Actual exam question from Palo Alto Networks's PCCSE

Question #: 1

Topic #: 1

[All PCCSE Questions]

Given a default deployment of Console, a customer needs to identify the alerted compliance checks that are set by default.

Where should the customer navigate in Console?

A. Monitor > Compliance

B. Defend > Compliance

C. Manage > Compliance

D. Custom > Compliance

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 2

Topic #: 1

[All PCCSE Questions]

Which container scan is constructed correctly?

A. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest

B. twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

C. twistcli images scan -u api -p api --address https://us-west1.cloud.twistlock.com/us-3-123456789 --details myimage/latest

D. twistcli images scan -u api -p api --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 3

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 4

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 5

Topic #: 1

[All PCCSE Questions]

A customer has a requirement to terminate any Container from image topSecret:latest when a process named ransomWare is executed.

How should the administrator configure Prisma Cloud Compute to satisfy this requirement?

A. set the Container model to manual relearn and set the default runtime rule to block for process protection.

B. set the Container model to relearn and set the default runtime rule to prevent for process protection.

C. add a new runtime policy targeted at a specific Container name, add ransomWare process into the denied process list, and set the action to ɹ€preventɹ€.

D. choose ɹ€copy into ruleɹ€ for the Container, add a ransomWare process into the denied process list, and set the action to ɹ€blockɹ€.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 6

Topic #: 1

[All PCCSE Questions]

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 certificate. 2. Retrieve the Prisma Cloud Console images using 'docker pull'.

D. To retrieve Prisma Cloud Console images using URL auth: 1. Access registry-auth.twistlock.com, and authenticate using the user certificate. 2. Retrieve the Prisma Cloud Console images using 'docker pull'.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 7

Topic #: 1

[All PCCSE Questions]

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

A. Run and Network policies belong to the configuration policy set.

B. Build and Audit Events policies belong to the configuration policy set.

C. Run policies monitor resources, and check for potential issues after these cloud resources are deployed.

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

E. Run policies monitor network activities in your environment, and check for potential issues during runtime.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 8

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 9

Topic #: 1

[All PCCSE Questions]

A customer does not want alerts to be generated from network traffic that originates from trusted internal networks.

Which setting should you use to meet this customer's request?

A. Trusted Login IP Addresses

B. Anomaly Trusted List

C. Trusted Alert IP Addresses

D. Enterprise Alert Disposition

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 10

Topic #: 1

[All PCCSE Questions]

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 investigate the attack using Vulnerability Explorer and Runtime Radar.

B. The SecOps lead should use Incident Explorer and Compliance Explorer.

C. The SecOps lead should use the Incident Explorer page and Monitor > Events > Container Audits.

D. The SecOps lead should review the vulnerability scans in the CI/CD process to determine blame.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 11

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 12

Topic #: 1

[All PCCSE Questions]

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

A. Create a read-only role with in-line policies

B. Create a Cloudtrail with SNS Topic

C. Enable Flow Logs

D. Enter the RoleARN and SNSARN

E. Create a S3 bucket

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 13

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 14

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 15

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 16

Topic #: 1

[All PCCSE Questions]

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. enable flow logs for Prisma Cloud.

B. create the Prisma Cloud role.

C. enable the required APIs for Prisma Cloud.

D. publish the flow log to a storage bucket.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 17

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE
Question #: 18
Topic #: 1
[All PCCSE Questions]

An administrator sees that a runtime audit has been generated for a host.
The audit message is:
`Service postfix attempted to obtain capability SHELL by executing /bin/sh /usr/libexec/postfix/postfix-script.stop. Low severity audit, event is automatically added to the runtime model`
Which runtime host policy rule is the root cause for this runtime audit?

A. Custom rule with specific configuration for file integrity

B. Custom rule with specific configuration for networking

C. Default rule that alerts on capabilities

D. Default rule that alerts on suspicious runtime behavior

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 19

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 20

Topic #: 1

[All PCCSE Questions]

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

A. Host

B. Container

C. Functions

D. Image

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 21

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 22

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 23

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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.)

Select and Place:

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	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 24

Topic #: 1

[All PCCSE Questions]

A customer is interested in PCI requirements and needs to ensure that no privilege containers can start in the environment.

Which action needs to be set for `do not use privileged containers`?

A. Prevent

B. Alert

C. Block

D. Fail

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 25

Topic #: 1

[All PCCSE Questions]

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 Ensure that each node has its own storage for Console data 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 Create an EFS file system and mount to each node in the cluster Create the Console task definition Deploy the task definition

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 26

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 27

Topic #: 1

[All PCCSE Questions]

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. click the update button in the web-interface.

D. generate a new DaemonSet file.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 28

Topic #: 1

[All PCCSE Questions]

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

A. High

B. Medium

C. Low

D. Very High

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 29

Topic #: 1

[All PCCSE Questions]

Given this information:

- ✑ The Console is located at https://prisma-console.mydomain.local
- ✑ The username is: cluster
- ✑ The password is: password123
- ✑ The image to scan is: myimage:latest

Which twistcli command should be used to scan a Container for vulnerabilities and display the details about each vulnerability?

A. twistcli images scan --console-address https://prisma-console.mydomain.local -u cluster -p password123 --details myimage:latest

B. twistcli images scan --console-address prisma-console.mydomain.local -u cluster -p password123 --vulnerability-details myimage:latest

C. twistcli images scan --address prisma-console.mydomain.local -u cluster -p password123 --vulnerability-details myimage:latest

D. twistcli images scan --address https://prisma-console.mydomain.local -u cluster -p password123 --details myimage:latest

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 30

Topic #: 1

[All PCCSE Questions]

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 Host CNAF policy, targeted at a specific resource, check the box for XSS attack protection, and set the action to ɹ€preventɹ€.

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

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

D. create a Container CNAF policy, targeted at a specific resource, and they should set ɹ€Explicitly allowed inbound IP sourcesɹ€ to the IP address of the pod.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 31

Topic #: 1

[All PCCSE Questions]

The Prisma Cloud administrator has configured a new policy.

Which steps should be used to assign this policy to a compliance standard?

A. Edit the policy, go to step 3 (Compliance Standards), click + at the bottom, select the compliance standard, fill in the other boxes, and then click Confirm.

B. Create the Compliance Standard from Compliance tab, and then select Add to Policy.

C. Open the Compliance Standards section of the policy, and then save.

D. Custom policies cannot be added to existing standards.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 32

Topic #: 1

[All PCCSE Questions]

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 $WEBSOCKET_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 $CONSOLE_ADDRESS \ --user $ADMIN_USER \ --cluster-address $WEBSOCKET_ADDRESS

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 33

Topic #: 1

[All PCCSE Questions]

Which options show the steps required after upgrade of Console?

A. Uninstall Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicable Allow the Console to redeploy the Defender

B. Update the Console image in the Twistlock hosted registry Update the Defender image in the Twistlock hosted registry Uninstall Defenders

C. Upgrade Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicable

D. Update the Console image in the Twistlock hosted registry Update the Defender image in the Twistlock hosted registry Redeploy Console

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 34

Topic #: 1

[All PCCSE Questions]

An organization wants to be notified immediately to any `High Severity` alerts for the account group `Clinical Trials` via Slack.

Which option shows the steps the organization can use to achieve this goal?

A. 1. Configure Slack Integration 2. Create an alert rule and select ɹ€Clinical Trialsɹ€ as the account group 3. Under the ɹ€Select Policiesɹ€ tab, filter on severity and select ɹ€High4 €ɹ. Under the Set Alert Notification tab, choose Slack and populate the channel 5. Set Frequency to ɹ€As it Happensɹ€

B. 1. Create an alert rule and select ɹ€Clinical Trialsɹ€ as the account group 2. Under the ɹ€Select Policiesɹ€ tab, filter on severity and select ɹ€High3 €ɹ. Under the Set Alert Notification tab, choose Slack and populate the channel 4. Set Frequency to ɹ€As it Happens5 €ɹ. Set up the Slack Integration to complete the configuration

C. 1. Configure Slack Integration 2. Create an alert rule 3. Under the ɹ€Select Policiesɹ€ tab, filter on severity and select ɹ€High4 €ɹ. Under the Set Alert Notification tab, choose Slack and populate the channel 5. Set Frequency to ɹ€As it Happensɹ€

D. 1. Under the ɹ€Select Policiesɹ€ tab, filter on severity and select ɹ€High2 €ɹ. Under the Set Alert Notification tab, choose Slack and populate the channel 3. Set Frequency to ɹ€As it Happens4 €ɹ. Configure Slack Integration 5. Create an Alert rule

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 35

Topic #: 1

[All PCCSE Questions]

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/account/aws

C. https://api.prismacloud.io/cloud/aws

D. https://api.prismacloud.io/accountgroup/aws

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 36

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 37

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 38

Topic #: 1

[All PCCSE Questions]

What is the behavior of Defenders when the Console is unreachable during upgrades?

A. Defenders continue to alert, but not enforce, using the policies and settings most recently cached before upgrading the Console.

B. Defenders will fail closed until the web-socket can be re-established.

C. Defenders will fail open until the web-socket can be re-established.

D. Defenders continue to alert and enforce using the policies and settings most recently cached before upgrading the Console.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 39

Topic #: 1

[All PCCSE Questions]

How are the following categorized?

- ✑ Backdoor account access
- ✑ Hijacked processes
- ✑ Lateral movement
- ✑ Port scanning

A. audits

B. incidents

C. admission controllers

D. models

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 40

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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>	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 41

Topic #: 1

[All PCCSE Questions]

Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?

A. single sign-on

B. SAML

C. basic authentication

D. access key

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 42

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 43

Topic #: 1

[All PCCSE Questions]

A customer has a requirement to automatically protect all Lambda functions with runtime protection.

What is the process to automatically protect all the Lambda functions?

A. Configure a function scan policy from the Defend/Vulnerabilities/Functions page.

B. Configure serverless radar from the Defend/Compliance/Cloud Platforms page.

C. Configure a manually embedded Lambda Defender.

D. Configure a serverless auto-protect rule for the functions.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 44

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 45

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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.)

Select and Place:

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	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 46

Topic #: 1

[All PCCSE Questions]

What are two ways to scan container images in Jenkins pipelines? (Choose two.)

A. twistcli

B. Jenkins Docker plugin

C. Compute Jenkins plugin

D. Compute Azure DevOps plugin

E. Prisma Cloud Visual Studio Code plugin with Jenkins integration

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 47

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 48

Topic #: 1

[All PCCSE Questions]

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. httsp://api.prismacloud.cn

D. https://api2.prismacloud.io

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 49

Topic #: 1

[All PCCSE Questions]

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 Monitor > Vulnerabilities > CVE Viewer

B. Navigate to Defend > Vulnerabilities > VM Images

C. Navigate to Defend > Vulnerabilities > Hosts

D. Navigate to Monitor > Vulnerabilities > Hosts

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 50

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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

Select and Place:

Answer Area

Unordered Options	Ordered Options
Enter RoleARN and SNSARN	
Create Stack	
Enter SNS Topic in CloudTrail	
Create CloudTrail with S3 as storage	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 51

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 52

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE
Question #: 53
Topic #: 1
[All PCCSE Questions]

You have onboarded a public cloud account into Prisma Cloud Enterprise. Configuration Resource ingestion is visible in the Asset Inventory for the onboarded account, but no alerts are being generated for the configuration assets in the account.
Config policies are enabled in the Prisma Cloud Enterprise tenant, with those policies associated to existing alert rules. ROL statements on the investigate matching those policies return config resource results successfully.
Why are no alerts being generated?

A. The public cloud account is not associated with an alert notification.

B. The public cloud account does not have audit trail ingestion enabled.

C. The public cloud account does not access to configuration resources.

D. The public cloud account is not associated with an alert rule.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 54

Topic #: 1

[All PCCSE Questions]

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 Defender names.

D. scope the policy to Host names.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 55

Topic #: 1

[All PCCSE Questions]

The InfoSec team wants to be notified via email each time a Security Group is misconfigured.

Which Prisma Cloud tab should you choose to complete this request?

A. Notifications

B. Policies

C. Alert Rules

D. Events

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 56

Topic #: 1

[All PCCSE Questions]

An administrator has access to a Prisma Cloud Enterprise.

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

A. Pull the Defender image to the ec2 node, copy and execute the curl | bash script, and start the Defender to ensure it is running.

B. Execute the curl | bash script on the ec2 node.

C. Configure the cloud credential in the console and allow cloud discovery to auto-protect the ec2 node.

D. Generate DaemonSet file and apply DaemonSet to the twistlock namespace.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 57

Topic #: 1

[All PCCSE Questions]

A customer wants to turn on Auto Remediation.

Which policy type has the built-in CLI command for remediation?

A. Anomaly

B. Audit Event

C. Network

D. Config

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 58

Topic #: 1

[All PCCSE Questions]

A customer is deploying Defenders to a Fargate environment. It wants to understand the vulnerabilities in the image it is deploying.

How should the customer automate vulnerability scanning for images deployed to Fargate?

A. Set up a vulnerability scanner on the registry

B. Embed a Fargate Defender to automatically scan for vulnerabilities

C. Designate a Fargate Defender to serve a dedicated image scanner

D. Use Cloud Compliance to identify misconfigured AWS accounts

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 59

Topic #: 1

[All PCCSE Questions]

Which container image scan is constructed correctly?

A. twistcli images scan --docker-address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

B. twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 myimage/latest

C. twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest

D. twistcli images scan --address https://us-west1.cloud.twistlock.com/us-3-123456789 --container myimage/latest --details

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 60

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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.)

Select and Place:

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	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 61

Topic #: 1

[All PCCSE Questions]

Which two processes ensure that builds can function after a Console upgrade? (Choose two.)

A. allowing Jenkins to automatically update the plugin

B. updating any build environments that have twistcli included to use the latest version

C. configuring build pipelines to download twistcli at the start of each build

D. creating a new policy that allows older versions of twistcli to connect the Console

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 62

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 63

Topic #: 1

[All PCCSE Questions]

Review this admission control policy:

```
match[{"msg": msg}] {
input.request.operation == "CREATE"
input.request.kind.kind == "Pod"
input.request.resource.resource == "pods"
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 all pods on a Privileged host.

B. The policy will replace Defender with a privileged Defender.

C. The policy will alert only the administrator when a privileged pod is created.

D. The policy will block the creation of a privileged pod.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 64

Topic #: 1

[All PCCSE Questions]

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. Target section within an Alert Rule.

B. Notification Template section within Alerts.

C. Users section within Settings.

D. Set Alert Notification section within an Alert Rule.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 65

Topic #: 1

[All PCCSE Questions]

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 function scan <SERVERLESS_FUNCTION.ZIP>

B. twistcli scan serverless <SERVERLESS_FUNCTION.ZIP>

C. twistcli serverless AWS <SERVERLESS_FUNCTION.ZIP>

D. twiscli serverless scan <SERVERLESS_FUNCTION.ZIP>

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE
Question #: 66
Topic #: 1
[All PCCSE Questions]

A customer has a development environment with 50 connected Defenders. A maintenance window is set for Monday to upgrade 30 stand-alone Defenders in the development environment, but there is no maintenance window available until Sunday to upgrade the remaining 20 stand-alone Defenders.
Which recommended action manages this situation?

A. Go to Manage > Defender > Manage, then click Defenders, and use the Scheduler to choose which Defenders will be automatically upgraded during the maintenance window.

B. Find a maintenance window that is suitable to upgrade all stand-alone Defenders in the development environment.

C. Upgrade a subset of the Defenders by clicking the individual Actions > Upgrade button in the row that corresponds to the Defender that should be upgraded during the maintenance window.

D. Open a support case with Palo Alto Networks to arrange an automatic upgrade.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 67

Topic #: 1

[All PCCSE Questions]

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

A. AWS Inspector

B. Qualys

C. Tenable

D. PagerDuty

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 68

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 69

Topic #: 1

[All PCCSE Questions]

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 functions are not overly permissive.

B. Ensure host devices are not directly exposed to containers.

C. Ensure images are created with a non-root user.

D. Ensure compliant Docker daemon configuration.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 71

Topic #: 1

[All PCCSE Questions]

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 72

Topic #: 1

[All PCCSE Questions]

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. 443

B. 80

C. 8080

D. 8888

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 73

Topic #: 1

[All PCCSE Questions]

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

A. Public

B. Private

C. International

D. Differential

E. Conditional

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 74

Topic #: 1

[All PCCSE Questions]

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. Navigate to Monitor > Events > Host Log Inspection

B. The audit logs can be viewed only externally to the Console

C. Navigate to Manage > Defenders > View Logs

D. Navigate to Manage > View Logs > History

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 75

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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.)

Select and Place:

Answer Area

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 76

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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.)

Select and Place:

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	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 77

Topic #: 1

[All PCCSE Questions]

DRAG DROP -

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.)

Select and Place:

Answer Area

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 78

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 79

Topic #: 1

[All PCCSE Questions]

A customer has a large environment that needs to upgrade Console without upgrading all Defenders at one time.

What are two prerequisites prior to performing a rolling upgrade of Defenders? (Choose two.)

A. manual installation of the latest twistcli tool prior to the rolling upgrade

B. all Defenders set in read-only mode before execution of the rolling upgrade

C. a second location where you can install the Console

D. additional workload licenses are required to perform the rolling upgrade

E. an existing Console at version n-1

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 80

Topic #: 1

[All PCCSE Questions]

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.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 81

Topic #: 1

[All PCCSE Questions]

Which `kind` of Kubernetes object is configured to ensure that Defender is acting as the admission controller?

A. MutatingWebhookConfiguration

B. DestinationRules

C. ValidatingWebhookConfiguration

D. PodSecurityPolicies

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 82

Topic #: 1

[All PCCSE Questions]

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. Apply rule only when vendor fixes are available

D. Failure threshold

E. Grace Period

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 83

Topic #: 1

[All PCCSE Questions]

Which component(s), if any, will Palo Alto Networks host and run when a customer purchases Prisma Cloud Enterprise Edition?

A. Defenders

B. Console

C. Jenkins

D. twistcli

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 84

Topic #: 1

[All PCCSE Questions]

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

A. 53

B. 25

C. 8084

D. 8083

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 85

Topic #: 1

[All PCCSE Questions]

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 ı€select all policiesı€ 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 checkbox as part of the alert rule 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 one or more policies 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 ı€select all policiesı€ checkbox as part of the alert rule Add alert notifications Confirm the alert rule

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 86

Topic #: 1

[All PCCSE Questions]

A customer has configured the JIT, and the user created by the process is trying to log in to the Prisma Cloud console. The user encounters the following error message:

```
Saml Missing Required Auto Provision Attributes
Error occurred due to unexpected value of required field 'SAML_RESPONSE'
Expected Value: 'unavailable'
Actual Value: '[ROLE=[3ed546ec-a509-4774-b872-e55cb2cfd60b]]'.
```

What is the reason for the error message?

A. The attribute name is not set correctly in JIT settings.

B. The user does not exist.

C. The user entered an incorrect password

D. The role is not assigned for the user.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 87

Topic #: 1

[All PCCSE Questions]

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

A. container name

B. image name

C. hostname

D. image labels

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 88

Topic #: 1

[All PCCSE Questions]

Which policy type in Prisma Cloud can protect against malware?

A. Data

B. Config

C. Network

D. Event

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 89

Topic #: 1

[All PCCSE Questions]

If you are required to run in an air-gapped environment, which product should you install?

A. Prisma Cloud Jenkins Plugin

B. Prisma Cloud Compute Edition

C. Prisma Cloud with self-hosted plugin

D. Prisma Cloud Enterprise Edition

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 90

Topic #: 1

[All PCCSE Questions]

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

A. 1

B. 2

C. 3

D. 4

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 91

Topic #: 1

[All PCCSE Questions]

DRAG DROP

-

Put the steps involved to configure and scan using the IntelliJ plugin in the correct order.

	Answer Area
Scan using the Prisma Cloud plugin	
Add Prisma Cloud plugin	
Install IntelliJ IDE	
Configure the Prisma Cloud plugin	

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 92

Topic #: 1

[All PCCSE Questions]

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

Which policy type should be used?

A. config-run

B. config-build

C. network

D. audit event

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 93

Topic #: 1

[All PCCSE Questions]

One of the resources on the network has triggered an alert for a Default Config policy.

Given the following resource JSON snippet:

```
{
    "password_enabled": "false",
    "password_last_used": "N/A",
    "user_creation_time": "2021-02-09T06:56:33Z",
    "access_key_1_active": true,
    "access_key_2_active": false,
    "cert_1_last_rotated": "N/A",
    "cert_2_last_rotated": "N/A",
    "password_last_changed": "N/A",
    "password_next_rotation": "N/A",
    "access_key_1_last_rotated": "2021-02-09T06:57:20Z",
}
```

Which RQL detected the vulnerability?

A. `config from cloud.resource where api.name = 'aws-ecs-service' AND json.rule = launchType equals EC2 as X; config from cloud.resource where api.name = 'aws-ecs-cluster' AND json.rule = status equals ACTIVE and registeredContainerInstancesCount equals 0 as Y; filter '$.X.ckusterArn equals $.Y.clusterArn'; show Y;`

B. `config from cloud.resource where cloud.type = 'aws' and api.name = 'aws-iam-get-credential-report' AND json.rule = '(access_key_1_active is true and access_key_1_last_rotated != N/A and _DateTime.ageInDays(access_key_1_last_rotated) > 90) or (access_key_2_active is true and access_key_2_last_rotated != N/A and _DateTime.ageInDays(access_key_2_last_rotated) > 90)'`

C. `config from cloud.resource where cloud.type = 'aws' AND api.name ='aws-ec2-describe-images' AND json.rule = image.platform contains windows and image.imageId contains ami-1e542176`

D. `config from cloud.resource where cloud.type = 'aws' AND api.name= 'aws-ec2-describe-security-groups' AND json.rule = isShared is false and (ipPermissions[?any((ipProtocol equals tcp or ipProtocol equals icmp or ipProtocol equals icmpv6 or ipProtocol equals udp) and (ipRanges[*] contains 0.0.0.0/0 or ipv6Ranges[*].cidrIpv6 contains ::/0))] exists)`

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 94

Topic #: 1

[All PCCSE Questions]

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. Vulnerabilities

C. Radar

D. Compliance

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 95

Topic #: 1

[All PCCSE Questions]

A customer has serverless functions that are deployed in multiple clouds.

Which serverless cloud provider is covered be “overly permissive service access” compliance check?

A. Alibaba

B. GCP

C. AWS

D. Azure

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 96

Topic #: 1

[All PCCSE Questions]

A customer has a requirement to restrict any container from resolving the name www.evil-url.com.

How should the administrator configure Prisma Cloud Compute to satisfy this requirement?

A. Choose “copy into rule” for any Container, set www.evil-url.com as a blocklisted DNS name in the Container policy and set the policy effect to alert.

B. Set www.evil-url.com as a blocklisted DNS name in the default Container runtime policy, and set the effect to block.

C. Choose “copy into rule” for any Container, set www.evil-url.com as a blocklisted DNS name, and set the effect to prevent.

D. Set www.evil-url.com as a blocklisted DNS name in the default Container policy and set the effect to prevent.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 97

Topic #: 1

[All PCCSE Questions]

Which API calls can scan an image named myimage: latest with twistcli and then retrieve the results from Console?

A. $ twistcli images scan \
--address \
--user \
--password \
--verbose \
myimage: latest

B. $ twistcli images scan \
--address \
--user \
--password \
--details \
myimage: latest

C. $ twistcli images scan \
--address \
--user \
--password \
myimage: latest

D. $ twistcli images scan \
--address \
--user \
--password \
--console \
myimage: latest

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 98

Topic #: 1

[All PCCSE Questions]

Given the following RQL:

event from cloud.audit_logs where operation IN ('CreateCryptoKey', 'DestroyCryptoKeyVersion', 'v1.compute.disks.createSnapshot')

Which audit event snippet is identified?

A.
```
"request": { "resource": "604173093072", "@type":
"type.googleapis.com/google.iam.v1.SetIamPolicyRequest", "policy": { "bindings": [
```

B.
```
], "stateTransitionReason": "", "elasticGpuAssociations": [], "capacityReservationSpecification": {
 "capacityReservationPreference": "open" }, "elasticInferenceAcceleratorAssociations": []
```

C.
```
{ "Statement": [ { "Action": "*", "Effect": "Allow", "Resource": "*"
 } ], "Version": "2012-10-17"
```

D.
```
"payload": { "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0
(+https://www.terraform.io) Terrafom-Plugin-SDK/2.1.0 terraform-provider-google/3.50.0,gzip(gfe)",
 "callerIp": "34.265.226.252" }, "request": { "@type":
"type.googleapis.com/compute.disks.createSnapshot" },
```

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 99

Topic #: 1

[All PCCSE Questions]

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

A. Username

B. SSO Certificate

C. Assertion Consumer Service (ACS) URL

D. SP (Service Provider) Entity ID

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 100

Topic #: 1

[All PCCSE Questions]

An administrator sees that a runtime audit has been generated for a container.

The audit message is:

"/bin/ls launched and is explicitly blocked in the runtime rule. Full command: ls -latr"

Which protection in the runtime rule would cause this audit?

A. Networking

B. File systems

C. Processes

D. Container

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 101

Topic #: 1

[All PCCSE Questions]

Which data security default policy is able to scan for vulnerabilities?

A. Objects containing Vulnerabilities

B. Objects containing Threats

C. Objects containing Malware

D. Objects containing Exploits

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 102

Topic #: 1

[All PCCSE Questions]

Given the following audit event activity snippet:

```
{
   "payload": {
       "requestMetadata": {
           "callerSuppliedUserAgent": "google-loud-sdk gcloud/274.0.1 command/gloud.compute.firewall-rules.delete invocation-
id/edda7aa325264545a4322f516ec15791 environment/None environment-version/None interactive/False from-script/False python/2.7.15
term/ (Linux 4.14.186-146.268.amzn2.x86_64),gzip(gfe)",
           "callerIp": "52.87.62.40"
       },
       "request": {
           "@type": "type.googleapis.com/compute.firewalls.delete
} }
```

Which RQL will be triggered by the audit event?

A. `event from cloud.audit_logs where operation IN ('cloudsql.instances.update','cloudsql.sslCerts.create','cloudsql.instances.create','caloudsql.instances.delete')`

B. `event from cloud.audit_logs where operation IN ('storage.buckets.create', 'storage.setIamPermissions','storage.buckets.delete')`

C. `event from cloud.audit_logs where operation IN ('AuthorizeSecurityGroupEgress', 'AuthorizeSecurityGroupIngress', 'CreateVpc', 'DeleteFlowLogs', 'DeleteVpc', 'ModifyVpcAttribute', 'RevokeSecurityGroupIngress')`

D. `event from cloud.audit_logs where operation IN ('v1.compute.networks.delete','beta.compute.networks.insert','v1.compute.routes.delete','v1.compute.firewalls.insert','v1.compute.firewalls.delete')`

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 103

Topic #: 1

[All PCCSE Questions]

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. Tags

D. Access Key

E. Asset Name

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 104

Topic #: 1

[All PCCSE Questions]

Which of the following are correct statements regarding the use of access keys? (Choose two.)

A. Access keys must have an expiration date

B. Up to two access keys can be active at any time

C. System Admin can create access key for all users

D. Access keys are used for API calls

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 105

Topic #: 1

[All PCCSE Questions]

Given the following RQL:

```
event from cloud.audit_logs where operation IN ('v1.compute.urlMaps.update', 'v1.compute.urlMaps.delete',
'v1.compute.backendServices.delete', 'v1.compute.backendBuckets.delete', 'v1.compute.backendServices.update',
'v1.compute.globalForwardingRules.delete', 'v1.compute.urlMaps.delete', 'v1.compute.targetHttpsProxies.delete',
'v1.compute.targetHttpsProxies.setSslPolicy', ''v1.compute.targetHttpsProxies.setSslCertificates')
```

Which audit event snippet is identified by the RQL?

A.
```
"eventTime": "2021-05-19T14:34:08Z", "eventSource": "iam.amazonaws.com", "eventName": "AttachRolePolicy",
"awsRegion": "us-east-1"
```

B.
```
"payload": { > "requestMetadata": { "callerSuppliedUserAgent": "Terraform/0.14.0
(+https://www.terraform.io) Terraform-Plugin-SDK/2.1.0 terraform-provider-
google/3.50.0,gzip(gfe)", "callerIp": "34.235.226.252" }, "request": { "@type":
"type.googleapis.com/compute.backendServices.delete"
```

C.
```
"resource": "projects/_/buckets/gvtest110221", "permission": "storage.buckets.setIamPolicy",
 "resourceAttributes": {}, "granted": true
```

D.
```
"userIdentity": { "type": "Root", "principalId": "6849955112A19", "arn":
"arn:aws:iam::6849955112A9:root", "accountId": "689995514A219", "accessKeyId": ""
```

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 106

Topic #: 1

[All PCCSE Questions]

The development team is building pods to host a web front end, and they want to protect these pods with an application firewall.

Which type of policy should be created to protect this pod from Layer7 attacks?

A. The development team should create a WAAS rule for the host where these pods will be running.

B. The development team should create a WAAS rule targeted at all resources on the host.

C. The development team should create a runtime policy with networking protections.

D. The development team should create a WAAS rule targeted at the image name of the pods.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 107

Topic #: 1

[All PCCSE Questions]

A manager informs the SOC that one or more RDS instances have been compromised and the SOC needs to make sure production RDS instances are NOT publicly accessible.

Which action should the SOC take to follow security best practices?

A. Enable "AWS S3 bucket is publicly accessible" policy and manually remediate each alert.

B. Enable "AWS RDS database instance is publicly accessible" policy and for each alert, check that it is a production instance, and then manually remediate.

C. Enable "AWS S3 bucket is publicly accessible" policy and add policy to an auto-remediation alert rule.

D. Enable "AWS RDS database instance is publicly accessible" policy and add policy to an auto-remediation alert rule.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 108

Topic #: 1

[All PCCSE Questions]

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 an average rate of 5 and file extensions match on .tar.gz on WAAS

B. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar.gz on CNNF

C. A ban for DoS protection with a burst rate of 5 and file extensions match on .tar gz on WAAS

D. A ban for DoS protection with an average rate of 5 and file extensions match on .tar.gz on CNNF

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 109

Topic #: 1

[All PCCSE Questions]

What is an automatically correlated set of individual events generated by the firewall and runtime sensors to identify unfolding attacks?

A. policy

B. incident

C. audit

D. anomaly

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 110

Topic #: 1

[All PCCSE Questions]

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. Subscription ID

C. Active Directory ID

D. External ID

E. Role ARN

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 111

Topic #: 1

[All PCCSE Questions]

An administrator for Prisma Cloud needs to obtain a graphical view to monitor all connections, including connections across hosts and connections to any configured network objects.

Which setting does the administrator enable or configure to accomplish this task?

A. ADEM

B. WAAS Analytics

C. Telemetry

D. Cloud Native Network Firewall

E. Host Insight

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 112

Topic #: 1

[All PCCSE Questions]

Which two fields are required to configure SSO in Prisma Cloud? (Choose two.)

A. Prisma Cloud Access SAML URL

B. Identity Provider Issuer

C. Certificate

D. Identity Provider Logout URL

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 113

Topic #: 1

[All PCCSE Questions]

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

A. BitBucket

B. Visual Studio Code

C. CircleCI

D. IntelliJ

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 114

Topic #: 1

[All PCCSE Questions]

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

A. BitBucket

B. Visual Studio Code

C. CircleCI

D. IntelliJ

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 115

Topic #: 1

[All PCCSE Questions]

Given the following JSON query:

$.resource[*].aws_s3_bucket exists

Which tab is the correct place to add the JSON query when creating a Config policy?

A. Details

B. Compliance Standards

C. Remediation

D. Build Your Rule (Run tab)

E. Build Your Rule (Build tab)

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 116

Topic #: 1

[All PCCSE Questions]

Which two attributes of policies can be fetched using API? (Choose two.)

A. policy label

B. policy signature

C. policy mode

D. policy violation

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 117

Topic #: 1

[All PCCSE Questions]

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

A. Run the provided curl | bash script from Console to remove Defenders, and then use Cloud Discovery to automatically redeploy Defenders.

B. Remove Defenders DaemonSet, and then use Cloud Discovery to automatically redeploy the Defenders.

C. Remove Defenders, and then deploy the new DaemonSet so Defenders do not have to automatically update on each deployment.

D. Let Defenders automatically upgrade.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 118

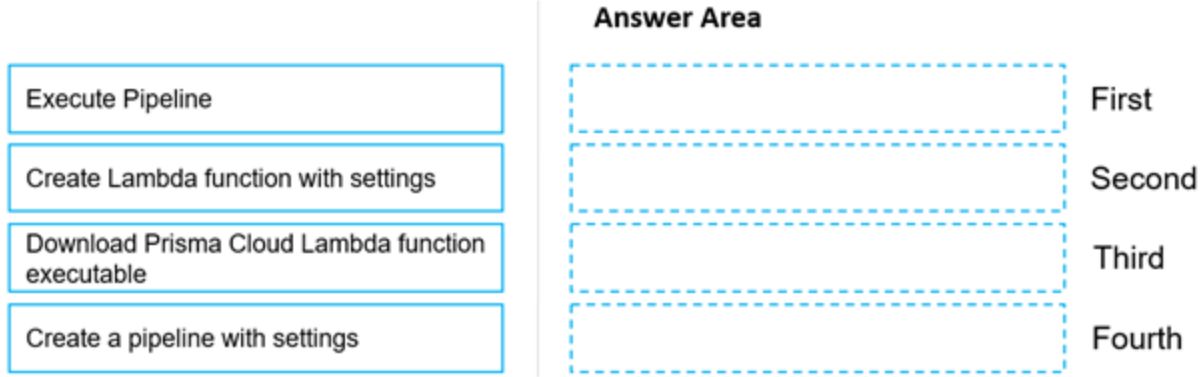
Topic #: 1

[All PCCSE Questions]

DRAG DROP

-

Move the steps to the correct order to set up and execute a serverless scan using AWS DevOps.



Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 119

Topic #: 1

[All PCCSE Questions]

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

What is the correct option to configure scanning?

A. Configure serverless radar from the Defend > Compliance > Cloud Platforms page.

B. Embed serverless Defender into the function.

C. Configure a function scan policy from the Defend > Vulnerabilities > Functions page.

D. Use Lambda layers to deploy a Defender into the function.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 120

Topic #: 1

[All PCCSE Questions]

An administrator has been tasked with a requirement by your DevSecOps team to write a script to continuously query programmatically the existing users, and the user's associated permission levels, in a Prisma Cloud Enterprise tenant.

Which public documentation location should be reviewed to help determine the required attributes to carry out this step?

A. Prisma Cloud Administrator's Guide (Compute)

B. Prisma Cloud API Reference

C. Prisma Cloud Compute API Reference

D. Prisma Cloud Enterprise Administrator's Guide

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 121

Topic #: 1

[All PCCSE Questions]

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 and when a Container is started form an Image

D. when the Image is built

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 122

Topic #: 1

[All PCCSE Questions]

Which two required request headers interface with Prisma Cloud API? (Choose two.)

A. Content-type:application/json

B. x-redlock-auth

C. >x-redlock-request-id

D. Content-type:application/xml

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 123

Topic #: 1

[All PCCSE Questions]

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 API settings for logging.

B. Enable the CSV export in the Console.

C. Enable the syslog option in the Console

D. Enable the Splunk option in the Console.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 124

Topic #: 1

[All PCCSE Questions]

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. The host will be taken offline.

B. Additional hosts will be prevented form starting.

C. Containers on a host will be stopped.

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

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 125

Topic #: 1

[All PCCSE Questions]

During an initial deployment of Prisma Cloud Compute, the customer sees vulnerabilities in their environment.

Which statement correctly describes the default vulnerability policy?

A. It blocks all containers that contain a vulnerability.

B. It alerts on any container with more than three critical vulnerabilities.

C. It blocks containers after 30 days if they contain a critical vulnerability.

D. It alerts on all vulnerabilities, regardless of severity.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 126

Topic #: 1

[All PCCSE Questions]

Console is running in a Kubernetes cluster, and you need to deploy Defenders on nodes within this cluster.

Which option shows the steps to deploy the Defenders in Kubernetes using the default Console service name?

A. From the deployment page in Console, choose pod name for Console identifier, generate DaemonSet file, and apply the DaemonSet to twistlock namespace.

B. From the deployment page configure the cloud credential in Console and allow cloud discovery to auto-protect the Kubernetes nodes.

C. From the deployment page in Console, choose twistlock-console for Console identifier, generate DaemonSet file, and apply DaemonSet to the twistlock namespace.

D. From the deployment page in Console, choose twistlock-console for Console identifier, and run the curl | bash script on the master Kubernetes node.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 127

Topic #: 1

[All PCCSE Questions]

Which RQL query type is invalid?

A. Event

B. IAM

C. Incident

D. Config

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 128

Topic #: 1

[All PCCSE Questions]

On which cloud service providers can you receive new API release information for Prisma Cloud?

A. AWS, Azure, GCP, Oracle, IBM

B. AWS, Azure, GCP, Oracle, Alibaba

C. AWS, Azure, GCP, IBM

D. AWS, Azure, GCP, IBM, Alibaba

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 129

Topic #: 1

[All PCCSE Questions]

Web-Application and API Security (WAAS) provides protection for which two protocols? (Choose two.)

A. HTTP

B. SSH

C. Tomcat Web Connector via AJP

D. TLS

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 130

Topic #: 1

[All PCCSE Questions]

What is the most reliable and extensive source for documentation on Prisma Cloud APIs?

A. prisma.pan.dev

B. docs.paloaltonetworks.com

C. Prisma Cloud Administrator's Guide

D. Live Community

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 131

Topic #: 1

[All PCCSE Questions]

How often do Defenders share logs with Console?

A. Every 10 minutes

B. Every 30 minutes

C. Every 1 hour

D. Real time

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 132

Topic #: 1

[All PCCSE Questions]

In Prisma Cloud Software Release 22.06 (Kepler), which Registry type is added?

A. Azure Container Registry

B. Google Artifact Registry

C. IBM Cloud Container Registry

D. Sonatype Nexus

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 133

Topic #: 1

[All PCCSE Questions]

Which three actions are required in order to use the automated method within Azure Cloud to streamline the process of using remediation in the identity and access management (IAM) module? (Choose three.)

A. Install boto3 & requests library.

B. Configure IAM Azure remediation script.

C. Integrate with Azure Service Bus.

D. Configure IAM AWS remediation script.

E. Install azure.servicebus & requests library.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 134

Topic #: 1

[All PCCSE Questions]

Which two roles have access to view the Prisma Cloud policies? (Choose two.)

A. Build AND Deploy Security

B. Auditor

C. Dev SecOps

D. Defender Manager

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 135

Topic #: 1

[All PCCSE Questions]

Which three elements are part of SSH Events in Host Observations? (Choose three.)

A. Startup process

B. User

C. System calls

D. Process path

E. Command

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 136

Topic #: 1

[All PCCSE Questions]

Which two variables must be modified to achieve automatic remediation for identity and access management (IAM) alerts in Azure cloud? (Choose two.)

A. API_ENDPOINT

B. SQS_QUEUE_NAME

C. SB_QUEUE_KEY

D. YOUR_ACCOUNT_NUMBER

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 137

Topic #: 1

[All PCCSE Questions]

An administrator has added a Cloud account on Prisma Cloud and then deleted it.

What will happen if the deleted account is added back on Prisma Cloud within a 24-hour period?

A. No alerts will be displayed.

B. Existing alerts will be displayed again.

C. New alerts will be generated.

D. Existing alerts will be marked as resolved.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 138

Topic #: 1

[All PCCSE Questions]

In which two ways can Prisma Cloud images be retrieved in Prisma Cloud Compute Self-Hosted Edition? (Choose two.)

A. Pull the images from the Prisma Cloud registry without any authentication.

B. Authenticate with Prisma Cloud registry, and then pull the images from the Prisma Cloud registry.

C. Retrieve Prisma Cloud images using URL auth by embedding an access token.

D. Download Prisma Cloud images from github.paloaltonetworks.com.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 139

Topic #: 1

[All PCCSE Questions]

Which action would be applicable after enabling anomalous compute provisioning?

A. It detects the activity caused by the spambot.

B. It detects unusual server port activity or unusual protocol activity from a client within or outside the cloud environment.

C. It detects potential creation of an unauthorized network of compute instances with AutoFocus.

D. It detects potential creation of an unauthorized network of compute instances either accidentally or for cryptojacking.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 140

Topic #: 1

[All PCCSE Questions]

What is the function of the external ID when onboarding a new Amazon Web Services (AWS) account in Prisma Cloud?

A. It is a unique identifier needed only when Monitor & Protect mode is selected.

B. It is the resource name for the Prisma Cloud Role.

C. It is a UUID that establishes a trust relationship between the Prisma Cloud account and the AWS account in order to extract data.

D. It is the default name of the PrismaCloudApp stack.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 141

Topic #: 1

[All PCCSE Questions]

Which IAM Azure RQL query would correctly generate an output to view users who have sufficient permissions to create security groups within Azure AD and create applications?

A. config where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions.allowedToCreateSecurityGroups is true and defaultUserRolePermissions.allowedToCreateApps is true

B. config from cloud.resource where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions exists

C. config from network where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions.allowedToCreateSecurityGroups is false and defaultUserRolePermissions.allowedToCreateApps is true

D. config from cloud.resource where api.name = 'azure-active-directory-authorization-policy' AND json.rule = defaultUserRolePermissions.allowedToCreateSecurityGroups is true and defaultUserRolePermissions.allowedToCreateApps is true

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 142

Topic #: 1

[All PCCSE Questions]

Which two bot types are part of Web Application and API Security (WAAS) bot protection? (Choose two.)

A. Chat bots

B. User-defined bots

C. Unknown bots

D. Customer bots

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 143

Topic #: 1

[All PCCSE Questions]

Which two actions are required in order to use the automated method within Amazon Web Services (AWS) Cloud to streamline the process of using remediation in the identity and access management (IAM) module? (Choose two.)

A. Install boto3 & requests library.

B. Configure IAM Azure remediation script.

C. Integrate with Azure Service Bus.

D. Configure IAM AWS remediation script.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 144

Topic #: 1

[All PCCSE Questions]

Which three public cloud providers are supported for VM image scanning? (Choose three.)

A. GCP

B. Alibaba

C. Oracle

D. AWS

E. Azure

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 145

Topic #: 1

[All PCCSE Questions]

Where can Defender debug logs be viewed? (Choose two.)

A. /var/lib/twistlock/defender.log

B. From the Console, Manage > Defenders > Manage > Defenders. Select the Defender from the deployed Defenders list, then click Actions > Logs

C. From the Console, Manage > Defenders > Deploy > Defenders. Select the Defender from the deployed Defenders list, then click Actions > Logs

D. /var/lib/twistlock/log/defender.log

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 146

Topic #: 1

[All PCCSE Questions]

How many CLI remediation commands can be added in a custom policy sequence?

A. 2

B. 1

C. 4

D. 5

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 147

Topic #: 1

[All PCCSE Questions]

An administrator wants to retrieve the compliance policies for images scanned in a continuous integration (CI) pipeline.

Which endpoint will successfully execute to enable access to the images via API?

A. GET /api/v22.01/policies/compliance

B. GET /api/v22.01/policies/compliance/ci

C. GET /api/v22.01/policies/compliance/ci/images

D. GET /api/v22.01/policies/compliance/ci/serverless

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 148

Topic #: 1

[All PCCSE Questions]

The attempted bytes count displays?

A. traffic that is either denied by the security group or firewall rules or traffic that was reset by a host or virtual machine that received the packet and responded with a RST packet.

B. traffic that is either denied by the security group or firewall rules.

C. traffic that is either denied by the firewall rules or traffic that was reset by a host or virtual machine that received the packet and responded with a RST packet.

D. traffic denied by the security group or traffic that was reset by a host or virtual machine that received the packet and responded with a RST packet.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 149

Topic #: 1

[All PCCSE Questions]

Anomaly policy uses which two logs to identify unusual network and user activity? (Choose two.)

A. Network flow

B. Audit

C. Traffic

D. Users

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 150

Topic #: 1

[All PCCSE Questions]

What are two alarm types that are registered after alarms are enabled? (Choose two.)

A. Onboarded Cloud Accounts status

B. Resource status

C. Compute resources

D. External integrations status

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 151

Topic #: 1

[All PCCSE Questions]

What is the correct method for ensuring key-sensitive data related to SSNs and credit card numbers cannot be viewed in Dashboard > Data view during investigations?

A. Go to Settings > Data > Snippet Masking and select Full Mask.

B. Go to Settings > Data > Data Patterns, search for SSN Pattern, edit it, and modify the proximity keywords.

C. Go to Settings > Cloud Accounts > Edit Cloud Account > Assign Account Group and select a group with limited permissions.

D. Go to Policies > Data > Clone > Modify Objects containing Financial Information publicly exposed and change the file exposure to Private.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 152

Topic #: 1

[All PCCSE Questions]

Which two integrations enable ingesting host findings to generate alerts? (Choose two.)

A. Splunk

B. Tenable

C. JIRA

D. Qualys

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 153

Topic #: 1

[All PCCSE Questions]

Which data storage type is supported by Prisma Cloud Data Security?

A. IBM Cloud Object Storage

B. AWS S3 buckets

C. Oracle Object Storage

D. Google storage class

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 154

Topic #: 1

[All PCCSE Questions]

Which action must be taken to enable a user to interact programmatically with the Prisma Cloud APIs and for a nonhuman entity to be enabled for the access keys?

A. Create a role with System Admin and generate access keys.

B. Create a user with a role that has minimal access.

C. Create a role with Account Group Read Only and assign it to the user.

D. Create a role and assign it to the Service Account.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 155

Topic #: 1

[All PCCSE Questions]

Which three types of runtime rules can be created? (Choose three.)

A. Processes

B. Network-outgoing

C. Filesystem

D. Kubernetes-audit

E. Waas-request

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 156

Topic #: 1

[All PCCSE Questions]

Who can access saved searches in a cloud account?

A. Administrators

B. Users who can access the tenant

C. Creators

D. All users with whom the saved search has been shared

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 157

Topic #: 1

[All PCCSE Questions]

The Compute Console has recently been upgraded, and the administrator plans to delay upgrading the Defenders and the Twistcli tool until some of the team's resources have been rescaled. The Console is currently one major release ahead.

What will happen as a result of the Console upgrade?

A. Defenders will disconnect, and Twistcli will stop working.

B. Defenders will disconnect, and Twistcli will remain working.

C. Both Defenders and Twistcli will remain working.

D. Defenders will remain connected, and Twistcli will stop working.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 158

Topic #: 1

[All PCCSE Questions]

What are two key requirements for integrating Okta with Prisma Cloud when multiple Amazon Web Services (AWS) cloud accounts are being used? (Choose two.)

A. Super Administrator permissions

B. A valid subscription for the IAM security module

C. An Okta API token for the primary AWS account

D. Multiple instances of the Okta app

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 159

Topic #: 1

[All PCCSE Questions]

Which resource and policy type are used to calculate AWS Net Effective Permissions? (Choose two.)

A. Service Linked Roles

B. Lambda Function

C. Amazon Resource Names (ARNs) using Wild Cards

D. AWS Service Control Policies (SCPs)

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 160

Topic #: 1

[All PCCSE Questions]

When an alert notification from the alarm center is deleted, how many hours will a similar alarm be suppressed by default?

A. 12

B. 8

C. 24

D. 4

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 161

Topic #: 1

[All PCCSE Questions]

Which component of a Kubernetes setup can approve, modify, or reject administrative requests?

A. Kube Controller

B. Terraform Controller

C. Admission Controller

D. Control plane

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 162

Topic #: 1

[All PCCSE Questions]

Which three actions are available for the container image scanning compliance rule? (Choose three.)

A. Allow

B. Snooze

C. Block

D. Ignore

E. Alert

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 163

Topic #: 1

[All PCCSE Questions]

What will happen when a Prisma Cloud Administrator has configured agentless scanning in an environment that also has Host and Container Defenders deployed?

A. Agentless scan will automatically be disabled, so Defender scans are the only scans occurring.

B. Agentless scans do not conflict with Defender scans, so both will run.

C. Defender scans will automatically be disabled, so agentless scans are the only scans occurring.

D. Both agentless and Defender scans will be disabled and an error message will be received.

Show Suggested Answer

Actual exam question from Palo Alto Networks's PCCSE

Question #: 164

Topic #: 1

[All PCCSE Questions]

An administrator of Prisma Cloud wants to enable role-based access control for Docker engine.

Which configuration step is needed first to accomplish this task?

A. Configure Docker's authentication sequence to first use an identity provider and then Console.

B. Set Defender's listener type to TCP.

C. Set Docker's listener type to TCP.

D. Configure Defender's authentication sequence to first use an identity provider and then Console.

Show Suggested Answer