

## Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

<https://www.2passeasy.com/dumps/PCCSE/>



#### NEW QUESTION 1

Which option shows the steps to install the Console in a Kubernetes Cluster?

- A. Download the Console and Defender image Generate YAML for Defender Deploy Defender YAML using kubectl
- B. Download and extract release tarball Generate YAML for Console Deploy Console YAML using kubectl
- C. Download the Console and Defender image Download YAML for Defender from the document site Deploy Defender YAML using kubectl
- D. Download and extract release tarball Download the YAML for Console Deploy Console YAML using kubectl

**Answer:** B

#### NEW QUESTION 2

Which step is included when configuring Kubernetes to use Prisma Cloud Compute as an admission controller?

- A. copy the Console address and set the config map for the default namespace.
- B. create a new namespace in Kubernetes called admission-controller.
- C. enable Kubernetes auditing from the Defend > Access > Kubernetes page in the Console.
- D. copy the admission controller configuration from the Console and apply it to Kubernetes.

**Answer:** B

#### NEW QUESTION 3

A customer has a requirement to scan serverless functions for vulnerabilities. Which three settings are required to configure serverless scanning? (Choose three.)

- A. Defender Name
- B. Region
- C. Credential
- D. Console Address
- E. Provider

**Answer:** BCE

#### NEW QUESTION 4

A customer finds that an open alert from the previous day has been resolved. No auto-remediation was configured. Which two reasons explain this change in alert status? (Choose two.)

- A. user manually changed the alert status.
- B. policy was changed.
- C. resource was deleted.
- D. alert was sent to an external integration.

**Answer:** CD

#### NEW QUESTION 5

Which port should a security team use to pull data from Console's API?

- A. 53
- B. 25
- C. 8084
- D. 8083

**Answer:** D

#### NEW QUESTION 6

Which statement is true about obtaining Console images for Prisma Cloud Compute Edition?

- A. To retrieve Prisma Cloud Console images using basic auth:\* 1. Access registry.paloaltonetworks.com, and authenticate using 'docker login'. 2.Retrieve the Prisma Cloud Console images using 'docker pull'.
- B. To retrieve Prisma Cloud Console images using basic auth:\* 1. Access registry.twistlock.com, and authenticate using 'docker login'. 2.Retrieve the Prisma Cloud Console images using 'docker pull'.
- C. To retrieve Prisma Cloud Console images using URL auth:\* 1. Access registry-url-auth.twistlock.com, and authenticate using the user certificat
- D. 2.Retrieve the Prisma Cloud Console images using 'docker pull'.
- E. To retrieve Prisma Cloud Console images using URL auth:\* 1. Access registry-auth.twistlock.com, and authenticate using the user certificat
- F. 2.Retrieve the Prisma Cloud Console images using 'docker pull'.

**Answer:** B

#### NEW QUESTION 7

An administrator has deployed Console into a Kubernetes cluster running in AWS. The administrator also has configured a load balancer in TCP passthrough mode to listen on the same ports as the default Prisma Compute Console configuration.

In the build pipeline, the administrator wants twistcli to talk to Console over HTTPS. Which port will twistcli need to use to access the Prisma Compute APIs?

- A. 8084
- B. 443
- C. 8083
- D. 8081

Answer: A

#### NEW QUESTION 8

Which order of steps map a policy to a custom compliance standard?

(Drag the steps into the correct order of occurrence, from the first step to the last.)

#### Answer Area

Unordered Options	Ordered Options
Add the custom compliance standard from the drop-down menu	
Create the custom compliance standard	
Edit the Policy	
Click on Compliance Standards	

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Diagram Description automatically generated

#### NEW QUESTION 9

Which three types of classifications are available in the Data Security module? (Choose three.)

- A. Personally identifiable information
- B. Malicious IP
- C. Compliance standard
- D. Financial information
- E. Malware

Answer: CDE

#### NEW QUESTION 10

A customer wants to harden its environment from misconfiguration.

Prisma Cloud Compute Compliance enforcement for hosts covers which three options? (Choose three.)

- A. Docker daemon configuration files
- B. Docker daemon configuration
- C. Host cloud provider tags
- D. Host configuration
- E. Hosts without Defender agents

Answer: BCD

#### NEW QUESTION 10

A security team has a requirement to ensure the environment is scanned for vulnerabilities. What are three options for configuring vulnerability policies? (Choose three.)

- A. individual actions based on package type
- B. output verbosity for blocked requests
- C. apply policy only when vendor fix is available
- D. individual grace periods for each severity level
- E. customize message on blocked requests

Answer: BCD

#### NEW QUESTION 11

The security team wants to protect a web application container from an SQLi attack. Which type of policy should the administrator create to protect the container?

- A. CNAF
- B. Runtime
- C. Compliance
- D. CNNF

Answer: A

#### NEW QUESTION 12

Which type of compliance check is available for rules under Defend > Compliance > Containers and Images > CI?

- A. Host
- B. Container
- C. Functions
- D. Image

**Answer:** B

#### NEW QUESTION 14

What is the order of steps to create a custom network policy?

(Drag the steps into the correct order of occurrence, from the first step to the last.)

**Answer Area**

Unordered Options	Ordered Options
Build your Query → New Search or Saved Search	
Select Compliance Standards	
From Policies tab → Add Policy → Network	
Click Confirm	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

A picture containing table Description automatically generated

#### NEW QUESTION 18

Which statement accurately characterizes SSO Integration on Prisma Cloud?

- A. Prisma Cloud supports IdP initiated SSO, and its SAML endpoint supports the POST and GET methods.
- B. Okta, Azure Active Directory, PingID, and others are supported via SAML.
- C. An administrator can configure different Identity Providers (IdP) for all the cloud accounts that Prisma Cloud monitors.
- D. An administrator who needs to access the Prisma Cloud API can use SSO after configuration.

**Answer:** A

#### NEW QUESTION 23

A customer wants to be notified about port scanning network activities in their environment. Which policy type detects this behavior?

- A. Network
- B. Port Scan
- C. Anomaly
- D. Config

**Answer:** A

#### NEW QUESTION 24

The development team wants to fail CI jobs where a specific CVE is contained within the image. How should the development team configure the pipeline or policy to produce this outcome?

- A. Set the specific CVE exception as an option in Jenkins or twistcli.
- B. Set the specific CVE exception as an option in Defender running the scan.
- C. Set the specific CVE exception as an option using the magic string in the Console.
- D. Set the specific CVE exception in Console's CI policy.

**Answer:** C

#### NEW QUESTION 25

Which option identifies the Prisma Cloud Compute Edition?

- A. Package installed with APT
- B. Downloadable, self-hosted software
- C. Software-as-a-Service (SaaS)
- D. Plugin to Prisma Cloud

**Answer:** B

#### NEW QUESTION 26

You are tasked with configuring a Prisma Cloud build policy for Terraform. What type of query is necessary to complete this policy?

- A. YAML
- B. JSON
- C. CloudFormation
- D. Terraform

**Answer:** B

#### NEW QUESTION 28

Which options show the steps required to upgrade Console when using projects?

- A. Upgrade all Supervisor Consoles Upgrade Central Console
- B. Upgrade Central Console Upgrade Central Console Defenders
- C. Upgrade Defender Upgrade Central Console Upgrade Supervisor Consoles
- D. Upgrade Central Console Upgrade all Supervisor Consoles

**Answer:** A

#### NEW QUESTION 33

Which statement about build and run policies is true?

- A. Build policies enable you to check for security misconfigurations in the IaC templates.
- B. Every type of policy has auto-remediation enabled by default.
- C. The four main types of policies are: Audit Events, Build, Network, and Run.
- D. Run policies monitor network activities in the environment and check for potential issues during runtime.

**Answer:** A

#### NEW QUESTION 36

A customer is reviewing Container audits, and an audit has identified a cryptominer attack. Which three options could have generated this audit? (Choose three.)

- A. The value of the mined currency exceeds \$100.
- B. High CPU usage over time for the container is detected.
- C. Common cryptominer process name was found.
- D. The mined currency is associated with a user token.
- E. Common cryptominer port usage was found.

**Answer:** BCD

#### NEW QUESTION 38

An administrator sees that a runtime audit has been generated for a Container. The audit message is “DNS resolution of suspicious name wikipedia.com. type A”. Why would this message appear as an audit?

- A. The DNS was not learned as part of the Container model or added to the DNS allow list.
- B. This is a DNS known to be a source of malware.
- C. The process calling out to this domain was not part of the Container model.
- D. The Layer7 firewall detected this as anomalous behavior.

**Answer:** A

#### NEW QUESTION 41

What is an example of an outbound notification within Prisma Cloud?

- A. AWS Inspector
- B. Qualys
- C. Tenable
- D. PagerDuty

**Answer:** D

#### NEW QUESTION 44

An S3 bucket within AWS has generated an alert by violating the Prisma Cloud Default policy “AWS S3 buckets are accessible to public”. The policy definition follows:

config where cloud.type = 'aws' AND api.name='aws-s3api-get-bucket-acl' AND json.rule="((((acl.grants[? (@.grantee=='AllUsers')] size > 0) or policyStatus.isPublic is true) and publicAccessBlockConfiguration does not exist) or ((acl.grants[?(@.grantee=='AllUsers')] size > 0) and publicAccessBlockConfiguration.ignorePublicAcis is false) or (policyStatus.isPublic is true and publicAccessBlockConfiguration.restrictPublicBuckets is false)) and

websiteConfiguration does not exist"  
Why did this alert get generated?

- A. an event within the cloud account
- B. network traffic to the S3 bucket
- C. configuration of the S3 bucket
- D. anomalous behaviors

**Answer:** B

#### NEW QUESTION 46

A security team has been asked to create a custom policy.  
Which two methods can the team use to accomplish this goal? (Choose two.)

- A. add a new policy
- B. clone an existing policy
- C. disable an out-of-the-box policy
- D. edit the query in the out-of-the-box policy

**Answer:** AB

#### NEW QUESTION 50

A security team notices a number of anomalies under Monitor > Events. The incident response team works with the developers to determine that these anomalies are false positives.  
What will be the effect if the security team chooses to Relearn on this image?

- A. The model is deleted, and Defender will relearn for 24 hours.
- B. The anomalies detected will automatically be added to the model.
- C. The model is deleted and returns to the initial learning state.
- D. The model is retained, and any new behavior observed during the new learning period will be added to the existing model.

**Answer:** B

#### NEW QUESTION 51

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCCSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCCSE Product From:

<https://www.2passeasy.com/dumps/PCCSE/>

## Money Back Guarantee

### PCCSE Practice Exam Features:

- \* PCCSE Questions and Answers Updated Frequently
- \* PCCSE Practice Questions Verified by Expert Senior Certified Staff
- \* PCCSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PCCSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year