

# Securaa Cyber Security Asset Management (CSAM) Administration Guide

Contact Information  
[support@securaai.io](mailto:support@securaai.io)

**Copyright@Bytamorph Zona Pvt Ltd**  
668/A,9th Cross, 1st Stage Vijay Eswari, Vijaya Nagar, Mysore KA 570017 IN  
**Last Revised: 28 January 2025**

## Table Of Contents

<b>Securaa CSAM Platform Overview.....</b>	<b>2</b>
<b>Installation Process.....</b>	<b>3</b>
Prerequisites for Deployment.....	3
Operating system requirements.....	4
Hardware Requirements.....	4
Network Connectivity Requirements.....	5
<b>Securaa CSAM Installation.....</b>	<b>6</b>
<b>Post Installation Configuration.....</b>	<b>8</b>
Business Hierarchy.....	10
<b>Inventory.....</b>	<b>10</b>
Inventory Browser Screen.....	10
Query filter.....	12
Export Assets.....	14
Import Assets.....	15
<b>Asset Overview.....</b>	<b>18</b>
<b>Asset Report.....</b>	<b>19</b>
<b>CSAM Node Dashboard.....</b>	<b>22</b>
<b>CSAM Automation Tasks.....</b>	<b>27</b>



## Securaa CSAM Platform Overview

Securaa CSAM (Cyber Security Asset Management) provides comprehensive visibility and management of your security assets at your finger CSAMs. It delivers a fully automated solution for asset discovery, classification, monitoring, and risk analysis across your entire digital environment. CSAM enables seamless data collection, intelligent asset processing, and enriched insights into security vulnerabilities and compliance gaps. It disseminates actionable information to stakeholders, empowering them to prioritize vulnerabilities effectively. With a user-friendly interface and advanced visualization tools, including a dynamic asset relationship graph, users can effortlessly categorize assets by risk level and initiate actions to remediate vulnerabilities, ensuring enhanced security and compliance posture.

The main features of Securaa CSAM are

- Fetching assets from cloud environments and on-premises infrastructure.
- Fetching vulnerabilities from Nessus.
- Fetching vulnerability details from the NVD (National Vulnerability Database).
- Setting business hierarchy content, tags, and comments for each asset.
- Exporting and importing assets.
- Fetching assets at three levels in the CSAM inventory: cloud level, service level, and asset level.
- Filtering data through query filters at all three levels.
- Exporting assets using filtered queries, ensuring only the filtered assets are exported.
- Generating reports for each asset.
- Providing drill-down views for detailed vulnerability and alert information for

each asset.

- Displaying a dashboard with comprehensive details of all assets.
- Offering a drill-down feature from dashboard details that redirects to the CSAM inventory.
- Including widgets for vulnerability breakdown, unscanned machines, coverage by tools, and high-risk assets categorized by business hierarchy.
- Providing drill-down views for the vulnerability breakdown and coverage by tools widgets.

## Installation Process

### Prerequisites for Deployment

Securaa CSAM needs the following for a successful deployment

- Connectivity to Securaa servers is required to download the latest software versions and Docker images. After establishing the connection, the application must be configured in the Application tab within the CSAM application. This configuration enables data fetching from cloud platforms, including AWS, Azure, and GCP, as well as on-premises infrastructure tools such as Nessus, QRadar, and Symantec.
- Port 8229 should be open in the CSAM machine to establish connectivity with SOAR.
- Administrative privileges on the operations system platform.
- SSH Connectivity tools like Putty to connect with Securaa CSAM machine.

- Browser software like Chrome to access the Securaa web interface.

## Operating system requirements

Securaa CSAM can be deployed on the following operating systems and must meet the minimum hardware requirements.

Operating System	Supported Version
RHEL	9.x, 8.x
Rocky Linux	8.x
Alma Linux	8.x
Centos	9.x

## Hardware Requirements

### MSSP POC (Proof of concept)

COMPONENT	Specification
CPU	4 CPU
Memory	16 GB RAM
Storage	300 GB SSD [ ~ 20 Million Records ]

## MSSP (PRODUCTION)

COMPONENT	Specification
CPU	8 CPU
Memory	32 GB RAM
Storage	500 GB SSD [ ~ 30 Million Records ]

**Note:** More storage needs to be added if records exceed 30 million.

### Network Connectivity Requirements

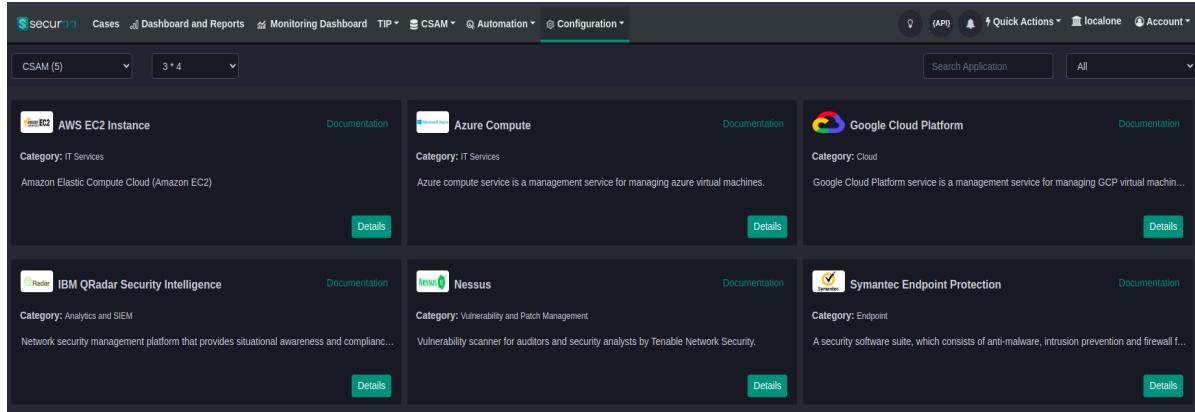
The following URLs need to be whitelisted before installation. Securaa downloads the latest software version, docker images, and other dependencies from these URLs:

- <https://s3.us-east-2.amazonaws.com/>
- <https://665853670667.dkr.ecr.us-east-2.amazonaws.com/>
- <https://release.securaa.io:9002>
- <https://repo.securaa.io/>

Application configuration that fetches data from cloud and on-premises environments:

- Onprem :
  - IBM QRadar Security Intelligence
  - Nessus
  - Symantec Endpoint Protection
- Clouds:

- AWS EC2 Instance.
- Azure Compute.
- Google Cloud platform.



The screenshot shows the Securaa CSAM interface with a dark theme. At the top, there's a navigation bar with links like 'Cases', 'Dashboard and Reports', 'Monitoring Dashboard', 'TIP', 'CSAM', 'Automation', 'Configuration' (which is highlighted), and 'Account'. Below the navigation is a search bar and a dropdown menu. The main area displays six cards representing different services:

- AWS EC2 Instance**: Category: IT Services. Description: Amazon Elastic Compute Cloud (Amazon EC2). Buttons: Documentation, Details.
- Azure Compute**: Category: IT Services. Description: Azure compute service is a management service for managing azure virtual machines. Buttons: Documentation, Details.
- Google Cloud Platform**: Category: Cloud. Description: Google Cloud Platform service is a management service for managing GCP virtual machin... Buttons: Documentation, Details.
- IBM QRadar Security Intelligence**: Category: Analytics and SIEM. Description: Network security management platform that provides situational awareness and complianc... Buttons: Documentation, Details.
- Nessus**: Category: Vulnerability and Patch Management. Description: Vulnerability scanner for auditors and security analysts by Tenable Network Security. Buttons: Documentation, Details.
- Symantec Endpoint Protection**: Category: Endpoint. Description: A security software suite, which consists of anti-malware, intrusion prevention and firewall f... Buttons: Documentation, Details.

## Securaa CSAM Installation

The below steps can be used to set up Securaa CSAM on a single virtual machine:

1. Take server SSH access and download the installer with the help of a URL shared by the Securaa team.

- Redhat

```
PS C:\Users\sbhos\Desktop> ssh -i '..\securaamasterkey (1).pem' ec2-user@3.22.164.217
The authenticity of host '3.22.164.217 (3.22.164.217)' can't be established.
ED25519 key fingerprint is SHA256:E6NQQT+3X+QUym+0Fh/iUFY0yy8oxcu2V+nZ/UjTxqvk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.22.164.217' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: rhc connect
```

- Ubuntu

```
PS C:\Users\sbhos\Desktop> ssh -i '..\securaamasterkey (1).pem' ubuntu@3.141.10.202
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1036-aws x86_64)
```

2. Below mentioned command can be used to run the RPM for the CSAM installation. Refer to Snap for more details.

**COMMAND:** wget RPM link

```
rpm -ivh RPM_NAME --nodeps --force
```

- Redhat

```
[ec2-user@ip-172-31-22-105 ~]$ sudo wget https://repo.securaa.io/installer/securaa_csam-6.0.0-1.x86_64.rpm
--2025-01-28 04:42:51-- https://repo.securaa.io/installer/securaa_csam-6.0.0-1.x86_64.rpm
Resolving repo.securaa.io (repo.securaa.io)... 18.223.129.72
Connecting to repo.securaa.io (repo.securaa.io)|18.223.129.72|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9733782 (9.3M) [application/x-redhat-package-manager]
Saving to: 'securaa_csam-6.0.0-1.x86_64.rpm'

securaa_csam-6.0.0-1.x86_64.rpm      100%[=====] 9.28M  --.-KB/s   in 0.09s
2025-01-28 04:42:51 (105 MB/s) - 'securaa_csam-6.0.0-1.x86_64.rpm' saved [9733782/9733782]
```

- Ubuntu

```
root@ip-172-31-17-164:/home/ubuntu# echo "sslVerify=False" >> /etc/yum.conf
root@ip-172-31-17-164:/home/ubuntu# wget https://repo.securaa.io/installer/install_csam_pkgs_debian-1.sh
--2025-01-28 05:49:33-- https://repo.securaa.io/installer/install_csam_pkgs_debian-1.sh
Resolving repo.securaa.io (repo.securaa.io)... 18.223.129.72
Connecting to repo.securaa.io (repo.securaa.io)|18.223.129.72|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2160 (2.1K) [application/octet-stream]
Saving to: 'install_csam_pkgs_debian-1.sh'

install_csam_pkgs_debian-1.sh      100%[=====] 2.11K  --.-KB/s   in 0s
2025-01-28 05:49:33 (500 MB/s) - 'install_csam_pkgs_debian-1.sh' saved [2160/2160]
```

```
root@ip-172-31-17-164:/home/ubuntu# wget https://repo.securaa.io/installer/securaa_csam-6.0.0-1.deb
--2025-01-28 05:56:18-- https://repo.securaa.io/installer/securaa_csam-6.0.0-1.deb
Resolving repo.securaa.io (repo.securaa.io)... 18.223.129.72
Connecting to repo.securaa.io (repo.securaa.io)|18.223.129.72|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10583116 (10M) [application/octet-stream]
Saving to: 'securaa_csam-6.0.0-1.deb'

securaa_csam-6.0.0-1.deb      100%[=====] 10.09M  --.-KB/s   in 0.1s
2025-01-28 05:56:18 (102 MB/s) - 'securaa_csam-6.0.0-1.deb' saved [10583116/10583116]
```

3. The installation will start.

- Redhat

```
[ec2-user@ip-172-31-22-105 ~]$ sudo rpm -ivh securaa_csam-6.0.0-1.x86_64.rpm --nodeps --force
Verifying...                                              #####[100%]
Preparing...                                               #####[100%]
Updating / installing...
  1:securaa_csam-6.0.0-1                                #####[100%]
Begin Installation !!
Installing zip and unzip for software unpackage...
package installed.
Installing wget package...
package installed.
Installing firewall...
Package installed.
Installing whois...
Package installed.
Installing docker ..
Installed docker.
All packages downloaded and installed successfully.
Log files created. : Successfully Executed. ✓
Log files created. : Successfully Executed. ✓
===== CSAM: ===== ✓
CSAM:[0]: : Successfully Executed. ✓
```

- Ubuntu

```
root@ip-172-31-17-164:/home/ubuntu# sudo dpkg -i securaa_csam-6.0.0-1.deb
Selecting previously unselected package securainstaller.
(Reading database ... 85193 files and directories currently installed.)
Preparing to unpack securaa_csam-6.0.0-1.deb ...
Unpacking securainstaller (6.0.0-1) ...
Setting up securainstaller (6.0.0-1) ...
  Log files created. : Successfully Executed. ✓
  Log files created. : Successfully Executed. ✓
===== CSAM: ===== ✓
CSAM:[0]: : Successfully Executed. ✓
```

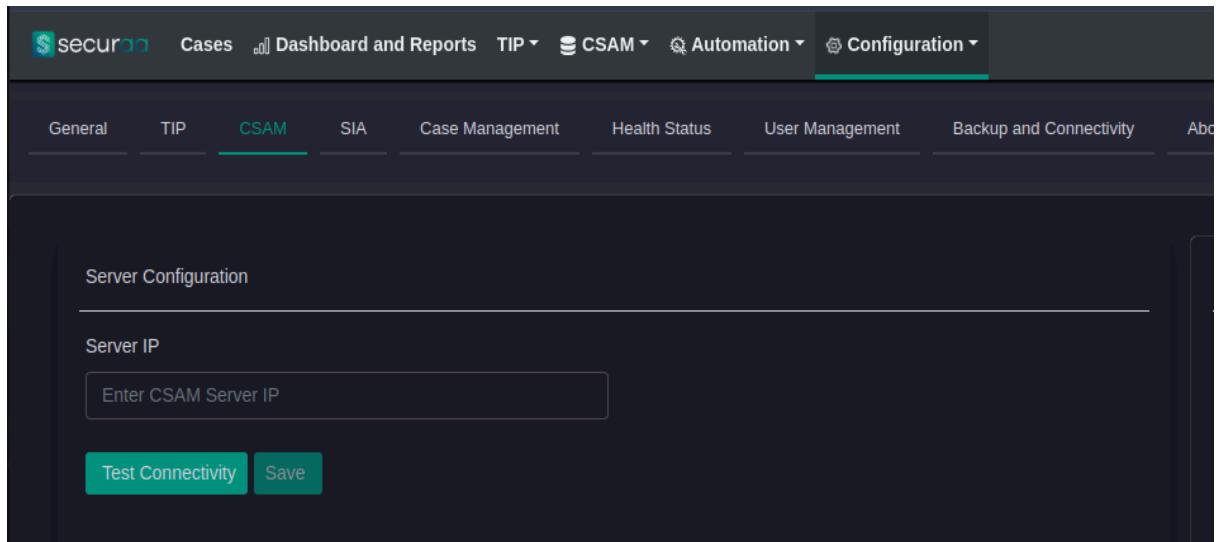
#### 4. After installation, Reboot the server.

```
SECURAA CSAM is Installed, Please Reboot the Machine ✓
vm.max_map_count = 462144
Created symlink /etc/systemd/system/default.target.wants/csam_manager.service → /etc/systemd/system/csam_manager.service.
[ec2-user@ip-172-31-22-105 ~]$ sudo reboot
```

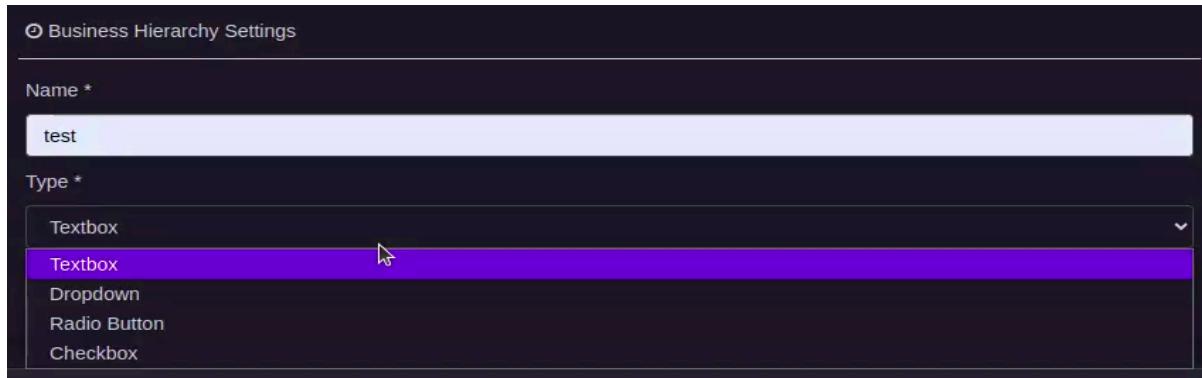
## Post Installation Configuration

NOTE: Please configure the following settings before you start using CSAM from securaa soar portal.

1. Login to Securaa Portal.
2. Connect Securaa SOAR platform to CSAM machine by providing a private CSAM server IP address in Configuration→ Platform→ CSAM→ CSAM Server Configuration.



3. Test connectivity after entering the IP address and click on save once connectivity is successful.
4. On successful connectivity, the User will be able to configure the following:-
  - Add the Business Hierarchy with type as radio button, Dropdown, Checkbox, and textbox as shown in the snapshot



## Business Hierarchy

The Business Hierarchy is a structured framework for organizing and classifying assets based on key attributes such as location, department, criticality, and ownership. By providing context to assets, this hierarchy simplifies tracking, management, and optimization. Aligning assets with the organization's structure enhances visibility, ensures compliance and supports more informed decision-making, ultimately improving operational efficiency and resource utilization.

## Inventory

### Inventory Browser Screen

Analysts can navigate from the CSAM menu to the **Inventory Browser** screen. The Inventory Browser lists all assets retrieved from the configured applications. The asset data is organized into three levels:

- **Level One:** Inventory
- **Level Two:** Services
- **Level Three:** Asset list



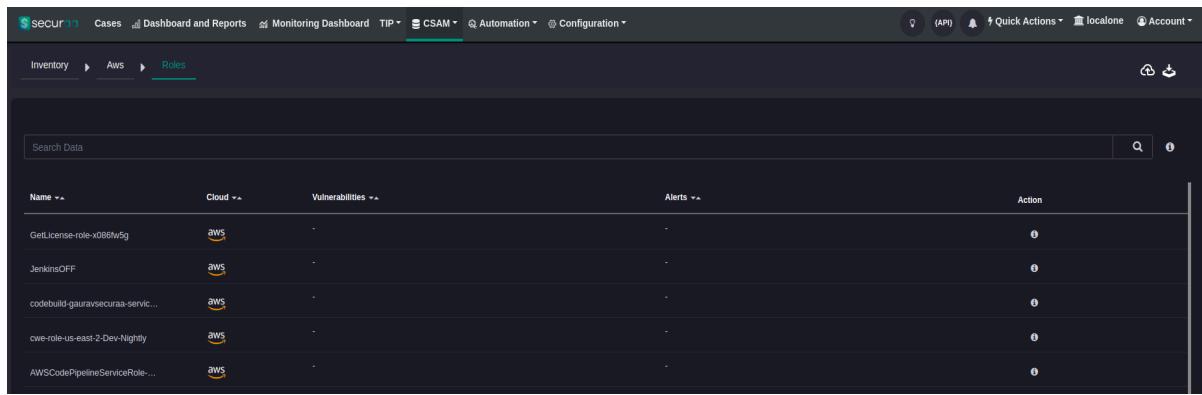
The **Inventory** page lists all cloud platforms retrieved from the configured applications. This page serves as the first level of the asset hierarchy, allowing users to view and select specific cloud types.

Type	Total	Data as of	Vulnerabilities	Alerts	Action
aws AWS	1076	20-01-2025 07:07:51 PM	C 0 H 3 M 17 L 0 U 187	C 0 H 3 M 0 L 0 U 3	
GCP	387	26-11-2024 03:29:49 PM	C 0 H 0 M 0 L 0 U 0	C 0 H 0 M 0 L 0 U 0	
OTHERS	2	21-01-2025 10:32:22 AM	C 0 H 0 M 0 L 0 U 0	C 0 H 0 M 0 L 0 U 0	
AZURE	1	21-01-2025 10:32:22 AM	C 0 H 0 M 0 L 0 U 0	C 0 H 0 M 0 L 0 U 0	

The **Service** page is accessed after a user selects a type or cloud from the **Inventory** page. It displays all the services associated with the selected cloud.

Service	Cloud	Total	Vulnerabilities	Alerts	Action
Elastic Container Registry	aws	277	Not scanned	-	
Volumes	aws	123	-	-	
Network interfaces	aws	122	-	C 0 H 1 M 0 L 0 U 1	
Security groups	aws	95	-	-	
EC2	aws	92	C 0 H 3 M 17 L 0 U 187	C 0 H 1 M 0 L 0 U 1	

The **Asset** list page is accessed after a user selects a service from the **Service** page. It displays all the assets that are associated with the service chosen.



Name	Cloud	Vulnerabilities	Alerts	Action
GetLicense-role-x086lw5g	aws	-	-	
JenkinsOFF	aws	-	-	
codebuild-gauravsecuraa-servic...	aws	-	-	
cwe-role-us-east-2-Dev-Nightly	aws	-	-	
AWSCodePipelineServiceRole...	aws	-	-	

## Query filter

Users can apply filters using **QueryFilter** at different levels:

- A **query filter** is used to refine and limit the data returned by a query based on specific criteria. It allows users to extract only the relevant subset of data from a larger dataset by applying conditions on fields or attributes.
- Filters use operators like equals (=), greater than (>), less than (<), and match to specify criteria.
- Multiple filters can be combined using **AND**, **OR**, and **NOT** to create complex conditions.
- On the **Inventory** page, filters are available for **Type (clouds)**, **Total assets**, **Vulnerabilities**, and **Alerts**.
- On the **Service** page, users can filter by **Services**, **Total assets**, **Vulnerabilities**, and **Alerts**.
- On the **Asset** page, users can view the list of assets for a specific service within a specific cloud and filter by **Name**, **Vulnerabilities**, and **Alerts**.



This screenshot shows the Inventory page of the securaa platform. At the top, there is a navigation bar with links to Cases, Dashboard and Reports, Monitoring Dashboard, TIP, CSAM, Automation, Configuration, and account settings. Below the navigation bar is a search bar labeled "Search Data". To the left of the main content area is a sidebar titled "fields" containing filter suggestions: Cases.Critical, Cases.High, Cases.Low, Cases.Medium, Cases.Unknown, Total, and Type. The main content area displays a table with columns: Total, Data as of, Vulnerabilities, Alerts, and Action. The table shows three rows of data corresponding to the filters selected in the sidebar.

This snapshot shows the query filter suggestions provided for users, allowing them to select and apply filters to refine their search results or data view.

This screenshot shows the Inventory page of the securaa platform after applying a search filter. The search bar now contains "Type:AWS". The main content area displays a table with columns: Type, Total, Data as of, Vulnerabilities, Alerts, and Action. The table shows one row of data for the AWS filter.

After the assets are listed, detailed information about a specific asset can be accessed by clicking on the asset. This action opens the asset information page, where users can view comprehensive details of the selected asset. Additionally, users have the option to update the **Business Hierarchy**, add or modify **Comments**, and add **Tags** to the asset.

This screenshot shows the asset information page for "Zona Google Translate". The page includes a breadcrumb navigation: Inventory > Aws > Elastic container registry > Zona Google Translate. The main content area shows the asset's details: Tags (testing), Overview, Business Hierarchy (selected), and Comments. A success message "Business Hierarchy updated." is displayed at the top right. Below the message is a form titled "Update Business Hierarchy" with fields for Assets (Laptop, Desktop, Mobile), location (mysore), and Department (IT). There are "Update" and "Cancel" buttons at the bottom right.



The screenshot shows the 'Comments' tab for the 'Sla Breach Monitor Batch' asset. It displays a single comment from 'Vignesh R' dated 21-01-2025 at 05:12:28.209 PM. The comment reads: 'Testing testing comment for documentation purpose'. A green success message at the top right says 'Comment added Successfully'.

Inside the asset details page, users can access comprehensive vulnerability information by selecting the corresponding **CVE\_ID**. This allows users to view detailed data about specific vulnerabilities associated with the asset, enabling more informed analysis and remediation actions.

The screenshot shows the 'Vulnerabilities (49)' tab for the 'Release.securaa.io' asset. It displays a summary of vulnerabilities across severity levels: All (49), Critical (0), High (1), Medium (2), and Low (0). On the right, a detailed view of CVE-2016-2183 is shown, including its CVSS score of 7.5, impact details (Version: 3.1, Attack Vector: NETWORK, etc.), and a weaknesses enumeration section.

## Export Assets

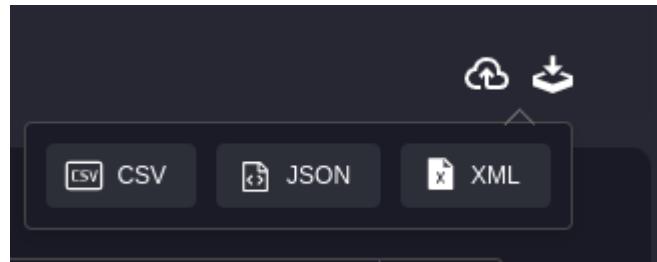
Analysts can download all the Asset data available in the CSAM in .CSV format by

clicking on the icon at the top right corner of the Inventory browser screen.

Analysts can also download asset data by applying filters using the **QueryFilter**. If a user needs specific data, such as a particular asset, cloud, service, or any other filtered set of data, they can use the QueryFilter to refine the results. The filtered data can then be exported, ensuring that only the required information is downloaded.

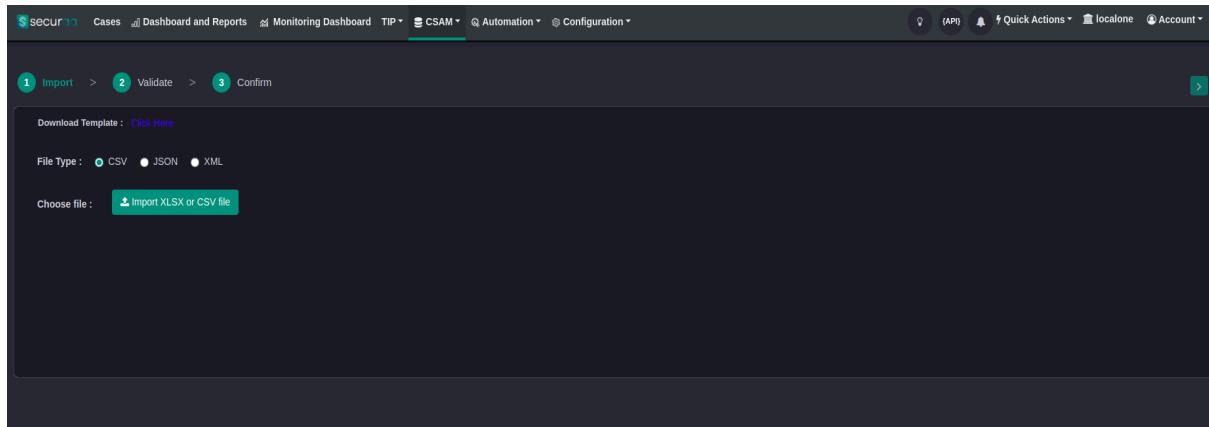
Also export asset will be exported in 3 different format

- CSV
- JSON
- XML



## Import Assets

Analysts can import Assets to Securaa CSAM by clicking on  the icon at the top right corner of the Inventory browser screen.



The steps to Import are as follows

1. Download template in three different format

- a. Fill all the Asset data in **CSV** file in the format shown in the below snapshot

	A	B	C	D	E
1	ipaddress	sources	asset_type	tags	business_hierarchy
2					

- b. Fill all the Asset data in **JSON** file in the format shown in the below snapshot

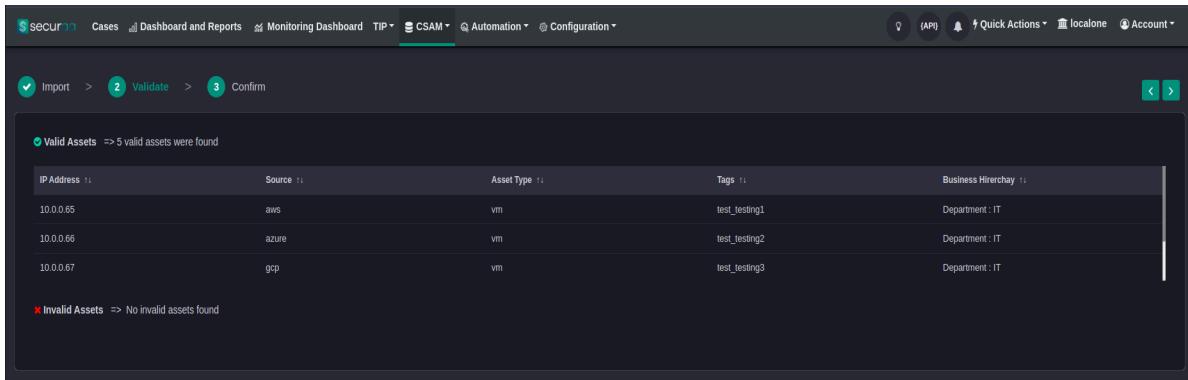
```

1 {
2   "Assets": [
3     {
4       "ipaddress": "10.0.0.29",
5       "sources": "qradar",
6       "asset_type": "vm",
7       "tags": "testingbot,malware",
8       "business_hierarchy":
9         {"Department": "IT"}
10      }
11    ]
12 }
```

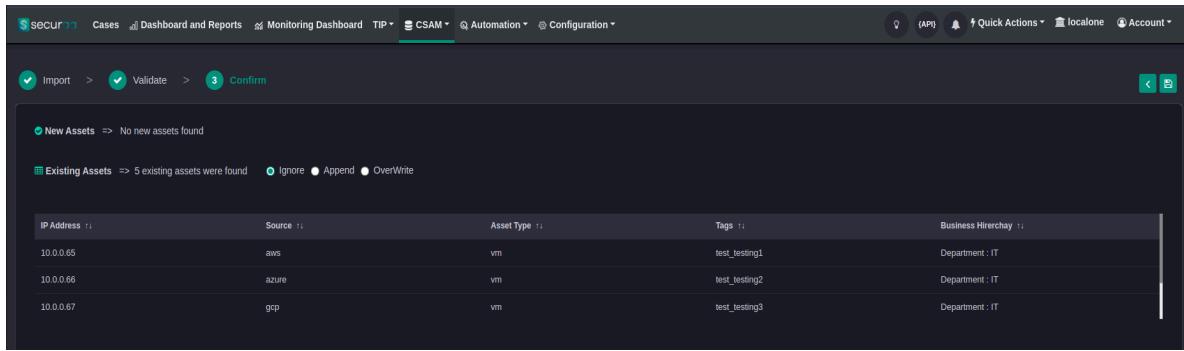
- c. Fill all the Asset data in **XML** file in the format shown in the below snapshot

```
1 <?xml version="1.0" encoding="UTF-8" ?>
2 <root>
3     <assets>
4         <ipaddress>1.1.1.1</ipaddress>
5         <sources>qradar</sources>
6         <asset_type>vm</asset_type>
7         <tags>testingbot malware</tags>
8         <business_hierarchy>
9             <Department>IT</Department>
10            </business_hierarchy>
11        </assets>
12    </root>
```

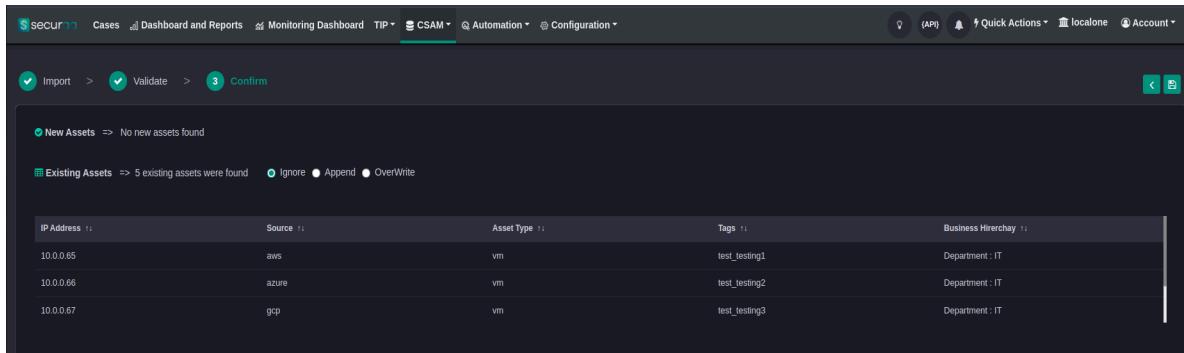
2. Upload the CSV containing Asset data.
3. Verify Asset details and confirm Assets that are being uploaded.



IP Address	Source	Asset Type	Tags	Business Hierarchy
10.0.0.65	aws	vm	test_testing1	Department : IT
10.0.0.66	azure	vm	test_testing2	Department : IT
10.0.0.67	gcp	vm	test_testing3	Department : IT



IP Address	Source	Asset Type	Tags	Business Hierarchy
10.0.0.65	aws	vm	test_testing1	Department : IT
10.0.0.66	azure	vm	test_testing2	Department : IT
10.0.0.67	gcp	vm	test_testing3	Department : IT



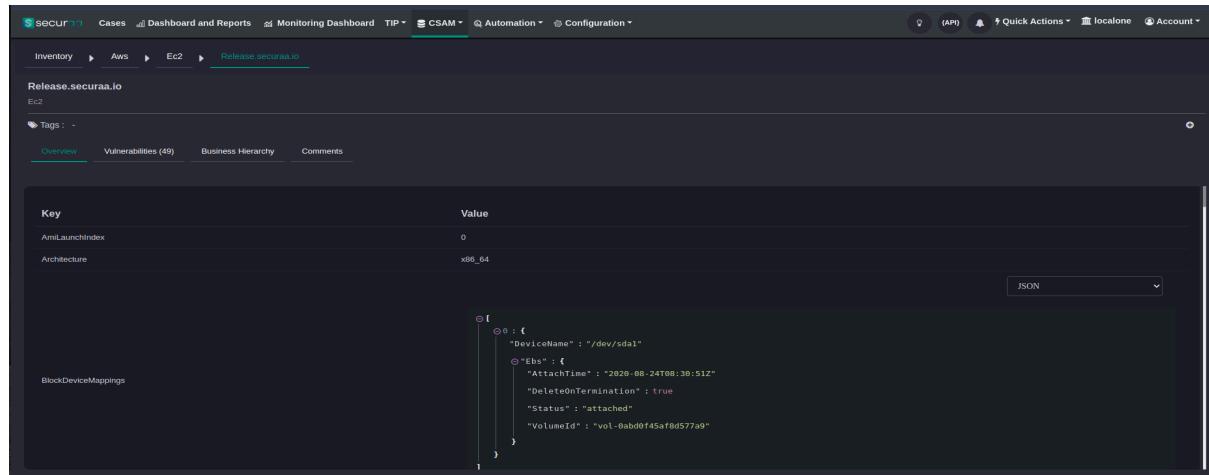
IP Address	Source	Asset Type	Tags	Business Hierarchy
10.0.0.65	aws	vm	test_testing1	Department : IT
10.0.0.66	azure	vm	test_testing2	Department : IT
10.0.0.67	gcp	vm	test_testing3	Department : IT

4. After the imported data is validated, it moves to the **Confirm** stage. At this stage, if an IP address already exists, the data is flagged as an existing asset. The user is then presented with three options:
  - **Ignore:** Skip the imported data without making any changes to the existing asset.
  - **Overwrite:** Replace the existing asset data with the new imported data.
  - **Append:** Add new information from the imported data to the existing asset without replacing current values.

Based on the user's input, the data is processed and saved accordingly.

## Asset Overview

Users can drill down by clicking on an asset in the Asset List Browser screen to view detailed information about that particular asset, specific to the respective service and cloud, as shown in the snapshot.



The screenshot shows the securaa interface for managing AWS resources. The navigation bar includes links for Cases, Dashboard and Reports, Monitoring Dashboard, TIP, CSAM, Automation, Configuration, and account-specific options like API, Quick Actions, and Account. The main content area shows a breadcrumb path: Inventory > Aws > Ec2 > Release.securaa.io. Below this, it displays an EC2 instance named 'Release.securaa.io'. The instance has no tags. It lists four tabs: Overview (selected), Vulnerabilities (49), Business Hierarchy, and Comments. The Overview tab displays a table with two rows: 'Key' and 'Value'. The first row has 'AmiLaunchIndex' under Key and '0' under Value. The second row has 'Architecture' under Key and 'x86\_64' under Value. A large JSON object is displayed below this table, representing the BlockDeviceMappings for the instance. The JSON structure is as follows:

```
{
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sda1",
      "Ebs": {
        "AttachTime": "2020-08-24T08:30:51Z",
        "DeleteOnTermination": true,
        "Status": "attached",
        "VolumeId": "vol-0abd0f45af8d577a9"
      }
    }
  ]
}
```

## Asset Report

The user can download the asset information in PDF report format from the Asset

Information screen. Upon clicking the **Asset Report** button , the asset details will be downloaded and presented in a PDF report, as shown in the snapshots below.

## Asset and Vulnerability Report

Asset Name: Checkpoint Firewall | Service Name: Aws

### Overview

Key	Value
AmiLaunchIndex	0
Architecture	x86_64
BootMode	-
CapacityReservationId	-
ClientToken	4d8d1778-4e81-421d-9804-5e554ce2d0f0
EbsOptimized	true
ElasticGpuAssociations	-
ElasticInferenceAcceleratorAssociations	-
EnaSupport	true
Hypervisor	xen
ImageId	ami-06c919bb36d164a19
InstanceId	i-020c322a009ffa1de
InstanceLifecycle	-
InstanceType	m5.xlarge
Ipv6Address	-
KernelId	-
KeyName	securaamasterkey
LaunchTime	2024-10-22T10:02:55Z
Licenses	-
OutpostArn	-
Platform	-
PlatformDetails	Linux/UNIX

Key	Value
RootDeviceType	ebs
SourceDestCheck	true
SpotInstanceRequestId	-
SriovNetSupport	-
StateTransitionReason	User initiated (2024-10-22 10:49:56 GMT)
SubnetId	subnet-006f044c
UsageOperation	RunInstances
UsageOperationUpdateTime	2024-05-22T06:47:49Z
VirtualizationType	hvm
VpcId	vpc-31983a5a

#### Business Hierarchy

Key	Value
No Data	

#### Alerts



#### Summary

Severity	Case ID	Description	Source	Status	Category	Risk
No Data						

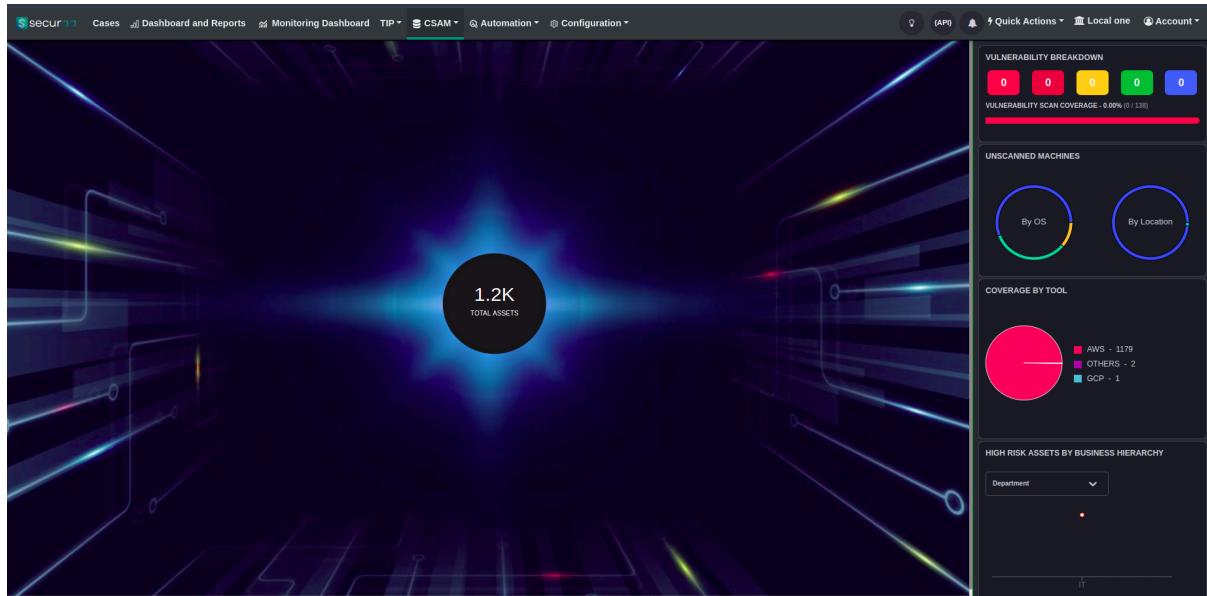
#### Vulnerabilities



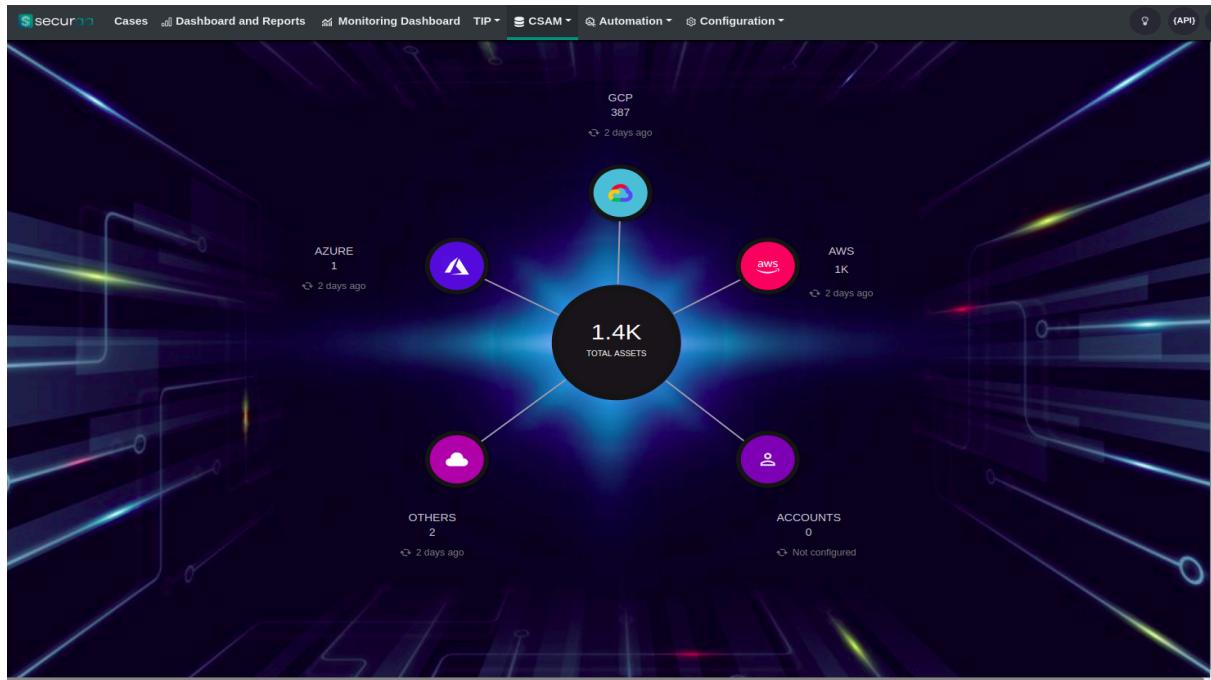
## CSAM Node Dashboard

The CSAM dashboard provides comprehensive visibility into security assets with various interactive widgets, such as **Vulnerability breakdown**, **Unscanned machines**, **Coverage by tools**, **High risk by business hierarchy**. CSAM is integrated with Securaa to enable efficient cyber security asset management, offering insights into asset inventory, vulnerabilities, and compliance status. The dashboard presents data in an easy-to-understand graphical format, allowing SOC Analysts to quickly assess the security posture. Analysts can click on widgets to drill down into detailed views, enabling them to analyze specific assets, vulnerabilities, and alerts, and take appropriate actions to mitigate risks and improve overall security.

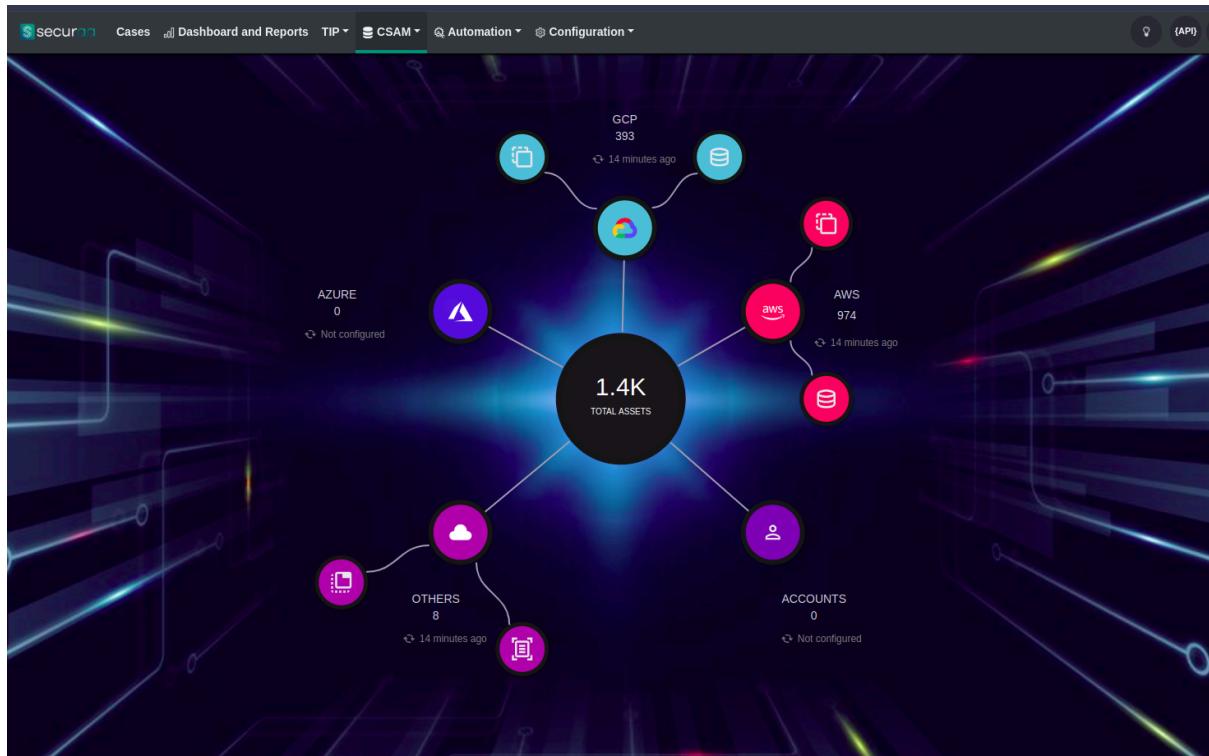
To access the CSAM Dashboard, go to the CSAM menu and select the Dashboard option. This will display the Dashboard interface as shown in the snapshot.



- The above snapshot shows a visual representation of the level one dashboard and the widget in the side panel.
- When we click on Total Assets, a visual representation of the level two dashboard is displayed, where we can see the clouds and on-premises infrastructure represented as nodes as shown in the snapshot.
- Clicking on a cloud name provides a drill-down that redirects to the inventory page of the respective cloud.



- In level two, after viewing the cloud nodes, clicking on a respective cloud displays the VM services and storage for each cloud, as shown in the snapshot.

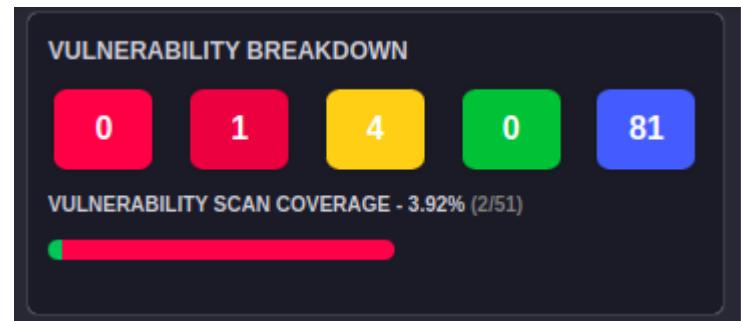


- After level two of the dashboard, where services are displayed upon clicking a cloud, clicking on each service provides a drill-down view that redirects to the inventory page of the respective service.

CSAM Widget consist of 4 widgets ,

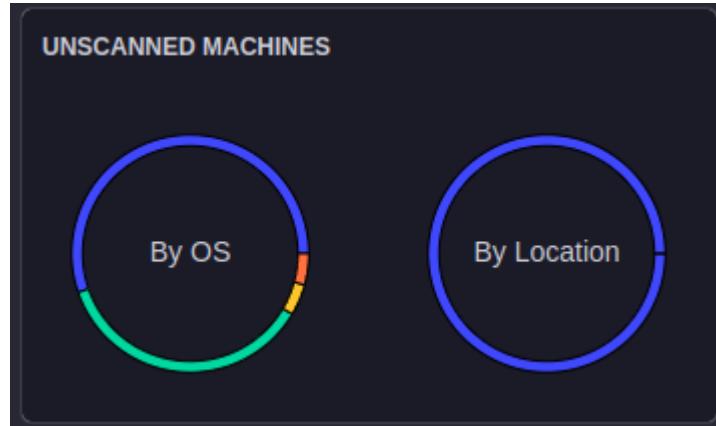
#### 1. Vulnerability breakdown

- The vulnerability breakdown shows the total count of vulnerabilities for each asset.
- We have provided a drill-down for the vulnerabilities, which will directly redirect to the inventory page.
- Additionally, the vulnerability breakdown widget displays the scan coverage percentage of the total vulnerabilities for VMs.



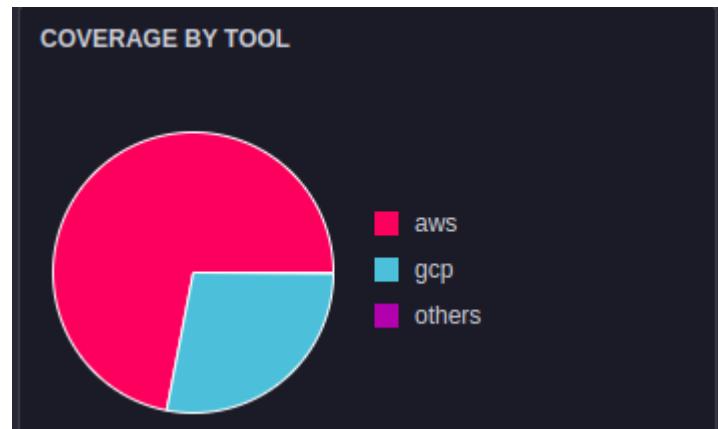
## 2. Unscanned machine

- The unscanned machines are displayed as "Unscanned Machines by OS" and "Unscanned Machines by Location."



## 3. Coverage by tool

- Coverage by tool shows the total number of each cloud in the pie chart format.
- Here we gave a drill-down through pie chart if we click on the pie chart it will redirect to inventory page .



#### 4. High risk by business hierarchy

- We provide a graphical representation of the business hierarchy, where the business hierarchy configuration data is grouped. By selecting a specific business hierarchy from the dropdown, you can view the risk associated with that particular business hierarchy.

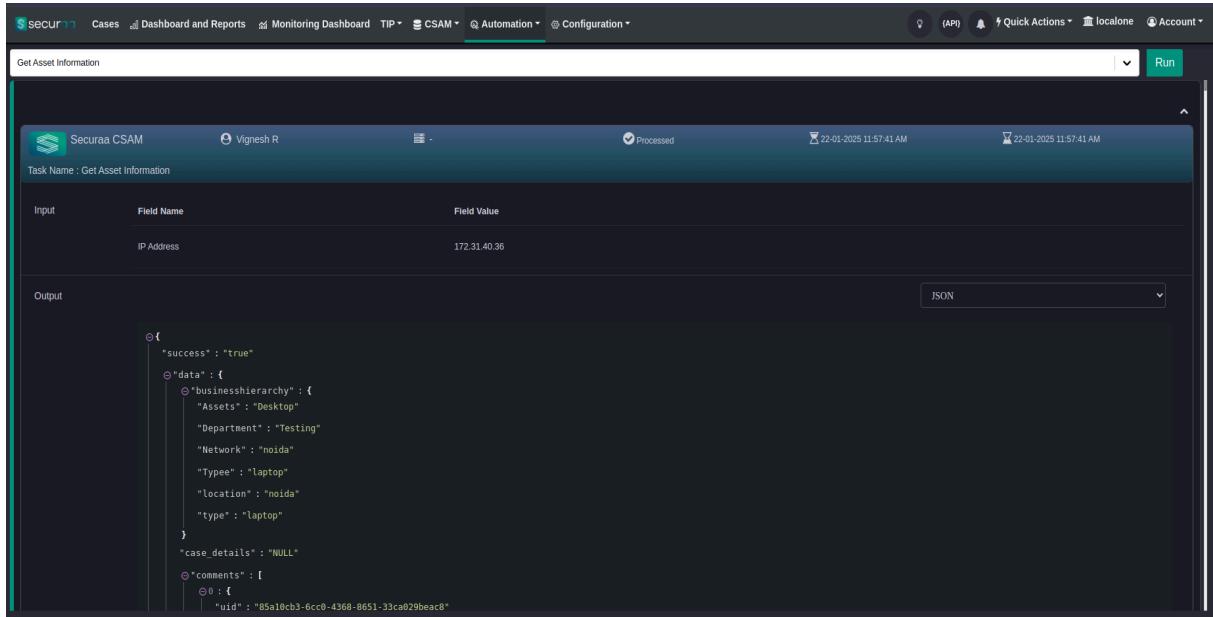


## CSAM Automation Tasks

Securaa CSAM supports one automated task. Below are the details of the task

### 1. Get Asset Information

This task helps in retrieving detailed information about the asset by providing its IP address.



The screenshot shows the Securaa CSAM task interface for the 'Get Asset Information' task. The task was run by Vignesh R on 22-01-2025 at 11:57:41 AM. The input field 'IP Address' contains the value 172.31.40.36. The output is displayed in JSON format:

```
{
  "success": true,
  "data": {
    "businesshierarchy": {
      "Assets": "Desktop",
      "Department": "Testing",
      "Network": "noida",
      "Typee": "laptop",
      "location": "noida",
      "type": "laptop"
    }
  },
  "case_details": null,
  "comments": [
    {
      "0": {
        "uid": "85a10cb3-6cc0-4368-8651-33ca029beac8"
      }
    }
  ]
}
```