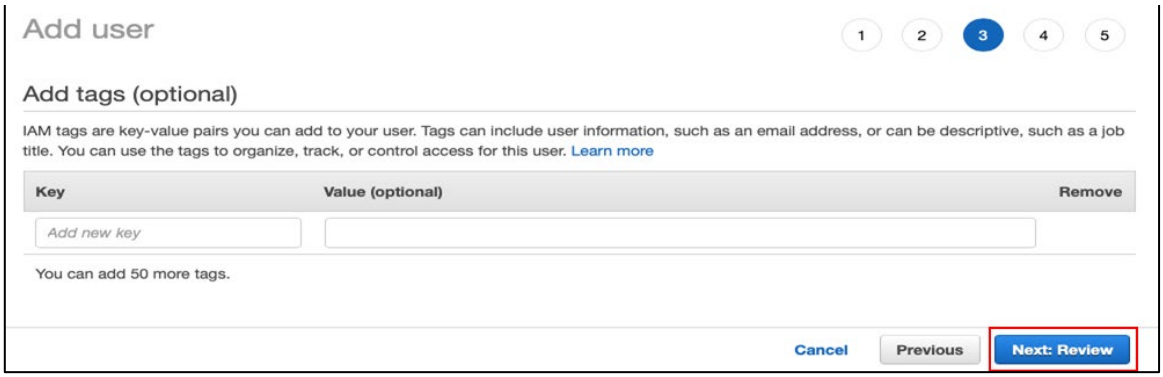
12. Select "Attach existing policies directly" and search for the "SecurityAudit" policy and check its box.



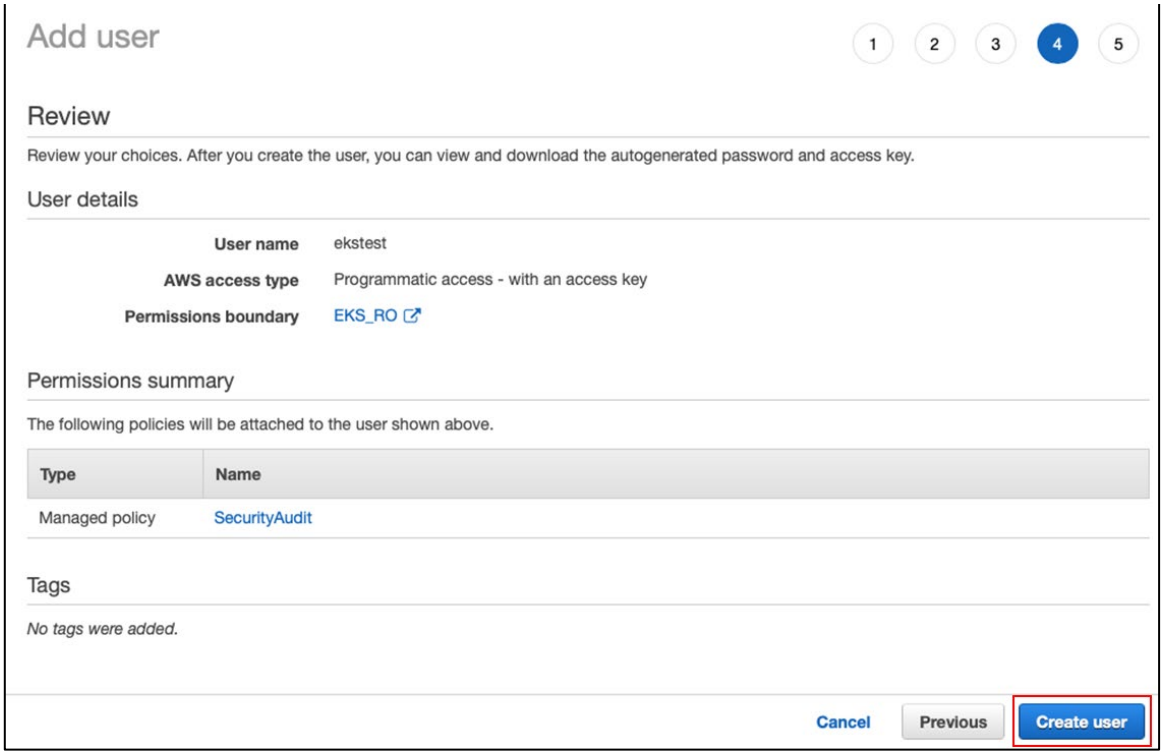
13. In the "Set permissions boundary" section select "Use a permissions boundary to control the maximum user permissions" and find the policy created earlier to select it. Click on "Next: Tags".



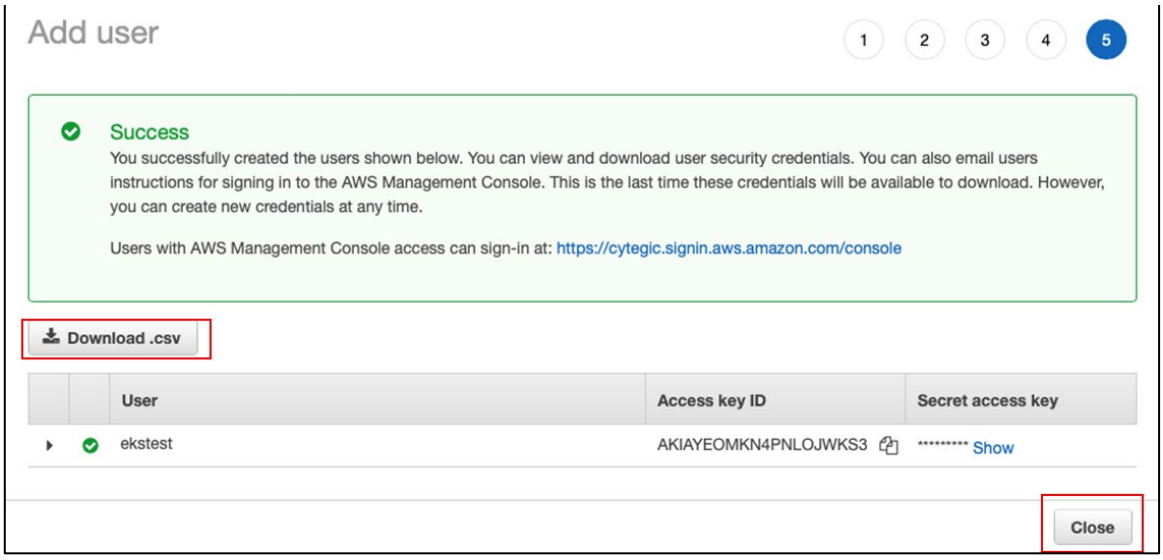
14. Click on "Next: Review".



15. Review the configurations and click on "Create user".



16. When a user is created, click on "Download .csv". The file contains the user's access key ID and secret access key. This information is essential for the next steps. Once the file is downloaded, click on "Close".



7. CIS-CAT Pro Configuration

1. CIS-CAT Pro Assessor is a Java-based tool that requires the OpenJDK v8 + to be installed on a client machine, check the Java version using the command:

   `java --version`

```
ubuntu@ip-172-20-25-148:/$ java --version
openjdk 11.0.14 2022-01-18
OpenJDK Runtime Environment (build 11.0.14+9-Ubuntu-0ubuntu2.20.04)
OpenJDK 64-Bit Server VM (build 11.0.14+9-Ubuntu-0ubuntu2.20.04, mixed mode, sha
ring)
```

2. CIS-CAT Pro Assessor must be extracted locally on a Linux machine (EC2 or another server) that has access to the EKS cluster servers.

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ ls
Assessor-CLI.bat  THIRD-PARTY-LICENSES  license      sce
Assessor-CLI.jar  benchmarks            logs         scripts
Assessor-CLI.sh   config                misc         setup
Assessor-GUI.exe  custom                python.log   third_party_licenses
README            lib                   reports
ubuntu@ip-172-20-25-148:~/Documents/CIS$
```

3. An automated assessment using the CIS Amazon EKS Benchmark must be performed as a local assessment or "local" session type. CIS-CAT Pro Assessor will run various "kubectl" and "kubelet" commands to perform the assessment.

4. Ensure security groups provide access to port 8080 from the Linux machine where the CIS-CAT Pro Assessor resides. Other ports may also need to be opened depending on each organization's specific configuration.

8. AWS CLI & "Kubectl" Configuration

1. It is also required that AWS CLI and "kubectl" are installed.

2. Verify that AWS CLI is installed using the command:

   ```
   aws –version
   ```

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ aws --version
aws-cli/1.18.69 Python/3.8.10 Linux/5.11.0-1022-aws botocore/1.16.19
```

3. Verify that "kubctl" is installed using the command:

   ```
   kubectl version --short --client
   ```

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ kubectl version --short --client
Client Version: v1.23.4
```

4. If AWS CLI and/or kubectl are not installed, install these components according to the instructions in the following links:

   Kubectl - https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html
   AWS CLI - https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

5. Configure AWS CLI connection to your AWS environment using credentials from the .csv file downloaded earlier that contains the user access key ID and secret access key with the command: `aws configure`

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ aws configure
AWS Access Key ID [****************QTZ3]: AKIAYEOMKN4PCSOQQTZ3
AWS Secret Access Key [****************2WT7]: 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
Default region name [us-east-2]: us-east-2
Default output format [None]:
```

6. After providing the credentials, execute the command:

   ```
   aws sts get-caller-identity
   ```

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ aws sts get-caller-identity
{
    "UserId": "AIDAJCAPGM74YSVPBRBSU",
    "Account": "559311122206",
    "Arn": "arn:aws:iam::559311122206:user/sergey"
}
```

7. Point AWS CLI to the desired EKS cluster for assessment using the following commands below.

```
aws eks --region <Target AWS region> describe-cluster --name <Target Cluster Name> --query cluster.status

aws eks --region <Target AWS region> update-kubeconfig --name <Target Cluster Name>

kubectl get svc
```

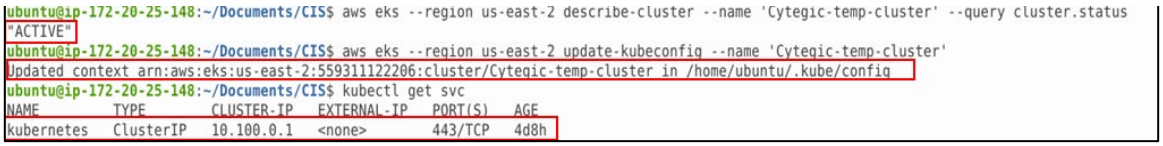
<Target AWS region> is the AWS region EKS locate (us-east-1, us-east-2, eu-central-1, etc.). Make sure to enter one region at a time.

<Target Cluster Name> is the EKS cluster name.

To locate the Clusters' name, execute the following command:

```
aws eks list-clusters
```

The output should be with similar values:



9. The Extraction Process

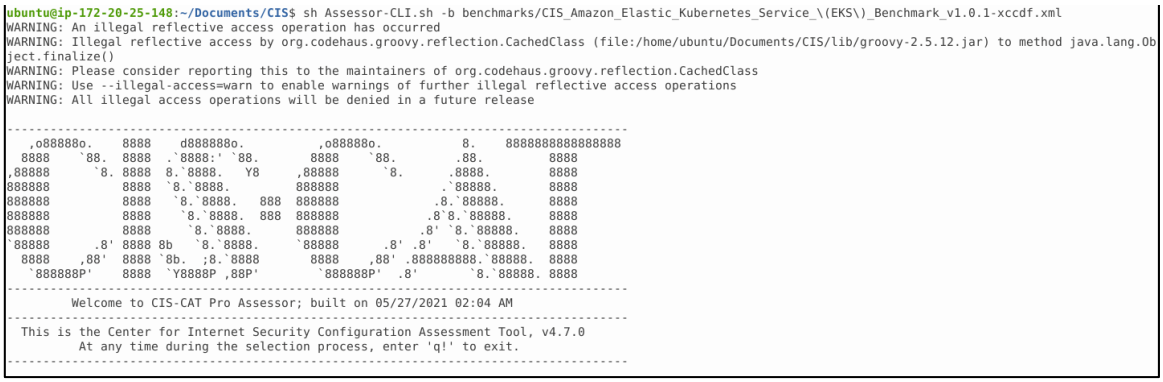
There are 2 methods for this process, the first one is a one-liner command executed to perform the analysis and the second one is via the CIS interactive dialog. Both lead to the same result differently.

Method 1 - Export the configuration using a command syntax:

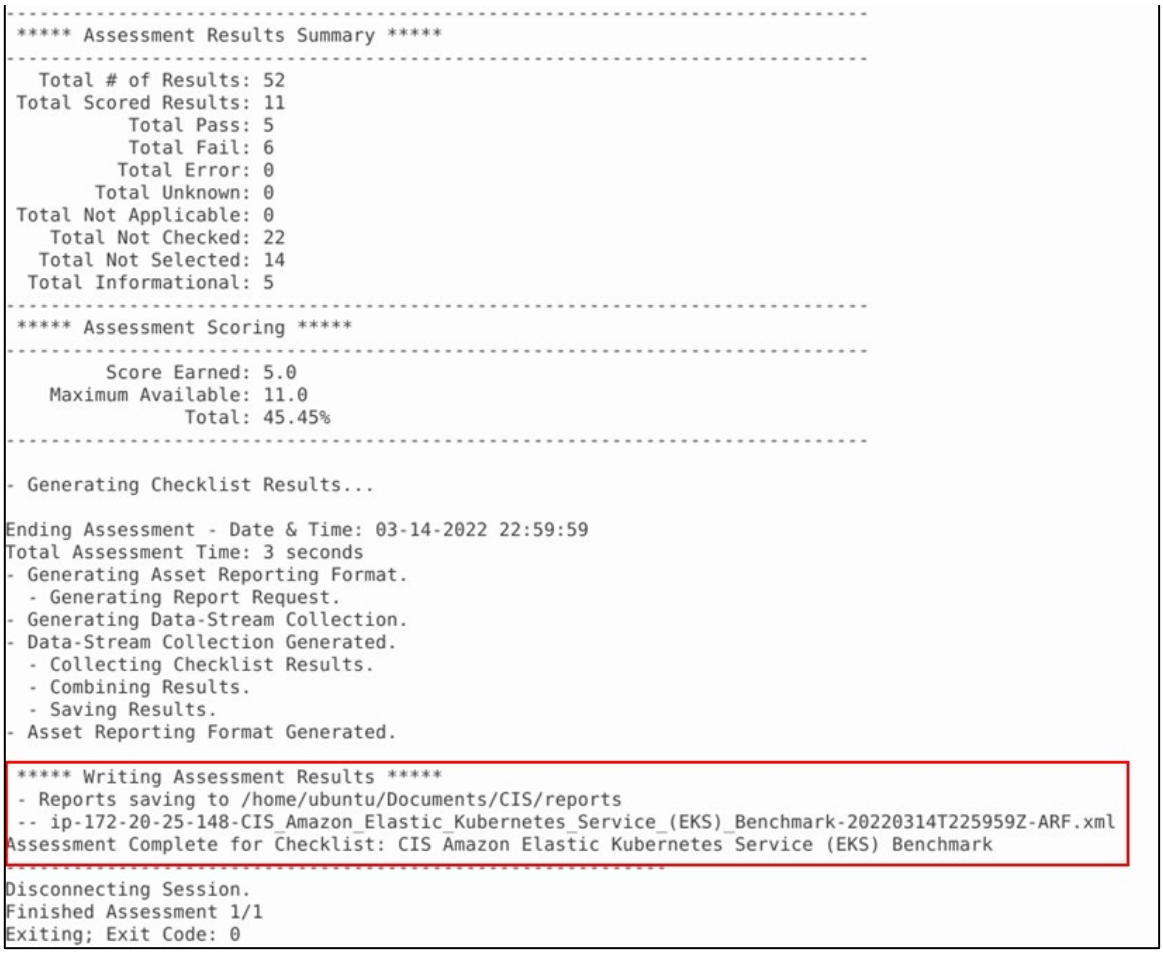
1. Navigate to the CIS folder location on the Linux machine and Execute the following command to export the configuration:

   ```
   sh Assessor-CLI.sh -b benchmarks/CIS_Amazon_Elastic_Kubernetes_Service_\(EKS\)_Benchmark_v1.0.1-xccdf.xml
   ```

   Note: The command above is an example of running a Level 1 assessment.



2. Once the Assessment is finished, locate the result file location provided under the ***Writing Assessment Results*** section.



```
--------------------------------------------------------------------------------
***** Assessment Results Summary *****
--------------------------------------------------------------------------------
  Total # of Results: 52
Total Scored Results: 11
          Total Pass: 5
          Total Fail: 6
         Total Error: 0
       Total Unknown: 0
Total Not Applicable: 0
   Total Not Checked: 22
  Total Not Selected: 14
 Total Informational: 5
--------------------------------------------------------------------------------
***** Assessment Scoring *****
--------------------------------------------------------------------------------
        Score Earned: 5.0
   Maximum Available: 11.0
               Total: 45.45%
--------------------------------------------------------------------------------

- Generating Checklist Results...

Ending Assessment - Date & Time: 03-14-2022 22:59:59
Total Assessment Time: 3 seconds
- Generating Asset Reporting Format.
  - Generating Report Request.
- Generating Data-Stream Collection.
- Data-Stream Collection Generated.
  - Collecting Checklist Results.
  - Combining Results.
  - Saving Results.
- Asset Reporting Format Generated.

***** Writing Assessment Results *****
- Reports saving to /home/ubuntu/Documents/CIS/reports
-- ip-172-20-25-148-CIS_Amazon_Elastic_Kubernetes_Service_(EKS)_Benchmark-20220314T225959Z-ARF.xml
Assessment Complete for Checklist: CIS Amazon Elastic Kubernetes Service (EKS) Benchmark
--------------------------------------------------------------
Disconnecting Session.
Finished Assessment 1/1
Exiting; Exit Code: 0
```

3. Proceed to the CyMA import part.

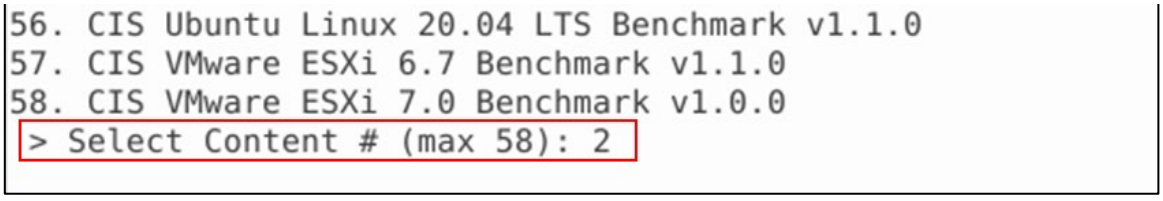
Method-2 - Export the configuration using interactive mode:

1. Execute the following command to export the configuration using interactive mode:

   ```
   sh Assessor-CLI.sh -i
   ```

2. Select the CIS Amazon Elastic Kubernetes Service (EKS) benchmark from the list.

3. Enter the benchmark number in the “Select Content” files.



4. Select the profile of "CIS Amazon Elastic Kubernetes Service (EKS) Benchmark v1.0.1". Level 1 or Level 2.

```
57. CIS VMware ESXi 6.7 Benchmark v1.1.0
58. CIS VMware ESXi 7.0 Benchmark v1.0.0
 > Select Content # (max 58): 2

Selected 'CIS Amazon Elastic Kubernetes Service (EKS) Benchmark'

Mar 14, 2022 11:14:07 PM com.sun.org.slf4j.internal.Logger warn
WARNING: The input bytes to the digest operation are null. This may be due to a problem with the Reference URI or its Transforms.
Assessment File CIS_Amazon_Elastic_Kubernetes_Service_(EKS)_Benchmark_v1.0.1-xccdf.xml has a valid Signature.
Profiles:
1. Level 1
2. Level 2
 > Select Profile # (max 2): 1

Selected Profile 'Level 1'
```

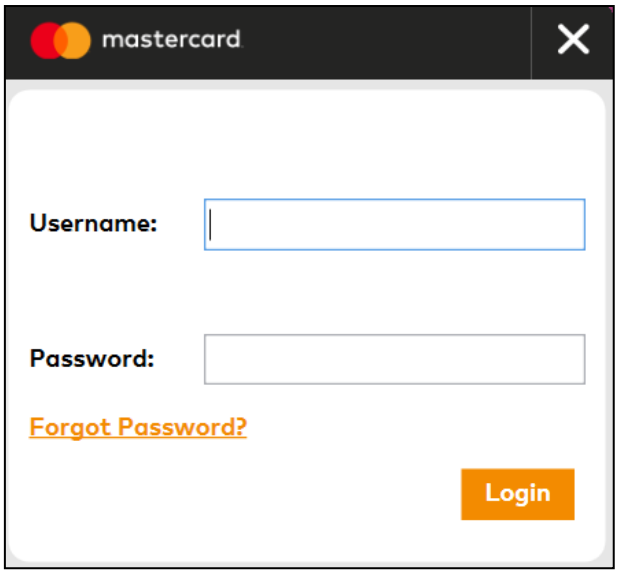
5. Once the Assessment is finished, locate the result file location provided under the ***Writing Assessment Results*** section.

```
-------------------------------------------------------------------------------
 ***** Assessment Results Summary *****
-------------------------------------------------------------------------------
   Total # of Results: 52
 Total Scored Results: 11
           Total Pass: 5
           Total Fail: 6
          Total Error: 0
        Total Unknown: 0
 Total Not Applicable: 0
    Total Not Checked: 22
   Total Not Selected: 14
  Total Informational: 5
-------------------------------------------------------------------------------
 ***** Assessment Scoring *****
-------------------------------------------------------------------------------
         Score Earned: 5.0
    Maximum Available: 11.0
                Total: 45.45%
-------------------------------------------------------------------------------

- Generating Checklist Results...

Ending Assessment - Date & Time: 03-14-2022 22:59:59
Total Assessment Time: 3 seconds
- Generating Asset Reporting Format.
  - Generating Report Request.
- Generating Data-Stream Collection.
- Data-Stream Collection Generated.
  - Collecting Checklist Results.
  - Combining Results.
  - Saving Results.
- Asset Reporting Format Generated.

 ***** Writing Assessment Results *****
 - Reports saving to /home/ubuntu/Documents/CIS/reports
 -- ip-172-20-25-148-CIS_Amazon_Elastic_Kubernetes_Service_(EKS)_Benchmark-20220314T225959Z-ARF.xml
Assessment Complete for Checklist: CIS Amazon Elastic Kubernetes Service (EKS) Benchmark
-------------------------------------------------------------
Disconnecting Session.
Finished Assessment 1/1
Exiting; Exit Code: 0
```

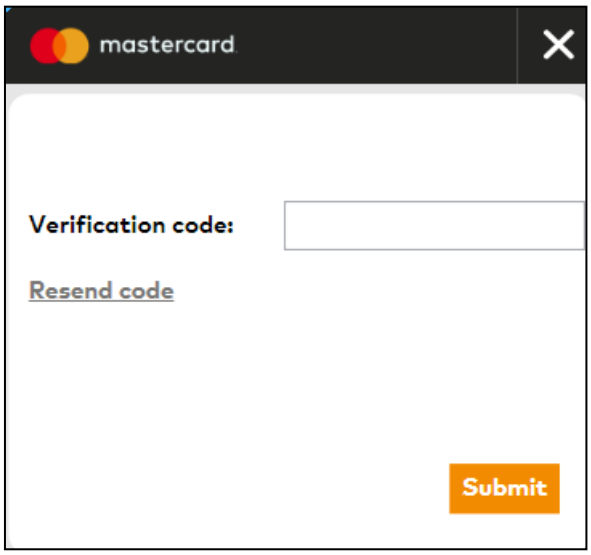
6. Proceed to the CyMA import part.

10. Open and Review Integration Results

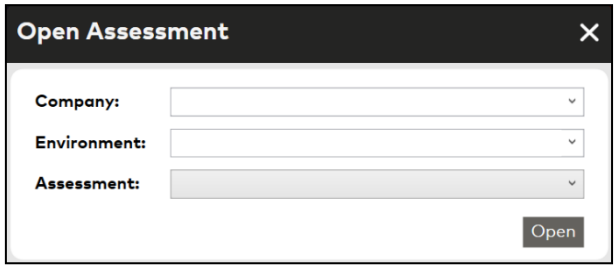
1. For instructions on how to download CyMA, please refer to the "CyMA Installation" tip sheet.
2. After Installation, execute the "Cyber Quant CyMA" client and log in.



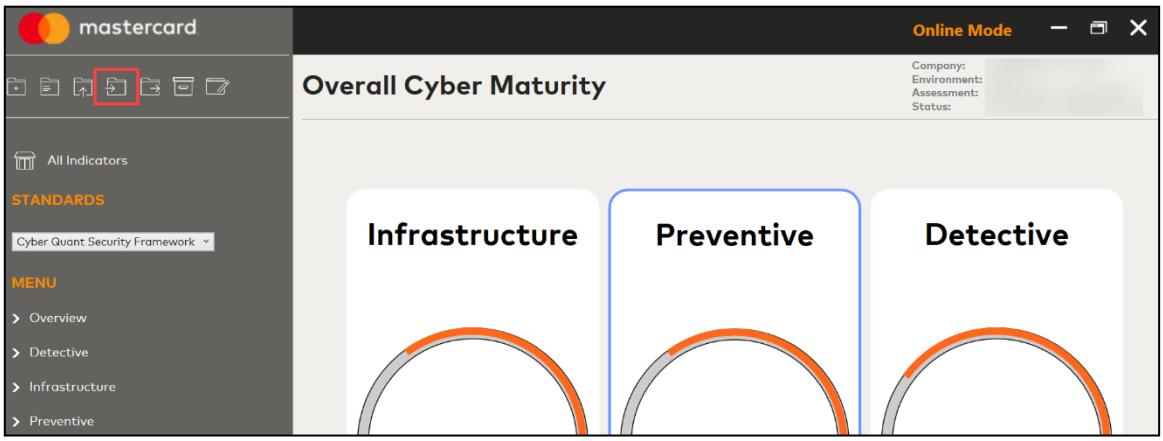
3. Enter the verification code sent to the account's email address.



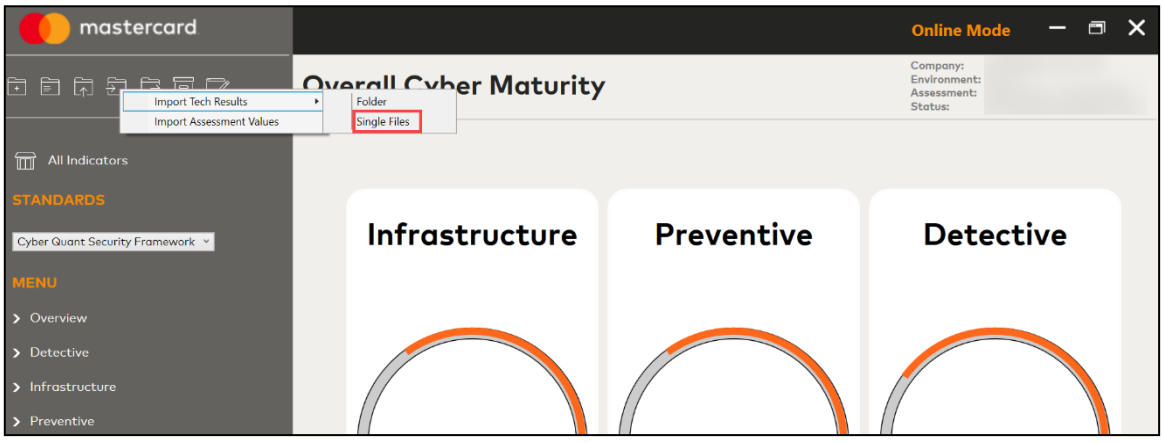
4. Select the desired company, environment, and assessment to import the report.



5. Click on the "Import Files" icon on the top left of the screen.

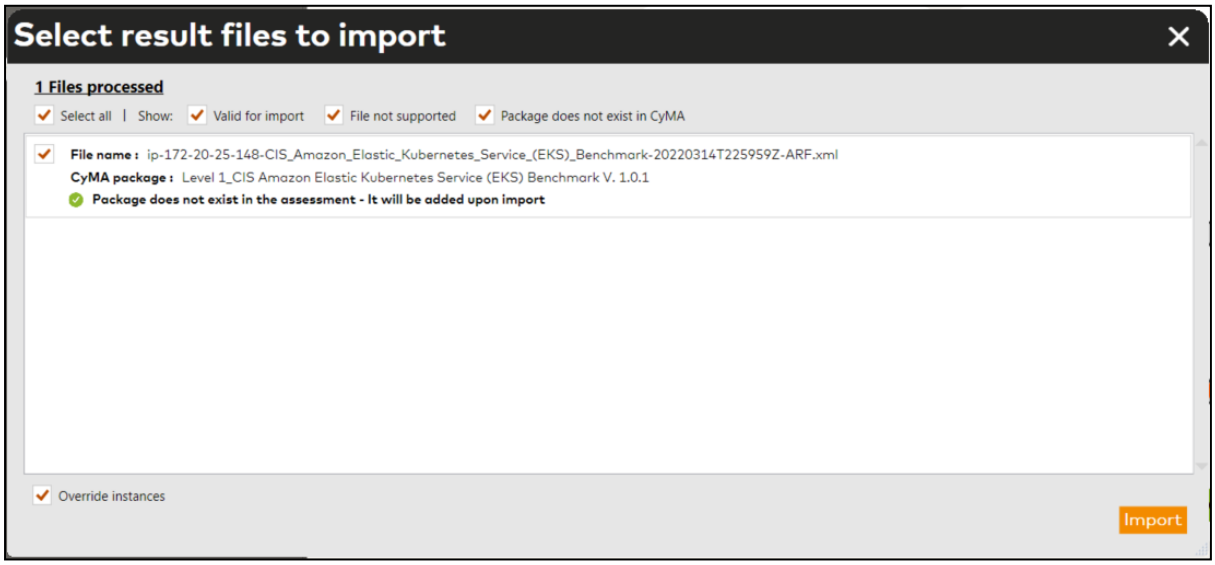


6. Hover over "Import Tech Results", click "Choose Single File".

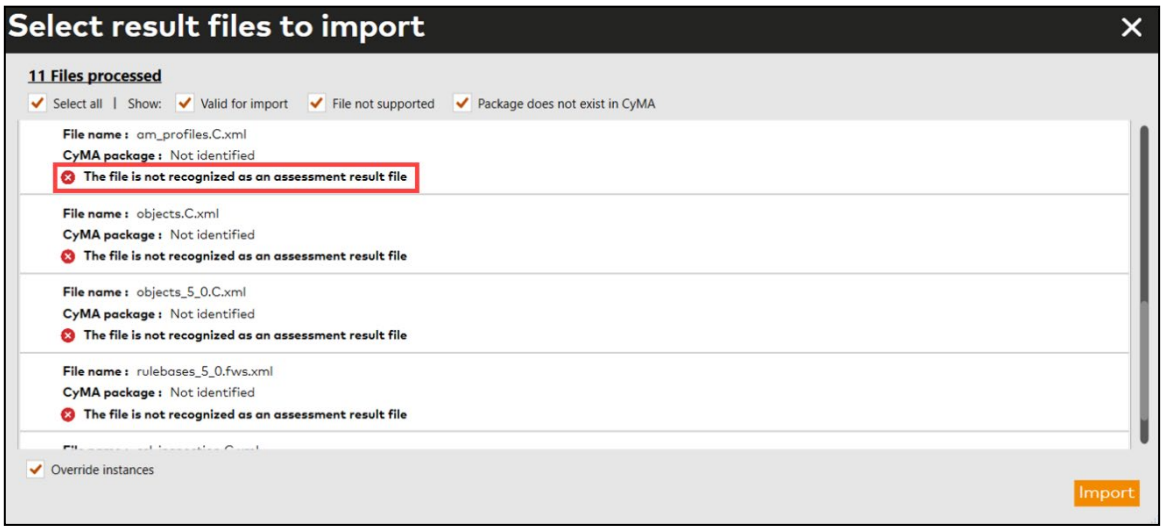


7. Browse to the dedicated folder where the configuration files are stored.

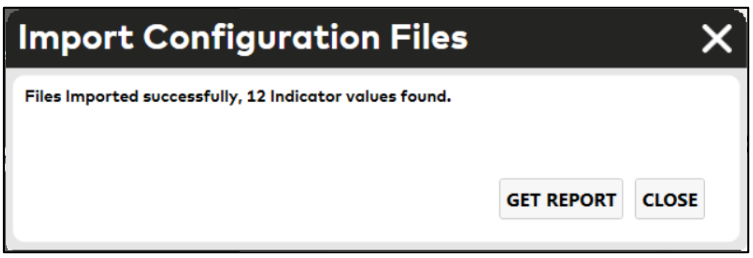
8. Once the report is open, select the file and click "Import". The following screen displays information regarding import errors and packages associated with the imported files.



A red mark is displayed below the package in case of an error.



9. Upon successful import, a confirmation notice is displayed, click "CLOSE". **Please note that the number of indicators may vary based on the input configuration files**.



10. The assessment results are now available for review.