Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

NEW QUESTION 1
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.

Answer: D

NEW QUESTION 2
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

Answer: C

NEW QUESTION 3
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 4
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.

Answer: A

NEW QUESTION 5
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.

Answer: C

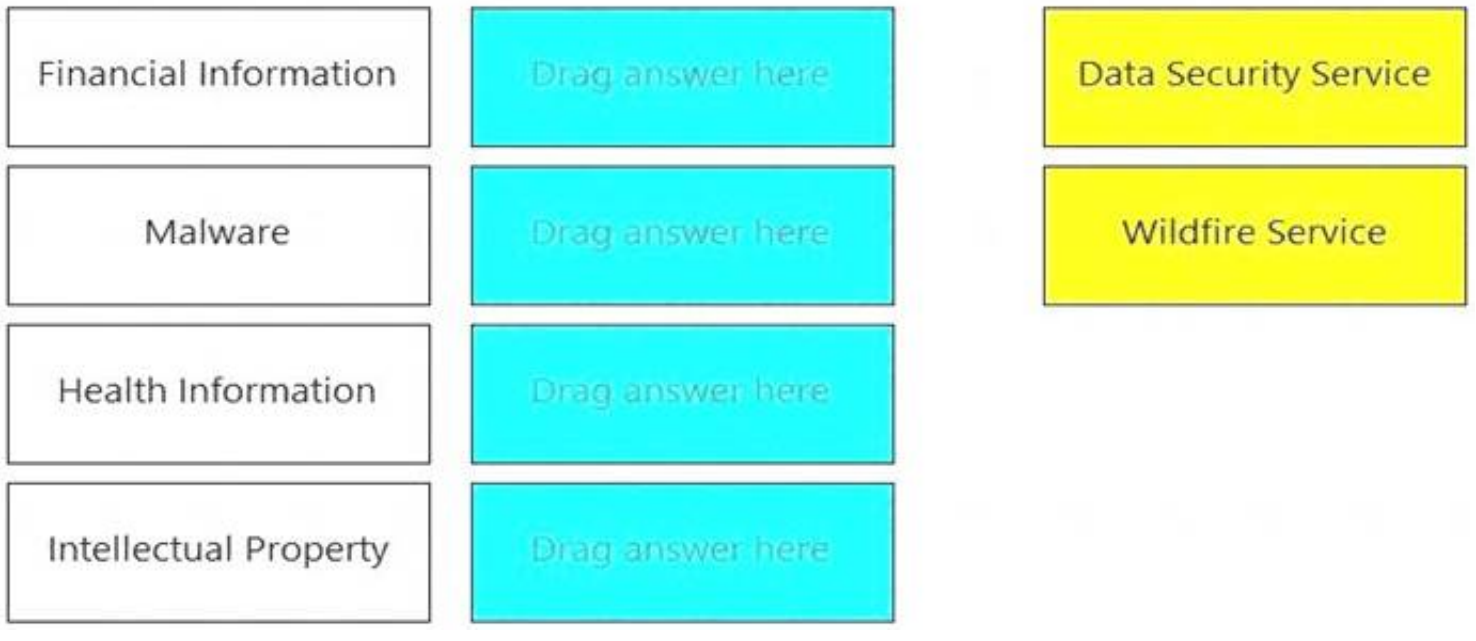
NEW QUESTION 6
Which method should be used to authenticate to Prisma Cloud Enterprise programmatically?

A. single sign-on
B. SAML
C. basic authentication
D. access key

Answer: D

NEW QUESTION 7
Match the service on the right that evaluates each exposure type on the left.
(Select your answer from the pull-down list. Answers may be used more than once or not at all.)

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 8
Which order of steps map a policy to a custom compliance standard?
(Drag the steps into the correct order of occurrence, from the first step to the last.)

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 9
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 10
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 10
Which statement accurately characterizes SSO Integration on Prisma Cloud?

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

Answer: A

NEW QUESTION 13
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 14
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 15
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.)

Answer Area

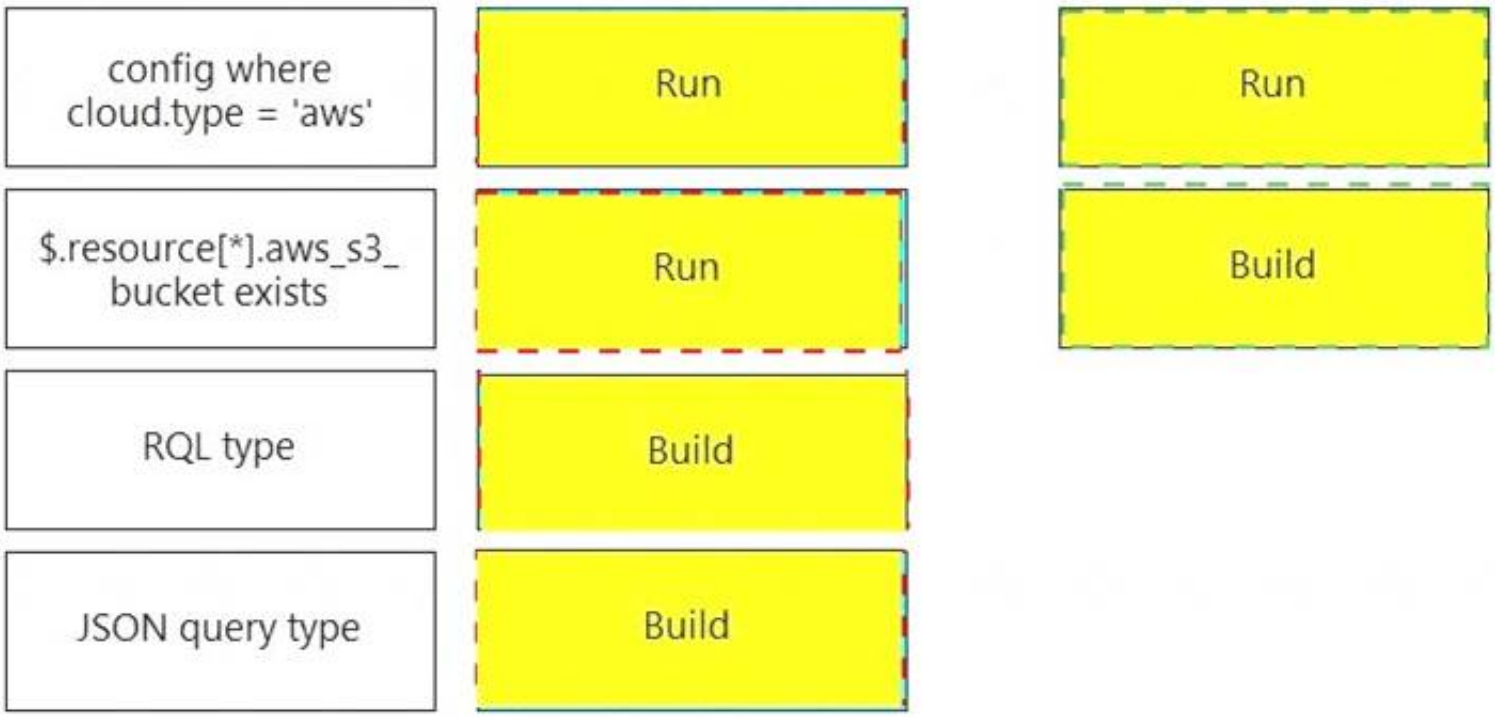
config where cloud.type = ‘aws’	Drag answer here	Run
$.resource[*].aws_s3_ bucket exists	Drag answer here	Build
RQL type	Drag answer here	
JSON query type	Drag answer here	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 19
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 21
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

Answer: D

NEW QUESTION 24
Which option identifies the Prisma Cloud Compute Edition?

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

Answer: B

NEW QUESTION 26
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>

Answer: D

NEW QUESTION 30
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

Answer: BCE

NEW QUESTION 33
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

Answer: D

NEW QUESTION 38
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 42
What is an example of an outbound notification within Prisma Cloud?

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

Answer: D

NEW QUESTION 44
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.

Answer: B

NEW QUESTION 48
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.

Answer: B

NEW QUESTION 53
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

Answer: D

NEW QUESTION 58
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

Answer: C

NEW QUESTION 59
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 64
.....

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