Prisma Cloud Overview

Prisma Cloud is a comprehensive cloud-native security platform with the industry's broadest security and compliance coverage. It protects cloud-native applications, data, networks, computing, storage, users, and higher-level PaaS services across cloud platforms. Prisma Cloud enables Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for comprehensive visibility and threat detection across your organization's hybrid, multi-cloud infrastructure. It dynamically discovers resources as they are deployed and correlates cloud-service-provided data to enable security and compliance insights into your cloud applications and workloads.

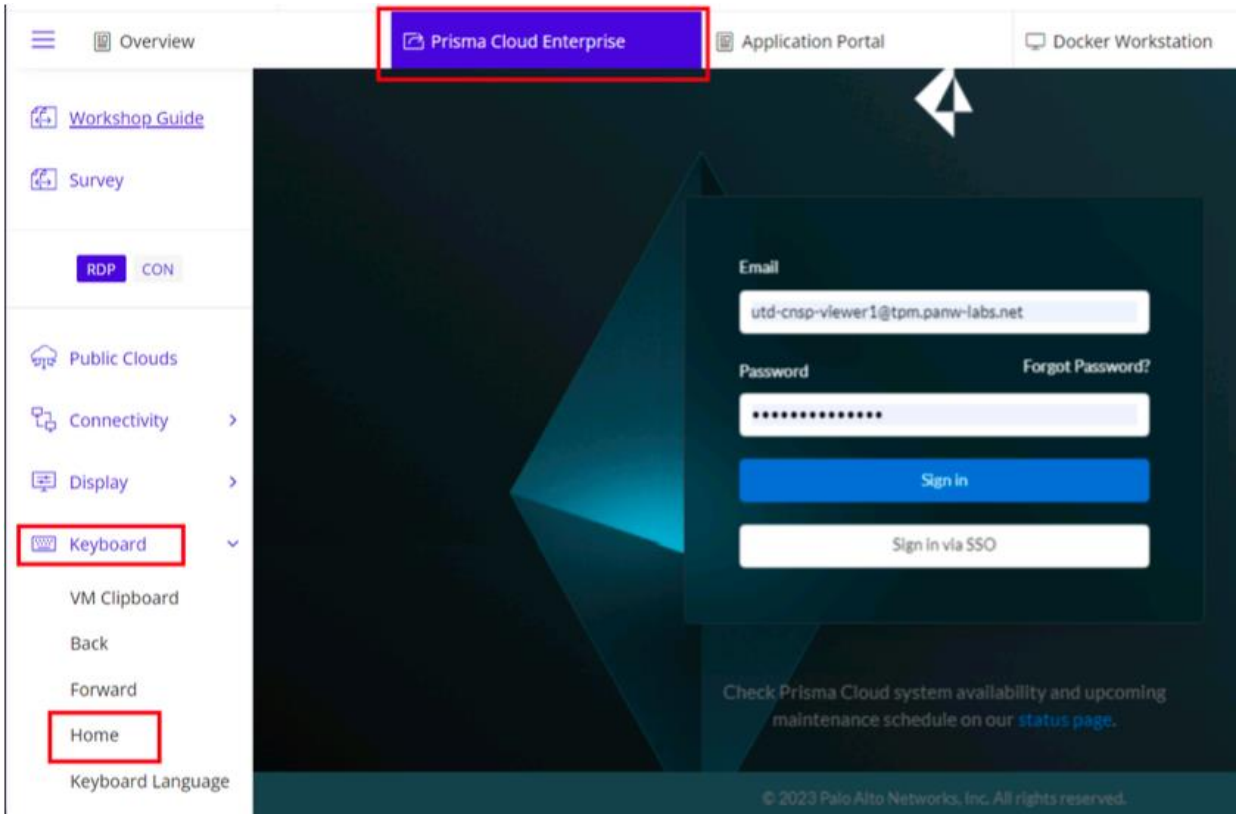
In this activity, you will:

- Log in to the Prisma Cloud Lab account
- Learn about the Prisma Cloud console and help center
- Review how to onboard an AWS account on Prisma Cloud tenant
- Review out-of-the-box policies, queries, compliance standards, and remediations

Note: This is a standalone activity and is not dependent on other activities.

---------- Task 1: Log in to Prisma Cloud Enterprise Edition Console ----------

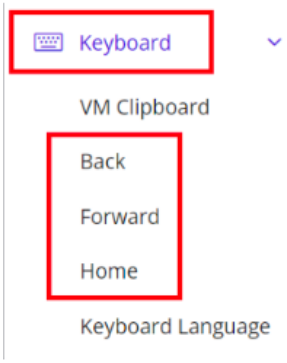
Step 1. Click on the Prisma Cloud Enterprise tab to open the demo tenant login.



Step 2. Follow the screen to log in and click the Prisma Cloud icon.

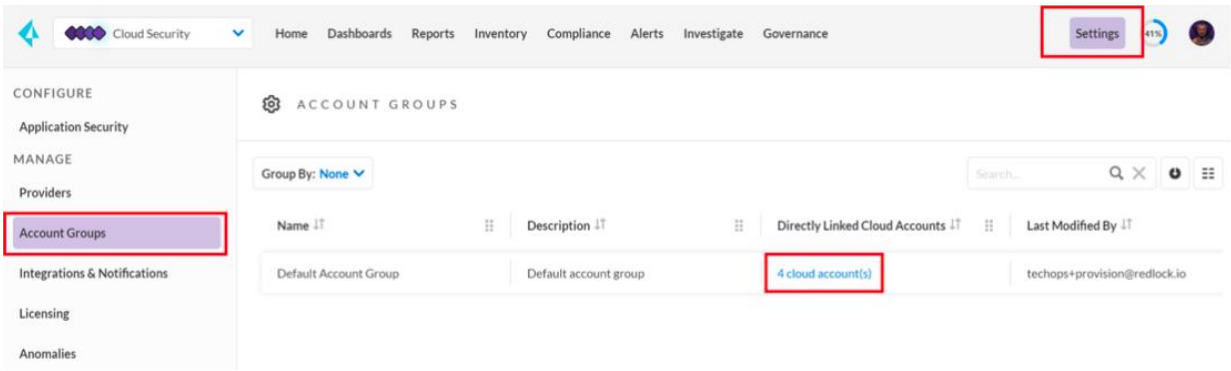
NOTE: If you see a page expired message then ***refresh*** *the web page by clicking on the* ***Home button*** *as highlighted in the screen capture.*

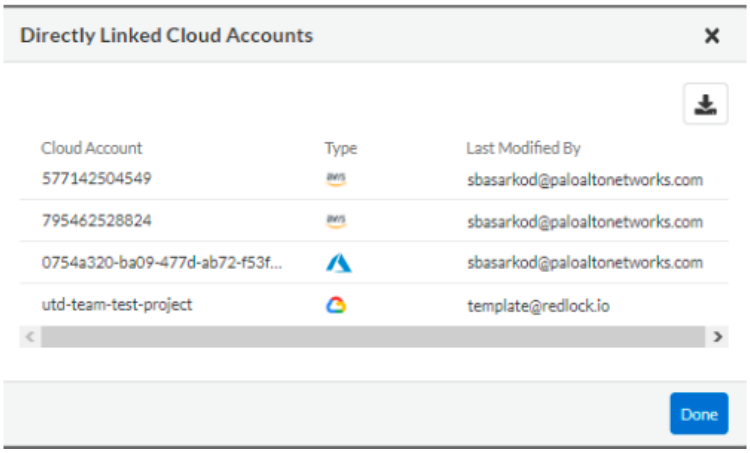
Step 3. While using the Prisma Cloud console, you can use CloudShare > Keyboard > Home | Back | Forward to navigate back and forth.



Step 4. To check the on-boarded public cloud accounts click on the **Settings** the and select **Account Groups.** Click on the **4 Cloud Account(s)** under **Default Account Group**. You can see the public cloud accounts connected to this Prisma Cloud demo account.

NOTE: *The screenshots captured in this workshop guide might vary slightly from the actual lab account.*





We have already connected AWS, Azure, and GCP accounts to this Prisma Cloud service, and this lab account can be used for testing across all three public cloud providers.

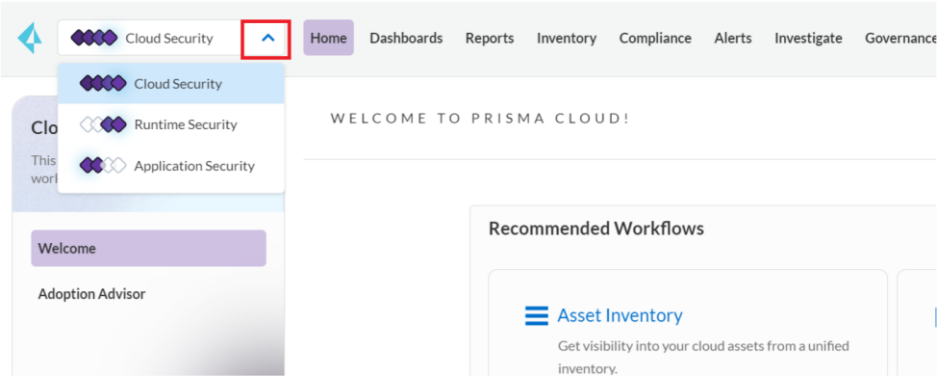
NOTE: *The Prisma Cloud Enterprise Edition account used in this lab is read-only, it does not have full access to the Prisma Cloud Service, and access to some functions is denied. This account cannot change the configuration of the associated Prisma Cloud Services.*

---------- Task 2: Prisma Cloud Dashboards and Inventory ----------

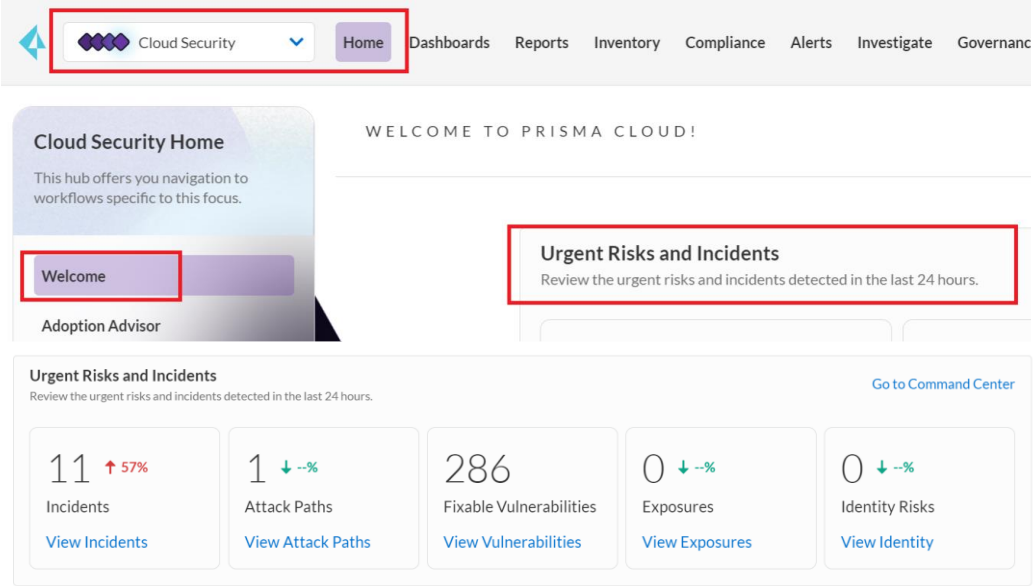
Step 1. In this task, we will explore various parts of the UI within Prisma Cloud that provide rich contextualized information correlated from various data sources within Prisma Cloud. For example, the **Dashboards** are meant to be a starting point for users in real-world situations to get an overview of their environment.

In our lab, some parts of the UI discussed in this specific section are not visible to the read-only user. Hence, we will try our best to show you an overview of what they are and what they look like via screenshots and descriptions.

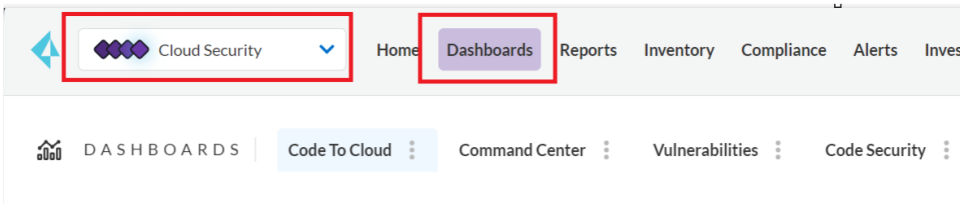
Step 2. When you first log in to Prisma Cloud, from the top left corner, you can select one of the 3 options for your current view: **Cloud Security**, **Runtime Security,** and **Application Security**. To get started, select **Cloud Security**.



Step 3. On the Welcome page, you can see the Urgent Risks and Incidents, which provide you with information such as Incidents, Attack Paths, Vulnerabilities, Exposures, and Identity Risks. **In the lab, this part is not visible as it's not available for the read-only user**.

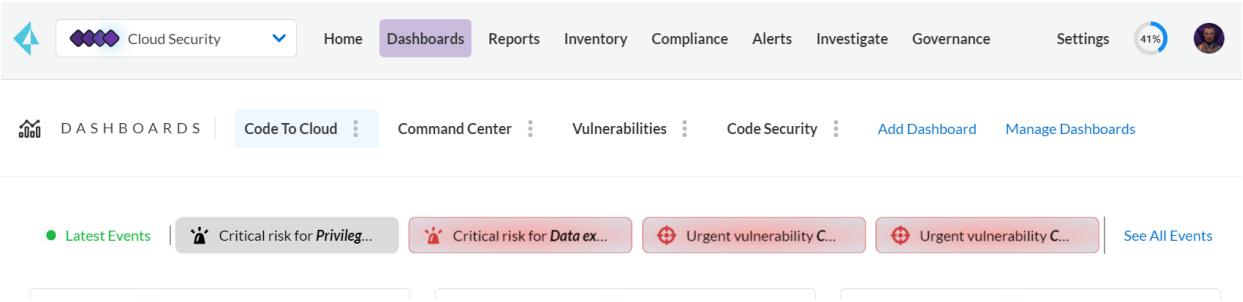


Step 4. When you select **Prisma Cloud > Cloud Security > Dashboards**, by default you will be able to see four dashboards and also the **Latest Events** section.

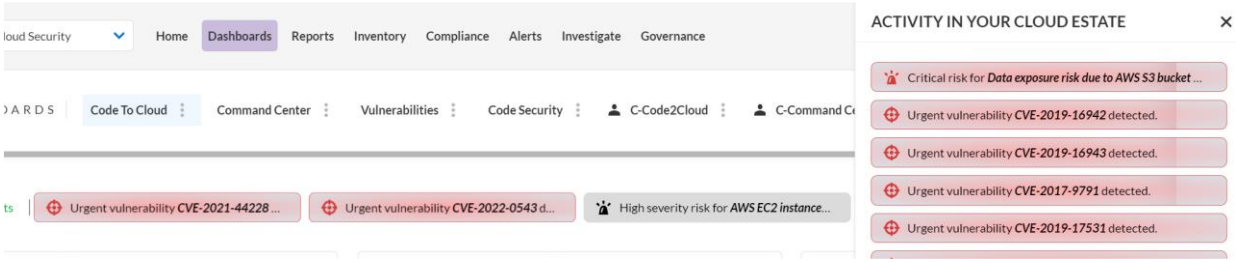


Step 5. Latest Events (Not Visible):

a) This presents immediate things that need your attention. This is a continuous real-time feed of events

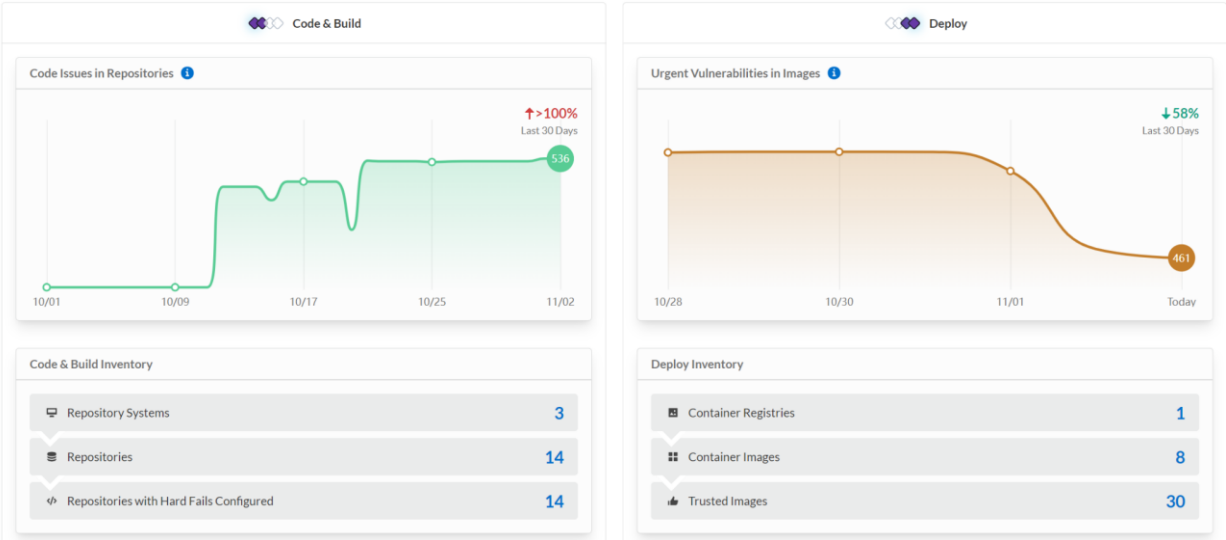


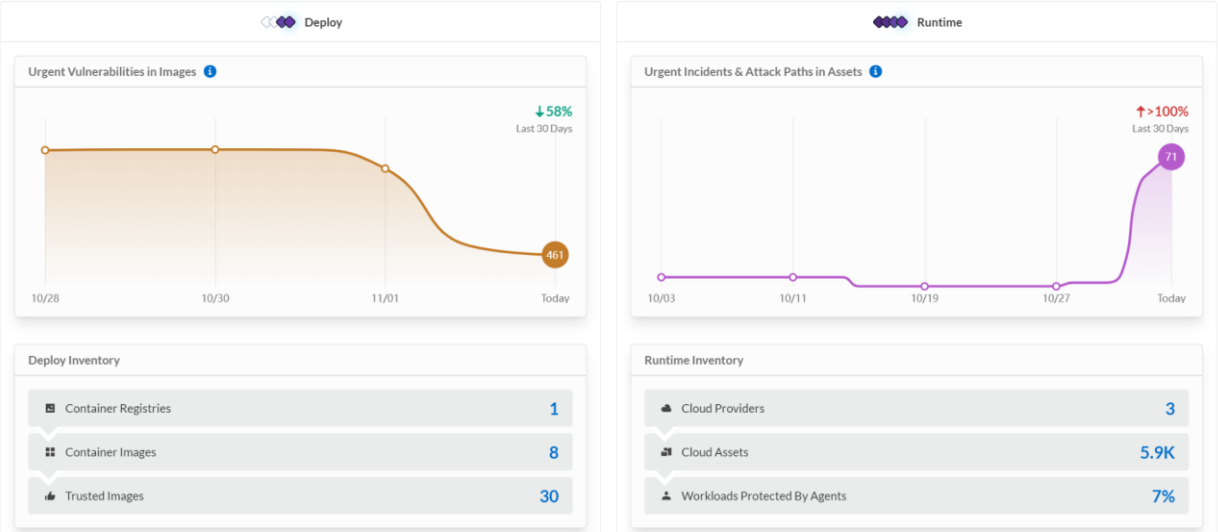
b) Clicking on **See All Events** will open up all the events



Step 6. Code To Cloud Dashboard (Not Visible):

a) This Dashboard provides visibility about various items in your environment categorized into the following 3 categories: **Code and Build, Deploy, and Runtime**. (screenshots are adjusted to fit the page)

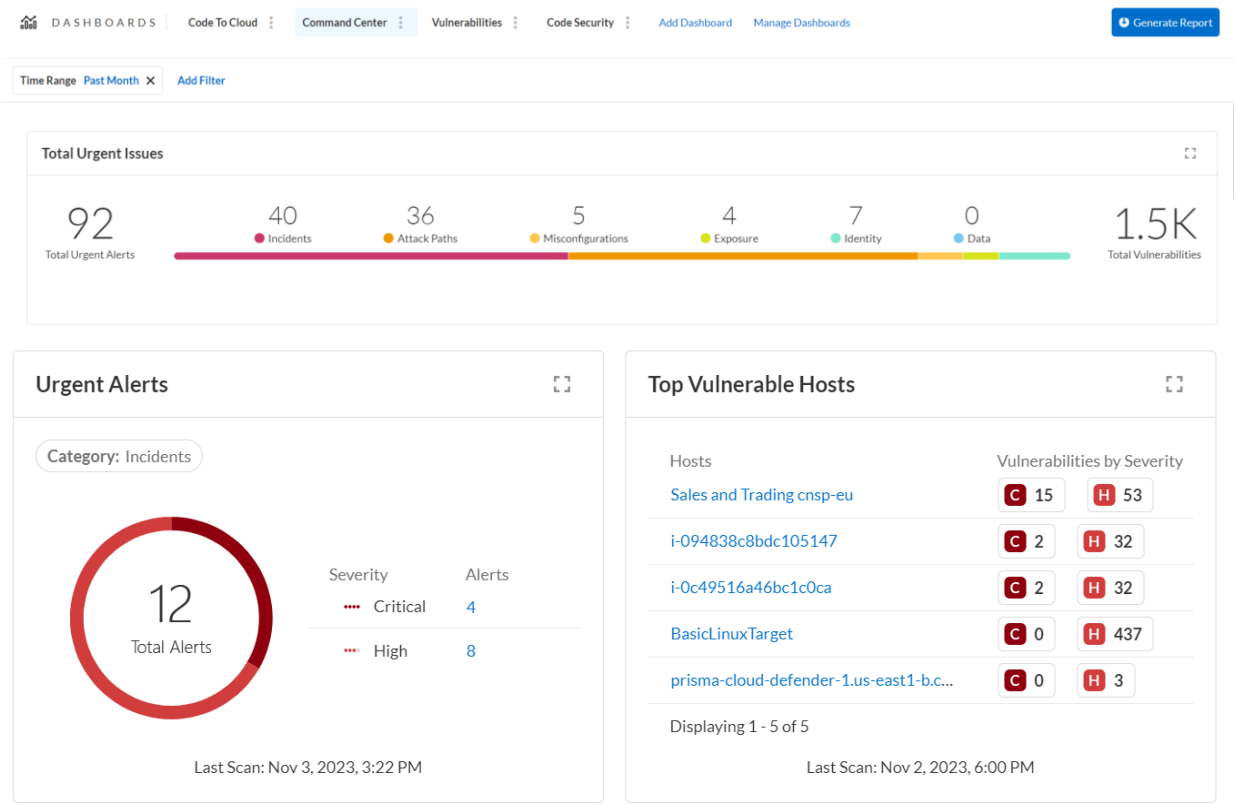


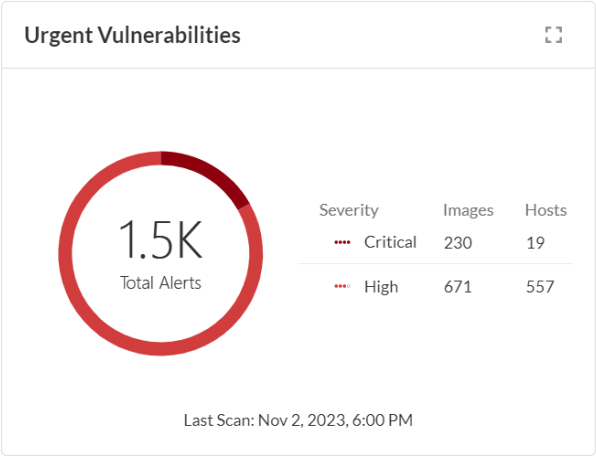


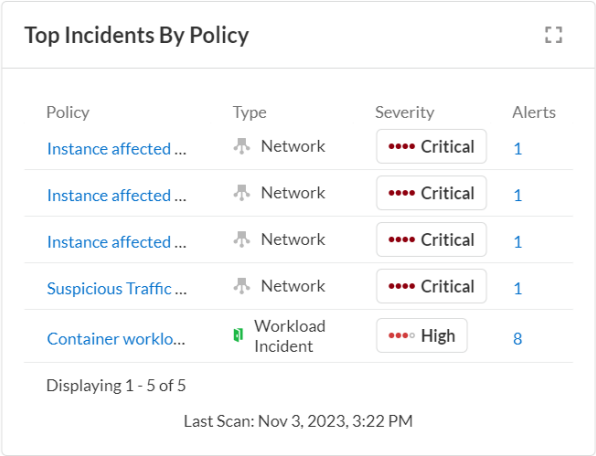
b) Clicking on items such as **Repository Systems, Repositories, Container images, Cloud Assets** etc will take you to their respective pages within Prisma Cloud. The Dashboard conveniently provides all things in one place.

Step 7. Command Center Dashboard (Not Visible):

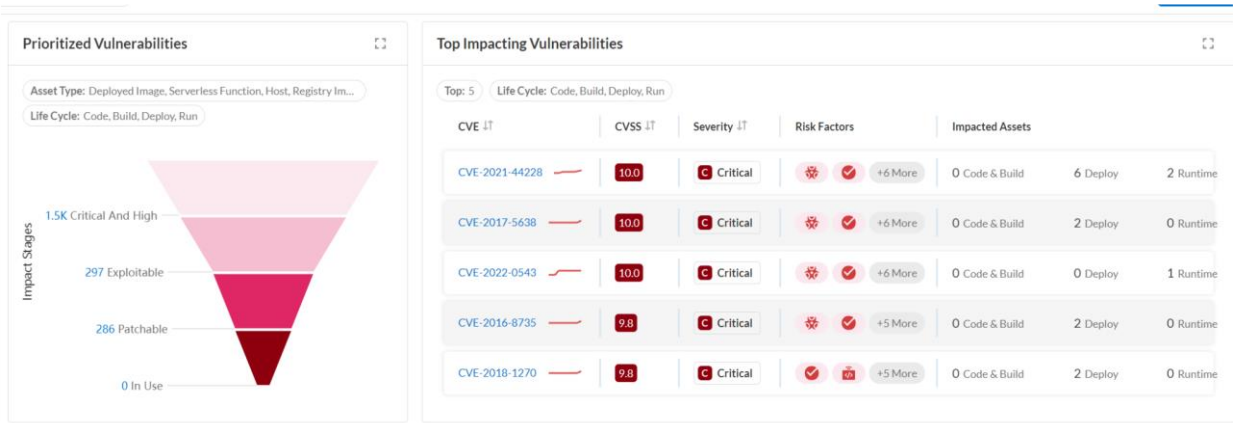
a) This dashboard is a command center, which provides information such as **Urgent Issues, Urgent Incidents, Top Incidents by Policy, Urgent Attack Paths,** etc. This is a highly customizable dashboard and the screenshots below do not represent all the options visible in the dashboard but merely provide you a glimpse of what's available.

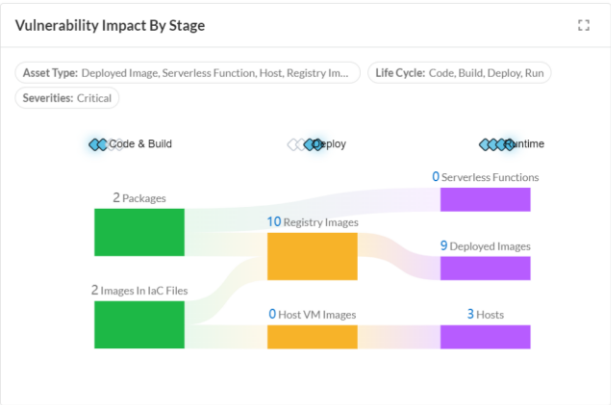


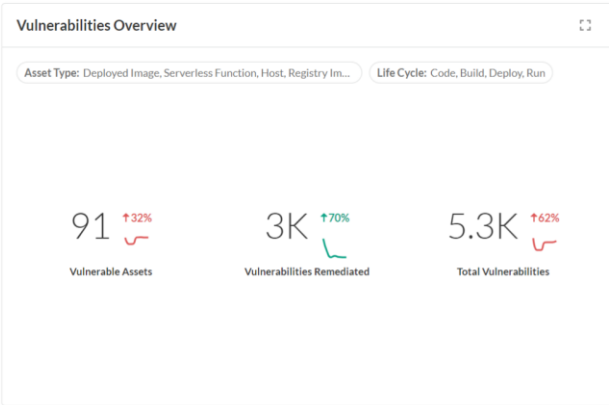




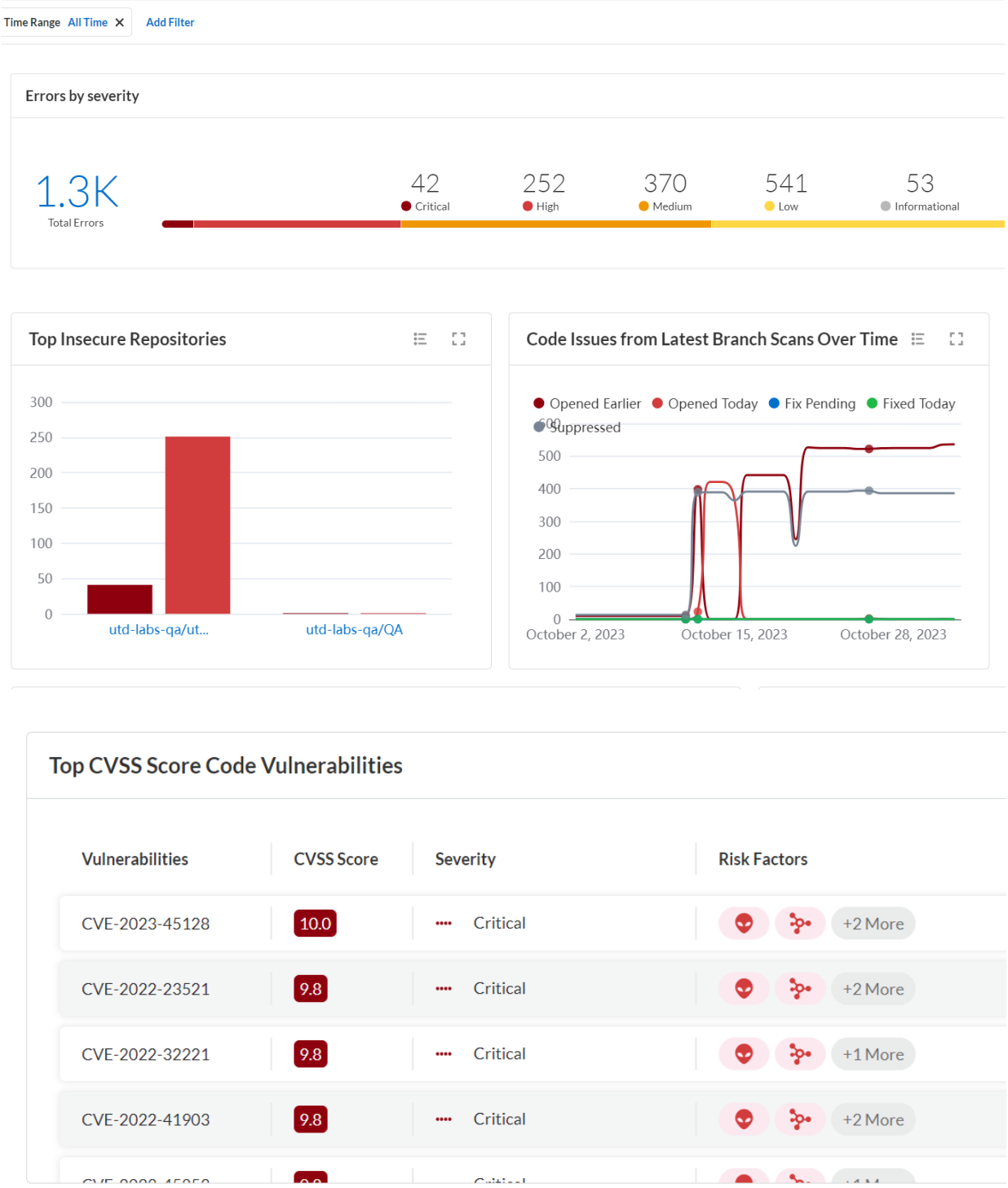
Step 8. Vulnerabilities Dashboard (Visible): This provides an overview of the current vulnerabilities that exist across your system. A modified version of this dashboard should be visible to you in the lab.



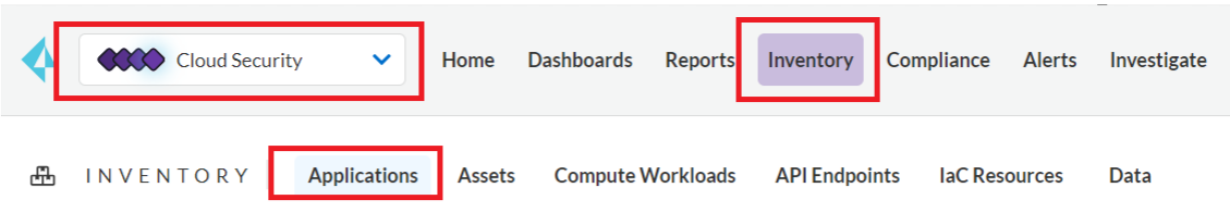




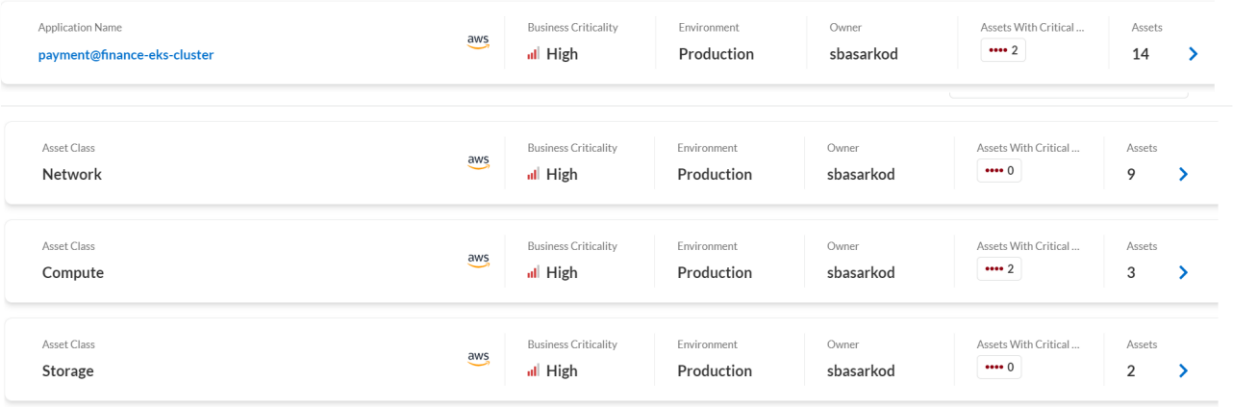
Step 9. Code Security Dashboard (Visible): This dashboard provides you with information about your code repositories currently on-boarded onto Prisma Cloud.



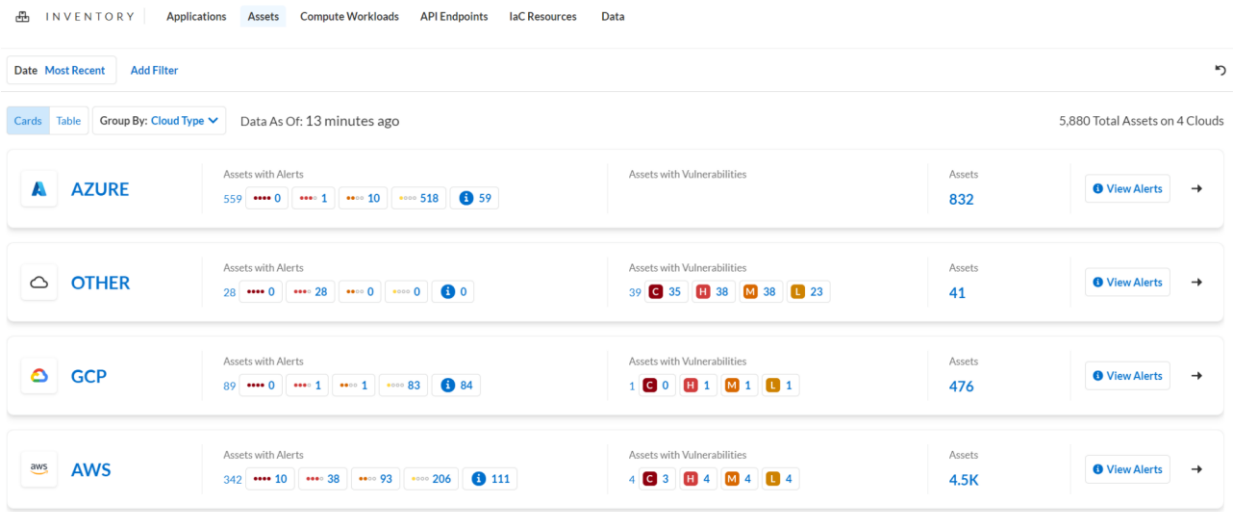
Step 10. Inventory: Prisma Cloud > Cloud Security > Inventory: Some parts of this section are not fully visible to the read-only user. But we will try our best to give you a brief overview of what it offers.



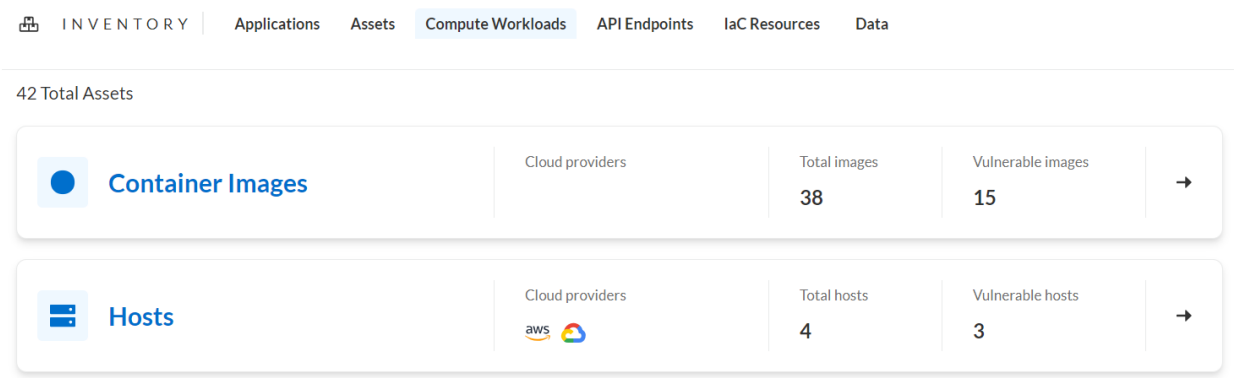
a) **Application (Not Visible):** This is the custom application running in a container environment (EKS) that Prisma Cloud has visibility into it. Clicking on this will further expand more items about that Cluster.

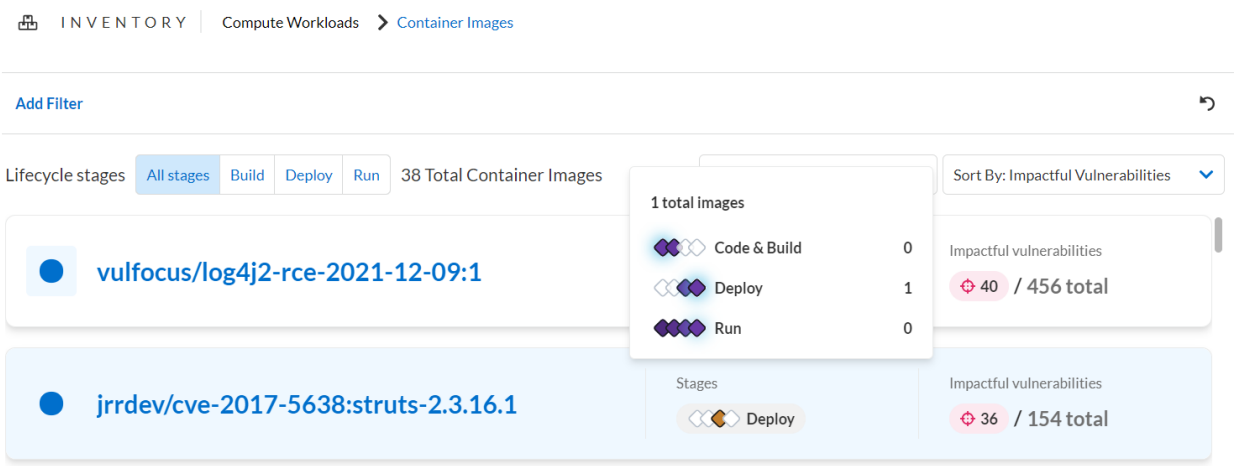


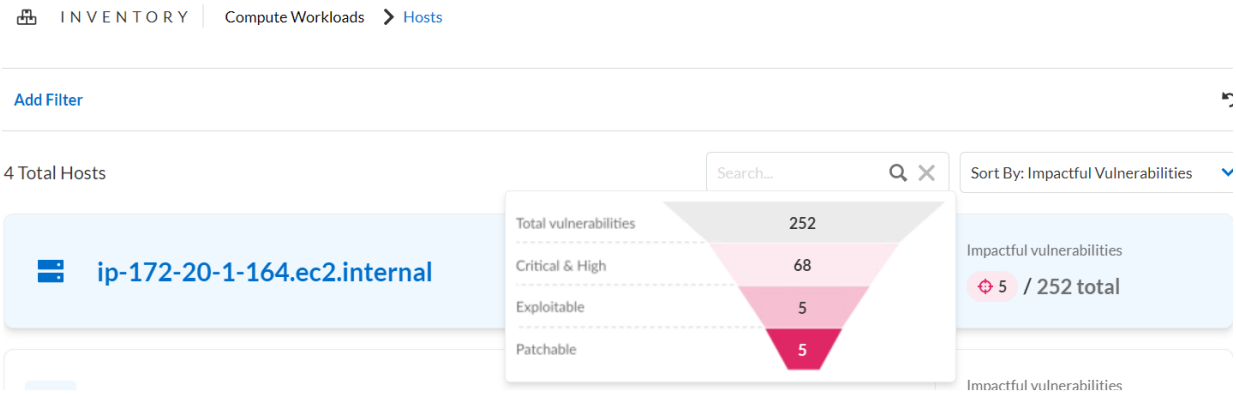
b) **Assets (Visible):** This part provides an overview of all the assets within your environment that Prisma Cloud has visibility and their vulnerabilities- All in one place. From this dashboard, you can immediately see alerts and asset information corresponding to a specific Cloud Account



c) **Compute Workloads (Partially Visible):** This provides visibility into Compute environments that includes Container Images and Hosts across all your environments.







d) **API Endpoints (Visible):** This provides information about API Endpoints that are deployed in your environment. We will be looking into this further in the next sections.

INVENTORY | Applications | Assets | Compute Workloads | API Endpoints | IaC Resources | Data

Add Filter

Cards | Table | Group By: None

Path	Method	Server	Hits	Risk factors	Workload	Cloud
/products/653fc3f4cb23dfb34d168889	GET	http://a65423273a39c45a6b...	397,851		gcr.io/vmwarecloudadvocacy/...	aws
/products	GET	http://52.0.237.7	227,372		gcr.io/vmwarecloudadvocacy/...	aws
/products	GET	http://a65423273a39c45a6b...	227,372		gcr.io/vmwarecloudadvocacy/...	aws
/cart/items/{parameter}	GET	http://cart:5000	56,764		gcr.io/vmwarecloudadvocacy/...	aws
/products/653fc3f4cb23dfb34d168889	GET	http://catalog:8082	483,090		gcr.io/vmwarecloudadvocacy/...	aws
/login	POST	http://users:8083	28,494		gcr.io/vmwarecloudadvocacy/...	aws

e) **IaC Resources (Not Visible):** This provides a list of your IaC resources by correlating the code from your onboarded repositories and the resources that are deployed by it, which is detected by Prisma Cloud in your Cloud environment.

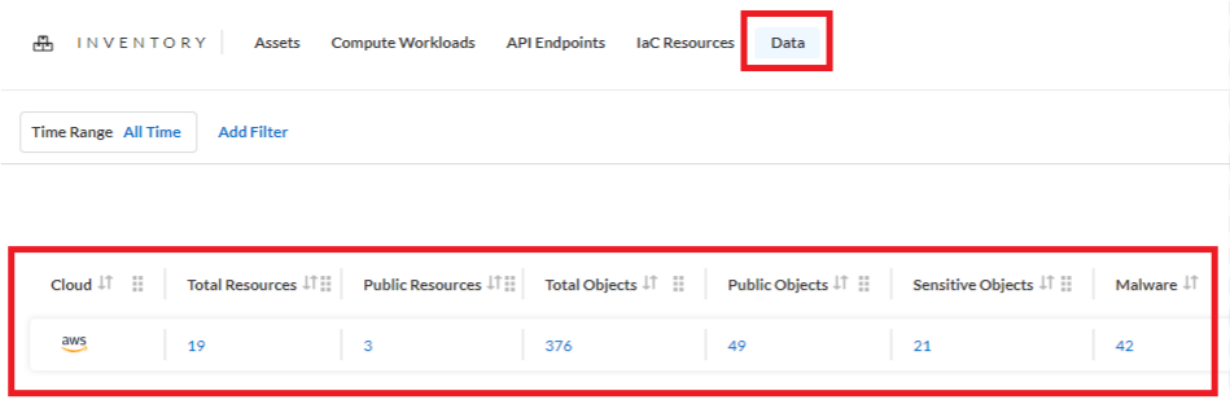
INVENTORY | Applications | Assets | Compute Workloads | API Endpoints | IaC Resources | Data

Add Filter

200 assets in 4 Frameworks

Framework	Total	Pass	Fail	Resources With Code Issues					Resources With Vulnerabilities					
Terraform	107	5	102	102	0	24	13	101	28	0	C 0	H 0	M 0	L 0	0
CloudFormation	45	6	39	39	0	4	8	39	6	0	C 0	H 0	M 0	L 0	0
Kubernetes	28	13	15	15	0	2	11	13	0	6	C 2	H 4	M 4	L 6	0
Docker	20	12	8	8	0	0	0	8	0	0	C 0	H 0	M 0	L 0	0

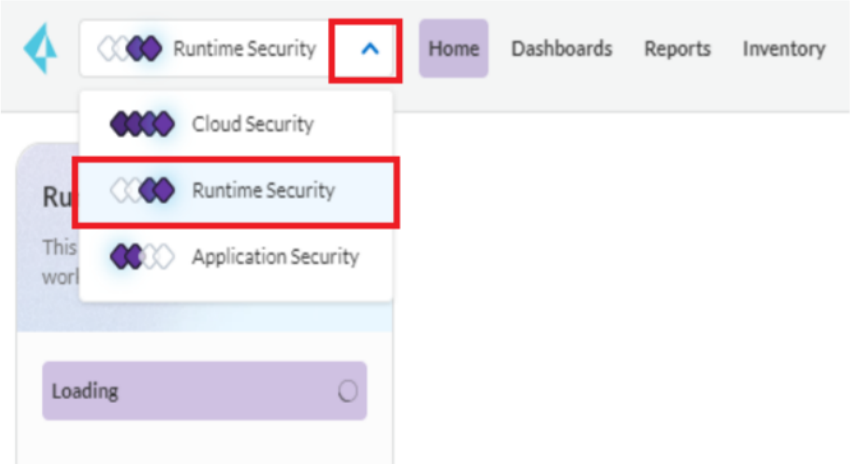
f) **Data (Visible):** Here you get visibility into your Data in Storage such as an S3 bucket. Prisma Cloud monitors your storage and you can see if there's any PII (Personal Identifiable Information) or Malware in your storage. This should be visible to the lab user.



---------- Task 3: Runtime Security Overview ----------

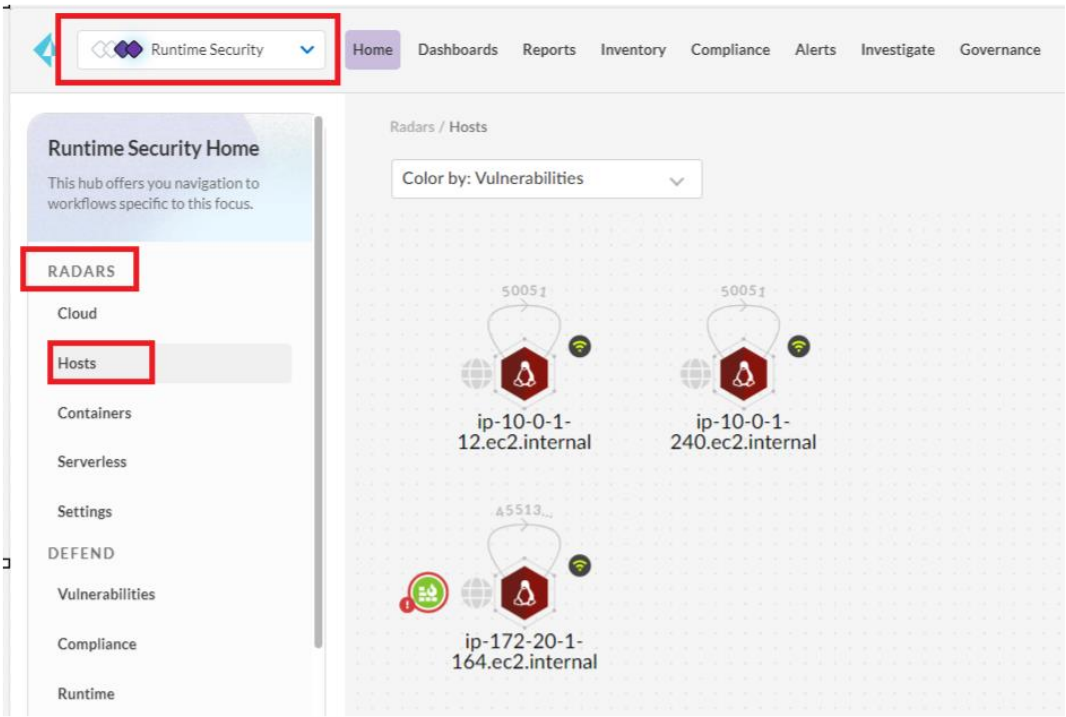
Step 1. This task provides an overview of the Runtime Security section of Prisma Cloud Enterprise Edition. Prisma Cloud Compute Edition is a standalone and self-hosted version of Prisma Cloud Enterprise version's Runtime Security.

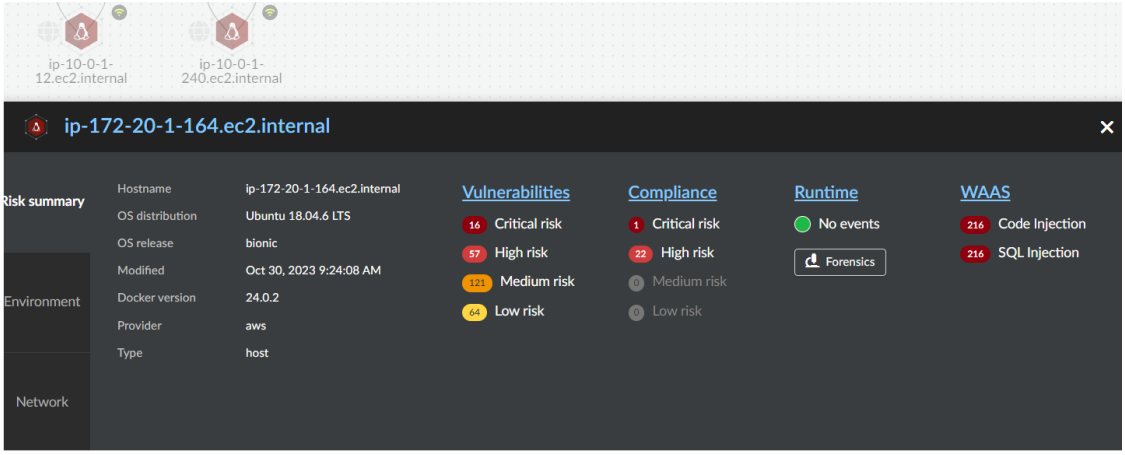
Step 2. Navigate to **Prisma Cloud** > **Runtime Security** > **Radars**



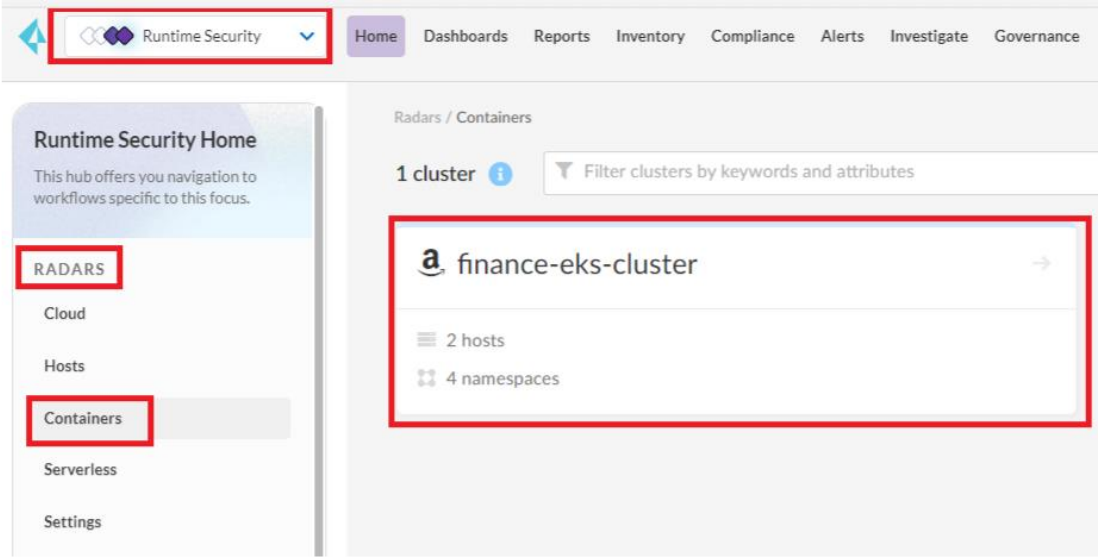
Step 3. Radars:

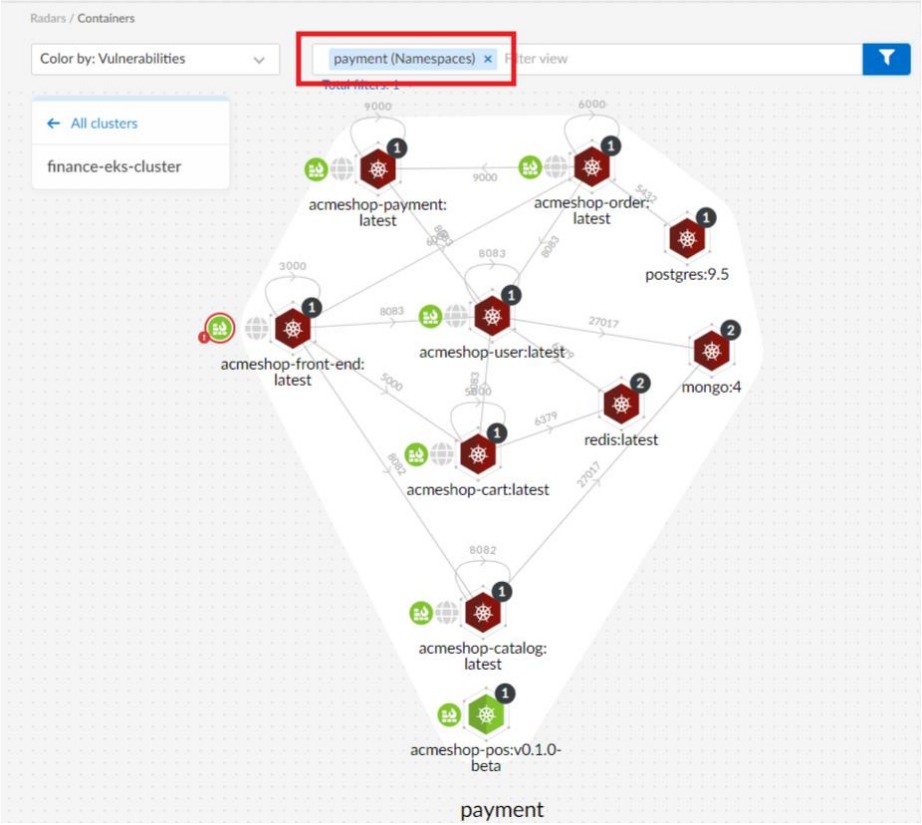
a) Select **Radars > Hosts**: This will show the currently monitored hosts. Clicking on one of the hosts will show more information.





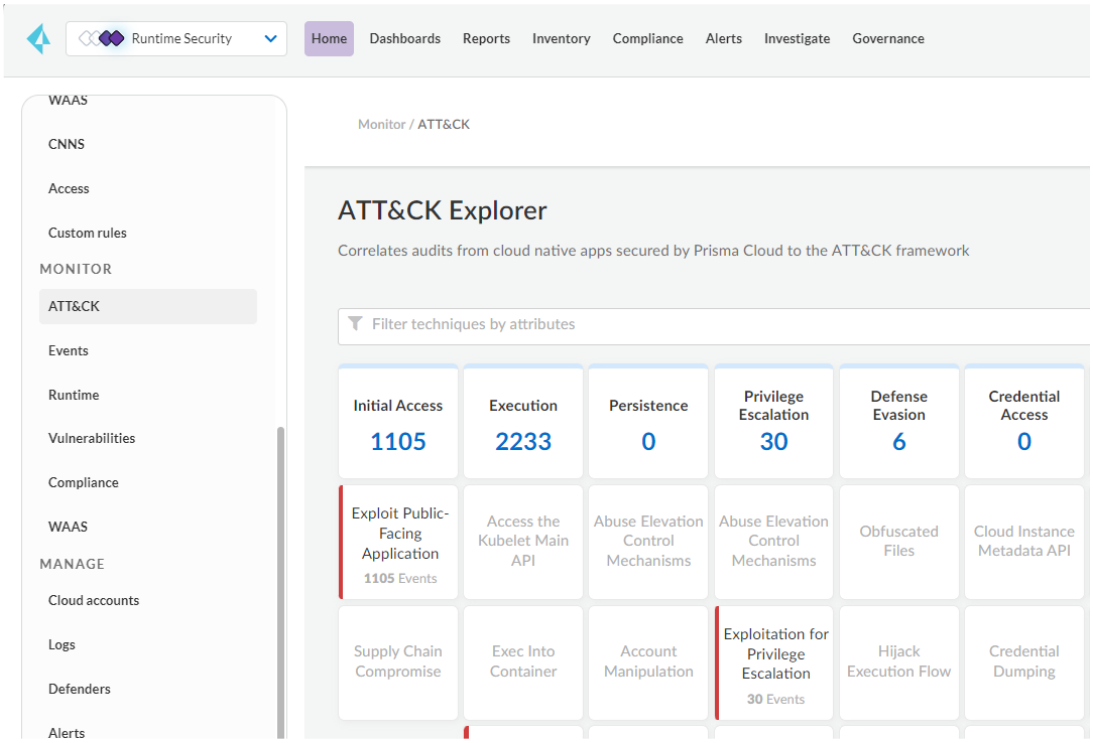
b) Clicking on **Radars > Containers** will show the currently deployed containers. Click on the **finance-eks-cluster** to explore further and get visibility into the application running in the cluster.



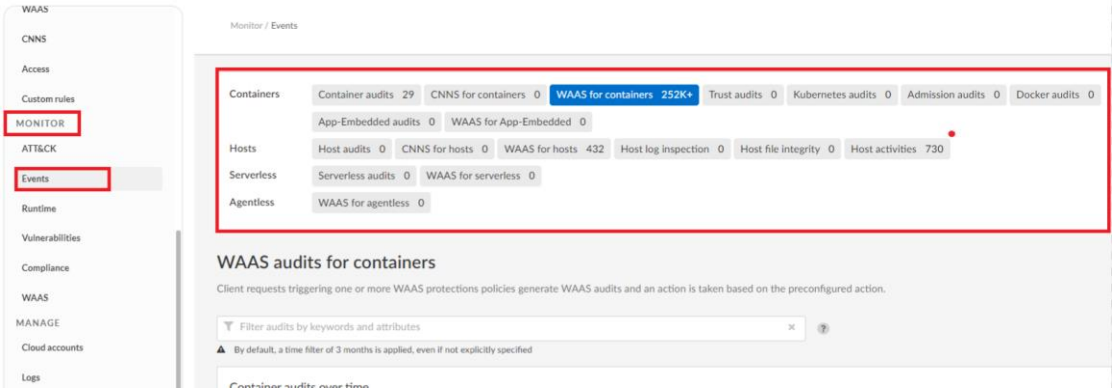


Step 4. ATT&CK

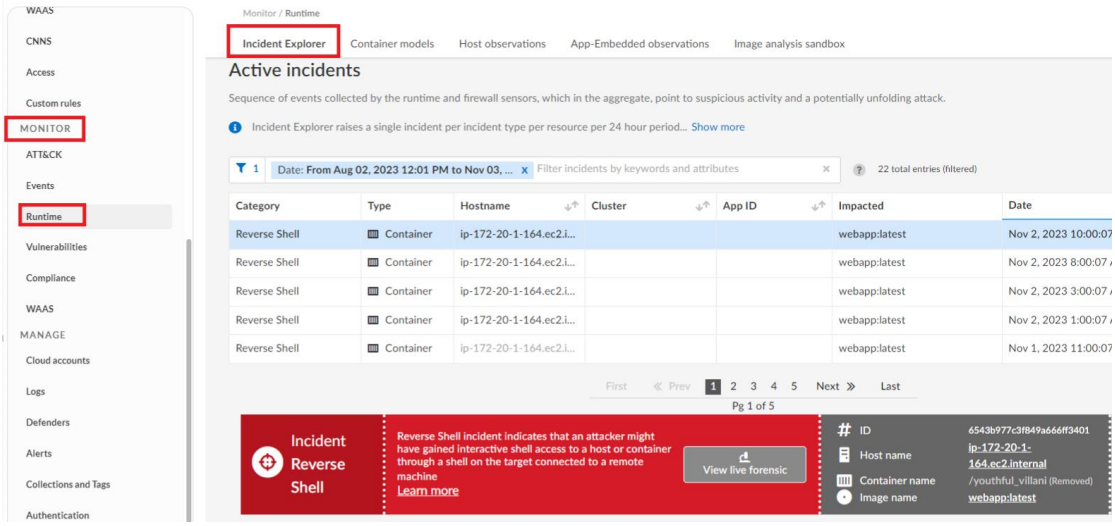
a) **Navigate to Monitor > ATT&CK**. This page correlates audits from cloud-native apps secured by Prisma Cloud to the ATT&CK framework



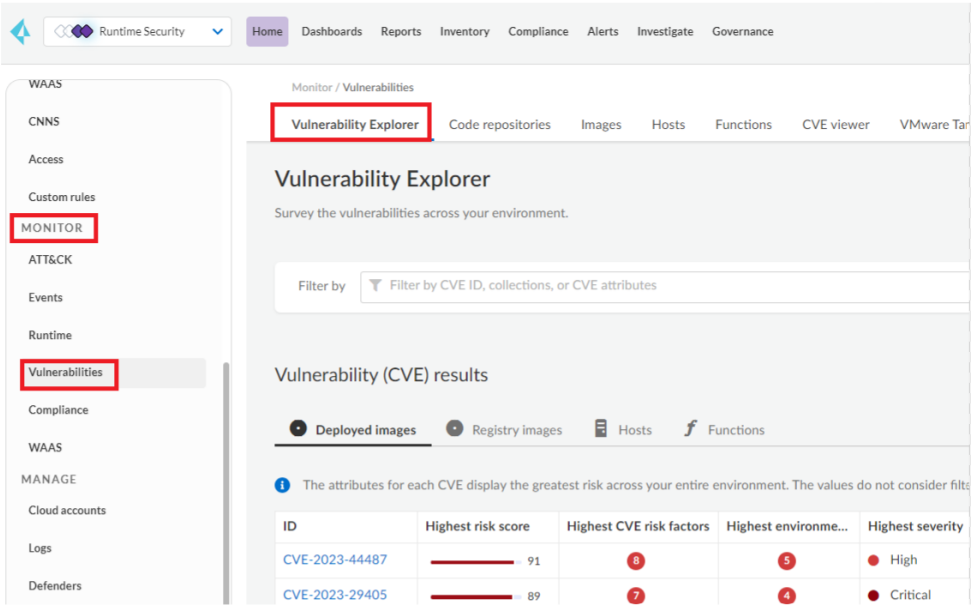
b) **Monitor > Events** shows the current events detected by the policies for **Hosts, Containers, Serverless and Agentless**. Here you can select different filters



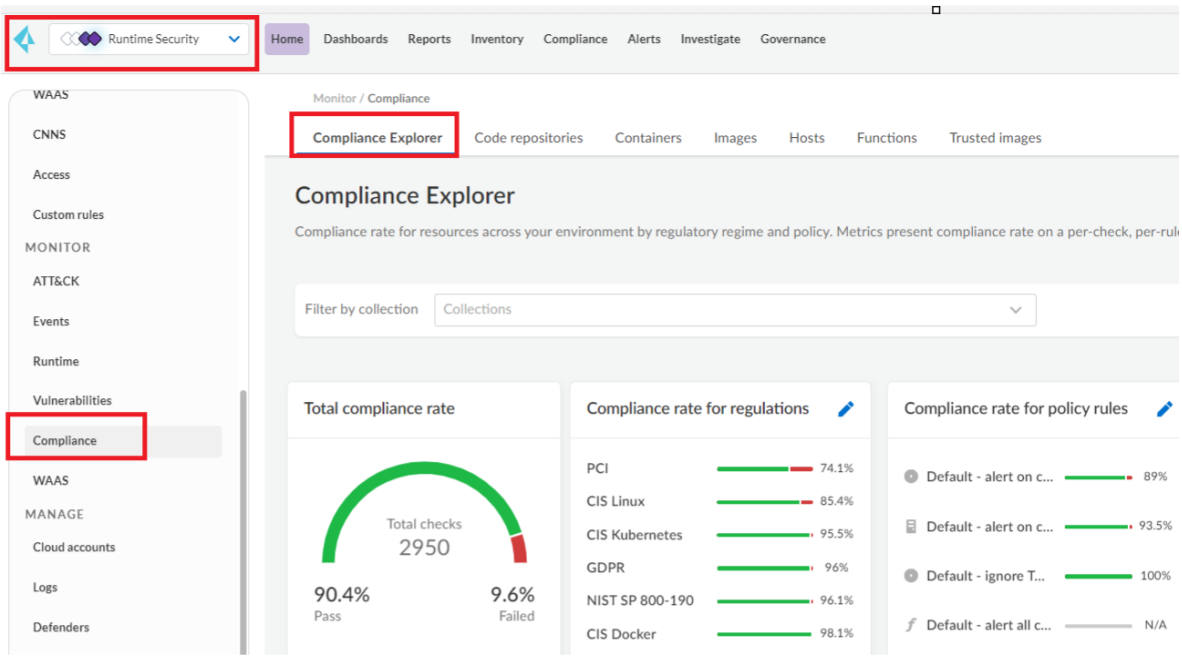
c) **Monitor > Runtime > Incident Explorer**: This shows the current active incidents.



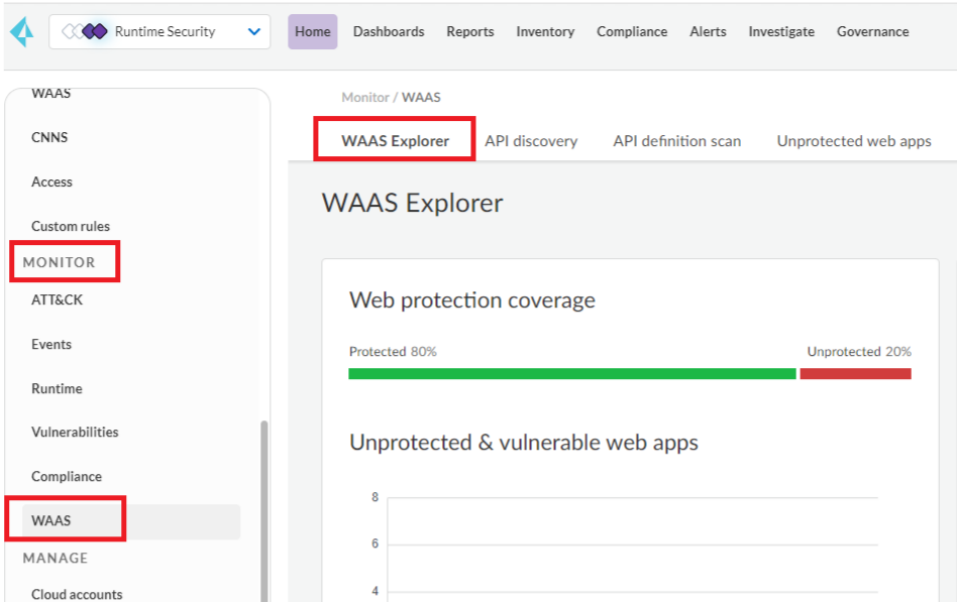
d) **Monitor > Vulnerabilities > Vulnerabilities Explorer** shows the various vulnerabilities detected in the current environment.

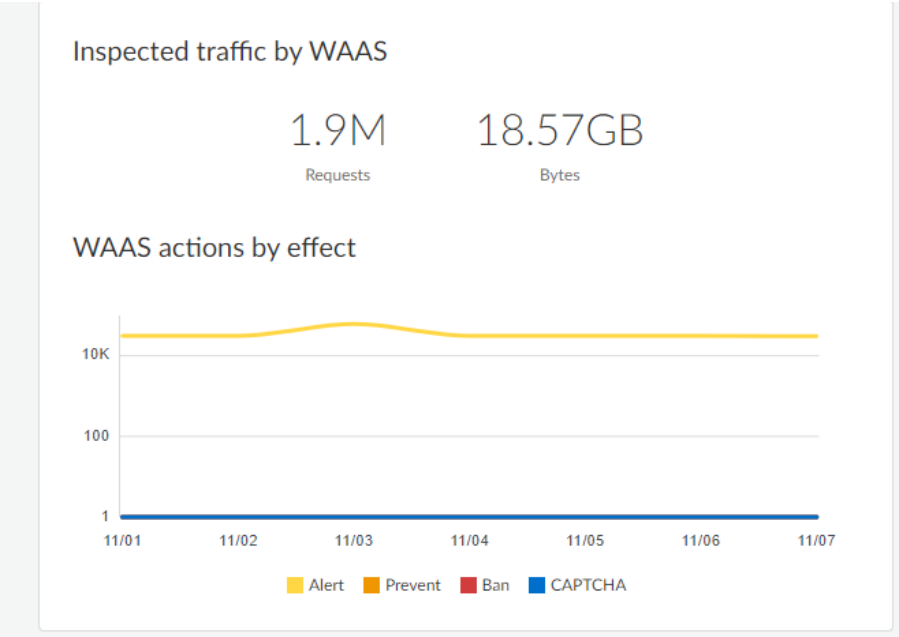


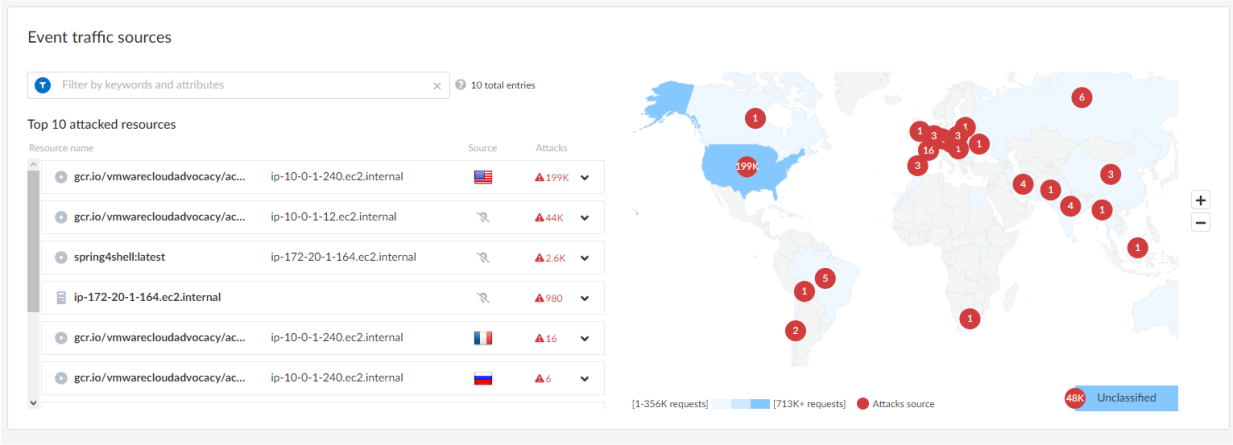
e) **Monitor > Compliance > Compliance Explorer** shows the compliance rate for resources across the environment by regulatory regime and policy



f) **Monitor > WAAS > WAAS Explorer**: Shows the Web Application and API Security Dashboard




Inspected traffic by WAAS
1.9M
Requests
18.57GB
Bytes
WAAS actions by effect
10K
100
1
11/01
11/02
11/03
11/04
11/05
11/06
11/07
Alert
Prevent
Ban
CAPTCHA


Event traffic sources
Filter by keywords and attributes
10 total entries
Top 10 attacked resources
Resource name
Source
Attacks
gcr.io/vmwarecloudadvocacy/ac... ip-10-0-1-240.ec2.internal 199K
gcr.io/vmwarecloudadvocacy/ac... ip-10-0-1-12.ec2.internal 44K
spring4shell:latest ip-172-20-1-164.ec2.internal 2.6K
ip-172-20-1-164.ec2.internal 980
gcr.io/vmwarecloudadvocacy/ac... ip-10-0-1-240.ec2.internal 16
gcr.io/vmwarecloudadvocacy/ac... ip-10-0-1-240.ec2.internal 6
[1-356K requests]
[713K+ requests]
Attacks source
48K
Unclassified

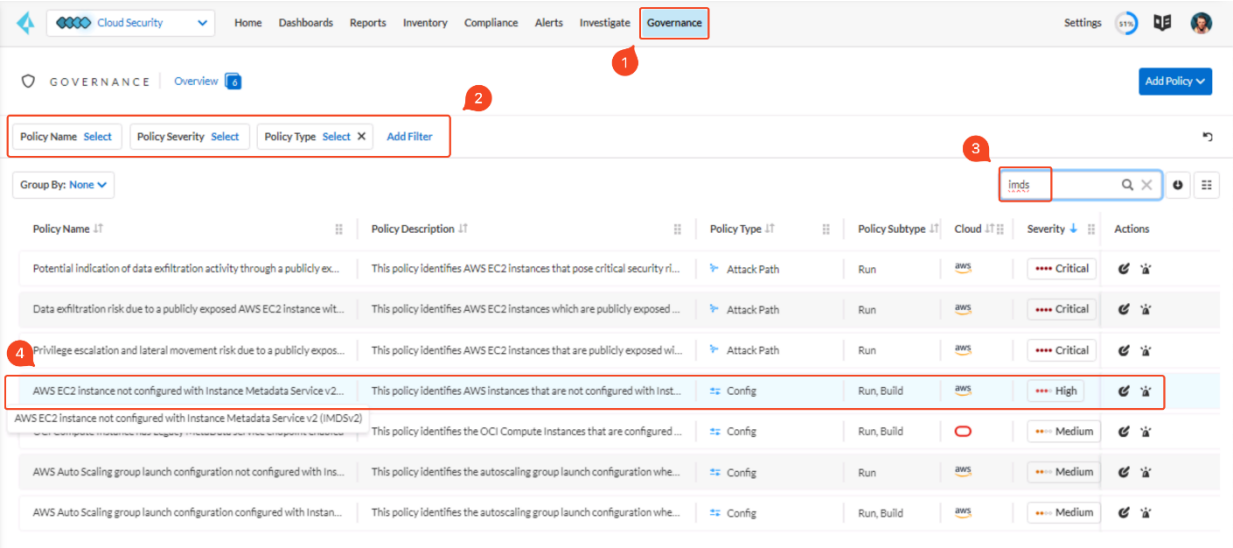
---------- Task 4: Looking into Prisma Cloud Governance & Policy ----------

In Prisma Cloud, a policy is a set of one or more constraints or conditions that must be adhered to. Prisma Cloud provides predefined policies for configurations and access controls that adhere to established security best practices such as Otoritas Jasa Keuangan (OJK) 38 POJK.03 206, PCI, GDPR, ISO 27001:2013, NIST, and a larger set of policies that enable you to validate security best practices with an impact beyond regulatory compliance. These Prisma Cloud default policies cannot be modified.

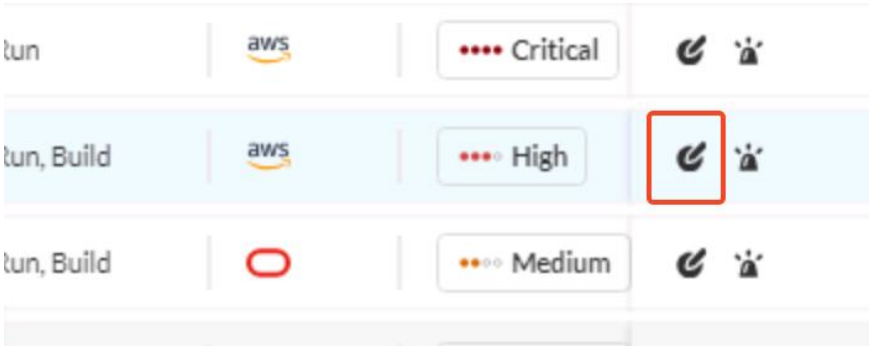
In addition to these predefined policies, you can create custom policies to monitor for violations and enforce your organizational standards. You can use the Default policies as templates to create custom policies. After you set up the policies, any new or existing resources that violate these policies are automatically detected.

Prisma Cloud includes out-of-the-box (OOTB) policies that are part of the Prisma Cloud Recommended Policies Pack.

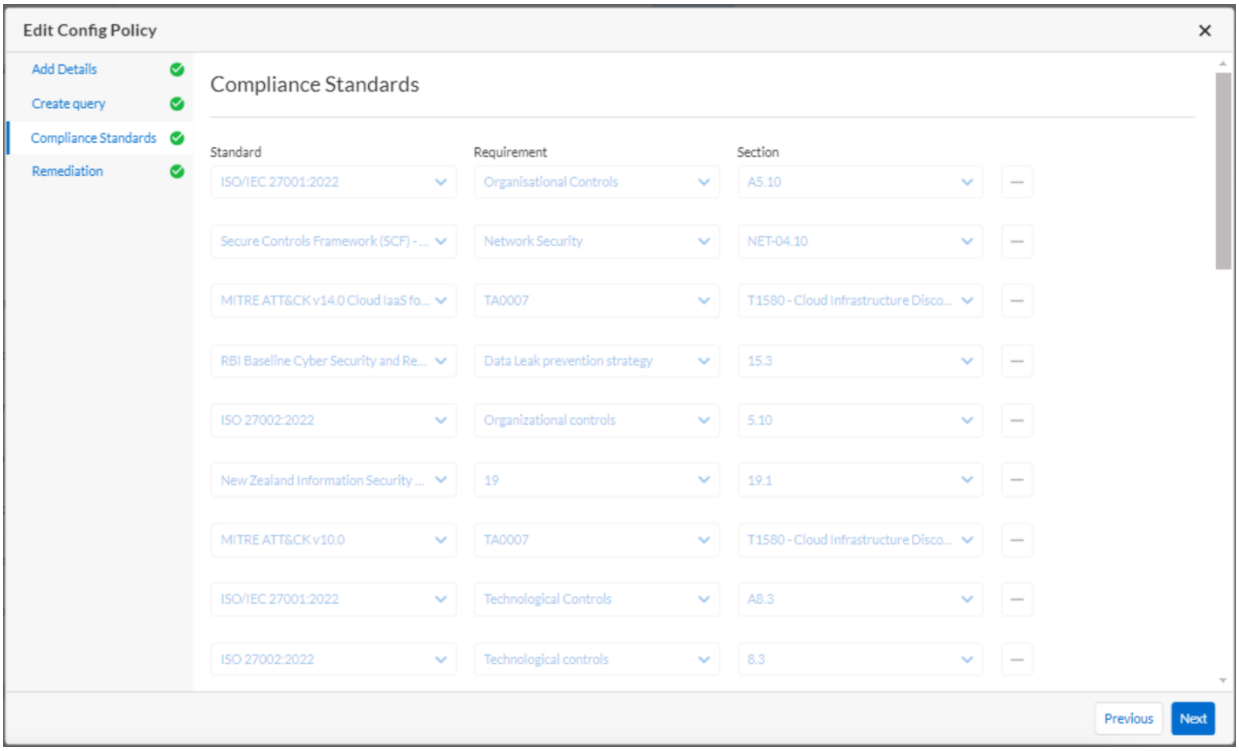
Step 1. In Prisma Cloud Enterprise Edition, click on Governance.



Step 2. Make sure the filters are cleared, type in "imds" into the search bar, and click on the Edit icon for the policy **"AWS EC2 instance not configured with Instance Metadata Service v2 (IMDSv2)"**.



Step 3. On the popped-out window, run through the policy description, then click Next.
Step 4. On the query section, notice that the query has been configured as this is an OOTB policy. Then, click Next.



Step 5. In the remediation section, the recommendation for Remediation has been provided as a manual procedure to remediate if there is a policy violation. CLI command has also been configured, where a CLI command will be provided to remediate the misconfiguration if there is a violation. Click "X" to close the window.

Prisma Cloud Compliance Overview

The Compliance Overview is a dashboard that provides a snapshot of your overall compliance posture across various compliance standards.

Use the Compliance Dashboard as a tool for risk oversight across all the supported cloud platforms and gauge the effectiveness of the security processes and controls you have implemented to keep your enterprise secure. You can also create compliance reports and run them immediately, or schedule them regularly to measure your compliance over time.

The Compliance Dashboard supports you whether you've spent a lot of time designing and establishing internal regulations and devising the right policies, or you use the built-in regulatory compliance standards available on Prisma Cloud.

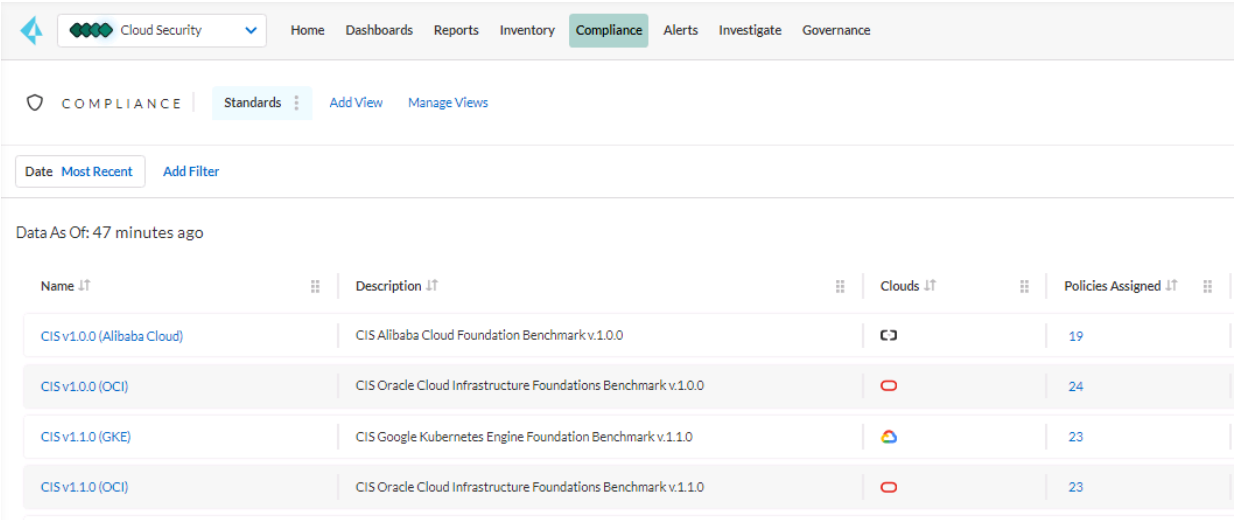
You can also find the list of compliance standards that Prisma Cloud supports here

In this activity, you will:

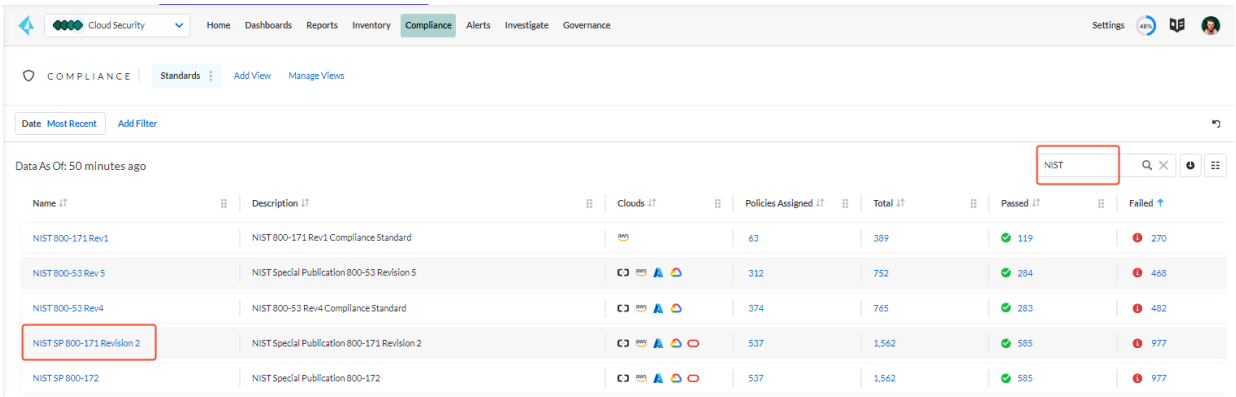
- Review Compliance Overview in Prisma Cloud Enterprise Edition
- Schedule and generate compliance reports for internal consumption

Note: This is a standalone activity and is not dependent on other activities.

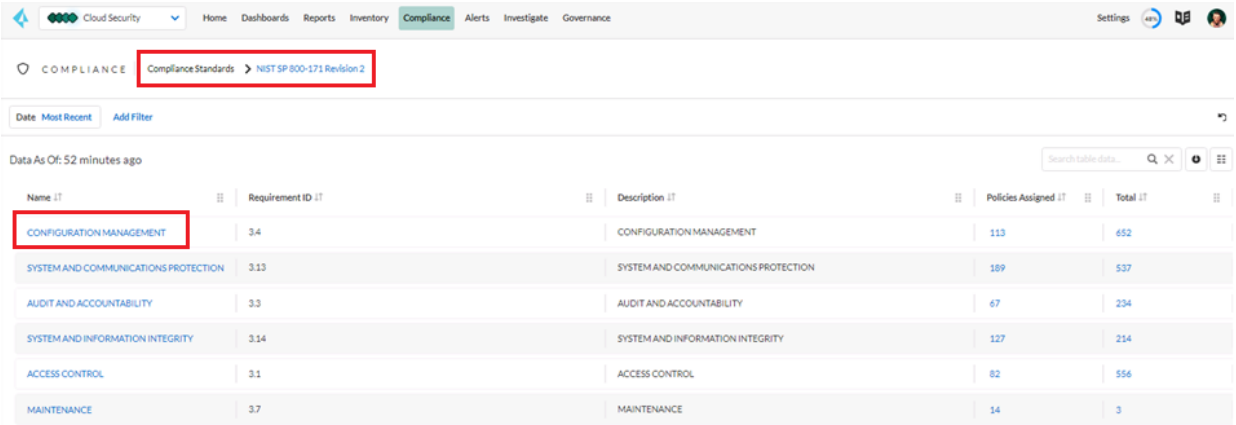
Step 1. Go to **Prisma Cloud Enterprise > Cloud Security > Compliance**
Step 2. Here you can see a list of compliance standards supported by Prisma Cloud out of the box:



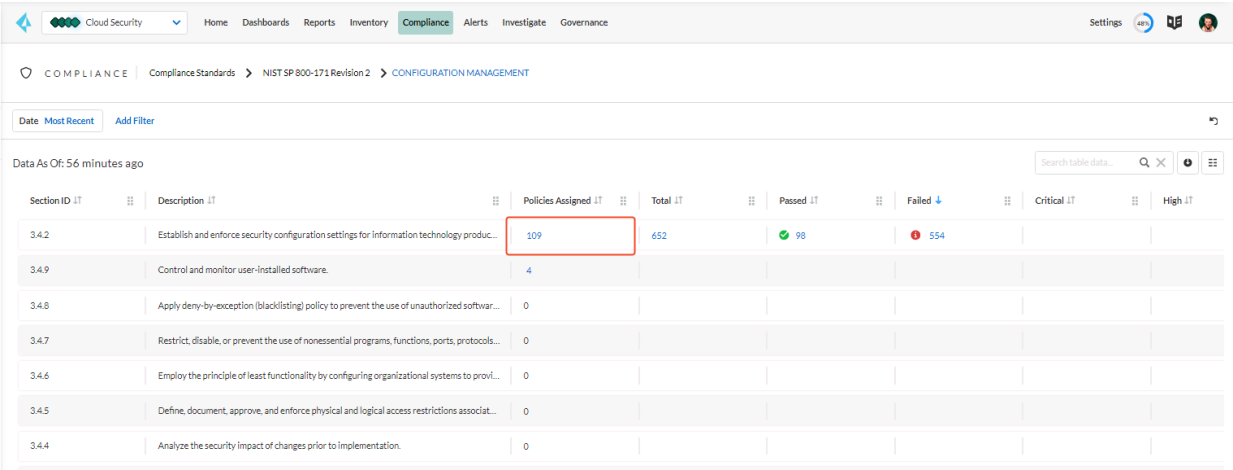
Step 3. Type **"NIST"** in the search bar in the top right corner to filter the compliance standards. **Click** on **"NIST SP 800-171 Revision 2".**



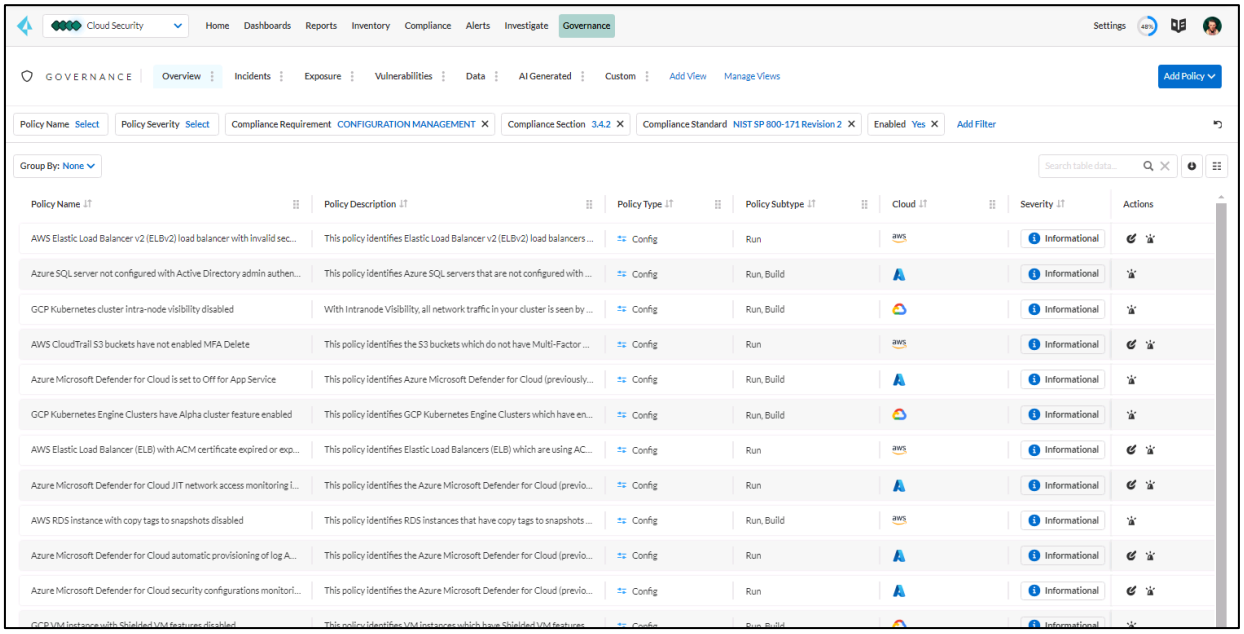
Step 4. On the next page, you can see how the compliance standard is being structured. This is based on the actual compliance requirement, and Prisma Cloud maps the policies according to each section of the compliance requirement. **Click** on **"CONFIGURATION MANAGEMENT"**.



Step 5. On the next page, you can also see how policies are mapped to each sub-section of the compliance standard. **Click** on the numbers under **Policies Assigned**, the same row as section **3.4.2**.



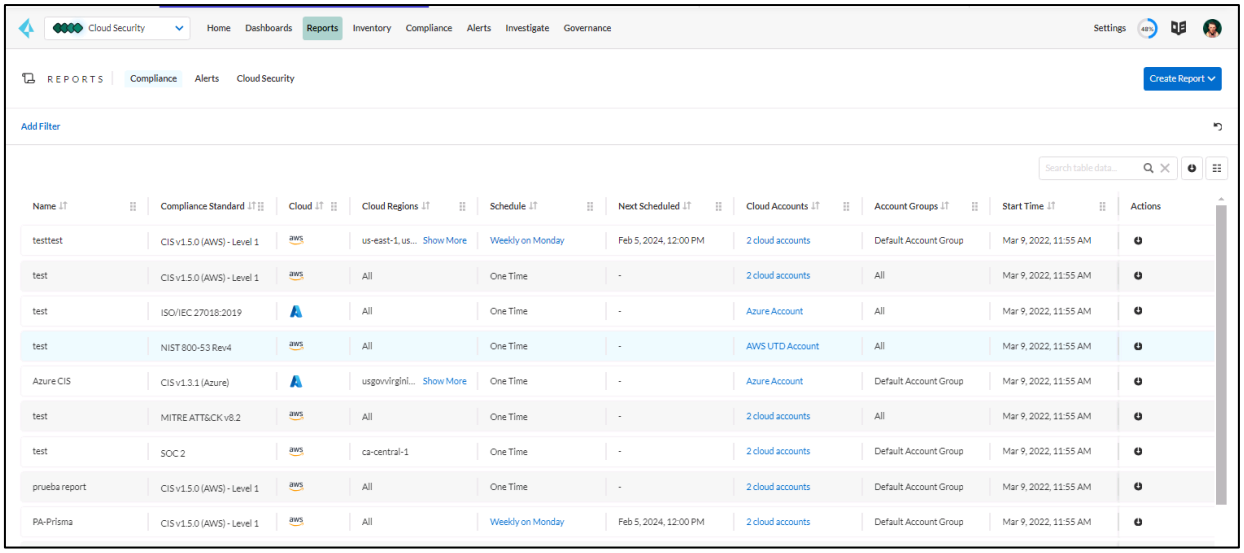
Step 6. On the next page, you will be able to see all the policies that are mapped to this particular sub-section. This allows you to understand how all the policies are built into the compliance requirement and how Prisma Cloud can assist organizations with their compliance with certain standards or regulatory requirements.



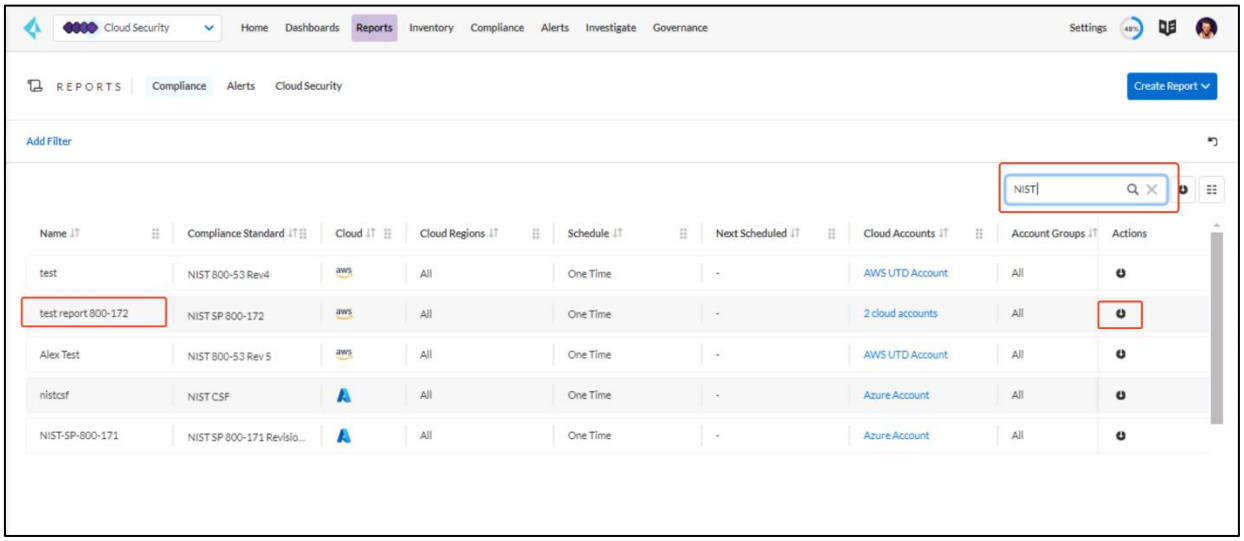
Download Compliance Report

Note: The lab uses a read-only user, which doesn't have access to generate a compliance report. Therefore, we'll only run through the steps to download a compliance report.

Step 1. Go to **Prisma Cloud Enterprise > Cloud Security > Reports**
Step 2. On this page, you will see all the different reports created by existing users or yourself, either for one-time usage or a regular schedule.



Step 3. On the search bar, type **"NIST"**. Click on the **Download** icon in the Action column to download the report.



Note: As you're accessing Prisma Cloud via a full-screen remote desktop, you might not be able to view the downloaded document. For a NIST sample report, refer to a sample document here.

Note: You can schedule a compliance report to be sent to specific teams in regular basis (weekly, daily, etc).