

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.

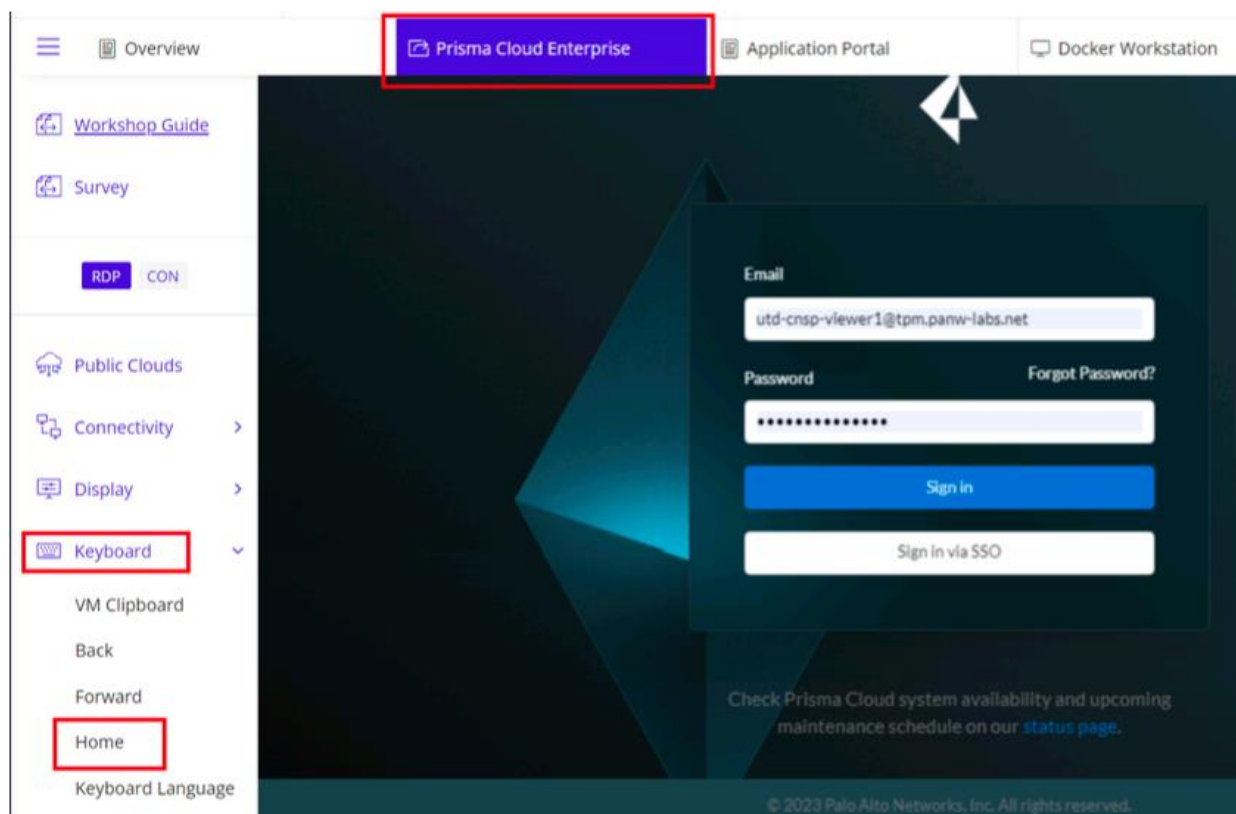
In this activity, you will:

- 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 -----

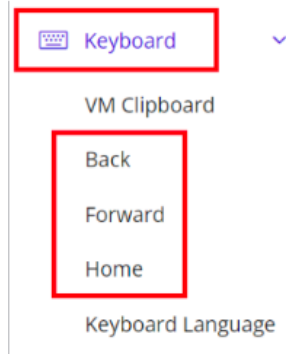
Step 1. Click on the **Prisma Cloud Enterprise** tab to open the demo tenant login.



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

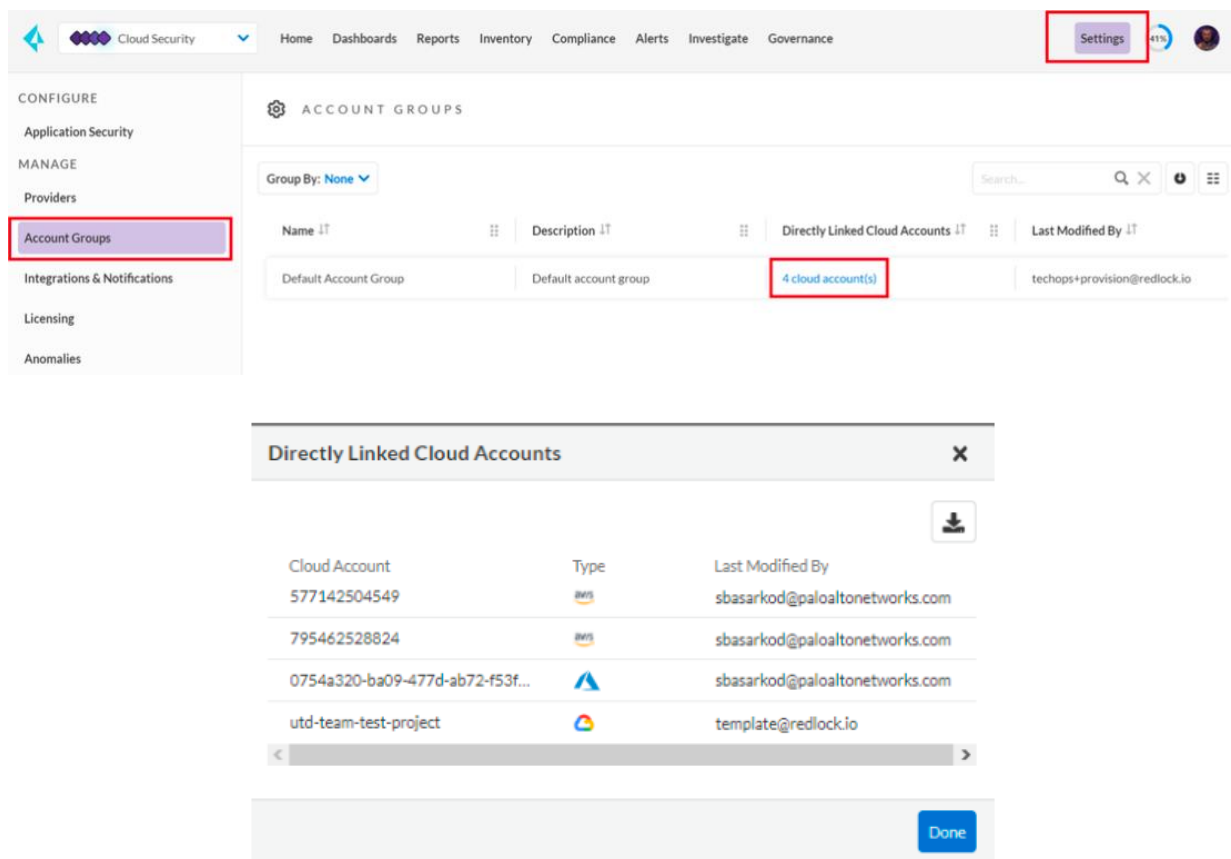
NOTE: If you see a page expired message then **refresh** the web page by clicking on the **Home button** as highlighted in the screen capture.

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.

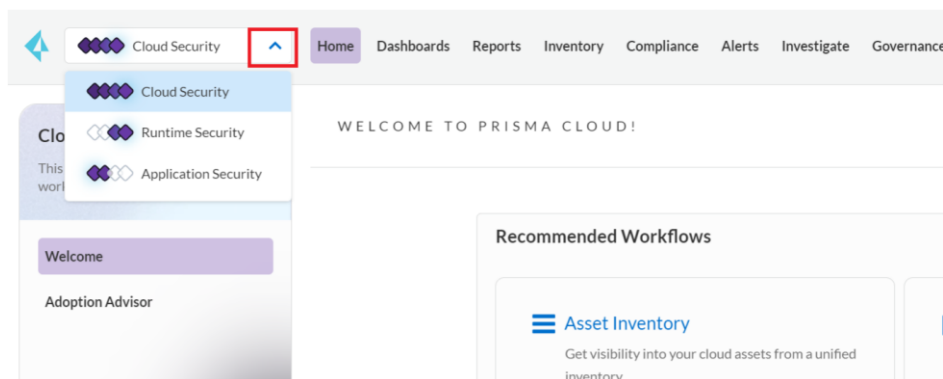
NOTE: The Prisma Cloud Enterprise Edition account used in this lab is read-only, it does not have full access to the Prisma Cloud Service, and access to some functions is denied. This account cannot change the configuration of the associated Prisma Cloud Services.

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

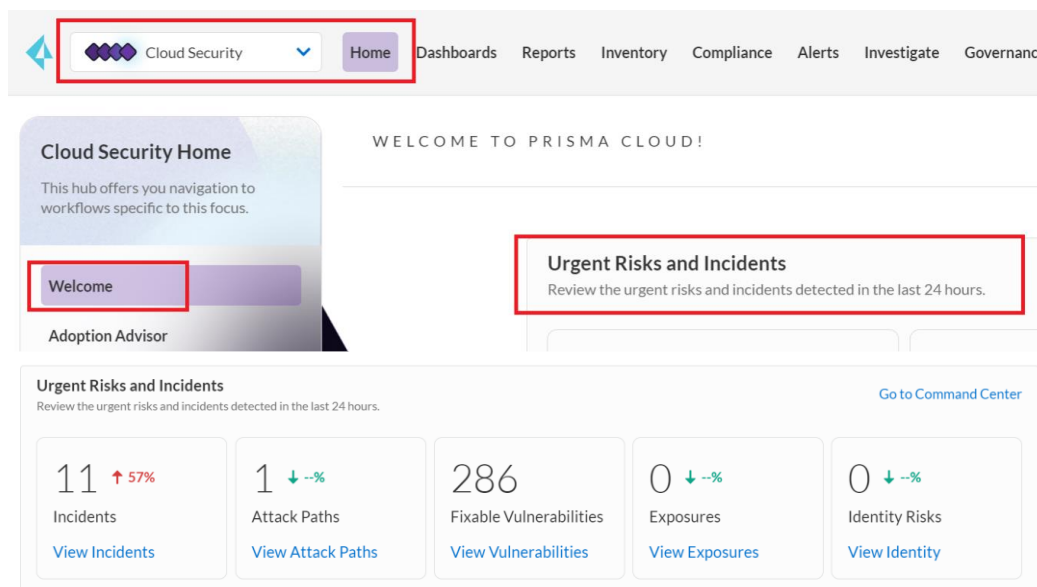
Step 1. In this task, we will explore various parts of the UI within Prisma Cloud that provide rich contextualized information correlated from various data sources within Prisma Cloud. For example, the **Dashboards** are meant to be a starting point for users in real-world situations to get an overview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

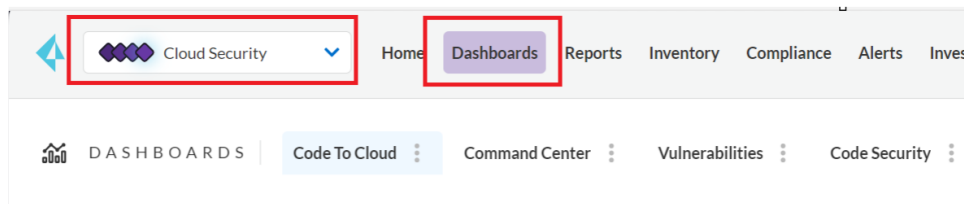
Step 2. When you first log in to Prisma Cloud, from the top left corner, you can select one of the 3 options for your current view: **Cloud Security**, **Runtime Security**, and **Application Security**. To get started, select **Cloud Security**.



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.**

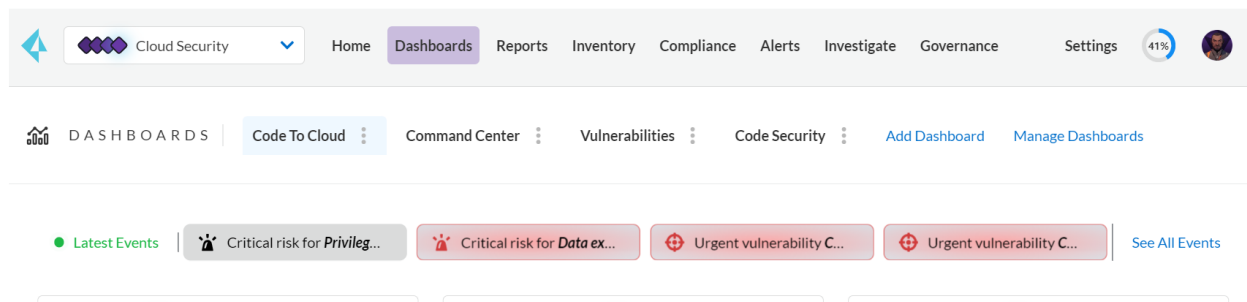


Step 4. When you select **Prisma Cloud > Cloud Security > Dashboards**, by default you will be able to see four dashboards and also the **Latest Events** section.

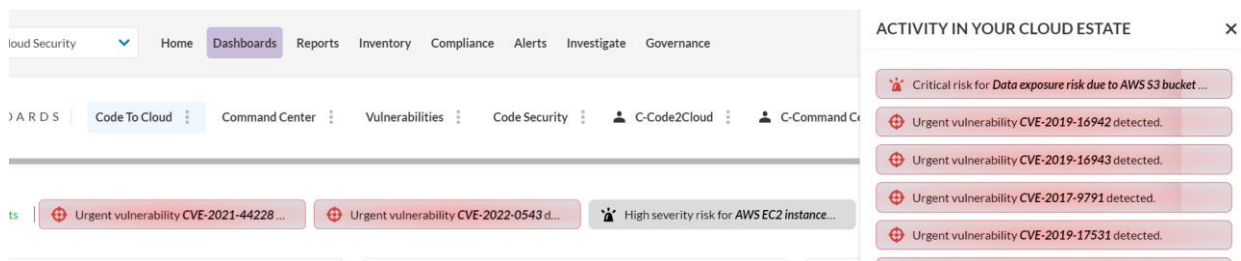


Step 5. Latest Events (Not Visible):

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

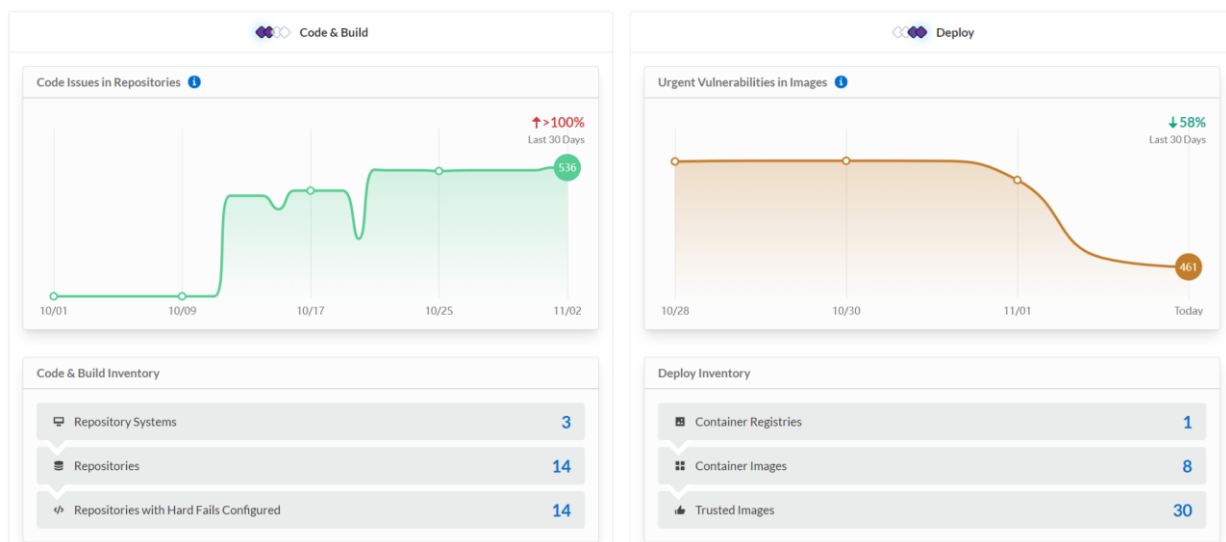


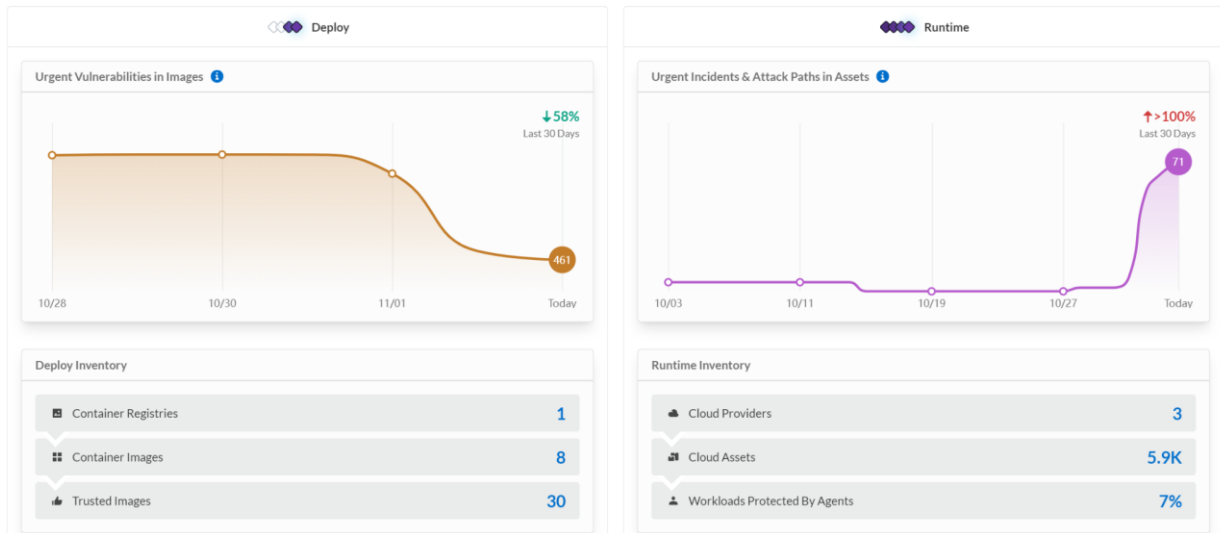
- b) Clicking on **See All Events** will open up all the events



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)

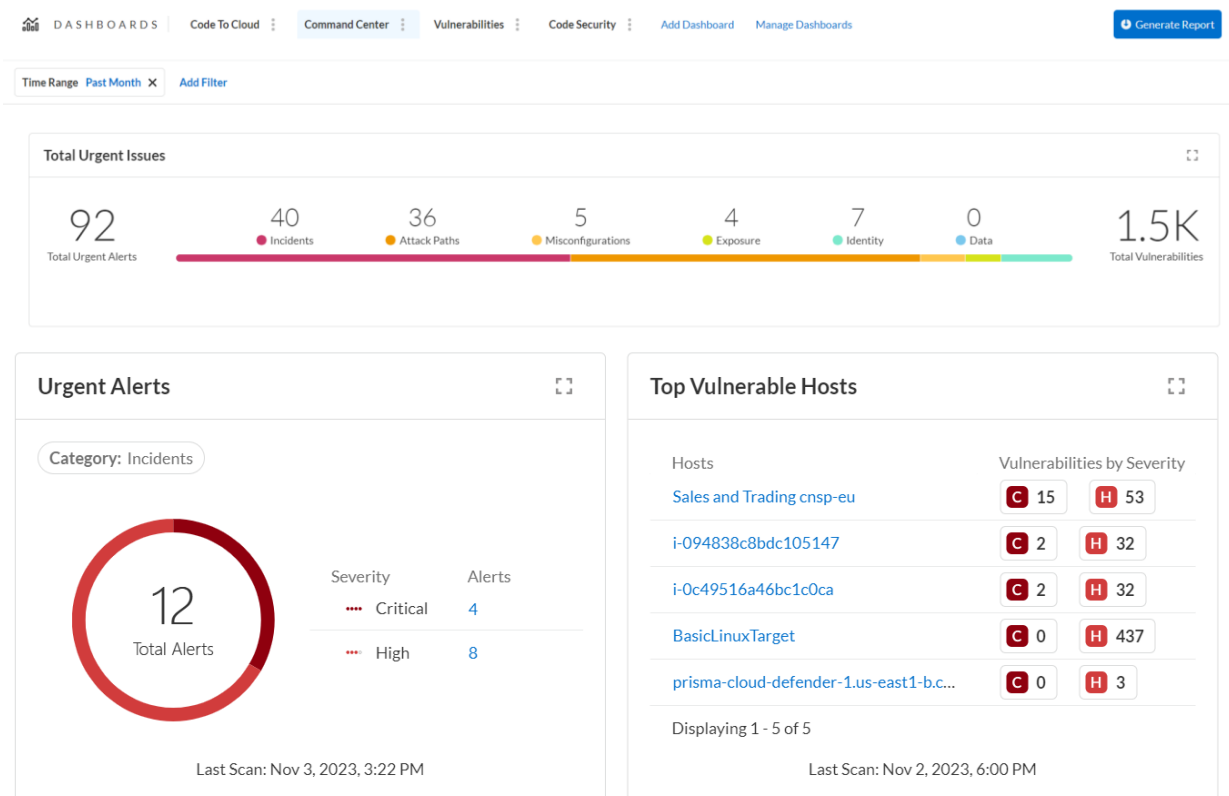


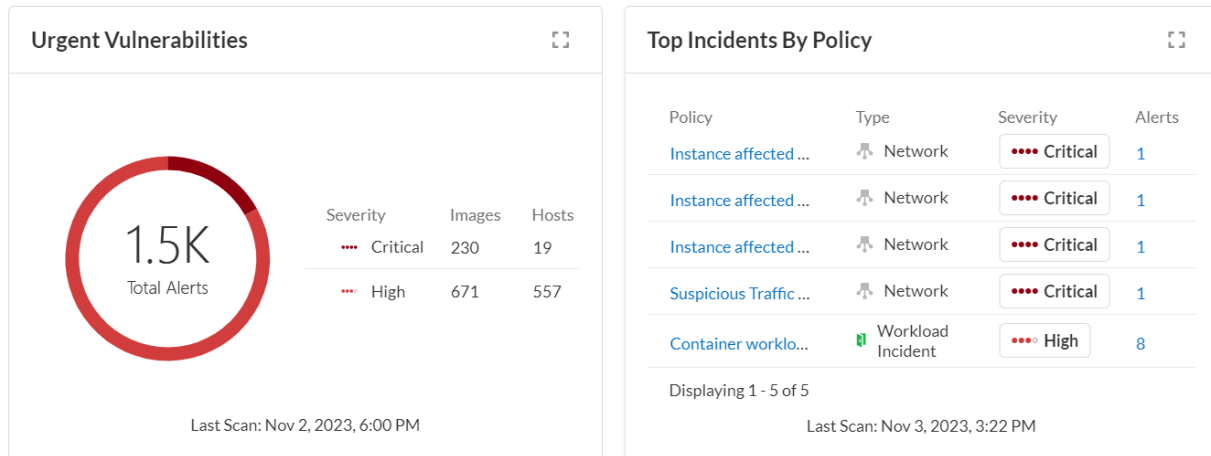


- b) Clicking on items such as **Repository Systems**, **Repositories**, **Container images**, **Cloud Assets** etc will take you to their respective pages within Prisma Cloud. The Dashboard conveniently provides all things in one place.

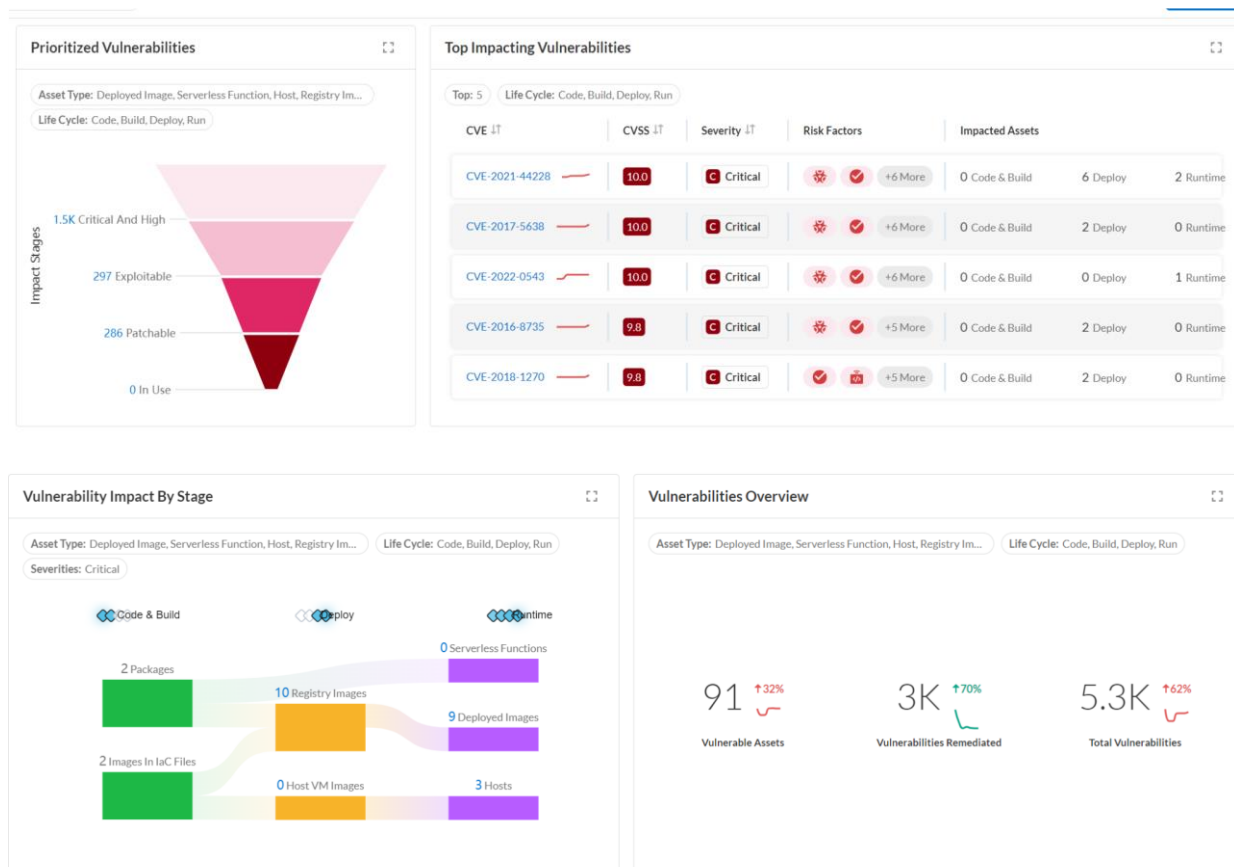
Step 7. Command Center Dashboard (Not Visible):

- 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.

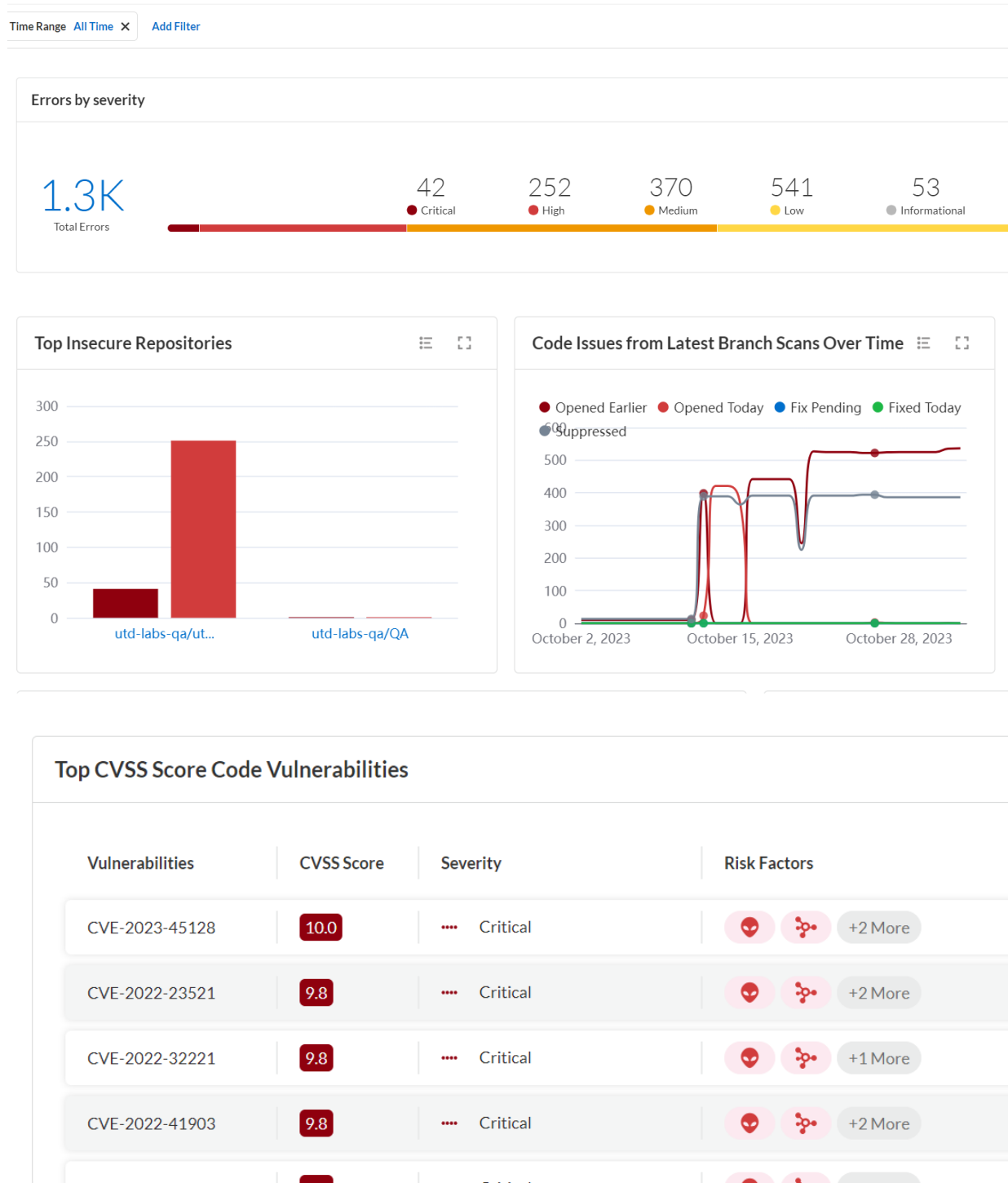




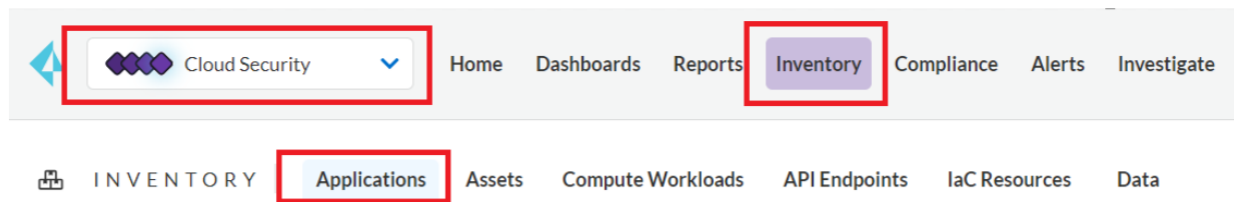
Step 8. Vulnerabilities Dashboard (Visible): This provides an overview of the current vulnerabilities that exist across your system. A modified version of this dashboard should be visible to you in the lab.



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.

Application Name payment@finance-eks-cluster	aws	Business Criticality High	Environment Production	Owner sbasarkod	Assets With Critical ... 2	Assets 14
Asset Class Network	aws	Business Criticality High	Environment Production	Owner sbasarkod	Assets With Critical ... 0	Assets 9
Asset Class Compute	aws	Business Criticality High	Environment Production	Owner sbasarkod	Assets With Critical ... 2	Assets 3
Asset Class Storage	aws	Business Criticality High	Environment Production	Owner sbasarkod	Assets With Critical ... 0	Assets 2





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

INVENTORY Applications Assets Compute Workloads API Endpoints IaC Resources Data			
Date: Most Recent Add Filter			
Cards Table Group By: Cloud Type Data As Of: 13 minutes ago 5,880 Total Assets on 4 Clouds			
AZURE	Assets with Alerts 559 0 1 10 518 59	Assets with Vulnerabilities	Assets 832 View Alerts →
OTHER	Assets with Alerts 28 0 28 0 0 0	Assets with Vulnerabilities 39 C 35 H 38 M 38 L 23	Assets 41 View Alerts →
GCP	Assets with Alerts 89 0 1 1 83 84	Assets with Vulnerabilities 1 C 0 H 1 M 1 L 1	Assets 476 View Alerts →
AWS	Assets with Alerts 342 10 38 93 206 111	Assets with Vulnerabilities 4 C 3 H 4 M 4 L 4	Assets 4.5K View Alerts →

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

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







42 Total Assets

 Container Images	Cloud providers	Total images 38	Vulnerable images 15	→
 Hosts	Cloud providers  	Total hosts 4	Vulnerable hosts 3	→

INVENTORY | Compute Workloads > **Container Images**

Add Filter

Lifecycle stages **All stages** Build Deploy Run 38 Total Container Images

 vulfocus/log4j2-rce-2021-12-09:1	<div>1 total images</div> <div>  Code & Build 0  Deploy 1  Run 0 </div>	Impactful vulnerabilities 40 / 456 total
 jrrdev/cve-2017-5638:struts-2.3.16.1	<div>Stages</div> <div>  Deploy </div>	Impactful vulnerabilities 36 / 154 total

INVENTORY | Compute Workloads > **Hosts**

Add Filter

4 Total Hosts

 ip-172-20-1-164.ec2.internal	<div>Search...</div> <div> <div>Total vulnerabilities</div> <div>Critical & High</div> <div>Exploitable</div> <div>Patchable</div> </div> <div> <div>252</div> <div>68</div> <div>5</div> <div>5</div> </div>	<div>Sort By: Impactful Vulnerabilities</div> <div>Impactful vulnerabilities 5 / 252 total</div>
---	---	---

- 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

Search...

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

Search table data...

Framework	Total	Pass	Fail	Resources With Code Issues	Resources With Vulnerabilities
Terraform	107	5	102	102	0
CloudFormation	45	6	39	39	0
Kubernetes	28	13	15	15	6
Docker	20	12	8	8	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.

 INVENTORY

Assets

Compute Workloads

API Endpoints















IaC Resources

Data

Time Range

All Time

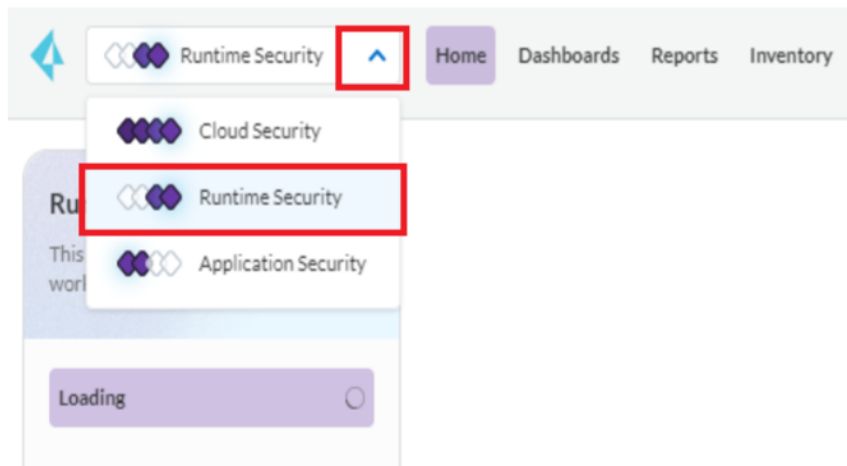
Add Filter

Cloud  	Total Resources  	Public Resources  	Total Objects  	Public Objects  	Sensitive Objects  	Malware 
	19	3	376	49	21	42

Task 3: Runtime Security Overview

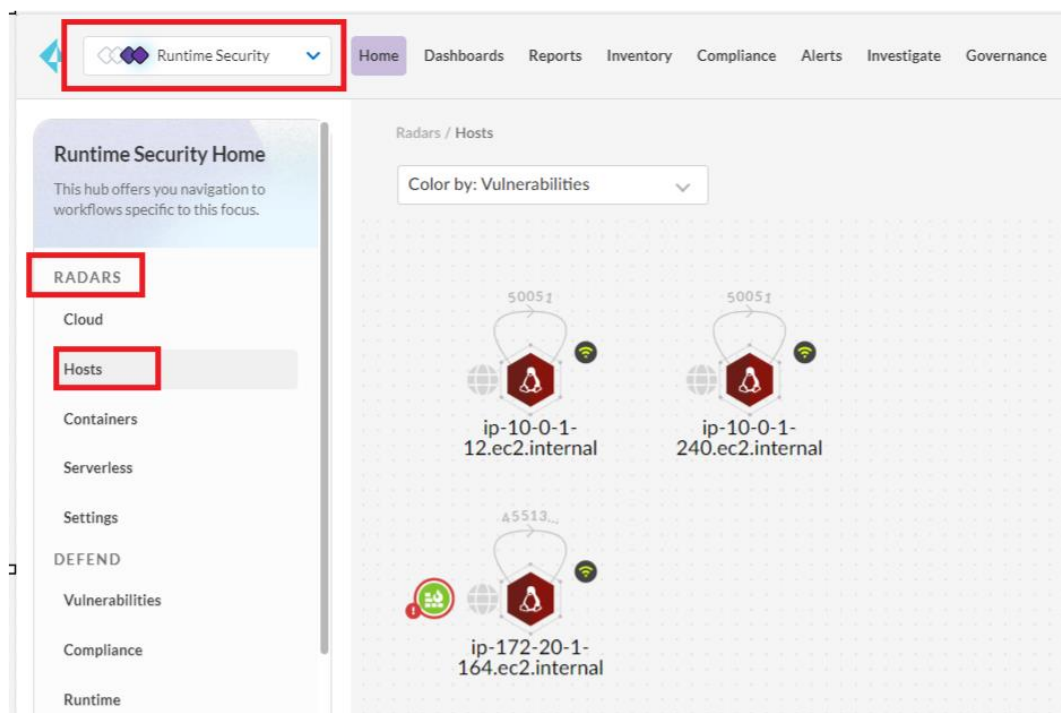
Step 1. This task provides an overview of the Runtime Security section of Prisma Cloud Enterprise Edition. Prisma Cloud Compute Edition is a standalone and self-hosted version of Prisma Cloud Enterprise version's Runtime Security.

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.



ip-172-20-1-164.ec2.internal

Category	Item	Value	Risk Level
Risk summary	Hostname	ip-172-20-1-164.ec2.internal	
	OS distribution	Ubuntu 18.04.6 LTS	
	OS release	bionic	
	Modified	Oct 30, 2023 9:24:08 AM	
Environment	Docker version	24.0.2	
	Provider	aws	
	Type	host	
Vulnerabilities	Critical risk	16	Critical risk
	High risk	57	High risk
	Medium risk	121	Medium risk
	Low risk	64	Low risk
Compliance	Critical risk	1	Critical risk
	High risk	22	High risk
	Medium risk	0	Medium risk
Runtime	No events	0	No events
	Forensics	0	Low risk
WAAS	Code Injection	216	Code Injection
	SQL Injection	216	SQL Injection

- 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.

Runtime Security

Home Dashboards Reports Inventory Compliance Alerts Investigate Governance

RADARS

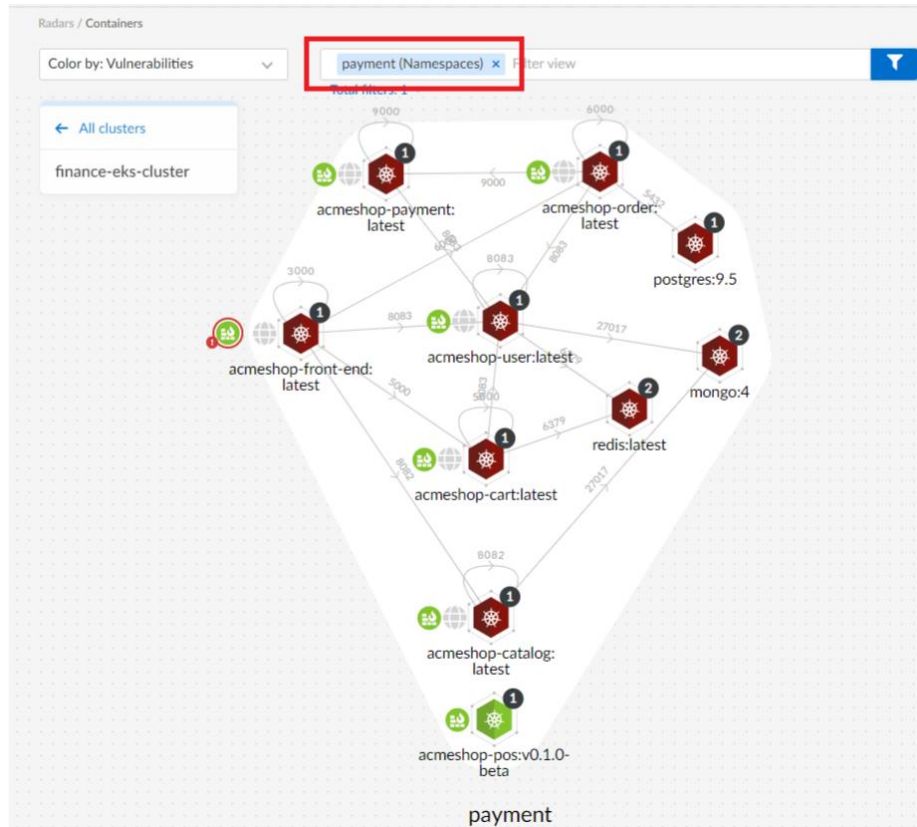
- Cloud
- Hosts
- Containers**
- Serverless
- Settings

Radars / Containers

1 cluster *Filter clusters by keywords and attributes*

finance-eks-cluster

- 2 hosts
- 4 namespaces



Step 4. ATT&CK

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

Runtime Security

Home Dashboards Reports Inventory Compliance Alerts Investigate Governance

WAAS

CNNS

Access

Custom rules

MONITOR

ATT&CK

Events

Runtime

Vulnerabilities

Compliance

WAAS

MANAGE

Cloud accounts

Logs

Defenders

Alerts

Monitor / ATT&CK

ATT&CK Explorer

Correlates audits from cloud native apps secured by Prisma Cloud to the ATT&CK framework

Filter techniques by attributes

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
1105	2233	0	30	6	0
Exploit Public-Facing Application 1105 Events	Access the Kubelet Main API	Abuse Elevation Control Mechanisms	Abuse Elevation Control Mechanisms	Obfuscated Files	Cloud Instance Metadata API
Supply Chain Compromise	Exec Into Container	Account Manipulation	Exploitation for Privilege Escalation 30 Events	Hijack Execution Flow	Credential Dumping

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

Monitor / Events

Containers: Container audits 29, CNNS for containers 0, **WAAS for containers 252K+**, Trust audits 0, Kubernetes audits 0, Admission audits 0, Docker audits 0

Hosts: App-Embedded audits 0, WAAS for App-Embedded 0, Host audits 0, CNNS for hosts 0, WAAS for hosts 432, Host log inspection 0, Host file integrity 0, Host activities 730

Serverless: Serverless audits 0, WAAS for serverless 0

Agentless: WAAS for agentless 0

WAAS audits for containers

Client requests triggering one or more WAAS protections policies generate WAAS audits and an action is taken based on the preconfigured action.

Filter audits by keywords and attributes

By default, a time filter of 3 months is applied, even if not explicitly specified

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

Monitor / Runtime

Incident Explorer Container models Host observations App-Embedded observations Image analysis sandbox

Active incidents

Sequence of events collected by the runtime and firewall sensors, which in the aggregate, point to suspicious activity and a potentially unfolding attack.

Incident Explorer raises a single incident per incident type per resource per 24 hour period... [Show more](#)

Filter incidents by keywords and attributes

22 total entries (filtered)

Category	Type	Hostname	Cluster	App ID	Impacted	Date
Reverse Shell	Container	ip-172-20-1-164.ec2.i...			webapp:latest	Nov 2, 2023 10:00:07
Reverse Shell	Container	ip-172-20-1-164.ec2.i...			webapp:latest	Nov 2, 2023 8:00:07
Reverse Shell	Container	ip-172-20-1-164.ec2.i...			webapp:latest	Nov 2, 2023 3:00:07
Reverse Shell	Container	ip-172-20-1-164.ec2.i...			webapp:latest	Nov 2, 2023 1:00:07
Reverse Shell	Container	ip-172-20-1-164.ec2.i...			webapp:latest	Nov 1, 2023 11:00:07

Reverse Shell incident indicates that an attacker might have gained interactive shell access to a host or container through a shell on the target connected to a remote machine. [Learn more](#)

View live forensic

Incident ID: 6543b977c3f849a66d#3401

Host name: ip-172-20-1-164.ec2.internal

Container name: /youthful_villani (Removed)

Image name: webapp:latest

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

Monitor / Vulnerabilities

Vulnerability Explorer Code repositories Images Hosts Functions CVE viewer VMware Tar

Vulnerability Explorer

Survey the vulnerabilities across your environment.

Filter by Filter by CVE ID, collections, or CVE attributes

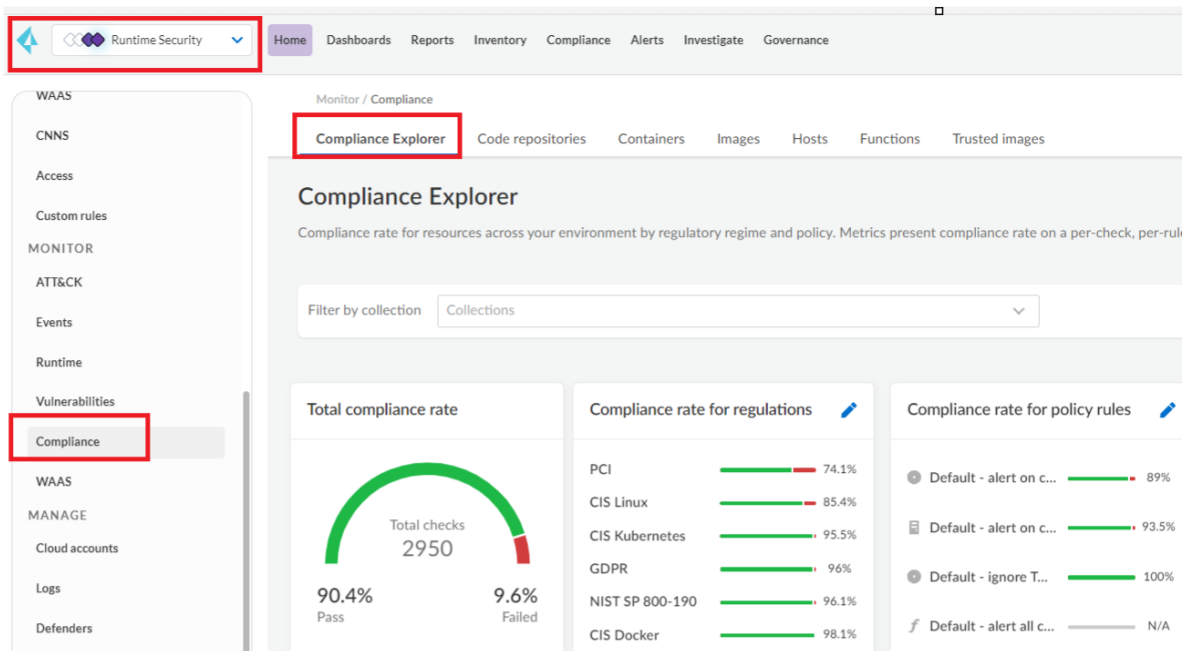
Vulnerability (CVE) results

Deployed images Registry images Hosts Functions

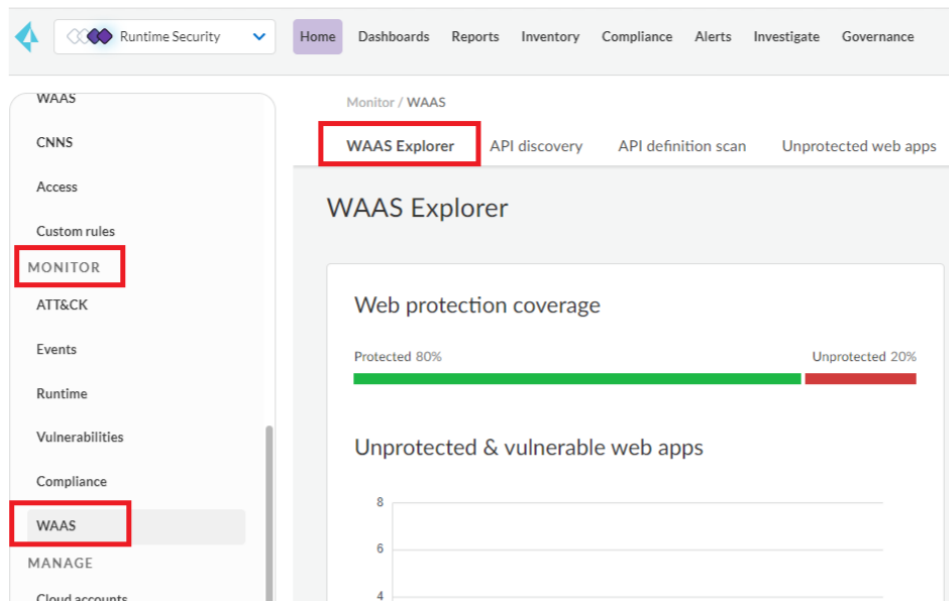
The attributes for each CVE display the greatest risk across your entire environment. The values do not consider filters.

ID	Highest risk score	Highest CVE risk factors	Highest environme...	Highest severity
CVE-2023-44487	91	6	5	High
CVE-2023-29405	89	7	4	Critical

- 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

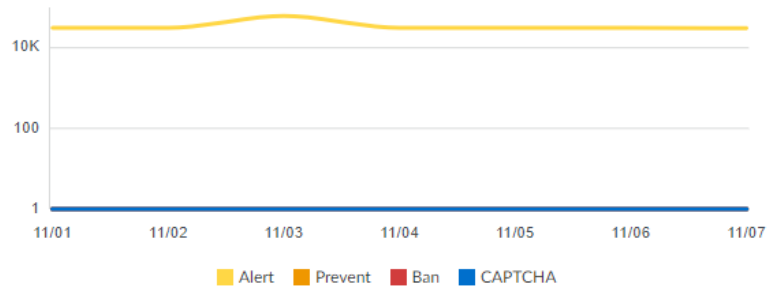


Inspected traffic by WAAS

1.9M
Requests

18.57GB
Bytes

WAAS actions by effect

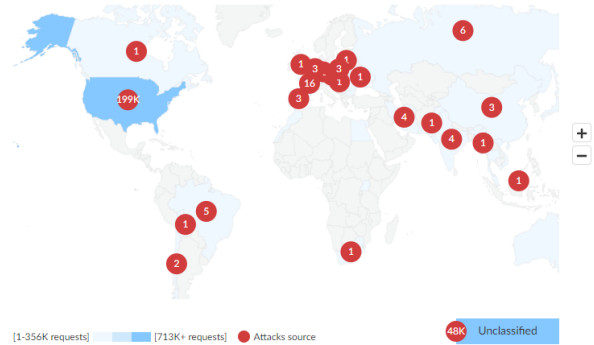


Event traffic sources

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



Step 4. On the query section, notice that the query has been configured as this is an OOTB policy. Then, click Next.

Standard	Requirement	Section
ISO/IEC 27001:2022	Organisational Controls	A5.10
Secure Controls Framework (SCF) - ...	Network Security	NET-04.10
MITRE ATT&CK v14.0 Cloud IaaS fo...	TA0007	T1580 - Cloud Infrastructure Disco...
RBI Baseline Cyber Security and Re...	Data Leak prevention strategy	15.3
ISO 27002:2022	Organizational controls	5.10
New Zealand Information Security ...	19	19.1
MITRE ATT&CK v10.0	TA0007	T1580 - Cloud Infrastructure Disco...
ISO/IEC 27001:2022	Technological Controls	A8.3
ISO 27002:2022	Technological controls	8.3

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](#)

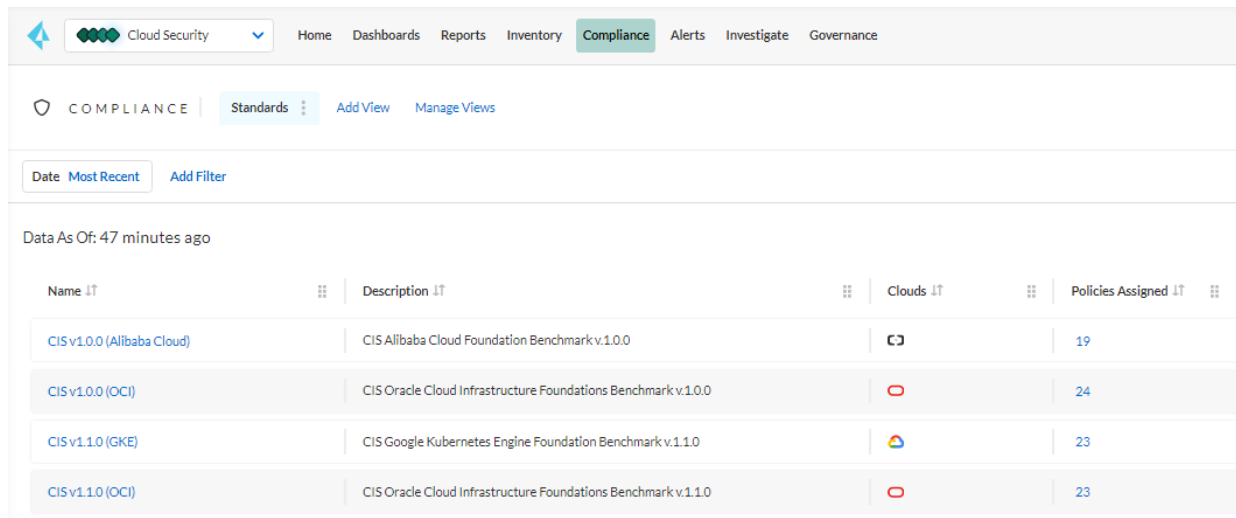
In this activity, you will:

- 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.

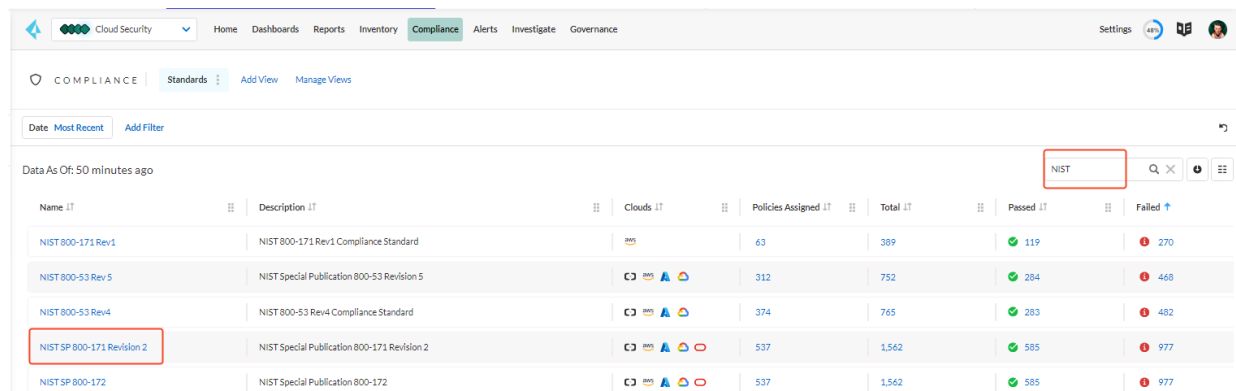
Step 1. Go to Prisma Cloud Enterprise > Cloud Security > Compliance

Step 2. Here you can see a list of compliance standards supported by Prisma Cloud out of the box:



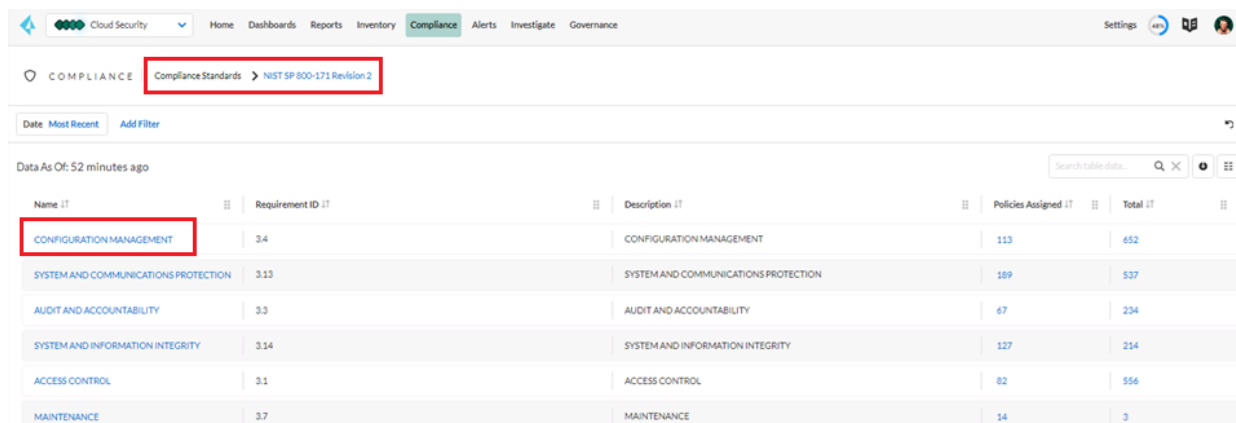
Name	Description	Clouds	Policies Assigned
CIS v1.0.0 (Alibaba Cloud)	CIS Alibaba Cloud Foundation Benchmark v.1.0.0		19
CIS v1.0.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.0.0		24
CIS v1.1.0 (GKE)	CIS Google Kubernetes Engine Foundation Benchmark v.1.1.0		23
CIS v1.1.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.1.0		23

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".



Name	Description	Clouds	Policies Assigned	Total	Passed	Failed
NIST 800-171 Rev1	NIST 800-171 Rev1 Compliance Standard		63	389	119	270
NIST 800-53 Rev5	NIST Special Publication 800-53 Revision 5		312	752	284	468
NIST 800-53 Rev4	NIST 800-53 Rev4 Compliance Standard		374	765	283	482
NIST SP 800-171 Revision 2	NIST Special Publication 800-171 Revision 2		537	1,562	585	977
NIST SP 800-172	NIST Special Publication 800-172		537	1,562	585	977

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".



Name	Requirement ID	Description	Policies Assigned	Total
CONFIGURATION MANAGEMENT	3.4	CONFIGURATION MANAGEMENT	113	652
SYSTEM AND COMMUNICATIONS PROTECTION	3.13	SYSTEM AND COMMUNICATIONS PROTECTION	189	537
AUDIT AND ACCOUNTABILITY	3.3	AUDIT AND ACCOUNTABILITY	67	234
SYSTEM AND INFORMATION INTEGRITY	3.14	SYSTEM AND INFORMATION INTEGRITY	127	214
ACCESS CONTROL	3.1	ACCESS CONTROL	82	556
MAINTENANCE	3.7	MAINTENANCE	14	3

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.

Section ID	Description	Policies Assigned	Total	Passed	Failed	Critical	High
3.4.2	Establish and enforce security configuration settings for information technology produc...	109	652	98	554		
3.4.9	Control and monitor user-installed software.	4					
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized softwar...	0					
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols...	0					
3.4.6	Employ the principle of least functionality by configuring organizational systems to provi...	0					
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associat...	0					
3.4.4	Analyze the security impact of changes prior to implementation.	0					

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.

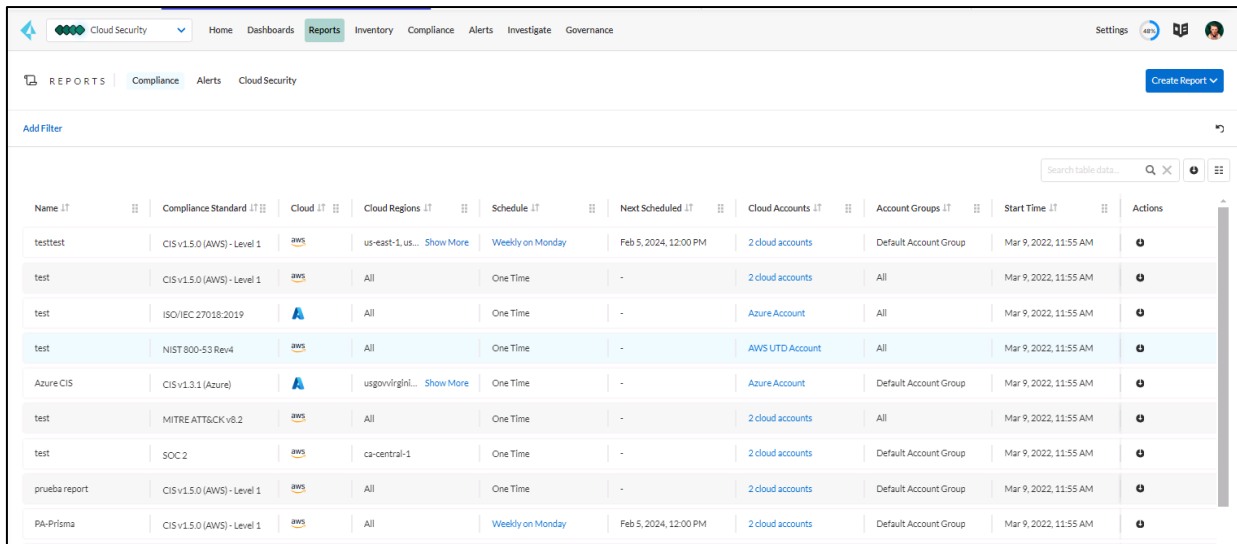
Policy Name	Policy Description	Policy Type	Policy Subtype	Cloud	Severity	Actions
AWS Elastic Load Balancer v2 (ELBv2) load balancer with invalid sec...	This policy identifies Elastic Load Balancer v2 (ELBv2) load balancers ...	Config	Run	AWS	Informational	
Azure SQL server not configured with Active Directory admin authen...	This policy identifies Azure SQL servers that are not configured with ...	Config	Run, Build	Azure	Informational	
GCP Kubernetes cluster intra-node visibility disabled	With Intranode Visibility, all network traffic in your cluster is seen by ...	Config	Run, Build	GCP	Informational	
AWS CloudTrail S3 buckets have not enabled MFA Delete	This policy identifies the S3 buckets which do not have Multi-Factor ...	Config	Run	AWS	Informational	
Azure Microsoft Defender for Cloud is set to Off for App Service	This policy identifies Azure Microsoft Defender for Cloud (previ...	Config	Run, Build	Azure	Informational	
GCP Kubernetes Engine Clusters have Alpha cluster feature enabled	This policy identifies GCP Kubernetes Engine Clusters which have en...	Config	Run, Build	GCP	Informational	
AWS Elastic Load Balancer (ELB) with ACM certificate expired or exp...	This policy identifies Elastic Load Balancers (ELB) which are using AC...	Config	Run	AWS	Informational	
Azure Microsoft Defender for Cloud JIT network access monitoring i...	This policy identifies the Azure Microsoft Defender for Cloud (previ...	Config	Run	Azure	Informational	
AWS RDS instance with copy tags to snapshots disabled	This policy identifies RDS instances that have copy tags to snapshots ...	Config	Run, Build	AWS	Informational	
Azure Microsoft Defender for Cloud automatic provisioning of log A...	This policy identifies the Azure Microsoft Defender for Cloud (previ...	Config	Run	Azure	Informational	
Azure Microsoft Defender for Cloud security configurations monitori...	This policy identifies the Azure Microsoft Defender for Cloud (previ...	Config	Run	Azure	Informational	
GCP VM instances with Shared VM features disabled	This policy identifies VM instances which have Shared VM features...	Config	Run, Build	GCP	Informational	

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.

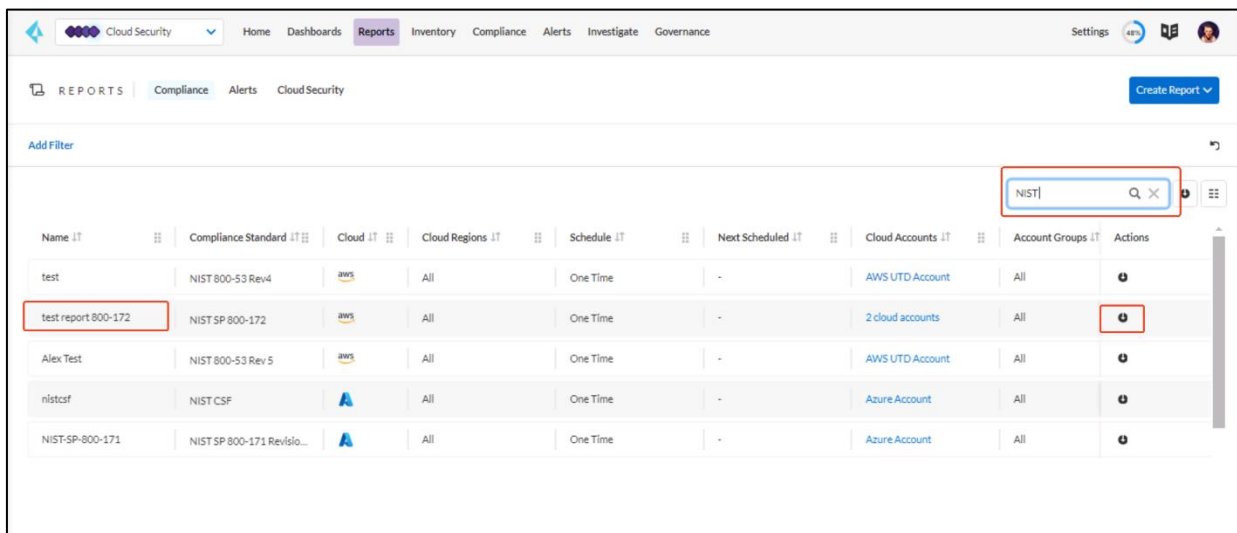
Step 1. Go to **Prisma Cloud Enterprise > Cloud Security > Reports**

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.



Name	Compliance Standard	Cloud	Cloud Regions	Schedule	Next Scheduled	Cloud Accounts	Account Groups	Start Time	Actions
testtest	CIS v1.5.0 (AWS) - Level 1	aws	us-east-1, us... Show More	Weekly on Monday	Feb 5, 2024, 12:00 PM	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
test	CIS v1.5.0 (AWS) - Level 1	aws	All	One Time	-	2 cloud accounts	All	Mar 9, 2022, 11:55 AM	
test	ISO/IEC 27018:2019	A	All	One Time	-	Azure Account	All	Mar 9, 2022, 11:55 AM	
test	NIST 800-53 Rev4	aws	All	One Time	-	AWS UTD Account	All	Mar 9, 2022, 11:55 AM	
Azure CIS	CIS v1.3.1 (Azure)	A	usgovvirginia... Show More	One Time	-	Azure Account	Default Account Group	Mar 9, 2022, 11:55 AM	
test	MITRE ATT&CK v8.2	aws	All	One Time	-	2 cloud accounts	All	Mar 9, 2022, 11:55 AM	
test	SOC 2	aws	ca-central-1	One Time	-	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
prueba report	CIS v1.5.0 (AWS) - Level 1	aws	All	One Time	-	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
PA-Prisma	CIS v1.5.0 (AWS) - Level 1	aws	All	Weekly on Monday	Feb 5, 2024, 12:00 PM	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	

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



Name	Compliance Standard	Cloud	Cloud Regions	Schedule	Next Scheduled	Cloud Accounts	Account Groups	Actions
test	NIST 800-53 Rev4	aws	All	One Time	-	AWS UTD Account	All	
test report 800-172	NIST SP 800-172	aws	All	One Time	-	2 cloud accounts	All	
Alex Test	NIST 800-53 Rev 5	aws	All	One Time	-	AWS UTD Account	All	
nistcsf	NIST CSF	A	All	One Time	-	Azure Account	All	
NIST-SP-800-171	NIST SP 800-171 Revisio...	A	All	One Time	-	Azure Account	All	

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).