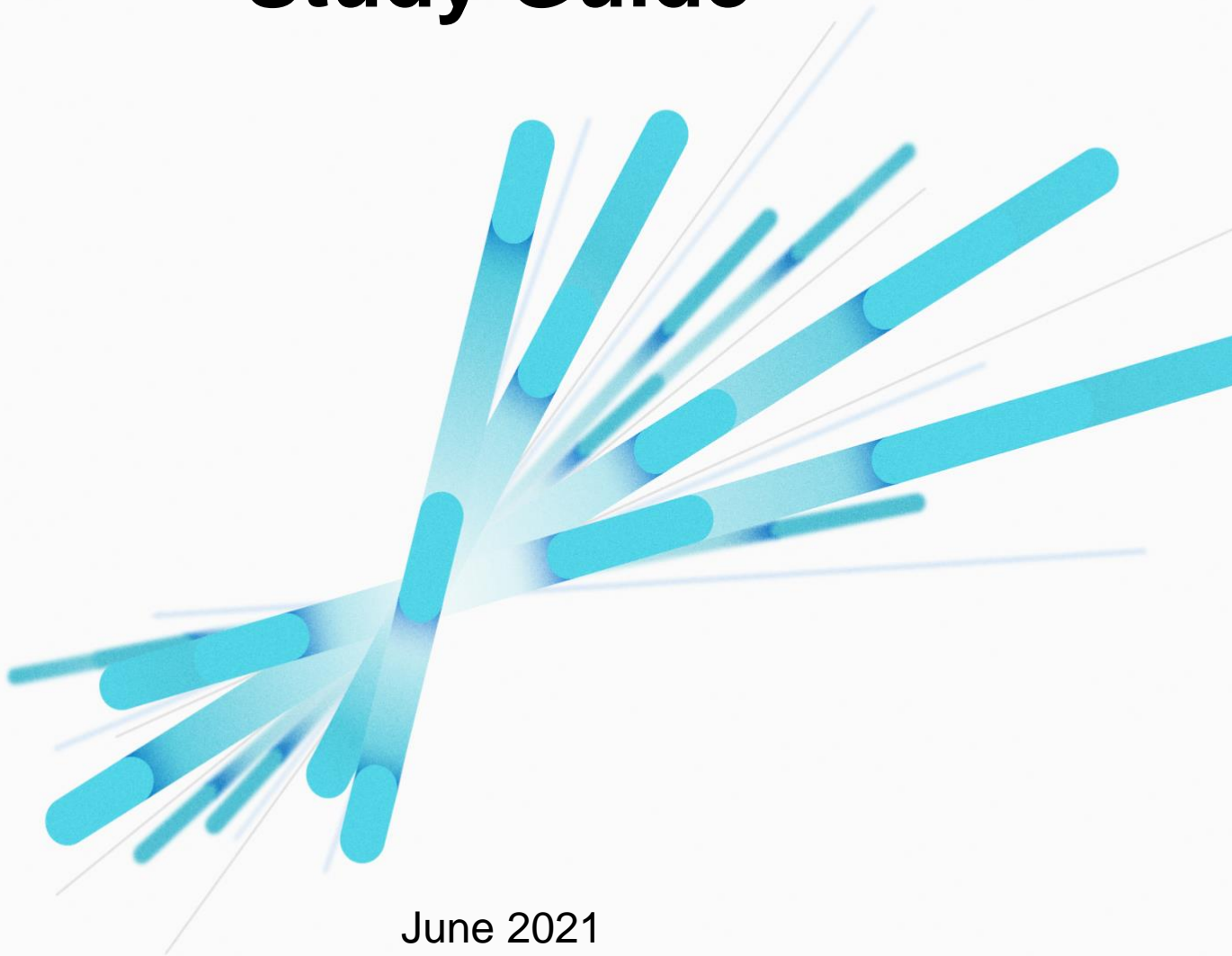




Palo Alto Networks Prisma Certified Cloud Security Engineer Study Guide



June 2021

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2021 Palo Alto Networks – all rights reserved.

Aperture, AutoFocus, GlobalProtect, Palo Alto Networks, PAN-OS, Panorama, Traps, and WildFire are trademarks of Palo Alto Networks, Inc. All other trademarks are the property of their respective owners

Table of Contents

Prisma Certified Cloud Security Engineer Study Guide	5
Overview	5
Exam Format.....	6
How to Take This Exam	6
Preparation Resources.....	6
Exam Domains and Objectives	7
1 Install and Upgrade	7
1.1 Deploy and Manage the Console for the Compute Edition	7
1.2 Deploy and Manage Defenders	8
2 Visibility, Security, Compliance and Data Security	10
2.1 Configure policies	10
2.2 Configure alerting and notifications	12
2.3 Understand third-party integrations	14
2.4 Perform ad hoc investigations	15
2.5 Identify assets in a cloud account.....	18
2.6 Use Prisma Cloud APIs	19
2.7 Remediation.....	19
2.8 Onboarding	22
2.9 Use Data Dashboard features	22
2.10 Assess Data Policies and Alerts	23
3 Cloud Workload Protection Platform	24
3.1 Monitor and protect against image vulnerabilities	24
3.2 Monitor and protect against host vulnerabilities	25
3.3 Monitor and enforce Docker image and container compliance	27
3.4 Monitor and enforce host compliance.....	29
3.5 Monitor and enforce container runtime.....	30
3.6 Configure web-application and API security (WAAS) policies	31
3.7 Monitor and protect against serverless vulnerabilities	32
4 Web Application and API Security (WAAS)	33
4.1 Configure WAAS policies and an App rule	33
4.2 Configure application-firewall settings and exceptions	36
4.3 Investigate WAAS Runtime Audit	39

5 DevSecOps Security (Shift Left)	40
5.1 Implement scanning for IAC templates	40
5.2 Configure policies in the Console for IaC scanning	41
5.3 Integrate Compute scans into CI/CD pipeline	42
5.4 Configure CI policies for Compute scanning	43
6 Prisma Cloud Administration	45
6.1 Onboard accounts	45
6.2 Configure RBAC	46
6.3 Configure the admission controller	47
6.4 Configure logging	48
6.5 Manage enterprise settings	49
6.6 Understand third-party integrations	51
6.7 Leverage Cloud and Compute APIs	53
Sample Questions	55
Answers to Sample Questions	85
Glossary	88

Prisma Certified Cloud Security Engineer Study Guide

Welcome to the *Prisma Certified Cloud Security Engineer Study Guide*. The purpose of this guide is to prepare you for your Prisma Certified Cloud Security Engineer exam and achieve your PCCSE credential.

Overview

The PCCSE program is a formal, third-party proctored certification. Success on the PCCSE exam shows that you possess the in-depth skills and knowledge needed to administer cloud solutions, including the areas of:

- visibility
- data-loss prevention
- security and compliance
- web application and API security
- Dev SecOps security

Your success on the PCCSE exam demonstrates the highest standard of deployment methodology and operational best practices associated with the Palo Alto Networks Prisma Cloud. The exam is not intended to trick you or to test obscure detail. However, a nuanced understanding, and the ability to make subtle technical distinctions, will help you choose better answers.

More information is available from the Palo Alto Networks Prisma public page:

<https://docs.paloaltonetworks.com/prisma.html>

Prisma Cloud technical documentation is located at this link:

<https://docs.paloaltonetworks.com/prisma/prisma-cloud.html>

Exam Format

The test format is 75 to 85 multiple-choice items. Candidates will have five minutes to complete the non-disclosure agreement (NDA), 90 minutes (1 hour, 30 minutes) to complete the questions, and five minutes to complete a survey at the end of the exam.

The approximate distribution of items by topic (Exam Domain) and topic weightings are shown in the following table.

Exam Domain	Weight (%)
Install and Upgrade	8%
Visibility, Security, Compliance and Data Security	33%
Cloud Workload Protection Platform	18%
Web Application and API Security (WAAS)	8%
DevSecOps security (Shift Left)	13%
Prisma Cloud administration	20%
	100%

How to Take This Exam

The exam is available through the third-party Pearson VUE testing platform. To register for the exam, visit: <https://home.pearsonvue.com/paloaltonetworks>

Preparation Resources

The document is a compilation of key resources to guide exam preparation. These resources cover the material designated by the exam objectives. To study efficiently, focus on the suggested topics listed for each resource. Be sure that you have a clear and complete understanding of these topics before you take the exam.

Exam Domains and Objectives

1 Install and Upgrade

This domain describes the software for Prisma Cloud Compute. In contrast with the rest of the Prisma Cloud suite, which is software as a service (SaaS), Prisma Cloud Compute requires the installation of Defenders. You also can install your own console instead of using the SaaS console. In this domain, you can validate your knowledge of how to deploy and manage Prisma Cloud Compute.

1.1 Deploy and Manage the Console for the Compute Edition

For Prisma Cloud Compute, you can use a data-collection and user-interface platform hosted by Palo Alto Networks. Or you can host your own console with software provided to you as a Docker image. See the following links for more information.

Prisma Cloud container images

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/twistlock_container_images.html

The Console for a Onebox configuration

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_onebox.html

The Console for Kubernetes

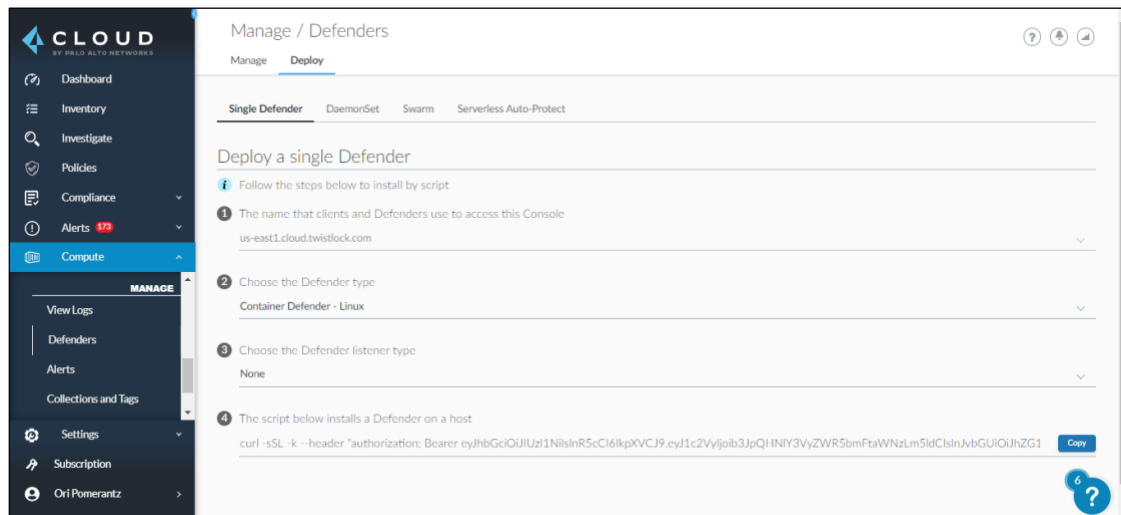
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_kubernetes.html

An upgrade on the console

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/upgrade.html>

1.2 Deploy and Manage Defenders

Whether you use a hosted console or the SaaS console, you need to install Defenders in your application's infrastructure to enforce the policies from Prisma Cloud Compute.



There are multiple types of Defenders, with different capabilities.

CAPABILITIES		DEFENDER TYPE			
		>Container ¹	>Host	>Serverless	>App Embedded
Deployment methods	Console UI	Y	Y	Y	Y
	API	Y	Y	Y	Y
	twistcli	Y			Y
Vulnerability management		Y	Y	Y ²	Y ³
Compliance		Y	Y	Y ²	
Runtime defense	Behavioral modeling	Y	N		
	Process	Y	Y	Y	Y
	Networking	Y	Y	Y	Y
	File system	Y	Y	Y	
	Forensics	Y	Y		
Firewalls	WAAS	Y	Y	Y	Y
	CNNF	Y	Y		
	Radar (visualization)	Y	Y		

Understand Defender types

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/defender_types.html

Install container Defenders

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_single_container_defender.html

Deploy host Defenders

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/audit/host_activity
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/runtime_defense/runtime_defense_hosts
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/compliance/host_scanning

Deploy serverless Defenders

- https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_serverless_defender.html
- https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_serverless_defender_layer.html

Deploy app-embedded Defenders

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_app_embedded_defender.html
- https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_app_embedded_defender_fargate.html
- https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_app_embedded_defender_pivotal_pas.html

Configure networking for Defender to Console connectivity

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/getting_started.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/install/install_defender/install_single_container_defender.html

Perform an upgrade on Defenders

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/upgrade.html>

2 Visibility, Security, Compliance and Data Security

In this domain, you will validate your knowledge of how to use Prisma Cloud to view activity with your applications, ensure system security, and verify compliance with required standards.

2.1 Configure policies

Policies in Prisma Cloud have two primary elements.

1. A query to identify elements that are insecure or out of compliance

1 Details — 2 Build Your Rule — 3 Compliance Standards — 4 Remediation

Run

This is a policy subtype for deployed cloud resources (RQL)

New Search Saved Search

Select saved search

GCP Firewall rule allows all traffic on RDP...

Query

```
config from cloud.resource where cloud.type = 'gcp' AND api.name='gcloud-compute-firewall-rules-list' AND json.rule= 'sourceRanges[*] contains 0.0.0.0/0 and allowed[?any(ports contains _Port.inRange(3389,3389) or (ports does not exist and (IPProtocol contains tcp or IPProtocol contains udp)) )] exists'
```

1 Details — 2 Build Your Rule — 3 Compliance Standards — 4 Remediation

Run

This is a policy subtype for deployed cloud resources (RQL)

Recommendation for Remediation

If the Firewall rule reported indeed needs to restrict all traffic, follow the instructions below:

1. Login to GCP Console
2. Go to 'VPC Network'
3. Go to the 'Firewall'
4. Click on the reported Firewall rule
5. Click on 'EDIT'
6. Modify Source IP ranges to specific IP
7. Click on 'SAVE'.

Enter CLI Command ⓘ

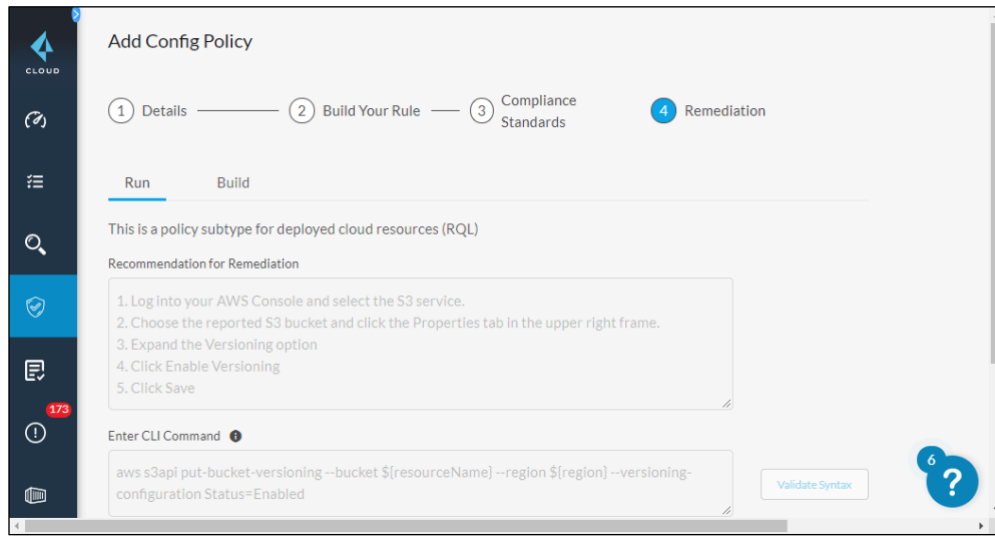
gcloud -q compute --project=\${account} firewall-rules delete \${resourceName}

Validate Syntax

CLI Command Description ⓘ

This CLI command requires 'gcloud.compute.firewall-rules.delete' permission. Successful execution will delete this firewall rule blocking internet traffic to RDP port (3389).

2. Remediation action to fix the problem



In this task, you will validate that you can create and manage these policies.

2.1.1 Understand policies related to compliance standards

Understand policies related to compliance standards

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/compliance/compliance_explorer.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/compliance/manage_compliance.html

2.1.2 Build custom policies

Build custom policies

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference.html>

2.1.3 Identify policy types

Create a custom policy on Prisma Cloud

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy>

Identify Policy Types

You can monitor cloud resources and Infrastructure as Code (IaC) development environments in Prisma Cloud. Become familiar with these two policy types when you select a policy.

- Run – Policy sub-type used to monitor deployed cloud resources
- Build – Policy sub-type used for IaC scans during your DevOps process

The screenshot shows a policy configuration form with the following fields:

- Policy Name ***: AWS S3 buckets are accessible to public
- Policy Subtype ***: Run (checked) and Build (checked)
- Description**: This policy identifies S3 buckets which are publicly accessible. Amazon S3 allows customers to store or retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example, to host website content. However, these buckets often contain highly sensitive enterprise data which if left open to public may result in sensitive data leaks.
- Severity ***: High (indicated by three red dots)
- Labels**: PCI DSS v3.2 (with a close icon)

2.2 Configure alerting and notifications

Prisma Cloud alerts can trigger a notification to a manual and/or automatic remediation.

The screenshot shows the 'Alert Rules' table in Prisma Cloud. The table has the following columns: NAME, NOTIFICATION CHANNELS, LAST MODIFIED BY, LAST MODIFIED, TYPE, AUTOMATED REMEDIATION, and OPTIONS. The table contains three rows of data.

NAME ↓↑	NOTIFICATION CHANNELS ↓↑	LAST MODIFIED BY ↓↑	LAST MODIFIED ↓	TYPE ↓↑	AUTOMATED REMEDIATION ↓↑	OPTIONS
mbowling Default	✉	Mark Bowling	6 days ago	Run		⋮
AWS IAM Role	✉	SecOps User	10 months ago	Run		⋮
Default Alert Rule	✉	SecOps User	10 months ago	Run		⋮

At the bottom of the table, there is a pagination bar showing '1 to 3 of 3' and 'Page 1 of 1'.

2.2.1 Understand alert states

View and Respond to Prisma Cloud Alerts

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/view-respond-to-prisma-cloud-alerts.html>

2.2.2 Build alert rules

Build alert rules

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/create-an-alert-rule.html>

2.2.3 Create alert notifications

Send Prisma Cloud Alert Notifications to Third-Party Tools

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/send-prisma-cloud-alert-notifications-to-third-party-tools.html>

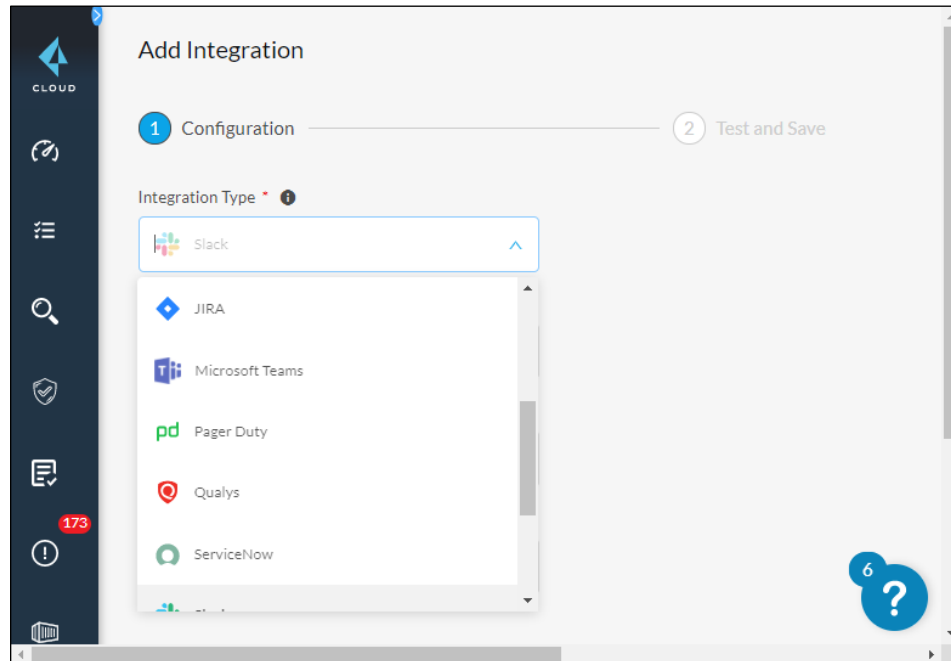
2.2.4 Investigate alerts

Investigate alerts

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/view-respond-to-prisma-cloud-alerts.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/generate-reports-on-prisma-cloud-alerts.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/alert-payload.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/risk-rating-for-a-resource.html>

2.3 Understand third-party integrations

An organization's IT department typically has existing alert mechanisms. This task describes how to connect these alert mechanisms with Prisma Cloud.



2.3.1 Understand inbound and outbound notifications

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts.html>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/alert_mechanism.html
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/email.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/slack.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud.html>

2.4 Perform ad hoc investigations

Ad hoc investigations happen when an administrator sees a vulnerability or suspicious activity and decides to investigate further. This investigation has two purposes.

1. Identify whether the relevant entity (virtual machine instance, Docker container, etc.) really has been broken into. For example, a vulnerability could exist but never have been exploited.
2. If the entity has been broken into, identify the harm done and whether the entity itself was used as a conduit for attacking other entities.

An investigation typically starts with an RQL query that shows details about what is happening in your cloud environment.

Examples of investigation queries include: config, event, IAM, and network.

DESCRIPTION	RQL
View users who enabled console access with both access keys and passwords.	<pre>config from cloud.resource where api.name = 'aws-iam-get-credential-report' AND json.rule = access_key_1_active is true or access_key_2_active is true and password_enabled is true</pre> <div>Copy</div>
DESCRIPTION	RQL
Detect activities from non-automated events and from specific IP addresses.	<pre>event from cloud.audit_logs where ip EXISTS AND ip IN (152.1.1.1)</pre> <div>Copy</div>
DESCRIPTION	RQL
Find all effective permissions of a specific IAM user	<pre>config from iam where source.cloud.service.name = 'iam' and source.cloud.resource.type = 'user' and source.cloud.resource.name = 'my-user'</pre>
DESCRIPTION	RQL
View traffic originating from the Internet & suspicious IPs to resource with Database role.	<pre>network from vpc.flow_record where source.publicnetwork IN ('Suspicious IPs' , 'Internet IPs') and dest.resource IN (resource where role IN ('AWS RDS' , 'Database'))</pre> <div>Copy</div>

For example, here is the result of a query asking which APIs were used and when.



Next, you can drill down for additional information about a specific data point, such as the query for the cloudresource manager.googleapis.com in June 2020. This query returns a list of the items that were aggregated. In this case, it is a list of events.

cloudresource manager.googleapis.com						
Modern Table (Beta) <input checked="" type="checkbox"/> Search <input type="text"/>						
ENTITY <input type="text"/>	CLOUD ACCOUNT <input type="text"/>	OPERATION <input type="text"/>	SERVICE <input type="text"/>	IP ADDRESS <input type="text"/>	OPTIONS	
jnr1138@gmail.com	MyGoogleCloudAccount	SetiamPolicy	cloudresource manager.googleapis.com	35.230.94.207	<input type="button" value="eye"/>	
one-platform-tenant-manager@system.gserviceaccount.com	MyGoogleCloudAccount	SetiamPolicy	cloudresource manager.googleapis.com	2002:a05:612a:1bce::	<input type="button" value="eye"/>	
one-platform-tenant-manager@system.gserviceaccount.com	MyGoogleCloudAccount	SetiamPolicy	cloudresource manager.googleapis.com	2002:a9e:7481::	<input type="button" value="eye"/>	
one-platform-tenant-manager@system.gserviceaccount.com	MyGoogleCloudAccount	SetiamPolicy	cloudresource manager.googleapis.com	2002:a9e:7481::	<input type="button" value="eye"/>	
one-platform-tenant-manager@system.gserviceaccount.com	MyGoogleCloudAccount	SetiamPolicy	cloudresource manager.googleapis.com	2002:a6a:8f87::	<input type="button" value="eye"/>	
one-platform-tenant-manager@system.gserviceaccount.com	MyGoogleCloudAccount	SetiamPolicy	cloudresource manager.googleapis.com	2002:a05:612a:1bce::	<input type="button" value="eye"/>	

You can then click the **eye** icon on any line in the list for its full details.

Raw Event

Copy to Clipboard Toggle Search

```
1 {
2   "labels": "{}",
3   "logName": "cloudaudit.googleapis.com%2Factivity",
4   "payload": {
5     "status": {},
6     "request": {
7       "@type": "type.googleapis.com/google.iam.v1.SetIamPolicyRequest",
8       "policy": {
9         "etag": "BwWOYkrUt3c=",
10        "bindings": [
11          {
12            "role": "projects/inlaid-sentinel-226923/roles/CustomRedLockViewer",
13            "members": [
14              "serviceAccount:redlock-sa@inlaid-sentinel-226923.iam.gserviceaccount.com"
15            ]
16          },
17          {
18            "role": "roles/compute.securityAdmin",
19            "members": [
20              "serviceAccount:redlock-sa@inlaid-sentinel-226923.iam.gserviceaccount.com"
21            ]
22          },
23          {
24            "role": "roles/compute.serviceAgent",
25            "members": [
26              "serviceAccount:service-283205634344@compute-system.iam.gserviceaccount.com"
27            ]
28          }
29        ]
30      }
31    }
32  }
```

2.4.1 Investigate resource configurations with RQL

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/config-query.html>

2.4.2 Investigate user activity using RQL

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/event-query.html>

2.4.3 Investigate network activity using RQL

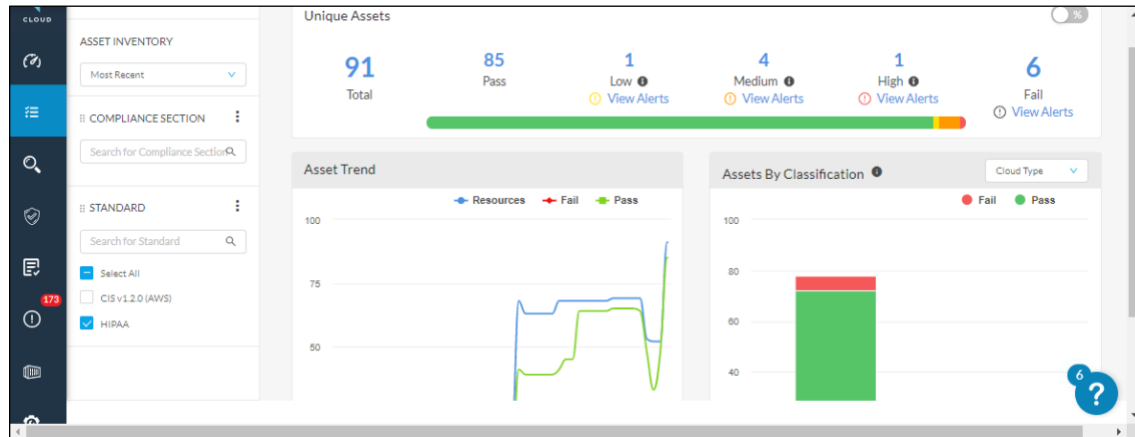
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/network-query.html>

2.4.4 Investigate anomalous user event(s)

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-rql-reference/rql-reference/event-query/event-query-attributes.html#id192IG500ES0>

2.5 Identify assets in a cloud account

This task identifies assets and distinguishes between assets that comply with the policy and those that do not, and then generates an alert.



2.5.1 Identify the inventory of resources in a cloud account

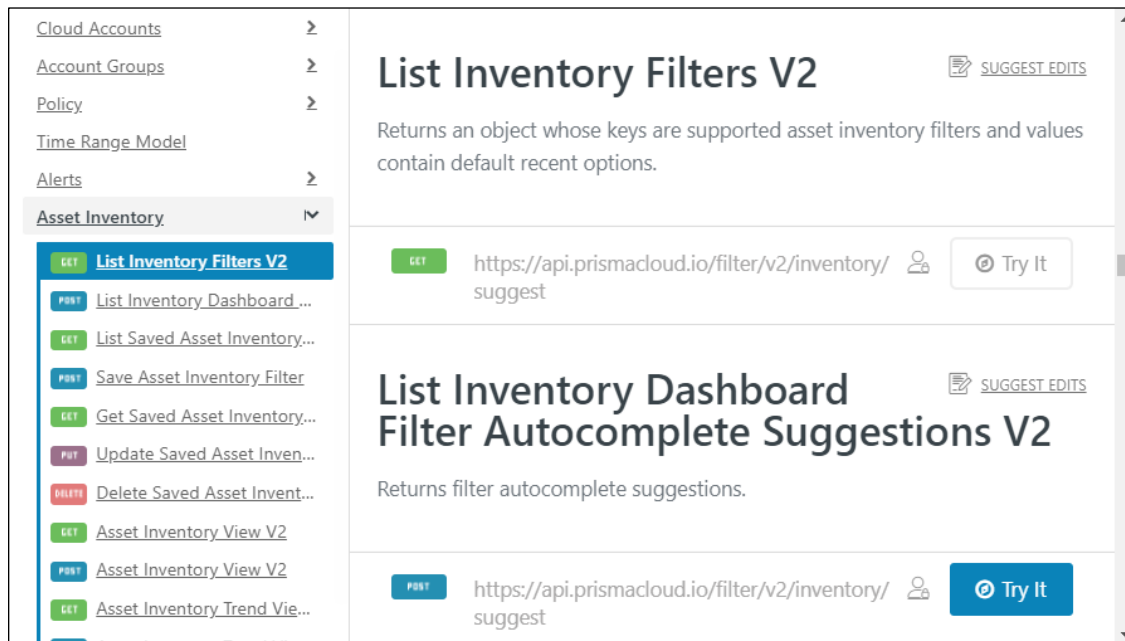
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-dashboards/asset-inventory>

2.5.2 Identify how to check resource-configuration history

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase.html>

2.6 Use Prisma Cloud APIs

You can automate repetitive tasks using the Prisma Cloud API.



2.6.1 Use APIs for the automation of tasks

- <https://api.docs.prismacloud.io/reference>

2.6.2 Use APIs for custom queries

- <https://api.docs.prismacloud.io/reference#search-manager>
- <https://api.docs.prismacloud.io/reference#search>

2.7 Remediation

When Prisma Cloud detects a policy violation on a cloud resource, an alert is triggered. The alert is presented in several locations, SecOps dashboard, Compliance Dashboards, Alerts page, Policy pages, and results through Prisma Cloud investigations. Remediation is the process of resolving or clearing alerts to bring a cloud resource back in compliance with a Prisma Cloud policy. Any policies associated with the alert are referenced to aid in the remediation of alerts.

2.7.2 Identify the requirements to use auto-remediation

References

Configure Prisma Cloud to Automatically Remediate Alerts

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/configure-prisma-cloud-to-automatically-remediate-alerts.html#id77ff61ca-a7ae-4830-9c47-516c79be3f9a>

Configuration on Cloud Provider

Policy violations are captured in Prisma Cloud. However, the remediation happens on the respective connected cloud account, (AWS, Azure, GCP, Alibaba, and OCI). Once the violation is remediated on the connected cloud account, the alert will show remediated in Prisma Cloud.

2.7.2 Differentiate between when to use manual versus automated remediation

There are two remediation methods in Prisma Cloud:

Manual Remediation

The Manual Remediation method includes recommended actions an administrator must take to remediate an alert. The manual remediation method requires that the administrator access the cloud console and perform the recommended steps to reconfigure the resource back into compliance.

[< Back](#) Filter(s): Alert Status = Resolved Cloud Type = aws Remediable = true

AWS Security Group allows all traffic on SSH port (22)





This policy identifies Security groups that allow all traffic on SSH port 22. Doing so, may allow a bad actor to brute force their way into the system and access SSH solely to known static IP addresses. Limit the access list to include known hosts, services, or specific employees only.

Recommendation

Before making any changes, please check the impact to your applications/services. If the Security Group reported indeed need to restrict all traffic, follow these steps:

1. Log in to the AWS Console
2. Navigate to the 'VPC' service
3. Select the 'Security Group' reported in the alert
4. Click on the 'Inbound Rule'
5. Remove the rule which has 'Source' value as 0.0.0.0/0 or :::/0 and 'Port Range' value as 22 (or range containing 22)

Violating Resources

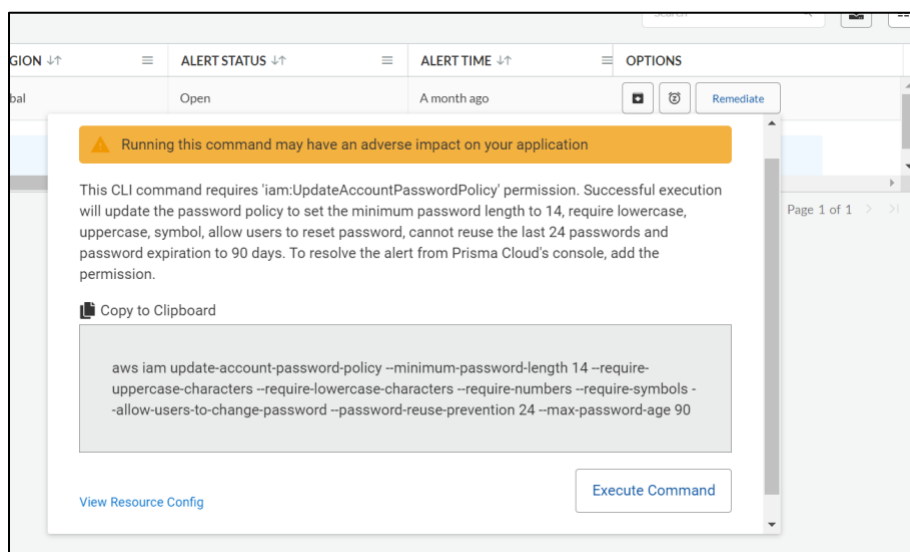
<input type="checkbox"/>	ALERT ID 	RESOURCE NAME 
<input type="checkbox"/> >	P-314	VM-Series Next-Generation Firewall Bundle 2-PAN-OS 7-1-6-AutogenByAWSMP- 
<input type="checkbox"/> >	P-315	VM-Series Next-Generation Firewall Bundle 2-PAN-OS 7-1-6-AutogenByAWSMP- 

Automatic Remediation

Automatic Remediation is performed directly from Prisma Cloud where CLI commands are executed to resolve or clear an alert. There are two requirements for Automatic Remediation: Prisma Cloud must have write-access into the cloud account (monitor and protect) and a remediable policy must be used on the cloud resource.

There are two Automatic Remediation methods:

1) **Guided Remediation** – A guided remediation is the process of executing CLI commands directly from the Prisma Cloud console. The administrator reviews the alerts and, if the alert is associated with a remediable policy, the administrator can resolve the alert by sending the CLI commands directly from Prisma Cloud.



2) **Automatic Remediation** – An automatic remediation is performed via an Alert Rule that is configured with a remediable policy. No manual administrator actions are required. When Prisma Cloud detects a policy violation, an alert is triggered. An associated Alert Rule automatically executes the CLI commands defined under the remediable policy assigned to the Alert Rule.



2.8 Onboarding

2.8.1 Identify the process for onboarding cloud accounts with data protection

Prisma Cloud Data Security requires you to configure an AWS CloudTrail bucket. To save cost, ensure that you follow the instructions to select only Write events instead of Read and Write events.

2.8.2 Configure CloudTrail and SNS

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/enable-data-security-module/add-a-new-aws-account.html>

Only monitor mode is supported.

2.8.3 Configure scan options

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud.html>

2.9 Use Data Dashboard features

The new Data Dashboard tab provides complete visibility into your S3 storage. This tab is available under the Dashboard menu and the widgets show you:

- How many storage buckets and objects you have
- Which kind of data is stored in those objects, across which regions
- Who owns what
- What the exposure is of the objects.

2.9.1 Classify objects

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/object-explorer.html>

2.9.2 List object permissions for visibility

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/exposure-evaluation.html>

2.9.3 Viewing data inventory

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/data-inventory.html>

2.9.4 Viewing Resource Explorer

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/resource-explorer.html>

2.9.5 List object identifiers

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/object-explorer.html>

2.9.6 Knowing object-exposure states

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/exposure-evaluation.html>

2.10 Assess Data Policies and Alerts

Prisma Cloud includes default data policies to help you start scanning.

2.10.1 Differentiate differences between malware and regular policies

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/data-policies.html>

2.10.2 Understand the scope of alert notifications

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-data-security/monitor-data-security-scan-prisma-cloud/data-policies.html>

3 Cloud Workload Protection Platform

In this domain, you can validate your knowledge about how to use Prisma Cloud to protect your workloads, whether they are running as virtual machines, Docker containers, or serverless functions. This protection involves three different areas:

1. Protect against known vulnerabilities by scanning, updating, and removing libraries known to contain those vulnerabilities.
2. Monitor for compliance with standards that improve security.
3. Reduce the attack surface by deploying the Cloud Native Application Firewall (CNAF).

3.1 Monitor and protect against image vulnerabilities

This task shows you how Prisma Cloud Compute can scan the Docker images that you intend to use to identify any vulnerabilities. Steps can then be taken to remove those vulnerabilities before they can put the integrity of the container at risk.



The screenshot displays the 'Monitor / Vulnerabilities' page in the Prisma Cloud interface. The 'Images' tab is selected, showing a table of deployed images. The table includes columns for Registry, Repository, Tag, Hosts, Vulnerabilities, Risk Factors, and Collections. Two images are listed: 'my_apache2' and 'twistlock/private'. The 'my_apache2' image has 48 vulnerabilities and 2012 risk factors, while the 'twistlock/private' image has 0 vulnerabilities and 0 risk factors.

Registry	Repository	Tag	Hosts	Vulnerabil...	Risk Factors	Collectio...
	my_apache2	latest	secure-these-d...	48 2012	7	—
	twistlock/private	defender_20_04_1...	secure-these-d...	0	0	—

3.1.1 Understand how to investigate image vulnerabilities

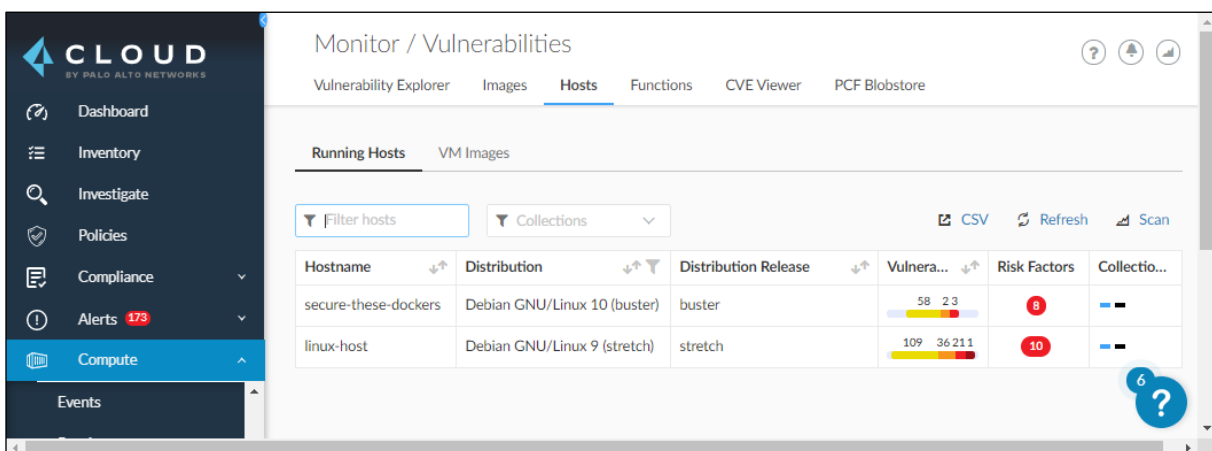
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_explorer.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/registry_scanning.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/registry_scanning0.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/search_cves.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/windows_image_scanning.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/cvss_scoring.html

3.1.2 Configure image vulnerability policy

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_management_rules.html

3.2 Monitor and protect against host vulnerabilities

This task teaches you to secure the hosts that run your application by removing vulnerable code. Even if you use Docker, a chain is only as strong as its weakest link. A Docker container running inside an insecure host is vulnerable if that host is successfully attacked.



3.2.1 Understand how to investigate host vulnerabilities

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_explorer.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/search_cves.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vm_image_scanning.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/detect_vulns_unpackaged_software.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/cvss_scoring.html

3.2.2 Configure a Host Vulnerability policy

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_management_rules.html

3.3 Monitor and enforce Docker image and container compliance

Task 3.1 was about identifying known vulnerabilities in images. This task is about ensuring compliance with accepted standards.

Monitor / Compliance						
<div>Compliance Explorer Containers Images Hosts Functions Trusted Images Cloud Discovery Cloud Compliance</div>						
<div>Filter containers</div>		<div>All , ref-app-arch , inlaid...</div>		<div>CSV Refresh Scan</div>		
Name	Image	Hostname	Command	Compliance	Collectio...	
reverent_swanson	my_apache2:latest	secure-these-dockers	httpd-foreground	<div>6 1</div>	<div></div>	
twistlock_defender_20_04_177	twistlock/private:defender_20_04_177	secure-these-dockers	defender	<div>0</div>	<div></div>	

Edit Default - ignore Twistlock components

Rule name

Default - ignore Twistlock components

Notes

Enter notes

1

Compliance actions

Filter


























All types

Set action for all checks

Ignore Alert Block

ID	Type	Severity	Action	Description
406	image	medium	<div>Ignore Alert Block</div>	Add HEALTHCHECK instruction to the container image
41	image	high	<div>Ignore Alert Block</div>	Image should be created with a non-root user
420	image	medium	<div>Ignore Alert Block</div>	Image is not updated to latest
422	image	critical	<div>Ignore Alert Block</div>	Image contains malware

The compliance rules that Prisma enforces come from various standards, such as CCPA 2018, SA CCM 3.10.1, GDPR, and Palo Alto Networks own research.

NAME ↓↑	DESCRIPTION ↓↑	CLOUD ↓↑	CREATED BY ↓↑	LAST MODIFIED BY ↓↑
CCPA 2018	California Consumer Privacy Act of 2018 [1798.100 - 1798.199]	  	Prisma Cloud System Admin	Prisma Cloud System Admin
CIS v1.0.0 (GCP)	Center for Internet Security Benchmark for Google Cloud Platform Foundation v1.0.0		Prisma Cloud System Admin	Prisma Cloud System Admin
CIS v1.1 (Azure)	Center for Internet Security Benchmark for Azure v1.1.0		Prisma Cloud System Admin	Prisma Cloud System Admin
CIS v1.2.0 (AWS)	Center for Internet Security Standard version 1.2.0		Prisma Cloud System Admin	Prisma Cloud System Admin
CSA CCM v3.0.1	Cloud Security Alliance: Cloud Controls Matrix Version 3.0.1	  	Prisma Cloud System Admin	Prisma Cloud System Admin
Custom Compliance Standard	Custom Compliance Standard		SecOps User	SecOps User
GDPR	General Data Protection Regulation	  	Prisma Cloud System Admin	Prisma Cloud System Admin
HIPAA	Health Insurance Portability and Accountability Standard	  	Prisma Cloud System Admin	Prisma Cloud System Admin
HITRUST CSF v9.3	HITRUST CSF v9.3	  	Prisma Cloud System Admin	Prisma Cloud System Admin
ISO 27001:2013	ISO 27001:2013 Compliance Standard	  	Prisma Cloud System Admin	Prisma Cloud System Admin
MITRE ATT&CK [Beta]	MITRE ATT&CK Cloud Matrix for Enterprise [Beta]	  	Prisma Cloud System Admin	Prisma Cloud System Admin

3.3.1 Understand how to investigate image and container compliance

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/compliance_explorer.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance.html

3.3.2 Configure image and container compliance policy

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/cis_benchmarks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/prisma_cloud_compliance_checks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/custom_compliance_checks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/extensible_compliance_checks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/detect_secrets.html

3.4 Monitor and enforce host compliance

As is the case with vulnerabilities, hosts need to comply with security standards to be safe for applications running directly on the host or for Docker containers.

Monitor / Compliance

Compliance Explorer

Containers

Images

Hosts

Functions

Trusted Images

Cloud Discovery

Cloud Compliance

Running Hosts

VM Images

Filter hosts

All

ref-app-arch

inlaid...

CSV

Refresh

Scan

Hostname	Distribution	Distribution Release	Compliance	Collectio...
linux-host	Debian GNU/Linux 9 (stretch)	stretch	8	— —
secure-these-dockers	Debian GNU/Linux 10 (buster)	buster	12	— —

3.4.1 Understand how to investigate host compliance

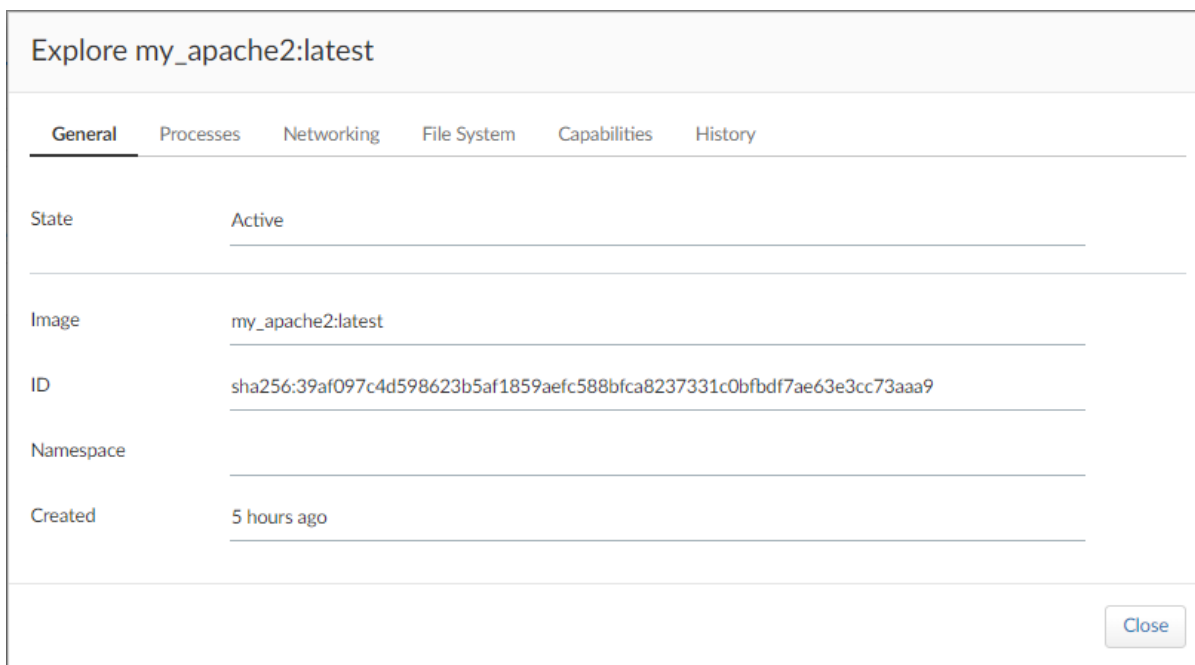
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/compliance_explorer.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/manage_compliance.html

3.4.2 Configure Host Compliance policy

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/cis_benchmarks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/prisma_cloud_compliance_checks.html
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/windows.html>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/custom_compliance_checks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/extensible_compliance_checks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/host_scanning.html

3.5 Monitor and enforce container runtime

Containers are not supposed to be flexible. To change container behavior, you typically need to create an image with the new behavior, stop the old container, and deploy a new container using the new image. Therefore, you almost always should investigate anomalous container behavior.



3.5.1 Understand container models

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_overview

3.5.2 Configure container runtime policies

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/vuln_management_rules.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/custom_runtime_rules.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_processes.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_networking.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_fs.html

3.5.3 Understand container runtime audits

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/runtime_defense_overview.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/discrete_blocking.html

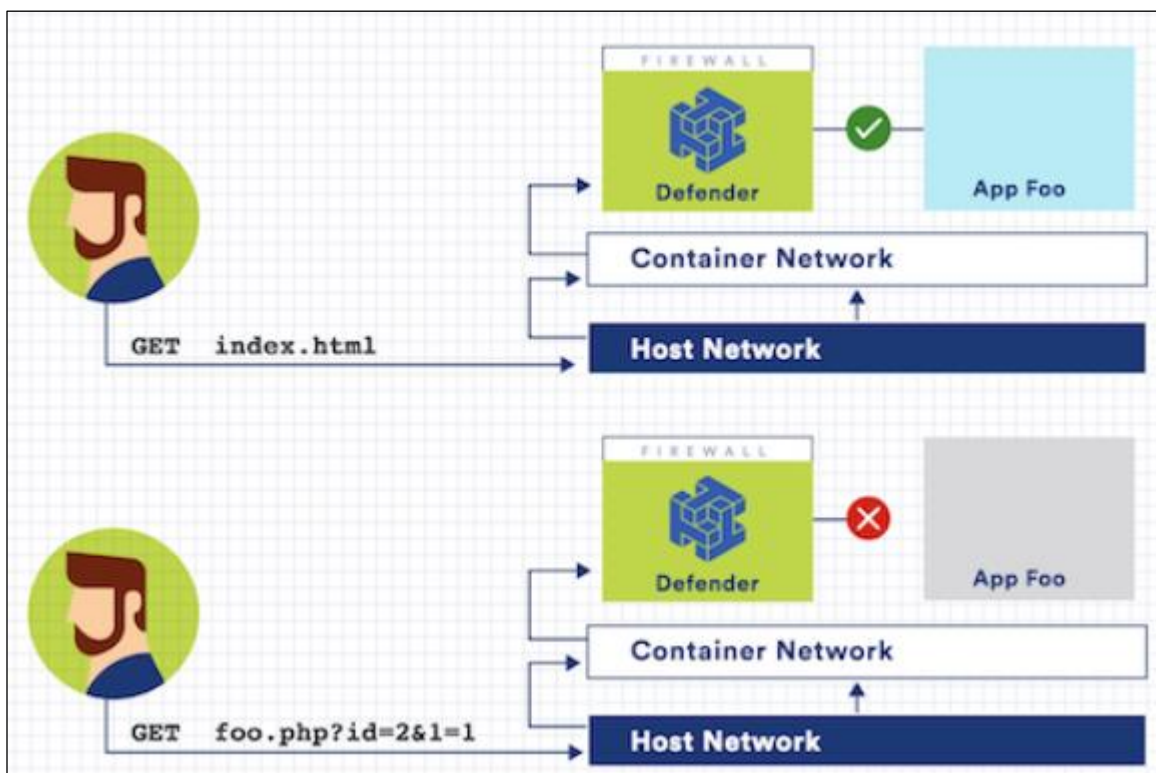
3.5.4 Investigate incidents using Incident Explorer

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/runtime_defense/incident_explorer.html

3.6 Configure web-application and API security (WAAS) policies

Cloud Compute provides web-application and API security (WAAS) through a web-application firewall (WAF) designed for both hosts and containers. This WAF secures web apps by inspecting and filtering Layer 7 traffic to and from the application.

WAAS enhances the traditional WAF for container environments by binding itself to containerized web apps. It can do this binding regardless of the cloud, orchestrator, node, or IP address where that containerized web app is running and without configuring complicated routing. For non-containerized web apps, WAAS simply binds to the host where the app runs.



3.6.1 Configure WAAS policies to create a relevant WAAS rule

- <https://www.paloaltonetworks.com/prisma/cloud/web-application-API-security>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/firewalls/waas.html>

3.7 Monitor and protect against serverless vulnerabilities

This task shows you how to identify and protect against vulnerabilities in serverless apps. The term “serverless” does not mean there is no server. It means that for most purposes you can ignore the server, because it is managed by the service provider. However, it still is implemented on a virtual machine (possibly on a Docker container) that runs an application runtime environment such as Node.js or Tomcat. This environment, and any libraries you import into your serverless app, still can contain vulnerabilities.

The screenshot shows the 'Create new vulnerability rule' configuration window. It includes the following fields and options:

- Rule name:** Normal security
- Notes:** If it's critical, it is better to have downtime than risk our data. In other cases we need an alert.
- Severity based actions:**
 - Alert threshold:** Off. A horizontal bar shows severity levels: Low (yellow), Medium (orange), High (red), and Critical (blue). The text 'Alert on [Low, Medium, High, Critical]' is displayed.
 - Failure threshold:** Off. A horizontal bar shows severity levels: Low (yellow), Medium (orange), High (red), and Critical (blue). The text 'Fail on [Critical]' is displayed.
- Scope:** Functions. Two tags are present: 'processThis' and 'processThat', followed by a 'Specify a function' input field.

At the bottom right, there are 'Cancel' and 'Save' buttons.

3.7.1 Understand how to investigate serverless vulnerabilities

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/serverless_functions.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/search_cves.html

3.7.2 Configure serverless vulnerability policy

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/serverless.html>

3.7.3 Configure serverless auto-protect functionality

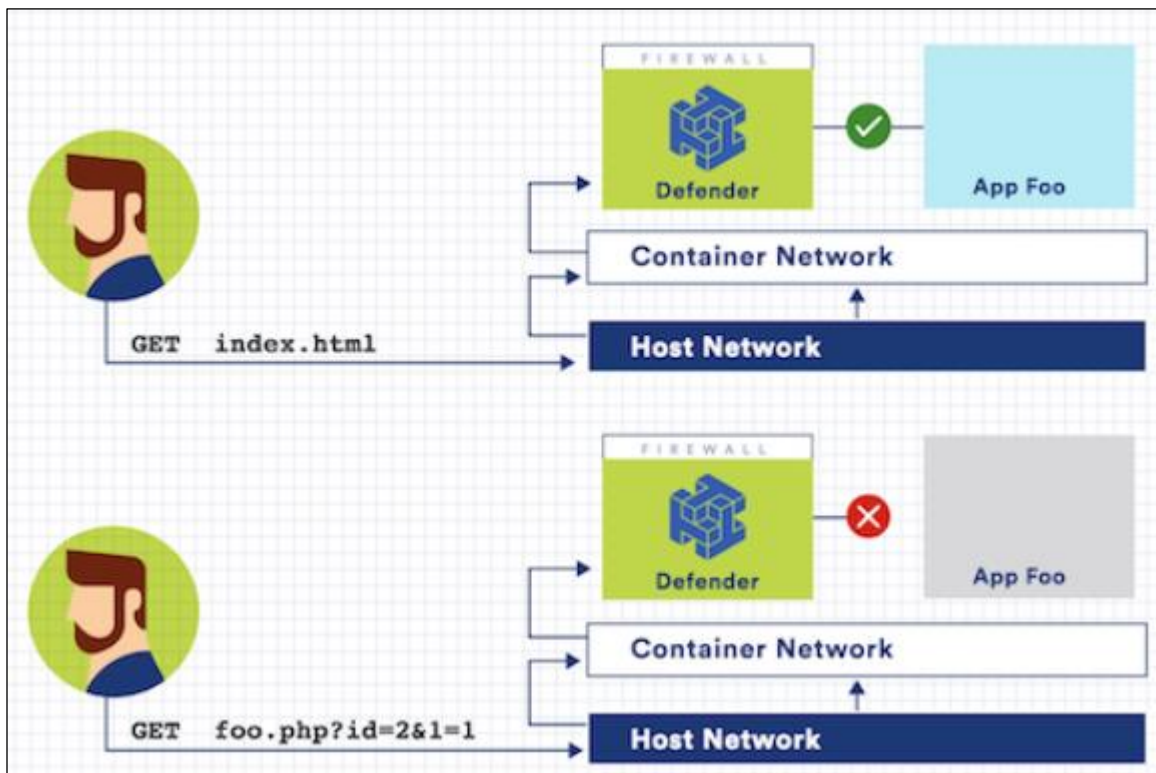
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_defender/install_serverless_defender
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/install/install_defender/install_serverless_defender_layer.html

4 Web Application and API Security (WAAS)

In this domain, you can validate your knowledge of how to limit access to RESTful APIs using Prisma Cloud and segmentation.

4.1 Configure WAAS policies and an App rule

WAAS can restrict the HTTP header fields (as illustrated in the following image) and types of files permitted to upload. It can also stop various common HTTP attacks, and more.



Edit Limit HTTP to Apache

General
HTTP Headers
File Uploads
Intelligence Gathering
Advanced

Rule name: Limit HTTP to Apache

Notes:

Action: Disable Alert Prevent

☒ Prisma Cloud Advanced Threat Protection

☐ SQLi attack protection
☒ XSS attack protection
☒ CSRF protection
☒ Clickjacking protection
☒ Attack tool protection
☒ Shellshock protection
☒ Malformed request protection

Ports	Application Port	TLS	Actions
	80	false	...

Cancel
Save

4.1.1 Define the application specifications

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/firewalls/waas.html>

4.1.2 Define or import API methods

Use WAAS to define and import custom API methods. WAAS supports API security, based upon specifications defined by Swagger or Open API files. Define the endpoint methods and paths.

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_api_protection.html

Path ↓ Methods Actions

Add new Path

Resource path /product

Select method ☒ GET ☐ PUT ☒ POST ☐ DELETE ☐ OPTIONS ☐ HEAD ☐ PATCH

Parameters for Nothing selected ▼ + Add parameter

Parameter name	Type	Location	Range	Actions
There is no data to show				

Cancel Create path

4.1.3 Limit access to different REST API endpoints

Protect endpoint by verifying and configuring the base paths.

Endpoint setup API protection

Description (optional) Add a description ⓘ

Protected endpoints **1**

1 total entry + Add endpoint

HTTP host	Port	Base path	TLS	HTTP/2	Actions
▼ *	80	/* 2	Off	Off	🗑️

4.2 Configure application-firewall settings and exceptions

Configure API protection through the use of API actions defined under App Firewall. Define protection methods for SQL Injection, cross-site scripting, and OS command injection. Set the mode for each protection to Alert, Prevent, or Ban.

Protection	Mode	Exceptions	Actions
SQL Injection	Disable Alert Prevent Ban		
Cross-Site Scripting (XSS)	Disable Alert Prevent Ban		
OS Command Injection	Disable Alert Prevent Ban		

4.2.1 Configure DoS protection

Denial-of-service (DoS) protection allows you to further protect apps by applying rate-limiting, setting alert notifications, and banning connections. With DoS, you can set rate limits to the number of requests against apps. The Burst Rate is a request rate that is calculated over a five-second period. The Average Rate is the request rate calculated over a 120-second period. Once a matching condition is met, define an effect to Alert or Ban. Define conditions for HTTP methods, file extensions, and HTTP response codes.

DoS protection: ☒ On

Rate limit & Ban are applied by Client IP. Prisma Session Cookies are required to be enabled for App DoS protection based on session. [Enable Cookies](#)

Effect: Alert Ban

Burst rate: 1 (Avg. Requests/Second) Average rate: 1 (Avg. Requests/Second)

Match Conditions: + Add Match Condition

Methods	File Extensions	Response Codes	Actions
There is no data to show			

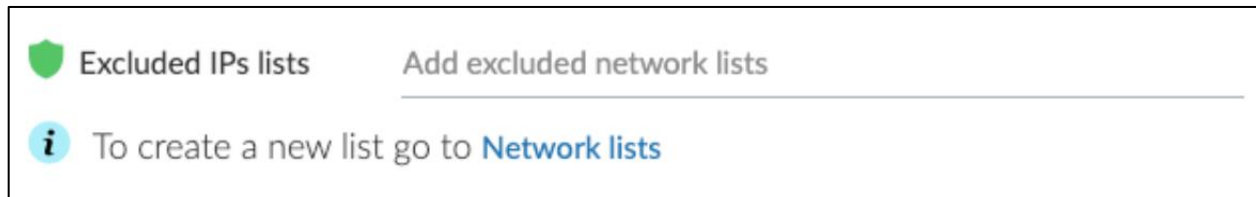
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_dos_protection.html

4.2.2 Configure access controls to limit inbound sources

- <https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-remote-networks-with-prisma-access/secure-inbound-access>

4.2.3 Manage network lists

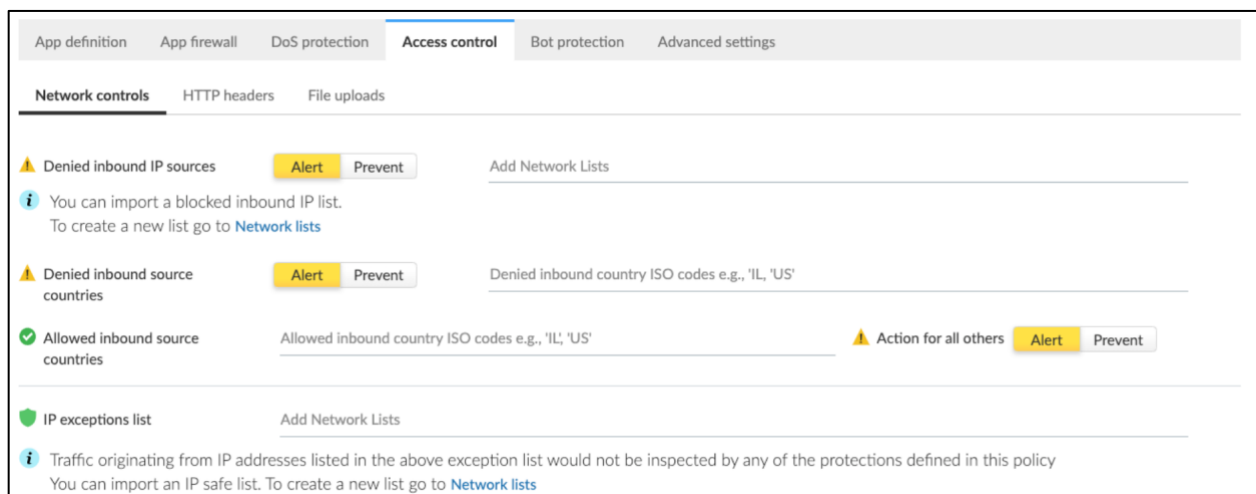
Network list allow you to set exclusions from trusted or known endpoints. Define a network list that includes the IP addresses of know or trusted IP addresses.



4.2.4 Configure access controls to enforce HTTP headers and file uploads

Access Control includes defining where your apps can be accessed from and whether the endpoints can upload files. There are three Access Control parameters: Network Controls, HTTP headers, and File Uploads.

Network Controls define your inbound-source IP addresses and inbound-source countries. You can set control methods to either send an Alert or Prevent. For known or trusted endpoints, you can define exception lists for inbound-source countries and IP addresses.



- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_access_control.html

HTTP headers allow you to block or allow HTTP requests based upon a matching header string. Define an HTTP header with an Allow or Blacklisted value. Set an action to either send an Alert or Prevent (block).

The screenshot shows the 'Add HTTP Header' dialog box in the Palo Alto Networks Prisma Cloud Admin console. The dialog is titled 'Add HTTP Header' and contains the following fields and controls:

- Name:** A text input field labeled 'Header name'.
- Value:** Two radio buttons: 'Allowed' (selected) and 'Blocklisted'.
- Action:** Two radio buttons: 'Alert' (selected) and 'Prevent'.
- Blocklisted values:** A text input field labeled 'Comma separated values'.
- Required:** A toggle switch labeled 'Off'.

At the bottom right of the dialog are two buttons: 'Cancel' and 'Create HTTP Header'.

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_access_control.html

File Uploads

Configure WAAS to protect against malicious file uploads. Configure file uploads to explicitly allow file extensions, while alerting or preventing other file extensions.

The screenshot shows the 'File Uploads' configuration page in the Palo Alto Networks Prisma Cloud Admin console. The page has a toggle switch for 'File uploads' which is currently 'On'. Below the toggle, there is a section for 'Explicitly allowed file extensions' with a text input field for 'List of allowed extensions without leading dot (e.g., .jpg, docx, zip)'. To the right of this field is a warning icon and the text 'Action for all others', followed by two radio buttons: 'Alert' (selected) and 'Prevent'.

Below this section, there are five columns of file extensions, each with a checkbox:

- Audio:** ☐ aac, ☐ mp3, ☐ wav
- Compressed archives:** ☐ 7zip, ☐ gzip, ☐ rar, ☐ zip
- Documents:** ☐ odf, ☐ Office legacy, ☐ Office Open XML, ☐ pdf
- Images:** ☐ bmp, ☐ gif, ☐ ico, ☐ jpeg, ☐ png
- Video:** ☐ avi, ☐ mp4

4.2.5 Configure bot protection

WAAS can detect bot activity and protect your apps from coordinated attacks. There are several bot categories. Some bots are known and deemed good. Other bots are malicious and can compromise your apps. Become familiar with the various bot categories and the static and active methods used to detect bots.

For each bot category, configure an Effect method of Alert, Prevent, or Ban.

Known bots		Unknown bots	Active bot detection	User defined bots	
Bot category		Effect			
Generic bots		Disable	Alert	Prevent	Ban
Web automation tools		Disable	Alert	Prevent	Ban
Web scrapers		Disable	Alert	Prevent	Ban
API libraries		Disable	Alert	Prevent	Ban
HTTP libraries		Disable	Alert	Prevent	Ban
Request anomalies	Lax enforcement	Disable	Alert	Prevent	Ban
Bot impersonators		Disable	Alert	Prevent	Ban
Browser impersonators		Disable	Alert	Prevent	Ban

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/waas/waas_bot_protection.html

4.3 Investigate WAAS Runtime Audit

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit.html>

4.3.1 Determine the reasons for a WAAS runtime audit

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/audit/host_activity.html

5 DevSecOps Security (Shift Left)

In this domain, you can validate your knowledge of how to integrate Prisma Cloud capabilities into DevSecOps practices.

5.1 Implement scanning for IAC templates.

Infrastructure as code (IaC) allows the infrastructure's configuration to be specified, including the network topology and server configurations, as a text file. Prisma Cloud can scan these files for vulnerabilities and compliance problems before they are instantiated into a working configuration.

```
# Specify the template type. Valid values are as follows.
# - For Terraform: TF
# - For AWS CloudFormation: CFT
# - For Kubernetes: K8S

template_type: TF

# The valid values for terraform_version are 0.11 or 0.12

terraform_version: 0.11

# If terraform_version is 0.11, then terraform_011_parameters
# is required.
# The value for variable_files is an array of custom variable file
# names. The path of each file is relative to your repository
# branch root directory
# The value for variable_values is an array of name/value pairs
# that identify the input variables your template uses.

terraform_011_parameters:
variable_files:
- scan/rich-value-types/network/variables.tf
variable_values:
- name: check
  value: public-read-write
```

The information in the configuration files is queried by means of a JSON query, even if those files are written in a different standard, such as YAML.

Add Config Policy

1 Details 2 Build Your Rule 3 Compliance Standards 4 Remediation

Run Build

This is a policy subtype for IaC scan during DevOps process

Template Type *

Terraform, CloudFormation

▼ Terraform

Cloud Type *

AWS

JSON Query *

✓ \$.resource[*].aws_s3_bucket exists and (\$.resource[*].aws_s3_bucket[*].versioning[*].enabled does not exist or \$.resource[*].aws_s3_bucket[*].versioning[*].enabled anyFalse)

> CloudFormation

Previous Next Cancel Confirm 6 ?

5.1.1 Differentiate between Terraform and CloudFormation scanning configurations

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/set-up-your-prisma-cloud-configuration-file-for-iac-scan.html#id3fa84acb-db42-46ab-a3bc-d19e7589c47e_id06996fc0-8d8e-4bd0-ae3f-423d2b7d2d7a

5.1.2 List of out-of-the-box (OOTB) IaC scanning integrations

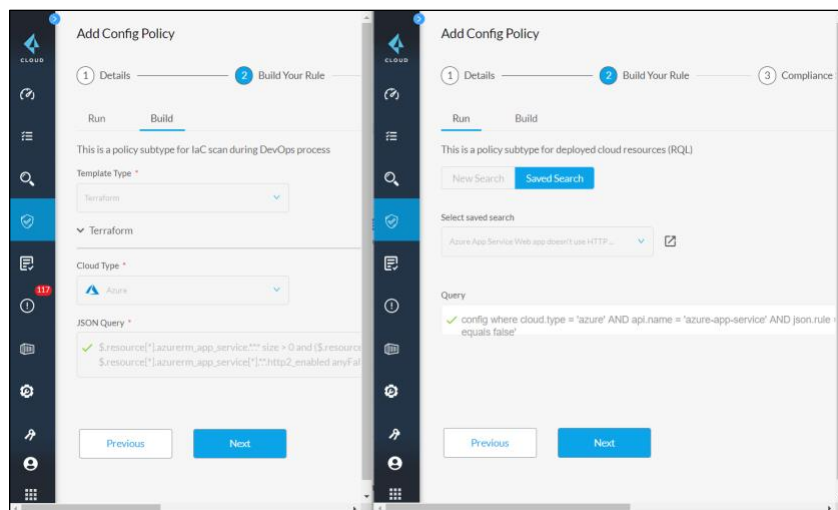
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/set-up-your-prisma-cloud-configuration-file-for-iac-scan.html>

5.1.3 Configure API scanning for IaC templates

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-devops-security/use-the-prisma-cloud-iac-scan-rest-api.html>

5.2 Configure policies in the Console for IaC scanning

Policies can be defined in Prisma Cloud to scan IaC files during the build process. Three types of files are supported: CloudFormation, Terraform, and Kubernetes. The primary difference between compliance policies for runtime and build-time is that runtime-compliance policies are written as RQL queries and build-time-compliance policies are written as JSON queries.



5.2.1 Review OOTB policies for IaC scanning

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase.html>

5.2.2 Configure custom-build policies for IaC scanning

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy/prisma-cloud-create-config-build-policy.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-policies/create-a-policy/prisma-cloud-iac-scan-policy-operators.html>

5.3 Integrate Compute scans into CI/CD pipeline

Continuous integration and continuous delivery (CI/CD) systems automatically identify when a module, such as a container or a serverless function, is ready to be pushed into the pipeline. After a module is pushed, it goes through multiple tests before it is actually deployed as part of an application. Prisma Cloud allows one of those scans to be a compliance test. If you are using Jenkins or CloudBees, you can use the plugin. For other systems you will need to add a call to the executable, called **twistcli**.

5.3.1 Integrate container scans into the CI/CD pipeline

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_plugin.html

5.3.2 Integrate serverless scans into CI/CD pipeline

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/serverless_functions

5.3.3 Identify different options for scanning: twistcli and plugins

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_plugin.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_freestyle_project.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_maven_project.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/jenkins_pipeline_project.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/cloudbees_core_pipeline_k8s.html

5.4 Configure CI policies for Compute scanning

With these policies, you control the Prisma Cloud Compute scan during the continuous-integration process. These scans can identify compliance issues and vulnerabilities.

Create new compliance rule

Rule name

Enter rule name

PCI

Notes

Enter notes

1

Compliance actions

Filter

image

Set action for all checks

Ignore

Alert

Fail

ID	Type	Severity	Action	Description
406	image	medium	<div>Ignore</div> <div>Alert</div> <div>Fail</div>	Add HEALTHCHECK instruction to the container image
41	image	high	<div>Ignore</div> <div>Alert</div> <div>Fail</div>	Image should be created with a non-root user

Create new vulnerability rule

Rule name

Enter rule name

Notes

Enter notes

Severity based actions

Alert threshold

Off

Low

Medium

High

Critical

Alert on [Low, Medium, High, Critical]

Failure threshold

Off

Low

Medium

High

Critical

Failure disabled

Scope

Images

* Specify an image

Labels

* Specify a label (e.g., to filter by project use JOB_NAME:<project>)

[Advanced settings](#)

5.4.1 Review default CI policies for Compute scanning

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins.html
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase.html>

5.4.2 Configure custom CI policies for Compute scanning

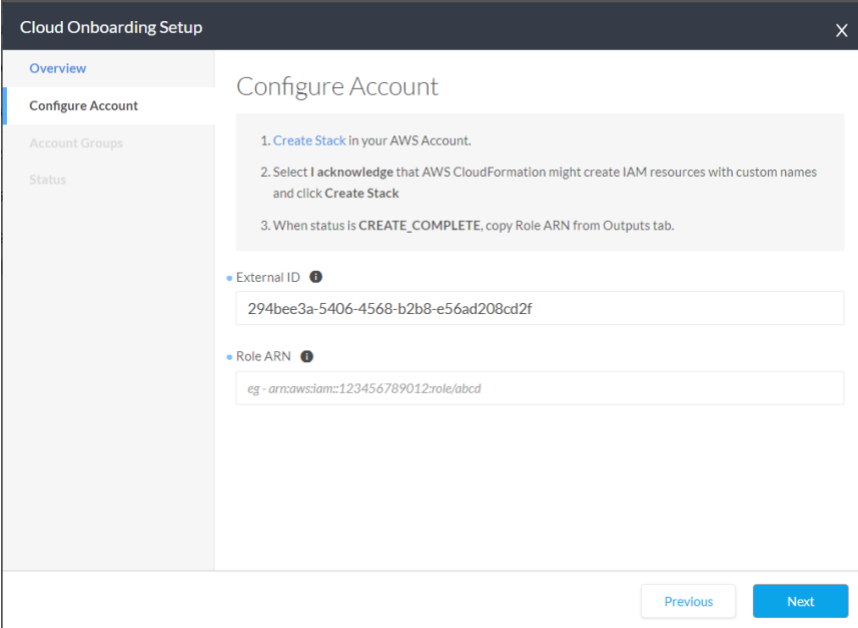
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/continuous_integration/set_policy_ci_plugins.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/custom_compliance_checks.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/compliance/extensible_compliance_checks.html

6 Prisma Cloud Administration

In this domain, you can validate your knowledge of how to administer Prisma Cloud.

6.1 Onboard accounts

Before Prisma Cloud can manage your cloud accounts, it needs certain information and appropriate permissions. These permissions depend on the cloud type and the mode in which you will use Prisma Cloud. The platform can be used in a detect mode (monitor mode) or in a detect-and-correct mode (monitor and protect mode).



The screenshot shows the 'Cloud Onboarding Setup' window with the 'Configure Account' tab selected. The left sidebar contains 'Overview', 'Configure Account', 'Account Groups', and 'Status'. The main area displays instructions for creating an AWS account and fields for 'External ID' and 'Role ARN'. The 'External ID' field contains the value '294bee3a-5406-4568-b2b8-e56ad208cd2f'. The 'Role ARN' field contains the value 'eg - arn:aws:iam::123456789012:role/abcd'. At the bottom right are 'Previous' and 'Next' buttons.

Cloud Onboarding Setup

Overview

Configure Account

Account Groups

Status

Configure Account

1. Create Stack in your AWS Account.
2. Select I acknowledge that AWS CloudFormation might create IAM resources with custom names and click Create Stack
3. When status is CREATE_COMPLETE, copy Role ARN from Outputs tab.

External ID ⓘ

294bee3a-5406-4568-b2b8-e56ad208cd2f

Role ARN ⓘ

eg - arn:aws:iam::123456789012:role/abcd

Previous Next

6.1.1 Onboard cloud accounts

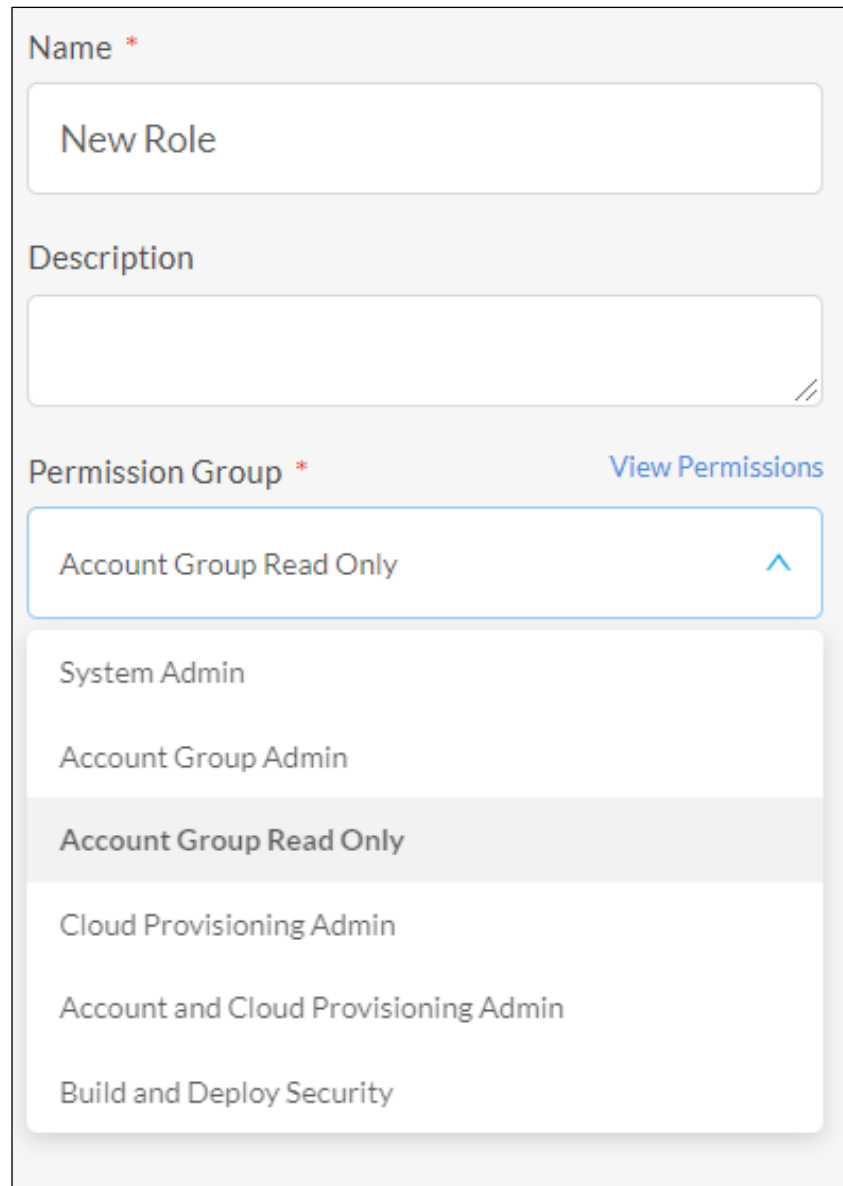
- https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma/prisma-cloud/prisma-cloud-admin/connect-your-cloud-platform-to-prisma-cloud/onboard-your-aws-account.html
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/connect-your-cloud-platform-to-prisma-cloud/onboard-your-azure-account.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/connect-your-cloud-platform-to-prisma-cloud/onboard-your-gcp-account.html>

6.1.2 Configure account groups

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-account-groups>

6.2 Configure RBAC

Security systems are a high-priority target for attackers. If they can steal the credentials of a Prisma Cloud security administrator, they can stop the data collection of Prisma Cloud and disable all the Defenders of Prisma Cloud Compute.



The screenshot shows a web form for configuring a new role. It includes a 'Name' field with a red asterisk, a 'Description' field, and a 'Permission Group' dropdown menu with a red asterisk. A 'View Permissions' link is located to the right of the dropdown. The dropdown menu is open, showing a list of permission groups: 'Account Group Read Only' (highlighted), 'System Admin', 'Account Group Admin', 'Cloud Provisioning Admin', 'Account and Cloud Provisioning Admin', and 'Build and Deploy Security'.

Name *

New Role

Description

Permission Group * View Permissions

Account Group Read Only ^

System Admin

Account Group Admin

Account Group Read Only

Cloud Provisioning Admin

Account and Cloud Provisioning Admin

Build and Deploy Security

6.2.1 Differentiate between Prisma Cloud and Compute roles

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/prisma-cloud-admin-permissions.html>

6.2.2 Configure Prisma Cloud and Compute roles

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/prisma-cloud-administrator-roles.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/prisma-cloud-admin-permissions.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/manage-roles-in-prisma-cloud.html>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/authentication/prisma_cloud_user_roles.html

6.3 Configure the admission controller

The Kubernetes specifications include the ability to consult an admission controller, which is a piece of code that intercepts requests to the Kubernetes API server after requests are authenticated and authorized, but before the operation is saved.

The Prisma Cloud Compute Open Policy Agent accepts policies from the user interface, converts them to the Rego language, and uses them to decide whether to permit requests or reject them. If you need more complicated processing, you can write Rego expressions and import them.

Edit Default - deny all

Standard | Advanced

Rule name: Default - deny all

Notes:

Effect: ☒ Deny | Audit allowed actions: ☐ Off

Show: All Categories | ☒ All

Actions:

Configs

- ☒ config_create
- ☒ config_remove
- ☒ config_inspect
- ☒ config_update
- ☒ config_list

Containers

- ☒ container_archive
- ☒ container_archive_head
- ☒ container_attach

6.3.1 Configure defender as an admission controller

- <https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/access-control/open-policy-agent.html>

6.3.2 Create open policy agent (OPA) policies

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/access-control/open-policy-agent.html>
- <https://www.openpolicyagent.org/docs/latest/>
- <https://www.openpolicyagent.org/docs/latest/policy-language/>

6.4 Configure logging

Any user-facing system should have an Audit log, so you can see what those users did and when. Audit logs are particularly important in a security system, such as Prisma Cloud. To locate the user Audit logs for Prisma Cloud, go to **Settings > Audit Logs** (for Prisma Cloud) and **Manage > View Logs** (for Prisma Cloud Compute).

TIME ↓	USER ↓↑	IP ADDR... ↓↑	RE... ↓↑	NAME ↓↑	OPERATION ↓↑
A day ago	ori@securedynamics.net	99.16.140.5	Login	ori@securedynamics.net	'ori@securedynamics.net'(with role 'System Admin':'System Admin') logged in via SSO-SA
A day ago	ori@securedynamics.net	99.16.140.5	Login	ori@securedynamics.net	'ori@securedynamics.net'(with role 'System Admin':'System Admin') logged in via SSO-SA
A day ago	ori@securedynamics.net	174.197.7.120	Login	ori@securedynamics.net	'ori@securedynamics.net'(with role 'System Admin':'System Admin') logged in via SSO-SA

Type	User	Source IP	API	Status	Date
login	ori@securedyn...	10.240.0.44	/api/v1/authenticate	successful login attempt	Sep 18, 2020 2:01:37 PM
login	ori@securedyn...	10.240.0.44	/api/v1/authenticate	successful login attempt	Sep 18, 2020 1:59:58 PM
login	ori@securedyn...	10.240.0.212	/api/v1/authenticate	successful login attempt	Sep 18, 2020 12:40:18 ...

6.4.1 Familiarize with audit logging

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/view-audit-logs>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit.html>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/audit_admin_activity
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/host_activity.html

6.4.2 Enable defender logging

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/kubernetes_auditing

6.5 Manage enterprise settings

Several enterprise settings are global within a single Prisma Cloud instance, including those that refer to machine learning for anomaly detection.

Enterprise Settings

Anomaly Enterprise Settings can now be found here

User Idle Timeout * ⓘ

Custom ▼

120

Mins

Auto enable new default policies of the type: ⓘ

☐ High

☐ Medium

☐ Low

Make Alert Dismissal Reason Mandatory ⓘ

☐

Populate User Attribution In Alerts Notifications ⓘ

☐

Anomaly Settings

Alerts and Thresholds

Anomaly Trusted List

▼ Network

	Alert Disposition	Training Model Threshold
Port scan activity (External) Current policy settings to detect an external host scanning a local instance.	Conservative	
Port scan activity (Internal) Current policy settings to detect a local instance scanning another host.	Conservative	
Port sweep activity (External) Current policy settings to detect an external host scanning multiple local instances, on the same port.	Conservative	
Port sweep activity (Internal) Current policy settings to detect a local instance scanning multiple hosts, on the same port.	Conservative	
Spambot activity Current policy settings to detect a local host with no prior history of outbound SMTP traffic.	Conservative	High
Unusual protocol activity (External) Current policy settings to detect outbound traffic using a protocol not previously observed.	Conservative	High
Unusual protocol activity (Internal) Current policy settings to detect internal traffic using a protocol not previously observed.	Conservative	High

Port scan activity (External)

Alert Disposition

Conservative

☒ Conservative ☐ Moderate ☐ Aggressive

Generate alerts when scan activity includes 500 ports or more.

Reset

Close

> Unusual User Activity / UEBA

Familiarize yourself with the enterprise settings

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings>

6.5.1 Differentiate Anomaly settings

- <https://www.paloaltonetworks.com/cyberpedia/what-is-ueba>
- <https://blog.paloaltonetworks.com/2020/01/cloud-ueba/>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings#id5326b191-bf23-4545-bc05-620d113bf54d_id6f5bd95c-b5b5-48bf-b397-312f4de3e08c

6.5.2 Configure idle timeout

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings#id5326b191-bf23-4545-bc05-620d113bf54d_idd4770f5f-a3c1-4886-ad80-e4be14f04f98

6.5.3 Set auto-enable policies

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings#id5326b191-bf23-4545-bc05-620d113bf54d_id896a5270-03cf-4518-8f43-eddce70d922d

6.5.4 Set mandatory-dismissal reason

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/define-prisma-cloud-enterprise-settings#id5326b191-bf23-4545-bc05-620d113bf54d_id896a5270-03cf-4518-8f43-eddce70d922d

6.5.5 Enable user attribution

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/setup-sso-integration-on-prisma-cloud/set-up-jit-on-okta.html>

6.6 Understand third-party integrations

Most Prisma Cloud deployments are “brown field,” which means that the organization is adding Prisma Cloud to an existing infrastructure. This task connects Prisma Cloud to that existing infrastructure to enable notifications in both directions.

The screenshot shows the 'Add Integration' configuration page in the Prisma Cloud interface. The left sidebar contains navigation links: Dashboard, Inventory, Investigate, Policies, Compliance, Alerts (117), Compute, Settings (selected), SSO, Integrations, Trusted IP Addresses, Licensing, and Audit Logs. The main content area is titled 'Add Integration' and has two steps: 1 Configuration and 2 Test and Save. The 'Integration Type' is set to 'Slack'. The 'Integration Name' is 'prisma-cloud-to-slack'. The 'Description' field is empty. The 'Webhook URL' is 'https://hooks.slack.com/services/...'. A 'Next' button is at the bottom. A blue question mark icon with the number 7 is in the bottom right corner.

The screenshot shows the 'Create new profile' configuration page. The 'Name' field is 'Post to slack channel' and the 'Provider' is 'Slack'. The 'Alert settings' section includes the 'Incoming Webhook URL' (https://hooks.slack.com/services/...), 'Channels' (sec-alerts x, e.g., general), and 'Users' (e.g., slackbot). A note states: 'Avoid targeting too many users for alert messages because Slack is not designed to handle large message bursts.' The 'Alert triggers' section lists: Access, Admission Audits, Cloud Native App, Firewall, Cloud Native, Network Firewall, Container and Image, and Vulnerabilities. The 'Alert on' section has a dropdown menu with 'All rules' selected. Below it, 'Select rules to be alerted on' has two options: 'Default - ignore Twistlock components' (checked) and 'Default - alert all components' (unchecked). 'Cancel' and 'Save' buttons are at the bottom right.

6.6.1 Understand inbound and outbound notifications

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts.html>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/alert_mechanism.html
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/email.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/alerts/slack.html>
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud.html>

6.6.2 Configure third-party integration for alerts

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/configure-external-integrations-on-prisma-cloud/prisma-cloud-integrations>
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/annotate_audits.html
- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/audit/logging.html>

6.7 Leverage Cloud and Compute APIs

The Compute API allows you to integrate Prisma Cloud Compute into systems that need the information. For example, the enterprise can use a custom dashboard to see the major issues that are happening right now.

6.7.1 Authenticate with APIs

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/api/access_api.html
- https://cdn.twistlock.com/docs/api/twistlock_api.html#authenticate_client

6.7.2 Locate API documentation

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/api.html>
- https://cdn.twistlock.com/docs/api/twistlock_api.html

6.7.3 List policies by API

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/api/manage_compliance_api.html
- https://cdn.twistlock.com/docs/api/twistlock_api.html#policies

6.7.4 Manage alerts using APIs

- https://cdn.twistlock.com/docs/api/twistlock_api.html#alert_profiles

6.7.5 Create reports using APIs

- https://cdn.twistlock.com/docs/api/twistlock_api.html#containers
- https://cdn.twistlock.com/docs/api/twistlock_api.html#hosts
- https://cdn.twistlock.com/docs/api/twistlock_api.html#images
- https://cdn.twistlock.com/docs/api/twistlock_api.html#pcf_droplets
- https://cdn.twistlock.com/docs/api/twistlock_api.html#registry
- https://cdn.twistlock.com/docs/api/twistlock_api.html#scans
- https://cdn.twistlock.com/docs/api/twistlock_api.html#serverless

6.7.6 Download vulnerability results via API

- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/api/manage_compliance_api.html
- https://cdn.twistlock.com/docs/api/twistlock_api.html#containers
- https://cdn.twistlock.com/docs/api/twistlock_api.html#hosts
- https://cdn.twistlock.com/docs/api/twistlock_api.html#images
- https://cdn.twistlock.com/docs/api/twistlock_api.html#pcf_droplets
- https://cdn.twistlock.com/docs/api/twistlock_api.html#registry
- https://cdn.twistlock.com/docs/api/twistlock_api.html#scans
- https://cdn.twistlock.com/docs/api/twistlock_api.html#serverless

6.7.7 Configure Single Sign On

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/setup-sso-integration-on-prisma-cloud.html>

6.7.8 Use the access key

- <https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-administrators/create-access-keys.html>

Sample Questions

Note: Answers are in the “Answers to Sample Questions” section.

Locate and download Prisma Cloud release software

1. Which registry do you use to download the Prisma Cloud Compute Defender image?
 - a. registry.redlock.com
 - b. registry.twistlock.com
 - c. registry.prisma.com
 - d. registry.paloaltonetworks.com
2. What is a valid tag for a Prisma Cloud Compute Docker image?
 - a. defender_20.04.177
 - b. defender.20.04.177
 - c. defender_20_04_177
 - d. defender-20-04-177
3. An organization that uses a private cloud in a black site that has no internet connection can use which product?
 - a. Google Cloud
 - b. AWS S3 Management.
 - c. Prisma Cloud Compute
 - d. Prisma Cloud

Install the Console in a Onebox configuration

4. In Prisma Cloud Compute, what is the default HTTPS port for the Console?
 - a. 443
 - b. 8083
 - c. 8443
 - d. 9443
5. What is the name of the configuration file that controls a Onebox configuration?
 - a. twistlock.cfg
 - b. twistlock.json
 - c. redlock.cfg
 - d. redlock.json

Install the Console in Kubernetes

6. In which format does the twistcli create the configuration file for the Console when using Kubernetes?
 - a. JSON
 - b. YAML
 - c. XML
 - d. CSV
7. What are the two external items that need to be deployed in Kubernetes together with a console? (Choose two.)
 - a. a database (DB) to store the console's state
 - b. a load balancer, which is used to expose the console to the network
 - c. an ephemeral volume (EV) for the console's temporary data
 - d. a Kubernetes authorization engine to make sure only authorized administrators use the console
 - e. a persistent volume (PV) to store the console's state

Perform upgrade on the console

8. What is the procedure to upgrade a non-SaaS Prisma Cloud Compute implementation?
 - a. manually upgrade the console, then manually upgrade the Defenders
 - b. manually upgrade the Defenders, then manually upgrade the console
 - c. manually upgrade the console, which then automatically upgrades the Defenders
 - d. manually upgrade both the console and Defenders in any order
9. Which command do you use to upgrade the console in Kubernetes?
 - a. **kubectl apply -f twistlock_console.yaml**
 - b. **kubectl upgrade -f twistlock_console.yaml**
 - c. **twistcli apply -f kubectl.yaml**
 - d. **twiscli upgrade -f kuberctl.yaml**

Deploy Container Defenders

10. Which command do you use to install a container Defender on Linux?
 - a. **rpm**
 - b. **apt install**
 - c. either **rpm** or **apt install**, depending on the Linux distribution
 - d. **curl**

11. How does the Docker Defender receive information from the console?
- a. Pull, the Docker Defender connects to the console using TCP to ask for the information.
 - b. Pull, the Docker Defender connects to the console using UDP to ask for the information.
 - c. Push, the Docker Defender listens on a TCP port to receive information from the console.
 - d. Push, the Docker Defender listens on a UDP port to receive information from the console.
12. The TCP listener setting in a Docker Defender running on Linux allows the Defender to function as what?
- a. a firewall
 - b. a Docker proxy
 - c. an SSH proxy
 - d. an HTTP proxy
13. Where do you install the Docker Defender?
- a. on the hosts that run the Docker containers of the application
 - b. on the images that become the Docker containers of the application
 - c. on the Docker containers that implement the application
 - d. on both the hosts and the images

Deploy Host Defenders

14. How do you deploy a host Defender on Windows?
- a. Download an .msi package using the browser.
 - b. Run the provided command line using the old (cmd.exe) shell.
 - c. Run the provided command line using PowerShell.
 - d. Download an .exe command package using the browser.
15. Which two versions of Windows support the host Defender? (Choose two.)
- a. Windows 10
 - b. Windows 2016
 - c. Windows 2017
 - d. Windows 2019

16. Which version of Windows supports the host Defenders runtime defense functionality?
- a. Windows 10
 - b. Windows 2016
 - c. Windows 2017
 - d. Windows 2019

Deploy Serverless Defenders

17. Which serverless platform is supported by the serverless layer deployment type?
- a. AWS Lambda
 - b. GCP Cloud
 - c. GCP On-Premises
 - d. Azure
18. Which three runtimes are supported by the serverless Defender? (Choose three.)
- a. PowerShell
 - b. Ruby
 - c. Node.js
 - d. C#
 - e. Python
19. Which three serverless platforms are supported by the serverless embedded deployment type? (Choose three.)
- a. AWS Lambda
 - b. GCP Cloud
 - c. GCP On-Premises
 - d. Azure Functions
 - e. Google App Engine

Deploy App-embedded Defenders

20. Where do you install an app-embedded Defender?
- a. on the hosts that run the Docker containers of the application
 - b. on the images that become the Docker containers of the application
 - c. on the Docker containers that implement the application
 - d. on both the hosts and the images
21. Which option is not a way to deploy an app-embedded Defender?
- a. Fargate
 - b. Dockerfile
 - c. Shell script
 - d. manual

Configure networking for Defender to Console connectivity

22. How do alerts propagate from the Defenders to the Console in Kubernetes?
- a. Pull, the console connects to port 8083 on the Defender.
 - b. Pull, the console connects to port 8084 on the Defender.
 - c. Push, the Defender connects to port 8083 on the console.
 - d. Push, the Defender connects to port 8084 on the console.

Perform upgrades on Defenders

23. What is the usual order of upgrades if you use a self-hosted console in Prisma Cloud Compute?
- a. The console identifies that there's a new version, upgrades itself automatically, and then upgrades the Defenders automatically.
 - b. The console identifies that there's a new version and upgrades itself automatically. You then upgrade the Defenders manually during a scheduled maintenance window.
 - c. You upgrade the console manually, and then it upgrades the Defenders automatically.
 - d. You upgrade both the console and Defenders manually.

24. Can Defender upgrades be restricted to a specific window of time?
- a. No. Upgrades happen automatically. However, those upgrades do not cause downtime.
 - b. You can disable auto-upgrade, but then you can't upgrade the Defenders. You need to uninstall and reinstall them for the upgrade.
 - c. You can disable auto-upgrade, and then upgrade the Defenders during the window from the web-based interface (Action > Upgrade).
 - d. You can specify the maintenance window in the console, and then Defender upgrades will happen only during that time.

Understand policies related to compliance standards

25. How many queries can a policy include? How many standards?
- a. one query, one standard
 - b. one query, multiple standards
 - c. multiple queries, one standard
 - d. multiple queries, multiple standards

Build custom policies

26. Which three protocols are identified by the following RQL query? (Choose three.)
- a. protocol='TCP' AND dest.port IN (21,23,80) AND source.publicnetwork IN ('Internet IPs' , 'Suspicious IPs')
 - b. HTTP
 - c. Telnet
 - d. SSH
 - e. HTTPS
 - f. FTP
27. Which parameter can you use in RQL to look at a field that Prisma Cloud does not parse?
- a. config.external
 - b. json.value
 - c. json.rule
 - d. config.internal

Identify policy types

28. Which of the following is not a Prisma Cloud policy category?
- a. Config
 - b. Network
 - c. Anomaly
 - d. Audit Event
29. Which two Prisma Cloud policy categories allow you to be reactive, but not proactive? (Choose two.)
- a. Config
 - b. Network
 - c. Anomaly
 - d. Audit Event
 - e. User Activity

Understand alert states

30. What is the alert state after the next scan when Prisma Cloud detects that excessive access was allowed to an AWS S3 bucket?
- a. Open
 - b. Resolved
 - c. Closed
 - d. Deleted
31. Which two alert states would be used by an administrator that is trying to hide the alerts caused by their actions? (Choose two.)
- a. Open
 - b. Resolved
 - c. Snoozed
 - d. Dismissed
 - e. Closed

Build alert rules

32. Which option shows the targets that an alert rule-checks?
- a. policies
 - b. users
 - c. cloud accounts
 - d. account groups

Create alert notifications

33. Which request type do web hooks use?
- a. GET
 - b. POST
 - c. PUT
 - d. ALERT
34. Which two integrations can send alerts to a system that is behind dynamic source-address translation? (Choose two.)
- a. Tenable
 - b. Webhooks
 - c. Email
 - d. Qualys
 - e. Slack

Investigate alerts

35. How should an administrator respond to an alert opened at 2 a.m. and resolved at 4 a.m.
- a. Verify the Alert log file to gather additional information to investigate the occurrence in detail.
 - b. Investigate further. Somebody may have disabled a safeguard at 2 a.m., committed a crime, and re-enabled it at 4 a.m. to avoid detection.
 - c. Evidence of malware is clear. The administrator must shut down the system in which it occurred.
 - d. Document the incident. If it happens multiple times it needs to be investigated.

36. An alarm resulted from device A connecting to device B. Which device should you investigate first?
- a. Device A
 - b. Device B
 - c. The network firewalls
 - d. The device that contains more valuable information

Understand inbound and outbound notifications

37. In which format are alert details provided to accepting systems?
- a. XML
 - b. JSON
 - c. CSV
 - d. HTTP
38. Which is not a field in the alert notification?
- a. accountName
 - b. policyLabels
 - c. riskLevel
 - d. alertRemediationCli

Investigate resource configuration with RQL

39. What does this query mean on GCP?
- a. `api.name='gcloud-sql-instances-list'` and `json.rule = 'settings.ipConfiguration.requireSsl is true'`
 - b. list instances where SSL is configured
 - c. list instances where SSL is not configured
 - d. list SQL instances where SSL is configured
 - e. list SQL instances where SSL is not configured
40. This query looks for which type of S3 buckets with rules?
- a. `api.name='aws-s3api-get-bucket-acl'` AND `json.rule="(acl.grants[?(@.grantee=='AllUsers')].size>0)"`
 - b. allow access to all users
 - c. deny access to all users
 - d. allow access to some external users
 - e. deny access to some external users

Investigate user activity using RQL

41. You suspect that the desktop at IP 6.6.6.6 has malware. Which event query will show whether malware performed any cloud activity on your instances?
- a. event where sourceIP IN (6.6.6.6)
 - b. event where ip IN (6.6.6.6)
 - c. event where inetIP IN (6.6.6.6)
 - d. event where adminIP IN (6.6.6.6)
42. You type this query: event where user = 'root'. Where would the events you see originate?
- a. AWS
 - b. Azure
 - c. GCP
 - d. Google Cloud

Investigate network activity using RQL

43. You suspect that the desktop at 6.6.6.6 has malware. Which two queries will show whether it contacted any suspicious IPs? (Choose two.)
- a. network where source.ip = 6.6.6.6 AND dest.publicnetwork = 'Suspicious IPs'
 - b. network where source.ip = 6.6.6.6 AND dest.ip IN ('Suspicious IPs')
 - c. network where source.publicnetwork = 'Suspicious IPs' AND dest.ip = 6.6.6.6
 - d. network where source.ip = 'Suspicious IPs' AND dest.ip = 6.6.6.6
 - e. network where source.ip = 6.6.6.6 OR dest.ip = 6.6.6.6
44. Which traffic will the following query identify?
- a. dest.resource IN (resource where virtualnetwork.name != 'default')
 - b. IP addresses of resources that are in the virtual network default
 - c. IP addresses of resources that are not in the virtual network default
 - d. traffic events where the destination is in the virtual network default
 - e. traffic events where the destination is not in the virtual network default

Investigate anomalous user event(s)

45. What is a valid anomaly type?
- a. too many login attempts
 - b. impossible time travel (account hijacking)
 - c. new device
 - d. excessive login failures

46. Which is a valid anomaly type for a device?
- a. fingerprint
 - b. retinal scan
 - c. MAC address
 - d. IP address

Identify inventory of resources in a cloud account

47. In a Prisma Cloud asset inventory, which is not an option for the Assets by Classification widget?
- a. Cloud Type (AWS, Alibaba Cloud, GCP, Azure)
 - b. Asset Type (Instance, Network, Database, etc.)
 - c. Account Name
 - d. Region
48. Which two criteria can be used to filter the asset inventory? (Choose two.)
- a. Resource Type
 - b. CIDR Network Block
 - c. Resource Name
 - d. Standard
 - e. IP Type (Internal vs. External)

Identify how to check the resource-configuration history

49. Which two template types are supported by build rules? (Choose two.)
- a. JavaScript
 - b. CloudFormation
 - c. Bash scripts with configuration commands
 - d. Terraform
 - e. XML
50. Which type of query do you use to validate that a build policy is being followed?
- a. SQL query
 - b. JavaScript code to calculate the answer
 - c. RQL
 - d. JSON query

Use API for automation of tasks

51. Your auditor wants a weekly report of how compliant you were with SOC 2. Can you do it, and if so how?
- a. No. You can get only current compliance.
 - b. You can automate it from the web interface.
 - c. Do a GET
`https://api.prismacloud.io/compliance/posture?timeType=relative&timeAmount=<n>&timeUnit=week&policy.complianceStandard=SOC%202, loop on <n>`
 - d. Do a GET `https://api.prismacloud.io/compliance/SOC2?timeType=relative&timeAmount=<n>_weeks, loop on <n>`
52. How can you delete Audit log entries older than a year?
- a. Audit log entries are not under administrator control.
 - b. You can do it from the web interface.
 - c. Do a DELETE
`https://api.prismacloud.io/audit/redlock?timeType=relative&timeAmount=1&timeUnit=year`
 - d. Do a DELETE
`https://api.prismacloud.io/audit/redlock?timeType=absolute&time=<<one year ago, in ISO 8601 notation, YYYY-MM-DD>>`

Use API for custom queries

53. Which format do you use with a config search?
- a. RQL
 - b. SQL
 - c. JSON query
 - d. XML query
54. Which HTTP method do you use with an event search?
- a. GET
 - b. PUT
 - c. POST
 - d. HEAD

Understand how to investigate Docker image vulnerabilities

55. Which of these is not a tab in the registry details for a Docker image?
- a. Layers
 - b. Process Info
 - c. Network Connections
 - d. Packages

Configure Image Vulnerability policy

56. Which vulnerability rule policy does not make sense?
- a. Alert threshold Low, Block threshold: Medium
 - b. Alert threshold Low, Block threshold: High
 - c. Alert threshold Medium, Block threshold: Low
 - d. Alert threshold Low, Block threshold: Medium
57. What are three ways to limit the applicability of a vulnerability rule? (Choose three.)
- a. scope (containers, images, etc.)
 - b. operating system (Linux vs. Windows)
 - c. cloud environment (AWS vs. Azure vs. GCP)
 - d. exceptions to the rule by CVEs and/or tags
 - e. apply the rule only if there is a vendor fix

Understand how to investigate host vulnerabilities

58. Which type of virtual machine can Prisma Cloud scan without running an agent on it?
- a. Amazon Machine Image (AMI) running Linux
 - b. Amazon Machine Image (AMI) running Linux or Windows
 - c. Any VM image on the three major cloud providers (AWS, Azure, and GCP) running Linux
 - d. Any VM image on the three major cloud providers (AWS, Azure, and GCP) running Windows

59. How can Prisma Cloud Compute detect vulnerabilities in software installed directly rather than through a package manager?
- a. It uses the MD5 Hash Generator of the executables to know what is running.
 - b. Some apps are so popular that they are supported if you activate unpackaged scan in the web interface.
 - c. Some apps are so popular that they are supported. This action is activated automatically.
 - d. It uses the MD5 of executables to know what is running.

Configure Host Vulnerability policy

60. Which image vulnerability policy field is not available in Host Vulnerability policies?
- a. Alert threshold
 - b. Block threshold
 - c. Apply rule only when vendor fixes are available
 - d. Exceptions
61. Which two criteria can you use for exceptions in a Host Vulnerability policy? (Choose two.)
- a. CVE ID
 - b. OS version
 - c. Is there a vendor fix available?
 - d. Severity
 - e. Tag

Understand how to investigate Docker image and cloud compliance

62. If a Docker image raises a high-severity compliance concern, what is the first digit of the compliance ID?
- a. 2
 - b. 3
 - c. 4
 - d. 5
63. If a Docker container raises a medium-severity compliance concern, what is the first digit of the compliance ID?
- a. 2
 - b. 3
 - c. 4
 - d. 5

Configure Docker image and Container Compliance policy

64. Which is not a valid action for a Docker compliance rule?
- a. Ignore
 - b. Alert
 - c. Remediate
 - d. Block
65. Which three criteria can be used to restrict the scope of a container and image-compliance rule? (Choose three.)
- a. Container name
 - b. Image name
 - c. Tag
 - d. Cloud type (AWS, Azure, and/or GCP)
 - e. Label
66. Which is not a compliance template that can be used for a Container Compliance policy?
- a. GDPR
 - b. ISO 27001
 - c. PCI
 - d. HIPAA

Understand how to investigate host compliance

67. Which category and type identify the compliance problem described in the following statement?
- “While the system administrator can establish secure permissions for users’ home directories, the users can easily override these.”
- a. Windows, host
 - b. Linux, host
 - c. Docker, daemon config
 - d. Apache, daemon config
68. Which entity creates the host compliance policies that Prisma Cloud checks?
- a. Palo Alto Networks research department
 - b. Center for Internet Security
 - c. Committee for Information Safety
 - d. National Institute of Standards and Technology

Configure Host Compliance policy

69. Which two fields can be used to limit the scope of a host compliance rule? (Choose two.)
- a. Operating system
 - b. Tag
 - c. Account ID
 - d. Host name
 - e. Project ID
70. If you keep the default policy, what action is performed on each severity level?
- a. Low: Ignore, Medium: Alert, High: Alert, Critical: Block
 - b. Low: Ignore, Medium: Alert, High: Alert, Critical: Alert
 - c. Low: Ignore, Medium: Ignore, High: Alert, Critical: Block
 - d. Low: Ignore, Medium: Ignore, High: Alert, Critical: Alert

Understand container models

71. An application has five hosts that run 30 Docker containers based on 10 images. What is the total number of container models in the application?
- a. 5
 - b. 10
 - c. 20
 - d. 30
72. Which is not a tab in the container model?
- a. Process
 - b. Networking
 - c. File System
 - d. Memory

Configure container-runtime policies

73. Which tab does not have a Prevent effect in a container runtime rule?
- a. Processes
 - b. Networking
 - c. File system
 - d. Operations

Understand container-runtime audits

74. Which container-runtime effect applies to a single action rather than to an entire container?
- a. Alert
 - b. Prevent
 - c. Block
 - d. Delete
75. Which Docker storage driver, does not support Prevent effects?
- a. devicemapper
 - b. overlay2
 - c. aufs
 - d. virtualmapper

Investigate container-runtime audits

76. When does Prisma Cloud Compute gather forensic information about containers?
- a. all the time
 - b. at the time of a breach
 - c. at the time of a breach and for a short time afterward
 - d. at the time of the breach and for 10 minutes
77. Which time period is covered by the forensic information sent to the console?
- a. all the time
 - b. the time of a breach and a short period before it
 - c. the time of a breach and a short period afterward
 - d. a short period before the time of a breach and a short period afterward

Understand how to investigate serverless vulnerabilities

78. In Prisma Cloud Compute, which three languages can have their packages scanned for vulnerabilities in serverless? (Choose three.)
- a. JavaScript (Node.js)
 - b. Go
 - c. C#
 - d. Rust
 - e. Python
 - f. Java

79. Which component of Prisma Cloud Compute scans serverless functions for vulnerabilities?
- a. Container Defenders
 - b. the Console
 - c. Serverless Defenders
 - d. Network Defenders
80. Which permission does Prisma Cloud Compute need to have to scan AWS Lambda functions?
- a. AWSLambdaShortAccess
 - b. AWSLambdaRole
 - c. AWSLambdaReadOnlyAccess
 - d. AWSLambdaFullAccess

Configure Serverless Vulnerability policy

81. What two scope restrictions can a serverless vulnerability policy have? (Choose two.)
- a. Runtimes
 - b. Functions
 - c. Cloud Platforms
 - d. Account IDs
 - e. Trigger Types
82. Which two effects can an exception to a Vulnerability policy rule have? (Choose two.)
- a. Disable
 - b. Ignore
 - c. Alert
 - d. Prevent
 - e. Block

Configure serverless auto-protect functionality

83. In Prisma Cloud Compute, which two languages are not supported for the serverless Defender? (Choose two.)
- a. JavaScript (Node.js)
 - b. Go
 - c. C#
 - d. Rust
 - e. Python

84. How do you add a serverless Defender to a GCP cloud function?
- a. Use serverless Defender on AWS Lambda.
 - b. Add code to the serverless function.
 - c. Add a layer to the serverless configuration.
 - d. Add a layer to the serverless function.

Configure CloudTrail and SNS

85. What type of event do you need to log for DLP to work?
- a. Read
 - b. Write
 - c. Upload
 - d. Download
86. Which cloud service can use DLP?
- a. AWS S3
 - b. Azure Blob
 - c. Google Cloud
 - d. Google Cloud Messaging
87. How does Prisma Cloud get information about new files that need to be checked for DLP?
- a. AWS SNS
 - b. Azure Event Grid
 - c. Google Messaging
 - d. HTTP to a Prisma Cloud web hook

Configure scan options

88. What does Forward-only scanning mean?
- a. scan only files going in the forward direction from the organization being protected to the rest of the world
 - b. scan only files going in the forward direction from the rest of the world to the organization being protected
 - c. scan only files forward in time, new files being uploaded to the storage service
 - d. scan only files forward in time, previous seen files being uploaded to the storage service

89. Which extensions is supported for malware scanning?

- a. .exe
- b. .jar
- c. .tar
- d. Msi

Use Data Dashboard features

90. What is not an exposure level that would apply to a storage bucket?

- a. Public
- b. Partial
- c. Conditional
- d. Private

Assess data policies and alerts

91. Which option is a PII data pattern?

- a. Bank – Bankruptcy Filings
- b. Driver License – Estonia
- c. Credit card number
- d. Health – DEA

92. What is the recommended bucket time-to-live (TTL) in the CloudTrail bucket?

- a. one day
- b. five days
- c. one month
- d. five months

Configure Cloud Native Application Firewall policies

93. Which protocol or protocols does the Cloud Native Application Firewall (CNAF) process?

- a. LDAP
- b. SSL
- c. SSH
- d. HTTP

94. Which is not a valid action in a CNAF rule?

- a. Disable
- b. Log
- c. Alert
- d. Prevent

Differentiate between Terraform and CloudFormation scanning configurations

95. Which cloud service can consume CloudFormation configuration files?

- a. AWS
- b. Azure
- c. Google Storage
- d. GCP

96. In which type of template does `.prismaCloud/config.yml` have a `variable_files` setting?

- a. Terraform
- b. CloudFormation
- c. CloudField
- d. Kubernetes

List out-of-the-box (OOTB) infrastructure as code scanning integrations

97. Which two integrations integrate with an IDE? (Choose two.)

- a. Jenkins
- b. AWS DevOps
- c. Visual Studio Code
- d. Azure DevOps
- e. IntelliJ IDEA

98. Which two integrations integrate with source code management software? (Choose two.)

- a. GitHub
- b. GitLab
- c. CircleCI
- d. IntelliJ IDEA
- e. Jenkins

99. Which type of software does not have integrations with Prism Cloud to manage IaC?
- a. CI/CD
 - b. SCM
 - c. Compiler
 - d. IDE

Configure API scanning for IaC templates

100. Which HTTP method is used to request the scan results for a Terraform template?
- a. GET
 - b. POST
 - c. PUT
 - d. DELETE
101. What is the content-type value use to scan a single YAML CloudFormation template file?
- a. text/plain
 - b. text/x-yaml
 - c. application/yaml
 - d. application/plain

Review OOTB policies for IaC scanning

102. The OOTB policy to verify that versioning is turned on in AWS S3 buckets is applied to which two code options? (Choose two.)
- a. CloudFormation
 - b. Terraform
 - c. CloudField
 - d. Kubernetes
103. The OOTB policy to verify that versioning is turned on in GCP Storage log buckets is applied to which code option?
- a. CloudFormation
 - b. Terraform
 - c. CloudField
 - d. Kubernetes

Configure custom-build policies for IaC scanning

104. Which type of query do you use in an IaC build policy?
- a. JSON
 - b. YAML
 - c. RQL
 - d. SQL
105. What does the expression **\$.resource[*]** mean?
- a. the value of the resource field of the root object
 - b. the number of items inside the resource field of the root object
 - c. all the keys inside the resource field of the root object
 - d. all the values inside the resource field of the root object

Integrate container scans into CI/CD pipeline

106. Which CI/CD software communicates with Prisma Cloud Compute to request scans of new container images?
- a. Jenkins
 - b. Maven
 - c. Freestyle
 - d. Malware
107. Which kind of relationship is allowed between the Console release and the Jenkins plugin release?
- a. The Jenkins plugin can be the same release as the Console or newer.
 - b. The Jenkins plugin and the Console must be the same release.
 - c. The Console can be the same release as the Jenkins release or newer.
 - d. Any version of the Jenkins plugin works with any version of the Console.
108. How do you configure communications between Jenkins (with the plugin) and the Prisma Console?
- a. The plugin you install has the Console identity and the account to use on it.
 - b. You configure the console identity and authentication on Jenkins.
 - c. You configure the Jenkins identity and authentication on the Console.
 - d. On each side (Jenkins and Prism Console) you need to configure the identity and authentication for the other side.

Identify different options for scanning: twistcli and plugins

109. What is the return code of twistcli if the image passes the test?

- a. -1
- b. 0
- c. 1
- d. 2

110. At what point does a twistcli scan check the image?

- a. before the image is created
- b. after the image is created
- c. after the image is deployed
- d. before the image is created

Review default CI policies for Compute scanning

111. Which two policy types are valid for CI, before the image is deployed? (Choose two.)

- a. Compliance
- b. Network Event
- c. Vulnerability
- d. Audit
- e. Access

112. What is the earliest stage of the toolchain where Prisma Cloud Compute can protect you?

- a. Coding
- b. Building
- c. Testing
- d. Deploying

Onboarding cloud accounts

113. Which option shows the types of cloud accounts supported by Prisma Cloud?

- a. AWS and Azure
- b. AWS, Azure, and GCP
- c. AWS, Azure, GCP, and Alibaba
- d. AWS, Azure, GCP, Alibaba, and IBM Cloud

114. Which two modes are supported to secure cloud accounts? (Choose two.)

- a. Read only
- b. Observe
- c. Monitor
- d. Observe & Prevent
- e. Monitor & Protect

Configure account groups

115. What is the relationship between cloud accounts and account groups?

- a. One to one. Each account group has exactly one cloud account.
- b. One to many. Each account group has multiple cloud accounts, but a cloud account can be in only one group.
- c. One to many. Each account has multiple accounts groups, but a group can include at most one account.
- d. Many to many. Each account can be a member of multiple account groups, and each group can contain multiple accounts.

116. What are the two ways in which account groups are used? (Choose two.)

- a. Prisma Cloud > Compliance, to see the compliance status of a specific group (for example, apps that process credit cards)
- b. Prisma Cloud > Policies, to specify on which accounts groups Prisma Cloud can use auto remediation for each policy
- c. Prisma Cloud Compute > Radar (one of the options to color different containers and serverless functions is by account group)
- d. Prisma Cloud Compute > Defend > Vulnerabilities; you can ask to get a report of all the vulnerabilities of a specific account group
- e. in the security roles, to permit users to access only specific account groups

Differentiate between Prisma Cloud and Compute roles

117. An administrator has a Prisma Cloud role of Account Group Admin. What is the administrator's role in Prisma Cloud Compute?

- a. also Account Group Admin because they use the same roles
- b. Auditor
- c. DevSecOps User
- d. Defender Manager

118. Which two actions are permitted for Cloud Provisioning Admins? (Choose two.)
- a. View SSO Settings
 - b. Deploy new Prisma Cloud Compute Defenders
 - c. View Alerts
 - d. View Policy
 - e. View Prisma Cloud account details (for an account administered by them)

Configure Prisma Cloud and Compute roles

119. Which role in Prisma Cloud Compute do you give a team lead from development permission to see only continuous integration reports?
- a. CI User
 - b. DevOps User
 - c. DevSecOps User
 - d. Auditor
120. An employee from Operations who works the night shift needs to be able to see everything in case of problems but should not be able to change anything. Which role do you assign in Prisma Cloud Compute?
- a. CI User
 - b. DevOps User
 - c. DevSecOps User
 - d. Auditor

Configure Defender as an admission controller

121. Which type of Defender installation do you need for an admission controller?
- a. Single Defender
 - b. DaemonSet
 - c. Swarm
 - d. Multiple Defender DaemonSet
122. Which is the name of the file you apply to Kubernetes to install OPA?
- a. admin_ctrl.yaml
 - b. opa.yaml
 - c. webhook.yaml
 - d. opa.json

Create OPA policies

123. What is the Rego expression to select only nginx images?
- a. `input.request.object.spec.containers[].image`
 - b. `input.request.object.spec.containers[*].image`
 - c. `input.request.object.containers[].image`
 - d. `input.request.object.containers[*].image`
124. Which three operations are supported in OPA policies? (Choose three.)
- a. CREATE
 - b. READ
 - c. MODIFY
 - d. UPDATE
 - e. CONNECT

Understand audit logging

125. Users connect to the Console through `app.prismacloud.io`. Which Audit log has the IP of the user that connected to it?
- a. Prisma Cloud
 - b. Prisma Cloud Compute
 - c. Prisma Cloud Log
 - d. Prisma Cloud Compute Log

Enable Defender logging

126. Where is the Defender log file located?
- a. on the Console
 - b. `/var/lib/twistlock/log/defender.log`
 - c. `/usr/lib/twistlock/log/defender.log`
 - d. `/etc/lib/twistlock/log/defender.log`

Differentiate UEBA settings

127. Which two values are legitimate entries in an anomaly trusted list? (Choose two.)
- a. 10.0.0.0/8
 - b. 2.2.2.2/16
 - c. 8.8.8.8
 - d. joe@prismacloud.io
 - e. 172.16.1.1/32
128. Which three criteria can be used to limit the applicability of an anomaly trusted list? (Choose three.)
- a. Anomaly policy type(s)
 - b. Account ID
 - c. VPC
 - d. Subnet
 - e. DNS Domain

Configure idle timeout

129. What is the maximum idle timeout without using a custom value?
- a. 30 minutes
 - b. 45 minutes
 - c. 60 minutes
 - d. 120 minutes
130. When you set a custom idle timeout, which units can you use?
- a. minutes
 - b. hours
 - c. days
 - d. months

Set mandatory dismissal reason(s)

131. What can an administrator require when somebody dismisses an alert?
- a. Administrators are authorized to dismiss alerts.
 - b. An administrator can configure the system so administrators must type a reason, but what they type can't be controlled.
 - c. Administrators are required to type a reason and require it to be of a certain length.
 - d. Administrators are always required to type a reason.

132. Understand inbound and outbound notifications

- a. Which system can serve as a source of information for Prisma Cloud?
- b. Slack
- c. Amazon GuardDuty
- d. Amazon SQS
- e. Jira

133. Which system can be used to display Prisma Cloud alerts, but not to feed it information?

- a. AWS Inspector
- b. Tenable
- c. Qualys
- d. ServiceNow

Configure third-party integration for alerts

134. Where in the user interface do you specify integrations for Prisma Cloud to alert other products?

- a. Settings > Integrations
- b. Manage > Alerts
- c. Prisma Cloud Settings > Integrations
- d. Prisma Cloud Manage > Alerts

135. Where do you configure outbound notifications for CNAF?

- a. Settings > Integrations
- b. Manage > Alerts
- c. Prisma Cloud Settings > Integrations
- d. Manage > CNAF > Alerts

Manage alerts using APIs

136. You want to test an alert channel using `/api/v1/alert-profiles/test`. Which format should you use?

- a. GET
- b. JSON
- c. YAML
- d. Python

Create reports using APIs

137. Which command will start an images scan?
- a. GET /images/scan
 - b. POST /images/scan
 - c. GET /results/images/download
 - d. POST /results/images/download

Download vulnerability results via API

138. Which command will get the results of a container scan?
- a. GET /results/containers/download
 - b. POST /results/containers/download
 - c. GET /containers/download
 - d. POST /containers/download

Answers to Sample Questions

1. b
2. c
3. c
4. b
5. a
6. b
7. b, e
8. c
9. a
10. d
11. a
12. b
13. a
14. c
15. b, d
16. d
17. a
18. c, e
19. a, b, d
20. b
21. c
22. d
23. c
24. c
25. b
26. a, b, e
27. c
28. c
29. b, d
30. b
31. b, c
32. d
33. b
34. a, d
35. b
36. a
37. a
38. c
39. c
40. a
41. b
42. a
43. a, c
44. d
45. b
46. a

- 47. b
- 48. a, d
- 49. a, d
- 50. d
- 51. c
- 52. a
- 53. a
- 54. a
- 55. c
- 56. c
- 57. a, d, e
- 58. a
- 59. c
- 60. b
- 61. a, e
- 62. c
- 63. d
- 64. c
- 65. a, b, e
- 66. b
- 67. b
- 68. b
- 69. c, d
- 70. d
- 71. b
- 72. d
- 73. b
- 74. b
- 75. c
- 76. a
- 77. d
- 78. a, e, f
- 79. b
- 80. c
- 81. b, d
- 82. b, c
- 83. b, d
- 84. c
- 85. b
- 86. a
- 87. a
- 88. c
- 89. a
- 90. b
- 91. b
- 92. c
- 93. d
- 94. b

- 95. a
- 96. a
- 97. c, e
- 98. a, b
- 99. c
- 100. b
- 101. a
- 102. a, b
- 103. b
- 104. a
- 105. d
- 106. a
- 107. b
- 108. b
- 109. b
- 110. b
- 111. a, c
- 112. b
- 113. c
- 114. c, e
- 115. d
- 116. a, e
- 117. b
- 118. b, e
- 119. b
- 120. d
- 121. b
- 122. c
- 123. a
- 124. a, d, e
- 125. a
- 126. b
- 127. a, e
- 128. a, b, c
- 129. c
- 130. a
- 131. b
- 132. b
- 133. d
- 134. c
- 135. b
- 136. b
- 137. b
- 138. c

Glossary

Admission Controller: The admission controller is a component in a Kubernetes setup that can approve, modify, or reject administrative requests. It is a specific version of an application firewall.

API: The application program interface (API) is the interface that a program exposes to other programs.

App Embedded: App embedded is a way to install (embed) Prisma Cloud Defenders inside an application's Docker containers.

Application Firewall: An application firewall is a firewall built to understand and protect a specific application protocol, for example, HTTP.

Asset: An asset is any system that is used as part of a business application. In the cloud it can be a virtual machine, a Docker container, a serverless function, a database hosted by the provider, etc.

AWS: Amazon Web Services (AWS) is Amazon's cloud product.

AWS Lambda: AWS Lambda is Amazon's serverless product. It is distinguished from the competition by the availability of a layer feature that lets you wrap the serverless functions with other functions, such as a Prisma Cloud Defender.

Azure: Azure is Microsoft's cloud product. For more information, visit:

<https://azure.microsoft.com/en-us/>

Build Time: Build time is the integration process that takes written code and turns it into a running application.

CI/CD: Continuous integration/continuous delivery is an automated process for building, running, and monitoring applications.

CloudBees: CloudBees is the version of Jenkins used for Kubernetes.

CloudFormation: CloudFormation is an Amazon program that takes configuration files and connects them to an AWS account to provision the infrastructure in the way specified by those files.

Compliance: Compliance relates to a set of rules (or standards) defined by an industry, government, or regulatory body that must be followed to ensure that a certain level of security is being established and maintained.

Console: A console is the user interface that allows an administrator to interact with a product. For Prisma Cloud Compute the user interface can be a SaaS offering or hosted by the organization that bought Prisma Cloud Compute. In Prisma Cloud the user interface is always a SaaS solution.

Defenders: Defenders are software entities that Prisma Cloud Compute uses to secure hosts, containers, and serverless functions.

Docker Container: A Docker container is a piece of software running on Docker. Docker containers use their own libraries and file system, but rely on the kernel of the operating system on which they run. For more information, visit:

<https://www.docker.com/resources/what-container>

Docker Image: A Docker image is software packaged for deployment in the form of a Docker container. For more information, visit <https://docs.docker.com/engine/reference/commandline/image/>.

Firewall: A firewall is a system that monitors the communications (ingress and egress) between components and approves, rejects, or modifies the information being communicated in accordance with predefined policies.

GCP: Google Cloud Platform (GCP) is Google's cloud product. For more information, visit:

<https://cloud.google.com/>

Google Cloud Functions: Google Cloud Functions is Google's serverless product. For more information, visit:

<https://cloud.google.com/functions>

Host: A host is the compute platform being used to run software. In relation to Prisma Cloud, the host runs either Docker or a virtual machine.

Infrastructure as Code (IaC): Infrastructure as code (IaC) specifies the configuration of the infrastructure, such as its network topology and server configurations, as a text file. For more information, visit:

https://en.wikipedia.org/wiki/Infrastructure_as_code

Integration: Integration is the process of setting two or more systems up to communicate with one another for some purpose. For example, Prisma Cloud can be integrated with Slack to propagate alerts to a Slack channel.

Jenkins: Jenkins is open source software for CI/CD. For more information, visit <https://www.jenkins.io/>.

JSON: JSON is a textual format used for computer information. For more information, visit:

<https://en.wikipedia.org/wiki/JSON>

Kubernetes: Kubernetes is an open source system that allows the management of multiple Docker installations running on separate computers (or virtual machines). For more information, visit:

<https://kubernetes.io/>

Microsoft Azure Functions: Microsoft Azure Functions is Microsoft's serverless product. For more information, visit:

<https://azure.microsoft.com/en-us/services/functions/>

Out-of-the-box (OOTB): Out-of-the-box (OOTB) is software, policies, or configurations that are provided with a product, for example, the security policies that come with Prisma Cloud.

Open Policy Agent (OPA): An open policy agent (OPA) is the admission controller used with Prisma Cloud Compute to restrict access to Kubernetes.

Role-Based Access Control (RBAC): Role-based access control (RBAC) is offered by a system that can map users to roles and then apply policies that enforce a set of permissions for each role.

Rego: Rego is a language used to query JSON data structures in the Prisma Cloud Computes OPA, which acts as the admission controller for Kubernetes.

Role: A role is the job function that a user fulfills. It often is tied to the permissions that the user is granted so that they can fulfill their function.

Resource Query Language (RQL): The Resource Query Language (RQL) is language used by Prisma Cloud to query different resources.

Runtime: Runtime can refer to an application that is running (functioning or working).

Runtime Environment: The runtime environment is the software and libraries that form the environment for an application.

Software as a Service (SaaS): Software as a service (SaaS) is software that runs on infrastructure managed by a provider and used by another organization through the internet. For more information, visit:

https://en.wikipedia.org/wiki/Software_as_a_service

Serverless: Serverless is a method of running software in which the cloud provider is responsible for the hardware, virtual machine, container, and runtime. The consuming organization is responsible only for the functions that are called to implement the application's functionality.

Terraform: Terraform is an open source program that takes configuration files and connects them to a cloud account to provision the infrastructure in the way specified by those files. For more information, visit:

<https://www.terraform.io/>

User and entity behavior analytics (UEBA): User and entity behavior analytics (UEBA) is technology that identifies and alerts on user behavior that deviates (is anomalous) from what is normal or expected.

Vulnerability: A vulnerability is a software bug that allows users to abuse the system in some way. Those vulnerabilities often exist not directly in the application software but in the libraries that the software uses.

Workload: A workload is software running on an asset that implements part of a business application.

YAML: YAML is a text format used for computer information. For more details, visit:

<https://yaml.org/>