Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

NEW QUESTION 1
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

Answer: D

NEW QUESTION 2
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

Answer: BDE

NEW QUESTION 3
The security team wants to target a CNAF policy for specific running Containers. How should the administrator scope the policy to target the Containers?

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

Answer: B

NEW QUESTION 4
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 5
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 6
How are the following categorized?
Backdoor account access Hijacked processes Lateral movement Port scanning

A. audits
B. incidents
C. admission controllers
D. models

Answer: B

NEW QUESTION 7
A customer finds that an open alert from the previous day has been resolved. No auto-remediation was configured.
Which two reasons explain this change in alert status? (Choose two.)

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

Answer: CD

NEW QUESTION 8
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 9
Which port should a security team use to pull data from Console's API?

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

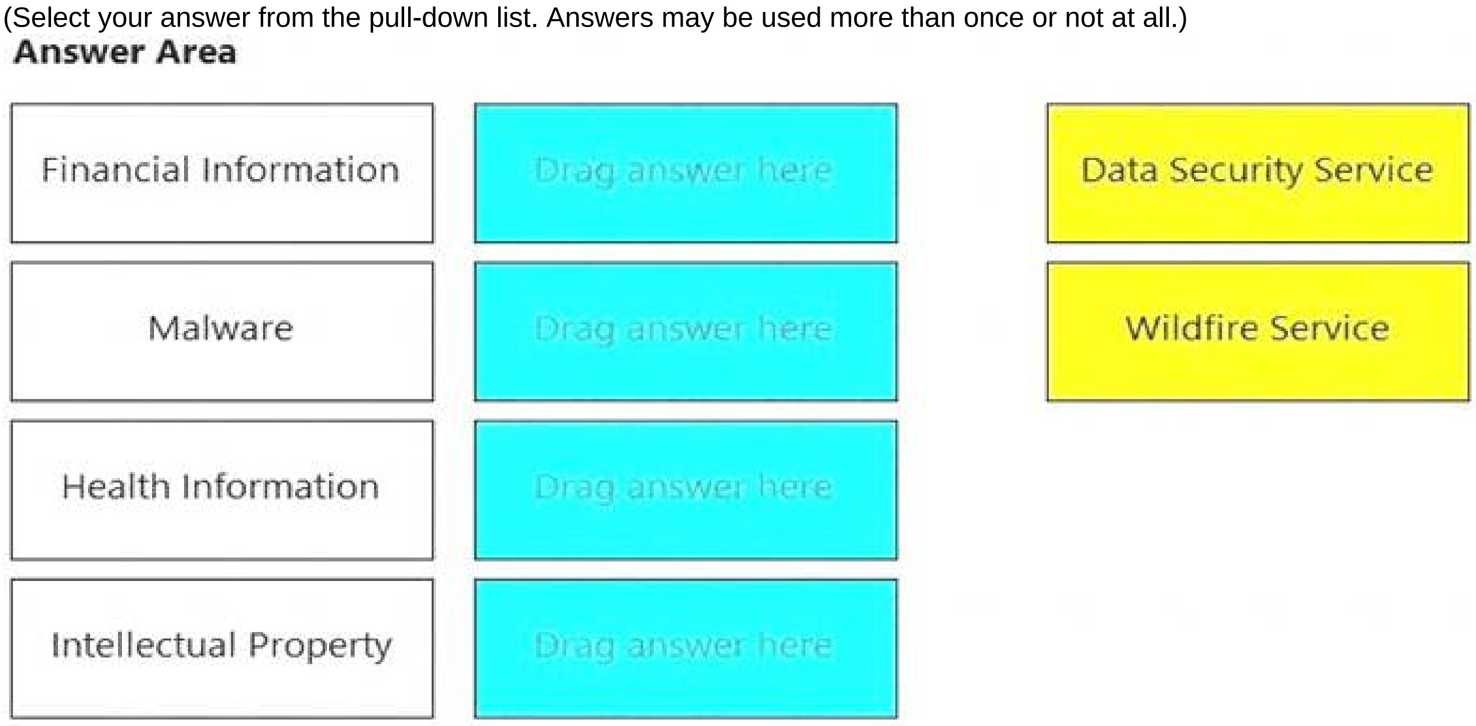
Answer: D

NEW QUESTION 10
Which statement is true about obtaining Console images for Prisma Cloud Compute Edition?

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

Answer: B

NEW QUESTION 10
Match the service on the right that evaluates each exposure type on the left.
(Select your answer from the pull-down list. Answers may be used more than once or not at all.)



Answer Area

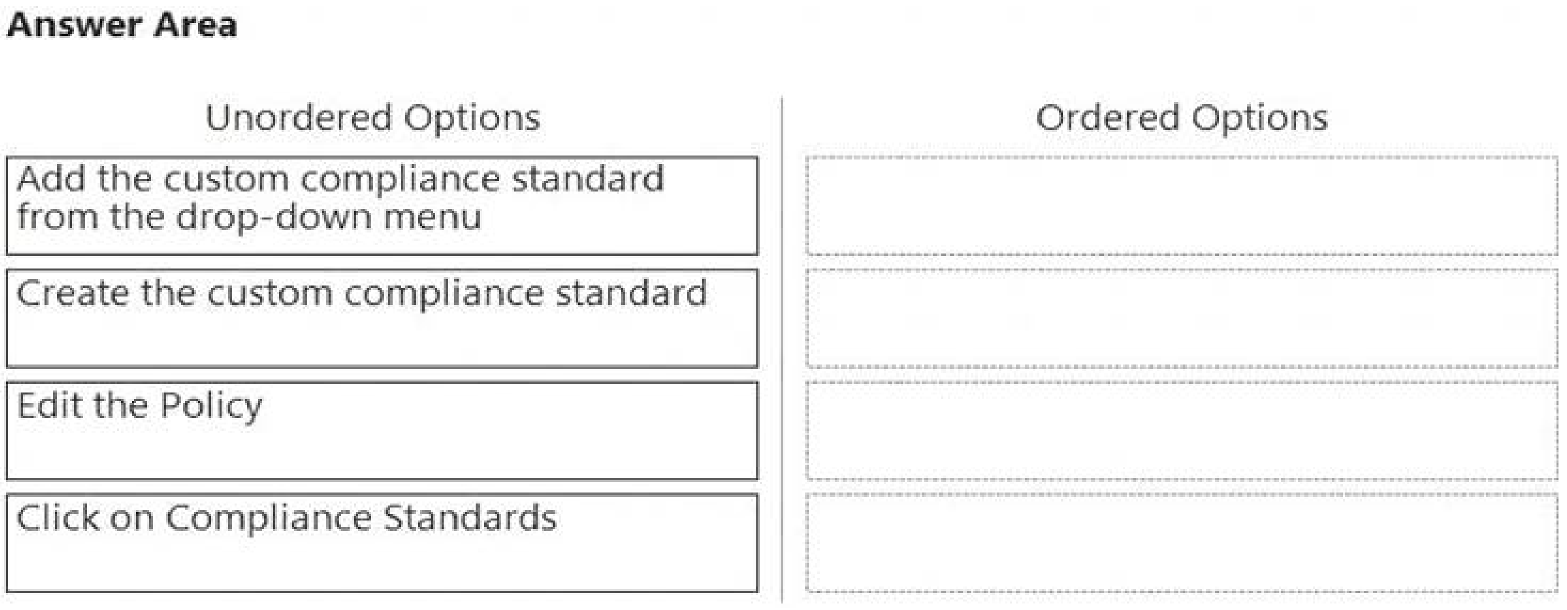
Financial Information	Drag answer here	Data Security Service
Malware	Drag answer here	Wildfire Service
Health Information	Drag answer here	
Intellectual Property	Drag answer here	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 15
Which order of steps map a policy to a custom compliance standard?
(Drag the steps into the correct order of occurrence, from the first step to the last.)



Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Diagram Description automatically generated

NEW QUESTION 18
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

Answer: B

NEW QUESTION 22
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.

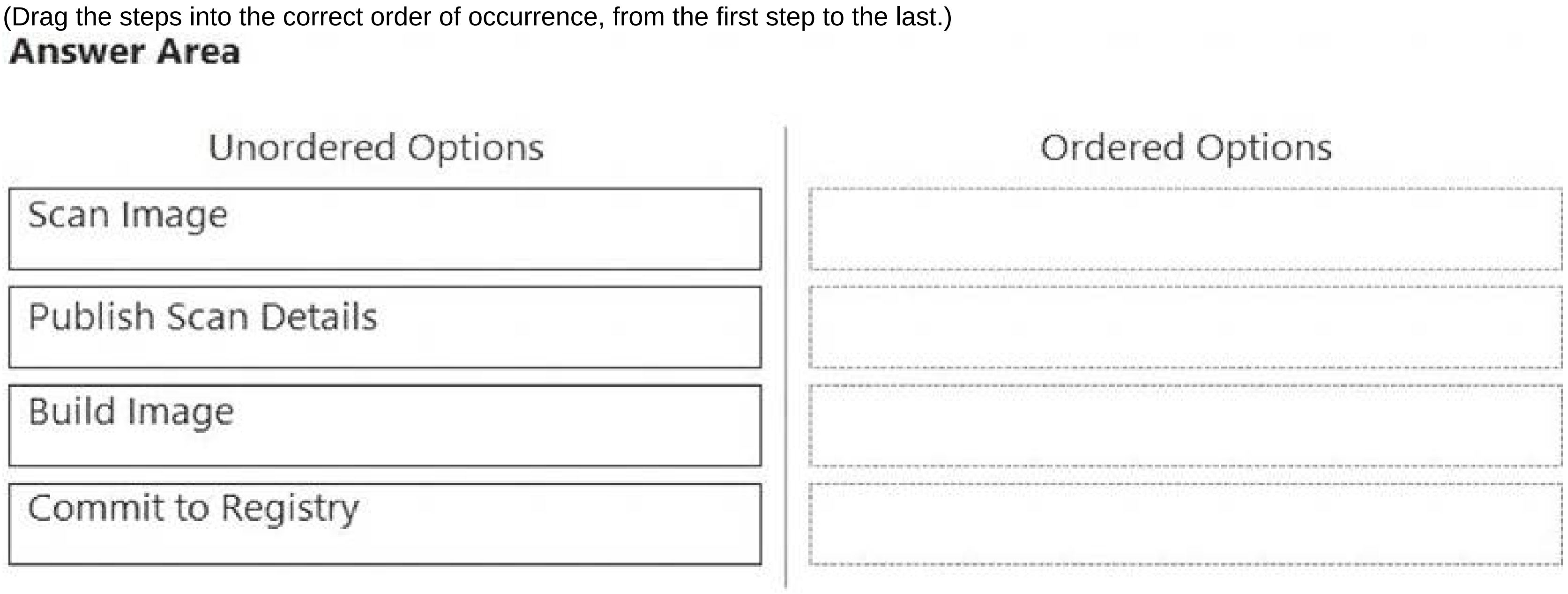
Answer: D

NEW QUESTION 23
The security team wants to protect a web application container from an SQLi attack. Which type of policy should the administrator create to protect the container?

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

Answer: A

NEW QUESTION 24
What is the order of steps in a Jenkins pipeline scan?
(Drag the steps into the correct order of occurrence, from the first step to the last.)



Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated with medium confidence

NEW QUESTION 26
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 30
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 34
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.

Answer: C

NEW QUESTION 37
The compliance team needs to associate Prisma Cloud policies with compliance frameworks. Which option should the team select to perform this task?

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

Answer: B

NEW QUESTION 41
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 46
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 49
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 51
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 54
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 55
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 59
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

Answer: CDE

NEW QUESTION 61
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 63
A customer is reviewing Container audits, and an audit has identified a cryptominer attack. Which three options could have generated this audit? (Choose three.)

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

Answer: BCD

NEW QUESTION 65
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 69
A security team has been asked to create a custom policy.
Which two methods can the team use to accomplish this goal? (Choose two.)

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

Answer: AB

NEW QUESTION 74
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 75
......

Relate Links

Contact us