Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

NEW QUESTION 1
Which option shows the steps to install the Console in a Kubernetes Cluster?

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

Answer: B

NEW QUESTION 2
Which step is included when configuring Kubernetes to use Prisma Cloud Compute as an admission controller?

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

Answer: B

NEW QUESTION 3
A customer has a 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

Answer: BE

NEW QUESTION 4
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

Answer: B

NEW QUESTION 5
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

Answer: AB

NEW QUESTION 6
Which port should a security team use to pull data from Console's API?

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

Answer: D

NEW QUESTION 7
An administrator has deployed Console into a Kubernetes cluster running in AWS. The administrator also has configured a load balancer in TCP passthrough mode to listen on the same ports as the default Prisma Compute Console configuration.
In the build pipeline, the administrator wants twistcli to talk to Console over HTTPS. Which port will twistcli need to use to access the Prisma Compute APIs?

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

Answer: A

NEW QUESTION 8
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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing graphical user interface Description automatically generated

NEW QUESTION 9
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 “prevent”.
D. choose “copy into rule” for the Container, add a ransomWare process into the denied process list, and set the action to “block”.

Answer: C

NEW QUESTION 10
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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing graphical user interface Description automatically generated

NEW QUESTION 10
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

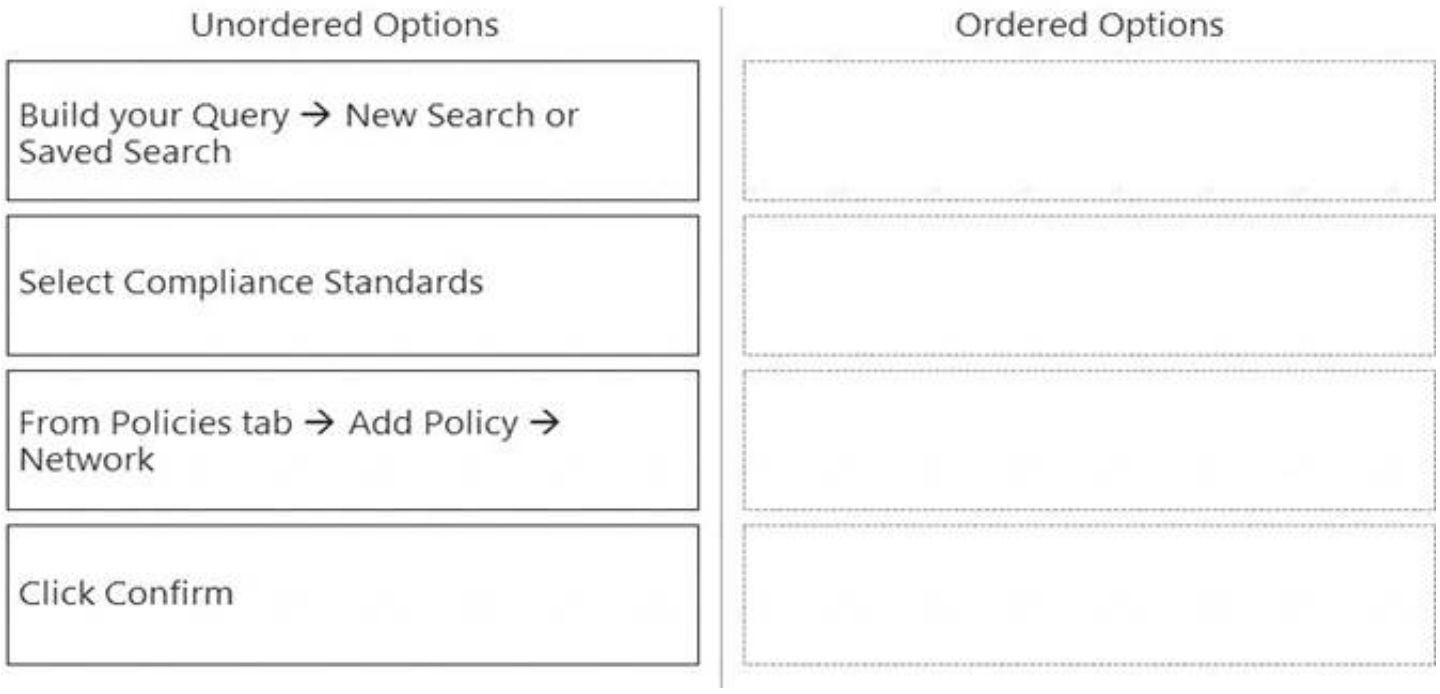
Answer: A

NEW QUESTION 13
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.

Answer: D

NEW QUESTION 15
What is the order of steps to create a custom network policy?
(Drag the steps into the correct order of occurrence, from the first step to the last.)
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing table Description automatically generated

NEW QUESTION 17
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.

Answer: BE

NEW QUESTION 21
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 “Clinical Trials” as the account group * 3.Under the “Select Policies” tab, filter on severity and select “High” * 4.Under the Set Alert Notification tab, choose Slack and populate the channel * 5.Set Frequency to “As it Happens”
B. * 1. Create an alert rule and select “Clinical Trials” as the account group * 2.Under the “Select Policies” tab, filter on severity and select “High” * 3.Under the Set Alert Notification tab, choose Slack and populate the channel * 4.Set Frequency to “As it Happens”* 5.Set up the Slack Integration to complete the configuration
C. * 1. Configure Slack Integration * 2.Create an alert rule* 3.Under the “Select Policies” tab, filter on severity and select “High” * 4.Under the Set Alert Notification tab, choose Slack and populate the channel* 5.Set Frequency to “As it Happens”
D. * 1. Under the “Select Policies” tab, filter on severity and select “High” * 2.Under the Set Alert Notification tab, choose Slack and populate the channel * 3.Set Frequency to “As it Happens”* 4.Configure Slack Integration * 5.Create an Alert rule

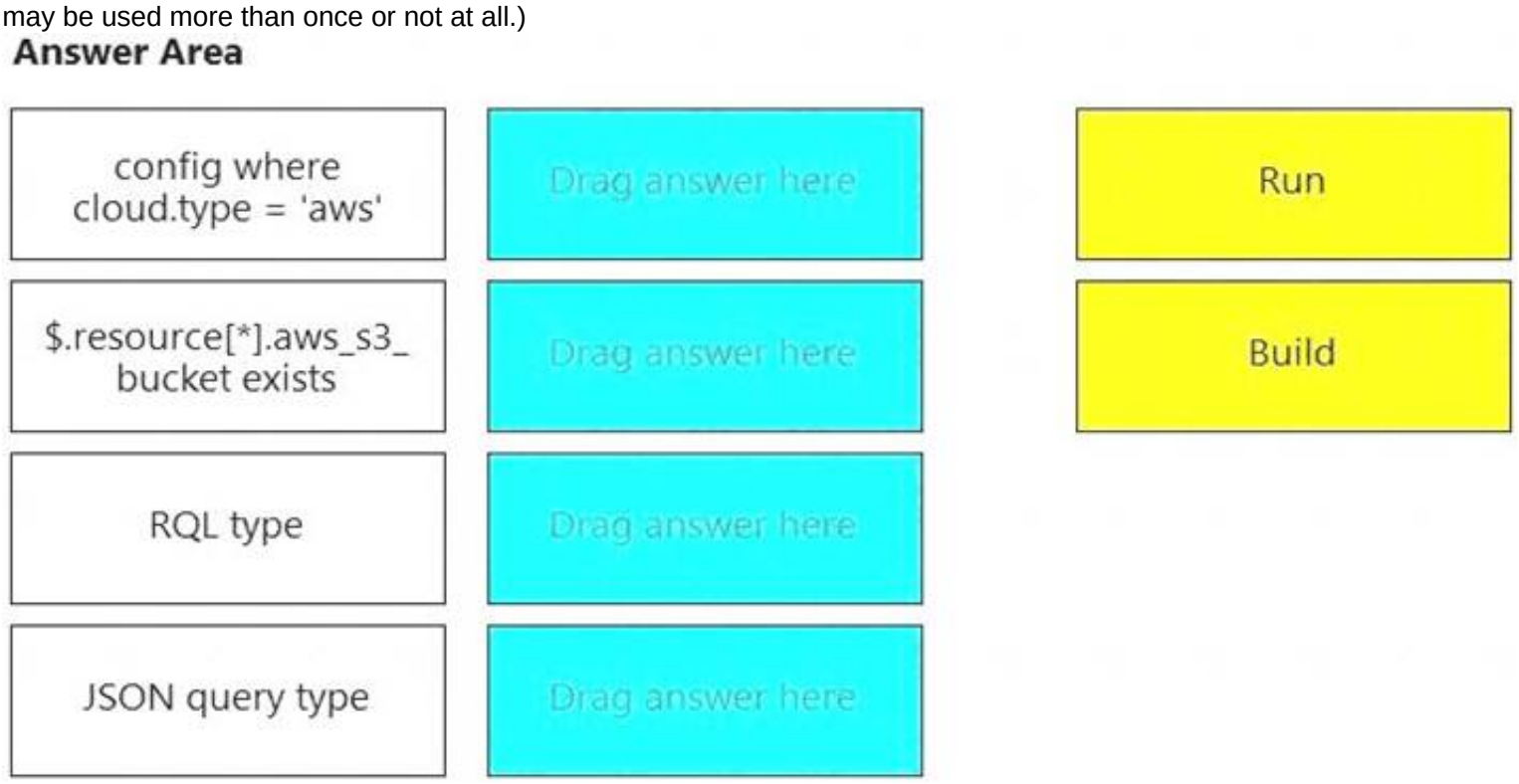
Answer: B

NEW QUESTION 23
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

Answer: B

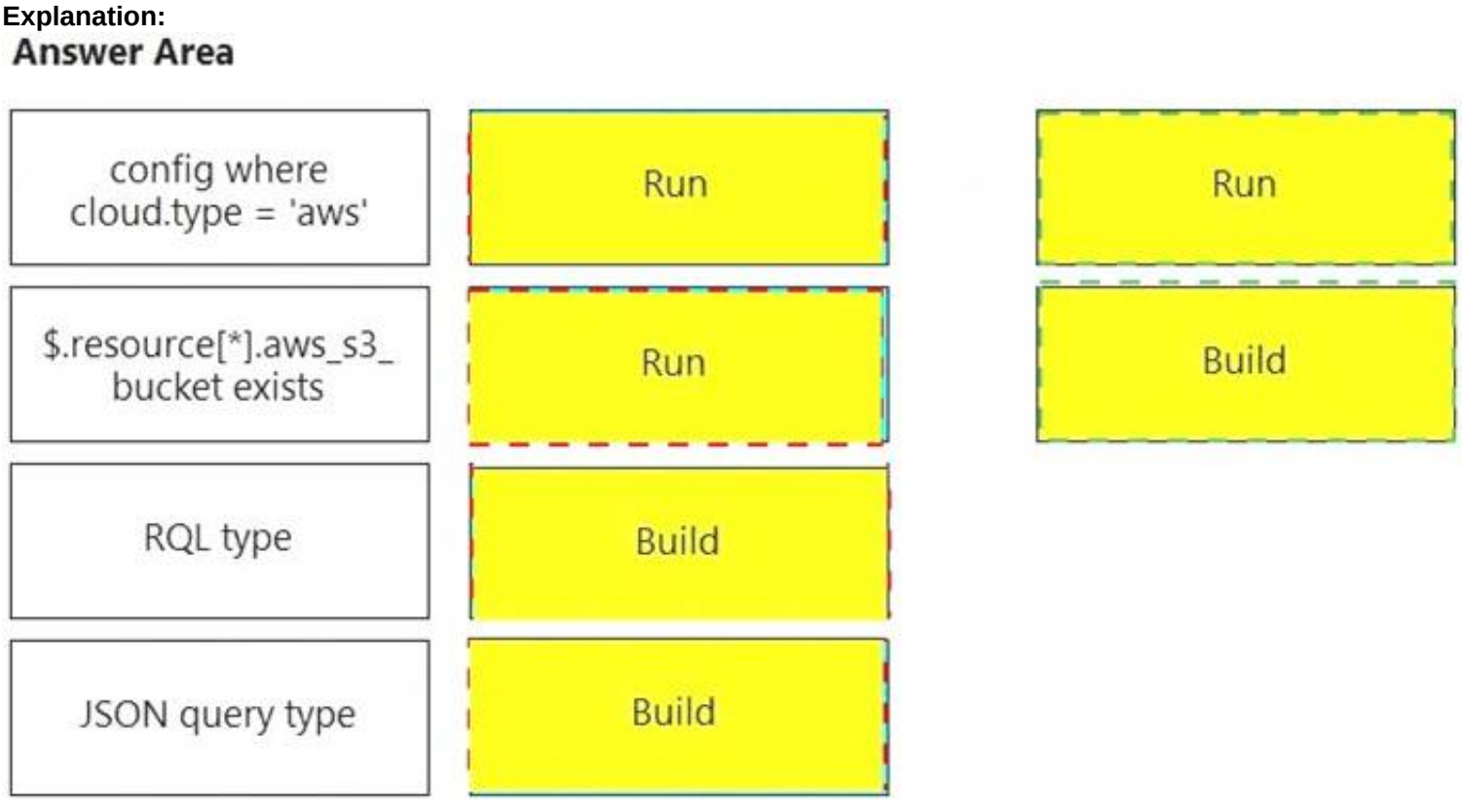
NEW QUESTION 24
You wish to create a custom policy with build and run subtypes. Match the query types for each example. (Select your answer from the pull-down list. Answers may be used more than once or not at all.)



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 28
The development team wants to fail CI jobs where a specific CVE is contained within the image. How should the development team configure the pipeline or policy to produce this outcome?

A. Set the specific CVE exception as an option in Jenkins or twistcli.

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

Answer: C

NEW QUESTION 33
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

Answer: B

NEW QUESTION 34
You are tasked with configuring a Prisma Cloud build policy for Terraform. What type of query is necessary to complete this policy?

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

Answer: B

NEW QUESTION 37
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

Answer: C

NEW QUESTION 42
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.

Answer: AC

NEW QUESTION 43
An administrator sees that a runtime audit has been generated for a Container. The audit message is "DNS resolution of suspicious name wikipedia.com. type A".
Why would this message appear as an audit?

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

Answer: A

NEW QUESTION 46
Which options show the steps required after upgrade of Console?

A. Uninstall Defenders Upgrade Jenkins Plugin Upgrade twistcli where applicableAllow 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

Answer: C

NEW QUESTION 51
An S3 bucket within AWS has generated an alert by violating the Prisma Cloud Default policy "AWS S3 buckets are accessible to public". The policy definition follows:
config where cloud.type = 'aws' AND api.name='aws-s3api-get-bucket-acl' AND json.rule="((((acl.grants[? (@.grantee=='AllUsers')] size > 0) or policyStatus.isPublic is true) and publicAccessBlockConfiguration does not exist) or ((acl.grants[?(@.grantee=='AllUsers')] size > 0) and publicAccessBlockConfiguration.ignorePublicAcis is false) or (policyStatus.isPublic is true and publicAccessBlockConfiguration.restrictPublicBuckets is false)) and

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

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

Answer: B

NEW QUESTION 53
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

Answer: C

NEW QUESTION 55
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

Answer: A

NEW QUESTION 57
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 ruleSelect “select all 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 ruleSelect 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 ruleSelect 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 ruleSelect “select all policies” checkbox as part of the alert rule Add alert notifications Confirm the alert rule

Answer: C

NEW QUESTION 59
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PCCSE Practice Exam Features:

* PCCSE Questions and Answers Updated Frequently

* PCCSE Practice Questions Verified by Expert Senior Certified Staff

* PCCSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCCSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year