



# 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 attach it to the new user.

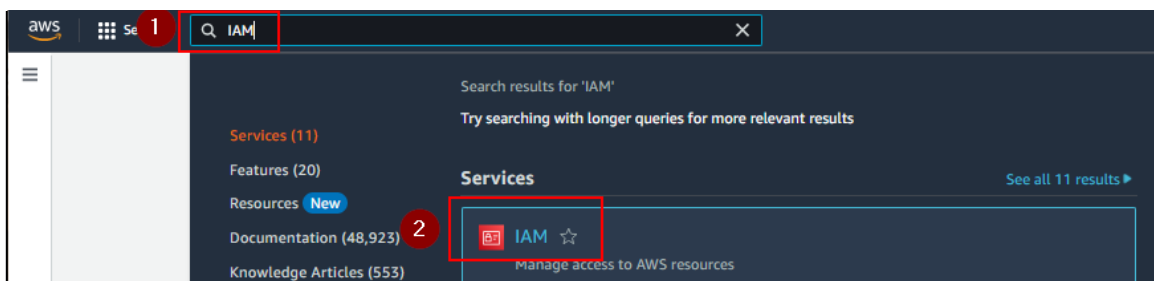
Connect the AWS CLI to the appropriate AWS EKS region and cluster to extract the information from.

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

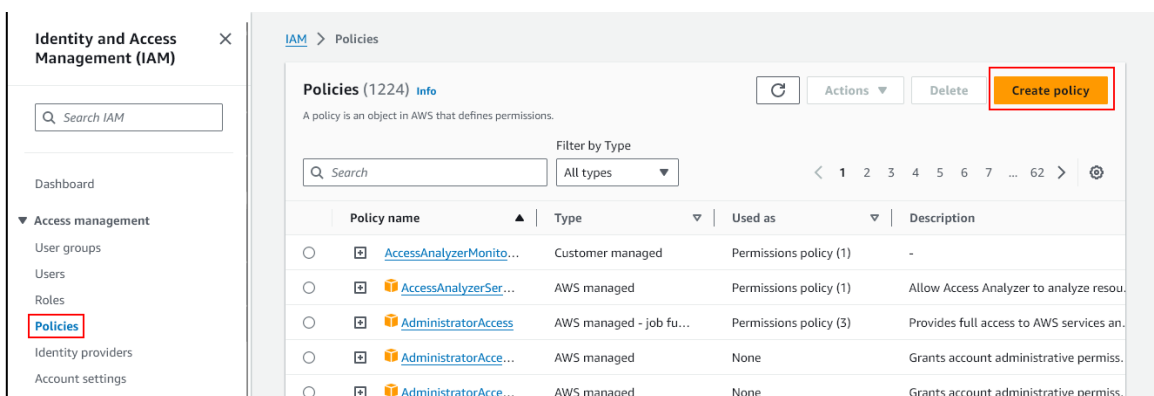


## 6. AWS - Creating Dedicated User & Policy

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.

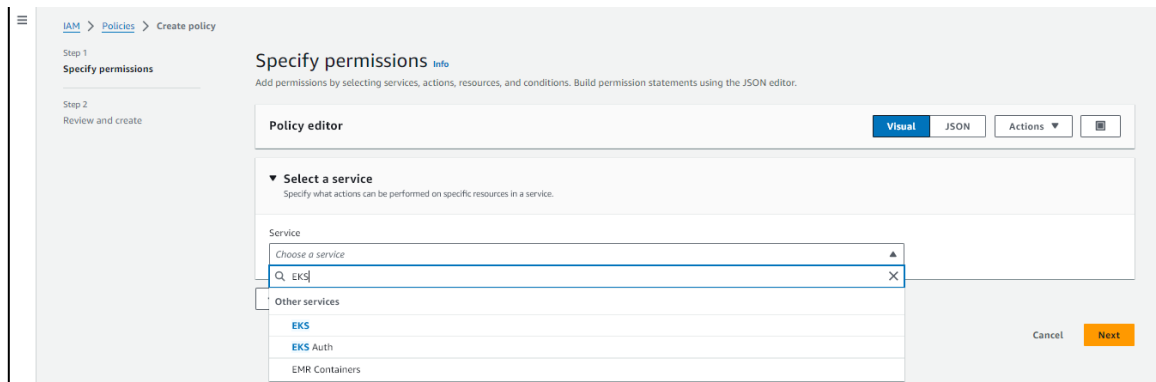


3. In the menu on the left, under the "Access management" section, click on "Policies" and then on "Create Policy".

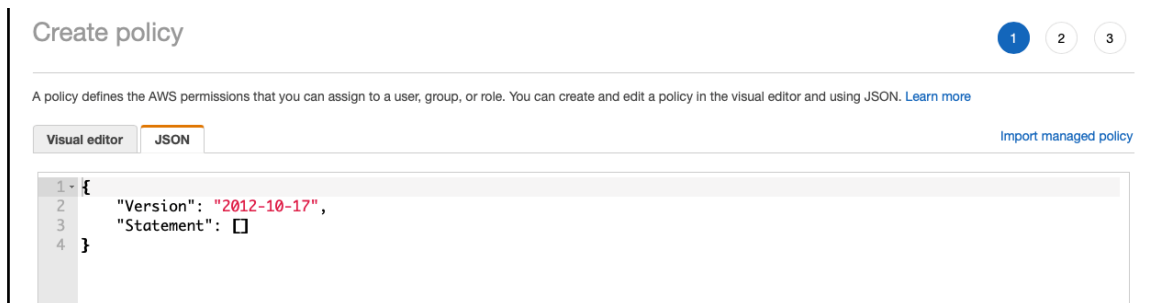




4. Select EKS Service in the Visual editor.



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": "*"
    }
  ]
}
```



- Paste the example text inside the JSON editor and click on "Next: Tags" until you get to the 'Review policy' page.

The screenshot shows the 'Create policy' interface in the AWS IAM console. The 'JSON' tab is selected, and the following JSON is pasted into the editor:

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "VisualEditor0",
6-       "Effect": "Allow",
7-       "Action": [
8-         "eks:ListNodegroups",
9-         "eks:DescribeFargateProfile",
10-        "eks:ListTagsForResource",
11-        "eks:ListAddons",
12-        "eks:DescribeAddon",
13-        "eks:ListFargateProfiles",
14-        "eks:DescribeNodegroup",
15-        "eks:DescribeIdentityProviderConfig",
16-        "eks:ListUpdates",
17-        "eks:DescribeUpdate",
18-        "eks:AccessKubernetesApi",
19-        "eks:DescribeCluster",
20-        "eks:ListIdentityProviderConfigs"
21-      ],
22-      "Resource": "arn:aws:eks:*:[Owner ID]:cluster/*"
23-    },
24-    {
25-      "Sid": "VisualEditor1",
26-      "Effect": "Allow",
27-      "Action": [
28-        "eks:ListClusters",
29-        "eks:DescribeAddonVersions"
30-      ],
31-      "Resource": "*"
32-    }
33-  ]
34- }
```

At the bottom of the editor, there is a status bar showing 'Security: 0', 'Errors: 1', 'Warnings: 0', and 'Suggestions: 0'. Below the editor, the 'Character count: 573 of 6,144.' is displayed. The 'Next: Tags' button is highlighted in blue.



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

Create policy 1 2 3

Review policy

Name\*   
Use alphanumeric and '+', '@', '-' characters. Maximum 128 characters.

Description   
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Summary 

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose [Show remaining](#). [Learn more](#)

Service	Access level	Resource	Request condition
Allow (1 of 317 services) <a href="#">Show remaining 316</a>			
EKS	Full: List Limited: Read	Multiple	None

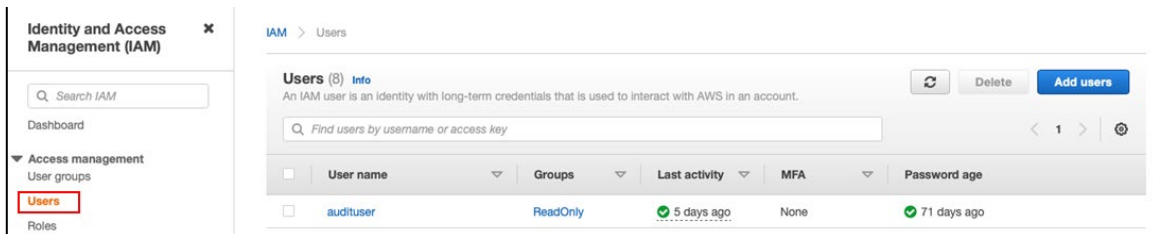
Tags 

Key	Value
No tags associated with the resource.	

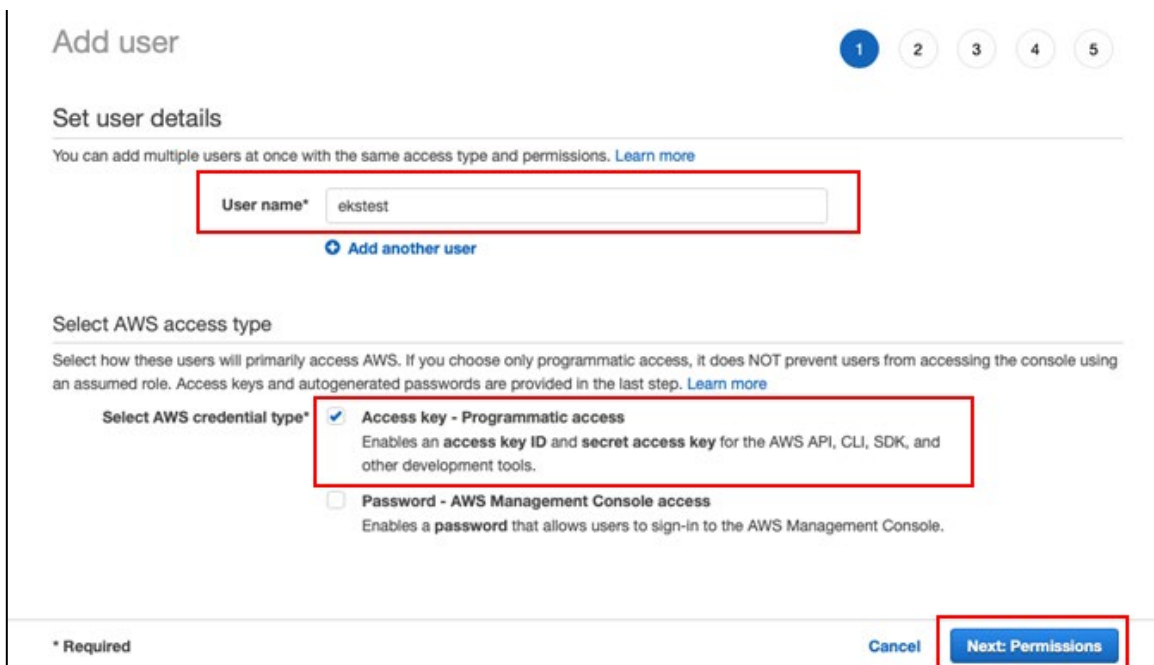
\* Required Cancel Previous Create policy



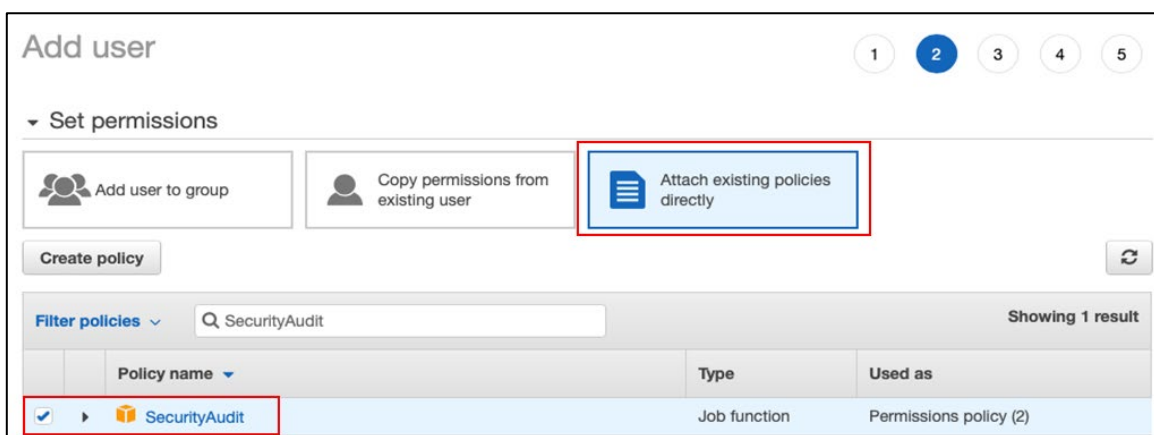
10. In the IAM management panel, select the “Users section” and click on “Add users”.



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".

Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

Create user without a permissions boundary  
 Use a permissions boundary to control the maximum user permissions

Select policy to set the permissions boundary

Create policy ↻

Filter policies  Showing 1 result

Policy name	Type	Used as
<input checked="" type="radio"/> EKS_RO	Customer managed	None

Cancel Previous **Next: Tags**

14. Click on "Next: Review".

Add user 1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

You can add 50 more tags.

Cancel Previous **Next: Review**



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

**Add user** 1 2 3 4 5

### Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

#### User details

User name	ekstest
AWS access type	Programmatic access - with an access key
Permissions boundary	<a href="#">EKS_RO</a>

#### Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	<a href="#">SecurityAudit</a>

#### Tags

No tags were added.

[Cancel](#) [Previous](#) [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".

**Add user** 1 2 3 4 5

**Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://cytegitic.signin.aws.amazon.com/console>

[Download .csv](#)

User	Access key ID	Secret access key
<a href="#">ekstest</a>	AKIAYEOMKN4PNLOJWKS3	..... <a href="#">Show</a>

[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 "kubectl" 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]: AKIAYEOMKN4PCS0QQTZ3  
AWS Secret Access Key [*****2WT7]: zvcieL3fdRV2cNC2AUyMz0+F0BHyMpFRH0Ep2WT7  
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:

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ aws eks --region us-east-2 describe-cluster --name 'Cyteqic-temp-cluster' --query cluster.status  
"ACTIVE"  
ubuntu@ip-172-20-25-148:~/Documents/CIS$ aws eks --region us-east-2 update-kubeconfig --name 'Cyteqic-temp-cluster'  
Updated context arn:aws:eks:us-east-2:559311122206:cluster/Cyteqic-temp-cluster in /home/ubuntu/.kube/config  
ubuntu@ip-172-20-25-148:~/Documents/CIS$ kubectl get svc  
NAME          TYPE          CLUSTER-IP    EXTERNAL-IP    PORT(S)    AGE  
kubernetes    ClusterIP     10.100.0.1    <none>         443/TCP    4d8h
```



## 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_\(EKS\) _Bench  
mark_v1.0.1-xccdf.xml
```

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

```
ubuntu@ip-172-20-25-148:~/Documents/CIS$ sh Assessor-CLI.sh -b benchmarks/CIS_Amazon_Elastic_Kubernetes_Service_\(EKS\) _Benchmark_v1.0.1-xccdf.xml  
WARNING: An illegal reflective access operation has occurred  
WARNING: Illegal reflective access by org.codehaus.groovy.reflection.CachedClass (file:/home/ubuntu/Documents/CIS/lib/groovy-2.5.12.jar) to method java.lang.Object.finalize()  
WARNING: Please consider reporting this to the maintainers of org.codehaus.groovy.reflection.CachedClass  
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations  
WARNING: All illegal access operations will be denied in a future release  
-----  
.,o88888o. 8888 88888888o. ,o88888o. 8. 888888888888888888  
8888 `88. 8888 `8888:' `88. 8888 `88. `88. 8888  
,88888 `8. 8888 8.`8888. Y8 888888 `8. `88888. 8888  
8888888 8888 `8.`8888. 888 888888 888888. 888888. 8888  
8888888 8888 `8.`8888. 888 888888 `8.`888888. 8888  
8888888 8888 `8.`8888. 8888888 `8.`8.`888888. 8888  
8888888 `8' 8888 8b `8.`8888. `88888 `8' `8' `8.`88888. 8888  
8888 `88' 8888 `8b.;8.`8888 8888 `88' `8888888888.`88888. 8888  
`888888P' 8888 `Y8888P`88P' `888888P' `8' `8.`88888. 8888  
-----  
Welcome to CIS-CAT Pro Assessor; built on 05/27/2021 02:04 AM  
-----  
This is the Center for Internet Security Configuration Assessment Tool, v4.7.0  
At any time during the selection process, enter 'q!' to exit.  
-----
```



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
```





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.

mastercard

Username:

Password:

[Forgot Password?](#)

Login

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

mastercard

Verification code:

[Resend code](#)

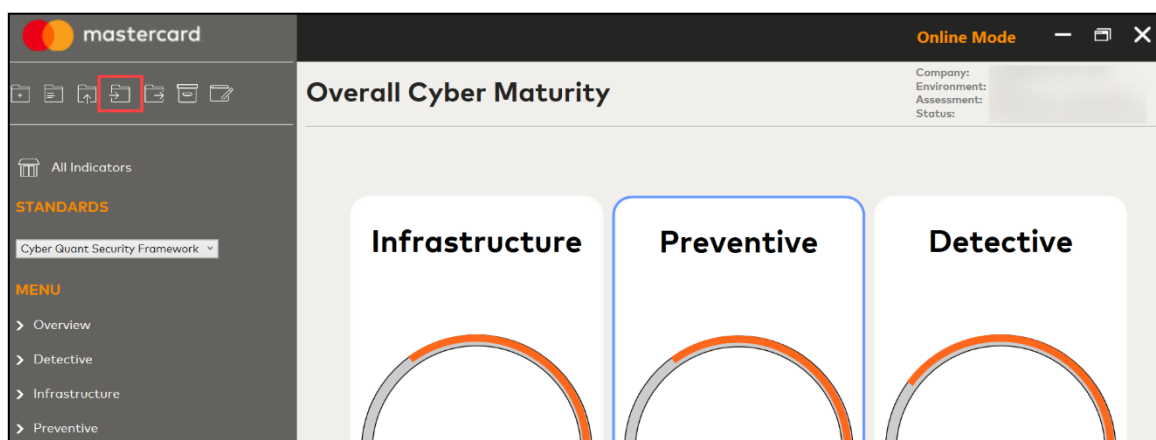
Submit



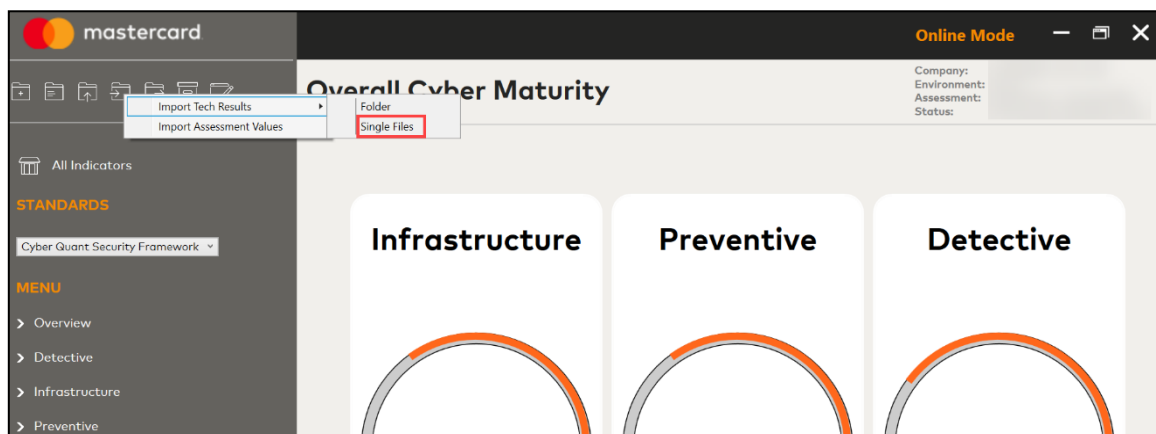
4. Select the desired company, environment, and assessment to import the report.

The image shows a dialog box titled "Open Assessment" with a close button (X) in the top right corner. It contains three dropdown menus labeled "Company:", "Environment:", and "Assessment:". Below the dropdowns is an "Open" button.

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



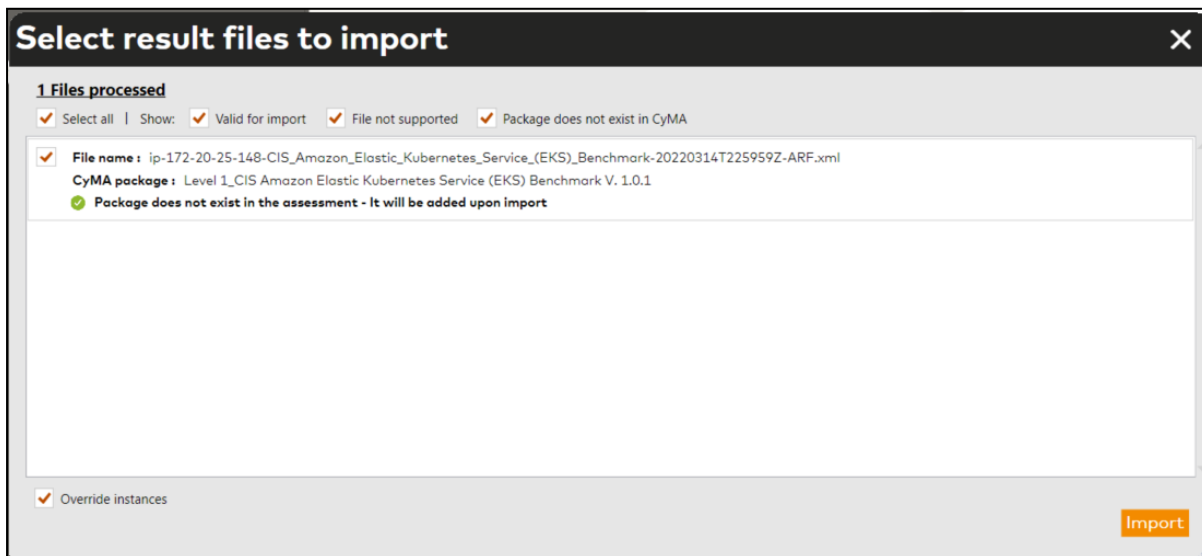
6. Hover over "Import Tech Results", click "Choose Single File".



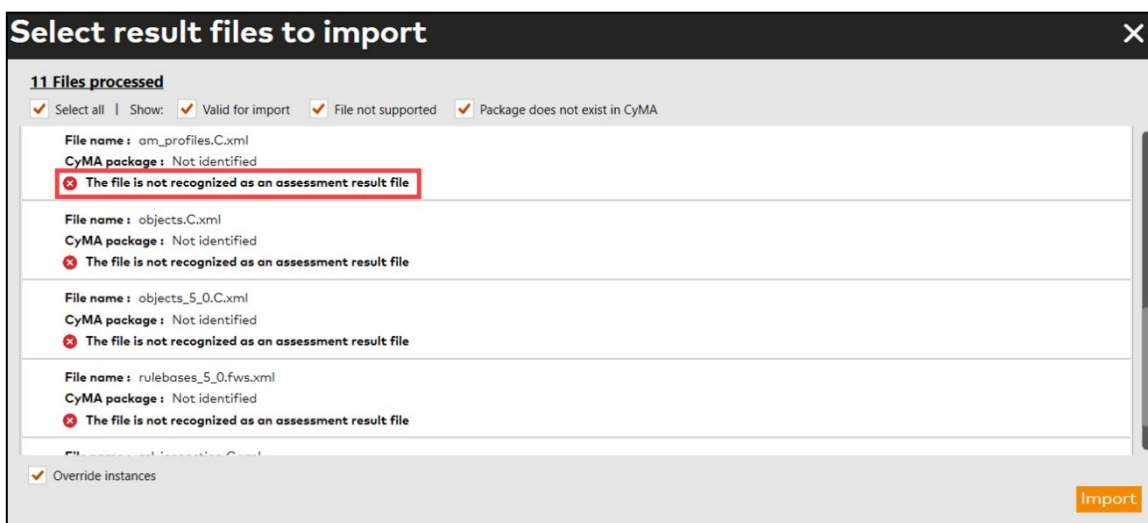
7. Browse to the dedicated folder where the configuration files are stored.



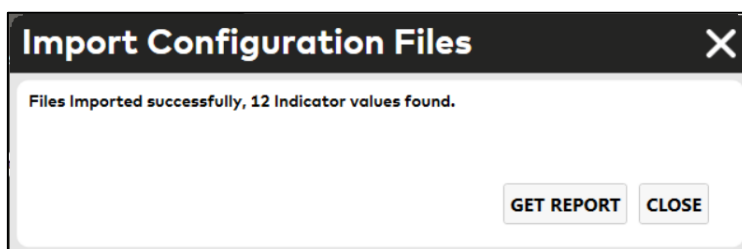
- Once the report is open, select the file and click "Import". The following screen displays information regarding import errors and packages associated with the imported files.



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



- 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.

The screenshot displays the 'Indicators' section of the CIS Assessor tool. The interface includes a sidebar on the left with 'STANDARDS' and 'MENU' sections. The main area shows a table of indicators with the following columns: NAME, DESCRIPTION, RELEVANT, INSTANCES, OVERRIDE VALUE, SCORE, and SOURCE. The table lists five indicators related to audit logs and kubelet configurations, all of which are marked as 'RELEVANT' and 'YES'.

NAME	DESCRIPTION	RELEVANT	INSTANCES	OVERRIDE VALUE	SCORE	OVERRIDE SCORE	SOURCE	UNIT
Enable audit Logs	The audit logs are part of the EKS managed Kubernetes control plane logs that are managed by Amazon EKS. Ama...	NO YES	1				Level 1_CIS Amazon Elastic Kubernetes Service (EKS) Benchmark V. 1.0.1	Av
	[Expand]							
Ensure that the kubeconfig f...	If kubelet is running, and if it is using a file-based kubeconfig file, ensure that the proxy kube...	NO YES	1				Level 1_CIS Amazon Elastic Kubernetes Service (EKS) Benchmark V. 1.0.1	Av
	[Expand]							
Ensure that the kubelet kubec...	If kubelet is running, ensure that the file ownership of its kubeconfig file is set to rootroot. The ku...	NO YES	1				Level 1_CIS Amazon Elastic Kubernetes Service (EKS) Benchmark V. 1.0.1	Av
	[Expand]							
Ensure that the kubelet conf...	Ensure that if the kubelet refers to a configuration file with the --config argument, that file has permiss...	NO YES	1				Level 1_CIS Amazon Elastic Kubernetes Service (EKS) Benchmark V. 1.0.1	Av
	[Expand]							
Ensure that the kubelet confi...	Ensure that if the kubelet refers to a configuration file with the --config argument, that file is own...	NO YES	1				Level 1_CIS Amazon Elastic Kubernetes Service (EKS) Benchmark V. 1.0.1	Av