

PaloAltoNetworks.PCCSE.v2023-01-12.q77

Exam Code:	PCCSE
Exam Name:	Prisma Certified Cloud Security Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	77
Version:	v2023-01-12
# of views:	1999
# of Questions views:	770
https://www.freeqas.com/qa/Palo-Alto-Networks/PCCSE/PaloAltoNetworks.PCCSE.v2023-01-12.q77.html	

NEW QUESTION: 1

When would a policy apply if the policy is set under Defend > Vulnerability > Images > Deployed?

- A. when a serverless repository is scanned
- B. when a Container is started form an Image
- C. when the Image is built
- D. when the Image is built and when a Container is started form an Image

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 2

You are an existing customer of Prisma Cloud Enterprise. You want to onboard a public cloud account and immediately see all of the alerts associated with this account based off ALL of your tenant's existing enabled policies. There is no requirement to send alerts from this account to a downstream application at this time. Which option shows the steps required during the alert rule creation process to achieve this objective?

- A. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select "select all policies" checkbox as part of the alert rule Add alert notifications Confirm the alert rule
- B. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select one or more policies as part of the alert rule Add alert notifications Confirm the alert rule
- C. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select "select all policies" checkbox as part of the alert rule Confirm the alert rule
- D. Ensure the public cloud account is assigned to an account group Assign the confirmed account group to alert rule Select one or more policies checkbox as part of the alert rule Confirm the alert rule

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 3

The security team wants to target a CNAF policy for specific running Containers. How should the administrator scope the policy to target the Containers?

- A. scope the policy to Image names.
- B. scope the policy to namespaces.
- C. scope the policy to Host names.
- D. scope the policy to Defender names.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4


Which intensity setting for anomaly alerts is used for the measurement of 100 events over 30 days?

- A. Medium
- B. High
- C. Very High
- D. Low

Answer: A (LEAVE A REPLY)

NEW QUESTION: 5

You wish to create a custom policy with build and run subtypes. Match the query types for each example. (Select your answer from the pull-down list. Answers may be used more than once or not at all.)

config where cloud.type = 'aws'		Run
\$.resource[*].aws_s3_bucket exists	Drag answer here	Build
RQL type	Drag answer here	
JSON query type	Drag answer here	

Answer:

Answer Area

config where cloud.type = 'aws'	Run	Run
\$.resource[*].aws_s3_bucket exists	Run	Build
RQL type	Build	
JSON query type	Build	

Answer Area

config where cloud.type = 'aws'	Run	Run
\$.resource[*].aws_s3_bucket exists	Run	Build
RQL type	Build	
JSON query type	Build	

NEW QUESTION: 6

Which two of the following are required to be entered on the IdP side when setting up SSO in Prisma Cloud?
(Choose two.)

- A. Assertion Consumer Service (ACS) URL
- B. Username
- C. SSO Certificate
- D. SP (Service Provider) Entity ID

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 7

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

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 8

A customer has Defenders connected to Prisma Cloud Enterprise. The Defenders are deployed as a DaemonSet in OpenShift.

How should the administrator get a report of vulnerabilities on hosts?

- A. Navigate to Defend > Vulnerabilities > VM Images
- B. Navigate to Defend > Vulnerabilities > Hosts
- C. Navigate to Monitor > Vulnerabilities > Hosts
- D. Navigate to Monitor > Vulnerabilities > CVE Viewer

Answer: C (LEAVE A REPLY)

NEW QUESTION: 9

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 10

What is the maximum number of access keys a user can generate in Prisma Cloud with a System Admin role?

- A. 2
- B. 3
- C. 1
- D. 4

Answer: A (LEAVE A REPLY)

NEW QUESTION: 11

An administrator needs to detect and alert on any activities performed by a root account.

Which policy type should be used?

- A. config-build
- B. config-run
- C. audit event
- D. network

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 12

A customer has a requirement to scan serverless functions for vulnerabilities.

Which three settings are required to configure serverless scanning? (Choose three.)

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

Answer: A,B,D ([LEAVE A REPLY](#))

NEW QUESTION: 13

Per security requirements, an administrator needs to provide a list of people who are receiving e-mails for Prisma Cloud alerts.

Where can the administrator locate this list of e-mail recipients?

- A. Set Alert Notification section within an Alert Rule.
- B. Target section within an Alert Rule.
- C. Notification Template section within Alerts.
- D. Users section within Settings.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

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

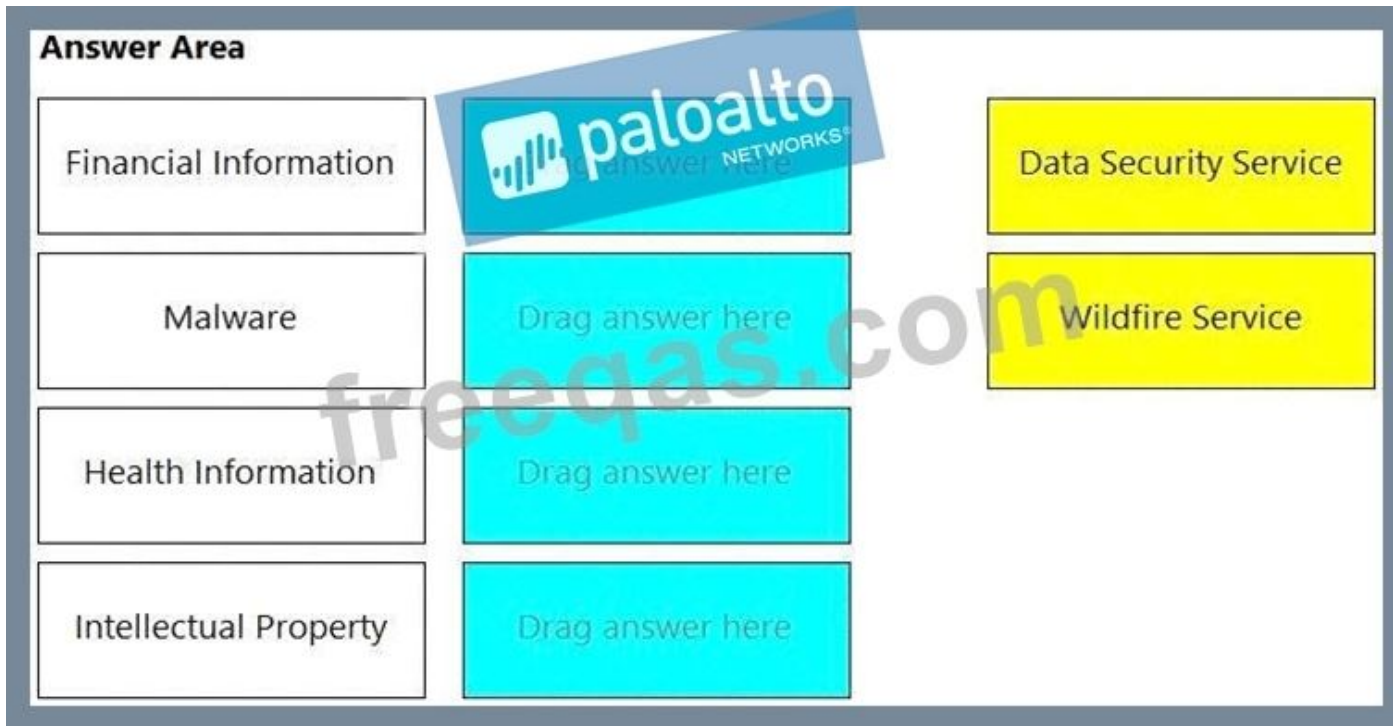
- A. Config
- B. Port Scan
- C. Network
- D. Anomaly

Answer: C ([LEAVE A REPLY](#))

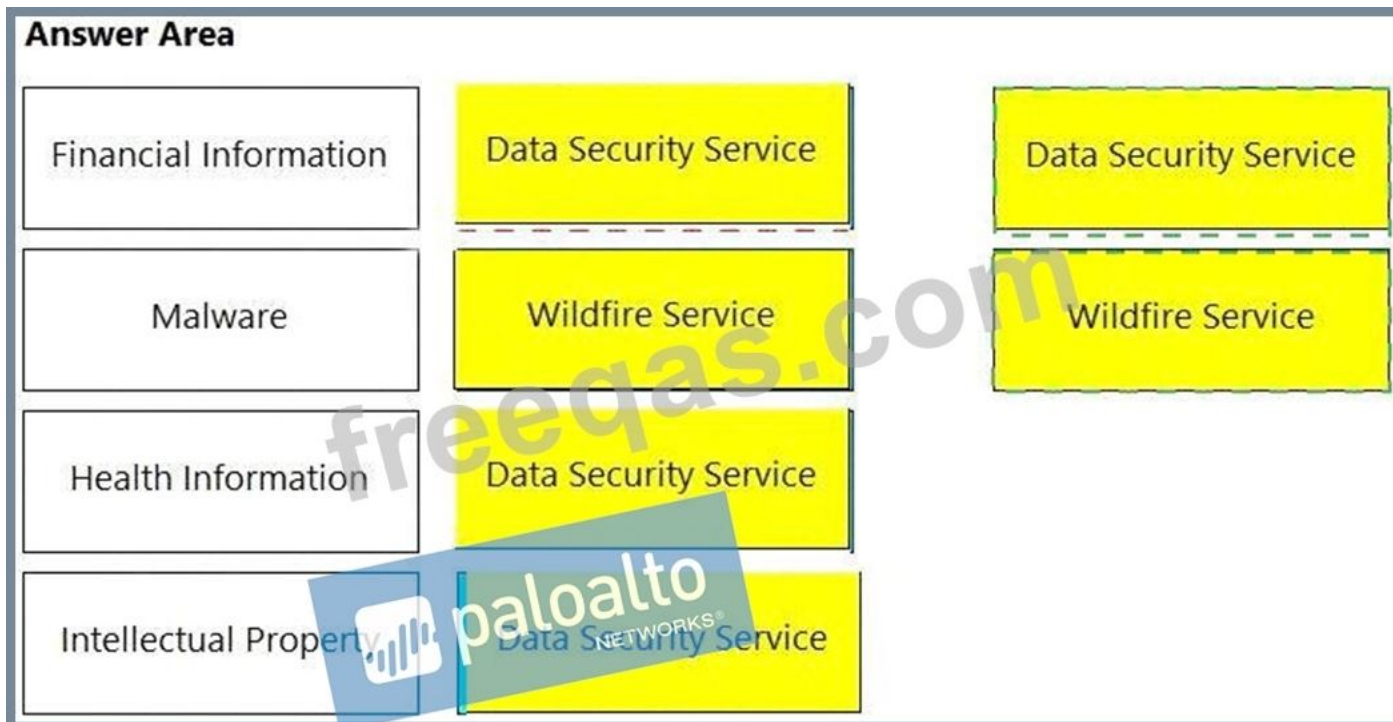
NEW QUESTION: 15

Match the service on the right that evaluates each exposure type on the left.

(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

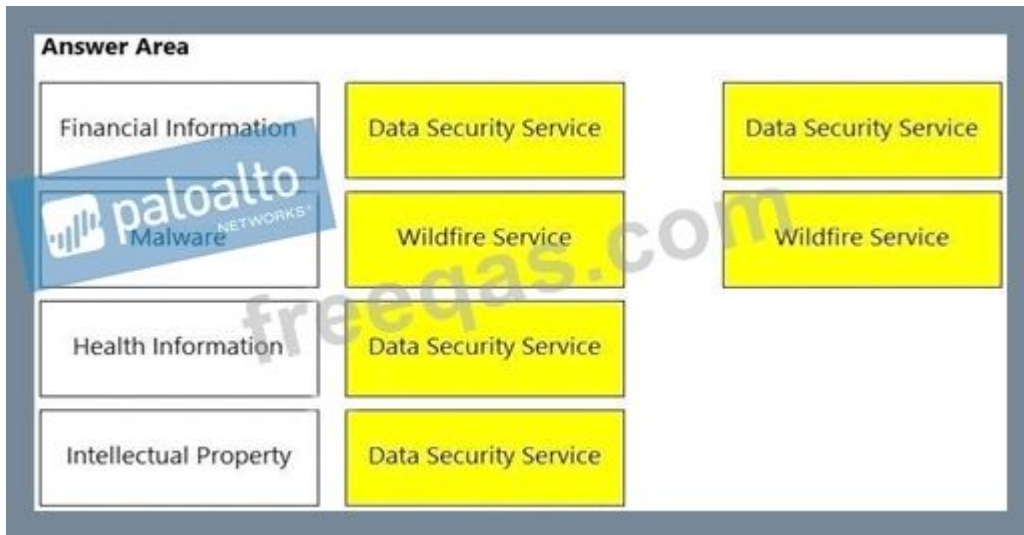


Answer:



Explanation

Diagram Description automatically generated



NEW QUESTION: 16

Review this admission control policy:

```

msg := "msg": msg}} {
  request.operation == "CREATE"
  input.request.kind.kind == "Pod"
  input.request.resource.resource == "Privileged"
  input.request.object.spec.containers[_].securityContext.privileged
  msg := "Privileged"
}

```

Which response to this policy will be achieved when the effect is set to "block"?

- A. The policy will block the creation of a privileged pod
- B. The policy will alert only the administrator when a privileged pod is created
- C. The policy will replace Defender with a privileged Defender
- D. The policy will block all pods on a Privileged host

Answer: C (LEAVE A REPLY)

Valid PCCSE Dumps shared by PrepPdf.com for Helping Passing PCCSE Exam! PrepPdf.com now offer the **newest PCCSE exam dumps**, the PrepPdf.com PCCSE exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PCCSE dumps with Test Engine here: <https://www.preppdf.com/Palo-Alto-Networks/PCCSE-prepaway-exam-dumps.html> (260 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17

Which three steps are involved in onboarding an account for Data Security? (Choose three.)

- A. Create a S3 bucket
- B. Create a Cloudtrail with SNS Topic
- C. Enter the RoleARN and SNSARN
- D. Enable Flow Logs
- E. Create a read-only role with in-line policies

Answer: C,D,E ([LEAVE A REPLY](#))

NEW QUESTION: 18

The compliance team needs to associate Prisma Cloud policies with compliance frameworks. Which option should the team select to perform this task?

- A. Custom Compliance
- B. Policies
- C. Compliance
- D. Alert Rules

Answer: ([SHOW ANSWER](#))

Reference:

[compliance/compliance-dashboard.html](#)

NEW QUESTION: 19

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: A,D,E ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 20

The administrator wants to review the Console audit logs from within the Console Which page in the Console should the administrator use to review this data, if it can be reviewed at all?

- A. The audit logs can be viewed only externally to the Console
- B. Navigate to Monitor > Events > Host Log Inspection
- C. Navigate to Manage > View Logs > History
- D. Navigate to Manage > Defenders > View Logs

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 21

A customer has Prisma Cloud Enterprise and host Defenders deployed

What are two options that allow an administrator to upgrade Defenders'? (Choose two)

- A. with auto-upgrade, the host Defender will auto-upgrade.
- B. auto deploy the Lambda Defender
- C. generate a new DaemonSet file
- D. click the update button in the web-interface

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 22

The Unusual protocol activity (Internal) network anomaly is generating too many alerts. An administrator has been asked to tune it to the option that will generate the least number of events without disabling it entirely. Which strategy should the administrator use to achieve this goal?

- A. Disable the policy
- B. Set the Alert Disposition to Conservative
- C. Change the Training Threshold to Low
- D. Set Alert Disposition to Aggressive

Answer: C (LEAVE A REPLY)

Section: (none)

Explanation

NEW QUESTION: 23

A Prisma Cloud administrator is onboarding a single GCP project to Prisma Cloud. Which two steps can be performed by the Terraform script? (Choose two.)

- A. create the Prisma Cloud role
- B. enable the required APIs for Prisma Cloud
- C. publish the flow log to a storage bucket
- D. enable flow logs for Prisma Cloud.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 24

Which two IDE plugins are supported by Prisma Cloud as part of its DevOps Security? (Choose two.)

- A. Visual Studio Code
- B. BitBucket
- C. CircleCI
- D. IntelliJ

Answer: (SHOW ANSWER)

NEW QUESTION: 25

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: D (LEAVE A REPLY)

Explanation

https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-04/prisma-cloud-compute-edition-admin/access_cont step 2

NEW QUESTION: 26

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	

Answer:

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

Explanation

1. click on compliance standard.
2. add custom compliance standard.
3. edit policies.
4. add compliance standard from drop-down menu

https://docs.prismacloudcompute.com/docs/enterprise_edition/compliance/custom_compliance_checks.html#cre

NEW QUESTION: 27

An administrator has been tasked with creating a custom service that will download any existing compliance report from a Prisma Cloud Enterprise tenant.

In which order will the APIs be executed for this service?

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

Answer Area

Unordered Options

POST https://api.prismacloud.io/login

GET https://api.prismacloud.io/report

GET https://api.prismacloud.io/report/id/download

Ordered Options

Answer:

ANSWER AREA

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	GET https://api.prismacloud.io/report
GET https://api.prismacloud.io/report	GET https://api.prismacloud.io/report/id/download
GET https://api.prismacloud.io/report/id/download	POST https://api.prismacloud.io/login

Explanation

A picture containing graphical user interface Description automatically generated

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	GET https://api.prismacloud.io/report
GET https://api.prismacloud.io/report	GET https://api.prismacloud.io/report/id/download
GET https://api.prismacloud.io/report/id/download	POST https://api.prismacloud.io/login

NEW QUESTION: 28

Which two options may be used to upgrade the Defenders with a Console v20.04 and Kubernetes deployment?

(Choose two.)

- A. Let Defenders automatically upgrade.
- B. Remove Defenders DaemonSet, and then use Cloud Discovery to automatically redeploy the Defenders.
- C. Run the provided curl | bash script from Console to remove Defenders, and then use Cloud Discovery to automatically redeploy Defenders.
- D. Remove Defenders, and then deploy the new DaemonSet so Defenders do not have to automatically update on each deployment.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 29

An administrator needs to write a script that automatically deactivates access keys that have not been used for 30 days.

In which order should the API calls be used to accomplish this task? (Drag the steps into the correct order from the first step to the last.) Select and Place:

Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	
GET https://api.prismacloud.io/access_keys	
PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>	

Answer:
Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	GET https://api.prismacloud.io/access_keys
GET https://api.prismacloud.io/access_keys	PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>
PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>	POST https://api.prismacloud.io/login

Explanation

A picture containing graphical user interface Description automatically generated

Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	GET https://api.prismacloud.io/access_keys
GET https://api.prismacloud.io/access_keys	PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>
PATCH https://api.prismacloud.io/access_keys/<id>/status/<status>	POST https://api.prismacloud.io/login

NEW QUESTION: 30

Which three options are selectable in a CI policy for image scanning with Jenkins or twistcli? (Choose three.)

- A. Scope - Scans run on a particular host
- B. Apply rule only when vendor fixes are available
- C. Grace Period
- D. Failure threshold
- E. Credential

Answer: C,D,E (LEAVE A REPLY)

NEW QUESTION: 31

You are an existing customer of Prisma Cloud Enterprise. You want to onboard a public cloud account and immediately see all of the alerts associated with this account based off ALL of your tenant's existing enabled policies. There is no requirement to send alerts from this account to a downstream application at this time. Which options shows the steps required during the alert rule creation process to achieve this objective?

- A. Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select one or more policies checkbox as part of the alert rule

Confirm the alert rule

- B. Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select one or more policies as part of the alert rule

Add alert notifications

Confirm the alert rule

- C. Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select "select all policies" checkbox as part of the alert rule

Add alert notifications

Confirm the alert rule

- D. Ensure the public cloud account is assigned to an account group

Assign the confirmed account group to alert rule

Select "select all policies" checkbox as part of the alert rule

Confirm the alert rule

Answer: B (LEAVE A REPLY)

Valid PCCSE Dumps shared by PrepPdf.com for Helping Passing PCCSE Exam! PrepPdf.com now offer the **newest PCCSE exam dumps**, the PrepPdf.com PCCSE exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PCCSE dumps with Test Engine here:

NEW QUESTION: 32

A customer wants to scan a serverless function as part of a build process. Which twistcli command can be used to scan serverless functions?

- A. twistcli serverless AWS <SERVERLESS_FUNCTION.ZIP>
- B. twiscli serverless scan <SERVERLESS_FUNCTION.ZIP>
- C. twistcli scan serverless <SERVERLESS_FUNCTION.ZIP>
- D. twistcli function scan <SERVERLESS_FUNCTION.ZIP>

Answer: B (LEAVE A REPLY)

NEW QUESTION: 33


Which three Options are selectable in a CI policy for image scanning with Jenkins or twistcli? (Choose three.)

- A. Scope - Scans run on a particular host
- B. Credential
- C. Failure threshold
- D. Apply rule only when vendor fixes are available
- E. Grace Period

Answer: A,B,D (LEAVE A REPLY)

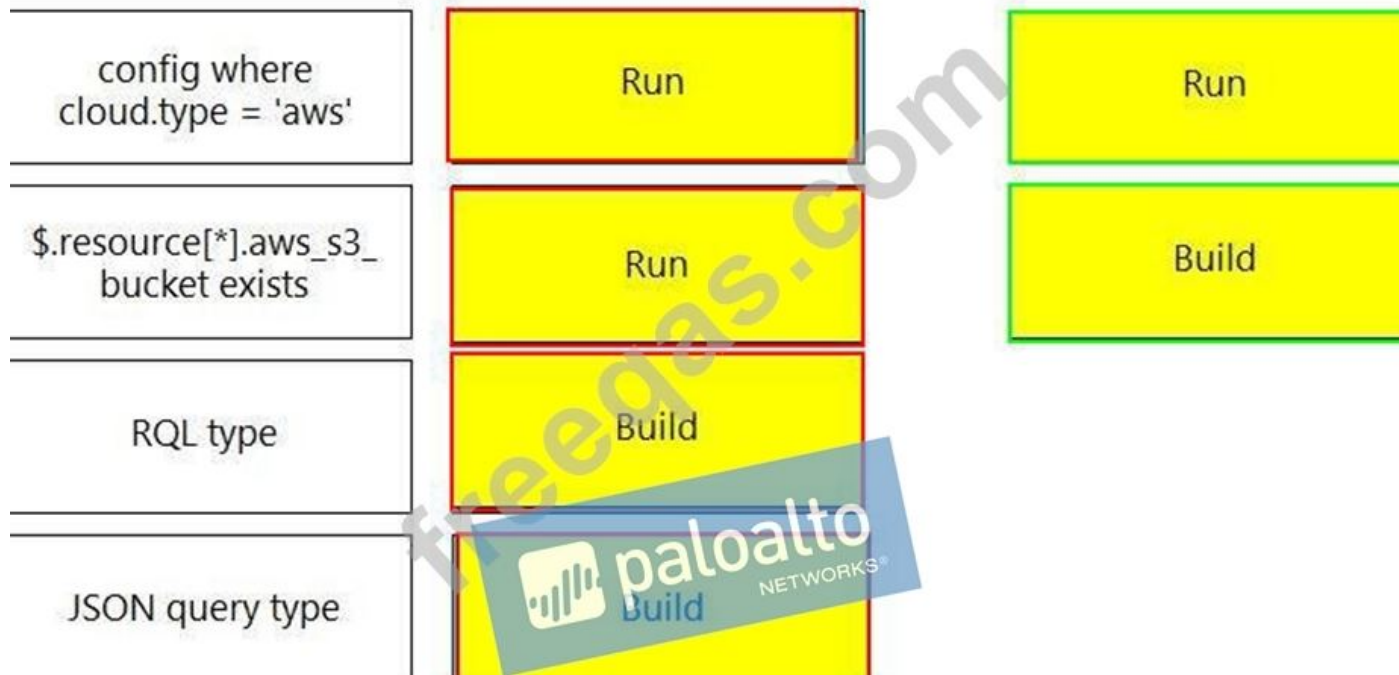
NEW QUESTION: 34

You wish to create a custom policy with build and run subtypes. Match the query types for each example. (Select your answer from the pull-down list. Answers may be used more than once or not at all.)

config where cloud.type = 'aws'		Run
\$.resource[*].aws_s3_bucket exists	Drag answer here	Build
RQL type	Drag answer here	
JSON query type	Drag answer here	

Answer:

Answer Area



Reference:

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

NEW QUESTION: 35

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 36

A Prisma Cloud administrator is tasked with pulling a report via API. The Prisma Cloud tenant is located on app2.prismacloud.io.

What is the correct API endpoint?

- A. <https://api.prismacloud.io>
- B. <https://api2.eu.prismacloud.io>
- C. <https://api.prismacloud.cn>
- D. <https://api2.prismacloud.io>

Answer: D (LEAVE A REPLY)

Explanation

<https://prisma.pan.dev/api/cloud/api-urls/>

NEW QUESTION: 37

A DevOps lead reviewed some system logs and notices some odd behavior that could be a data exfiltration attempt. The DevOps lead only has access to vulnerability data in Prisma Cloud Compute, so the DevOps lead passes this information to SecOps.

Which pages in Prisma Cloud Compute can the SecOps lead use to investigate the runtime aspects of this attack?

- A. The SecOps lead should review the vulnerability scans in the CI/CD process to determine blame.
- B. The SecOps lead should use Incident Explorer and Compliance Explorer.
- C. The SecOps lead should investigate the attack using Vulnerability Explorer and Runtime Radar.
- D. The SecOps lead should use the Incident Explorer page and Monitor > Events > Container Audits.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

A business unit has acquired a company that has a very large AWS account footprint. The plan is to immediately start onboarding the new company's AWS accounts into Prisma Cloud Enterprise tenant immediately. The current company is currently not using AWS Organizations and will require each account to be onboarded individually. The business unit has decided to cover the scope of this action and determined that a script should be written to onboard each of these accounts with general settings to gain immediate posture visibility across the accounts.

Which API endpoint will specifically add these accounts into the Prisma Cloud Enterprise tenant?

- A. `https://api.prismacloud.io/accountgroup/aws`
- B. `https://api.prismacloud.io/cloud/`
- C. `https://api.prismacloud.io/cloud/aws`
- D. `https://api.prismacloud.io/account/aws`

Answer: (SHOW ANSWER)

NEW QUESTION: 39

Which three fields are mandatory when authenticating the Prisma Cloud plugin in the IntelliJ application?

(Choose three.)

- A. Secret Key
- B. Prisma Cloud API URL
- C. Access Key
- D. Asset Name
- E. Tags

Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 40

The development team wants to block Cross Site Scripting attacks from pods in its environment. How should the team construct the CNAF policy to protect against this attack?

- A. create a Container CNAF policy, targeted at a specific resource, and they should set "Explicitly allowed inbound IP sources" to the IP address of the pod.

B. create a Host CNAF policy targeted at a specific resource, check the box for XSS attack protection and set the action to "prevent"

C. create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection and set the action to prevent

D. create a Container CNAF policy, targeted at a specific resource, check the box for XSS attack protection and set the action to alert

Answer: B (LEAVE A REPLY)

NEW QUESTION: 41

What are the two ways to scope a CI policy for image scanning? (Choose two.)

A. image name

B. container name

C. image labels

D. hostname

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 42

Which statement about build and run policies is true?

A. Run policies monitor network activities in the environment and check for potential issues during runtime

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. Build policies enable you to check for security misconfigurations in the IaC templates.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 43

The security team wants to enable the "block" option under compliance checks on the host.

What effect will this option have if it violates the compliance check?

A. Containers on a host will be stopped.

B. Additional hosts will be prevented from starting.

C. No containers will be allowed to start on that host.

D. The host will be taken offline.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 44

Match the service on the right that evaluates each exposure type on the left.

(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Answer Area

Financial Information	Drag answer here	Data Security Service
Malware	Drag answer here	Wildfire Service
Health Information	Drag answer here	
Intellectual Property	Drag answer here	

Answer:

Answer Area		
Financial Information	Data Security Service	Data Security Service
Malware	Wildfire Service	Wildfire Service
Health Information	Data Security Service	
Intellectual Property	Data Security Service	

Reference:

<https://www.paloaltonetworks.com/prisma/cloud/cloud-data-security>

NEW QUESTION: 45

A customer wants to monitor the company's AWS accounts via Prisma Cloud, but only needs the resource configuration to be monitored for now.

Which two pieces of information do you need to onboard this account? (Choose two.)

- A. Cloudtrail
- B. External ID
- C. Active Directory ID

- D. Role ARN
- E. Subscription ID

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 46

A security team is deploying Cloud Native Application Firewall (CNAF) on a containerized web application. The application is running an NGINX container. The container is listening on port 8080 and is mapped to host port 80.

Which port should the team specify in the CNAF rule to protect the application?

- A. 8888
- B. 443
- C. 8080
- D. 80

Answer: C ([LEAVE A REPLY](#))

Valid PCCSE Dumps shared by PrepPdf.com for Helping Passing PCCSE Exam! PrepPdf.com now offer the **newest PCCSE exam dumps**, the PrepPdf.com PCCSE exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PCCSE dumps with Test Engine here: <https://www.preppdf.com/Palo-Alto-Networks/PCCSE-prepaway-exam-dumps.html> (260 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

An administrator has access to a Prisma Cloud Enterprise

What are the steps to deploy a single container Defender on an ec2 node?

- A. Configure the cloud credential in the console and allow cloud discovery to auto-protect the ec2 node
- B. Pull the Defender image to the ec2 node, copy and execute the curl | bash script, and start the Defender to ensure it is running.
- C. Generate DaemonSet file and apply DaemonSet to the twistlock namespace.
- D. Execute the curl | bash script on the ec2 node.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 48

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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

A 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-acr AND json.rule="((((acl grants{?(@ grantee='AllUsers'})] size > 0) or policyStatusisPubiic is true) and publicAccessBlockConfiguration does not exist) or ((ad.grantsp(@ grantee=='All Users']) size > 0) and publicAccessBlockConfiguration ignorePubhcAds 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. configuration of the S3 bucket
- C. anomalous behaviors
- D. network traffic to the S3 bucket

Answer: C (LEAVE A REPLY)

NEW QUESTION: 50

Which statement is true regarding CloudFormation templates?

- A. Scan support does not currently exist for nested references, macros, or intrinsic functions.
- B. A single template or a zip archive of template files cannot be scanned with a single API request.
- C. Request-Header-Field 'cloudformation-version' is required to request a scan.
- D. Scan support is provided for JSON, HTML and YAML formats.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 51

What is the order of steps in a Jenkins pipeline scan?

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

Answer Area

Unordered Options	Ordered Options
Scan Image	
Publish Scan Details	
Build Image	
Commit to Registry	

Answer:

Answer Area

Unordered Options

Scan Image
Publish Scan Details
Build Image
Commit to Registry

Ordered Options

Scan Image
Publish Scan Details
Build Image
Commit to Registry

Explanation

Table Description automatically generated with medium confidence

Answer Area

Unordered Options

Scan Image
Publish Scan Details
Build Image
Commit to Registry

Ordered Options

Scan Image
Publish Scan Details
Build Image
Commit to Registry

NEW QUESTION: 52

An administrator has been tasked with creating a custom service that will download any existing compliance report from a Prisma Cloud Enterprise.

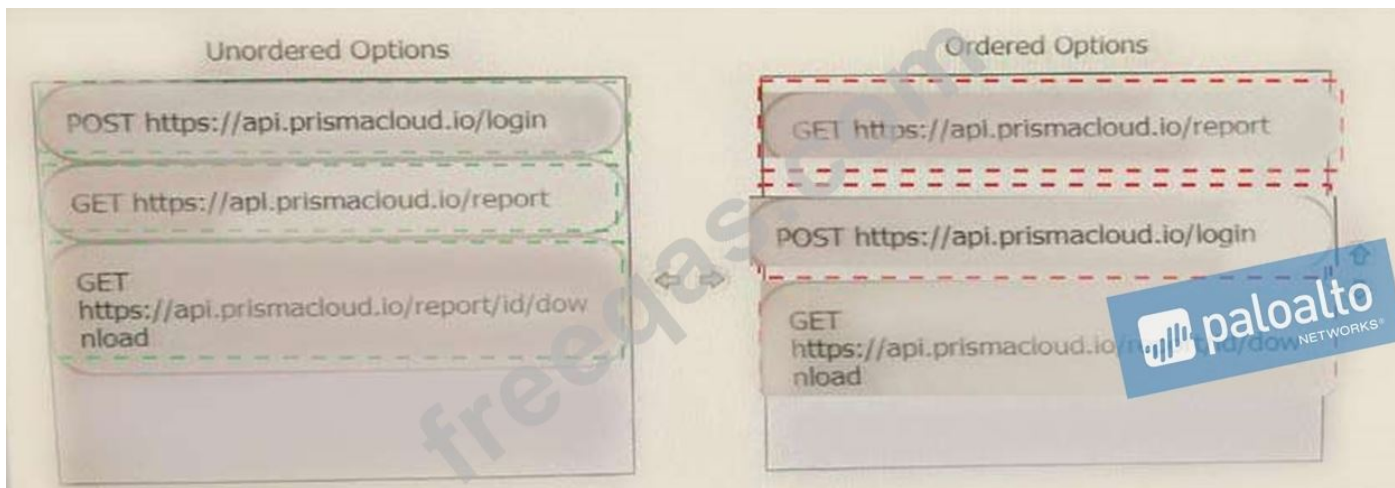
tenant-In which order will the APIs be executed for this service? (Drag the steps into the correct order of occurrence from the first step to the last)

Unordered Options

POST https://api.prismacloud.io/login
GET https://api.prismacloud.io/report
GET https://api.prismacloud.io/report/download

Ordered Options

Answer:



NEW QUESTION: 53

The security team wants to target a CMAF policy for specific running Containers How should the administrator scope the policy to target the Containers?

- A. scope the policy to Defender names.
- B. scope the policy to Image names
- C. scope the policy to namespaces
- D. scope the policy to Host names

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 54

An administrator has a requirement to ingest all Console and Defender logs to Splunk. Which option will satisfy this requirement in Prisma Cloud Compute?

- A. Enable the CSV export in the Console.
- B. Enable the API settings for logging.
- C. Enable the Splunk option in the Console.
- D. Enable the syslog option in the Console

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

An administrator wants to enforce a rate limit for users not being able to post five (5) .tar.gz files within five (5) seconds.

What does the administrator need to configure?

- A. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar.gz on CNNF
- B. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on WAAS
- C. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on CNNF
- D. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar.gz on WAAS

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 56

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

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 57

Given an existing ECS Cluster, which option shows the steps required to install the Console in Amazon ECS?

- A. The console cannot natively run in an ECS cluster. A onebox deployment should be used.
- B. Download and extract the release tarball
Create an EFS file system and mount to each node in the cluster
Create the Console task definition
Deploy the task definition
- C. Download and extract release tarball
Download task from AWS
Create the Console task definition
Deploy the task definition
- D. Download and extract the release tarball
Ensure that each node has its own storage for Console data
Create the Console task definition
Deploy the task definition

Answer: B (LEAVE A REPLY)

NEW QUESTION: 58

An administrator wants to install the Defenders to a Kubernetes cluster. This cluster is running the console on the default service endpoint and will be exporting to YAML
Console Address \$CONSOLE_ADDRESS
Websocket Address \$WEBSOCKET_ADDRESS
User: \$ADMIN_USER
Which command generates the YAML file for Defender install?

A)

```
<PLATFORM>/twistcli defender export kubernetes \  
-address $CONSOLE_ADDRESS \  
-user $ADMIN_USER \  
-cluster-address $WEBSOCKET_ADDRESS
```

B)

```
<PLATFORM>/twistcli defender \  
-address $CONSOLE_ADDRESS \  
-user $ADMIN_USER \  
-cluster-address $CONSOLE_ADDRESS
```

C)

```
<PLATFORM>/twistcli defender YAML kubernetes \  
-address $CONSOLE_ADDRESS \  
-user $ADMIN_USER \  
-cluster-address $WEBSOCKET_ADDRESS
```

D)

```
<PLATFORM>/twistcli defender export kubernetes \
--address $WEBSOCKET_ADDRESS \
--user $ADMIN_USER \
--cluster-address $CONSOLE_ADDRESS
```

- A. Option A
- B. Option C
- C. Option D
- D. Option B

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 59

Match the correct scanning mode for each given operation.
 (Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Create SNS Topic Triggers	Drag answer here	No data security scan
Select an S3 bucket	Drag answer here	Forward Scan only
Select an S3 bucket with existing files	Drag answer here	Forward or Backward Scan
Link an S3 logging to CloudTrail	Drag answer here	Backward Scan only

Answer:

Answer Area

Create SNS Topic Triggers	Forward or Backward Scan	No data security scan
Select an S3 bucket	No data security scan	Forward Scan only
Select an S3 bucket with existing files	Backward Scan only	Forward or Backward Scan
Link an S3 logging to CloudTrail	Forward Scan only	Backward Scan only

Explanation

Diagram Description automatically generated

Create SNS Topic Triggers	Forward or Backward Scan	No data security scan
Select an S3 bucket	No data security scan	Forward Scan only
Select an S3 bucket with existing files	Backward Scan only	Forward or Backward Scan
Link an S3 logging to CloudTrail	Forward Scan only	Backward Scan only

NEW QUESTION: 60

A customer has multiple violations in the environment including:

User namespace is enabled

An LDAP server is enabled

SSH root is enabled

Which section of Console should the administrator use to review these findings?

- A. Manage
- B. Radar

C. Vulnerabilities

D. Compliance

Answer: A (LEAVE A REPLY)

NEW QUESTION: 61

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. 8081

B. 443

C. 8084

D. 8083

Answer: C (LEAVE A REPLY)

Explanation

<https://docs.paloaltonetworks.com/prisma/prisma-cloud/20-12/prisma-cloud-compute-edition-admin/howto/con>

Valid PCCSE Dumps shared by PrepPdf.com for Helping Passing PCCSE Exam! PrepPdf.com now offer the **newest PCCSE exam dumps**, the PrepPdf.com PCCSE exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PCCSE dumps with Test Engine here: <https://www.preppdf.com/Palo-Alto-Networks/PCCSE-prepaway-exam-dumps.html> (260 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 62

Which statement about build and run policies is true?

A. The four main types of policies are: Audit Events, Build, Network, and Run.

B. Run policies monitor network activities in the environment and check for potential issues during runtime.

C. Every type of policy has auto-remediation enabled by default.

D. Build policies enable you to check for security misconfigurations in the IaC templates.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 63

Order the steps involved in onboarding an AWS Account for use with Data Security feature.

Answer Area

Unordered Options

Enter RoleARN and SNSARN

Create Stack

Enter SNS Topic in CloudTrail

Create CloudTrail with S3 as storage

Ordered Options

Four empty dashed boxes for ordering the options.

Answer:

Answer Area

Unordered Options

Enter RoleARN and SNSARN

Create Stack

Enter SNS Topic in CloudTrail

Create CloudTrail with S3 as storage

Ordered Options

Create Stack

Create CloudTrail with S3 as storage

Enter SNS Topic in CloudTrail

Enter RoleARN and SNSARN

NEW QUESTION: 64

What is the order of steps in a Jenkins pipeline scan?

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

Answer Area

Unordered Options

Scan Image

Publish Scan Details

Build Image

Commit to Repo

Ordered Options

Four empty dashed boxes for ordering the options.

Answer:

Answer Area

Unordered Options

- Scan Image
- Publish Scan Details
- Build Image
- Commit to Registry

Ordered Options

- Scan Image
- Publish Scan Details
- Build Image
- Commit to Registry

NEW QUESTION: 65

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

The security auditors need to ensure that given compliance checks are being run on the host. Which option is a valid host compliance policy?

- A. Ensure compliant Docker daemon configuration
- B. Ensure images are created with a non-root user
- C. Ensure functions are not overly permissive.
- D. Ensure host devices are not directly exposed to containers.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 67

An administrator wants to install the Defenders to a Kubernetes cluster. This cluster is running the console on the default service endpoint and will be exporting to YAML.

Console Address: \$CONSOLE_ADDRESS Websocket Address: \$WEBSOCKET_ADDRESS User: \$ADMIN_USER

Which command generates the YAML file for Defender install?

- A. `<PLATFORM>/twistcli defender \`
`--address $CONSOLE_ADDRESS \`

```

--user $ADMIN_USER \
--cluster-address $CONSOLE_ADDRESS
B. <PLATFORM>/twistcli defender export kubernetes \
--address $CONSOLE_ADDRESS \
--user $ADMIN_USER \
--cluster-address $WEBSOCKET_ADDRESS
C. <PLATFORM>/twistcli defender export kubernetes \
--address $WEBSOCKET_ADDRESS \
--user $ADMIN_USER \
--cluster-address $CONSOLE_ADDRESS
D. <PLATFORM>/twistcli defender YAML kubernetes \
--address $CONSOLE_ADDRESS \
--user $ADMIN_USER \
--cluster-address $WEBSOCKET_ADDRESS

```

Answer: B (LEAVE A REPLY)

NEW QUESTION: 68

An administrator needs to write a script that automatically deactivates access keys that have not been used for 30 days In which order should the API calls be used to accomplish this task? (Drag the steps into the correct order from the first step to the last.)

Answer:

NEW QUESTION: 69

Which statement accurately characterizes SSO Integration on Prisma Cloud?

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 70

A customer is deploying Defenders to a Fargate environment. It wants to understand the vulnerabilities in the images it is deploying. How should the customer automate vulnerability scanning for images deployed to Fargate?

- A. Use Cloud Compliance to identify misconfigured AWS accounts
- B. Set up a vulnerability scanner on the registry
- C. Designate a Fargate Defender to serve as a dedicated image scanner
- D. Embed a Fargate Defender to automatically scan for vulnerabilities

Answer: D (LEAVE A REPLY)

NEW QUESTION: 71

Which statement is true regarding CloudFormation templates?

- A. Request-Header-Field 'cloudformation-version' is required to request a scan.
- B. Scan support is provided for JSON, HTML, and YAML formats.
- C. A single template or a zip archive of template files cannot be scanned with a single API request.
- D. Scan support does not currently exist for nested references, macros, or intrinsic functions.

Answer: (SHOW ANSWER)


NEW QUESTION: 72

An administrator has been tasked with creating a custom service that will download any existing compliance report from a Prisma Cloud Enterprise tenant.

In which order will the APIs be executed for this service?

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

Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	
GET https://api.prismacloud.io/report	
GET https://api.prismacloud.io/report/id/download	

Answer:
Answer Area

Unordered Options	Ordered Options
POST https://api.prismacloud.io/login	GET https://api.prismacloud.io/report
GET https://api.prismacloud.io/report	GET https://api.prismacloud.io/report/id/download
GET https://api.prismacloud.io/report/id/download	POST https://api.prismacloud.io/login

NEW QUESTION: 73

A business unit has acquired a company that has a very large AWS account footprint. The plan is to immediately start onboarding the new company's AWS accounts into Prisma Cloud Enterprise tenant immediately. The current company is currently not using AWS Organizations and will require each account to be onboarded individually.

The business unit has decided to cover the scope of this action and determined that a script should be written to onboard each of these accounts with general settings to gain immediate posture visibility across the accounts.

Which API endpoint will specifically add these accounts into the Prisma Cloud Enterprise tenant?

- A. https://api.prismacloud.io/cloud/
- B. https://api.prismacloud.io/cloud/aws
- C. https://api.prismacloud.io/account/aws
- D. https://api.prismacloud.io/accountgroup/aws

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 74

Which container image scan is constructed correctly?

- A. `twistcli images scan -address https //us-west1 cloud twistlock com/us-3-123456789 -container myimage/latest`
- B. `twistcli images scan -address https://us-west1. cloud.twistlock.com/us-3-123456789 -container myimage/latest -details`
- C. `twistcii images scan -address https7/us-west1 cloud.twistlockxom/us-3-123456789 myimage/latest`
- D. `twistcii images scan -docker-address https://us-west1 cloud twistlock com/us-3-123456?89 myimage/latest`

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 75

Match the correct scanning mode for each given operation.

(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Answer:

NEW QUESTION: 76

Which two statements are true about the differences between build and run config policies? (Choose two.)

- A. Build policies enable you to check for security misconfigurations in the IaC templates and ensure that these issues do not get into production.

- B. Run policies monitor network activities in your environment, and check for potential issues during runtime.
- C. Run and Network policies belong to the configuration policy set
- D. Build and Audit Events policies belong to the configuration policy set
- E. Run policies monitor resources, and check for potential issues after these cloud resources are deployed

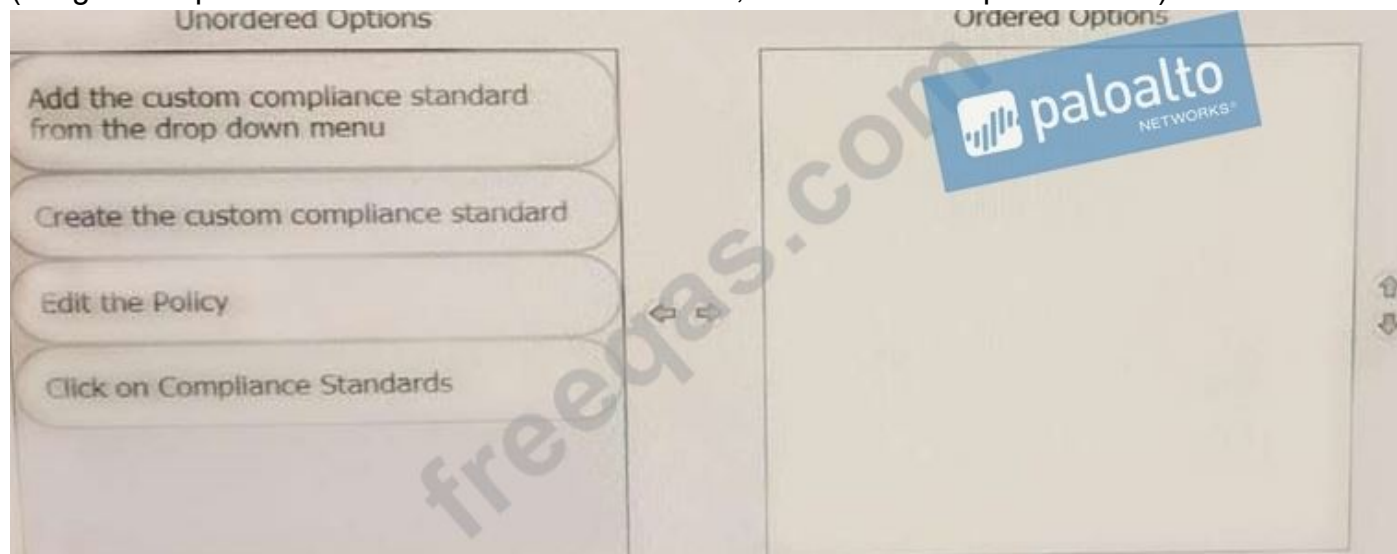
Answer: ([SHOW ANSWER](#))

Valid PCCSE Dumps shared by PrepPdf.com for Helping Passing PCCSE Exam! PrepPdf.com now offer the **newest PCCSE exam dumps**, the PrepPdf.com PCCSE exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PCCSE dumps with Test Engine here: <https://www.preppdf.com/Palo-Alto-Networks/PCCSE-prepaway-exam-dumps.html> (260 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

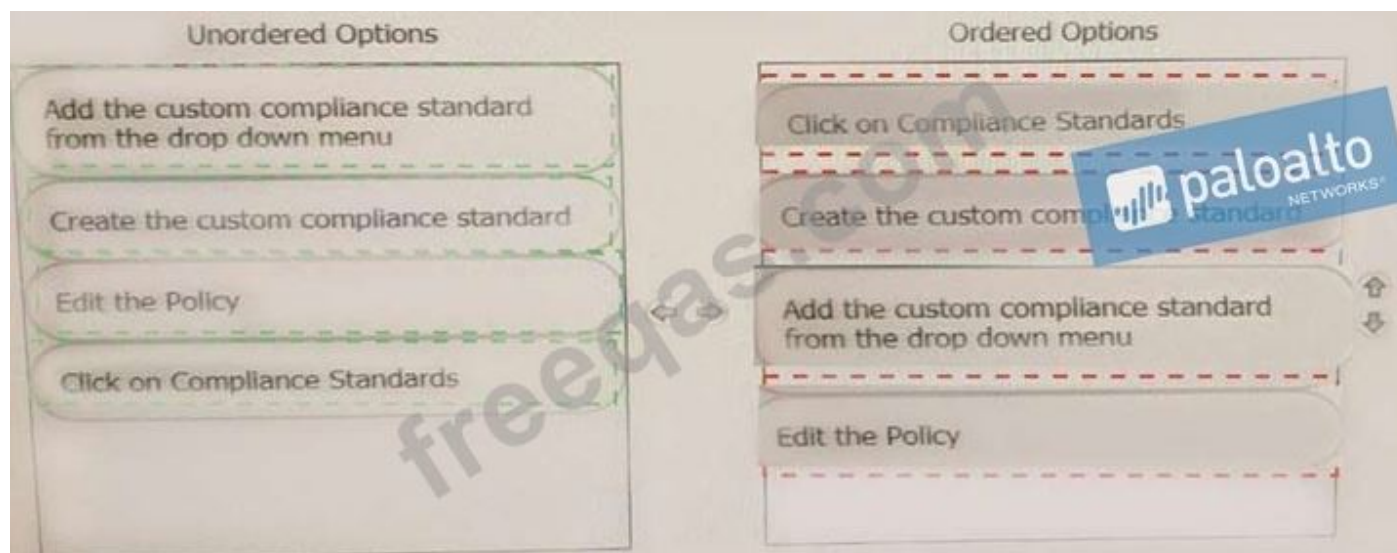
NEW QUESTION: 77

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:



Valid PCCSE Dumps shared by PrepPdf.com for Helping Passing PCCSE Exam! PrepPdf.com now offer the **newest PCCSE exam dumps**, the PrepPdf.com PCCSE exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PCCSE dumps with Test Engine here: <https://www.preppdf.com/Palo-Alto-Networks/PCCSE-prepaway-exam-dumps.html> (**260** Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)