Paloalto-Networks

Exam Questions PCCSE

Prisma Certified Cloud Security Engineer

NEW QUESTION 1
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

Answer: C

NEW QUESTION 2
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 3
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 4
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 5
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

Answer: BCE

NEW QUESTION 6
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 7
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 8
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 9
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 10
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

Answer: B

NEW QUESTION 10
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 13
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 17
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 21
Which statement is true regarding CloudFormation templates?

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

Answer: A

NEW QUESTION 23
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

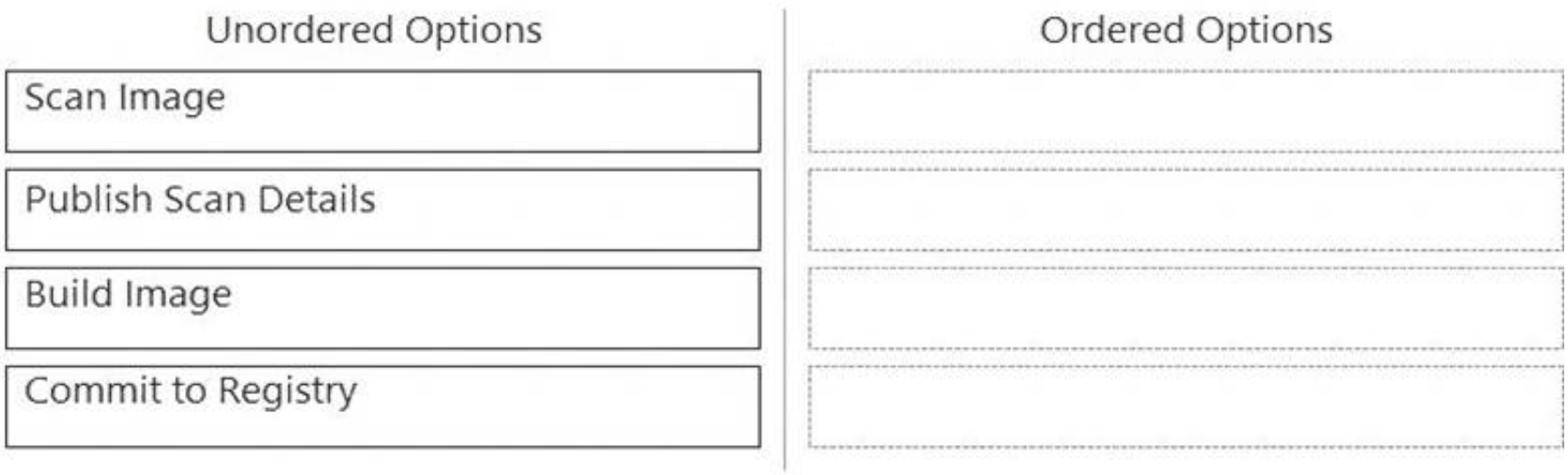
NEW QUESTION 28
Per security requirements, an administrator needs to provide a list of people who are receiving e-mails for Prisma Cloud alerts.
Where can the administrator locate this list of e-mail recipients?

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.

Answer: A

NEW QUESTION 32
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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated with medium confidence

NEW QUESTION 33
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

Answer: D

NEW QUESTION 37
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 40
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

Answer: BE

NEW QUESTION 43
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 46

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.

Answer: A

NEW QUESTION 49
Order the steps involved in onboarding an AWS Account for use with Data Security feature.
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated with medium confidence

NEW QUESTION 53
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 56
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 57
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 58
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
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 61
What is an example of an outbound notification within Prisma Cloud?

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

Answer: D

NEW QUESTION 64
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 66
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 69
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 73
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.

Answer: D

NEW QUESTION 78
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 81
.....

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